INFORMATION TECHNOLOGY RISK MANAGEMENT USING ISO 31000 BASED ON THE ISSAF PENETRATION TESTING FRAMEWORK

MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 BERBASIS KERANGKA KERJA PENGUJIAN PENETRASI ISSAF

Muhammad Egi Perdianza[1], Mgs Afriyan Firdaus[2*], Dwi Rosa Indah[3]
[1, 2, 3]Universitas Sriwijaya, Jl. Palembang – Prabumulih KM.32, Ogan Ilir, Sumatera Selatan, Indonesia
muhammadegiperdianza842@gmail.com[1], afriyan_firdaus@unsri.ac.id[2], indah812@unsri.ac.id[3]

Abstract – Information security is critical for higher education institutions, which manage large amounts of sensitive data in the digital age. Data breach incidents in Indonesia's academic sector reached 2,217 in 2021. A university website with 36 web-based information system services was found to have been defaced. SQL injection and XSS attacks, which can lead to data breaches, system manipulation, and disruption of academic services, are also common. These attacks underscore the importance of strong security measures to protect data and preserve the reputation of education. This research assesses the security risk of the XYZ University website using the ISSAF and ISO 31000. ISSAF was applied in four stages: information gathering, network mapping, vulnerability identification, and penetration testing with customization for university web systems. ISO 31000 was used to assess risk severity, resulting in classifications of two high, six medium, and twelve low risks. Security recommendations were developed to address the key risks and can be applied to other universities facing similar threats. The findings provide great insight for educational institutions to strengthen their cybersecurity. Implementing appropriate measures not only improves privacy, but also builds trust and reputation. Proactive information security is becoming a critical asset for the sustainability and credibility of higher education institutions in this vulnerable digital age.
Keywords - information security, Information System Security Assessment Framework, penetration testing, risk management, ISO 31000

Abstrak – Keamanan informasi sangat penting bagi lembaga pendidikan tinggi yang mengelola sejumlah besar data sensitive pada era digital. Insiden kebocoran data di sektor akademik Indonesia mencapai 2.217 pada tahun 2021. Laman situs web universitas yang memiliki 36 layanan sistem informasi berbasis web ditemukan telah mengalami defacement. Serangan SQL Injection dan XSS yang dapat mengakibatkan kebocoran data, manipulasi sistem, hingga gangguan layanan akademik juga kerap terjadi. Serangan ini menegaskan pentingnya langkah keamanan ketat untuk melindungi data dan menjaga reputasi pendidikan. Penelitian ini menilai risiko keamanan situs web Universitas XYZ menggunakan ISSAF dan ISO 31000. ISSAF diterapkan dalam empat tahap: pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, dan pengujian penetrasi dengan penyesuaian untuk sistem web universitas. ISO 31000 digunakan untuk mengevaluasi keparahan risiko, menghasilkan klasifikasi dua risiko tinggi, enam sedang, dan dua belas rendah.. Temuan ini memberi wawasan luas bagi institusi pendidikan dalam memperkuat keamanan siber mereka. Implementasi langkah-langkah tepat tidak hanya meningkatkan perlindungan data tetapi juga membangun kepercayaan dan reputasi. Keamanan informasi proaktif menjadi aset penting bagi keberlanjutan dan kredibilitas lembaga pendidikan tinggi di era digital yang rentan ini.
Kata Kunci - keamanan informasi, *Infomation System Security Assessment Framework*, pengujian penetrasi, manajemen risiko, ISO 31000

I. PENDAHULUAN

Pada era digital saat ini, hampir semua institusi perguruan tinggi di Indonesia menggunakan situs web untuk mengoptimalkan layanan informasi kampus. Universitas XYZ, sebagai salah satu perguruan tinggi negeri, memanfaatkan layanan berbasis web baik untuk pemberian informasi maupun dalam mendukung pengelolaan akademik dan non-akademik di lingkungan kampus. Universitas ini mengelola sejumlah besar data pribadi mahasiswa dan staf, termasuk data akademik dan keuangan, yang bersifat sensitif dan rahasia, sehingga rentan terhadap ancaman serangan siber. Dalam upaya memastikan keamanan informasi pada situs web, kombinasi Information System Security Assessment Framework (ISSAF) dan ISO 31000 memungkinkan deteksi kerentanan secara teknis sekaligus menganalisis dampak dan manajemen risiko secara strategis. ISSAF adalah kerangka kerja untuk pengujian penetrasi yang menyediakan panduan terstruktur bagi penguji dalam mengidentifikasi dan mengeksploitasi celah keamanan [1]. Di sisi lain, ISO 31000 adalah standar internasional yang berfokus pada manajemen risiko, memungkinkan organisasi untuk mengidentifikasi, mengevaluasi, dan memitigasi risiko berdasarkan ancaman yang ditemukan [2].

Universitas sering menjadi target utama serangan siber karena mereka menyimpan data sensitif dan mengoperasikan infrastruktur kritis [3]. Serangan seperti SQL Injection dan Cross-Site Scripting (XSS) kerap terjadi, yang dapat mengakibatkan kebocoran data, manipulasi sistem, hingga gangguan layanan akademik [4], [5]. Kebocoran data di sektor pendidikan, termasuk universitas, juga menjadi target signifikan bagi pelaku serangan siber, dengan laporan meningkatnya aktivitas serangan terhadap sektor akademik di Indonesia, mencapai 2.217 kasus web defacement pada tahun 2021 [6]. Serangan terhadap situs web instansi pendidikan harus menjadi perhatian khusus karena di dalamnya terdapat data pribadi penting, seperti identitas lengkap pelajar, pengajar, dan keluarga mereka. Sebagai contoh, salah satu universitas di Indonesia memiliki 36 layanan sistem informasi berbasis web yang dapat diakses melalui portal daringnya. Berdasarkan observasi pada 19 Mei 2021, ditemukan bahwa situs web universitas tersebut telah diserang, dengan salah satu laman yang mengalami *defacement* [7]. Kasus semacam ini menegaskan pentingnya penerapan langkah pencegahan yang efektif untuk menjaga keutuhan dan kerahasiaan data. Meskipun berbagai metode keamanan telah diterapkan, implementasinya sering kali kurang optimal, membuka peluang bagi peretas untuk mengeksploitasi sistem [8]. Oleh karena itu, dibutuhkan penilaian kerentanan secara berkala melalui pengujian penetrasi dan manajemen risiko menyeluruh. Penelitian ini bertujuan untuk mengidentifikasi jenis-jenis kerentanan yang terdapat di situs web Universitas XYZ dan mengevaluasi efektivitas penerapan ISSAF dan ISO 31000 dalam manajemen risiko. Selain itu, penelitian ini akan memberikan rekomendasi strategis untuk meningkatkan keamanan situs web guna mencegah kebocoran data dan serangan siber di masa mendatang[9]. Dengan adanya penelitian ini, diharapkan situs web Universitas XYZ dapat lebih aman dari ancaman eksternal dan operasional kampus dapat berlangsung dengan lancar.

II. SIGNIFIKANSI STUDI

A. Pengujian Penetrasi

Implementasi keamanan sistem bertujuan mengatasi masalah teknis dan nonteknis yang memengaruhi kinerja sistem seperti ketersediaan, kerahasiaan, dan integritas [10]. Pengujian penetrasi membantu mengidentifikasi kerentanan, kesalahan konfigurasi sistem, serta kelemahan operasional [11],[12]. Hal ini mendorong semakin banyak perusahaan menggunakannya untuk memastikan keamanan sistem informasi [13].

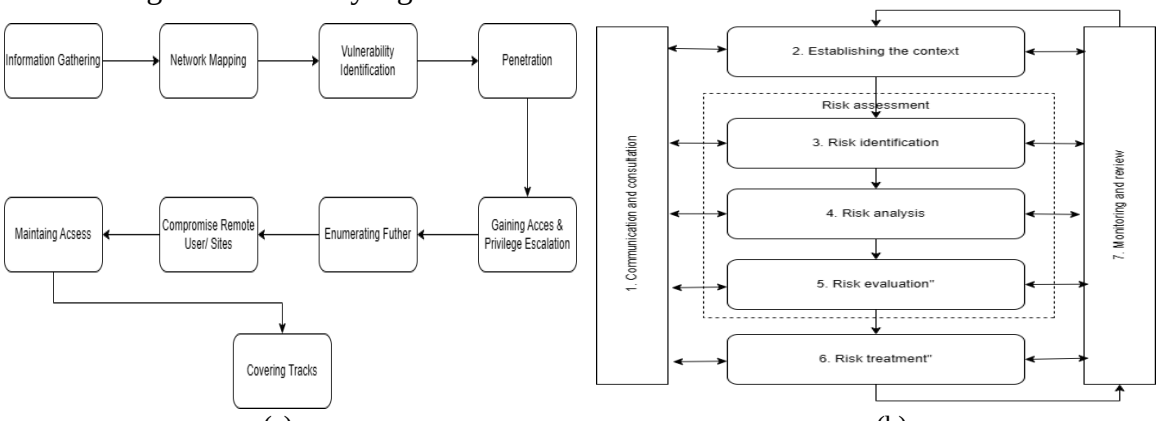
Pengujian real-time pada aplikasi web terbukti efektif meningkatkan keamanan dan mengidentifikasi celah [14], serta mengevaluasi kebijakan keamanan dan kesadaran karyawan terhadap keamanan [2], [10]. Proses ini meliputi pengumpulan data, penentuan titik penetrasi, dan pelaporan hasil [14], yang akan menjadi input penting dalam manajemen risiko, di mana setiap kerentanan dinilai berdasarkan ISO 31000 untuk menentukan dampak, probabilitas risiko, serta prioritas mitigasi. Evaluasi kerentanan dilakukan dalam kerangka ISO 31000 dalam menilai tingkat ancaman untuk merumuskan mitigasi yang tepat. Pengujian ini memberikan informasi rinci tentang ancaman aktual dan membantu organisasi mengatasi masalah keamanan dengan cepat [15].

B. Manajemen Resiko

Manajemen risiko adalah proses mengelola bahaya yang dihadapi organisasi, termasuk pemantauan, pengukuran, dan penilaian risiko [16]. Manajemen risiko sistem informasi yang efektif mengurangi frekuensi serta dampak insiden yang merugikan aset informasi. ISO 31000 menyediakan panduan umum yang perlu disesuaikan dengan konteks spesifik organisasi [17]. Dalam penelitian ini, hasil pengujian penetrasi dengan ISSAF memandu penilaian risiko pada kerangka ISO 31000, di mana kelemahan sistem dikelompokkan berdasarkan tingkat risiko dan prioritas penanganan. Integrasi ISSAF dan ISO 31000 memastikan identifikasi risiko serta mitigasi yang sesuai dengan kebutuhan organisasi. Manajemen risiko TI membantu eksekutif menghemat sumber daya dan mengintegrasikannya ke dalam manajemen risiko perusahaan secara keseluruhan serta memberikan panduan praktis bagi kepemimpinan [9].

C. Kerangka Kerja ISSAF

Open Information Systems Security Group (OISSG) mengembangkan *Information System Security Assessment Framework* (ISSAF) untuk menilai kontrol jaringan, sistem, dan aplikasi [18]. ISSAF menyediakan metodologi pengujian penetrasi yang komprehensif, membantu penguji menghindari kesalahan akibat serangan yang tidak terstruktur [19]. Framework ini terbagi dalam tiga tahap utama: perencanaan dan persiapan, penilaian dan laporan, serta pembersihan dan penghancuran artefak. Pada tahap perencanaan, informasi awal dipertukarkan dan persiapan dilakukan, dilanjutkan dengan sembilan langkah penilaian [9]. Setiap langkah tidak hanya berfokus pada identifikasi kerentanan tetapi juga pada penyediaan informasi yang mendukung manajemen risiko, sehingga organisasi dapat membuat keputusan yang lebih baik dalam mengatasi ancaman yang ditemukan.



(a) (b)

Gambar 1. (a) Metodologi Kerangka Kerja ISSAF (b) Manajemen Risiko ISO 31000[9]

Evaluasi dimulai dengan pengumpulan informasi umum dan jaringan target, diikuti pemindaian kerentanan dan simulasi penetrasi untuk mengidentifikasi celah keamanan. Setelah sistem

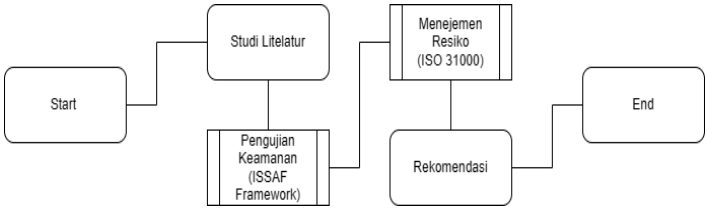
diakses, dilakukan eskalasi hak istimewa dan enumerasi informasi, termasuk password. Tahap selanjutnya melibatkan kompromi pengguna jarak jauh, penanaman backdoor, dan penghapusan jejak serangan, diakhiri dengan pembersihan data dan pelaporan hasil pengujian.

D. Kerangka Kerja ISO 31000

ISO 31000 adalah standar manajemen risiko internasional yang diterbitkan oleh *International Organization for Standardization* pada 13 November 2009, sebagai pengganti AS/NZS 4360:2004 [20],[21]. Standar ini menawarkan kerangka kerja komprehensif untuk berbagai organisasi, dengan pendekatan "*Plan-Do-Check-Action*" yang mencakup penilaian, penanganan, penetapan konteks, serta pemantauan risiko [15], [16], [21]. Integrasi ISO 31000 dan ISSAF memungkinkan evaluasi risiko berdasarkan hasil pengujian penetrasi, memastikan kelemahan keamanan dikelola secara sistematis, membantu universitas memprioritaskan perbaikan, dan mengurangi risiko pada sistem informasi mereka. Manajemen risiko melibatkan komunikasi, penetapan konteks, penilaian, penanganan, serta pemantauan risiko [9].

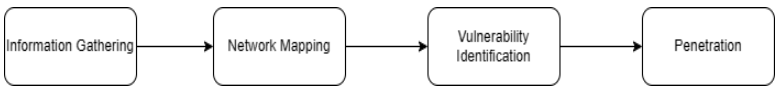
E. Metodologi Penelitian

Alur penelitian ini mencakup studi literatur, pengujian penetrasi dan manajemen risiko pada Situs Web Universitas XYZ, serta penyusunan rekomendasi berdasarkan hasil pengujian seperti yang diilustrasikan pada Gambar 2.



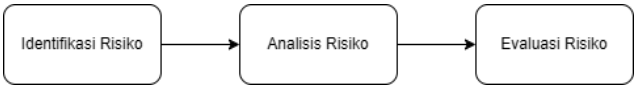
Gambar 2 Diagram alur Penelitian

Gambar 2 menunjukkan tahapan penelitian dimulai dengan studi literatur mengenai teknik serangan dan manajemen risiko di situs web Universitas XYZ. Selanjutnya, pengujian penetrasi menggunakan Framework ISSAF dilakukan untuk mengidentifikasi celah keamanan, diikuti dengan evaluasi risiko menggunakan ISO 31000 dan perumusan tindakan mitigasi. Penelitian diakhiri dengan rekomendasi untuk universitas atau institusi serupa. Dalam pengujian penetrasi menggunakan Framework ISSAF, terdapat empat tahap utama yang dilaksanakan, mengingat batasan izin yang diberikan oleh pihak terkait hanya mencakup hingga tahap penetrasi. Sub-tahapan pengujian penetrasi berdasarkan Framework ISSAF meliputi empat langkah yang diilustrasikan pada Gambar 3.



Gambar 3 Diagram alur Pengujian Penetrasi

Gambar 3 menampilkan alur pengujian penetrasi berdasarkan Framework ISSAF. Proses dimulai dari tahap *Information Gathering* umum tentang Situs Web Universitas XYZ, diikuti oleh *Network Mapping* untuk mendapatkan informasi spesifik terkait struktur jaringan. Tahap selanjutnya adalah *Vulnerability Identification* menggunakan berbagai tools untuk menemukan kelemahan, dan terakhir adalah *Penetration* (*Cross Site Scripting, Local File Inclusion, SQL Injection*) guna mengidentifikasi celah keamanan.



Gambar 4 Diagram alur Pengujian Penetrasi

Setelah penetration testing selesai, proses berlanjut ke manajemen risiko menggunakan ISO 31000, yang mencakup tiga langkah utama: identifikasi risiko, analisis risiko, dan evaluasi risiko, seperti pada Gambar 5. Identifikasi risiko di Situs Web Universitas XYZ mencakup gambaran dan dampaknya, dengan hasil pengujian penetrasi sebagai input utama. Analisis risiko menilai likelihood dan impact dari setiap risiko, sementara evaluasi risiko menentukan tingkat risiko berdasarkan perkalian nilai likelihood dan impact.

Integrasi ISSAF dan ISO 31000 dalam penelitian ini mengaitkan hasil pengujian penetrasi yang mengidentifikasi kerentanan sistem dan dievaluasi menggunakan kerangka manajemen risiko ISO 31000 untuk menentukan tingkat risiko dan prioritas mitigasi. Dengan demikian, pengujian penetrasi tidak hanya mengungkapkan masalah keamanan, tetapi juga memberikan dasar yang kuat untuk pengambilan keputusan terkait kebijakan keamanan di Universitas XYZ. Implementasi rekomendasi berdasarkan analisis ISSAF dan ISO 31000 dapat mengarah pada kebijakan keamanan yang lebih kuat dan lebih efektif di universitas, yang pada akhirnya akan melindungi data sensitif dan meningkatkan kepercayaan publik terhadap keamanan informasi lembaga pendidikan.

III. HASIL DAN PEMBAHASAN

A. Pengaturan Eksperimen

Penelitian ini menggunakan pendekatan sistematis dengan dua langkah utama yaitu pengujian penetrasi dan manajemen risiko. Tujuannya adalah untuk mengidentifikasi dan mengatasi potensi celah keamanan pada situs web Universitas XYZ. Pengujian ini dilakukan menggunakan kerangka kerja ISSAF yang berjalan di dua sistem operasi: Windows 11 dan Kali Linux, yang dipilih karena kelengkapan alat-alat pengujian penetrasi yang dapat digunakan. Kedua sistem ini memberikan fleksibilitas dalam mengidentifikasi potensi kerentanan pada tingkat aplikasi dan jaringan.

B. Pengujian Penetrasi menggunakan Framework ISSAF

Pengujian penetrasi yang dilakukan melalui empat tahap utama: pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, dan pengujian penetrasi. Setiap tahap memiliki peran penting dalam menganalisis keamanan sistem. Detail mengenai kontribusi tiap alat yang digunakan dijelaskan pada tahap-tahap berikut:

1. Analisis Hasil Pengumpulan Informasi

   Tabel 1 menyajikan hasil dari pengumpulan informasi menggunakan berbagai tools seperti Whois Domain, Reverse IP Lookup Scanner, dan Spamhaus. Dari total 30 informasi yang diinginkan, 18 informasi berhasil diperoleh, dengan tingkat keberhasilan sebesar 60%. Temuan ini menunjukkan tingginya tingkat eksposur informasi publik pada domain xyz.ac.id, yang memudahkan peretas untuk menyusun strategi serangan lebih lanjut. Informasi seperti DNS, alamat IP, dan server otoritatif yang berhasil diidentifikasi menjadi landasan bagi serangan berikutnya.

TABEL I
HASIL UJI PENGUMPULAN INFORMASI

Konten	Tools	xyz.ac.id	reg.xyz.ac.id	ppid.xyz.ac.id
Locate the target web presence	Whois Domain	✓	X	X
Find Out domain registration info	Whois Domain	✓	X	X

Konten	Tools	xyz.ac.id	reg.xyz.ac.id	ppid.xyz.ac.id
Check for the Authoritative Name Servers	Whois Domain	✓	X	X
Check for Reverse DNS lookup presence	Dig	X	X	X
Check for Reverse IP lookup presence	Reverse IP	✓	✓	✓
Check Spam/Attackers databases lookup	Lookup Scanner Spamhaus, Spamcom	✓	✓	✓
Check to change WHOIS information	Whois Domain	✓	✓	✓
Search System/Network Survey Sites	Netcraft	✓	✓	✓
Search on Internet Relay Chat	miRC	X	X	X
Search Underground Sites	NMAP	✓	✓	✓

2. Analisis Pemetaan Jaringan

Tahap ini menggunakan Nmap dan Traceroute dan lin-lain untuk mengidentifikasi topologi jaringan dan layanan yang berjalan. Hasil yang disajikan dalam Tabel 2 mengungkapkan bahwa 15 dari 21 jenis informasi berhasil dikumpulkan. Temuan penting meliputi port SSH (22), HTTP (80), dan HTTPS (443) yang terbuka di seluruh domain. Hal ini membuka peluang bagi penyerang untuk melakukan serangan brute force atau mengeksploitasi kerentanan web yang ditemukan pada layanan-layanan ini.

TABEL II
HASIL UJI PEMETAAN JARINGAN

Kategori	Tools	xyz.ac.id	reg.xyz.ac.id	ppid.xyz.ac.id
Identify Live Host	Nmap	✓	✓	✓
TCP Port Scanning	Nmap	✓	✓	✓
UDP Port Scanning	Nmap	X	X	X
Banner Grabbing	Nmap	✓	✓	✓
ARP Discovery	Arping	X	X	X
Identify Perimeter Network	Traceroute	✓	✓	✓
Perform FIN/ACK Scan	Nmap	✓	✓	✓

3. Analisis Identifikasi Kerentanan

Pada Tabel 3, hasil identifikasi kerentanan menunjukkan bahwa domain xyz.ac.id memiliki beberapa kerentanan tingkat tinggi seperti Blind SQL Injection dan Cross-Site Scripting (XSS). Kerentanan ini dapat dimanfaatkan dalam serangan nyata, seperti mengakses data pengguna atau mengubah data tanpa izin yang dapat menyebabkan gangguan serius pada operasional situs. Sementara itu, domain lainnya, seperti reg.xyz.ac.id, menunjukkan kerentanan tingkat sedang, seperti file .htaccess yang dapat dibaca, yang memungkinkan penyerang mengakses pengaturan server untuk eksploitasi lebih lanjut.

TABEL III
HASIL UJI IDENTIFIKASI KERENTANAN

Domain	Kerentanan	Tingkat
xyz.ac.id	Blind SQL Injection	Tinggi
	Cross site scripting	Tinggi
	Folder backup	Sedang
	HTML form without CSRF protection	Sedang
	PHP allow_url_fopen enabled	Sedang
	File upload	Rendah
reg.xyz.ac.id	Blind SQL Injection	Tinggi
	. htaccess file readable	Sedang
	HTML form without CSRF protection	Sedang
	Clickjacking: X-Frame-Options header missing	Rendah

	Cookie(s) without HttpOnly flag set	Rendah
	Possible sensitive files	Rendah
ppid.xyz.ac.id	Content Security Policy (CSP) not implemented	Informasi
	Error page web server version disclosure	Informasi

4. Analisis Hasil Pengujian Penetrasi

Pada Tabel 4 dapat terlihat hasil pengujian penetrasi menunjukkan keberhasilan serangan SQL Injection pada dua domain: xyz.ac.id dan ppid.xyz.ac.id. Serangan ini dilakukan dengan memanfaatkan parameter POST dan GET tanpa validasi yang memadai, sehingga penyerang dapat mengakses dan memodifikasi basis data. Namun, pengujian *Cross-Site Scripting* (XSS) dan *Local File Inclusion* (LFI) pada beberapa subdomain gagal, yang mengindikasikan bahwa mekanisme keamanan untuk serangan tersebut bekerja dengan baik, meski masih memerlukan penguatan lebih lanjut.

TABEL IV
HASIL UJI PENETRASI

Domain	Metode Serangan	Lokasi Kerentanan	Hasil
xyz.ac.id	SQL Injection	Permintaan POST ke https://xyz.ac.id/wisuda/ yang menargetkan field input idprodi dengan payload seperti 0'XOR(if(now()=sysdate(),sleep(12), 0))XOR'Z	✓
	Cross Site Scripting	-	X
	Local File Inclusion (LFI)	-	X
reg.xyz. ac.id	SQL Injection	-	X
	Cross Site Scripting	-	X
	Local File Inclusion (LFI)	-	X
ppid.xyz. ac.id	SQL Injection	Permintaan GET ke /page.php?idn=79	✓
	Cross Site Scripting	-	X
	Local File Inclusion (LFI)	-	X

C. Manajemen Resiko menggunakan ISO 31000

Proses manajemen risiko dilakukan menggunakan kerangka kerja ISO 31000, dengan tiga langkah utama: identifikasi risiko, analisis risiko, dan evaluasi risiko. Hasil analisis kerentanan dari pengujian penetrasi digunakan untuk menyusun daftar risiko teridentifikasi, yang disajikan dalam Tabel 5.

1. Identifikasi Risiko

Tabel 5 menunjukkan 22 risiko spesifik yang ditemukan selama pengujian, masing-masing dikategorikan berdasarkan sumber risiko dan dampaknya. Beberapa risiko dengan potensi dampak besar seperti Blind SQL Injection (R10) dan Cross-site Scripting (R11) memerlukan mitigasi segera karena dapat mempengaruhi data dan operasional situs web universitas.

TABEL V
TABEL HASIL IDENTIFIKASI RISIKO

Kode Risiko	Sumber Risiko	Deskripsi Risiko	Dampak
R1	Check for Reverse IP Lookup Presence	Identifikasi domain lain terkait IP sama.	Memungkinkan serangan terkoordinasi antar domain.
R2	Check Spam/ Attackers Databases Lookup	Domain terdeteksi di database spam/penyerang.	Dapat memicu serangan lanjutan karena reputasi buruk.
R3	Check to Change WHOIS Information	Informasi WHOIS diubah oleh penyerang.	Dapat menyebabkan kebingungan atau kehilangan kontrol atas domain oleh pemilik sah.
R4	Search System/Network Survey Sites	Informasi sistem dikumpulkan dari survei.	Memberikan informasi kepada penyerang tentang arsitektur sistem yang dapat dieksploitasi.
R5	Identify Live Host	Host aktif teridentifikasi.	Memberikan titik awal serangan.
R6	TCP Port Scanning	Port TCP terbuka ditemukan	Layanan rentan dapat dieksploitasi.
R7	Banner Grabbing	Versi perangkat lunak terungkap.	Eksploitasi kerentanan versi tertentu.
R8	Identify Perimeter Network	Perimeter jaringan teridentifikasi.	Memudahkan penyerang dalam merencanakan serangan berdasarkan titik lemah dalam perimeter.
R9	Perform FIN/ACK Scan	Firewall dan konfigurasi terungkap.	Penyerang mengidentifikasi celah untuk serangan.
R10	Blind SQL Injection	Injeksi SQL terjadi via POST yang menargetkan field input idprodi dan Permintaan GET ke /page.php?idn=79	Penyerang dapat mengakses dan memodifikasi basis data tanpa izin, berpotensi menyebabkan kebocoran data sensitif dan manipulasi informasi yang merugikan operasional.
R11	Cross Site Scripting (XSS)	XSS pada form input xyz.ac.id.	Jika berhasil, Penyerang bisa mencuri data dan mengambil alih akun.
R12	Folder Backup	File backup dapat diakses tanpa otentikasi.	Kebocoran data dan potensi serangan lanjutan.
R13	HTML Form without CSRF Protection	Form HTML di xyz.ac.id tidak memiliki perlindungan CSRF.	Penyerang bisa memanipulasi data tanpa sepengetahuan pengguna.
R14	PHP allow_url_fopen Enabled	Konfigurasi PHP tidak aman (allow_url_fopen aktif).	Potensi eksekusi skrip berbahaya dari sumber luar.
R15	File Upload Vulnerability	Terdapat kerentanan terkait upload file yang tidak terverifikasi.	Penyerang dapat mengunggah file berbahaya ke server, berpotensi menjalankan kode jahat atau menyebabkan kerusakan pada sistem.
R16	. htaccess File Readable	File .htaccess terbaca publik.	Informasi aturan server terekspos, memudahkan eksploitasi.
R17	Clickjacking: X-Frame-Options Header Missing	Header X-Frame-Options tidak ada. Potensi clickjacking.	Pengguna bisa ditipu berinteraksi dengan situs berbahaya.
R18	Cookies without HttpOnly Flag Set	Cookie tanpa atribut HttpOnly.	Potensi pencurian sesi pengguna via XSS.
R19	Possible Sensitive Files	File sensitif terungkap.	Memberikan informasi untuk serangan privilege escalation.
R20	Content Security Policy (CSP) Not Implemented	CSP tidak diterapkan.	Risiko XSS meningkat.
R21	Error Page Web Server Version Disclosure	Versi server terungkap di halaman error.	Memudahkan eksploitasi kerentanan server.
R22	Local File Inclusion (LFI)	Kerentanan LFI tidak teridentifikasi, Potensi akses ke file lokal server.	Jika berhasil, penyerang dapat mengambil informasi sensitif dari file lokal, yang berpotensi mengancam keamanan sistem secara keseluruhan.

2. Analisis Risiko

Penilaian risiko didasarkan pada skala likelihood dan impact dengan skor 1 hingga 5. Penilaian dilakukan dengan menggunakan best practices dari ISO 31000, yang telah disesuaikan dengan konteks keamanan institusi pendidikan. Setiap tingkat kriteria, baik untuk kemungkinan (Tabel 6) maupun dampak (Tabel 7), telah dikalibrasi dengan data historis serangan yang pernah terjadi di universitas lain

TABEL VI
TABEL KRITERIA KEMUNGKINAN

Kemungkinan		Keterangan
Peringkat	Kriteria	
1	Rare(Langka)	Hampir tidak pernah terjadi
2	Unlikely(Tidak mungkin)	Mungkin tapi jarang
3	Possible(Mungkin)	Itu mungkin terjadi kadang-kadang
4	Likely(Kemungkinan)	Kemungkinan besar terjadi (sering)
5	Almost Certain(Hampir Pasti)	Pasti Hampir selalu terjadi

TABEL VII
TABEL KRITERIA DAMPAK

Dampak		**Keterangan**
Peringkat	**Kriteria**	
1	Insignificant(Tidak signifikan)	Informasi umum diperoleh, tidak menyebabkan kerusakan pada keamanan system
2	Minor(Kecil)	Informasi tentang keamanan sistem diperoleh tetapi tidak berdampak pada kerusakan sistem dan kebocoran data sensitif
3	Moderate(Sedang)	Beberapa data sensitif diperoleh, lubang keamanan untuk akses tidak sah sulit diperoleh, dan tidak berdampak pada kerusakan system
4	Major(Besar)	Beberapa data sensitif diperoleh, celah keamanan untuk akses tidak sah mudah diperoleh, menyebabkan sedikit kerusakan pada sistem
5	Catastrophic(Bencana)	Semua data sensitif diperoleh, sebagian besar sistem dapat rusak sehingga mengganggu layanan informasi sistem

3. Evaluasi Risiko

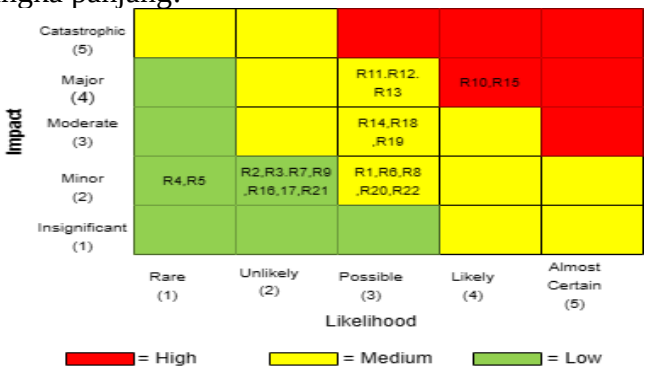
Hasil penilaian likelihood dan impact disajikan dalam Tabel 8. Setiap risiko dikategorikan dalam tiga tingkatan: tinggi, sedang, dan rendah, berdasarkan hasil dari panel ahli yang terdiri dari tim IT security dan stakeholders utama. Metodologi ini memastikan bahwa penilaian risiko konsisten dan dapat digunakan untuk menentukan langkah mitigasi yang paling efektif.

TABEL VIII
TABEL HASIL ANALISIS RISIKO

Kode Risiko	Kemungkinan	Dampak
R1	Possible (3)	Minor (2)
R2	Unlikely (2)	Minor (2)
R3	Unlikely (2)	Minor (2)
R4	Rare (1)	Minor (2)
R5	Rare (1)	Minor (2)
R6	Possible (3)	Minor (2)
R7	Unlikely (2)	Minor (2)
R8	Possible (3)	Minor (2)
R9	Unlikely (2)	Minor (2)
R10	Likely (4)	Major (4)
R11	Possible (3)	Major (4)
R12	Possible (3)	Major (4)
R13	Possible (3)	Major (4)
R14	Possible (3)	Moderate (3)
R15	Likely (4)	Major (4)
R16	Unlikely (2)	Minor (2)

R17	Unlikely (2)	Minor (2)
R18	Possible (3)	Moderate (3)
R19	Possible (3)	Moderate (3)
R20	Possible (3)	Minor (2)
R21	Unlikely (2)	Minor (2)
R22	Possible (3)	Minor (2)

Gambar 5 menunjukkan matriks evaluasi risiko yang mengidentifikasi konsentrasi risiko di area web application security dan access control. Beberapa risiko dengan level tinggi (R10 dan R15) memerlukan perhatian segera, sementara risiko lainnya berada di zona medium yang masih memerlukan mitigasi jangka panjang.



Gambar 5 Hasil Matriks Evaluasi Risiko

Berdasarkan hasil evaluasi, rekomendasi difokuskan pada risiko tinggi dan sedang seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan *File Upload Vulnerability*. Implementasi *Content Security Policy* (CSP), penggunaan parameterized queries, dan perlindungan CSRF pada form web diharapkan mampu memitigasi risiko signifikan terhadap keamanan situs web ini. Rekomendasi pada risiko tingkat rendah disederhanakan atau dihilangkan karena tidak berkontribusi signifikan pada risiko keseluruhan.

D. Rekomendasi

Tabel 9 menyajikan rekomendasi pencegahan untuk risiko-risiko yang teridentifikasi, dengan fokus pada risiko tinggi dan sedang. Solusi yang diusulkan mencakup penerapan *parameterized queries* untuk mencegah *SQL Injection*, peningkatan perlindungan *Content Security Policy* (CSP) untuk mengurangi risiko XSS, dan pembatasan akses pada file backup untuk mencegah kebocoran data. Implementasi setiap rekomendasi dibagi menjadi tiga fase: immediate, short-term, dan long-term, masing-masing dengan target keberhasilan spesifik.

TABEL IX
REKOMENDASI PENCEGAHAN RISIKO

Kode Resiko	Tingkatan	Rekomendasi
R10	High (Likely + Major)	- Terapkan validasi input yang ketat dan gunakan parameterized queries untuk mencegah Blind SQL Injection. - Monitor log server secara rutin untuk mendeteksi aktivitas mencurigakan terkait SQL Injection.
R11	High (Possible + Major)	- Gunakan Content Security Policy (CSP) untuk meminimalisir risiko Cross Site Scripting (XSS). - Terapkan filter pada input untuk mencegah injeksi skrip berbahaya.
R12	High (Possible + Major)	- Pastikan akses ke file backup dibatasi hanya kepada pengguna yang sah. - Implementasikan enkripsi pada backup dan hapus file yang tidak diperlukan dari server.

R13	High (Possible + Major)	- Tambahkan perlindungan Cross-Site Request Forgery (CSRF) pada semua form di website untuk mencegah perubahan data tanpa otorisasi. - Audit form secara berkala untuk memeriksa adanya kelemahan.
R15	High (Possible + Major)	- Terapkan validasi ketat pada file upload, batasi tipe file yang diizinkan, dan gunakan sandboxing untuk mencegah eksekusi kode berbahaya. - Pastikan ada otentikasi sebelum upload file.
R16	Medium (Possible + Moderate	- Tambahkan atribut HttpOnly dan Secure pada cookies untuk mencegah serangan XSS dan melindungi data sesi pengguna. - Lakukan audit keamanan cookies secara rutin.
R19	Medium (Possible + Moderate	- Lakukan audit keamanan untuk memastikan file sensitif terlindungi dengan baik dan tidak terekspos ke publik. - Gunakan enkripsi dan batasi akses ke file sensitif.
R20	Medium (Possible + Moderate	- Implementasikan Content Security Policy (CSP) untuk melindungi dari serangan XSS dengan membatasi skrip yang dapat dijalankan di halaman web. - Perbarui konfigurasi keamanan web server.

Hasil dari penelitian ini dapat diadopsi sebagai template untuk pengembangan framework keamanan pada institusi pendidikan lain yang memiliki kebutuhan keamanan serupa. framework ini dapat diadaptasi sesuai dengan karakteristik dan kebutuhan masing-masing institusi.

IV. KESIMPULAN

Penelitian ini mengadopsi tahapan pengujian penetrasi menggunakan kerangka kerja ISSAF dan prinsip manajemen risiko ISO 31000 untuk menganalisis dan mengatasi risiko keamanan pada situs web Universitas XYZ. Proses pengujian penetrasi ISSAF terdiri dari empat langkah utama, yaitu pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, dan penetrasi yang dilaksanakan dengan memperhatikan batasan. Melalui proses ini, teridentifikasi beberapa celah keamanan, seperti *Blind SQL Injection*, akses tidak aman terhadap file cadangan, dan kurangnya perlindungan terhadap CSRF, XSS dan lain-lain. *Blind SQL Injection*, sebagai salah satu kerentanan tingkat tinggi, memungkinkan penyerang untuk memodifikasi kueri basis data yang dapat mengakibatkan pencurian data sensitif atau perubahan data yang merusak, seperti nilai akademik mahasiswa. Kerentanan unggahan file juga memungkinkan penyerang untuk memasukkan file berbahaya ke dalam sistem, yang dapat menyebabkan peretasan lebih lanjut atau merusak sistem internal universitas.

Proses manajemen risiko mengikuti kerangka kerja ISO 31000, yang meliputi pengidentifikasian risiko, analisis risiko, dan evaluasi risiko. Output dari pengujian penetrasi digunakan sebagai informasi utama dalam tahap identifikasi risiko. Evaluasi risiko mengungkapkan dua risiko dengan tingkat tinggi, yaitu *Blind SQL Injection* dan kerentanan terkait unggahan file. Langkah mitigasi, seperti pembatasan akses unggahan file dan penerapan kebijakan filter yang lebih ketat, telah mengurangi potensi ancaman dari kerentanan ini. Selain itu, terdapat enam risiko dengan tingkat sedang, termasuk kerentanan XSS dan akses tidak aman terhadap file sensitif, serta beberapa risiko dengan tingkat rendah yang tidak berpengaruh signifikan terhadap sistem. Untuk kerentanan XSS, meskipun beberapa risiko masih memerlukan peningkatan lebih lanjut, mitigasi awal telah berhasil menurunkan risiko serangan dengan menambah lapisan verifikasi input dan pengaturan kebijakan keamanan yang lebih ketat. Penanganan risiko tingkat tinggi dan sedang diberikan prioritas untuk menjaga integritas dan keamanan situs Universitas XYZ.

REFERENSI

[1] F. R. Mahtuf, P. Hatta, and E. S. Wihidiyat, "Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan," *Journal of Information Technology and Computer Science (JOINTECS)*, vol. 4, no. 1, 2019.

[2] U. Nugraha and R. Istambul, "Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment," 2019. [Online]. Available: www.ijicc.net

[3] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," May 03, 2020, *Taylor and Francis Inc.* doi: 10.1080/08874417.2018.1432996.

[4] V. Vikas, G. Saisri, T. S. Meghana, A. S. Harshini, and G. Kaveri, "Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security," *Int J Res Appl Sci Eng Technol*, vol. 11, no. 7, pp. 794–805, Jul. 2023, doi: 10.22214/ijraset.2023.54658.

[5] A. K. Priyanka and S. S. Smruthi, "WebApplication Vulnerabilities:Exploitation and Prevention," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2020, pp. 729–734. doi: 10.1109/ICIRCA48905.2020.9182928.

[6] Tedyyana, Agus, et al. "Enhance Telecommunication Security Through the Integration of Support Vector Machines." *International Journal of Advanced Computer Science & Applications* 15.3 (2024).

[7] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *Jurnal Komtika (Komputasi dan Informatika)*, vol. 5, no. 1, pp. 35–42, Jul. 2021, doi: 10.31603/komtika.v5i1.5134.

[8] D. R. Sahu and D. S. Tomar, "Analysis of Web Application Code Vulnerabilities using Secure Coding Standards," *Arab J Sci Eng*, vol. 42, no. 2, pp. 885–895, Feb. 2017, doi: 10.1007/s13369-016-2362-5.

[9] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. Sri Arsa, "Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city)," *International Journal of Computer Network and Information Security*, vol. 12, no. 4, pp. 30–40, Aug. 2020, doi: 10.5815/ijcnis.2020.04.03.

[10] I. Riadi, S. Sunardi, and E. Handoyo, "Security Analysis of Grr Rapid Response Network using COBIT 5 Framework," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, p. 29, May 2019, doi: 10.24843/lkjiti.2019.v10.i01.p04.

[11] M. Z. Hasan, M. Z. Hussain, M. Taimoor, and A. Chughtai, "Penetration Testing In System Administration," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 6, no. 06, 2017, [Online]. Available: www.ijstr.org

[12] A. G. Bacudio, X. Yuan, B. T. Bill Chu, and M. Jones, "An Overview of Penetration Testing," *International Journal of Network Security & Its Applications*, vol. 3, no. 6, pp. 19–38, Nov. 2011, doi: 10.5121/ijnsa.2011.3602.

[13] M. Mirjalili, A. Nowroozi, and M. Alidoosti, "A survey on web penetration test," 2014. [Online]. Available: https://www.researchgate.net/publication/270523617

[14] Tedyyana, Agus, et al. "Transforming the voting process integrating blockchain into e-voting for enhanced transparency and securiy." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 22.2 (2024): 311-320.

[15] B. Vito Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web," 2017. [Online]. Available: http://j-ptiik.ub.ac.id

[16] N. Zukhrufatul Firdaus, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)," 2018. [Online]. Available: http://j-ptiik.ub.ac.id

[17] P. Sukapto, J. D. H. Desena, P. K. Ariningsih, and S. Susanto, "Integration of risk engineering by ISO 31000 and safety engineering: A case study in a production floor of sport footwear industry in Indonesia," *International Journal of Simulation: Systems, Science and Technology*, vol. 19, no. 4, pp. 22.1-22.12, 2018, doi: 10.5013/IJSSST.a.19.04.22.

[18] B. Rathore *et al.*, "Information Systems Security Assessment Framework (ISSAF) draft 0.2," 2005.

[19] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, "Analisis Uji Penetrasi Menggunakan ISSAF," *Hacking Digit. Forensics Expo*, pp. 32–40, 2017.

[20] A. Lubis and A. Tarigan, "Security Assessment of Web ApplicationThrough Penetration System Techniques," *Jend. Gatot Subroto Km*, vol. 4, no. 100, pp. 296–303, 2017.

[21] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)."