Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau

PENETRATION TESTING INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)

TUGAS AKHIR

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik
Pada Jurusan Teknik Informatika

Oleh

ZUL AZIS KHAN

NIM. 1195111754

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2024

UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

LEMBAR PERSETUJUAN

Penetration Testing Information System Security Assessment Framework (ISSAF)

TUGAS AKHIR

Oleh

Zul Azis Khan
NIM. 11950111754

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 04 Januari 2024

Pembimbing I,

Nazruddin Safaat H, S.T., M.T.
NIP. 130517100

UIN SUSKA RIAU

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PENGESAHAN

Penetration Testing Information System Security Assessment Framework (ISSAF)

Oleh

Zul Azis Khan

NIM. 11950111754

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik
pada Universitas Islam Negeri Sultan Syarif Kasim Riau

Pekanbaru, 04 Januari 2024

Mengesahkan,

Dekan,

Dr. Hartono, M.PD.

NIP. 19640301 199203 1 003

Ketua Jurusan,

Iwan Iskandar, S.T., M.T.

NIP. 19821216 201503 1 003

DEWAN PENGUJI

Ketua	: Febi Yanto, M. Kom
Pembimbing I	: Nazruddin Safaat H, S.T., M.T.
Penguji I	: Muhammad Irsyad, S.T., M.T.
Penguji II	: Teddie Darmizal, S.T., M.T.I.

UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak cipta milik UIN Suska Riau

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum dengan ketentuan bahwa hak cipta pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan seizin penulis dan harus disertai dengan kebiasaan ilmiah untuk menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan yang meminjamkan Tugas Akhir ini untuk anggotanya diharapkan untuk mengisi nama, tanda peminjaman dan tanggal pinjam.

State Islamic University of Sultan Syarif Kasim Riau

UIN SUSKA RIAU

UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 04 Juniari 2024

Yang membuat pernyataan,

ZUL AZIS KHAN

NIM. 1195111754

UIN SUSKA RIAU

UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulillahirabbil ‘alamin

Dengan mengucapkan syukur pada Allah subhanahu wa ta’ala, dan shalawat serta salam kepada Nabi kita Muhammad shallallahu Alaihi wasallam,

telah saya selesaikan Tugas Akhir ini...

Saya persembahkan Tugas Akhir Saya Ini Untuk

Kedua Orang Tua, Keluarga, dan Teman-Teman...

Semoga Tugas Akhir ini bermanfaat bagi pembacanya

UIN SUSKA RIAU

UIN SUSKA RIAU

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama	: Zul Azis Khan
NIM	: 11950111754
Tempat/Tgl.Lahir	: Kandis, 18 April 2001
Fakultas	: Sains dan Teknologi
Prodi	: Teknik Informatika
Judul Skirpsi	:Penetration Testing Information System Security Assessment Framework (ISSAF)

Menyatakan dengan sebenar-benarnya bahwa:

1. Penulisan Skripsi dengan judul sebagaimana tersebut diatas adalah hasil pemikiran penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernnya.
3. Oleh karena itu, Skripsi saya ini, saya nyatakan bebas dari plagiat.
4. Apabila dikemudian hari terbukti terdapat plagiat dalam penulisan Skripsi saya tersebut, maka saya bersedia menerima sanksi sesuai perundang-undangan.

Demikian Surat Pernyataan ini saya buat dengan penuh kesadaraan dan tanpa paksa pihak manapun juga.

Pekanbaru, 05 Januari 2024

Yang membuat pernyataan,

ZUL AZIS KHAN

NIM. 11950111754

UIN SUSKA RIAU

Penetration Testing Information System Security Assessment Framework (ISSAF)

Zul Azis Khan*, Nazruddin Safaat H, Muhammad Irsyad, Teddie Darmizal

Fakultas Sains dan Teknologi, Teknik Informatika, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia
Email: 1*aziskhan0401@gmail.com, 2nazruddin.safaat@uin-suska.ac.id , 3irsyadtech@uin-suska.ac.id,
4teddie.darmizal@uin-suska.ac.id
Email Penulis Korespondensi: aziskhan0401@gmail.com

Abstrak−Perkembangan teknologi informasi memiliki dampak positif di berbagai bidang, salah satunya adalah bidang teknologi web. Teknologi informasi saat ini sudah manjadi sebuah kebutuhan dalam peningkatan kinerja organisasi maupun institusi pendidikan dalam mencapai tujuan. Website menjadi alternatif bagi institusi dalam mempromosikan kepada masyarakat umum. Website https://kekampus.umri.ac.id/ merupakan sistem informasi yang dimiliki kampus UMRI yang digunakan untuk PKKMB dan MASTA UMRI, sebagai website yang menyimpan data perlu dilakukan peningkatan keamanan untuk mencegah terjadi nya serangan hacker, terdapat beberapa metode yang bisa dipakai salah satu nya Framework ISSAF adalah standar pengujian penetrasi yang digunakan untuk menguji ketahanan situs web. Tujuan penelitian ini adalah untuk mengetahui celah keamanan website https://kekampus.umri.ac.id/ dengan menggunakan metode penetration testing dengan Framework ISSAF. Framework ISSAF meliputi sembilan asesmen pengujian yang meliputi Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access, dan Covering Tracks. Pada penelitian ini hanya melakukan empat tahap dari sembilan tahap yang ada pada Framework ISSAF. Penelitian ini menggunakan starategi blackbox yaitu penguji hanya diberi akses domain website target.Penelitian ini dilakukan karena permasalahan yang sering terjadi slot gacor pada salah satu sistem informasi UMRI.Jadi hasil yang didapatkan yaitu ditemukan beberapa kerentanan yang kurang pada website yaitu serangan sql injection, cross javascript, cookie secure flag yang terdapat pada website https://kekampus.umri.ac.id/. dan memberikan saran atau rekomendasi untuk meningkatkan kemanan pada website https://kekampus.umri.ac.id/.

Kata Kunci: Framework ISSAF; Vulnerability Website; Blackbox; Penetration Testing

Abstrak−The development of information technology has had a positive impact on various fields, including the field of web technology. Information technology has now become a necessity in improving the performance of organizations and educational institutions in achieving goals. Websites are a tool for institutions to promote to the general public. The https://kekampus.umri.ac.id/ website is an information system owned by the Umri campus which is used for PKKMB and Umri Masters, as a website that functions in storing data, it is necessary to increase security to prevent hacker attacks, there are several methods used, one of which is The ISSAF framework is a penetration testing standard used to test the resilience of websites. The aim of this research is to determine the security gaps of the https://kekampus.umri.ac.id/ website by using the penetration testing method with the ISSAF Framework. The ISSAF framework includes nine test assessments which include Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromising Remote Users/Sites, Maintaining Access, and Covering Tracks. In this study, examiners only carried out four stages of the nine stages in the ISSAF framework. This research uses a black box strategy where testers are only given access to the target website domain. This research was conducted because of the problems that often occur in gacor slots in one of UMRI's information systems. The results of the analysis carried out found that there were several vulnerabilities that were lacking on the website, namely SQL injection attacks, cross JavaScript, cookie secure flags on the https://kekampus.umri.ac.id/ website. and provide suggestions or recommendations to improve security on the https://kekampus.umri.ac.id/ website.

Keywords: Framework ISSAF; Vulnerability Website; Blackbox; Penetration Testing

PENDAHULUAN

Perkembangan teknologi informasi memiliki dampak positif di berbagai bidang, salah satunya adalah bidang teknologi web. Website menjadi alternatif bagi institusi dalam mempromosikan kepada masyarakat umum. Penerapan teknologi sangat berguna untuk meningkatkan aktifitas media informasi dan komunikasi untuk yang mudah yang bisa mendukung perguruan tinggi dalam bersaing.

UPT Teknologi Informasi dan Pangkalan Data (TIPD) merupakan unit pelaksanaan tugas Universitas Muhammadiyah Riau (UMRI) yang bergerak di bidang Teknologi Informasi dan Komunikasi. UPT UMRI selaku pihak yang bertanggung jawab atas segala sistem yang ada di kampus tersebut. Namun terdapat permasalahan yang sering terjadi pihak kampus banyak yang kurang memperhatikan tentang kemanan informasi, didukung dengan masih banyak ditemukan teknologi informasi yang tidak memberikan efek manfaat dan timbal balik kepada tiap institusi atau organisasi "IT Productivity Paradox"[1] dan padahal ini hal penting pada sistem informasi yang diterepkan manajemen[2]. Pada kasus sebelumnya pernah terjadi serangan slot gacor pada salah satu sistem informasi kampus UMRI yang menyebabkan salah satu halaman sistem informasi yaitu https://sikuli.umri.ac.id/ menjadi halaman judi online, sehigga sampai saat ini belum dapat diketahui tingkat keamanan pada sistem informasi di kampus UMRI.

Berdasarkan kondisi yang ada terdapat beberapa indikator yang menyatakan bahwa tata kelola sistem informasi yang diterapkan pada kampus UMRI masih kurang berjalan dengan baik, dan akibat serangan slot gacor pada sistem informasi https://sikuli.umri.ac.id/, sehingga perlu adanya peningkatan keamanan pada sistem informasi kampus UMRI. Sehingga didapatkan sebuah sistem informasi yang baik dan sesuai standar yang berlaku.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

UIN SUSKA RIAU
Hak cipta dan penggunaan kembali:
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau

Pada studi ini penelitian ini berfokus pada pengujian keamanan[3] website https://kekampus.umri.ac.id/ yang dilakukan melalui metode pengujian *penetration testing*[4] menggunakan Framework ISSAF[5]. Tujuan dilakukannya penelitian ini ialah mengetahui celah keamanan pada website berdasarkan pada pengujian penetration testing dengan Framework ISSAF, kemudian dari hasil pengujian yang dilakukan dibuatkan kesimpulan pada bagian mana dari website yang memiliki kerentanan terhadap serangan untuk menjadi bahan evaluasi website yang dapat diterapkan di kampus UMRI sebagai rujukan website kedepan agar website semakin menjadi lebih baik.

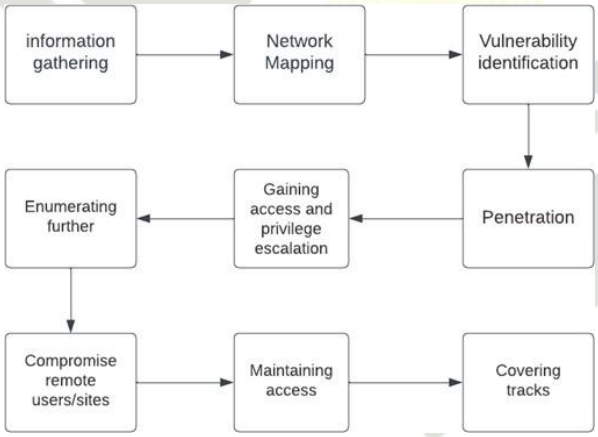
Beberapa penelitian sebelumnya telah membahas *penetration testing*, antara lain dilakukan oleh Sulis Andriyani mengenai Analisis celah keamanan pada website dengan menggunakan metode *penetration testing*[6], Bahar dan Riyan mengenai Implementasi *penetration testing* dengan metode ISSAF[7] pada keamanan sistem di PT.Dataquest Laverage Indonesia; Stefanus Eko Prasetyo mengenai Analisis keamanan website Universitas Internasional Batam menggunakan metode ISSAF[8], Darmayuda mengenai *penetration testing* pada web server menggunakan metode ISSAF (studi kasus website X).Tujuan penelitian ini untuk menemukan celah ke pada website https://kekampus.umri.ac.id/.

Oleh karena itu berdasarkan keterangan diatas, dalam penelitian ini peneliti tertarik mengangkat topik penetration testing framework information system security assesmant framework.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Pada tahapan penelitian ini penguji merujuk pada kerangka kerja ISSAF[9] (*information system security assessmant framework*) adalah sebuah kerangka kerja keamanan sistem informasi yang dirancang untuk memberikan struktur yang terstruktur untuk mengevaluasi dan meningkatkan keamanan sistem informasi[10] .ISSAF[11] membantu dalam mengidentifikasi potensi kerentanan dan memberikan saran serta masukan untuk memastikan keamanan sistem. Kerangka kerja ini memecah keamanan sistem informasi ke dalam berbagai kategori dan menyediakan alur kerja yang spesifik untuk evaluasi. Disini peneliti melakukan pengujian dengan strategi *blackbox* yaitu penguji penetrasi ditempatkan dalam peran rata-rata peretas, tanpa pengetahuan internal tentang sistem target. Penguji tidak diberikan diagram arsitektur atau kode sumber apa pun yang tidak tersedia untuk umum. Uji penetrasi *blackbox* menentukan kerentanan dalam sistem yang dapat dieksploitasi dari luar jaringan[12]. Berikut tahapan metode ISSAF yang ditujukan pada gambar 1.



Gambar 1. Tahapan Penelitian

Penjelasan dari masing-masing tahapan pada metode *information system security assessmant framework* sebagai berikut:

a. Information Gathering, merupakan tahapan awal dalam melakukan pengujian keamanan sistem dan jaringan komputer. Istilah lain dari *Information Gathering* adalah *Reconnaissance*. Tujuan melakukan *Information Gathering* diantaranya mengumpulkan dan mendapatkan informasi berupa *ip address*, domain dan kerangka cms yang di pakai. Pada tahap ini dilakukan pengumpulan informasi mengenai https://kekampus.umri.ac.id/, dan sebagai tahap persiapan *penetration testing*. Pengujian pada tahap ini antara lain untuk mengetahui *ip address* dan identifikasi CMS.
b. Network Mapping & port scanning, metode untuk menentukan port mana di jaringan yang terbuka dan dapat menerima atau mengirim data. Ini juga merupakan proses pengiriman paket ke port tertentu pada host dan menganalisis respons untuk mengidentifikasi kerentanan. Pada tahap ini melakukan *scanning* pada server https://kekampus.umri.ac.id/ menggunakan tools nmap[13], *scanning* dilakukan diluar area kampus UMRI. Tujuannya yaitu memperoleh informasi port dan yang terbuka pada server dan memperoleh informasi service yang berjalan di server.
c. Vulnerability Identification, proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat keparahan pada kerentanan keamanan yang ada pada sebuah jaringan komputer, sistem, aplikasi, atau bagian lain yang ada di ekosistem IT berdasarkan risiko yang ada. Pada tahap ini melakukan *scanning* pada sistem https://kekampus.umri.ac.id/ menggunakan tools ZAP sehingga memperoleh infomasi kerentanan pada sistem[14].

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak Cipta Milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau

Tujuannya yaitu memperolah informasi celah keamanan[15] pada sistem https://kekampus.umri.ac.id/, memperoleh risiko tingkat kerentanan pada sistem https://kekampus.umri.ac.id/, dan mengolah celah keamanan tersebut untuk ketahap selanjutnya.

d. Penetration testing, proses menguji keamanan suatu sistem jaringan komputer dengan cara melakukan simulasi nyata. Tujuan dari *pentest* adalah mencari tahu kelemahan-kelemahan dalam sistem tadi dan mencegah adanya kemungkinan *hacking*. Pada tahap ini melakukan *penetrasi test* pada sistem sehingga bisa melakukan *exploitasi* pada sistem https://kekampus.umri.ac.id/. Bertujuan untuk melakukan percobaan *exploitasi* dengan celah keamanan yang di perolah dari tahap sebelumnya.

e. Gaining Access and Privilege Escalation, merupakan tahapan mendapatkan akses hak istimewa dengan mendapatkan akses ke akun melalui beberapa cara, yaitu mencoba kombinasi username dan password, misal *Brute-force attacks* atau *Dictionary Attacks* dan mencoba *blank password* atau *default password*. Bertujuan untuk mendapatkan akses untuk masuk kedalam sistem target dan mendapatkan hak akses sebagai administrator atau *root*.

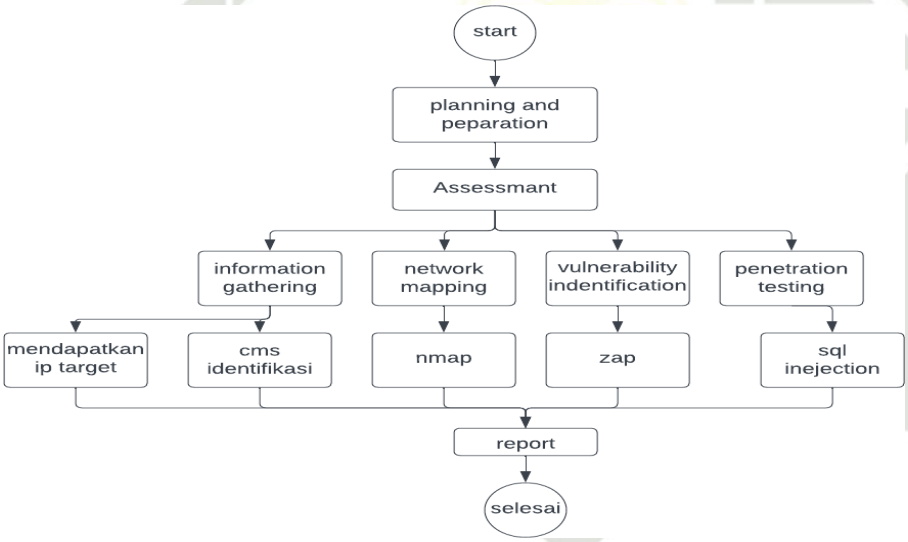
f. Enumerating Further, tahap *enumerating further* merupakan tahapan pengujian dengan melakukan pengambilan dan pemecahan seluruh informasi mengenai password yang diperoleh dari website https://kekampus.umri.ac.id/.

g. Compromise Remote User/Sites, tahap *compromise remote user/sites* merupakan tahapan pengujian dengan melakukan *eksploitasi* akses ke dalam *user root* melalui hubungan jarak jauh atau remote pada website https://kekampus.umri.ac.id/.

h. Maintaining Access, tahap *maintaining access* merupakan tahapan pengujian dengan melakukan penanaman *backdoor* ke dalam sistem website https://kekampus.umri.ac.id/. Penanaman *backdoor* dapat dilakukan dengan memanfaatkan fitur file upload yang tersedia pada website https://kekampus.umri.ac.id/.

i. Covering Tracks, tahap *covering tracks* merupakan tahapan terakhir dari pengujian *penetration testing*. Pengujian tahap ini yaitu dengan melakukan penghapusan *log* serangan yang telah dilakukan pada tahapan-tahapan sebelumnya.

Pada penelitian ini penguji hanya melakukan beberapa tahapan sebagai mana yang dijelaskan pada gambar 1 dan dirincikan pada gambar 2.



Gambar 1. Tahapan pengujian ISSAF

Pada gambar 2 di tunjukan tahapan ISSAF kemudian akan di perinci di tabel 1 tentang apa saja yang di lakukan dan apa saja tools nya dapat dilihat ditabel 1.

Tabel 1. Ringkasan tahapan impelentasi ISSAF

Tahap	Source	Tools
Information gathering	Ip addres, cms idenfitikasi	Ping, wappalyzer
Network mapping	Network info	Nmap
Vulnerability identification	Web scanner vulnerability	Zap
Penetration testing	Sql injection	sqlmap

Tahapan terakhir yaitu melakukan analisis dan membuat laporan dari hasil pengujian penetrasi yang sudah dilakukan berdasarkan Framework ISSAF.

3. HASIL DAN PEMBAHASAN

Dalam bagian ini, kita akan membahas langkah-langkah yang dilakukan bersama dengan hasil penelitian terhadap objek tertentu. Setelah mendapatkan hasil tersebut, akan disusun laporan beserta rekomendasi yang didasarkan pada hasil pengujian dengan tujuan perbaikan sistem ke depan.

UIN SUSKA RIAU
1. Dilarang menggunakan sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
Hak Cipta Dilindungi Undang-Undang
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

3.1 Infomation Gathering

Pada tahapan ini peneliti menggunakan sumber dari internet untuk memperoleh sebanyak mungkin infomasi dari target dengan memanfaanan teknik teknis, lalu mencari *ip address* dari target dan melakukan identifikasi tentang cms yang digunakan target.

3.1.1 Mendapatkan ip addres target

Langkah untuk mendapatkan *ip address* target dilakukan dengan menggunakan tools ping yang dimana tools ini digunakan untuk mengecek apakah target berjalan atau tidak dan bisa mendapatkan *ip address* target, untuk melakukan prosesnya menggunakan command ping https://kekampus.umri.ac.id/ pada terminal atau comandpromt pada gambar 3.

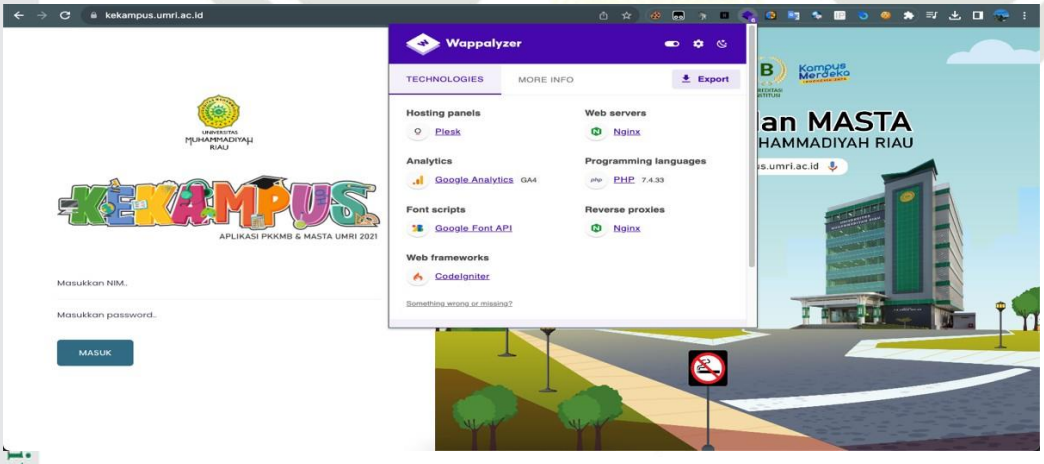
```
konan@konans-MacBook-Pro ~ % ping kekampus.umri.ac.id
PING kekampus.umri.ac.id (178.128.90.141): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
```

Gambar 3. Hasil pindai ip address target

Hasil yang di peroleh dari pemindai dengan tools ping didapatkan bahwa *ip address* dari https://kekampus.umri.ac.id/ adalah 178.128.90.142.

3.1.2 Identifikasi CMS

Setelah menemukan *ip address* dari target, mencari informasi tentang CMS dan teknologi yang digunakan https://kekampus.umri.ac.id/ dengan tools wappalyzer[16] yang di tunjukan pada gambar 4.



Gambar 4. Hasil identifikasi cms dengan tools wappalyzer

Setelah melakukan identifikasi dengan tools wappalyzer terdapat beberapa informasi yang di jelaskan pada tabel 2 sebagai berikut:

Tabel 2. Hasil pemindai tools wappalyzer

Technology	Version
Hosting panel	Plesk
Web framework	Code ignater
Web service	nginx
Bahasa pemrograman	php 7.4.33

3.2 Network Mapping

Pengujian pada tahap *network mapping* dilakukan dengan *scaning ip address* yang kemudian dilanjutkan dengan pemindai sistem informasi yang digunakan dan *scaning* layanan yang dipakai pada website.

3.2.1 Port Scanning

Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU
Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Scanning port dilakukan pada tahap pertama *netwotk mapping*, dengan menggunakan tools nmap[17] pada terminal atau nmap[18] versi GUI dengan mengetikkan comand nmap https://kekampus.umri.ac.id/ yang ditunjukan pada gambar 5.

```
konan — -zsh — 86×25
konan@konans-MacBook-Pro ~ % nmap kekampus.umri.ac.id
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 22:23 WIB
Nmap scan report for kekampus.umri.ac.id (178.128.90.141)
Host is up (0.021s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
2002/tcp closed globe
2004/tcp closed mailbox
8443/tcp open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 70.02 seconds
konan@konans-MacBook-Pro ~ %
```

Gambar 5. Hasil *scaning* dengan tools

Hasil proses *scaning port* menggunakan tools nmap pada gambar di atas didapatkan hasil beberapa port terbuka pada *scanning port* yang dilakukan menggunakan tools nmap pada gambar 5, diperoleh beberapa port yang terbuka pada website https://kekampus.umri.ac.id/ di tujukan pada tabel 3 dibawah.

Tabel 3. Hasil scaning nmap

Port	Port	Service
22/tcp	Open	ssh
80/tcp	Open	http
443/tcp	Open	https
2002/tcp	Closed	mailbox

3.2.2 Service and Oparation System Scanning

Pada tahap ini dilakukan *scanning* lebih lanjut untuk mendapatkan hasil lebih detail tentang website target, seperti layanan yang sedang berjalan dan sistem operasi yang digunakan terkait website target dengan menggunakan tools nmap dengan command nmap -sV https://kekampus.umri.ac.id/ yang di tunjukan pada gambar 6.

```
konan@konans-MacBook-Pro ~ % nmap -sV kekampus.umri.ac.id
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 22:32 WIB
Nmap scan report for kekampus.umri.ac.id (178.128.90.141)
Host is up (0.016s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp   open   http     nginx
443/tcp  open   ssl/http nginx
2002/tcp closed globe
2004/tcp closed mailbox

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.80 seconds
konan@konans-MacBook-Pro ~ %
```

Gambar 6. Hasil scanning lebih lanjut dengan tools nmap

Dari hasil *scanning* lebih lanjut menggunakan tools nmap dapat diperoleh layanan yang sedang berjalan, namun tidak berhasil diidentifikasi sistem operasi yang di gunakan, dijelaskan ditabel 4 sebagai berikut.

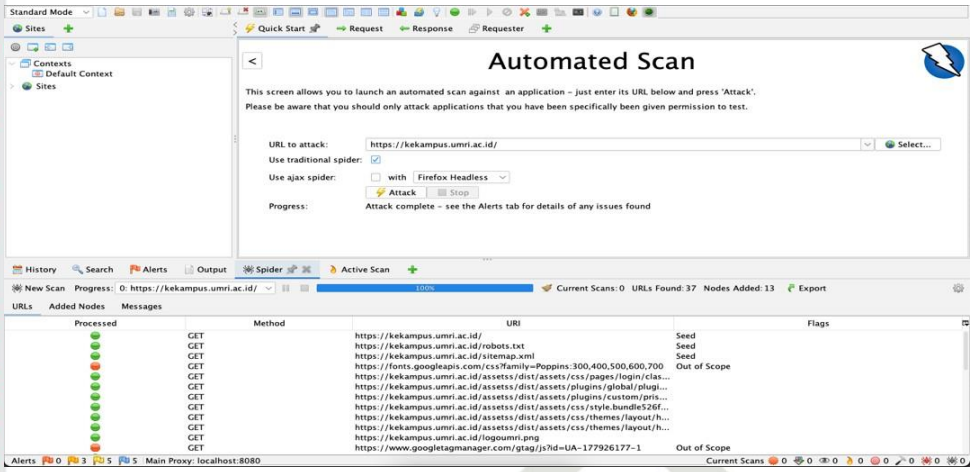
Tabel 4. Hasil scanning nmap lebih lanjut

Port	State	Service	Version
22/tcp	Open	ssh	open ssh 7.4 (protocol 2.0)
80/tcp	Open	http	nginx
443/tcp	Open	https/ssl	nginx
2002/tcp	Closed	globe	
2004/tcp	Closed	mailbox	

3.3 Vulnerability Identification

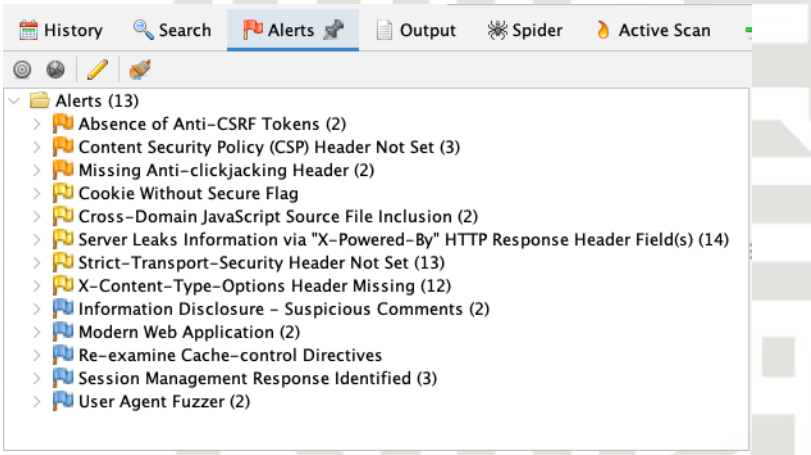
Pada tahapan ini pengidentifikasian dilakukan menggunakan tools zap[19] , tools ini diperuntukan *scanning* url target untuk dilakukan *attacking* yang ditujukan pada gambar 7.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau



Gambar 7. Proses scanning menggunakan tools ZAP

Setelah dilakukan *scaning* pada https://kekampus.umri.ac.id/ ditemukan beberapa kerentanan pada website yang dijelaskan pada gambar 8.



Gambar 8. Hasil scanning menggunakan tools zap

Dari hasil *scanning* yang ada di gambar di atas di temukan bahwa sistem memiliki celah kerentanan yang di jelaskan pada tabel 5 sebagai berikut:

Tabel 5. Informasi tentang kerentana dengan tools zap

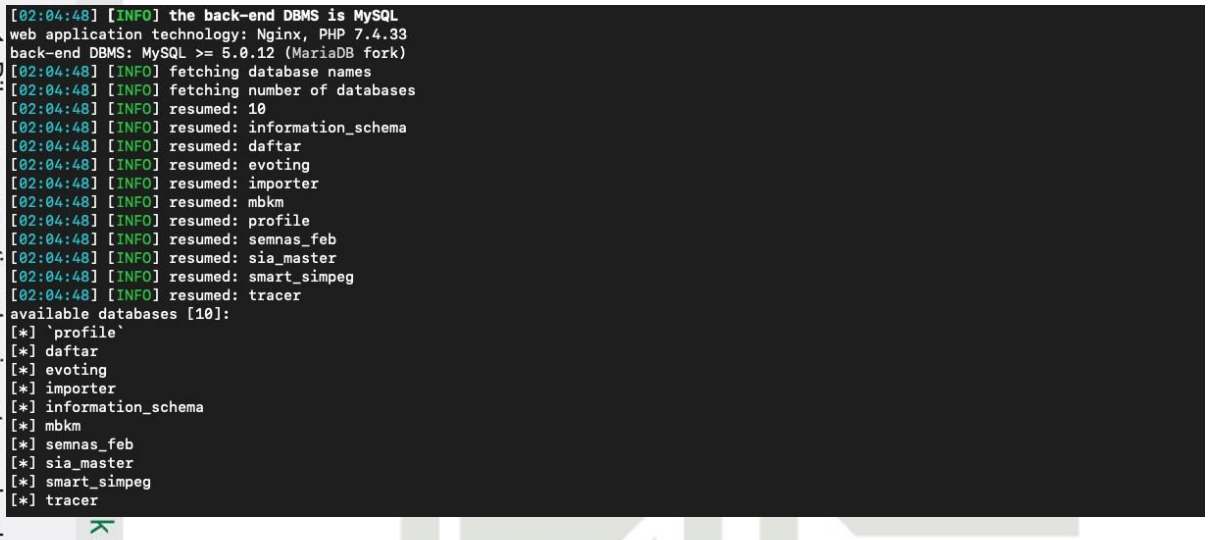
Kerentanan	Level
Absence of anti CSRF tokens	Medium
Content security policy	Medium
Missing anti Clickjacking headers	Medium
Cookie without secure flag	Low
Cross domain java script file inclution	Low
Server leaks information	Low
Strict transport security hader	Low
X-content type header missing	Low
Information disclousur	Informational
Modern web application	Informational
Re exmine chahce control directives	Informational
Sesion management response	Informational
User agent fuzzer	Informational

Pada tabel di atas pengujian *vulnerability identification* bawah dari *scanning* yang dilakukan oleh tools zap menunjukan beberapa kerentana yang level nya medium, ada juga yang level nya *low* dan informational.

3.4 Penetration Testing

Pada tahapan ini penguji melukukan *penetration testing* pada website target dengan melakukan serangan simulasi pada website untuk mencari celah keamanan, dalam tahap ini penguji melakukan dengan teknik *sql injection* dengan tujuan adalah untuk menguji keamanan sistem.

UIN SUSKA RIAU



Gambar 7. Hasil exploit menggunakan sqlmap

Pada gambar di atas dijelaskan hasil *exploit* menggunakan tools sqlmap[20] ternyata berhasil mendapatkan *database* dari website https://kekampus.umri.ac.id/ dan ternyata ada sekitar 9 *database* yang ada di server target.

Tabel 4. Informasi tentang service dari hasil sqlmap

DBMS	Mysql
Nginx	Php 7.4.33
Mysql	5.0.12 mariaDB

Tabel 5. Isi database hasil sqlmap

Database	Profile
	Daftar
	Evoting
	Importer
	Information schema
	Mbkm
	Semnas_feb
	Sia_master
	Smart_simpeg
	Tracer

3.5 Report and Result

Tahapan *result* dan *report* merupakan tahapn akhir yang dimana pengujian membuatkan laporan hasil *penetration testing* yang dilakukan pada website https://kekampus.umri.ac.id/ yaitu mengenai celah kemanan apa saja yang ditemukan pada website target, disimpulkan pada tabel 8 sebagai berikut:

Tabel 8. Report and result

Vulnerability	Status	Level
Sql injection	Ada nya validasi atau pun filter setiap inputan yang ingin login ke dalam website https://kekampus.umri.ac.id/	High/critical

Dapat dilihat pada tabel diatas dari seluruh pengujian menggunakan Framework ISSAF yang dilakukan, terdapat beberapa celah yang dimana salah satu ada terdapat celah kerentanan yang *critical* pada website https://kekampus.umri.ac.id/ yang berhasil didapat dari tahapan *penetration testing*, namun beberapa temuan yang menggunakan tools ZAP kerentanan yang ada tidak bisa dieksekusi sehingga hanya menjadi sebuah *alert* atau peringtan saja.

Dari hasil penemuan pada penelitian ini mendukung temuan pada penelitian dimana celah keamanan pada website yang paling rentan adalah *sql injection* yang mana merupakan sumber celah terbanyak[21], celah lain nya juga terdapat pada port-port yang terbuka yang beresiko terhadap serangan. Ditambah juga dalam satu server terdapat beberapa *database website* lain yang ada dalam website https://kekampus.umri.ac.id/ akan menyebabkan serangn massal terhadap

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

UIN SUSKA RIAU
Hak cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
©Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau

seluruh sistem yang ada pada server. Pemberian rekomendasi pada website ini ialah adanya validasi pada *php* dan filter pada setiap inputan yang di masukan kedalam form *login* untuk mencegah serangan *sql injection*,[21] dan melakukan pemisahan tiap database website lain agar tidak menjadi satu dalam satu server.

4. KESIMPULAN

Dari penelitian yang telah dilakukan, didapatkan beberapa temuan terkait website yang diuji di antara lain yaitu *anti clickjacking, cross javascrip* dan *sql injection*, dari beberapa temuan tersebut ada satu temuan yang memiliki level *high* atau *critical* yaitu *sql injection* adalah kerentanan web yang memungkinkan penyerang mengganggu kueri database pada sistem. Serangan ini biasanya digunakan untuk mengambil isi database dalam sistem. Kerentanan ini terdapat pada inputan form login yang tidak ada filter setiap inputan yang masuk setiap akan melakukan login kedalam https://kekampus.umri.ac.id/. Efek dari kerentanan ini adalah dapat melihat seluruh isi database yang ada pada website target yang mana akan menguntungkan penyerang untuk bisa mengakses banyak data dan informasi. Metode ISSAF yang dipakai mendapatkan hasil dari sembilan tahapan yang penguji hanya melakukan empat dari sembilan tahapan tersebut, di peroleh bahwa webiste https://kekampus.umri.ac.id/ dipandang kurang aman dari segi serangan *sql injection* dengan level kerentanan itu berada di *high* atau *critical* yang ini sangat berbahaya bagi website itu sendiri. Dari hasil yang diperoleh diharapkan dapat ditindak lanjuti pengembangan website dari segi kemanan website dan menutup segalah kemungkinan celah kerentanan yang ada supaya mendapatkan website yang menjadi lebih baik.

REFERENCES

[1] M. Harist Murdani, M. Usniyah Sari, and U. Wijaya Putra Surabaya, “IT Productivity Paradox pada Perguruan Tinggi Swasta 1,” Jurnal Ilmiah Teknologi Informasi Asia, vol. 12, no. 2, pp. 81–90, 2018.
[2] A. R. Tanaamah and F. J. Indira, “Analysis of Information Technology Security Management SWCU SIASAT Using ISO/IEC 27001:2013,” IJITEE, vol. 5, no. 2, pp. 68–74, 2021.
[3] R. Ashar, “Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF,” Jurnal Informasi dan Teknologi, vol. 4, no. 4, pp. 211–218, 2022, doi: 10.37034/jsisfotek.v4i4.233.
[4] G. Suprianto, “Penetration Testing Pada Sistem Informasi Jabatan Universitas Hayam Wuruk Perbanas,” InComTech : Jurnal Telekomunikasi dan Komputer, vol. 12, no. 2, pp. 129–138, Aug. 2022, doi: 10.22441/incomtech.v12i2.15093.
[5] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” JURNAL ILMIAH MERPATI, vol. 8, no. 2, pp. 113–124, 2020.
[6] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, “Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar,” LEDGER: Journal Informatic and Information Technology, vol. 2, no. 1, pp. 2963–8798, 2023.
[7] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, “Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf,” TRANSMISI : JURNAL ILMIAH TEKNIK ELEKTRO, vol. 24, no. 3, pp. 83–91, Aug. 2022, doi: 10.14710/transmisi.24.3.83-91.
[8] S. E. Prasetyo and N. Hassanah, “Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF,” Jurnal Informasi dan Teknologi, vol. 09, no. 02, pp. 82–86, 2022.
[9] M. A. Nabila, P. E. Mas’udia, and R. Saptono, “Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema,” Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi), vol. 13, no. 1, 2023.
[10] Guntoro, L. Costaner, and Musfawita, “Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning),” JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), vol. 05, no. 01, pp. 45–55, 2020.
[11] A. Zein, “Evaluasi Keamanan Wireless Lan Menggunakan Issaf (Information System Security Assessment Framework),” SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI, vol. 32, no. 2, pp. 29–35, 2022, doi: 10.37277/stch.v32i2.
[12] H. Poston, “What are black box, grey box, and white box penetration testing? [Updated 2020],” INFOSEC. Accessed: Dec. 15, 2023. [Online]. Available: https://resources.infosecinstitute.com/topics/penetration-testing/what-are-black-box-grey-box-and-white-box-penetration-testing/
[13] M. Shivanandhan, “What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time,” freeCodeCamp. Accessed: Dec. 15, 2023. [Online]. Available: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/
[14] I. Riadi, A. Yudhana, and P. Korspondensi, “Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment,” Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 7, no. 4, pp. 853–860, 2018, doi: 10.25126/jtiik.202071928.
[15] L. Kestina and G. Widi Nurcahyo, “Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci),” INNOVATIVE: Journal Of Social Science Research, vol. 3, no. 4, pp. 9192–9203, 2023.
[16] Y. Novriko Rahman, R. Maulana Hadi, M. Nabilah, M. Hanif Waskito, and N. Aini Rakhmawati, “Analisis Penggunaan Framework Website Jdih Khusus Peraturan Kementerian Republik Indonesia,” JURNAL TEKNOLOGI DAN OPEN SOURCE, vol. 3, no. 1, pp. 78–89, 2020.
[17] D. Sudirman and Akma Nurul Yaqin, “Network Penetration dan Security Audit Menggunakan Nmap,” SATIN - Sains dan Teknologi Informasi, vol. 7, no. 1, pp. 32–44, Jun. 2021, doi: 10.33372/stn.v7i1.702.

[18] N. Herawati, V. Budiyanto, and Uminingsih, “ANALISIS KEAMANAN SEBUAH DOMAIN MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) Zap,” JURNAL TEKNOLOGI TECHNOSCIENTIA, vol. 15, no. 2, pp. 27–36, Mar. 2023, doi: 10.34151/technoscientia.v15i2.4013.
[19] G. Gio, et al., “Analisis Perbandingan Tools SQL Injection Menggunakan SQLmap, SQLsus dan The Mole,” JURNAL INFORMATIK, vol. 18, no. 3, pp. 286–292, 2022.
[20] I. W. Wardhana and H. B. Seta, “Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ,” JURNAL INFORMATIK, vol. 17, no. 3, pp. 226–237, 2021.
[21] K. Umar, I. Riadi, M. Ihya, and A. Elfatiha, “Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF,” Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, vol. 12, no. 1, pp. 280–292, 2023.

UIN SUSKA RIAU
Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU