Vulnerability Assessment And Penetration Testing (Vapt) Pada *Website* Layanan Akademik Universitas Xyz

1st Ridwan Gymnatsiar
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ridwangymnatsiar@student.telkomuniversity.ac.id

2nd Umar Yunan Kurnia Septo Hediyanto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

3rd Muhammad Fathinuddin
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
muhammadfathinuddin@telkomuniversity.ac.id

***Abstrak* — Banyak perusahaan maupun organisasi mulai menggunakan *website* dalam menjalankan proses bisnis dan memberikan layanan. Tetapi dalam penggunaannya, sering ditemukan adanya kekurangan yang muncul dari *website*. *Vulnerability Assessment and Penetration Testing (VAPT)* merupakan metode yang digunakan dalam analisis dan pengujian dari kerentanan yang dimiliki oleh *website*. Universitas XYZ menggunakan *website* dalam menjalankan proses bisnis dan pengelolaan data, seperti layanan akademik. Penerapan dari aspek keamanan informasi sudah diterapkan didalam sistem. Terdapat kekurangan dalam penerapannya dengan adanya kerentanan yang muncul dari proses *vulnerability detection*. Perlu adanya evaluasi kembali dalam menjaga aspek keamanan informasi sudah diterapkan pada *website*. Dalam pengujian dari celah keamanan *website* layanan akademik Universitas XYZ, penulis memilih menggunakan metode *Vulnerability Assessment and Penetration Testing (VAPT)* dengan menggunakan beberapa *tools* seperti *NMAP*, *Nessus*, *OWASP ZAP*, dan *Burp suite* kemudian dibuatkan reporting. Dasar dari pemilihan metode ini yaitu dapat menyesuaikan dari kebutuhan pengujian sesuai dengan *scope* yang sudah ditentukan dan melakukan *remediation* sebagai upaya evaluasi keamanan dari pengujian sistem *website*. Hasil dari *vulnerability detection* ditemukan beberapa kerentanan dengan kategori risiko masing - masing. Kerentanan yang ditemukan dilakukan proses *remediation* dengan melakukan *update* dari versi terbaru hingga konfigurasi ulang dari *file website*. Kerentanan yang tidak berhasil diperbaiki akan menjadi rekomendasi mitigasi sistem.**

***Kata kunci*— *vulnerability*, celah keamanan, *vulnerability assessment*, *penetration testing*, *vapt*, *website* layanan akademik universitas xyz**

I. PENDAHULUAN

Teknologi mengalami perkembangan yang sangat pesat, salah satunya yaitu penggunaan *website*. Banyak perusahaan maupun organisasi mulai menggunakan *website* dalam menjalankan proses bisnis dan memberikan layanan kepada pelanggan. Tetapi dalam penggunaannya, sering ditemukan adanya kekurangan yang muncul dari *website* itu sendiri. Kekurangan ini bisa memunculkan celah kerentanan yang bisa berakibat fatal bagi *website*. *Vulnerability* merupakan kerentanan dari suatu sistem atau jaringan yang memungkinan adanya akses tanpa izin oleh orang yang tidak bertanggung jawab. Kerentanan ini bisa muncul dari pengelolaan keamanan yang kurang dari pihak pengembang *website* maupun terdapat bug yang tidak diketahui dan belum diperbaiki. Jika kerentanan pada *website* tidak diperbaiki, maka dapat memunculkan peluang terkena serangan siber dan menimbulkan kerugian bagi perusahaan atau organisasi.

Universitas XYZ adalah perusahaan yang bergerak di bidang pendidikan dan memiliki beberapa fakultas yang dimiliki. Universitas XYZ menggunakan *website* dalam menjalankan proses bisnis dan pengelolaan data, seperti pengelolaan keuangan dan layanan akademik. Dalam *website* layanan akademik terdapat informasi yang bersifat rahasia, seperti data Nomor Induk Mahasiswa (NIM) , Nomor Induk Pegawai (NIP), tempat tanggal lahir pengguna, alamat pengguna, dan lainnya.

Pentingnya dalam menjaga informasi yang dimiliki oleh *website* sehingga perlu adanya penerapan aspek dari keamanan informasi yang terdiri dari *Confidentiality, Integrity*, dan *Availibility* (Andress, 2014). Penerapan dari aspek keamanan informasi pada *website* Universitas XYZ dalam upaya menjaga keamanan data sudah diterapkan didalam sistem. Tetapi terdapat kekurangan dalam penerapannya dengan adanya kerentanan yang muncul dari proses *vulnerability detection*. Sehingga dalam hal ini perlu adanya evaluasi kembali dalam menjaga aspek keamanan informasi sudah diterapkan pada *website*.

Dalam pengujian dari celah keamanan *website* layanan akademik Universitas XYZ, penulis memilih menggunakan metode *Vulnerability Assessment and Penetration Testing (VAPT)* dengan menggunakan beberapa *tools* seperti *NMAP*, *Nessus*, *OWASP ZAP*, dan *Burp suite* kemudian dibuatkan reporting. Dengan metode ini dapat dijelaskan celah apa yang dimiliki oleh *website* berikut dengan bukti pengujian dan diberikan rekomendasi dalam melakukan mitigasi sistem.

II. KAJIAN TEORI

Adapun kajian teori yang berkaitan dengan variabel - variabel penelitian disajikan dalam pembahasan berikut.

A. Keamanan Informasi

Keamanan informasi merupakan upaya perlindungan terhadap sistem dan hardware yang digunakan yang memiliki informasi penting (Michael E. Whitman, 2013). Keamanan

informasi juga termasuk kedalam regulasi yang ada di industri untuk memastikan semua organisasi atau perusahaan memiliki tingkat keamanan informasi yang sama (ISO/IEC 27001:2013). Pentingnya keamanan informasi yaitu untuk mencegah dan menghadapi setiap ancaman yang bisa muncul kepada sistem dan hardware yang kita gunakan, terutama data data penting yang ada didalamnya dan bagi organisasi atau perusahaan bisa menjaga kepercayaan publik. Aspek dari keamanan informasi harus dapat dipenuhi semua sehingga jika salah satu aspek tidak dapat terpenuhi maka terjadi kegagalan dalam penerapan keamanan informasi. Terdapat 3 (tiga) aspek yang harus diperhatikan dalam keamanan informasi berdasarkan konsep *CIA Triad* (Andress, 2014) yaitu sebagai berikut :

1. *Confidentiality*

Merupakan aspek yang menjelaskan data hanya bisa diakses oleh orang yang berwenang, sehingga menjamin kerahasiaan data.

2. *Integrity*

Merupakan aspek yang menjelaskan data tidak dapat dirubah atau dimodifikasi tanpa seizin dari pihak yang berwenang, sehingga menjamin keutuhan data.

3. *Availibility*

Merupakan aspek yang menjelaskan data harus bisa diakses ketika dibutuhkan oleh pengguna tanpa hambatan.

B. Vulnerability

Vulnerability dalam bahasa Indonesia diartikan sebagai kerentanan. Didalam sistem komputer terdapat *vulnerability* yang bisa berdampak buruk ketika diketahui oleh orang yang tidak bertanggung jawab. Salah satu bahaya dari adanya *vulnerability* yaitu adanya pengambilan alih kontrol sistem operasi ataupun *database* server yang bisa menyebabkan kerugian (Cross, 2007). Banyak kasus yang terjadi dikarenakan *vulnerability* dari sistem tidak diperbaiki, seperti kasus pencurian data.

C. Vulnerability assessment and penetration testing (vapt)

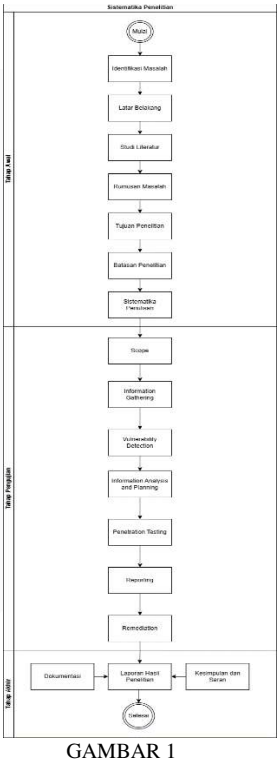
Vulnerability Assessment and Penetration Testing (VAPT) merupakan metode yang digunakan dalam memberikan penilaian terhadap keamanan sistem. Fungsi dari metode ini yaitu melakukan identifikasi dan evaluasi dari kelemahan yang dimiliki *website* kemudian memberikan rekomendasi dalam melakukan mitigasi sistem untuk mengurangi potensi terjadinya serangan siber (Umrao et al., n.d.). *Vulnerability Assessment and Penetration Testing (VAPT)* terdiri dari 2 proses utama, yaitu *Vulnerability Assessment* dan *Penetration Testing*. *Vulnerability Assessment* merupakan proses identifikasi dan evaluasi dari sistem yang digunakan dengan mengetahui celah keamanan dari sistem. Tujuan dari *Vulnerability Assessment* ini yaitu mencegah serangan siber yang bisa berdampak buruk kepada sistem yang digunakan (P. S. Shinde and S. B. Ardhapurkar , 2016). *Penetration Testing* merupakan proses pengujian mendapatkan akses secara tidak resmi kepada sistem yang telah diberikan izin untuk uji coba. *Penetration Testing* biasa diketahui merupakan usaha meretas/membobol suatu sistem sehingga memiliki tingkat kesulitan tersendiri (Lamba, 2020)

D. *Common VULNERABILITIES And Exposures*

CVE adalah merupakan *database* yang berukuran besar yang memiliki informasi mengenai berbagai macam *vulnerabilities* atau celah keamanan yang biasa digunakan oleh ahli sekuritas dalam melakukan evaluasi keamanan sistem mereka. *CVE* dikelola oleh *National Vulnerability Database* (NVD) di Amerika Serikat. *CVE* sendiri sering mendapatkan pembaharuan dan setiap *vulnerabilities* yang ditemukan akan masuk kedalam *database* dan dicatat dengan numerik *CVE* yang unik. *Database CVE* terdiri dari vulnerabilites umum dan terekspos ke publik sehingga bisa diakses oleh siapa saja (Reis Femi, 2022)

III. METODE

Pada pengujian keamanan dari *website* layanan akademik Universitas XYZ terdapat metode pengujian dalam menemukan, menganalisa, dan menguji celah keamanan yang dimiliki *website*. Metode yang akan digunakan pada pengujian yaitu metode *Vulnerability Assessment and Penetration Testing (VAPT)*. Dasar dari pemilihan metode ini yaitu dapat menyesuaikan dari kebutuhan pengujian sesuai dengan *scope* yang sudah ditentukan dan melakukan *remediation* sebagai upaya evaluasi keamanan dari pengujian sistem *website*.



GAMBAR 1
Sistematika Penyelesaian Masalah

Terdapat beberapa tahapan yang menjelaskan bagaimana *Vulnerability Assessment and Penetration Testing (VAPT)* dilakukan penelitian, yaitu:

A. Tahap Awal

Pada tahap awal penelitian ini dilakukan identifikasi dari masalah. Setelah itu akan dibuatkan latar belakang bersama dengan dilakukannya studi literatur untuk mendapatkan

informasi. Kemudian dibuatkan rumusan masalah, tujuan penelitian, batasan dari penelitian, dan sistematika penulisan.

B. Tahap Pengujian

Pada tahap ini dilakukan perancangan untuk tahapan pengujian. Dimulai dari *scope* pemilihan *tools* yang akan digunakan pada saat melakukan *information gathering* hingga *penetration testing*. Setelah menentukan *tools* selanjutnya akan melakukan pengujian dalam mencari informasi sistem melalui *Information gathering*. Kemudian dilanjutkan dengan mencari celah kerentanan dengan *vulnerability scanning*. Hasil dari *Information gathering* dan *vulnerability Scanning* akan lanjut kepada tahap *Information Analysis and Planning* yang menjelaskan kesimpulan mengenai celah kerentanan kemudian dibuatkan prioritas celah yang akan dilanjutkan ketahap *penetration testing* dan dijelaskan skema pengujian dari *penetration testing*. Selanjutnya mengenai pengujian dari celah kerentanan yang ditemukan. Jika tahap *penetration testing* berhasil maka celah keamanan yang ada di *website* terbukti ada dan akan dilaporkan dalam reporting. Setelah itu akan dilakukan *remediation* untuk melakukan evaluasi dari kerentanan yang ditemukan dengan menutup celah, memperbaiki sistem sesuai dengan prioritas kerentanan.

C. Tahap Akhir

Pada tahap ini akan dilampirkan hasil pengujian dengan menambahkan dokumentasi, kesimpulan dan saran untuk penelitian selanjutnya.

IV. HASIL DAN PEMBAHASAN

A. PERANCANGAN PENGUJIAN

Pada proses pengujian dari *website* layanan akademik Universitas XYZ diperlukan adanya perangkat hardware dan software yang mendukung jalannya proses pengujian. berikut adalah spesifikasi dari Hardware dan Software yang digunakan:

TABEL 1
Spesifikasi Hardware

Nama Perangkat	Spesifikasi	
Lenovo Thinkpad T480	*Processor*	*I5-8350U (4 Core 8 Thread)*
	RAM	*8GB DDR4 2666 Mhz*
	Storage	*256 GB SSD*

TABEL 2
Spesifikasi Software

Nama *Software*	Versi	Fungsionalitas
Windows	11 Pro	*Main OS* pada perangkat *hardware*
VirtualBox	7.0.8	Membuat perangkat virtualisasi
Kali Linux	2023.1	*Main OS* pada perangkat virtual
Nessus	10.5.2 Linux Essentials	*Vulnerability Scan*
OWASP ZAP	2.13.0 Community Edition	*Vulnerability Scan* dan *Penetration Testing*
NMAP	7.94	*Information gathering*
Burp suite	2023.7.3 Community Edition	*Penetration Testing*

B. HASIL *INFORMATION GATHERING* MENGGUNAKAN *NMAP*

NMAP merupakan *tools* bawaan dari *Kali Linux* yang berfungsi untuk melakukan *scanning* terhadap jaringan. Dalam tahap ini informasi yang didapatkan menggunakan *NMAP* berupa informasi umum mengenai *website* layanan akademik Universitas XYZ seperti nama domain, *IP Address*, dan *port default server*.

TABEL 3
Hasil informasi *website* dengan *NMAP*

No	Spesifikasi	Keterangan
1	Nama Domain	toss2-xxxxx.xxx
2	Alamat IP	165.22.61.130
3	*Port* yang digunakan	21,22,25,80,1723,8084

TABEL 4
Port yang digunakan *website*

No	*Port*	Penjelasan
1	21/*TCP*	Merupakan *port* yang digunakan pada service *SSH* yang berfungsi menjadi komunikasi antara komputer *client* dan *server*. Status dari *port* ini yaitu *open*
2	22/*TCP*	Merupakan *port SSH* yang berfungsi menghubungkan *server* dari jarak jauh. Status dari *port* ini yaitu *open*
3	25/*TCP*	Merupakan *port SMTP* yang berfungsi keamanan dari pengiriman *email* antar sesama *SMTP server*. Status dari *port* ini yaitu *filtered*
4	80/*TCP*	Merupakan *port* yang digunakan untuk *HTTP*. Status dari *port* ini yaitu *open*
5	1723/*TCP*	Merupakan *port* yang digunakan untuk *Point-to-Point Tunneling Protocol (PPTP)* dan *PPTP Virtual Private Networking (VPN)* . Status dari *port* ini yaitu *open*
6	8084/*TCP*	Merupakan *port* yang berfungsi untuk pengguna *internal* menggunakan layanan audio atau video dari internet. Status dari *port* ini yaitu *open*

C. HASIL *VULNERABILITY* SCAN MENGGUNAKAN *NESSUS*

Nessus merupakan salah satu *tools* yang digunakan dalam melakukan *vulnerability scanning* untuk menemukan celah kerentanan dari suatu *website* (Bolton James, 2019). Pada tahap ini *Nessus* akan melakukan *scanning* dengan automated *scanning*. Tahapan dari penggunaan *tools* ini yaitu dengan membuat *new scan* dan memasukan domain dari target, dalam pengujian ini menarget domain toss2-xxxxx.xxx dengan pemilihan *vulnerabilities* yaitu *web* aplication test. Setelah itu memilih menu start dan menunggu hasil dari

scanning.Berikut dijelaskan mengenai hasil dari *vulnerability scanning* menggunakan *Nessus* :

TABEL 5
Hasil *scanning* menggunakan *Nessus*

No	*Severity*	CVSS	Judul Kerentanan	Penjelasan
1	*Critical*	9.8	*PHP* 8.0.x < 8.0.25 *Multiple Vulnerabilities*	Terdapat beberapa kerentanan dari penggunaan versi *php* dibawah 8.0.25.
2	*Critical*	9.1	*PHP* 8.0.x < 8.0.27	Terdapat kerentanan dari penggunaan versi *php* dibawah 8.0.27.
No	*Severity*	CVSS	Judul Kerentanan	Penjelasan
3	*High*	7.5	*PHP* 8.0.x < 8.0.28	Terdapat kerentanan dari penggunaan versi *php* dibawah 8.0.28.
4	*High*	7.5	*PHP* 8.0.x < 8.0.30 *Multiple Vulnerabilities*	Terdapat beberapa kerentanan dari penggunaan versi *php* dibawah 8.0.30.
5	*Medium*	6.5	*PHP* 8.0.x < 8.0.24 *Multiple Vulnerabilities*	Terdapat beberapa kerentanan dari penggunaan versi *php* dibawah 8.0.24.
6	*Medium*	4.3	*PHP* 8.0.x < 8.0.29	Terdapat kerentanan dari penggunaan versi *php* dibawah 8.0.29.
7	*Medium*	4.3	*Web* Application Potentially *Vulnerable* to *Clickjacking*	Terdapat kerentanan pada bagian *header website* yang dapat diserang dengan *clickjacking*
8	*Low*	2.6	*Web Server Transmits Cleartext Credentials*	Terdapat kerentanan pada bagian form *HTML* dalam mengirimkan informasi kepada *server* dalam bentuk *cleartext*
9	*Low*	N/A	*Web Server Allows Password Auto-Completion*	Kerentanan pada bagian form *HTML* yang mengizinkan fitur *auto complete* pada bagian *password*

D. HASIL *VULNERABILITY* SCAN MENGGUNAKAN *OWASP ZAP*

OWASP ZAP merupakan *tools* yang terkenal untuk melakukan *scanning*. Pada tahap ini *OWASP ZAP* akan melakukan *scanning* dengan *automated scanning*. Tahapan dari penggunaan *tools* ini yaitu dengan membuat *automated scan* dan memasukan domain dari target, dalam pengujian ini menarget domain toss2-xxxxx.xxx. Selanjutnya memilih menu attack dan menunggu hasil dari *scanning*. Berikut dijelaskan mengenai hasil dari *vulnerability scanning* menggunakan *OWASP ZAP*:

TABEL 6
Hasil *scanning* menggunakan *OWASP ZAP*

No	*Severity*	Judul Kerentanan	Penjelasan
1	*Medium*	*.htaccess Information Leak*	Terdapat kebocoran *file .htaccess* yang bisa diakses oleh publik.
2	*Medium*	*Content Security Policy (CSP) Header Not Set*	Terdapat kerentanan pada bagian *CSP* yang belum dikonfigurasi.
3	*Medium*	*Missing Anti-clickjacking Header*	Terdapat kerentanan pada bagian *header website* yang dapat diserang dengan *clickjacking*.
4	*Medium*	*Vulnerable JS Library*	Terdapat kerentanan dari penggunaan versi lama *JS Library*.
5	*Low*	*Big Redirect Detected (Potential Sensitive Information Leak)*	Terdapat kerentanan dari *server website* mengenai *redirect link*.

6	*Low*	*Cookie No. HttpOnly Flag*	Terdapat kerentanan dari konfigurasi *cookie httponly* yang belum dikonfigurasi
7	*Low*	*Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*	Terdapat kebocoran dari *website* pada bagian *header*
8	*Low*	*HTTP Server Response Header*	Terdapat kebocoran dari *website* pada bagian *header*
9	*Low*	*X-Content-Type-Options Header Missing*	Terdapat kerentanan dari konfigurasi *xcontent* yang belum dikonfigurasi

E. TABEL PERBANDINGAN *TOOLS NESSUS* DAN *OWASP ZAP*

Berdasarkan tahapan yang telah dilakukan pada *vulnerability detection* dengan menggunakan *tools Nessus* dan *OWASP ZAP* ditemukan beberapa perbedaan diantara kedua *tools* yang digunakan dalam menemukan celah kerentanan yang dimiliki oleh *website* layanan akademik Universitas XYZ. Perbandingan secara umum mengenai *tools Nessus* dan *OWASP ZAP* dapat dilihat melalui tabel berikut.

TABEL 7
Perbandingan *tools Nessus* dan *OWASP ZAP*

No	Kategori Perbandingan	*Nessus*	*OWASP ZAP*
1	Kategori	*vulnerability scanning*	*vulnerability scanning*, *penetration testing*
2	Support *API*	Tidak	Ya
3	Jumlah kerentanan yang ditemukan	6	14
4	Informasi *CVE* kerentanan	Mayoritas terdapat penjelasan *CVE*	Hanya sebagian kerentanan yang dijelaskan
5	Durasi *scanning*	2 jam	20 menit

F. HASIL *VULNERABILITY MINING*

Dari tahap *vulnerability detection* dengan menggunakan beberapa *tools* terdapat beberapa celah kerentanan yang ditemukan pada *website* layanan akademik Universitas XYZ. Beberapa dari celah kerentanan memiliki *CVE* atau Common *vulnerabilities* And Exposures yang merupakan *database* yang berukuran besar yang memiliki informasi mengenai berbagai macam *vulnerabilities* atau celah keamanan yang biasa digunakan oleh ahli sekuritas dalam melakukan evaluasi keamanan sistem mereka (Reis Femi, 2022). Berikut dijelaskan mengenai celah kerentanan yang ditemukan dengan *tools Nessus* dan *OWASP ZAP*:

TABEL 8
Cve vulnerability mining

No	*Severity*	*CVE*	Penjelasan
1	*Critical*	*CVE*-2022-37454	Terdapat celah dari penerepan Keccak XKCP SHA-3 sebelum fdc6fef yang dapat menyebabkan *buffer overflow*
2	*Critical*	*CVE*-2022-31630	Terdapat celah dari versi *PHP* 8.0.25 ketika menggunakan *imageloadfont()* di *gd extension*
3	*Critical*	*CVE*-2022-31631	Terdapat beberapa celah yang muncul dari penggunaan *PHP* 8.0.27 yang terkena dampak pada *website* yang menggunakan *PHP* 8.0.25
4	*High*	*CVE*-2023-0662	Terdapat celah pada bagian *form HTTP* yang dapat menyebabkan penggunaan sumber daya *server* yang besar
No	*Severity*	*CVE*	Penjelasan
5	*High*	*CVE*-2023-3823	Terdapat beberapa celah yang muncul dari penggunaan *PHP* 8.0.30 yang terkena dampak pada *website* yang menggunakan *PHP* 8.0.25
6	*High*	*CVE*-2023-3824	Terdapat celah ketika *loading file phar* yang bisa menyebabkan *buffer overflow*
7	*Medium*	*CVE*-2022-31628	Terdapat celah ketika *uncompressor code* pada *phar* yang menyebabkan perulangan tidak terbatas
8	*Medium*	*CVE*-2022-31629	Terdapat celah keamanan yang muncul ketika situs berada pada 1 jaringan antara *attacker* dan *victim* yang menyerang bagian cookie
9	*Medium*	*CVE*-2023-3247	Terdapat celah keamanan pada bagian *SOAP HTTP Digest*
10	*Medium*	*CVE*-2021-41184	Terdapat celah keamanan dari *jquery-UI*
11	*Medium*	*CVE*-2020-11023	Terdapat celah keamanan dari versi yang tidak ter*update*

G. PRIORITAS *VULNERABILITY* DALAM HAL MITIGASI

Setelah dilakukan pengujian dengan *vulnerability detection* dengan *tools Nessus* dan *OWASP ZAP* didapatkan beberapa celah kerentanan dengan kategori risiko yang berbeda. Prioritas utama yang akan dilakukan untuk pengujian *penetration testing* dan mitigasi sistem yaitu celah kerentanan yang memiliki kategori risiko *Critical*, *High*, dan *Medium*. Berikut beberapa kategori risiko yang akan dilakukan pengujian selanjutnya

TABEL 9
Priorias perbaikan celah kerentanan

No	Kategori Risiko	*VULNERABILITY*
1	*Critical*	*PHP 8.0.x < 8.0.25 Multiple Vulnerabilities*
2	*Critical*	*PHP 8.0.x < 8.0.27*
3	*High*	*PHP 8.0.x < 8.0.28*
4	*High*	*PHP 8.0.x < 8.0.30 Multiple Vulnerabilities*
5	*Medium*	*PHP 8.0.x < 8.0.24 Multiple Vulnerabilities*
6	*Medium*	*PHP 8.0.x < 8.0.29*
7	*Medium*	*.htaccess Information Leak*
8	*Medium*	*Content Security Policy (CSP) Header Not Set*
9	*Medium*	*Missing Anti-clickjacking Header*
10	*Medium*	*Vulnerable JS Library*

H. ANALISIS CELAH KERENTANAN

Pada proses pengujian eksploitasi terhadap *website* layanan akademik Universitas XYZ, indikator proses eksploitasi berhasil yaitu menampilkan proses request dan server menjalankan proses tersebut. Berikut penjelasan dari kerentanan – kerentanan yang dilakukan analisis penyebab dan eksploitasi berdasarkan prioritas kerentanan:

1. *PHP Version* 8.0.x

Kerentanan ini ditemukan pada *website* dikarenakan penggunaan versi *PHP* pada server tidak menggunakan versi terbaru. Sehingga dapat memunculkan peluang dari serangan yaitu *buffer overflow*. *Buffer overflow* merupakan serangan yang dilakukan dengan menyerang bagian buffer sistem yang berfungsi sebagai tempat sementara dari penyimpanan data. Ketika buffer ini mengalami kelebihan data yang harus ditampung sehingga menimbulkan crash kepada sistem (Gordon & Garrie, 2020).

2. *htaccess Information Leak*

Kerentanan ini ditemukan pada *website* ketika menggunakan *OWASP ZAP* dan dari *tools* ini bisa memunculkan *file .htaccess*. Dari *file .htaccess* ini terhadap konfigurasi autentikasi, *request file*, dan *controller* yang dimiliki oleh *website*

GAMBAR 2
File .htaccess

3. *Content Security Policy (CSP) Header Not Set*

Kerentanan dari *website* ini disebabkan karena *website* tidak mengkonfigurasi Content Secuity Policy (CSP) yang berfungsi untuk mendeteksi dan mitigasi dari serangan tertentu. Akibat tidak melakukan konfigurasi CSP yaitu *website* rentan terhadap serangan *XSS, data injection*, dan *clickjacking*

4. *Missing Anti-clickjacking Header*

Clickjacking merupakan serangan *website* yang menyebabkan korban secara tidak sengaja mengklik elemen dari halaman *website* yang sebetulnya tidak ingin diklik. Celah kerenantan ini ditemukan pada *website* target. Pengujian dari *clickjacking* ini menggunakan *tools Burp suite Community Edition.*

GAMBAR 3
Pengujian Clickjacking

5. *Vulnerable JS Library*

JQuery merupakan kumpulan kode dari *javascript* yang berfungsi untuk menyederhanakan kode *javascript* dengan cara memanggil fungsi yang disediakan oleh *jquery*. Kerentanan yang ditemukan dari *website* dengan menggunakan *tools OWASP ZAP* yaitu versi yang digunakan merupakan versi lama dan tidak ter*update* sehingga terdapat celah kerentanan. Terdapat 2 jquery yang belum menggunakan versi terbaru dari *website*, yaitu *jquery* dan *jquery UI*

GAMBAR 4
jQuery UI

GAMBAR 5
jQuery

I. PERANCANGAN MITIGASI

Hasil dari analisis celah kerentanan yang sudah diujikan dalam *penetration testing* selanjutnya akan dilakukan perancangan dalam mitigasi sistem dari *website* layanan akademik Universitas XYZ. Beberapa rekomendasi diberikan dalam upaya perbaikan dari keamanan *website* sesuai dengan kerentanan yang sudah diujikan.

TABEL 10
Perancagan Mitigasi

No	*Vulnerability*	Rekomendasi
1	*PHP Version 8.0.x*	Melakukan *upgrade* ke versi terbaru *PHP*

2	*.htaccess Information Leak*	Melakukan konfigurasi dari *file .htaccess*
3	*Content Security Policy (CSP) Header Not Set*	Melakukan konfigurasi pada *file config.php*
4	*Missing Anti-clickjacking Header*	Melakukan konfigurasi pada bagian *header website*
5	*Vulnerable JS Library*	Melakukan *update* dari *file jquery* dan *jquery* UI ke versi terbaru

Berdasarkan Tabel 10 terdapat rekomendasi yang diberikan dalam upaya perbaikan sistem dan akan dilakukan mitigasi kepada sistem *website* layanan akademik Universitas XYZ. Setelah dilakukan mitigasi akan dilakukan pengujian ulang yang berfungsi untuk membandingkan hasil pengujian sebelum dan sesudah dilakukannya mitigasi kepada sistem *website*.

J. PENGUJIAN ULANG PASCA MITIGASI

Berdasarkan perancangan mitigasi terdapat rekomendasi untuk mitigasi sistem dan sudah dilakukan mitigasi sistem. Pada tahapan ini akan diujikan kembali apakah celah kerentanan yang sebelumnya diperbaiki sudah tidak ada lagi pada sistem *website* layanan akademik Universitas XYZ. Pengujian pada tahap ini akan menggunakan *tools Nessus* dan *OWASP ZAP* dalam mencari kembali celah kerentanan dari *website*

TABEL 11
Analisis *vulnerability detection* pasca mitigasi

No	*Vulnerability Scanning* Sebelum Mitigasi	*Vulnerability Scanning* Setelah Mitigasi	Keterangan
1	*PHP* Version 8.0.x	*PHP* Version 8.0.x	Perlu dilakukan *update* dari *PHP* oleh pengembang *website* pada *server*
2	*.htaccess Information Leak*	*.htaccess Information Leak*	Perlu dilakukan konfigurasi *file .htaccess* oleh pengembang *website*
3	Content *Security* Policy (*CSP*) *Header Not Set*	Content *Security* Policy (*CSP*) *Header Not Set*	Perlu dilakukan konfigurasi *file config.php* oleh pengembang *website*
4	Missing Anti-*clickjacking Header*	Missing Anti-*clickjacking Header*	Perlu dilakukan konfigurasi *file header* oleh pengembang *website*
5	*Vulnerable* JS Library	*Vulnerable* JS Library	Perlu dilakukan *update* dari *jquery* dan *jquery* UI oleh pengembang *website* pada *server*

Berdasarkan tabel 11 dijelaskan mengenai kerentanan yang ditemukan kembali pada *website* layanan akademik Universitas XYZ. Celah kerentanan yang ditemukan kembali ini memerlukan upaya perbaikan dari pihak pengembang *website* dikarenakan keterbatasan akses dari pengujian sehingga celah kerentanan ini dapat ditemukan kembali. Pada tahap mitigasi sistem ini akan dijadikan rekomendasi bagi pengembang website dalam upaya melakukan mitigasi sistem untuk memberikan evaluasi terhadap penilaian keamanan sistem.

V. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan dengan metode *Vulnerability Assessment and Penetration Testing (VAPT)* yang meliputi pengumpulan informasi, analisis kerentanan, eksploitasi, dan mitigasi terhadap *website* layanan akademik Universitas XYZ menggunakan *tools Nessus*, *Burp suite*, dan *OWASP ZAP*, dapat disimpulkan bahwa dari hasil *vulnerability detection* menggunakan *tools Nessus* dan *OWASP ZAP* terhadap *website* target, yaitu *WEBSITE* layanan akademik Universitas XYZ ditemukan beberapa kerentanan dengan kategori risiko masing - masing. Dari *tools Nessus* terdapat 6 kerentanan dengan kategori risiko yaitu 2 *critical*, 2 *high*, dan 2 *medium*. Dari keseluruhan kerentanan semuanya disebabkan oleh penggunaan versi *PHP* yang tidak terbaru. Dari *tools OWASP ZAP* terdapat 14 kerentanan dengan kategori risiko yaitu 4 *medium*, 4 *low*, dan 5 *informational*. Terdapat pengujian dari beberapa celah keamanan yang dieksploitasi seperti *file .htaccess* dan *clickjacking*. Dari kerentanan yang ditemukan dilakukan proses *remediation* dengan melakukan *update* dari versi terbaru hingga konfigurasi ulang dari *file website*. Kerentanan yang tidak berhasil diperbaiki akan menjadi rekomendasi mitigasi perbaikan sistem. Dari penelitian ini ditemukan beberapa celah kerentanan yang dimiliki oleh *website* layanan akademik Universitas XYZ melalui proses *vulnerability detection* hingga *remediation*. Dari hasil penemuan ini bisa dijadikan masukan bagi pengembang *website* untuk evaluasi dari sekuritas *website*. Untuk penelitian kedepannya dapat mengembangkan penelitian dengan berdasarkan rancangan yang sudah dilakukan.

REFERENSI

Andress. (2014). J. The Basics of *Information* Security: Understanding the Fundamentals of InfoSec in Theory and Practice.

Bolton James. (2019). CEH v10 Certified Ethical Hacker Practice Exams & Dumps. https://www.google.co.id/books/edition/CEH_v10_Certified

_Ethical_Hacker_Practic/B0zHDwAAQBAJ?hl=en&gbpv=1&dq=*nessus*+definition&pg=PA44&printsec=frontcover

Cross, M. (2007). *WEB* application *VULNERABILITIES* : detect, exploit, prevent.

Zakir Anas. (2022). Cybersecurity & Digital Forensics. https://www.google.co.id/books/edition/Cybersecurity_Digital_Forensics/G8tkEAAAQBAJ?hl=en&gbpv=1&dq=owasp+zap&pg=PA431&printsec=frontcover

DEWI, M. (2022). *VULNERABILITY ASSESSMENT* PADA *WEBSITE* REKRUITASI ASISTEN (IRIS) FAKULTAS REKAYASA INDUSTRI MENGGUNAKAN NIKTO DAN *NESSUS*. https://openlibrary.telkomuniversity.ac.id/home/catalog/id/181209/slug/*VULNERABILITY-ASSESSMENT*-pada-*WEBSITE*-rekruitasi-asisten-iris-fakultas-rekayasa-industri-menggunakan-nikto-dan-*nessus*.html

Goel, J. N., & Mehtre, B. M. (2015). *VULNERABILITY ASSESSMENT & PENETRATION TESTING* as a Cyber Defence Technology. Procedia Computer Science, 57, 710–715. https://doi.org/10.1016/j.procs.2015.07.458

Gordon, L. M., & Garrie, D. B. (2020). Cybersecurity & the courthouse : safeguarding the judicial process. 140.

Id-SIRTII. (2022). LAPORAN BULANAN PUBLIK Hasil Monitoring Keamanan Siber 2022. www.idsirtii.or.id

INDERA, R. (2022). *VULNERABILITY ASSESSMENT* PADA SITUS *WEB* KERJA PRAKTEK DAN PENGABDIAN MASYARAKAT FAKULTAS REKAYASA INDUSTRI DENGAN *BURP SUITE* DAN INTRUDER. https://openlibrary.telkomuniversity.ac.id/home/catalog/id/181206/slug/*VULNERABILITY-ASSESSMENT*-pada-situs-*WEB*-kerja-praktek-dan-pengabdian-masyarakat-fakultas-rekayasa-industri-dengan-burp-suite-dan-intruder.html

Lamba, A. (2020). Cyber Attack Prevention using *VAPT Tools* (*VULNERABILITY ASSESSMENT & PENETRATION TESTING*). https://ssrn.com/abstract=3516069

Listartha, E., Arna, G., Saskara, J., Gede, D., & Santyadiputra, S. (2021). PENGUJIAN KERENTANAN DAN PENETRASI KEAMANAN PADA APLIKASI *WEB* MANAJEMEN SKRIPSI PRODI XYZ. ScientiCO : Computer Science and Informatics Journal, 4(2).

Lozano, C. A., Shah, Dhruv., & Ahemed Walikar, Riyaz. (2019). Hands-On Application *PENETRATION TESTING* with *Burp suite* : Use *Burp suite* and Its Features to Inspect, Detect, and Exploit Security *VULNERABILITIES* in Your *WEB* Applications. 356.

Michael E. Whitman, H. J. M. (2013). Management of *Information* Security - Michael E. Whitman, Herbert J. Mattord. https://books.google.co.id/books?hl=en&lr=&id=naB0AgAAQBAJ&oi=fnd&pg=PP1&dq=Whitman,+M.+E.,+%26+Mattord,+H.+J.,+2013&ots=yB7CXmU_fR&sig=kQIgwBthqehOODbHHDwzu1CS7EU&redir_esc=y#v=onepage&q&f=false

Wahana Komputer. (2010). Membangun *WEBSITE* Tanpa Modal. https://www.google.co.id/books/edition/Membangun_*WEBSITE*_Tanpa_Modal/fhUF7oSUI1gC?hl=en&gbpv=1&dq=sejarah+*WEBSITE*&pg=PA1&printsec=frontcover

PUTRA, S. A. (2022). *VULNERABILITY* ASSESMENT *WEB* PROPOSAL TUGAS AKHIR MAHASISWA FRI MENGGUNAKAN ACUNETIX DAN *NMAP*. https://openlibrary.telkomuniversity.ac.id/home/catalog/id/180214/slug/*VULNERABILITY*-assesment-*WEB*-proposal-tugas-akhir-mahasiswa-fri-menggunakan-acunetix-dan-*nmap*.html

Sahtyawan, R. (2019). PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY MISCONFIGURATION PADA *VAPT* (*VULNERABILITY ASSESSMENT* AND *PENETRATION TESTING*) (Vol. 1, Issue 1).

Reis Femi. (2022). Something About Everything—CompTIA Security+ SY0-601 Certification Exams. https://www.google.co.id/books/edition/Something_About_Everything_CompTIA_Secur/FXnGEAAAQBAJ?hl=en&gbpv=0

Umrao, S., Kaur, M., Govind, &, & Gupta, K. (2012). *VULNERABILITY ASSESSMENT* AND *PENETRATION TESTING*. In International Journal of Computer & Communication Technology ISSN (PRINT (Issue 3).

Wibowo, S. H., Irawan, J. D., S, W., Winardi, B., Santoso, L. W., Sari, D. P., Dewantara, R., Jamaludin, Nurhadi, Sihombing, F. A., Aulia, A. P., Heryana, N., & Kurnaedi, D. (2023). Cyber Crime di Era Digital. 223. https://www.google.co.id/books/edition/Cyber_Crime_di_Era_Digital/xOqmEAAAQBAJ?hl=id&gbpv=0