TUGAS AKHIR – KS141501

EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA APLIKASI WEB SISTEM INFORMASI MAHASISWA (STUDI KASUS: PERGURUAN TINGGI XYZ)

RAHADIYAN DANAR AJI
NRP 5212 100 124

Dosen Pembimbing
Dr. Apol Pribadi Subriadi, S.T., M.T.
Bekti Cahyo Hidayanto, S.Si., M.Kom.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT – KS141501

VULNERABILITY RISK EVALUATION USING OPEN WEB APPLICATION SECURITY PROJECT (OWASP) METHODOLOGY FOR STUDENT INFORMATION SYSTEM WEB APPLICATION (CASE STUDY : PERGURUAN TINGGI XYZ)

RAHADIYAN DANAR AJI
NRP 5212 100 124

Supervisor :
Dr. Apol Pribadi Subriadi, S.T., M.T.
Bekti Cahyo Hidayanto, S.Si., M.Kom.

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institute of Technology Sepuluh Nopember
Surabaya 2015

LEMBAR PENGESAHAN

EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA APLIKASI WEB SISTEM INFORMASI MAHASISWA (STUDI KASUS: PERGURUAN TINGGI XYZ)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

RAHADIYAN DANAR AJI
NRP. 5212 100 124

Surabaya, Januari 2016

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom
NIP.19650310 199102 1 001

LEMBAR PERSETUJUAN

EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA APLIKASI WEB SISTEM INFORMASI MAHASISWA (STUDI KASUS: PERGURUAN TINGGI XYZ)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

RAHADIYAN DANAR AJI
NRP 5212 100 124

Disetujui Tim Penguji : Tanggal Ujian: Juli 2016
Periode Wisuda: September 2016

Dr. Apol Pribadi Subriadi, S.T., M.T. **(Pembimbing I)**

Bekti Cahyo Hidayanto, S.Si., M.Kom. **(Pembimbing II)**

Hanim Maria Astuti, S.Kom, M.Sc. **(Penguji I)**

Eko Wahyu Tyas D, S.Kom, MBA **(Penguji II)**

EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA APLIKASI WEB SISTEM INFORMASI MAHASISWA (STUDI KASUS: PERGURUAN TINGGI XYZ)

Nama Mahasiswa : RAHADIYAN DANAR AJI
NRP : 5212 100 124
Jurusan : SISTEM INFORMASI FTIF-ITS
Dosen Pembimbing 1 : Dr. Apol Pribadi Subriadi, S.T., M.T.
Dosen Pembimbing 2 : Bekti Cahyo Hidayanto, S.Si., M.Kom.

ABSTRAK

Penggunaan teknologi informasi, salah satunya adalah aplikasi Sistem Informasi berbasis Web merupakan salah satu pendorong kemajuan organisasi pendidikan, dalam kasus ini adalah Perguruan Tinggi XYZ. Namun, perlu disadari bahwa dalam sebuah sistem informasi berbasis Web terdapat celah – celah keamanan yang dapat di ekploitasi melalui Internet. Eksploitasi tersebut dapat menyebabkan kerugian, baik secara materi maupun non materi.

Penelitian ini bertujuan untuk mengevaluasi keamanan dari salah satu sistem informasi berbasis Web milik Perguruan Tinggi XYZ, yaitu Sistem Informasi Mahasiswa (Simas-Online) menggunakan metodologi Web Application Penetration testing dan Risk Rating milik OWASP (Open Web Application Security Project). Metodologi Web Application Penetration Testing Versi 4 milik OWASP memiliki 11 subkategori untuk menguji keamanan dari sebuah website Secara garis besar metode yang digunakan OWASP adalah injeksi dengan menggunakan request dan response method yaitu memanfaatkan HTTP Verb untuk kemudian dilihat apakah

terdapat kerentanan yang dapat mengakibatkan dampak terhadap aplikasi.

Adapun Sistem Informasi Mahasiswa miliki PERGURUAN TINGGI XYZ yaitu SIMAS ONLINE belum pernah diuji tingkat keamanannya, sehingga dikhawatirkan akan adanya tindak eksploitasi yang merugikan Perguruan Tinggi XYZ . Dengan demikian, dapat diketahui secara lebih detil dampak dari celah keamanan yang ada, sehingga dapat dirumuskan tindakan mitigasi .

Kata Kunci : OWASP , Eksploitasi, Evaluasi keamanan sistem informasi , Penetration Testing

VULNERABILITY RISK EVALUATION USING OPEN WEB APPLICATION SECURITY PROJECT (OWASP) METHODOLOGY FOR STUDENT INFORMATION SYSTEM WEB APPLICATION
(CASE STUDY : PERGURUAN TINGGI XYZ)

Name	**:**	**RAHADIYAN DANAR AJI**
NRP	**:**	**5212 100 124**
Departement	**:**	**INFORMATION SYSTEM FTIF-ITS**
Supervisor 1	**:**	**Dr. Apol Pribadi Subriadi, S.T., M.T.**
Supervisor 2	**:**	**Bekti Cahyo Hidayanto, S.Si., M.Kom.**

ABSTRACT

The use of information technology , one of them is the information system web-based application which is now being the catalyst of the advanced educational organizations , in this case is PERGURUAN TINGGI XYZ . However , we need to realize that web-based information systems are vulnerable to exploited via internet usage by anonymous user . Exploitation may lead to losses , both material and non material .

This study aimed to evaluate the safety of a Web-based infomation systems belonging to PERGURUAN TINGGI XYZ , that called SIMAS ONLINE (Sistem Informasi Mahasiswa) using Web Application Penetration Testing and Risk Rating methodology that belong to OWASP (Open Web Application Security Project . Web Application Penetration Testing Methodology Version 4 that is belong to OWASP has 11 subtest to be tested for the security matter . The method using an injection using the request and response method , utilizing HTTP Verb to be seen whether there is a vulnerability that could result in an impact on application

In this case , the web based application called SIMAS Online that is belong to PERGURUAN TINGGI XYZ are never tested in security matter, so this system seems vulnerable for exploitation that can cause negative impact to the

PERGURUAN TINGGI XYZ . Then , by this test PERGURUAN TINGGI XYZ now can see the detail of security holes they have in the application , so that mitigation measures can be formulated

Keywords — OWASP , Exploitation , Information Security Evaluation , Penetration Testing

KATA PENGANTAR

Alhamdulillah atas karunia, rahmat, barakah, dan jalan yang telah diberikan Allah SWT selama ini sehingga penulis mendapatkan kelancaran dalam menyelesaikan tugas akhir dengan judul:

EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA APLIKASI WEB SISTEM INFORMASI MAHASISWA (STUDI KASUS: PERGURUAN TINGGI XYZ)

Terima kasih atas pihak-pihak yang telah mendukung, memberikan saran, motivasi, semangat, dan bantuan baik materi maupun spiritual demi tercapainya tujuan pembuatan tugas akhir ini. Secara khusus penulis akan menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada:

1. Mas Antok dan rekan-rekan dari PERGURUAN TINGGI XYZ yang sangat membantu dan meluangkan waktunya dalam pengumpulan data tugas akhir ini.
2. Bapak Apol dan Bapak Bekti selaku dosen pembimbing yang meluangkan waktu, memberikan ilmu, petunjuk, dan motivasi untuk kelancaran Tugas Akhir ini.
3. Bapak Tony dan Ibu Hanim selaku dosen penguji yang telah memberikan masukan untuk pengembangan tugas akhir ini.
4. Ibu Mahendrawati selaku dosen wali, terima kasih atas bimbingan yang diberikan selama penulis menjadi mahasiswa sarjana di Jurusan Sistem Informasi ITS.
5. Bapak dan Ibu orang tua penulis Serta kakak yang senantiasa mendoakan dan mendukung serta mendorong penulis untuk segera menyelesaikan Tugas Akhir ini.
6. Seluruh dosen Jurusan Sistem Informasi ITS yang telah memberikan ilmu yang sangat berharga bagi penulis.

7. Pak Hermono, selaku admin laboratoriun PPSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir.
8. Untuk Prasanti Asriningpuri yang selalu memberikan dukungan dan bantuan kepada penulis untuk dapat menyelesaikan penelitian ini.
9. Grup #hopin, #mk56, tim TA PERBANAS dan teman-teman dekat yang selalu memberikan semangat kepada penulis
10. Teman-teman organisasi mulai dari Dagri sinergi, ISE 2013, ISE 2014, IC Manage 2014 yang telah memberikan pengetahuan lebih kepada peneliti terkait kerja tim yang hebat.
11. Teman-teman SOLA12IS yang sudah menemani selama 7 semester perkuliahan, kakak-kakak FOXIS, BASILISK dan adek-adek BELTRANIS yang sudah memberikan saya pelajaran.
12. Berbagai pihak yang membantu dalam penyusunan Tugas Akhir ini dan belum dapat disebutkan satu per satu.

Penyusunan laporan ini masih jauh dari sempurna, untuk itu saya menerima adanya kritik dan saran yang membangun untuk perbaikan di masa mendatang. Semoga buku tugas akhir ini dapat memberikan manfaat pembaca

DAFTAR ISI

DAFTAR GAMBAR

(Halaman ini sengaja dikosongkan.)

DAFTAR TABEL

(Halaman ini sengaja dikosongkan.)

BAB I
PENDAHULUAN

Pada bab pendahuluan ini penulis akan menjelaskan mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat dari pembuatan tugas akhir bagi akademis dan institusi serta relevansi tugas akhir dari mata kuliah yang telah ditempuh dan penelitian sebelumnya yang telah ada.

1.1. Latar Belakang

Saat ini, perkembangan teknologi informasi dan komunikasi membawa perubahan yang sangat signifikan di berbagai bidang kehidupan manusia sehingga telah memasuki sebuah era baru yang tak pernah dibayangkan sebelumnya . Salah satu hasil dari kemajuan teknologi adalah dihasilkannya komputer sebagai alat bantu manusia dalam melakukan pekerjaan dan juga internet sebagai sarana komunikasi penghubung yang digunakan melalui komputer . [1]

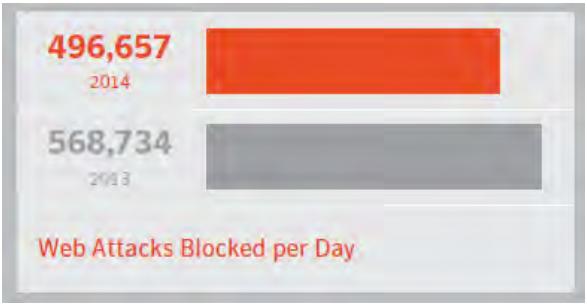
Internet sebagai salah satu dari hasil kemajuan teknologi informasi , menghasilkan banyak sekali dasar perubahan yang terjadi dalam bidang ekonomi , sosial , dan budaya . Hal ini dikarenakan internet menjadi sebuah katalis yang membuat informasi mudah tersebar dan sampai kepada seluruh penggunanya di seluruh dunia tanpa terbatas ruang dan waktu . Namun dari informasi-informasi tersebut tidak semua adalah sifatnya bebas untuk di konsumsi oleh masyarakat umum , ada juga informasi yang sifatnya adalah konfidensial dan hanya orang berwenang yang dapat mengaksesnya . Walaupun data konfidensial ini tidak boleh diakses oleh sembarang orang , tetapi data-data ini harus tetap ada untuk menunjang proses bisnis dari sebuah organisasi / instansi itu sendiri .

Data-data konfidensial tersebut lalu biasanya akan disimpan dalam sebuah storage dari aplikasi yang dilengkapi dengan keamanan dan privilege, sehingga data tersebut tetap aman dari akses yang tidak di inginkan . Tingkat keamanan ini

lah yang nantinya harus di uji untuk menentukan sejauh mana data-data konfidensial ini aman dari serangan-serangan yang datang . Dari data yang di peroleh oleh Symantec Internet Security Threat Report 2015 (ISTR) [2] terdapat 6787 Kerentanan baru yang muncul pada tahun 2013 dan 6549 pada tahun 2014 . Angka ini menunjukkan bahwa *administrator* dari aplikasi web harus terus melakukan *update* terhadap sistem keamanan yang dimiliki .

Gambar 1.1 Vulnerability baru per tahun

Yang lebih mengejutkan lagi adalah terdapat 568.734 percobaan serangan web yang digagalkan atau berhasil di blok per hari pada tahun 2013 , dan menurun menjadi 496.657 per hari di tahun 2014 . Walaupun menurun pada tahun 2014 , kondisi ini masih perlu menjadi perhatian bagi pengelola aplikasi web yang ter-*publish* di *internet* karena masih menunjukkan percobaan serangan web yang masih sangat tinggi .



Gambar 1.2 Web Attack Blocked per hari

Sebagai salah satu perguruan tinggi di Indonesia, Perguruan Tinggi XYZ telah menerapkan sistem informasi berbasis *Web*, salah satunya Sistem Informasi Mahasiswa, dalam rangka menunjang proses bisnisnya. Namun, hingga saat ini, Sistem Informasi Mahasiswa yang digunakan belum pernah diuji keamanannya. Sebagaimana telah dipaparkan sebelumnya, sebuah sistem informasi yang berbasis *Web* memiliki celah keamanan yang dapat dimanfaatkan dengan menggunakan akses *Internet*, sehingga timbul kekhawatiran akan terjadinya eksploitasi celah keamanan sistem informasi tersebut

Berangkat dari fakta yang terjadi , Perguruan Tinggi XYZ selaku client meminta mahasiswa ITS untuk melakukan evaluasi untuk aplikasi web Sistem Informasi Mahasiswa yang mereka miliki . Maka dilakukan penelitian berupa evaluasi dengan input dari pengujian celah keamanan yang disebut dengan *Penetration Testing* . *Penetration Testing* merupakan metode yang digunakan untuk mengevaluasi keamanan sistem atau jaringan komputer dengan melakukan sebuah simulasi penyerangan. Pada metodologi (Open Web Application Security Project) OWASP Web Application Security Testing difokuskan hanya pada keamanan aplikasi web, dimana prosesnya melibatkan analisis secara aktif terhadap aplikasi web, untuk menemukan kelemahan, kecacatan teknis, dan

kelemahan. Masalah-masalah keamanan yang telah ditemukan akan diberikan kepada pemilik sistem, yang disertakan dengan laporan yang berisi informasi tentang perkiraan dampak yang timbul dan juga solusi-solusi teknik untuk masalah-masalah tersebut. Penetration testing dikenal juga sebagai black box testing atau ethical hacking. Penetration testing merupakan seni dari pengujian sistem aplikasi web yang sedang berjalan, tanpa mengetahui apa yang dikerjakan di dalam aplikasi web itu sendiri. Seorang penguji berperan sebagai penyerang (attacker) dan berusaha untuk menemukan dan mengeksploitasi bagian dari aplikasi web yang memiliki sifat mudah diserang (vulnerabilities).

Dari penetration testing ini nantinya akan menjadi sebuah input yang dilanjutkan dengan metodologi berikutnya yaitu *risk rating* . Rangkaian metodologi tersebut yaitu evaluasi yang terdiri dari identifikasi risiko dan analisis risiko yang selanjutnya dapat digunakan sebagai rekomendasi dalam menentukan tindakan-tindakan yang harus dilakukan untuk membuat aplikasi memiliki tingkat keamanan tinggi dan menjaga data konfidensial yang ada di dalam nya .

1.2. Batasan Pengerjaan Tugas Akhir

Berikut ini merupakan batasan masalah pada Tugas Akhir :

1. Penelitian dilakukan pada Aplikasi web Sistem Informasi Mahasiswa Perguruan Tinggi XYZ.
2. Penelitian dilakukan dengan mengacu pada metodologi *OWASP (Open Web Application Security Project)* dengan pengujian berjenis *blackbox*
3. Tindakan pengelolaan berupa usulan solusi yang dapat dijadikan sebagai bahan pertimbangan.
4. Hasil penelitian berupa laporan tertulis.

1.3. Tujuan Tugas Akhir

Penelitian ini bertujuan untuk mengevaluasi aplikasi berbasis web Sistem Informasi Mahasiswa milik Perguruan Tinggi XYZ dari segi keamanan informasi, serta merumuskan usulan solusi untuk mengelola dampak yang dapat ditimbulkan dari eksploitasi / celah keamanan yang ditemukan .

1.4. Manfaat Tugas Akhir

Penelitian ini diharapkan dapat membantu Perguruan Tinggi XYZ dalam mengevaluasi aplikasi web Sistem Informasi Mahasiswa dari perspektif keamanan informasi. Selain itu, penelitian ini juga dapat diharapkan sebagai bahan pertimbangan dalam pengembangan institusi terkait dengan keamanan informasi, baik secara teknis maupun non teknis.

1.5. Relevansi

Usulan Tugas Akhir yang diajukan oleh penulis akan memanfaatkan ilmu pengetahuan mengenai keamanan informasi, yang telah diajarkan dalam mata kuliah Keamanan Aset Informasi (KAI) . Sehingga dapat disimpulkan bahwa Usulan Tugas Akhir yang diajukan penulis sesuai dengan ranah penelitian Sistem Informasi.

Selain relevansi dengan ranah penelitian Sistem Informasi secara umum, perlu dibuktikan adanya relevansi antara penelitian yang akan dilakukan dengan ranah penelitian yang ada pada laboratorium Manajemen Sistem Informasi (MSI), yang terletak pada Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember Surabaya. Sesuai dengan hasil sosialisasi laboratorium di Jurusan Sistem Informasi ITS pada tanggal 18 September 2015, laboratorium tempat penulis Tugas Akhir akan mengikuti dosen pembimbing 1. Adapun dosen pembimbing 1 dari penulis adalah dosen pada laboratorium Manajemen Sistem Informasi. Sehingga dapat disimpulkan

bahwa Topik Tugas Akhir yang penulis ajukan merupakan topik untuk laboratorium MSI.

1.6. Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, berikut merupakan rumusan masalah pada tugas akhir diantaranya adalah :

1. Apa saja risiko celah keamanan yang ada pada aplikasi web Sistem Informasi Mahasiswa (SIMAS)?
2. Bagaimana identifikasi risiko celah keamanan yang dapat ditimbulkan dengan adanya eksploitasi celah keamanan tersebut?
3. Bagaimana analisa risiko dari hasil identifikasi risiko yang dilakukan ?
4. Apa tindakan yang dapat dilakukan untuk mengelola dampak yang ditimbulkan dari eksploitasi celah keamanan tersebut?

BAB II
TINJAUAN PUSTAKA

Dalam penyusunan Tugas Akhir, terdapat beberapa penelitian terkait yang sebelumnya telah dilakukan oleh pihak lain. Adapun hasil – hasil penelitian tersebut akan dijadikan sebagai referensi dalam penyusunan Tugas Akhir

2.1 Penelitian Sebelumnya

Berikut ini merupakan penelitian-penelitian yang berkaitan dengan topik tugas akhir

Tabel 2.1 Penelitian Sebelumnya

Judul Penelitian	Penulis	Metodologi Penelitian yang digunakan	Isi Penelitian
Web application security vulnerabilities detection approaches: A systematic mapping study	Rafique, S.	Vulnerability Analysis & Penetration Testing	Teknik & Perangkat Pengujian Keamanan Sistem Informasi
Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology	Jai Narayan Goel & B.M. Mehtre	Vulnerability Analysis & Penetration Testing	Teknik & Perangkat Pengujian Keamanan Sistem Informasi
Vulnerability assessment of web applications - a	Vibhandik, R.	Vulnerability Analysis &	Teknik & Perangkat Pengujian Keamanan

testing approach		Penetration Testing	Sistem Informasi
Evaluation of static analysis tools for software security	AlBreiki, H.H.	Vulnerability Analysis & Penetration Testing	Teknik & Perangkat Pengujian Keamanan Sistem Informasi
OWASP Top 10 - 2013 rc1 The Ten Most Critical Web Application Security Risk	Dave Wichers , Jeff Williams , Andrew Van Der Stock	Vulnerability Analysis & Penetration Testing	Teknik & Perangkat Pengujian Keamanan Sistem Informasi

2.2 Uji Penetrasi (Penetration Testing)

Menurut Engebretson [3], *Penetration Testing* merupakan sebuah percobaan yang legal dan diijinkan untuk melakukan eksploitasi terhadap sebuah sistem dengan tujuan meningkatkan kualitas keamanan dari sistem tersebut. Dengan kata lain, *Penetration Testing* merupakan sebuah aktivitas pengujian keamanan dari sebuah sistem. Dari hasil pengujian tersebut, didapatkan sejumlah celah keamanan pada sistem yang kemudian menjadi bahan rekomendasi kepada organisasi yang memiliki sistem tersebut untuk dibenahi.

Adapun istilah *Penetration Testing* seringkali disalahartikan sebagai *Vulnerability Analysis*. Dalam *Vulnerability Analysis*, dilakukan proses pemeriksaan terhadap sebuah sistem untuk memastikan keberadaan kemungkinan celah keamanan. Sedangkan dalam proses *Penetration Testing*, dilakukan simulasi berupa penyerangan terhadap sistem layaknya dilakukan oleh seorang *hacker* untuk memastikan adanya celah keamanan tersebut. Sehingga dapat disimpulkan

bahwa *Penetration Testing* merupakan kelanjutan dari *Vulnerability Analysis*.

Secara umum, terdapat beberapa tujuan utama dari dilakukannya *Penetration Testing* sebagaimana dicatat oleh EC – Council [4] , yaitu:

- Menguji tingkat efisiensi dari proses perlindungan informasi yang dilakukan oleh organisasi
- Memberikan pandangan kepada organisasi mengenai celah keamanan sistem miliknya ketika dieksploitasi secara internal maupun eksternal
- Menyediakan informasi bagi tim pelaksana audit
- Meminimalisir biaya pelaksanaan audit keamanan
- Membantu proses prioritisasi dari organisasi untuk membenahi sistem yang diuji
- Mengetahui risiko apa saja yang ada pada sistem milik organisasi
- Mengevaluasi tingkat efisiensi perangkat yang digunakan, misalnya *firewall*, *router*, dan sebagainya
- Memberikan gambaran mengenai apa yang harus dilakukan untuk mencegah terjadinya eksploitasi
- Mengetahui apakah diperlukan pergantian ataupun pembaharuan dari infrastruktur sistem, baik *hardware* maupun *software*

Adapun terdapat beberapa metodologi yang dapat digunakan untuk melakukan *Penetration Testing*. Salah satu dari metodologi tersebut adalah OWASP (*Open Web Application Security Project*) yang akan digunakan dalam pengerjaan Tugas Akhir .

2.3 Black Box Testing

Black box testing merupakan teknik yang membutuhkan keahlian dari seorang penguji untuk melakukan penyerangan terhadap sistem. Pada skenario pengujian ini, penguji akan berperan sebagai seorang *hacker* yang melakukan penyerangan dari luar, maupun sebagai seorang *hacker* yang telah berhasil

memanfaatkan jaringan internal organisasi. Dalam pelaksanaannya, penguji tidak diberikan informasi apapun mengenai sistem yang akan diuji, baik informasi mengenai arsitektur jaringan maupun konfigurasi sistem. Proses ini dapat dilakukan dari luar maupun dari dalam wilayah dimana sistem tersebut berada.

Karena menggunakan black box testing maka nantinya prosedur uji penetrasi aplikasi pada Perguruan Tinggi XYZ akan menjadi seperti berikut :

1. Penguji melapor kepada admin Perguruan Tinggi XYZ untuk melakukan uji penetrasi
2. Admin menyiapkan space waktu untuk melakukan uji penetrasi
3. Penguji melakukan uji penetrasi pada space waktu yang telah disiapkan
4. Penguji melakukan dokumentasi terhadap penemuan celah keamanan
5. Penguji melapor kepada admin pada setiap interval waktu tertentu

2.4 Celah Keamanan

Menurut pengertian OWASP , Celah Keamanan (Vulnerability) merupakan sebuah lubang atau kelemahan pada aplikasi yang dapat muncul akibat design sistem yang buruk atau implementasi yang buruk . Lubang ini dapat mengakibatkan penyerang untuk membahayakan stakeholders dari aplikasi . Stakeholder termasuk pemilik aplikasi (Owner) , pengguna aplikasi , dan entitas lain yang bergantung pada aplikasi . Dari ada nya celah keamanan tersebut maka diperlukan mitigasi ancaman dan serangan yang dapat terjadi .

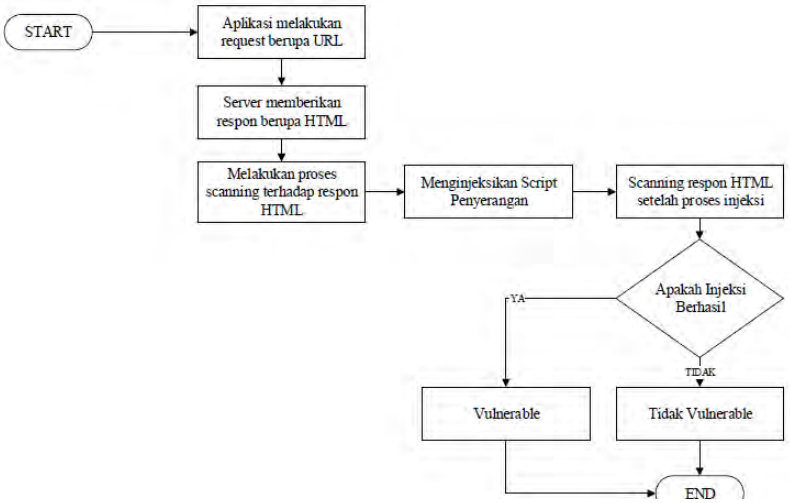
2.5 OWASP

OWASP (*Open Web Application Security Project*) merupakan organisasi/komunitas terbuka yang fokus di bidang Keamanan Aplikasi dan memiliki tujuan untuk meningkatkan *awareness* dan mengingatkan kepada setiap developer bahwa aplikasi berbasis web sebenarnya adalah tidak aman .

OWASP melakukan penelitian dan mensosialisasikan hasilnya untuk meningkatkan kesadaran akan keamanan aplikasi. OWASP memiliki beberapa project diantaranya *OWASP Web Application Penetration Testing* **,** *WebGoat, Webscarab* dan *OWASP top10*. Pada tugas akhir ini penulis akan menggunakan 2 metodologi yang dimiliki oleh OWASP yaitu Metodologi *Web Application Penetration Testing* dan *Risk Rating* .

2.6.1 Metodologi OWASP Web Application Penetration Testing

Pada *OWASP (Open Web Application Security Project) versi 4* terdapat 11 subkategori untuk menguji keamanan dari sebuah website yang disebut dengan *web application penetration testing methodology*. Secara garis besar metode yang digunakan OWASP adalah injeksi dengan menggunakan *request dan response method* yaitu memanfaatkan HTTP Verb (POST, GET, PUT, PATCH, and DELETE) untuk kemudian dilihat apakah terdapat kerentanan yang dapat mengakibatkan dampak terhadap aplikasi . Berikut adalah Flow Chart penetration testing dengan OWASP :



Gambar 2.1 Metodologi Web Application Penetration OWASP

1. Aplikasi melakukan *request* berupa *URL* ke *server*.
2. *Server* memberikan respon berupa *HTML*.
3. Aplikasi melakukan proses *scan* terhadap respon *HTML* dan menginjeksikan *script* injeksi.
4. *Server* memberikan respon berupa *HTML*.
5. Aplikasi melakukan proses *scan* terhadap respon *HTML* untuk memeriksa hasil proses injeksi.
6. Aplikasi memberikan laporan hasil proses *scan*.

Berikut adalah *Testing Guide* yang ada pada *OWASP* :

1. *Introduction and Objectives*

   Membuat tabel checklist mengenai testing yang akan dilakukan dan Mencari informasi mengenai fingerprint aplikasi seperti bahasa pemrograman yang digunakan aplikasi , dimana aplikasi di simpan , database apa yang digunakan , serta metafiles yang berisi informasi-informasi mengenai aplikasi .

   - ✓ *Testing Checklist*
   - ✓ *Information Gathering*
   - ✓ *Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)*
   - ✓ *Fingerprint Web Server (OTG-INFO-002)*
   - ✓ *Review Webserver Metafiles for Information Leakage (OTG-INFO-003)*
   - ✓ *Enumerate Applications on Webserver (OTG-INFO-004)*
   - ✓ *Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)*
   - ✓ *Identify application entry points (OTG-INFO-006)*
   - ✓ *Map execution paths through application (OTG-INFO-007)*
   - ✓ *Fingerprint Web Application Framework (OTG-INFO-008)*

- ✓ *Fingerprint Web Application (OTG-INFO-009)*
- ✓ *Map Application Architecture (OTG-INFO-010)*

2. *Configuration and Deployment Management Testing*
   Melakukan pengujian pada konfigurasi jaringan, pengujian penanganan ekstensi file, mencari backup file yang biasanya berisi informasi sensitive, pengujian http methods .
   - ✓ *Test Network/Infrastructure Configuration (OTG-CONFIG-001)*
   - ✓ *Test Application Platform Configuration (OTG-CONFIG-002)*
   - ✓ *Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)*
   - ✓ *Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)*
   - ✓ *Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)*
   - ✓ *Test HTTP Methods (OTG-CONFIG-006)*
   - ✓ *Test HTTP Strict Transport Security (OTG-CONFIG-007)*
   - ✓ *Test RIA cross domain policy (OTG-CONFIG-008)*
3. *Identity Management Testing*
   Melakukan pengujian terhadap manajemen akun yang dimiliki oleh aplikasi, seperti role dan akses aplikasi, proses registrasi user baru , dan provisioning akun.
   - ✓ *Test Role Definitions (OTG-IDENT-001)*
   - ✓ *Test User Registration Process (OTG-IDENT-002)*
   - ✓ *Test Account Provisioning Process (OTG-IDENT-003)*
   - ✓ *Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)*

- ✓ *Testing for Weak or unenforced username policy (OTG-IDENT-005)*

4. *Authentication Testing*

   Pengujian terhadap autentikasi aplikasi dengan mencari celah untuk bisa masuk sebagai user yang memiliki hak akses seperti mencari celah mekanisme pada directory traversal, backdoor yang sebelumnya dibuat, fitur lupa password / reset password .

   - ✓ *Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)*
   - ✓ *Testing for default credentials (OTG-AUTHN-002)*
   - ✓ *Testing for Weak lock out mechanism (OTG-AUTHN-003)*
   - ✓ *Testing for bypassing authentication schema (OTG-AUTHN-004)*
   - ✓ *Test remember password functionality (OTG-AUTHN-005)*
   - ✓ *Testing for Browser cache weakness (OTG-AUTHN-006)*
   - ✓ *Testing for Weak password policy (OTG-AUTHN-007)*
   - ✓ *Testing for Weak security question/answer (OTG-AUTHN-008)*
   - ✓ *Testing for weak password change or reset functionalities (OTG-AUTHN-009)*
   - ✓ *Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)*

5. *Authorization Testing*

   Pengujian terhadap otorisasi aplikasi dengan tidak menggunakan jalan masuk yang seharusnya dan tidak melakukan login untuk masuk sebagai pemilik akses, dengan memanfaatkan get dan post method http.

   - ✓ *Testing Directory traversal/file include (OTG-AUTHZ-001)*

- ✓ *Testing for bypassing authorization schema (OTG-AUTHZ-002)*
- ✓ *Testing for Privilege Escalation (OTG-AUTHZ-003)*
- ✓ *Testing for Insecure Direct Object References (OTG-AUTHZ-004)*

6. *Session Management Testing*

   Pengujian terhadap Session yang ditinggalkan oleh aplikasi yaitu cookies yang bisa dimanfaatkan untuk bisa masuk sebagai pemilik akses tanpa harus login.

   - ✓ *Testing for Bypassing Session Management Schema (OTG-SESS-001)*
   - ✓ *Testing for Cookies attributes (OTG-SESS-002)*
   - ✓ *Testing for Session Fixation (OTG-SESS-003)*
   - ✓ *Testing for Exposed Session Variables (OTG-SESS-004)*
   - ✓ *Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)*
   - ✓ *Testing for logout functionality (OTG-SESS-006)*
   - ✓ *Test Session Timeout (OTG-SESS-007)*
   - ✓ *Testing for Session puzzling (OTG-SESS-008)*

7. *Input Validation Testing*

   Pengujian terhadap validasi terhadap script yang dapat di eksekusi sehingga menyebabkan risiko yang berbahaya terhadap aplikasi seperti SQL Injection, XML Injection, CSS, dan lain-lain.

   - ✓ *Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)*
   - ✓ *Testing for Stored Cross Site Scripting (OTG-INPVAL-002)*
   - ✓ *Testing for HTTP Verb Tampering (OTG-INPVAL-003)*
   - ✓ *Testing for HTTP Parameter pollution (OTG-INPVAL-004)*

- ✓ *Testing for SQL Injection (OTG-INPVAL-005)*
- ✓ *Testing for LDAP Injection (OTG-INPVAL-006)*
- ✓ *Testing for ORM Injection (OTG-INPVAL-007)*
- ✓ *Testing for XML Injection (OTG-INPVAL-008)*
- ✓ *Testing for SSI Injection (OTG-INPVAL-009)*
- ✓ *Testing for XPath Injection (OTG-INPVAL-010)*
- ✓ *IMAP/SMTP Injection (OTG-INPVAL-011)*
- ✓ *Testing for Code Injection (OTG-INPVAL-012)*
- ✓ *Testing for Command Injection (OTG-INPVAL-013)*
- ✓ *Testing for Buffer overflow (OTG-INPVAL-014)*
- ✓ *Testing for incubated vulnerabilities (OTG-INPVAL-015)*
- ✓ *Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)*

8. *Testing for Error Handling*

   Pengujian terhadap penanganan eror yang terjadi , dari penanganan tersebut biasanya akan muncul beberapa informasi yang sifatnya credential seperti database, bugs, atau komponen-komponen yang terkait dengan aplikasi.

   - ✓ *Analysis of Error Codes (OTG-ERR-001)*
   - ✓ *Analysis of Stack Traces (OTG-ERR-002)*

9. *Testing for weak Cryptography*

   Pengujian terhadap kriptografi yang dimiliki oleh aplikasi dalam melakukan enkripsi informasi-informasi yang sifatnya adalah sensitif.

   - ✓ *Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)*

- ✓ *Testing for Padding Oracle (OTG-CRYPST-002)*
- ✓ *Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)*

10. *Business Logic Testing*

Pengujian terhadap celah yang ada pada proses bisnis aplikasi , setiap aplikasi memiliki detail logika yang berbeda-beda dalam menjalankan proses bisnis

- ✓ *Test Business Logic Data Validation (OTG-BUSLOGIC-001)*
- ✓ *Test Ability to Forge Requests (OTG-BUSLOGIC-002)*
- ✓ *Test Integrity Checks (OTG-BUSLOGIC-003)*
- ✓ *Test for Process Timing (OTG-BUSLOGIC-004)*
- ✓ *Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005)*
- ✓ *Testing for the Circumvention of Work Flows (OTG-BUSLOGIC-006)*
- ✓ *Test Defenses Against Application Mis-use (OTG-BUSLOGIC-007)*
- ✓ *Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)*
- ✓ *Test Upload of Malicious Files (OTG-BUSLOGIC-009)*

11. *Client Side Testing*

Pengujian terhadap celah yang dapat muncul pada sisi client, dengan memanfaatkan script yang dapat dijalankan dapat membahayakan client lain.

- ✓ *Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)*
- ✓ *Testing for JavaScript Execution (OTG-CLIENT-002)*
- ✓ *Testing for HTML Injection (OTG-CLIENT-003)*

- ✓ *Testing for Client Side URL Redirect (OTG-CLIENT-004)*
- ✓ *Testing for CSS Injection (OTG-CLIENT-005)*
- ✓ *Testing for Client Side Resource Manipulation (OTG-CLIENT-006)*
- ✓ *Test Cross Origin Resource Sharing (OTG-CLIENT-007)*
- ✓ *Testing for Cross Site Flashing (OTG-CLIENT-008)*
- ✓ *Testing for Clickjacking (OTG-CLIENT-009)*
- ✓ *Testing WebSockets (OTG-CLIENT-010)*
- ✓ *Test Web Messaging (OTG-CLIENT-011)*
- ✓ *Test Local Storage (OTG-CLIENT-012)*

Pada pengerjaan Tugas Akhir , penulis akan menggunakan *testing guide framework* yang dikembangan oleh OWASP. Adapun permasalahan pada biaya dapat diatasi dengan menggunakan aplikasi yang bersifat *open source*, sehingga tidak membutuhkan biaya. Sedangkan pada tahap *Penetration Testing*, penulis akan menggunakan *Black Box Testing*. Cara ini digunakan dengan pertimbangan akan kebutuhan akan adanya simulasi penyerangan sebagai seorang *hacker*. Adapun point nomor 2 yaitu *Configuration and Deployment Management Testing* tidak digunakan dalam penelitian ini karena termasuk dalam pengujian *white box* .

2.6.2 Metodologi OWASP Risk Rating

OWASP Risk Rating Methodology adalah metodologi OWASP yang digunakan sebagai proses penilaian risiko (risk assessment) dengan input hasil pengujian yang dilakukan dan hasil akhir evaluasi . Akan ada 5 tahap dalam melakukan penilaian risiko yaitu :

- Fase 1 - Mengidentifikasi risiko,
- Fase 2 - Estimasi tingkat kemungkinan risiko terjadi (Likelihood)
- Fase 3 - Estimasi tingkat pengaruh terhadap proses bisnis (Business Impact)

- Fase 4 - Menentukan nilai risiko (Severity)
- Fase 5 - Menentukan prioritas perbaikan dari risiko

Fase 1 - Mengidentifikasi risiko,

Langkah pertama yaitu mengidentifikasi risiko. Dalam mengidentifikasi risiko, perlu adanya informasi terkait jenis risiko apa saja yang mungkin terjadi, bentuk dan proses penyerangan risiko yang dapat di lakukan.

Fase 2 - Estimasi tingkat kemungkinan risiko terjadi (Likelihood)

Langkah kedua adalah menentukan faktor *likelihood*. Secara sederhana perhitungan *likelihood* dapat dilakukan dengan langsung membagi risiko ke dalam beberapa kategori yakni high, medium, low. Ada beberapa faktor yang dapat berpengaruh dalam penentuan *likelihood*, yang pertama adalah *threat agent*.:

- ***Skill Level***

  Bagaimana *technical skill* yang dimiliki oleh *threat agents* ?

Tabel 2.2 Skill Level Risk Rating

Security penetration skills (9),	Menggunakan tools yang di buat sendiri dengan menyesuaikan infrastruktur aplikasi dan off-script (diluar scenario penyerangan pada umumnya)
network and programming skills (6),	Menggunakan tools yang di buat sendiri dengan

	menyesuaikan infrastruktur aplikasi
advanced computer user (5),	Menggunakan lebih dari 1 tools dengan setting parameter
some technical skills (3),	Menggunakan 1 tools dengan setting parameter
no technical skills (1)	Menggunakan 1 tools atau sama sekali tidak menggunakan

- ***Motive***
  Bagaimana motivasi *threat agents* untuk menemukan dan membobol celah keamanan ?

Tabel 2.3 Motive Risk Rating

Low or no reward (1),	Tidak terdapat keuntungan atau keuntungan kecil
possible reward (4),	Mungkin bisa menjadi keuntungan
high reward (9)	Keuntungan besar

- ***Opportunity***
  Bagaimana kebutuhan dan peluang yang dibutuhkan *threat agents* untuk menemukan dan membobol celah keamanan ?

Tabel 2.4 Opportunity Risk Rating

Full access or expensive resources required (0),	Membutuhkan akses penuh atau membutuhkan sumber daya yang mahal
special access or resources required (4),	Membutuhkan akses special atau membutuhkan sumber daya

some access or resources required (7),	Membutuhkan beberapa akses atau membutuhkan sumber daya
no access or resources required (9)	Tidak memerlukan akses atau membutuhkan sumber daya

- ***Size***
  Seberapa besar kelompok user yang termasuk dalam *threat agents* ?

Tabel 2.5 Size Risk Rating

Developers (2),	Kategori Developer aplikasi
system administrators (2),	Kategori System Administrator
intranet users (4),	Kategori pengguna intranet
partners (5),	Kategori partner
authenticated users (6),	Kategori user yang memiliki akses
anonymous Internet users (9)	Kategori user di internet

Faktor berikutnya adalah *vulnerability factors*, dimana faktor ini dipakai untuk mengestimasi kemungkinan vulnerability ditemukan dan dipergunakan. *Vulnerability factors* juga dibagi ke dalam beberapa kriteria yakni sebagai berikut:

- ***Ease of Discover***
  Seberapa mudah kelompok *threat agents* ini dalam menemukan celah keamanan ?

Tabel 2.6 Ease of Discover Risk Rating

Practically impossible (1),	Bisa di deteksi dengan manual test (tools tidak tersedia) dan cenderung off script
difficult (3),	Bisa di deteksi dengan menggunakan lebih dari 1 tools
easy (7),	Terdapat tools yang khusus untuk mendeteksi celah keamanan
automated tools available (9)	Terdapat automated tools yang dapat mendeteksi celah keamanan

- ***Ease of Exploit***

  Seberapa mudah kelompok *threat agents* ini untuk membobol celah keamanan ?

Tabel 2.7 Ease of Exploit Risk Rating

Theoretical (1),	Bisa di bobol dengan manual test (tools tidak tersedia) dan cenderung off script
difficult (3),	Bisa di bobol dengan menggunakan lebih dari 1 tools
easy (5),	Terdapat tools yang khusus untuk membobol celah keamanan
automated tools available (9)	Terdapat automated tools yang dapat membobol celah keamanan

- ***Awareness***

Seberapa diketahuinya celah keamanan oleh kelompok *threat agents* ini ?

Tabel 2.8 Awareness Risk Rating

Unknown (1),	Tidak terdapat dalam daftar CWE (Common Weakness Enumerity)
hidden (4),	Tidak terdapat informasi mengenai cara penyerangan tetapi terdapat mitigasi pada CWE (Common Weakness Enumerity)
obvious (6),	Terdapat informasi mengenai cara penyerangan yang tidak detail dan mitigasi pada CWE (Common Weakness Enumerity)
public knowledge (9)	Terdapat informasi mengenai cara penyerangan detail dan mitigasi pada CWE (Common Weakness Enumerity)

- ***Intrusion Detection***
  Bagaimana deteksi dari pembobolan sistem ?

Tabel 2.9 Intrusion Detection Risk Rating

Active detection in application (1),	Terdeteksi sebagai penyerangan pada aplikasi
logged and reviewed (3),	Tercatat pada log dan terdapat review
logged without review (8),	Tercatat pada log namun tidak terdapat review

not logged (9)	Tidak tercatat pada log

Fase 3 - Estimasi tingkat pengaruh terhadap proses bisnis (Business Impact)

Langkah berikutnya adalah menghitung *impact* dari risiko yang ditemukan. Ada 2 jenis faktor dari *impact* yaitu *technical* dan *business impact* factor. Berikut adalah beberapa faktor dalam *technical impact* factor:

- ***Loss of Confidentiality***
  Seberapa besar data bisa yang di ungkapkan dan seberapa sensitif ?

Tabel 2.10 Loss of Confidentiality Risk Rating

Minimal non-sensitive data disclosed (2), 5	Sedikit (<2) dari data informational (berisi data informasi yang tidak *confidential*) terekspos
minimal critical data disclosed (6),	Sedikit (<2) dari data yang critical (berisi data *confidential*) terekspos
extensive non-sensitive data disclosed (6),	Banyak (>2) data informational (berisi data informasi yang tidak *confidential*) terekspos
extensive critical data disclosed (7),	Banyak (>2) data yang critical (berisi data *confidential*) terekspos
all data disclosed (9)	Seluruh data terekspos (akses penuh *CPanel administration*)

- ***Loss of Integrity***

Seberapa besar data yang bisa rusak dan seberapa besar tingkat keparahan nya ?

Tabel 2.11 Loss of Integrity Risk Rating

Minimal slightly corrupt data (1),	Sedikit (<2) dari data *corrupt* dengan tingkat ringan
minimal seriously corrupt data (3),	Sedikit (<2) dari data *corrupt* dengan tingkat berat
extensive slightly corrupt data (5),	Banyak (>2) dari data *corrupt* dengan tingkat ringan
extensive seriously corrupt data (7),	Banyak (>2) dari data *corrupt* dengan tingkat berat
all data totally corrupt (9)	Seluruh data *corrupt*

- ***Loss of Avalaibility***
  Seberapa banyak layanan yang bisa hilang dan seberapa vital ?

Tabel 2.12 Loss of Availability Risk Rating

Minimal secondary services interrupted (1),	Sedikit (<1) layanan sekunder terganggu
minimal primary services interrupted (5),	Sedikit (<1) layanan utama terganggu
extensive secondary services interrupted (5),	Banyak (>2) layanan sekunder terganggu
extensive primary services interrupted (7),	Banyak (>2) layanan utama terganggu

all services completely lost (9)	Seluruh layanan hilang

- ***Loss of Accountability***
  Apakah tindakan yang dilakukan threat agent dapat di lacak ?

Tabel 2.13 Loss of Accountability Risk Rating

Fully traceable (1),	Bisa di lacak
possibly traceable (7),	Memungkinkan untuk bisa di lacak
completely anonymous (9)	Anonim (tidak bisa di lacak)

Berikut adalah beberapa faktor dalam *business impact* factor :

- ***Financial Damage***
  Seberapa besar kerugian finansial yang dihasilkan dari pembobolan ?

Tabel 2.14 Financial Damage Risk Rating

Less than the cost to fix the vulnerability (1),	Memiliki kerugian kurang dari biaya *fixing* celah keamanan
minor effect on annual profit (3),	Memiliki kerugian kecil pada *annual profit*
significant effect on annual profit (7),	Memiliki kerugian besar pada *annual profit*
bankruptcy (9)	Kerugian yang menyebabkan kebangkrutan

- ***Reputation Damage***
  Apakah pembobolan dapat menghasilkan hilangnya reputasi yang membahayakan bisnis ?

Tabel 2.15 Reputation Damage Risk Rating

Minimal damage (1),	Kerusakan kecil
Loss of major accounts (4),	Kehilangan akun utama
loss of goodwill (5),	Kerusakan pada reputasi kinerja
brand damage (9)	Kerusakan pada nama baik

- ***Non-Compliance***
  Bagaimana pembobolan yang dilakukan terhadap jenis pelanggaran ?

Tabel 2.16 Non-Compliance Risk Rating

Minor violation (2),	Pelanggaran kecil
clear violation (5),	Pelanggaran besar dengan bukti yang jelas dan terdapat peraturan mengenai itu
high profile violation (7)	Pelanggaran besar dengan bukti yang tidak jelas dan terdapat peraturan mengenai itu

- ***Privacy Violation***
  Seberapa besar informasi personal yang dapat diungkapkan ?

Tabel 2.17 Privacy Violation Risk Rating

One individual (3),	1 orang
hundreds of people (5),	100 - 999 orang
thousands of people (7),	1000 - 1000000 orang
millions of people (9)	1000000 orang lebih

Fase 4 - Menentukan nilai risiko (Severity)

Tahap berikutnya adalah menentukan *severity* dari setiap risiko yang ditemukan dengan cara mencari rata-rata dari faktor setiap risiko. Setelah itu ditentukan levelnya melalui *likelihood and impact levels*. Setiap risiko mempunyai bobot *likelihood* dan *impact* yang berbeda, mulai dari *low,* lalu *medium*, dan yang paling tinggi adalah *high.* Gambar 2.2 menunjukkan *likelihood and impact level*.

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Gambar 2.2 Likelihood dan Impact Levels

Berikut adalah contoh dari pengisian *threat agents* dan *vulnerability factors* yang dapat mennentukan nilai *Likelihood*

Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Gambar 2.3 Threat Agents dan Vulnerability Factors

Berikut adalah contoh dari pengisian impact yang menentukan nilai masing-masing dari *Impact Levels*

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

Gambar 2.4 Technical dan Business Impact

Fase 5 - Menentukan prioritas perbaikan dari risiko

Nilai Severity yang terbesar akan menjadi prioritas dalam perbaikan (patching) , sehingga kerugian terhadap *technical* dan *financial* bisa diatasi . Untuk menentukan bagaimana nilai severity-nya adalah menggunakan tabel dibawah :

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Gambar 2.5 Overall Risk Severity

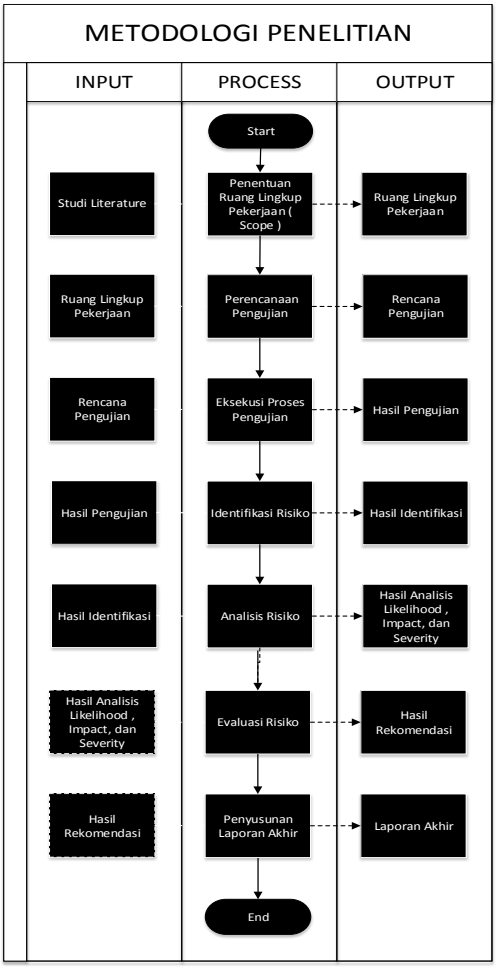
2.6 Common Weakness Enumeration (CWE)

CWE merupakan sebuah daftar yang berbentuk kamus berisi tentang celah keamanan aplikasi yang dapat terjadi dalam software architecture , design , atau code sehingga dapat memunculkan eksploitasi kerentanan keamanan . CWE diciptakan sebagai dasar dari bahasa umum yang digunakan dalam menggambarkan kelemahan perangkat lunak , dan memberikan standar dasar umum untuk identifikasi kelemahan , mitigasi , dan upaya pencegahan . CWE ditargetkan pada kedua pengembangan masyarakat dan komunitas praktisi keamanan . CWE nantinya akan digunakan penulis sebagai acuan dalam menentukan rekomendasi yang akan diberikan pada celah keamanan yang ditemukan .

Pada penentuan mitigasi nanti 1 celah keamanan akan di mapping dengan 1 kode CWE atau CAPEC (Common Attack Pattern Enumeration Classification) , CWE mewakili dari tipe dari celah keamanan yang ditemukan sedangkan CAPEC mewakili dari tipe serangan yang bisa dilakukan dalam memanfaatkan celah keamanan .

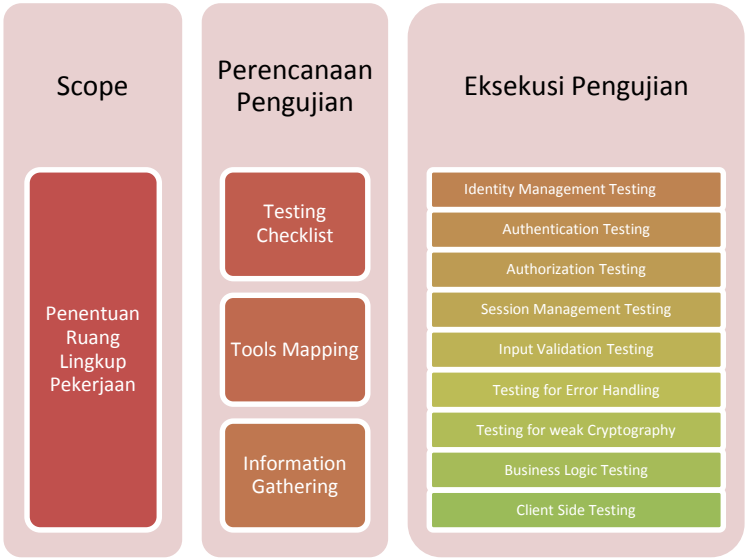
BAB III
METODOLOGI PENELITIAN

Pada bab ini penulis menjelaskan mengenai gambaran metode pengerjaan yang akan dilakukan untuk menyelesaikan penelitian tugas akhir. Bab ini akan menjadi acuan dalam pengerjaan tugas akhir agar menjadi terstruktur dan sistematis.

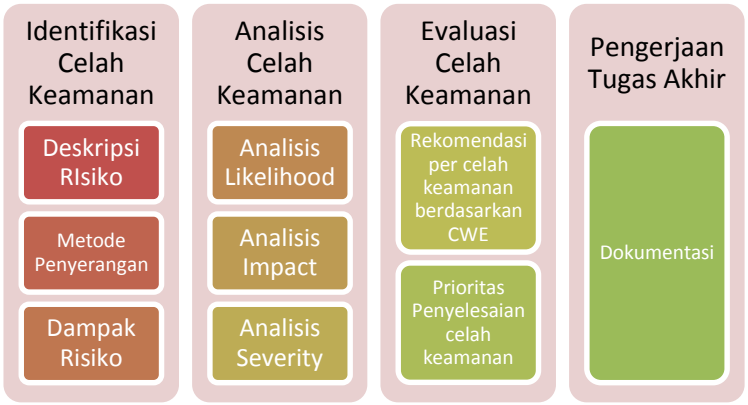


Gambar 3.1 Metodologi Penelitian

Gambar 3.2 Metodologi Penelitian 2



Gambar 3.3 Penjabaran Metodologi Penelitian



Gambar 3.4 Penjabaran Metodologi Penelitian 2

3.1 Penentuan Ruang Lingkup Pekerjaan

Menentukan ruang lingkup terhadap sistem aplikasi yang akan di uji dengan penetration attack.

3.2 Perencanaan Pengujian

- ✓ **Testing Checklist**

  Membuat daftar checklist untuk proses eksekusi pengujian yang akan dilakukan

- ✓ **Tools Mapping**

  Melakukan pemetaan terhadap tools yang akan digunakan dalam penetration testing

- ✓ **Information Gathering**

  Memulai pemeriksaan awal terhadap struktur sistem aplikasi yaitu pemeriksaan struktur *framework , network routing , port , operation system* , *web crawling* .

3.3 Eksekusi Proses Pengujian

Pengujian yang dilakukan ini adalah sebagai input untuk evaluasi celah keamanan yang akan dilakukan , tiap pengujian yang menghasilkan sebuah *findings* atau temuan celah keamanan akan di identifikasi , di analisis , dan di tentukan rekomendasi celah keamanan nya .

- ✓ **Identity Management Testing**

  Melakukan pengujian terhadap manajemen identifikasi sistem dalam menentukan user role yang memiliki level akses berbeda-beda .

- ✓ **Authentication Testing**

  Melakukan pengujian terhadap sistem otentikasi yang berlaku , seperti apa mekanisme otentikasi diterapkan dalam mengidentifikasi digital identity adalah benar atau tidak , contohnya adalah proses *log in* .

- ✓ **Authorization Testing**
  Melakukan pengujian terhadap sistem otorisasi yang berlaku , seperti apa mekanisme otorisasi diterapkan dalam memperbolehkan user untuk melakukan tindakan-tindakan tertentu sesuai dengan level akses yang dimiliki .
- ✓ **Session Management Testing**
  Melakukan pengujian terhadap manajemen session yang berlaku saat interaksi *user* dan *web-based application* berlangsung
- ✓ **Input Validation Testing**
  Melakukan pengujian dari validasi *input* yang diberikan oleh *user* , hal ini biasanya menjadi celah ketika user diperbolehkan untuk melakukan *input script* berbahaya .
- ✓ **Testing for Error Handling**
  Melakukan pengujian terhadap *Error Handling* yang ditampilkan , dari *error handling* yang muncul biasanya banyak ditemukan informasi-informasi yang berguna bagi penyerang untuk membobol celah keamanan
- ✓ **Testing for weak Cryptography**
  Melakukan pengujian terhadap *cryptography* yang diberlakukan pada sistem terhadap informasi sensitif .
- ✓ **Business Logic Testing**
  Melakukan pengujian terhadap logika proses bisnis yang diterapkan dalam sistem . Pengujian dilakukan dengan menerapkan hal-hal abnormal yang bisa menjadi celah untuk melakukan tindakan yang merugikan .
- ✓ **Client Side Testing**
  Melakukan pengujian *Client Side* , dimana hanya dilakukan eksekusi *code* pada *web browser* penguji

3.4 Identifikasi Celah Keamanan

Dari setiap celah kemanan yang ditemukan nantinya akan di identifikasi baik dari deskripsi celah keamanan , metode penyerangan yang dilakukan , dan dampak nya terhadap aplikasi

- ✓ **Deskripsi Celah Keamanan**

  Deskripsi celah keamanan akan berisi mengenai keterangan mengenai celah keamanan yang ditemukan , deskripsi ini akan mengacu pada daftar celah keamanan pada CWE (Common Weakness Enumeration) serta keterangan pada tools

- ✓ **Metode Penyerangan**

  Metode penyerangan yang dilakukan sehingga ditemukan celah keamanan dijabarkan pada bagian ini untuk memperjelas alur dari timbulnya celah keamanan

- ✓ **Dampak Celah Keamanan**

  Dampak yang terjadi dikarenakan celah keamanan yang ditemukan perlu dijelaskan sebagai bahan pertimbangan saat analisis celah keamanan

3.5 Analisis Celah Keamanan

Melakukan review terhadap celah keamanan yang ditimbulkan berdasarkan *Risk Methodology OWASP ,* akan terdiri dari 3 analisis yaitu likelihood , impact , dan severity .

- ✓ **Analisis Likelihood**

  Analisis mengenai tingkat kemungkinan terjadi nya celah keamanan akan berdasarkan pada 2 faktor yaitu *threat agents* dan *vulnerability factors*

- ✓ **Analisis Impact**

  Analisis mengenai tingkat dampak yang dihasilkan oleh celah keamanan akan berdasarkan pada 2 aspek dampak yaitu *technical* dan *business*

- ✓ **Analisis Severity**

  Tahap berikutnya adalah menentukan *severity* dari setiap celah keamanan yang ditemukan dengan cara mencari rata-rata dari faktor setiap celah keamanan. Setelah itu ditentukan levelnya melalui *likelihood and impact levels*. Setiap celah keamanan mempunyai bobot *likelihood* dan *impact* yang berbeda, mulai dari *low,* lalu *medium*, dan yang paling tinggi adalah *high*

3.6 Evaluasi Celah Keamanan

Setelah dilakukan analisis celah keamanan kemudian tahap akhir adalah menentukan rekomendasi celah keamanan yang harus dilakukan .

- ✓ **Rekomendasi per Celah Keamanan berdasarkan CWE (Common Weakness Enumeration)**

  Untuk setiap celah keamanan yang ditemukan akan di jabarkan mengenai rekomendasi tindakan yang harus dilakukan untuk meminimalkan celah keamanan yang mungkin terjadi . Rekomendasi akan mengacu pada *CWE (Common Weakness Enumeration)*

- ✓ **Prioritas Penyelesaian Celah Keamanan**

  Dengan mengacu pada nilai *severity* yang dihasilkan di setiap celah keamanan kemudian akan di urutkan sehingga di temukan prioritas yang harus diselesaikan terlebih dahulu (urgenitas)

3.7 Penyusunan Laporan Akhir

Melaporkan hasil dalam bentuk dokumen hasil akhir .

BAB IV
PERANCANGAN EVALUASI

Pada bab ini penulis akan menjelaskan mengenai perancangan melakukan evaluasi risiko celah keamanan. Tujuan dari bab perancangan ini adalah sebagai panduan dalam pengerjaan tugas akhir . Di dalam perancangan ini akan dibagi menjadi 2 sub bab yaitu perencanaan pengujian yang nantinya akan disiapkan sebelum melakukan eksekusi dari pengujian celah keamanan dan sub bab mengenai perancangan evaluasi yang dilakukan setelah adanya output dari hasil pengujian . Hasil akhir dari seluruh pengujian dan evaluasi ini akan di dokumentasikan dalam sebuah dokumen yaitu security assessment report .

4.1 Perencanaan Pengujian

Dalam perencanaan pengujian dilakukan persiapan untuk membantu proses pengujian yaitu dengan membuat testing checklist , tools mapping , dan pengumpulan informasi .

4.1.1 Testing Checklist

Testing checklist dibuat dengan berdasarkan metodologi *Web Application Penetration Testing* yang dibuat oleh OWASP , karena pengujian nanti adalah menggunakan black box testing (PERGURUAN TINGGI XYZ tidak memberikan hak akses admin) akan ada beberapa testing yang perlu dihilangkan . Checklist harus di perbarui setiap kali penguji melakukan pengujian celah keamanan , template untuk tabel checklist adalah sebagai berikut :

Tabel 4.1 Template tabel checklist

Test ID	Test Name	Status	Remark

Terdapat kolom Test ID , Test Name , Status , dan Remark .

- Test ID : Di isi sesuai dengan kode yang ada pada testing guide framework
- Test Name : Di isi sesuai dengan nama pengujian yang ada pada testing guide framework
- Status : Status dibagi menjadi 3 yaitu OK , On Progress , Not OK . OK apabila pengujian telah selesai dilakukan , On Progress apabila pengujian sedang dilakukan , dan Not OK apabila terjadi kendala dalam melakukan pengujian (status Not OK wajib mengisi remark).
- Remark : Di isi dengan keterangan tambahan ketika melakukan pengujian .

4.1.2 Tools Mapping

Pada testing guide framework disebutkan banyak sekali tools-tools yang dapat digunakan dalam melakukan pengujian , namun untuk mempermudah proses pengujian dilakukan pemetaan terhadap tools-tools tersebut sehingga tools digunakan tepat sasaran sesuai dengan sub pengujian yang akan dilakukan . Keseluruhan pemetaan tools ini adalah merupakan rekomendasi dari testing guide framework OWASP , dan mayoritas dari tools ini adalah merupakan hasil aplikasi yang dikembangkan oleh OWASP sendiri . Berikut adalah template tabel pemetaan tools :

Tabel 4.2 Template tools mapping

Test ID	Nama Pengujian	TOOLS

Terdapat kolom Test ID , Nama Pengujian , dan Tools

- Test ID : Di isi sesuai dengan kode yang ada pada testing guide framework
- Nama Pengujian : Di isi sesuai dengan nama pengujian yang ada pada testing guide framework
- Tools : Daftar tools yang akan digunakan pada sub pengujian, untuk beberapa pengujian yang tidak memerlukan tools akan di isi "Menggunakan pengujian manual"

4.1.3 Information Gathering

Dalam menyelesaikan penelitian tugas akhir ini diperlukan berbagai macam informasi mengenai aplikasi sistem informasi yang dimiliki oleh PERGURUAN TINGGI XYZ. Informasi tersebut akan digunakan untuk membantu peneliti dalam mempermudah pencarian celah keamanan. Berikut ini merupakan informasi yang akan di kumpulkan oleh peneliti :

1. Pencarian kebocoran informasi pada search engine
2. Webserver metafiles
3. Informasi mengenai webserver (WHOIS dan Subdomain)
4. Fingerprint dari aplikasi web
5. Arsitektur dari aplikasi web

Setiap temuan informasi kemudian di dokumentasikan dalam bagian sub bab information gathering pada laporan .

4.2 Perencanaan Identifikasi Celah Keamanan

Setelah pengujian dilakukan , setiap temuan atau *findings* dilaporkan dalam sebuah tabel identifikasi celah keamanan . Identifikasi celah keamanan ini yang nantinya akan di analisis dan memunculkan sebuah evaluasi untuk perbaikan dari aplikasi sistem informasi mahasiswa milik Perguruan Tinggi XYZ .

4.2.1. Tabel Deskripsi Celah Keamanan dan Metode Penyerangan

Sebelum mengidentifikasi celah keamanan yang ditemukan maka perlu di buat terlebih dahulu dokumentasi pengujian yang telah dilakukan sehingga sampai menemukan celah . Dokumentasi deskripsi celah dan metode penyerangan yang dilakukan di masukkan ke dalam tabel berikut :

Test ID	
Vuln ID	
Deskripsi	
URL	
Attack	

- Test ID : Di isi sesuai dengan kode yang ada pada testing guide framework
- Vulnerability ID : Di isi sesuai dengan Vulnerability ID yang ditentukan oleh peneliti , untuk memudahkan penomoran dari celah keamanan.
- Deskripsi : Di isi dengan deskripsi yang akan dijelaskan secara umum (general) dan mengacu pada CWE
- URL : Di isi dengan URL yang berhubungan dengan pengujian yang dilakukan
- Attack : Di isi dengan dokumentasi dari penyerangan yang dilakukan sampai dengan mendapatkan hasil celah keamanan

4.2.2. Tabel Risiko , CIA dan Dampak Bisnis

CIA Triad dibagi ke dalam 3 kategori yaitu Confidentiality, Integrity, dan Availability. Kategori tersebut dilihat dari areanya adalah sebagai berikut :

1. Confidentiality

Memastikan bahwa informasi dapat diakses hanya kepada mereka berwenang untuk mengaksesnya

2. **Integrity**
   Memastikan bahwa informasi tersebut akurat dan lengkap dan bahwa informasi tidak diubah tanpa izin
3. **Availability**
   Memastikan bahwa informasi tersebut dapat diakses oleh pengguna yang berwenang ketika dibutuhkan oleh pengguna

Template tabel risiko, CIA, dan dampak bisnis adalah sebagai berikut :

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak

- Vulnerability ID : Di isi sesuai dengan Vulnerability ID yang ditentukan oleh peneliti , untuk memudahkan penomoran dari celah keamanan.
- Nama Celah : Di isi sesuai dengan nama celah keamanan yang ditemukan
- Risiko : Di isi dengan risiko yang muncul dari celah keamanan yang ditemukan
- CIA : Di isi dengan CIA TRIAD (Confidentiality, Integrity, Availability) dan kemudian dijelaskan sesuai dengan CIA yang muncul
- Dampak : Di isi dengan dampak yang dihasilkan dari celah keamanan dari sisi bisnis

4.2.3. Tabel Dampak Teknikal dan Penyebab

Setelah diketahui deskripsi dan metode penyerangan yang dapat dilakukan maka dapat di identifikasi mengenai risiko , dampak dan penyebab yang muncul dari celah keamanan. Template tabel dampak teknikal dan penyebab tersebut adalah sebagai berikut :

Tabel 4.3 Tabel Dampak dan Penyebab

No	Vulnerability ID	Nama Celah	Dampak	Penyebab

- Vulnerability ID : Di isi sesuai dengan Vulnerability ID yang ditentukan oleh peneliti , untuk memudahkan penomoran dari celah keamanan.
- Nama Celah : Di isi sesuai dengan nama celah keamanan yang ditemukan
- Dampak : Di isi dengan dampak yang dihasilkan dari celah keamanan
- Penyebab : Di isi dengan penyebab sehingga celah keamanan bisa terjadi

4.3 Perencanaan Analisis Celah Keamanan

Setiap celah keamanan yang ditemukan akan di analisis melalui 3 aspek yaitu berdasarkan *Likelihood , Impact , dan Severity* berdasarkan dampak dan penyebab yang telah di identifikasi sebelumnya . Secara lengkap adalah dijabarkan dibawah :

- **Analisis Likelihood**
  Analisis mengenai tingkat kemungkinan terjadi nya celah keamanan akan berdasarkan pada 2 faktor yaitu *threat agents* dan *vulnerability factors*

- **Analisis Impact**
  Analisis mengenai tingkat dampak yang dihasilkan oleh celah keamanan akan berdasarkan pada 2 aspek dampak yaitu *technical* dan *business*

- **Analisis Severity**
  Tahap berikutnya adalah menentukan *severity* dari setiap celah keamanan yang ditemukan dengan cara mencari rata-rata dari faktor setiap celah keamanan. Setelah itu ditentukan levelnya melalui *likelihood and impact levels*. Setiap celah keamanan mempunyai bobot *likelihood* dan *impact* yang berbeda, mulai dari *low,* lalu *medium*, dan yang paling tinggi adalah *high*

4.3.1 Tabel Analisis Celah Keamanan

Tabel Analisis Celah Keamanan akan dibagi menjadi 2 bagian penilaian yaitu dari aspek *factors* dan *impact* . Threat Agent Factor dan Vulnerability Factor adalah bagian penilaian factors , sedangkan Technical Impact dan Business Impact adalah bagian penilaian Impact . Setiap 1 vulnerability akan memiliki 2 bagian penilaian tadi yaitu berdasarkan nilai faktor-faktor terjadinya celah keamanan dan nilai berdasarkan akibat yang ditimbulkan ketika celah keamanan di eksploitasi . Masing-masing bagian akan di hitung nilai overall dengan cara mencari nilai *mean* dari penilaian yang telah dilakukan .
Dibawah adalah tabel penilaian bagian factors, *Threat agent factors* memiliki sub factors didalamnya yaitu *Skill Level , Motive , Opportunity , dan Size* . Sedangkan *Vulnerability Factors* memiliki sub factors *Ease of Discovery , Ease of Exploit , Awareness , dan Intrussion Detection* . Penilaian akan mengacu pada metodologi OWASP Risk Rating .

Tabel 4.4 Factors Risk Rating

Threat Agent Factors			
Skill Level	Motive	Opportunity	Size
Vulnerability Factors			
Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
Overall Likelihood =			

Sedangkan dibawah ini adalah tabel penilaian bagian impact , Technical Impact memiliki sub impact di dalamnya yaitu Loss of confidentiality , Loss of Integrity , Loss of Availability , Loss of Accountability . Serta Business Impact memiliki sub impact yaitu Financial Damage , Reputation Damage , Non-compliance , dan Privacy Violation .

Tabel 4.5 Impact Risk Rating

Technical Impact			
Loss of Confidentiality	Loss of Integrity	Loss of availability	Loss of accountability
Business Impact			
Financial Damage	Reputation Damage	Non-compliance	Privacy violation
Overall Likelihood =			

BAB V
IMPLEMENTASI

Bab ini menjelaskan hasil dari implementasi perancangan studi kasus. Yang akan dijelaskan oleh penulis adalah hasil implementasi dari perancangan yang sebelumnya telah dibuat .

5.1 Pengujian

5.1.1 Persiapan

Pada tahap ini dilakukan persiapan dalam melakukan eksekusi pengujian yaitu membuat checklist yang mengacu pada metodologi *OWASP Web Application Penetration Testing* . Pada metodologi telah di jabarkan mengenai 11 tahapan testing namun beberapa sub tahapan akan dihilangkan dari checklist dikarenakan penelitian dibatasi hanya dari luar sistem admin atau simulasi penyerangan dari *anonymous user* . Persiapan pertama adalah mempersiapkan tabel *Testing Checklist* , Kolom **Test ID** dan **Test Name** adalah daftar test yang harus dilakukan tester dalam pelaksanaan pengujian ke depan , dan *Testing checklist* harus selalu di update setiap kali tester melakukan *sub test* dengan mengisi kolom **Status** dan **Remark**. Testing checklist akan memudahkan tester untuk memahami progress yang dilakukan saat eksekusi pengujian dan permasahalan yang terjadi .

Tabel 5.1 Testing checklist

Test ID	Test Name	Status	Remark
OTG-IDENT	**Identity Management Testing**		
OTG-IDENT-001	Test Role Definitions	OK	

OTG-IDENT-002	Test User Registration Process	OK	
OTG-IDENT-003	Test Account Provisioning Process	OK	
OTG-IDENT-004	Testing for Account Enumeration and Guessable User Account	OK	
OTG-IDENT-005	Testing for Weak or unenforced username policy	OK	
OTG-IDENT-006	Test Permissions of Guest/Training Accounts	OK	
OTG-IDENT-007	Test Account Suspension/Resumption Process	OK	

Untuk Testing Checklist yang lengkap terdapat pada lampiran A.

Berikutnya tester perlu mempersiapkan tools mapping sebagai penanda bahwa testing telah dilakukan dengan tools-tools yang sudah di rencanakan sebelumnya. Tools Mapping akan memudahkan tester dalam melakukan eksekusi nanti, tools yang digunakan juga akan mengacu pada metodologi OWASP Web Application Penetration Testing , namun tidak semua tools dipakai dan yang akan digunakan saja yang akan di list dalam tools mapping. Pemilihan tools akan disesuaikan dengan studi kasus yang diberikan .

Tabel 5.2 Tools Mapping

Test ID	Nama Pengujian	TOOLS
OTG-IDENT	**Identity Management Testing**	
OTG-IDENT-001	Test Role Definitions	Spidering Tools
OTG-IDENT-002	Test User Registration Process	HTTP Proxy
OTG-IDENT-003	Test Account Provisioning Process	HTTP Proxy
OTG-IDENT-004	Testing for Account Enumeration and Guessable User Account	WebScarab , CURL , PERL , Sun Java Access and Identity Manager users enumeration tools
OTG-IDENT-005	Testing for Weak or unenforced username policy	Menggunakan Manual Script atau Manual Test

Diatas adalah cuplikan tools mapping yang akan digunakan pada pengujian aplikasi Sistem Informasi Mahasiswa milik PERGURUAN TINGGI XYZ. Untuk Tools mapping yang lengkap terdapat pada lampiran A.

Tahap perencanaan yang terakhir adalah melakukan *Information Gathering*, tujuan dari information gathering adalah sebagai bekal informasi tester mengenai struktur yang dimiliki aplikasi. Dengan mengetahui struktur aplikasi akan

lebih mudah dalam melakukan eksekusi pengujian. Kegiatan Information Gathering adalah terdiri dari :

1. *Conduct Search Engine Discovery and Reconnaissance for Information Leakage*, yaitu melakukan penggalian informasi dari eksplorasi Search Engine. Search Engine biasanya menyimpan informasi-informasi penting terkait aplikasi yang seharusnya dibatasi untuk kepentingan keamanan .
2. *Review Webserver Metafiles for Information Leakage,* yaitu melakukan pencarian terhadap metafiles webserver yang terkadang bisa di akses oleh *anonymous user*. Biasanya adalah dengan mengakses robots.txt yang berisi metafiles webserver.
3. *Enumerate Applications on Webserver*, yaitu dengan melakukan penggalian informasi aplikasi yang ada di webserver dengan menggunakan *WHOIS* dan mencari *subdomain* apa saja yang dimiliki webserver selain *subdomain* target.
4. *Fingerprint Web Application,* yaitu dengan melakukan penggalian informasi mengenai fingerprint aplikasi web, seperti programming language yang digunakan atau framework yang digunakan .
5. *Map Application Architecture*, yaitu dengan melakukan penggalian informasi dari arsitektur aplikasi seperti informasi port dan network routing.

   Hasil dari information gathering yang dihasilkan untuk studi kasus PERGURUAN TINGGI XYZ ada pada lampiran A.

   Setelah perencanaan semua disiapkan langkah selanjutnya adalah melakukan eksekusi pengujian.

5.1.2 Eksekusi

Tahapan dalam melakukan eksekusi pengujian akan bervariasi sesuai dengan sub test yang dilakukan (mengacu pada testing

checklist) . Setiap test adalah menggunakan metodologi test seperti dibawah :

Penjelasan dari metode diatas adalah seperti dibawah :

1. Aplikasi melakukan *request* berupa *URL* ke *server*.
2. *Server* memberikan respon berupa *HTML*.
3. Aplikasi melakukan proses *scan* terhadap respon *HTML* dan menginjeksikan *script* injeksi.
4. *Server* memberikan respon berupa *HTML*.
5. Aplikasi melakukan proses *scan* terhadap respon *HTML* untuk memeriksa hasil proses injeksi.
6. Aplikasi memberikan laporan hasil proses *scan*.

Dibawah ini akan di jelaskan beberapa eksekusi pengujian yang dilakukan sampai dengan didapatkan nya vulnerable dengan menggunakan metode diatas .

5.1.2.1 XSS

a. Dengan melakukan *Spidering* aplikasi lalu melakukan test Request dan Response di modul *OWASP ZAP* didapatkan vulnerable URL dengan celah keamanan XSS, tester melakukan script injeksi XSS kepada aplikasi saat melakukan pengujian dan memberikan respon HTML yang positif terhadap vulnerable . Berikut adalah URL yang vulnerable :

   - /form/perpus/katalog/buku/report_buku_detail.php
   - /form/perpus/katalog/ta_lkp/report_ta_lkp_detail.php

b. Hasil test yang dilakukan mengeluarkan output vulnerability seperti berikut

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Dan HTML Responsenya adalah seperti dibawah :

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.1 HTML Response XSS

c. Dengan celah ini penyerang bisa memanipulasi tampilan yang ada dengan memanfaatkan *cross site scripting* , dimana script berbahaya yang di injeksi melalui URL akan di proses oleh web browser menjadi output yang bisa mengelabui user .

5.1.2.2 SQL Injection

a. Dengan melakukan *Spidering* aplikasi lalu melakukan test Request dan Response di modul *OWASP ZAP* didapatkan vulnerable URL dengan celah keamanan SQL Injection, tester melakukan script injeksi SQL Injection kepada aplikasi saat melakukan pengujian dan memberikan respon HTML yang positif terhadap vulnerable . Berikut adalah URL yang vulnerable :

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

b. Hasil test yang dilakukan mengeluarkan output vulnerability seperti dibawah :

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Dan HTML Response nya adalah seperti berikut :

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

c. Dengan menggunakan SQLMap ditemukan username dan password yang bisa digunakan untuk masuk ke dalam administrator aplikasi

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.2 Hasil SQL Injection di SQLMap

5.1.2.3 HTTP Verb Tampering

a. Untuk melakukan serangan ini , penyerang harus memiliki sebuah akun salah satu mahasiswa , karena fitur upload ini hanya dapat diakses ketika user sudah log in sebagai user mahasiswa Perguruan Tinggi XYZ
b. Buka menu softskill, pada modul ini terdapat form upload di bagian dokumen pendukung . Disinilah vulnerability untuk HTTP Verb Tampering

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.3 HTTP Verb Tampering 1

c. Tester melakukan percobaan dalam melakukan upload file berjenis php , namun ternyata sistem telah mengantisipasinya dengan membatasi jenis tipe file yang bisa di upload

d. Tester kemudian melakukan tampering tipe data yang tadinya jpg menjadi php menggunakan add on firefox *Open Tamper Data* lalu mengupload *malicious file* (backdoor) pada form upload yang disediakan . Backdoor yang tester gunakan adalah shell b374k dengan fitur yang dapat membahayakan aplikasi .

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.4 HTTP Verb Tampering 2

e. Upload berhasil dilakukan dan menampilkan output seperti dibawah

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.5 HTTP Verb Tampering 3

f. Cari path menuju file yang di upload tersebut dan melakukan request kepada URL web browser biasa .

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.6 HTTP Verb Tampering 4

g. Hasilnya Backdoor file yang diupload dapat di akses dan dapat digunakan untuk membobol aplikasi

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Gambar 5.7 HTTP Verb Tampering 5

5.1.3 Dokumentasi

Setiap hasil celah keamanan yang diperoleh dalam melakukan pengujian di dokumentasikan seperti contoh diatas , dijelaskan secara bertahap mengenai cara melakukan pengujian hingga ditemukan nya celah keamanan , hasil dokumentasi ini nantinya akan di masukkan ke dalam tabel identifikasi celah keamanan untuk membantu administrator dalam melakukan mitigasi .

5.2 Identifikasi Celah Keamanan

Identifikasi celah keamanan akan di tampilkan dalam 3 tabel yaitu pada tabel Deskripsi Celah keamanan dan Metode penyerangan , tabel Risiko dan Dampak Bisnis berbasis CIA TRIAD , serta tabel dampak dan penyebab.

5.2.1 Deskripsi Celah Keamanan dan Metode Penyerangan

Pada tabel identifikasi celah keamanan perlu di jabarkan secara detail mengenai celah keamanan yang ditemukan , deskripsi akan dijelaskan secara umum (general) Semua deskripsi ini akan mengacu pada CWE (Common Weakness Enumeration) . Sedangkan Metode penyerangan adalah diambil dari dokumentasi yang dihasilkan pada tahap pengujian .

5.2.2 Risiko , CIA , dan Dampak Bisnis

Dari celah keamanan tersebut kemudian dilakukan identifikasi risiko, CIA, dan dampak bisnis yang ditimbulkan dan ditampilkan dalam sebuah tabel yaitu tabel risiko, CIA, dan dampak bisnis . Risiko adalah memuat risiko yang bisa saja terjadi dengan adanya celah keamanan , beserta dengan penjelasan dari masing-masing nilai CIA tersebut , dan yang terakhir adalah dampak bisnis yang mungkin terjadi dari CIA yang muncul . CIA TRIAD adalah mencakup Confidentiality , Integrity , dan

Availability . Confidentiality adalah Memastikan bahwa informasi dapat diakses hanya kepada mereka berwenang untuk mengaksesnya , Integrity adalah Memastikan bahwa informasi tersebut akurat dan lengkap dan bahwa informasi tidak diubah tanpa izin, dan Availability adalah Memastikan bahwa informasi tersebut dapat diakses oleh pengguna yang berwenang ketika dibutuhkan oleh pengguna

Berikut adalah tabel Risiko, CIA, dan Dampak Bisnis berbasis CIA TRIAD yang ditampilkan pada tabel 5.3 dibawah :

Tabel 5.3 Risiko, CIA, dan Dampak Bisnis

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
1	*(OTG-AUTHZ-001) - 01*	*Directory Traversal*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya penyalahgunaan akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan , perampokan , penipuan , pemerasan , dan sebagainya
			Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan source code sehingga aplikasi memperbolehkan untuk memanipulasi fitur pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
2	*(OTG-AUTHZ-004) - 01*	*Directory Listing and Information Disclosure*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan , perampokan , penipuan , pemerasan , dan sebagainya
			Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan source code sehingga aplikasi memperbolehkan untuk memanipulasi fitur pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
3	*(OTG-AUTHZ-004) - 02*	*Possible Server Path Disclosure*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan ,

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
					perampokan , penipuan , pemerasan , dan sebagainya
			Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan source code sehingga aplikasi memperbolehkan untuk memanipulasi fitur pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
4	*(OTG-AUTHZ-004) - 03*	*Source Code Disclosure*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan ,

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
					perampokan , penipuan , pemerasan , dan sebagainya
			Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan source code sehingga aplikasi memperbolehkan untuk memanipulasi fitur pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
5	*(OTG-AUTHZ-004) - 04*	*Possible Sensitive Files*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan ,

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
					perampokan , penipuan , pemerasan , dan sebagainya
			Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan source code sehingga aplikasi memperbolehkan untuk memanipulasi fitur pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
6	*(OTG-SESS-005)- 01*	*Cross Site Request Forgery*	Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
				memanipulasi fitur pada aplikasi	- Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
			Manipulasi Informasi pada content aplikasi	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk memanipulasi informasi content alikasi pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
7	*(OTG-INPVAL-001) - 01*	*Cross Site Scripting*	Manipulasi fitur yang mengakibatkan pembobolan data user	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk memanipulasi fitur pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
			Manipulasi Informasi pada content aplikasi	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk memanipulasi informasi content alikasi pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
8	*(OTG-INPVAL-003) - 01*	*HTTP Verb Tampering*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan , perampokan , penipuan , pemerasan , dan sebagainya

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
			Web deface (mengganti tampilan dari web) yaitu perubahan source code sehingga menipu para user yang mengakses web	Availability : Adanya Web Deface yang melakukan manipulasi aplikasi sehingga aplikasi menjadi down / tidak bisa diakses	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik
			Manipulasi Informasi pada content aplikasi	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk memanipulasi informasi content alikasi pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
			Pembobol sengaja menghapus seluruh data confidential	Availability : Terjadinya system yang corrupt akibat data confidential yang di perlukan di hapus	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik
9	*(OTG-INPVAL-005) - 01*	*SQL Injection*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan , perampokan , penipuan , pemerasan , dan sebagainya
			Web deface (mengganti tampilan dari web) yaitu perubahan source code	Availability : Adanya Web Deface yang melakukan manipulasi aplikasi sehingga	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
			sehingga menipu para user yang mengakses web	aplikasi menjadi down / tidak bisa diakses	- Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik
			Manipulasi Informasi pada content aplikasi	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk memanipulasi informasi content alikasi pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
			Pembobol sengaja menghapus seluruh data confidential	Availability : Terjadinya system yang corrupt akibat data confidential yang di perlukan di hapus	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik
10	*(OTG-INPVAL-016) - 01*	*HTTP Response Splitting*	Kerusakan pada fitur Aplikasi	Availability : Terjadinya kerusakan akibat system yang corrupt karena adanya malicious script	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
11	*(OTG-ERR-001) - 01*	*Error Messages on page*	Kerusakan pada fitur Aplikasi	Availability : - Terjadinya kerusakan akibat system yang corrupt karena adanya malicious script	Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik
12	*(OTG-BUSLOGIC-009) - 01*	*File Upload All Files*	Pencurian data-data bersifat confidential baik dari data user , data institusi , dan lain nya	Confidentiality : Adanya kebocoran akses pada web server administrator	- Kerugian yang mengganggu jalan nya operasional layanan - Kerugian user layanan ketika data pribadinya disalahgunakan baik untuk kejahatan , perampokan , penipuan , pemerasan , dan sebagainya
			Web deface (mengganti tampilan dari web) yaitu perubahan source code sehingga	Availability : Adanya Web Deface yang melakukan manipulasi aplikasi sehingga aplikasi menjadi	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
			menipu para user yang mengakses web	down / tidak bisa diakses	
			Manipulasi Informasi pada content aplikasi	Integrity : Adanya kesalahan sehingga aplikasi memperbolehkan untuk memanipulasi informasi content alikasi pada aplikasi	- Nama baik Perguruan Tinggi XYZ yang tercoreng akibat adanya penyalahgunaan data user dan muncul whistleblower akibat kejadian tersebut - Berkurangnya kepercayaan user terhadap pihak Perguruan Tinggi XYZ
			Pembobol sengaja menghapus seluruh data confidential	Availability : Terjadinya system yang corrupt akibat data confidential yang di perlukan di hapus	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik

No	Vulnerability ID	Nama Celah	Risiko	CIA	Dampak
13	*(OTG-CLIENT-005)- 01*	*Old Jquery*	Kerusakan pada fitur Aplikasi	Availability : Terjadinya kerusakan akibat system yang corrupt karena adanya malicious script	- Kerugian yang dirasakan user karena tidak dapat melakukan layanan akademik - Berkurangnya loyalitas user dalam tetap menggunakan layanan akademik

5.2.3 Dampak Teknikal dan Penyebab

Langkah terakhir untuk melakukan identifikasi celah keamanan adalah dengan mengetahui dampak dan penyebab terkait celah keamanan yang ditemukan , berikut adalah tabel dampak dan penyebab :

Tabel 5.4 Dampak dan Penyebab

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
1	*(OTG-AUTHZ-001) - 01*	*Directory Traversal*	Memperbolehkan untuk mengakses restricted directories	Ada nya path traversal yang rentan karena special element yang tidak dibatasi oleh administrator aplikasi , seperti special element separator ".." dan "/" sehingga penyerang dapat mengakses file sensitif seperti "/usr/local/bin" .
			Melihat directories yang ada di web server	
			Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
2	*(OTG-AUTHZ-004) - 01*	*Directory Listing and Information Disclosure*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan Kebocoran struktur dan isi directories aplikasi	Listing Directory yang memperbolehkan penyerang untuk melihat dan membuka seluruh index dari seluruh isi direktori . Risiko dan konsekuensi yang terjadi akan bergantung pada files yang terekspos dan accessible
3	*(OTG-AUTHZ-004) - 02*	*Possible Server Path Disclosure*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan	Adanya kesalahan konfigurasi pada file PHP pada aplikasi sehingga muncul path sensitif yang merujuk pada informasi server

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
			Kebocoran struktur dan isi directories aplikasi	
4	*(OTG-AUTHZ-004) - 03*	*Source Code Disclosure*	Memberikan informasi struktur source code (string koneksi database atau logika kode) yang sensitif untuk mempermudah penyerangan	Terdapat source code yang bersifat readable/accessible oleh user dan berisi informasi sensitif mengenai logika yang dapat menjadi petunjuk bagi penyerang .
5	*(OTG-AUTHZ-004) - 04*	*Possible Sensitive Files*	Memberikan informasi yang bisa saja berbahaya seperti password files , configuration files , log files , database dumps dan file konfigurasi lain nya yang sensitif untuk mempermudah penyerangan	Aplikasi menyimpan data sensitif pada web document root dengan access control yang tidak cukup baik , yang mengakibatkan dapat di akses oleh untrusted user

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
6	*(OTG-SESS-005)- 01*	*Cross Site Request Forgery*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	Web server di desain dengan menerima request client tanpa adanya mekanisme dalam melakukan verifikasi apa yang akan dikirim kembali
7	*(OTG-INPVAL-001) - 01*	*Cross Site Scripting*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	Terdapat celah pada saat proses web browser menampilkan web page yaitu aplikasi memperbolehkan beberapa script yang bisa di eksekusi oleh web browser , seperti JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, dll .

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
			Akses cookie atau session token yang disimpan oleh browser user aplikasi dan administrator	
8	*(OTG-INPVAL-003) - 01*	*HTTP Verb Tampering*	Melakukan upload malicious files (backdoor, spyware, virus, dsb) Memperbolehkan untuk mengakses restricted directories	Adanya kerentanan pada aplikasi dalam mengantisipasi HTTP Verb (GET , PUT , TRACE , dll) sehingga penyerang bisa melakukan akses lebih dalam memanipulasi HTTP Verb .
			Melihat directories yang ada di web server	

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
			Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	
9	*(OTG-INPVAL-005) - 01*	*SQL Injection*	Memperbolehkan untuk mengakses administrator aplikasi	Terdapat celah yaitu kesalahan aplikasi yang dapat menerima statement dynamic SQL , sehingga memperbolehkan penyerang untuk melakukan modifikasi statement dan mengeksekusi arbitrary SQL commands
			Menjalankan perintah yang hanya bisa dilakukan oleh administrator aplikasi	
10	*(OTG-INPVAL-016) - 01*	*HTTP Response Splitting*	Merubah struktur HTTP header untuk menghasilkan serangan berbahaya seperti	Terdapat celah web server dalam merespon HTTP Response Stream

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
			cache poisoning atau hijacking pages dengan informasi user yang sensitif	yang kemudian menjadi 2 respon yang berbeda
11	*(OTG-ERR-001) - 01*	*Error Messages on page*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan	Aplikasi menampilkan pesan error yang berisi informasi sensitif mengenai environment , users , ataupun data .
			Kebocoran struktur dan isi directories aplikasi	
12	*(OTG-BUSLOGIC-009) - 01*	*File Upload All Files*	Melakukan upload malicious files (backdoor, spyware, virus, dsb) Memperbolehkan untuk mengakses restricted directories	Aplikasi memperbolehkan user untuk melakukan upload atau transfer files berbahaya yang bisa saja di proses otomatis oleh environment
			Melihat directories yang ada di web server	

No	Vulnerability ID	Nama Celah	Dampak Teknikal	Penyebab
			Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	
13	*(OTG-CLIENT-005)- 01*	*Old Jquery*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	Terdapat celah pada saat proses web browser menampilkan web page yaitu aplikasi memperbolehkan beberapa script yang bisa di eksekusi oleh web browser , seperti JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, dll , karena adanya JQuery yang out of date

Setelah penyebab dan dampak diketahui maka selanjutnya adalah mencari nilai risk rating dari masing-masing celah keamanan yang ditemukan , sehingga nantinya bisa menjadi prioritas dalam urgensi penyelesaian celah . Seperti sebelumnya dijelaskan bahwa penilaian akan berdasarkan 2 hal yaitu Faktor (Factors) dan Dampak (Impact) . Hal ini akan dilanjutkan pada analisis celah keamanan .

BAB VI
HASIL ANALISIS DAN EVALUASI

Bab ini menjelaskan hasil analisis dan evaluasi penelitian tugas akhir. Yang akan dijelaskan oleh penulis adalah merumuskan hasil analisis dan celah keamanan dari identifikasi celah keamanan yang ditemukan pada bab sebelumnya sebagaimana yang telah dijelaskan pada bab metodologi.

6.1 Hasil Analisis Celah Keamanan

Pada proses ini akan dilakukan analisis celah keamanan sehingga dapat mengetahui penyebab dan dampak yang mungkin akan terjadi terkait celah keamanan yang ada pada aplikasi Sistem Informasi Mahasiswa miliki Perguruan Tinggi XYZ .

- Vulnerability ID : Di isi sesuai dengan Vulnerability ID yang ditentukan oleh peneliti , untuk memudahkan penomoran dari celah keamanan.
- Nama Celah : Di isi sesuai dengan nama celah keamanan yang ditemukan
- Risiko : Di isi dengan risiko yang muncul dari celah keamanan yang ditemukan
- Dampak : Di isi dengan dampak yang dihasilkan dari celah keamanan dari sisi teknikal
- Penyebab : Di isi dengan penyebab yang dihasilkan dari celah keamanan dari sisi teknikal
- Threat Agent Factors : Terdiri dari nilai Threat Agent Factors
- Vulnerability Factors : Terdiri dari Vulnerability Factors

Berikut ini merupakan daftar celah keamanan beserta penyebab dan dampak yang mungkin terjadi :

Tabel 6.1 Hasil analisis Factors OWASP Risk Rating

FACTORS														
No	**Vuln ID**	**Nama Celah**	**Dampak**	**Penyebab**	**Threat Agent Factors**				**Vulnerabililty Factors**					**Overall Likelihood**
					Skill Level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion Detection	TOTAL	
1	*(OTG-AUTHZ-001) - 01*	*Directory Traversal*	Memperbolehkan untuk mengakses restricted directories Melihat directories yang ada di web server Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	Ada nya path traversal yang rentan karena special element yang tidak dibatasi oleh administrator aplikasi , seperti special element separator ".." dan "/" sehingga penyerang dapat mengakses file sensitif seperti "/usr/local/bin" .	3	4	7	9	3	3	6	9	5.5	Medium

2	*(OTG-AUTHZ-004) - 01*	*Directory Listing and Information Disclosure*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan Kebocoran struktur dan isi directories aplikasi	Listing Directory yang memperbolehkan penyerang untuk melihat dan membuka seluruh index dari seluruh isi direktori . Risiko dan konsekuensi yang terjadi akan bergantung pada files yang terekspos dan accessible	1	4	7	9	3	3	6	9	5.25	Medium
3	*(OTG-AUTHZ-004) - 02*	*Possible Server Path Disclosure*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan Kebocoran struktur dan isi directories aplikasi	Adanya kesalahan konfigurasi pada file PHP pada aplikasi sehingga muncul path sensitif yang merujuk pada informasi server	1	4	7	9	3	3	6	9	5.25	Medium

4	*(OTG-AUTHZ-004) - 03*	*Source Code Disclosure*	Memberikan informasi struktur source code (string koneksi database atau logika kode) yang sensitif untuk mempermudah penyerangan	Terdapat source code yang bersifat readable/accessible oleh user dan berisi informasi sensitif mengenai logika yang dapat menjadi petunjuk bagi penyerang .	1	4	4	6	7	1	9	9	5.125	Medium
5	*(OTG-AUTHZ-004) - 04*	*Possible Sensitive Files*	Memberikan informasi yang bisa saja berbahaya seperti password files , configuration files , log files , database dumps dan file konfigurasi lain nya yang sensitif untuk mempermudah penyerangan	Aplikasi menyimpan data sensitif pada web document root dengan access control yang tidak cukup baik , yang mengakibatkan dapat di akses oleh untrusted user	3	4	4	6	7	3	6	9	5.25	Medium

6	*(OTG-SESS-005)- 01*	*Cross Site Request Forgery*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	web server di desain dengan menerima request client tanpa adanya mekanisme dalam melakukan verifikasi apa yang akan dikirim kembali	9	9	4	9	3	1	9	9	6.625	High
7	*(OTG-INPVAL-001) - 01*	*Cross Site Scripting*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator Akses cookie atau session token yang disimpan oleh browser user aplikasi dan administrator	Terdapat celah pada saat proses web browser menampilkan web page yaitu aplikasi memperbolehkan beberapa script yang bisa di eksekusi oleh web browser , seperti JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, dll .	9	9	4	9	3	1	9	9	6.625	High

8	*(OTG-INPVAL-003) - 01*	*HTTP Verb Tampering*	Melakukan upload malicious files (backdoor, spyware, virus, dsb) Memperbolehkan untuk mengakses restricted directories Melihat directories yang ada di web server Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	Adanya kerentanan pada aplikasi dalam mengantisipasi HTTP Verb (GET , PUT , TRACE , dll) sehingga penyerang bisa melakukan akses lebih dalam memanipulasi HTTP Verb .	5	9	4	6	1	3	6	8	5.25	Medium
9	*(OTG-INPVAL-005) - 01*	*SQL Injection*	Memperbolehkan untuk mengakses administrator aplikasi	Terdapat celah yaitu kesalahan aplikasi yang dapat menerima statement dynamic SQL , sehingga	5	9	7	9	9	9	9	8	8.125	High

			Menjalankan perintah yang hanya bisa dilakukan oleh administrator aplikasi	memperbolehkan penyerang untuk melakukan modifikasi statement dan mengeksekusi arbitrary SQL commands										
10	*(OTG-INPVAL-016) - 01*	*HTTP Response Splitting*	Merubah struktur HTTP header untuk menghasilkan serangan berbahaya seperti cache poisoning atau hijacking pages dengan informasi user yang sensitif	Terdapat celah web server dalam merespon HTTP Response Stream yang kemudian menjadi 2 respon yang berbeda	3	4	7	9	1	3	6	3	4.5	Medium
11	*(OTG-ERR-001) - 01*	*Error Messages on page*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan	Aplikasi menampilkan pesan error yang berisi informasi sensitif mengenai environment , users , ataupun data .	1	4	7	9	1	3	4	9	4.75	Medium

			Kebocoran struktur dan isi directories aplikasi											
12	*(OTG-BUSLOGIC-009) - 01*	*File Upload All Files*	Melakukan upload malicious files (backdoor, spyware, virus, dsb) Memperbolehkan untuk mengakses restricted directories	Aplikasi memperbolehkan user untuk melakukan upload atau transfer files berbahaya yang bisa saja di proses otomatis oleh environment	3	9	7	6	3	3	4	3	4.75	Medium
			Melihat directories yang ada di web server											

			Menjalankan perintah yang hanya bisa dilakukan oleh admin web server											
13	*(OTG-CLIENT-005)-01*	*Old Jquery*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	Terdapat celah pada saat proses web browser menampilkan web page yaitu aplikasi memperbolehkan beberapa script yang bisa di eksekusi oleh web browser , seperti JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, dll , karena adanya JQuery yang out of date	9	4	7	9	3	3	6	9	6.25	High

Tabel 6.2 Hasil analisis Impact OWASP Risk Rating

IMPACT														
No	**Vuln ID**	**Nama Celah**	**Dampak**	**Penyebab**	Technical Impact				Business Impact					**Overall Likelihood**
					Loss of Confidentiali	Loss of	Loss of	Loss of	Financial Damage	Reputation	Non-	Privacy violation	TOTAL	
1	*(OTG-AUTHZ-001) - 01*	*Directory Traversal*	Memperbolehkan untuk mengakses restricted directories Melihat directories yang ada di web server Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	Ada nya path traversal yang rentan karena special element yang tidak dibatasi oleh administrator aplikasi , seperti special element separator ".." dan "/" sehingga penyerang dapat mengakses file sensitif seperti "/usr/local/bin" .	9	9	5	1	3	9	5	7	6	**High**

2	*(OTG-AUTHZ-004) - 01*	*Directory Listing and Information Disclosure*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan Kebocoran struktur dan isi directories aplikasi	Listing Directory yang memperbolehkan penyerang untuk melihat dan membuka seluruh index dari seluruh isi direktori . Risiko dan konsekuensi yang terjadi akan bergantung pada files yang terekspos dan accessible	6	5	5	1	3	4	5	7	4.5	**Medium**
3	*(OTG-AUTHZ-004) - 02*	*Possible Server Path Disclosure*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan Kebocoran struktur dan isi directories aplikasi	Adanya kesalahan konfigurasi pada file PHP pada aplikasi sehingga muncul path sensitif yang merujuk pada informasi server	6	5	5	1	3	4	5	7	4.5	**Medium**

4	*(OTG-AUTHZ-004) - 03*	*Source Code Disclosure*	Memberikan informasi struktur source code (string koneksi database atau logika kode) yang sensitif untuk mempermudah penyerangan	Terdapat source code yang bersifat readable/accessible oleh user dan berisi informasi sensitif mengenai logika yang dapat menjadi petunjuk bagi penyerang .	2	3	5	1	3	1	5	3	2.875	**Low**
5	*(OTG-AUTHZ-004) - 04*	*Possible Sensitive Files*	Memberikan informasi yang bisa saja berbahaya seperti password files , configuration files , log files , database dumps dan file konfigurasi lain nya yang sensitif untuk mempermudah penyerangan	Aplikasi menyimpan data sensitif pada web document root dengan access control yang tidak cukup baik , yang mengakibatkan dapat di akses oleh untrusted user	2	3	5	1	3	1	5	3	2.875	**Low**

6	*(OTG-SESS-005)- 01*	*Cross Site Request Forgery*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	web server di desain dengan menerima request client tanpa adanya mekanisme dalam melakukan verifikasi apa yang akan dikirim kembali	2	3	5	1	3	1	5	3	2.875	**Low**
7	*(OTG-INPVAL-001) - 01*	*Cross Site Scripting*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator Akses cookie atau session token yang disimpan oleh browser user aplikasi dan administrator	Terdapat celah pada saat proses web browser menampilkan web page yaitu aplikasi memperbolehkan beberapa script yang bisa di eksekusi oleh web browser , seperti JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, dll .	2	5	7	1	3	5	5	7	4.375	**Medium**

8	*(OTG-INPVAL-003) - 01*	*HTTP Verb Tampering*	Melakukan upload malicious files (backdoor, spyware, virus, dsb) Memperbolehkan untuk mengakses restricted directories Melihat directories yang ada di web server Menjalankan perintah yang hanya bisa dilakukan oleh admin web server	Adanya kerentanan pada aplikasi dalam mengantisipasi HTTP Verb (GET , PUT , TRACE , dll) sehingga penyerang bisa melakukan akses lebih dalam memanipulasi HTTP Verb .	9	9	7	1	3	9	5	7	6.25	**High**
9	*(OTG-INPVAL-005) - 01*	*SQL Injection*	Memperbolehkan untuk mengakses administrator aplikasi	Terdapat celah yaitu kesalahan aplikasi yang dapat menerima statement dynamic SQL , sehingga	9	9	7	1	3	9	5	7	6.25	**High**

			Menjalankan perintah yang hanya bisa dilakukan oleh administrator aplikasi	memperbolehkan penyerang untuk melakukan modifikasi statement dan mengeksekusi arbitrary SQL commands										
10	*(OTG-INPVAL-016) - 01*	*HTTP Response Splitting*	Merubah struktur HTTP header untuk menghasilkan serangan berbahaya seperti cache poisoning atau hijacking pages dengan informasi user yang sensitif	Terdapat celah web server dalam merespon HTTP Response Stream yang kemudian menjadi 2 respon yang berbeda	7	7	5	1	3	5	5	7	5	**Medium**
11	*(OTG-ERR-001) - 01*	*Error Messages on page*	Memberikan informasi struktur directories yang sensitif untuk mempermudah penyerangan	Aplikasi menampilkan pesan error yang berisi informasi sensitif mengenai environment , users , ataupun data .	6	2	1	1	3	1	5	7	3.25	**Medium**

			Kebocoran struktur dan isi directories aplikasi											
12	*(OTG-BUSLOGIC-009) - 01*	*File Upload All Files*	Melakukan upload malicious files (backdoor, spyware, virus, dsb) Memperbolehkan untuk mengakses restricted directories	Aplikasi memperbolehkan user untuk melakukan upload atau transfer files berbahaya yang bisa saja di proses otomatis oleh environment	7	7	7	1	3	5	5	7	5.25	**Medium**
			Melihat directories yang ada di web server											

			Menjalankan perintah yang hanya bisa dilakukan oleh admin web server											
13	*(OTG-CLIENT-005)-01*	*Old Jquery*	Manipulasi aplikasi yang membahayakan data confidential user aplikasi dan administrator	Terdapat celah pada saat proses web browser menampilkan web page yaitu aplikasi memperbolehkan beberapa script yang bisa di eksekusi oleh web browser , seperti JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, dll , karena adanya JQuery yang out of date	6	5	5	1	3	5	5	7	4.625	**Medium**

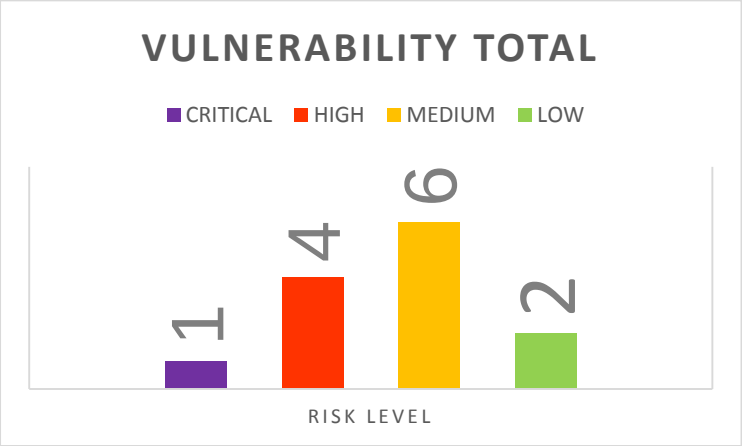
Berikutnya sesuai dengan tabel penentuan severity yaitu dengan melakukan persilangan Likelihood maka dihasilkan Overall Risk Severity sebagai berikut :

Tabel 6.3 Hasil Overall Risk Severity

Vuln ID	Nama Celah	Overall Risk Severity		
		Factors	Impact	Overall Risk Rating
(OTG-AUTHZ-001) - 01	*Directory Traversal*	Medium	High	**High**
(OTG-AUTHZ-004) - 01	*Directory Listing and Information Disclosure*	Medium	Medium	**Medium**
(OTG-AUTHZ-004) - 02	*Possible Server Path Disclosure*	Medium	Medium	**Medium**
(OTG-AUTHZ-004) - 03	*Source Code Disclosure*	Medium	Low	**Low**
(OTG-AUTHZ-004) - 04	*Possible Sensitive Files*	Medium	Low	**Low**
(OTG-SESS-005)- 01	*Cross Site Request Forgery*	High	Low	**Medium**
(OTG-INPVAL-001) - 01	*Cross Site Scripting*	High	Medium	**High**
(OTG-INPVAL-003) - 01	*HTTP Verb Tampering*	Medium	High	**High**
(OTG-INPVAL-005) - 01	*SQL Injection*	High	High	**Critical**
(OTG-INPVAL-016) - 01	*HTTP Response Splitting*	Medium	Medium	**Medium**

(OTG-ERR-001) - 01	*Error Messages on page*	Medium	Medium	**Medium**
(OTG-BUSLOGIC-009) - 01	*File Upload All Files*	Medium	Medium	**Medium**
(OTG-CLIENT-005)- 01	*Old Jquery*	High	Medium	**High**

Sehingga dihasilkan hasil jumlah celah keamanan seperti diagram dibawah :



Gambar 6.1 Jumlah celah keamanan

- Sebanyak **1** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **Critical**
- Sebanyak **4** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **High**

- Sebanyak **6** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **Medium**
- Sebanyak **2** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **Low**

6.2 Hasil Evaluasi Celah Keamanan

Setelah analisis dilakukan maka selanjutnya adalah melakukan evaluasi celah keamanan . Diketahui bahwa terdapat total 13 celah keamanan yang ditemukan dengan rincian 1 celah keamanan memiliki kategori Critical , 4 celah keamanan memiliki kategori High , 6 celah keamanan memiliki kategori Medium , dan 2 celah keamanan yang ber kategori Low . Artinya 1 celah keamanan dengan kategori Critical dan 4 celah keamanan dengan kategori High adalah memiliki prioritas lebih tinggi untuk segera dilakukan *fixing* atau perbaikan sehingga dampak yang dihasilkan bisa segera di kurangi atau bahkan hilang .

Dalam evaluasi celah keamanan perlu dilakukan tindakan mitigasi yang nantinya menjadi bahan pertimbangan administrator untuk melakukan perbaikan aplikasi web SIMAS-Online . Mitigasi ni akan mengacu pada standar CWE (Common Weakness Enumerity) . Berikut adalah tabel evaluasi celah keamanan untuk setiap celah keamanan yang ditemukan :

Tabel 6.4 Evaluasi Celah Keamanan

Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

Tabel evaluasi celah keamanan selengkapnya bisa dilihat pada Lampiran B .

LAMPIRAN A
PERSIAPAN PENGUJIAN

Lampiran Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

LAMPIRAN B
TABEL EVALUASI CELAH KEAMANAN

Lampiran Tidak Disertakan karena Tidak Diperbolehkan untuk di Publikasi

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini akan menjelaskan kesimpulan dari hasil penelitian dan saran untuk keberlanjutan penelitian.

7.1 Kesimpulan

Kesimpulan penelitian berisikan jawaban dari hasil analisis dan evaluasi yang telah dilakukan . Berikut ini merupakan beberapa poin hasil dari penelitian yang dilakukan penulis :

- Setelah melakukan pengujian ditemukan adanya risiko celah keamanan sebanyak 13 celah pada aplikasi web Sistem Informasi Mahasiswa (SIMAS-Online) Perguruan Tinggi XYZ, yaitu :
    1. Directory Traversal
    2. Directory Listing and Information Disclosure
    3. Possible Server Path Disclosure
    4. Source Code Disclosure
    5. Possible Sensitive Files
    6. Cross Site Request Forgery
    7. Cross Site Scripting
    8. HTTP Verb Tampering
    9. SQL Injection
    10. HTTP Response Splitting
    11. Error Messages on Page
    12. File Upload All Files
    13. Old JQuery

- Identifikasi Risiko dilakukan untuk mempermudah analisa celah keamanan dengan menjabarkan detail informasi dari setiap celah keamanan yang ditemukan . identifikasi risiko menjabarkan deskripsi secara umum

, dampak , penyebab , dan bagaimana penyerangan dilakukan .

- Analisa risiko dilakukan dengan menggunakan salah satu metodologi OWASP yaitu Risk Rating , hasilnya dari 13 celah keamanan yang ditemukan secara rinci ditemukan :
    - Sebanyak **1** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **Critical**
    - Sebanyak **4** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **High**
    - Sebanyak **6** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **Medium**
    - Sebanyak **2** celah keamanan yang memiliki Severity risk rating yang kategorikan sebagai celah keamanan yang tingkat vulnerability nya **Low**

- Tindakan yang dapat dilakukan untuk mengelola dampak yang ditimbulkan adalah dengan menggunakan mitigasi pada standar CWE , berikut adalah tindakan mitigasi yang dilakukan pada 1 celah dengan tingkat critical dan 4 celah keamanan dengan tingkat vulnerability High .
    - **SQL Injection**
        - *Phase: Architecture and Design*
        - Menggunakan library atau framework sebagai pencegah celah keamanan ini terjadi .

- Misalnya menggunakan persistence layer seperti Hibernate atau Enterprise Java Beans , dimana akan memberikan perlindungan signifikan terhadap SQL Injection jika digunakan semestinya .
- *Phase: Architecture and Design*
- Membuat konversi acceptable objects , seperti filename atau URL yang di mapping dalam sebuah bentuk fixed input values (numeric ID) di konversi menjadi filename aslinya atau URL tertentu . Serta menolak seluruh input yang lain .

- **HTTP Verb Tampering**
  - *Phase : Architecture and Design*
  - Pastikan bahwa hanya legitimate HTTP Verbs yang diperbolehkan (Allowed)
  - Jangan menggunakan HTTP Verbs sebagai faktor dalam *access decisions*

- **Directory Traversal**
  - *Phase : Implementation*
  - Input oleh user harus di *decoded* dan *canonicalized* pada aplikasi sebelum di validasi , pastikan bahwa decode yang dihasilkan tidak menghasilkan input yang sama pada aplikasi (input ganda) . Input ganda biasanya akan berujung pada error yang bisa di manfaatkan malicious user untuk membobol sistem . Path Traversal biasanya akan terjadi dengan input user berupa tanda ".." , maka dari itu aplikasi harus membuat

built-in path yang telah di canoncalized atau di normalisasi .

- Menggunakan aplikasi firewall yang bisa mendeteksi serangan terhadap celah ini . Firewall memiliki keuntungan pada kasus dimana celah tidak dapat diselesaikan dari fixing source code nya dalam waktu yang singkat, dan menjadikan firewall sebagai perlindungan darurat saat proses fixing berlangsung . Firewall juga akan menjadi perlindungan ganda bagi sistem .

- **Cross Site Scripting**
  - *Phase: Implementation; Architecture and Design*
  - Melakukan *encoding* dan *escaping* yang mengacu pada *XSS Prevention Cheat Sheet* .
  - *Phase: Architecture and Design*
  - Menggunakan library atau framework sebagai pencegah celah keamanan ini terjadi .
  - Contoh dari library atau framework yang dapat digunakan untuk menghasilkan encoded output yang benar adalah Microsoft's Anti-XSS Library , OWASP ESAPI Encoding module , atau Apache Wicket
  - *Phase: Operation*
  - Menggunakan aplikasi firewall yang bisa mendeteksi serangan terhadap celah ini . Firewall memiliki keuntungan pada kasus dimana celah tidak dapat diselesaikan dari fixing

source code nya dalam waktu yang singkat, dan menjadikan firewall sebagai perlindungan darurat saat proses fixing berlangsung . Firewall juga akan menjadi perlindungan ganda bagi sistem .

- **Old JQuery XSS**
- Update Jquery ke versi yang paling terbaru yaitu versi diatas 1.6.3

7.2 Saran

Berikut ini merupakan saran-saran yang dapat diberikan penulis untuk penelitian selanjutnya :

1. Penelitian ini adalah bersifat Blackbox Testing , sementara terdapat beberapa pengujian yang ada pada metodologi *web application penetration testing milik OWASP* mengharuskan pengujian dilakukan dengan Whitebox Testing , seperti misalnya pengujian dalam role yang ada pada aplikasi . Sehingga pengujian masih belum dikatakan maksimal .
2. Beberapa tools pada yang ada pada rekomendasi OWASP tidak up to date sehingga untuk ke depan nya akan susah untuk memenuhi kebutuhan evaluasi celah keamanan yang lebih up to date juga

(Halaman ini sengaja dikosongkan).

DAFTAR PUSTAKA

[1] J. Simarmata, Perancangan Basis Data, Yogyakarta: Andi, 2009.

[2] Symantec, "Symantec Internet Security Threat Report," 2015. [Online]. Available: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

[3] P. Engrebeston, The Basics of Hacking and Penetration Testing, Waltham, Massachusetts: Elsevier Inc., 2011.

[4] EC-Council, Penetration Testing Procdures & Methodologies, New York: Cengage Learning, 2011.

[5] O. Foundation, "OWASP Top 10 - 2013 Release Candidate," 2013. [Online]. Available: https://code.google.com/p/owasptop10/.

[6] O. Foundation, "OWASP Risk Rating Methodology.," 2014. [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

(Halaman ini sengaja dikosongkan.)

BIODATA PENULIS

Penulis yang lahir di Madiun, Jawa Timur, pada tanggal 9 Februari 1994 ini merupakan anak kedua dari dua bersaudara. Penulis telah menempuh pendidikan formal di SDN Pucang 4 Sidoarjo, SMPN 2 Sidoarjo, SMAN 1 Sidoarjo. Tahun 2012, penulis terdaftar di Jurusan Sistem Informasi ITS Surabaya dengan NRP 5212100124. Penulis memiliki pengalaman dalam bidang organisasi kemahasiswaan menjadi staff dalam negeri HMSI pada tahun 2013-2014 dan kepanitiaan acara nasional Information Systems Expo 2013 sebagai staff . Ditahun berikutnya, penulis memfokuskan diri untuk berkontribusi menjadi wakil ketua Information Systems Expo 2014 dan menjadi salah satu bagian *instructing committe* dari kaderisasi jurusan di ITS. Dalam tugas akhir ini, penulis mengambil bidang minat Manajemen Sistem Informasi (MSI) dengan topik Evaluasi risiko celah keamanan menggunakan metodologi *Open Web Application Security Project (OWASP)* pada aplikasi web Sistem Informasi Mahasiswa Perguruan Tinggi XYZ.