Evaluasi Risiko Celah Keamanan Pada Aplikasi Web Dengan Penilaian Kerentanan dan Pengujian Penetrasi Menggunakan Metode OWASP dan NIST SP 800-30 Revisi 1

Satria Dzaky Raihan
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
satriadzaky@student.telkomuniversity.ac.id

Sidik Prabowo, S.T., M.T.
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
pakwowo@telkomuniversity.ac.id

Dita Oktaria, S.Kom, M.T.
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
dioktaria@telkomuniversity.ac.id

***Abstrak* — Semenjak terjadinya pandemi, penggunaan teknologi informasi meningkat secara signifikan terutama pada penggunaan aplikasi berbasis web. Dalam penggunaan teknologi tersebut, tentunya tidak akan lepas dari berbagai macam risiko yang mengancam aset-aset berharga serta dapat menimbulkan kerugian. Untuk menghindari hal tersebut diperlukan tindakan evaluasi terhadap keamanan tidak terkecuali aplikasi web milik Institut XYZ. Terdapat berbagai macam cara yang dapat digunakan untuk melakukan evaluasi, salah satunya adalah dengan melakukan *vulnerability assessment & penetration testing* (VAPT). Dalam metode ini peneliti melakukan simulasi penyerangan sebagai peretas untuk mengidentifikasi dan menganalisis celah keamanan yang ada pada aplikasi web Institut XYZ. Pengujian yang dilakukan menggunakan panduan OWASP *Web Security Testing Guide version 4.2* yang dibuat khusus untuk pengujian aplikasi web. Setelah kerentanan berhasil diidentifikasi, kemudian dilanjutkan dengan analisis risiko menggunakan NIST SP 800-30 Rev 1. Hasil akhir dari tugas akhir ini adalah laporan mengenai risiko yang berhasil dievaluasi serta rekomendasi langkah mitigasi dari risiko-risiko tersebut. Diharapkan hasilnya dapat membantu untuk mengamankan aplikasi web milik Institut XYZ.**

***Kata kunci* — kerentanan, risiko, web, VAPT, OWASP, NIST**

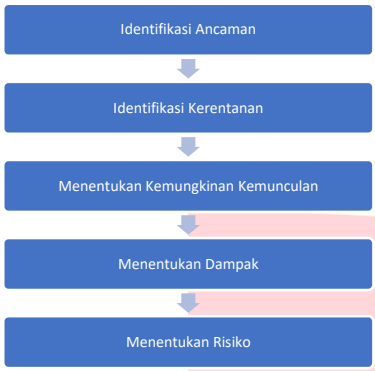
I. PENDAHULUAN

Semenjak terjadinya pandemi, mayoritas fungsi yang berjalan di masyarakat dipakasa untuk mengadopsi teknologi informasi sehingga penggunaannya meningkat secara signifikan terutama pada penggunaan aplikasi berbasis *web* dan *mobile* [1]. Dalam penggunaan teknologi tersebut, tentunya tidak akan lepas dari berbagai macam risiko yang mengancam aset-aset berharga, dimulai dari data pribadi hingga infrastruktur yang menjalankan teknologi itu sendiri. Di Indonesia sendiri pada tahun 2022 BSSN mencatat terjadi sebanyak 2.348 kasus *Web Defacement* dengan sektor yang paling terdampak adalah administrasi pemerintah dengan jumlah kasus sebanyak 885 kasus [2]. Beberapa penelitian terdahulu telah melakukan pencarian dan penanganan terhadap potensi risiko keamanan aplikasi berbasis website [3], [4], [5], [6]. Metodologi yang digunakan diantaranya adalah OWASP, dengan temuan menunjukkan bahwa OWASP efektif dalam pengujian keamanan berbasis web. Meskipun demikian, hasil temuan belum mencukupi untuk mengimplementasikan langkah-langkah keamanan yang memadai, sehingga analisis lebih lanjut diperlukan untuk mendapatkan nilai risiko yang akurat. Organisasi umumnya menggunakan metode evaluasi risiko seperti NIST SP 800-30, ISO 27005, dan ISO 31000. Berdasarkan penelitian sebelumnya, NIST SP 800-30 memiliki kelebihan memungkinkan seseorang untuk memprediksi risiko di masa depan [7]. Integrasi OWASP sebagai metodologi pendukung dapat mengatasi potensi kekurangan dalam metode NIST, menyediakan pendekatan holistik untuk memastikan keamanan aplikasi web dan memperkuat ketahanan terhadap risiko keamanan. Dalam implementasi framework tersebut, penambahan penggunaan *Common Vulnerability Scoring System* (CVSS) dapat meningkatkan akurasi perhitungan dampak kerentanan, sehingga nilai risiko yang dihasilkan menjadi lebih akurat. Institut XYZ adalah perguruan tinggi yang telah menggunakan teknologi informasi untuk mempermudah dalam pelaksanaan kegiatan operasional, yang mana sebagian besar menggunakan aplikasi website. Salah satu aplikasi yang banyak digunakan civitas akademika XYZ adalah aplikasi perpustakaan digital. Sayangnya kondisi sumber daya yang dimiliki Institut XYZ belum mencukupi untuk melakukan evaluasi risiko kemanan secara mandiri. Sehubungan dengan hal tersebut, peneliti melakukan evaluasi risiko terhadap celah kemanan pada aplikasi berbasis web pada institut XYZ. Dengan hasil dari penelitian ini diharapkan dapat membantu institusi XYZ meminimalisir risiko dengan memberikan rekomendasi langkah mitigasi risiko keamanan yang ada pada website Institut XYZ.

II. KAJIAN TEORI

A. NIST SP 800-30 Rev. 1

NIST SP 800-30 Rev. 1 adalah sebuah dokumen yang digunakan sebagai panduan untuk melakukan *risk assessment*.



Gambar 1. Tahapan NIST SP 800-30 Rev 1 [8]

Berikut adalah penjelasan setiap tahapan dari gambar 1:

1. Identifikasi Ancaman

   Yang pertama dilakukan adalah mengidentifikasi sumber ancaman. Sumber ancaman yang perlu diidentifikasi terdiri dari dua hal yakni *threat source* dan *threat event.*

2. Identifikasi Kerentanan

   Tahap ini melakukan identifikasi terhadap kerentanan yang ada pada aplikasi web XYZ. Dalam kegiatan identifikasi, VAPT dan OWASP WSTG digunakan sebagai framework acuan.

3. Menentukan *Likelihood*

   Pada tahap ini, ditentukan tingkatan pengaruh buruk yang kemungkinan akan terjadi terhadap lembaga XYZ dari ancaman-ancaman yang berhasil diidentifikasi.

4. Menentukan Dampak

   Pada tahap ini, ditentukan tingkat kemunculan terjadinya ancaman. Perhitungan berdasarkan karakteristik dari ancaman dan kerentanan yang berhasil diidentifikasi.

5. Menentukan Risiko

   Pada tahap ini, dilakukan penentuan nilai risiko pada lembaga XYZ terkait dengan ancaman yang sudah diidentifikasi. Penilaian yang didapat kemudian ditentukan berdasarkan kemunculan dan dampak dari suatu ancaman. Persamaan (1) digunakan untuk menentukan nilai risiko dari suatu ancaman.

$$Risk = likelihood \times impact \quad (1)$$

B. OWASP Web Security Testing Guide

OWASP *Web Security Testing Guide* (WSTG) adalah suatu metode yang digunakan untuk mengevaluasi keamanan sistem komputer atau jaringan. Metode ini difokuskan pada validasi dan verifikasi efektivitas kontrol keamanan pada tingkat aplikasi [9]. OWASP WSTG hanya berfokus pada evaluasi keamanan aplikasi web. Proses ini melibatkan analisis aktif dari aplikasi untuk setiap kelemahan teknis atau kerentanan. Secara garis besar pengujian pada OWASP WSTG dibagi kedalam beberapa bagaian sebagai berikut:

1. *Information Gathering*
2. *Configuration and Deployment Management Testing*
3. *Identity Management Testing*
4. *Authentication Testing*
5. *Authorization Testing*
6. *Session Management Testing*
7. *Input Validation Testing*
8. *Testing for Error Handling*
9. *Testing for Weak Cryptography*
10. *Business Logic Testing*
11. *Client-side Testing*
12. *API Testing*

C. Vulnerability Assessment & Penetration Testing

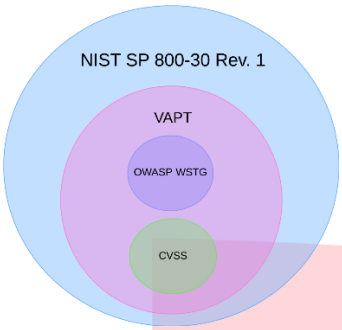
Vulnerability Assessment & Penetration Testing (VAPT) adalah suatu metodologi dalam melakukan uji keamanan terhadap suatu sistem. VAPT merupakan gabungan dari dua aktivitas yakni, *Vulnerability Assessment* dan *Penetration Testing* [10]. *Vulnerability Assessment* dan *Penetration Testing* adalah dua hal yang berbeda namun proses yang saling berkaitan dalam artian bahwa, *Vulnerability Assessment* dirancang untuk mengidentifikasi kerentanan dalam suatu sistem, dalam hal ini *stakeholder* sudah mengetahui bahwa mereka memiliki sebuah masalah pada sistem mereka dan karenanya hanya membutuhkan bantuan untuk mengidentifikasi dan memprioritaskannya. Sementara itu *Penetration Testing* dirancang untuk mencapai tujuan spesifik, yakni melakukan simulasi langkah-langkah yang kemungkinan diambil oleh penyerang.

D. Common Vulnerability Scoring System

Common Vulnerability Scoring System (CVSS) adalah kerangka kerja terbuka untuk mengkomunikasikan karakteristik dan tingkat keparahan suatu kerentanan pada perangkat lunak [11]. CVSS terdiri dari tiga kelompok metrik: Basis, Temporal, dan Lingkungan. Untuk melakukan perhitungan metrik basis perlu ditentukan terlebih dahulu nilai dari setiap komponen yang ada pada metrik basis. Komponen dari metrik basis terdiri dari: *attack vector*, *attack complexity*, *privilege required*, *user interaction*, *scope*, *confidentiality*, *integrity*, dan *availability*. Ketika semuanya sudah diidentifikasi, barulah tingkat keparahan dari suatu kerentanan dapat dihutung.

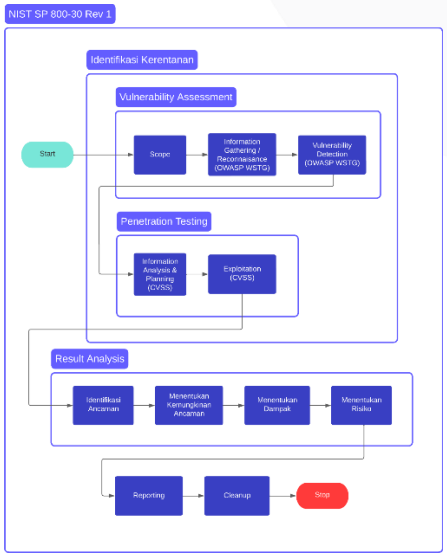
III. METODE

Penelitian ini bertujuan untuk melakukan evaluasi risiko dari kerentanan yang ada pada aplikasi web. Oleh karena itu metodologi yang digunakan dalam penelitian ini merupakan gabungan antara metode NIST SP 800-30 Rev 1, VAPT, OWASP WSTG, dan CVSS.

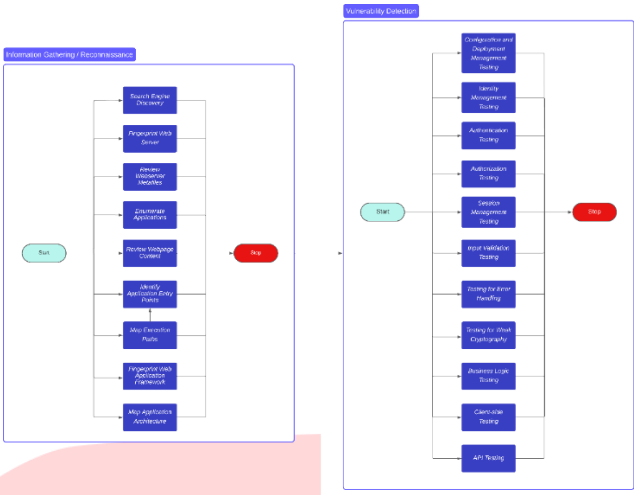


Gambar 2. Hubungan Metodologi

Sebagaimana terlihat dalam gambar 2, NIST SP 800-30 Rev. 1 dipilih sebagai fondasi metodologi yang diterapkan dalam penelitian ini. Pemilihan ini sejalan dengan tujuan penelitian, yaitu mengevaluasi risiko, di mana NIST SP 800-30 Rev. 1 diakui dapat memenuhi persyaratan tersebut. Salah satu tahap kunci dalam metodologi ini adalah identifikasi kerentanan, di mana peneliti perlu mengumpulkan data terkait kerentanan yang mungkin muncul pada sistem yang diteliti. Kebutuhan ini terpenuhi melalui implementasi VAPT pada sistem. Mengingat sistem yang diuji merupakan sebuah aplikasi berbasis website, VAPT difokuskan pada pengujian keamanan web dengan merujuk pada panduan OWASP WSTG. Hasil pengujian dari panduan OWASP WSTG selanjutnya dianalisis menggunakan CVSS guna mendapatkan nilai tingkat keparahan dari kerentanan yang berhasil diidentifikasi. Nilai tersebut kemudian dianalisis lebih lanjut pada tahapan-tahapan berikutnya dalam metodologi NIST SP 800-30 Rev. 1, yang pada akhirnya akan menghasilkan identifikasi risiko yang komprehensif. Berikut adalah tahapan dari metedologi yang dilakasanakan dalam penelitian.



Gambar 3. Tahapan Metodologi



Gambar 4. Tahapan Metodologi OWASP WSTG

Pada gambar 3, terlihat bahwa identifikasi kerentanan merupakan tahap awal dari metodologi yang digunakan. Dalam metodologi NIST SP 800-30 Rev. 1, langkah ini biasanya dilakukan setelah identifikasi ancaman. Namun, dalam penelitian ini, fokus utama adalah pada penilaian risiko berdasarkan kerentanan, sehingga urutan tahapan ini diubah. Selain itu, metode VAPT digunakan untuk menjalankan tahap Identifikasi kerentanan dengan tujuan mendapatkan hasil yang akurat. Panduan OWASP WSTG digunakan sebagai acuan dalam tahap ini yang detailnya bisa dilihat pada gambar 4. Panduan tersebut secara khusus membahas keamanan aplikasi web yang sesuai dengan cakupan penelitian ini. Detail dari setiap tahapan dijelaskan lebih lanjut pada sub bab berikut.

A. Scope

Pada tahap pertama ini ditentukan ruang lingkup pengujian. Penentuan ruang lingkup perlu disetujui oleh peneliti serta pemilik sistem. maka dari itu pada tahap ini diadakan focus group discussion antara peneliti dan Institut XYZ.

B. Information Gathering / Reconnaissance

Pada tahap ini peneliti mengumpulkan informasi mengenai target dari berbagai macam sumber. Sesuai dengan metodologi OWASP WSTG tahap ini termasuk kedalam bagian paling pertama yakni *Information Gathering* [9]. Maka dari itu pada tahap ini terbagi kedalam sembilan kegiatan yakni:

1. *Conduct Search Engine Discovery Reconnaissance for Information Leakage*
2. *Fingerprint Web Server*
3. *Review Webserver Metafiles for Information Leakage*
4. *Enumerate Applications on Webserver*
5. *Review Webpage Content for Information Leakage*
6. *Identify Application Entry Points*
7. *Map Execution Paths Through Application*
8. *Fingerprint Web Application Framework*
9. *Map Application Architecture*

Tools yang digunakan pada tahap ini sangat beragam seperti *search engine* (*Google, DuckDuckGo*, dll), *server fingerprinting tools* (*Nikto, Nmap*, dll), *DNS lookup tools* (*nslookup, dig*, dll), *data transfer tools* (*Wget, cURL*, dll), *framework-based fingerprinting tools* (*WhatWeb, Wappalyzer*), dan *browser developer tools*.

C. Vulnerability Detection

Pada tahap ini, peneliti melakukan proses pencarian celah dimana dalam pelaksanaannya dilakukan dengan cara *automatic* dan *manual testing* secara bersamaan. Untuk *automatic testing, software* yang digunakan yaitu *OWASP ZAP*, *Burpsuite*, dan *Nessus*. Untuk *manual testing*, peneliti langsung berinteraksi dengan target seolah-olah peneliti adalah seorang pengguna. Kemudian hasil dari kedua test tersebut dicek ulang secara manual oleh peneliti. Dari hasil pencarian tersebut akan didapatkan daftar celah yang kemudian digunakan untuk tahap selanjutnya. Pengujian tahap ini disesuaikan dengan metodologi OWASP WSTG [9].

D. Information Analysis & Planning

Pada tahap ini, peneliti melakukan analisis terhadap celah yang ditemukan pada tahap sebelumnya. Hasil dari tahap ini menentukan skenario dalam melakukan tahap selanjutnya yakni exploitation. Jika setelah dilakukan analisis ternyata didapat hasil dimana keamanan target sangat baik ataupun celah yang ditemukan tidak berdampak fatal, maka tahap exploitation akan dilewati dan dilanjutkan dengan result analysis. Analisis serta pembuatan skenario dibuat berdasarkan nilai CVSS dan data yang diperoleh dari hasil *Vulnerability Assessment*.

E. Exploitation

Pada tahap ini, peneliti melakukan simulasi eksploitasi terhadap sistem menggunakan celah yang sudah dianalisis sebelumnya. Eksploitasi yang dimaksud adalah percobaan untuk mengubah data/informasi yang tersedia, meningkatkan hak akses yang dimiliki, atau memasuki sistem melalui celah yang ada. Eksploitasi hanya dibatasi hingga mendapatkan bukti penyerangan berhasil dilakukan. Jika eksploitasi mencapai tahap yang dapat merusak sistem, maka eksploitasi tersebut akan dihentikan.

F. Result Analysis

Pada tahap ini, peneliti melakukan analisis risiko terhadap informasi-informasi yang telah didapat dalam serangkaian pengujian yang telah dilakukan pada tahap-tahap sebelumnya. Analisis risiko dilakukan dengan menggunakan metodologi NIST SP 800-30 Rev 1 yang dipadu dengan hasil CVSS sebelumnya. Setelah dilakukan analisis kemudian dibuatkan rekomendasi langkah mitigasi dari setiap risiko yang didapat. Rekomendasi yang dipilih bergantung pada kondisi setiap kerentanan yang dianalisis. Oleh karena itu rujukan yang dipilih untuk rekomendasi langkah mitigasi akan sangat beragam. Rujukan tersebut dapat berasal dari *vendor*, *framework*, ataupun sumber tidak resmi (blog, forum, dll.).

G. Reporting

Hasil yang didapat setelah dilakukannya pengujian serta analaisis pada tahap-tahap sebelumnya dituangkan ke dalam dokumen tugas akhir ini. Dokumen tersebut juga telah diserahkan kepada pemilik sistem sebagai masukan untuk tindakan mitigasi.

H. Cleanup

Pada tahap terakhir, peneliti melakukan pembersihan terhadap target pengujian. Pembersihan yang dimaksud adalah mengembalikan kondisi sistem kembali seperti semula. Aktivitas pembersihan yang dilakukan tergantung pada sejauh mana peneliti mengeksploitasi celah yang telah ditemukan. Selain itu peneliti juga menghapus semua data – data informasi penting yang peneliti dapatkan selama proses pengujian. Hal ini dilakukan untuk menjaga kerahasiaan dari sistem yang diuji.

IV. HASIL DAN PEMBAHASAN

A. Scope

Dalam penelitian ini, penentuan *scope* penelitian dan pemilihan aplikasi web dilakukan melalui *focus group discussion* (FGD) dengan rektor & wakil rektor Institut XYZ. Dalam FGD tersebut, beberapa kesimpulan penting berhasil diambil. Pertama, Institut XYZ memberikan izin sepenuhnya kepada peneliti untuk melaksanakan penelitian ini. Kedua, Institut XYZ menyerahkan penentuan aplikasi web yang menjadi fokus penelitian kepada peneliti. Ketiga, selama dilakukannya pengujian, penting untuk memastikan bahwa keberlangsungan aplikasi web tidak terganggu. Keempat, waktu yang ditetapkan untuk pengujian adalah selama enam bulan. Kelima, dengan mempertimbangkan keterbatasan kemampuan peneliti dan waktu yang terbatas, diputuskan bahwa pengujian hanya dilakukan pada satu aplikasi web.

B. Information Gathering / Reconnaissance

Pada tahap *Information Gathering/Reconnaissance*, dilakukan pencarian informasi terkait seluruh host yang terhubung dengan domain *xyz.ac.id*. Dalam penelitian ini, ditemukan total 25 host yang terhubung dengan domain tersebut. Penting untuk mencatat bahwa seluruh host yang ditemukan dihosting oleh *niagahoster*, kecuali satu aplikasi yang dijalankan pada *siakadcloud*. Selanjutnya, ditemukan bahwa versi *wordpress* yang digunakan pada host-host tersebut sangat beragam, mulai dari versi terlama 4.9.23 hingga versi terbaru 6.2.2. Dalam penelitian ini juga ditemukan bahwa untuk semua aplikasi *open source* yang digunakan, penggunaan versi-versi yang lebih lama telah diidentifikasi. Terakhir, terdapat dua host yang dicurigai telah mengalami serangan oleh pihak yang tidak berwenang sebelum dilakukannya pengujian. Hal ini menunjukkan bahwa keberadaan serangan sebelumnya telah mempengaruhi keadaan keamanan pada host-host tersebut.

Berdasarkan data yang diperoleh, host yang dipilih sebagai subjek pengujian adalah *digilib.xyz.ac.id*. Pemilihan host ini didasarkan pada pertimbangan yang matang,

menggabungkan aspek keamanan, risiko, dan ketersediaan sumber daya. Host *digilib.xyz.ac.id* adalah sebuah host yang berfungsi sebagai perpustakaan digital dari Institut XYZ. Host ini menyimpan beberapa *e-book* dan jurnal yang diterbitkan oleh Institut XYZ. Untuk mengelola perpustakaan digital, Institut XYZ menggunakan aplikasi *SENAYAN Library Management System* (SLiMS) versi 7 Cendana. Versi terakhir dari SLiMS versi 7 Cendana diperbarui pada tahun 2017. Pengembangan versi 7 Cendana telah dihentikan oleh pengembang SLiMS, dan mereka beralih ke versi 9 Bulian pada tahun 2020, yang terus dikembangkan hingga saat ini. Dengan adanya informasi ini, penggunaan versi 7 Cendana meningkatkan risiko keamanan. Hal ini dapat berdampak buruk bagi Institut XYZ.

C. Vulnerabilty Detection

Dalam tahap vulnerability detection, peneliti melakukan prosedur pengujian berdasarkan standar OWASP WSTG versi 4.2 untuk mengidentifikasi dan mengevaluasi kerentanan dalam aplikasi SLiMS versi 7 Cendana yang dikelola oleh Institut XYZ. Dari keseluruhan aktivitas pengujian, hanya sekitar setengah aktivitas yang berjalan dengan lancar. Sebagian besar aktivitas yang berhasil dilaksanakan termasuk dalam kategori input validation test, config and deploy test, dan authentication test. Hal ini menunjukkan bahwa beberapa aspek keamanan pada aplikasi ini telah diimplementasikan dengan baik. Dalam proses pengujian, peneliti berhasil menemukan 16 kerentanan dalam aplikasi. Dari jumlah tersebut, 2 kerentanan telah tercatat dalam *Common Vulnerabilities and Exposures* (CVE). Berdasarkan hasil pengujian ini, penting bagi Institut XYZ untuk memperhatikan dan mengatasi kerentanan yang ditemukan

D. Information Analysis & Planning

Setelah berhasil mengidentifikasi kerentanan pada tahap sebelumnya, langkah selanjutnya adalah melakukan analisis informasi. Peneliti menggunakan CVSS sebagai alat untuk mengevaluasi tingkat keparahan dan dampak dari kerentanan yang ditemukan. Cara perhitungannya dilakukan dengan mengidentifikasi karakterisitik yang dimiliki oleh sebuah kerentanan. Dalam proses ini, terdapat 2 kerentanan yang sudah memiliki nilai CVSS karena telah tercatat dalam CVE. Namun, kerentanan lainnya perlu dinilai oleh peneliti. Peneliti melakukan analisis lebih lanjut dengan memperoleh data tambahan yang diperlukan untuk mengukur tingkat keparahan dan dampaknya. Oleh karena itu, kerentanan-kerentanan ini dimasukkan ke tahap selanjutnya, yaitu tahap exploitation, di mana peneliti melakukan uji coba untuk menguji kemungkinan eksploitasi dan melihat efeknya terhadap sistem. Ada pula kerentanan-kerentanan yang tidak memerlukan penelitian lebih lanjut karena data yang telah diperoleh sudah mencukupi untuk menilai CVSS.

E. Exploitation

Pada tahap *exploitation*, peneliti melakukan uji coba untuk memanfaatkan kerentanan yang telah diidentifikasi sebelumnya. Peneliti mencoba menjalankan *exploit* yang tersedia di database *exploit-db.com*, Namun, *exploit-exploit* tersebut tidak berhasil berjalan sepenuhnya dikarenakan berbagai alasan. Peneliti juga melakukan uji coba eksploitasi *Cross-Site Scripting* (XSS) mulai dari yang paling sederhana hingga yang lebih kompleks. Untuk semua kerentanan XSS yang ditemukan, dapat diexploitasi untuk mendapatkan *cookie* dari pengguna. Melalui tahap eksploitasi ini, peneliti dapat menentukan kerentanan mana yang dapat dieksploitasi dan mana yang tidak. Hasil ini memberikan pemahaman yang lebih mendalam tentang tingkat keparahan dan kemungkinan penyalahgunaan kerentanan yang ditemukan pada aplikasi web. Hasil temuan disajikan ke dalam tabel 1.

Tabel 1. Nilai CVSS

Vulnerability ID	Score	Rating
VULN-1	5.3	Medium
VULN-2	5.3	Medium
VULN-6	2.7	Low
VULN-7	5.9	Medium
VULN-8	3.7	Low
VULN-9	3.7	Low
VULN-11	3.1	Low
VULN-12	4.2	Medium
VULN-13	4.2	Medium
VULN-14	5.4	Medium
VULN-15	4.3	Medium
VULN-16	3.7	Low

F. Identifikasi Ancaman

Threat source yang diidentifikasi hanya berfokus pada tipe adversarial. Keputusan tersebut diambil karena jika merujuk data statistik laporan keamanan, mayoritas serangan keamanan berasal dari *threat source* bertipe *adversarial*, terutama dari kelompok *cybercriminal* [2]. Untuk Identifikasi *threat source*, perlu diperhatikan bahwa Institut XYZ merupakan sebuah institusi pendidikan. Berdasarkan penelitian sebelumnya [12], Institut XYZ perlu mewaspadai beberapa *threat source* yang umum ditemukan pada serangan yang terjadi di institusi pendidikan. Berikut *threat source* yang perlu diwaspadai disajikan pada tabel 2.

Tabel 2. *Threat Source (Adversarial)*

ID	Threat Source	Capability	Intent	Targeting
ADV-1	Hacktivist	High	Moderate	High
ADV-2	Cyber Criminal	High	High	Moderate
ADV-3	Orang dalam	Moderate	High	Very High
ADV-4	Mata-Mata	Very High	Moderate	High
ADV-5	Oportunis	Low	Very Low	Very Low

Langkah berikutnya adalah menentukan *threat event* yang berkemungkinan muncul pada host *digilib*. Berbeda dengan pendekatan NIST SP 800-30 Rev 1 di mana *threat event* ditentukan berdasarkan *threat source*, dalam penelitian ini, *threat event* ditentukan berdasarkan kerentanan yang berhasil

diidentifikasi pada tahap sebelumnya. Pendekatan ini diambil untuk memastikan cakupan penelitian tetap terfokus pada evaluasi risiko kerentanan yang ada pada aplikasi web. Tanda pengenal dibuat untuk setiap *threat event* dan diatur dalam tabel 3. Tabel ini dapat membantu menyusun dan merujuk pada informasi yang terkait dengan *threat event* yang spesifik, memudahkan dalam pemahaman dan penilaian risiko yang lebih terstruktur dan sistematis.

Tabel 3. *Threat Event*

Threat Event ID	Threat Event	Penjelasan Singkat
TE-1	Rekognisi/pemindaian pada sistem	Aktivitas untuk mengumpulkan informasi tentang sistem target
TE-2	Pencurian informasi pengguna	Upaya untuk mengakses, mengambil, atau mencuri data pengguna
TE-3	Penyebaran malware	Tindakan menyebarkan perangkat lunak berbahaya atau kode jahat
TE-4	Manipulasi konten	Memodifikasi, mengubah, atau mengganti konten pada sebuah situs
TE-5	Serangan phishing	Mencoba mendapatkan informasi sensitif melalui pesan palsu
TE-6	Pembajakan akun pengguna	Mengambil alih kendali atas akun pengguna yang sah
TE-7	Gangguan operasional web	Upaya untuk mengganggu atau merusak operasional situs web
TE-8	Manipulasi atau menghapus data	Mengubah, menghapus, atau merusak data yang ada pada sistem
TE-9	Pengalihan pengguna ke situs yang tidak diinginkan	Mengarahkan pengguna ke situs web yang tidak diinginkan
TE-10	Mengakses secara tidak sah	Usaha untuk mengakses sumber daya atau sistem komputer tanpa izin

G. Menentukan *Likelihood*

Setelah berhasil mengidentifikasi ancaman, langkah selanjutnya adalah mengevaluasi tingkat kemungkinan masing-masing ancaman (*likelihood*). Untuk memperoleh skor *likelihood* keseluruhan, perlu ditentukan skor *initiation likelihood* dan skor *impact likelihood*. Skor kemungkinan inisiasi direpresentasikan oleh kombinasi faktor-faktor seperti *targeting*, *intent*, dan *capability* dari tabel 2. Selain itu, peneliti juga mempertimbangkan faktor jumlah *threat source* yang terkait dengan sebuah *threat event*. Kemudian diikuti dengan menentukan skor *impact likelihood* yang dapat diperoleh dengan kombinasi faktor-faktor seperti *capability* pada tabel 2 dan CVSS pada tabel 1. Keduanya lalu dianalisis sehingga mendapat tingkat *likelihood* yang disajikan pada tabel 4.

Tabel 4. *Overall Likelihood*

Threat Event ID	Initiation Likelihood	Impact Likelihood	Overall Likelihood
TE-1	High	Very High	Very High
TE-2	Moderate	Low	Low
TE-3	Low	High	Moderate
TE-4	Moderate	Very High	High
TE-5	Moderate	Moderate	Moderate
TE-6	Moderate	High	Moderate
TE-7	Very High	Very High	Very High
TE-8	Low	Moderate	Low
TE-9	Low	Very Low	Very Low
TE-10	Very High	High	Very High

H. Menentukan Dampak

Langkah selanjutnya adalah menentukan dampak yang dapat terjadi akibat dari setiap ancaman yang telah diidentifikasi sebelumnya. Pada tahap ini, dilakukan evaluasi terhadap tingkat kerugian yang mungkin timbul jika dampak tersebut berhasil terjadi. Penilaian dampak ini penting untuk memahami konsekuensi yang mungkin terjadi pada instansi dan aset yang terlibat. Dalam penentuan dampak, beberapa faktor yang diperhatikan antara lain adalah keterjaminan keaslian dan keutuhan data, keterjagaan informasi yang sensitif, dan kemampuan akses terhadap sumber daya. Selain itu, dampak juga ditentukan berdasarkan kondisi yang dihadapi pada host *digilib* baik pengguna, pihak ketiga, dan Institut XYZ. Setiap ancaman dinilai secara kolektif, dengan mempertimbangkan pengaruhnya terhadap setiap faktor yang telah disebutkan. Berikut adalah hasil dari penilaian dampak yang disajikan dalam tabel 5.

Tabel 5. *Impact*

Threat Event	Dampak	Tingkat Kerugian
TE-1	• Potensial kerentanan terungkap	Very Low
TE-2	• Hilangnya kepercayaan pengguna • Pencemaran reputasi • Pencurian Identitas • Potensi tuntutan hukum	High
TE-3	• Perangkat pengguna terinfeksi malware • Gangguan operasional • Kerugian finansial • Kebocoran data	High
TE-4	• Gangguan operasional • Pencemaran reputasi • Penipuan terhadap pengguna	Low
TE-5	• Pencurian Informasi • Pencurian Identitas	Moderate

TE-6	• Pencurian Identitas • Hilangnya akses pengguna • Akses tidak sah ke dalam sistem	Moderate
TE-7	• Gangguan operasional Penurunan produktivitas • Kerugian finansial	Moderate
TE-8	• Gangguan Operasional • Penipuan terhadap pengguna	Low
TE-9	• Kehilangan pengunjung	Very Low
TE-10	• Kebocoran data	Low

Jika diperhatikan dari data yang diperoleh dalam tabel 5, dapat disimpulkan bahwa mayoritas dampak yang teridentifikasi tidak memiliki pengaruh langsung terhadap Institut XYZ, melainkan melalui pengguna yang terhubung dengan sistem. Hal ini berkaitan erat dengan jenis aset yang disimpan di host *digilib*, di mana terdapat aset-aset penting yang terkait dengan pengguna. Selain itu, dampak-dampak yang teridentifikasi lebih banyak berdampak pada aset intelektual, seperti data pengunjung, dokumen jurnal, *e-book*, dan lain-lain. Ancaman-ancaman tersebut dapat memiliki konsekuensi yang signifikan terhadap operasional dan reputasi Institut XYZ.

I. Menentukan Risiko

Tahap terakhir yang dilakukan dalam penelitian ini adalah melakukan penilaian risiko. Tingkat risiko dapat diperoleh dengan menganalisis *likelihood* dari tabel 4 dan tingkat kerugian dampak dari tabel 5 dari suatu ancaman kedalam perhitungan (1). Dengan mengintegrasikan tingkat kerugian dampak dengan nilai *likelihood*, Institut XYZ dapat memperoleh pemahaman yang lebih jelas tentang tingkat risiko yang sedang dihadapi. Berikut adalah nilai risiko yang didapat dari keseluruhan penelitian disajikan dalam tabel 6.

Tabel 6. Risiko

Threat Event	Nilai Likelihood	Tingkat Dampak	Tingkat Risiko
TE-1	Very High	Very Low	Very Low
TE-2	Low	High	Low
TE-3	Moderate	High	Moderate
TE-4	High	Low	Low
TE-5	Moderate	Moderate	Moderate
TE-6	Moderate	Moderate	Moderate
TE-7	Very High	Moderate	Moderate
TE-8	Low	Low	Low
TE-9	Very Low	Very Low	Very Low
TE-10	Very High	Low	Low

Hasil akhir dari analisis risiko ini memberikan gambaran tentang tingkat risiko secara keseluruhan yang dimiliki oleh Institut XYZ. Informasi ini dapat digunakan sebagai dasar untuk mengambil langkah-langkah mitigasi yang sesuai dan memprioritaskan upaya pengamanan yang diperlukan. Penting bagi Institut XYZ untuk memahami dan menginterpretasikan hasil akhir ini dengan cermat. Dalam menangani risiko, instansi harus mempertimbangkan tingkat risiko yang dapat diterima, sumber daya yang tersedia, dan kebijakan keamanan yang relevan. Dengan demikian, Institut XYZ dapat mengambil langkah-langkah yang tepat dalam mengelola dan mengurangi risiko yang ada

J. Rekomendasi Langkah Mitigasi

Setelah melakukan evaluasi risiko terhadap kerentanan keamanan pada aplikasi web *digilib*, peneliti telah menyusun beberapa rekomendasi langkah mitigasi risiko untuk Institut XYZ dari berbagai macam sumber [13], [14], [15]. Langkah-langkah mitigasi ini bertujuan untuk mengurangi kemungkinan terjadinya ancaman yang telah diidentifikasi. Langkah-Langkah mitigasi berdasarkan ancaman dituangkan dalam tabel 7.

Tabel 7. Langkah Mitigasi

Threat Event ID	Langkah Mitigasi
TE-1	• Memperbarui dan memasang perlindungan yang kuat pada firewall dan sistem keamanan jaringan • Menggunakan tools untuk memonitor dan mendeteksi aktivitas mencurigakan pada jaringan • Melakukan patch dan update terhadap sistem secara teratur
TE-2	• Mengimplementasikan enkripsi data pengguna yang sensitive • Menggunakan protokol keamanan yang aman untuk transmisi data, seperti HTTPS • Melakukan penggunaan dan pembaruan yang tepat terhadap kebijakan keamanan
TE-3	• Memasang perangkat lunak keamanan yang andal dan mengupdate secara teratur • Menghindari mengklik tautan atau lampiran yang mencurigakan • Melakukan scan antivirus dan malware secara berkala pada sistem
TE-4	• Memastikan adanya validasi input yang memadai pada aplikasi • Melakukan review dan pengujian yang teratur terhadap aplikasi untuk mengidentifikasi kerentanan • Melakukan patch dan update aplikasi secara berkala
TE-5	• Melakukan edukasi dan kesadaran pengguna tentang serangan phishing dan teknik sosial engineering • Menggunakan fitur email filtering untuk mengidentifikasi email phishing • Memverifikasi keaslian situs web sebelum memasukkan informasi sensitif
TE-6	• Menggunakan autentikasi ganda (two-factor authentication) untuk akun pengguna • Menggunakan kebijakan keamanan yang kuat untuk pengaturan kata sandi • Memantau aktivitas akun pengguna secara teratur
TE-7	• Menggunakan proteksi DDoS dan firewall untuk melindungi server dan infrastruktur jaringan • Memastikan adanya pemantauan dan deteksi dini terhadap serangan DDoS • Menerapkan kebijakan dan prosedur pemulihan yang cepat
TE-8	• Melakukan backup rutin dan penyimpanan data yang aman

	• Mengimplementasikan kebijakan akses yang ketat untuk mencegah manipulasi atau penghapusan tidak sah • Melakukan enkripsi data yang sensitif untuk melindungi kerahasiaan dan integritas
TE-9	• Memperbarui dan mengamankan konfigurasi server dan aplikasi • Menggunakan mekanisme redireksi yang aman dan terpercaya • Melakukan verifikasi keaslian URL sebelum mengakses situs
TE-10	• Menggunakan autentikasi yang kuat untuk melindungi akses ke sistem dan aplikasi • Melakukan manajemen hak akses yang ketat untuk pengguna • Memonitor dan mendeteksi aktivitas yang mencurigakan pada sistem dan jaringan

K. Reporting

Proses pelaporan dilakukan dengan menyusun hasil penelitian dalam bentuk dokumen. Dokumen tersebut telah diserahkan kepada Institut XYZ sebagai referensi untuk meninjau kembali kebijakan keamanan yang telah diterapkan, terutama pada aplikasi web XYZ. Dengan menyediakan dokumen ini kepada Institut XYZ, diharapkan Institut XYZ dapat menggunakan informasi dan rekomendasi yang disampaikan untuk meningkatkan kebijakan keamanan, menerapkan langkah-langkah mitigasi yang relevan, dan memastikan perlindungan yang lebih baik terhadap aset, data, dan layanan yang disediakan.

L. Cleanup

Setelah proses pelaporan selesai, tahap terakhir dalam penelitian ini adalah tahap cleanup atau pembersihan. Tahap ini penting untuk memastikan bahwa kerentanan yang telah diidentifikasi dan dilaporkan tidak jatuh ke pihak yang tidak bertanggung jawab serta mengembalikan lingkungan sistem ke keadaan seperti semula.

V. KESIMPULAN

Dari keseluruhan hasil penelitian, dapat disimpulkan sebagai berikut. Pengujian keamanan menggunakan OWASP WSTG berhasil membuahkan hasil yakni teridentifikasinya beberapa kerentanan pada host digilib. Kerentanan tersebut memicu risiko dimana hasil evaluasi menggunakan NIST SP 800-30 Rev. 1 menghasilkan 4 ancaman memiliki tingkat risiko menengah, 4 ancaman memiliki tangkat risiko rendah, dan 2 ancaman memiliki tingkat risiko sangat rendah. Hasil penelitian ini menunjukkan bahwa metodologi yang digunakan efektif untuk mengevaluasi risiko keamanan pada kerentanan aplikasi berbasis web. Institut XYZ diharapkan untuk memitigasi risiko yang berhasil diidentifikasi dimulai dari tingkat yang paling tinggi.

Langkah-langkah mitigasi berhasil ditentukan berdasarkan kerentanan yang teridentifikasi serta risiko yang berhasil dievaluasi. Berdasarkan hasil tersebut, Institut XYZ sebaiknya mengutamakan untuk melakukan mitigasi berupa pembaruan atau migrasi ke versi terbaru yang lebih aman dan mendapatkan dukungan pengembangan yang lebih baik. Selain itu, langkah mitigasi lainnya perlu dilakukan untuk mengurangi risiko serta mencegah terjadinya kerugian.

Selain kesimpulan di atas, terdapat saran yang perlu diperhatikan. Sebaiknya proses evaluasi risiko NIST SP 800-30 Rev 1 dilakukan oleh sebuah tim khusus yang ahli dalam bidangnya. Dengan dibentuknya tim khusus memungkinkan untuk penggabungan berbagai perspektif dan keahlian yang berbeda. Dengan demikian, evaluasi dapat menghasilkan hasil yang lebih akurat.

Dengan menerapkan langkah-langkah mitigasi yang tepat dan meningkatkan kesadaran keamanan, diharapkan Institut XYZ dapat mengurangi risiko dan melindungi data serta layanan yang disediakan dari ancaman yang ada.

REFERENSI

[1] D. Vargo, L. Zhu, B. Benwell and Z. Yan, "Digital technology use during COVID-19 pandemic: A rapid," *Human Behavior and Emerging Technologies*, no. 3, pp. 13-24, 2020.

[2] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2022," Badan Siber dan Sandi Negara, 2022.

[3] R. D. Aji, "Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open Web Application Security Project (OWASP) Pada Aplikasi Web Sistem Informasi Mahasiswa (Studi Kasus: Perguruan Tinggi XYZ)," 2016.

[4] A. F. Zulfi, "Evaluasi Keamanan Aplikasi Sistem Informasi Mahasiswa Menggunakan Framework VAPT (Studi Kasus : Sister Universitas Jember)," 2017.

[5] T. R. Syarif and D. A. Jatmiko, "Analisis Perbandingan Metode Web Security PTES, ISSAF dan OWASP di Dinas Komunikasi Dan Informasi Kota Bandung," 2019.

[6] R. R. Putra, E. Setiawan and A. Ambarawati, "Analisis Manajemen Risiko TI Pada Keamanan Data E-Learning Dan Aset TI Menggunakan NIST SP 800-30 Revisi 1," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 6, no. 1, pp. 96-105, 2019.

[7] S. Salnyk, P. Sydorkin, S. Nesterenko, A. Zaytcev and M. Konotopetc, "Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems," *Social Development and Security*, vol. 10, no. 6, 2020.

[8] National Institute of Standards and Technology, "NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[9] E. Saad and R. Mitchell, Web Security Testing Guide Version 4.2, Open Worldwide Application Security Project Foundation, 2020.

[10] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, no. 11, pp. 27-49, 2015.

[11] National Institute of Standards and Technology, "NVD - Vulnerability Metrics," 20 September 2022. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

[12] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet*, vol. 39, no. 2, 2021.

[13] National Institute of Standards and Technology, "NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations," September 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5.

[14] International Organization for Standardization, "ISO/IEC 27005 Information security, cybersecurity and privacy protection — Guidance on managing information security risks," International Organization for Standardization, 2022.

[15] Open Worldwide Application Security Project Foundation, "OWASP Cheat Sheet Series," [Online]. Available: https://cheatsheetseries.owasp.org/index.html.