Analisis Keamanan Sistem Informasi Aplikasi Berbasis Website pada PTPN XII Menggunakan OWASP

Muhamad Arsyad[*1)], Muhamad Nasrullah[2)], Purnama Anaking[3)]
[1,2,3)]Sistem Informasi, Fakultas Teknologi Informasi dan Bisnis, Institut Teknologi Telkom Surabaya, Ketintang, Surabaya, 60231, Indonesia
marsyad@student.ittelkom-sby.ac.id

Abstrak

Banyak organisasi telah membangun aplikasi sistem informasi untuk menghadapi digitalisasi. Namun, dengan meningkatnya proses digitalisasi, juga terjadi peningkatan serangan siber. Pada tahun 2022, Indonesia mengalami peningkatan kasus serangan siber, seperti pelanggaran data. Penelitian ini melakukan pengujian keamanan pada tiga aplikasi berbasis website di PT XYZ untuk mengukur tingkat keamanannya. Pengujian keamanan mengikuti pedoman OWASP WSTG. Pengujian berfokus pada dua kategori: authentication testing dan input validation testing, hasilnya ditemukan total sembilan kerentanan, dengan risiko tertinggi terkait injeksi SQL dan cross-site scripting. Kerentanan ini dapat memungkinkan penyerang untuk mendapatkan informasi dari basis data aplikasi serta merusak konten situs web. Beberapa cara untuk memperbaiki kerentanan ini antara lain mengikuti standar keamanan pada framework yang digunakan dan memperbarui plugin atau teknologi ke versi terbaru.

Kata kunci: *Keamanan Sistem Informasi, Penetration Testing, web security, OWASP, WSTG*

1. Pendahuluan (Introduction)

Digitalisasi adalah proses penggunaan teknologi digital untuk meningkatkan efisiensi dan kualitas layanan dalam berbagai sektor. Pandemi COVID-19 telah mempercepat digitalisasi, terutama di sektor-sektor yang sebelumnya tertinggal (Florence Jaumotte, Myrto Oikonomou , Carlo Pizzinelli 2023). Website adalah salah satu contoh teknologi digital yang banyak digunakan untuk menyampaikan informasi dan layanan secara online. Namun, digitalisasi juga membawa tantangan dan risiko dalam hal keamanan siber, penelitian berjudul "*The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World*" (Almeida, Duarte Santos, dan Augusto Monteiro 2020) mengatakan bahwa *cybersecurity* serta privasi menjadi dua elemen kunci untuk mendukung integrasi teknologi. Meningkatnya aktivitas digital juga memicu peningkatan serangan siber, pada tahun 2022 kasus kebocoran data di Indonesia mengalami peningkatan. Menurut perusahaan keamanan siber Surfshark, pada kuartal tiga tahun 2022 Indonesia menduduki peringkat ketiga disusul oleh perancis pada peringkat dua dan rusia di urutan pertama (Surfshark 2022). Dari tahun 2021 sampai 2023 Indonesia sering mengalami masalah dalam serangan siber terutama kasus kebocoran data (TEMPO.CO 2021).

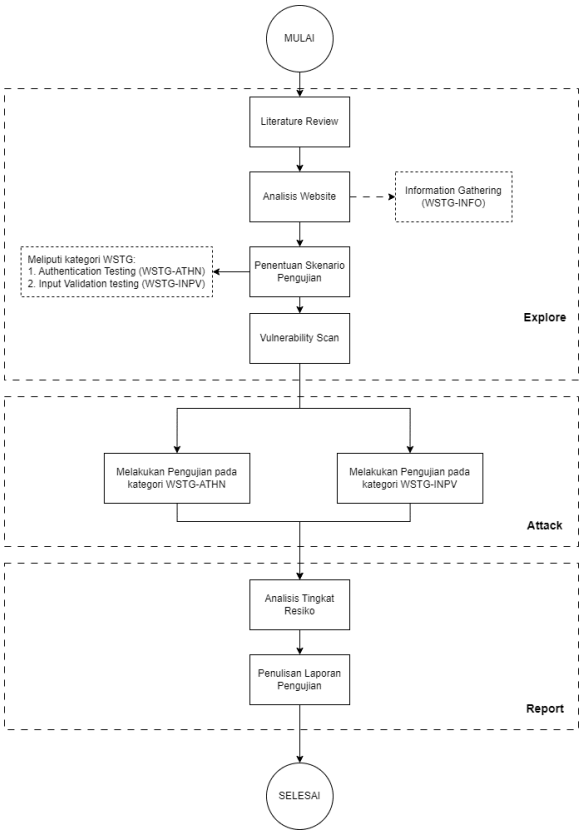
Keamanan dalam pengembangan sebuah aplikasi website juga tidak dapat diabaikan (Armando et al. 2022), salah satu contoh serangan yang sering diterima oleh website adalah web defacement. Serangan web defacement sendiri adalah serangan terhadap situs web yang bertujuan untuk merusak atau mengubah konten pada halaman situs web tersebut, dalam "Lanskap Keamanan Siber" Badan Sandi Siber Nasional (BSSN) web defacement selalu masuk ke dalam tiga teratas insiden dalam layanan BSSN, pada tahun 2021 terdapat 5.940 kasus web defacement dan selama tahun 2022 terjadi 2.348 kasus serangan web defacement (Badan Siber Dan Sandi Negara 2023), menurut BSSN selama tahun 2022

sektor yang paling banyak terkena serangan web defacement adalah sektor administrasi pemerintahan dengan jumlah kasus 885 kasus.

Sebuah studi oleh Frost dan Sullivan (Microsoft 2018) mengungkapkan bahwa potensi kerugian ekonomi rata – rata pada perusahan besar dapat mencapai 30 milliar dollar AS atau setara dengan 450 trilliun rupiah. Untuk itu, penting dilakukan analisis keamanan agar mengetahui apakah aplikasi yang sudah dibangun memiliki keamanan sudah memenuhi standar (Kristanto et al. 2019). Penelitian ini melakukan analisis keamanan terhadap tiga aplikasi website PT XYZ yang selanjutnya disebut *website* A, *website* B, *website* C. Pengujian dilakukan dengan menggunakan teknik *penetration testing*, yaitu simulasi serangan secara langsung terhadap aplikasi untuk menemukan celah keamanan. Pengujian dilakukan dengan *mengikuti Open Worldwide Security Application Project - Web Security Testing Guide* (OWASP – WSTG) yang merupakan sebuah standar industri yang diakui oleh banyak organisasi dan profesional keamanan siber di seluruh dunia (OWASP Foundation n.d.-a). Tujuan dilakukan analisis keamanan adalah untuk mengetahui tingkat keamanan aplikasi website PT XYZ serta memberikan rekomendasi untuk meningkatkan keamanan aplikasi.

2. Metode Penelitian (Methods)

Penelitian ini menggunakan kerangka kerja Open Worldwide Application Security Project - Web Security Testing Guide (OWASP – WSTG). Versi yang digunakan adalah WSTG versi 4.2 yang merupakan versi stabil. Alur metode penelitian lebih lengkap dapat dilihat pada gambar 1. Penelitian terdiri dari tiga tahapan, pertama yaitu tahap explore yaitu mempelajari tetang sistem yang akan diuji, kemudian tahap attack, pada tahap attack penguji mencoba mengeksploitasi kerentanan dan terakhir yaitu tahap report dimana pada tahap ini hasil pengujian ditulis dalam laporan termasuk kerentanan yang ditemukan, cara eksploitasi dan tingkat risiko dari kerentanan.



Gambar 1 Alur penelitian

2.1. Analisis Website

Pada tahap ini dilakukan analisis terhadap website untuk mengetahui teknologi yang dipakai oleh website serta informasi tentang sistem yang dipakai. Dengan mengetahui informasi tersebut dapat menghemat waktu dan menentukan ruang lingkup pengujian serta skenario pengujian yang cocok dengan website target. Analisis website dilakukan dengan mengikuti kategori *information gathering* pada WSTG dan observasi langsung terhadap website yang diuji. Detail dari proses *information gathering* WSTG dapat dilihat pada tabel 1. Proses analisis menggunakan bantuan tools untuk melakukan scanning otomatis. *Tools* yang digunakan meliputi: *Wappalyzer, Google, Duckduckgo, nmap, wpscan.* Selama proses pengujian setiap aktivitas akan dicatat pada WSTG *Checklist,* setiap skenario ID diberi tanda antara lain: *Pass* artinya tidak ada kerentanan atau masalah yang ditemukan; *Issues* artinya ada kerentanan atau masalah yang ditemukan; *Not Applicable* artinya tidak dapat diterapkan.

Tabel 1. Daftar information gathering

ID	Judul	Keterangan
WSTG-INFO-01	*Conduct Search Engine Discovery Reconnaissance for Information Leakage*	Mencari informasi terkait dengan aplikasi *website* menggunakan mesin pencari seperti (*google, bing, duckduckgo, dst).*
WSTG-INFO-02	*Fingerprint Web Server*	Mencari informasi tentang *web server* yang digunakan oleh aplikasi

ID	Judul	Keterangan
WSTG-INFO-03	*Review Webserver Metafiles for Information Leakage*	Mencari informasi tentang file atau metadata *webserver* seperti *(robot.txt, security.txt, dst.)*
WSTG-INFO-04	*Enumerate Applications on Webserver*	Mencari informasi aplikasi lain yang terkait dengan aplikasi *web* yang sedang diuji.
WSTG-INFO-05	*Review Web Page Content for Information Leakage*	Mencari informasi dari kontent *website* yang dapat diakses, kontent bisa meliputi komentar kode pada halaman *website*
WSTG-INFO-06	*Identify Application Entry Points*	Mengidentifikasi titik – titik injeksi ke dalam aplikasi.
WSTG-INFO-07	*Map Execution Paths Through Application*	Memahami struktur aplikasi
WSTG-INFO-08	*Fingerprint Web Application Framework*	Mencari informasi terkait kerangka kerja aplikasi
WSTG-INFO-10	*Map Application Architecture*	Memahami arsitektur dan teknologi pada aplikasi *website* yang diuji.

2.2. Skenario Pengujian

Dari hasil analisis website, ditentukan skenario – skenario pengujian yang sesuai berdasarkan OWASP : Web Security Testing Guide v4.2. Pada penelitian ini fokus terhadap dua kategori pengujian yaitu *Authentication Testing* dan *Input Validation Testing* dengan total 29 skenario pengujian. Sama seperti pada tahap *information gathering* selama proses pengujian setiap aktivitas akan dicatat pada WSTG *Checklist,* setiap skenario ID diberi tanda *Pass, Issues, Not Applicable.* Pengujian dilakukan dengan pendekatan *black-box testing* yang lebih berfokus kedalam *functional testing*

2.2.1. Authentication Testing

Kategori *authentication testing* merupakan pengujian yang berfokus pada fitur autentikasi yang ada pada aplikasi website. Daftar skenario pengujian untuk kategori *authentication testing* dapat dilihat pada tabel 2. Fitur autentikasi merupakan proses verifikasi identitas pengguna pada sebuah aplikasi dengan mencocokan kredensial yang tersimpan pada basis data dengan yang dimasukan oleh pengguna. fitur autentikasi merupakan fitur penting dalam menjaga keamanan sistem dan termasuk fundamental dalam web security (Awad et al. 2019).

Tabel 2. Daftar skenario pengujian *authentication testing*

ID Skenario Pengujian	Judul Pengujian
WSTG-ATHN-01	*Testing for Credential Transported Over an Encrypted Channel*
WSTG-ATHN-02	*Testing for Default Credentials*
WSTG-ATHN-03	*Testing for Weak Lock Out Mechanism*
WSTG-ATHN-04	*Testing for Bypassing Authentication Schema*
WSTG-ATHN-05	*Testing for Vulnerable Remember Password*
WSTG-ATHN-06	*Testing for Browser Cache Weaknesses*
WSTG-ATHN-07	*Testing for Weak Password Policy*
WSTG-ATHN-08	*Testing for Weak Security Question Answer*

ID Skenario Pengujian	Judul Pengujian
WSTG-ATHN-09	*Testing for Weak Password Change or Reset Functionalities*
WSTG-ATHN-10	*Testing for Weaker Authentication in Alternative Channel*

2.2.2. Input Validation Testing

kategori *input validation testing* berfokus pada pengujian validasi input data yang diterima oleh aplikasi. Validasi input merupakan proses memverifikasi dan memvalidasi setiap input data yang masuk ke dalam aplikasi web, sehingga dapat memastikan bahwa input tersebut sesuai dengan tipe, format, dan batasan yang telah ditentukan (Khalaf et al. 2021).

Tabel 3. Daftar skenario pengujian input validation testing

ID Skenario Pengujian	Judul Pengujian
WSTG-INPV-01	*Testing for Reflected Cross Site Scripting*
WSTG-INPV-02	*Testing for Stored Cross Site Scripting*
WSTG-INPV-03	*Testing for HTTP Verb Tampering*
WSTG-INPV-4	*Testing for HTTP Parameter Pollution*
WSTG-INPV-05	*Testing for SQL Injection*
WSTG-INPV-06	*Testing for LDAP Injection*
WSTG-INPV-07	*Testing for XML Injection*
WSTG-INPV-08	*Testing for SSI Injection*
WSTG-INPV-09	*Testing for XPath Injection*
WSTG-INPV-10	*Testing for IMAP SMTP Injection*
WSTG-INPV-11	*Testing for Code Injection*
WSTG-INPV-12	*Testing for Command Injection*
WSTG-INPV-13	*Testing for Format String Injection*
WSTG-INPV-14	*Testing for Incubated Vulnerability*
WSTG-INPV-15	*Testing for HTTP Splitting Smuggling*
WSTG-INPV-16	*Testing for HTTP Incoming Requests*
WSTG-INPV-17	*Testing for Host Header Injection*
WSTG-INPV-18	*Testing for Server-side Template Injection*
WSTG-INPV-19	*Testing for Server-Side Request Forgery*

2.3. Analisis Tingkat Risiko

Setiap item kerentanan yang ditermukan diberikan label tingkat risiko *Note, Critical, High, Moderate, dan Low*, pembagian klasifikasi risiko dapat dilihat pada tabel 5. Metode perhitugan risiko yang digunakan pada penelitian ini adalah pendekatan analisis risiko OWASP (OWASP Foundation). Model perhitungan risiko yang dipakai adalah sebagai berikut:

$$Risk = Likelihood \times Impact \quad (1)$$

Keterangan:

- *Risk* adalah keseluruhan risiko yang dihasilkan oleh suatu ancaman keamanan.
- *Likelihood* adalah probabilitas kemungkinan terjadinya suatu ancaman keamanan.
- *Impact* adalah dampak yang dapat diberikan oleh suatu ancaman keamanan.

2.3.1. Metode Memperkirakan *Likelihood*

Untuk memperkirakan nilai dari likelihood dihitung dari dua pasang faktor yang mempengaruhi likelihood yaitu Threat Agent Factors dan Vulnerability Factors. Threat Agent Factorsadalah faktor yang meliputi kemampuan, motivasi, dan sumber daya dari penyerang (agent) untuk mengeksploitasi kerentanan keamanan. *Threat agent factors* terdiri dari: *skill level; motive; opportunity;* dan *size*. Kemudian *Vulnerability Factors* merujuk kepada faktor – faktor yang terkait dengan kerentanan keamanan aplikasi, yang mencakup kompleksitas, tingkat kesulitan, dan atau potensi dampak dari eksploitasi keamanan tersebut. *Vulnerability factors* terdiri dari: Ease *of Discovery; Ease of Exploit; Awareness;* dan *Intrusion Detection*. Setiap faktor memiliki nilai terendah nol dan tertinggi sembilan.

2.3.2. Metode Memperkirakan *Impact*

Impact yang dihasilkan dari suatu ancaman keamanan dipengaruhi oleh dua faktor yaitu *Technical Impact Factors* dan *Business Impact Factors*. *technical impact factors* digunakan untuk mengevaluasi dampak teknis yang mungkin terjadi apabila kerentanan keamanan yang ditemukan dieksploitasi oleh penyerang. Terdiri dari: *Loss of Confidentiality; Loss of Integrity; Loss of Availability; Loss of Accountability.* Kemudian evaluasi dampak pada bisnis yang terdiri dari: *Financial damage; Reputation damage; Non-compliance; Privacy violation.*

2.3.3. Klasifikasi Kategori Tingkat Risiko

Nilai rata – rata dari likelihood dan impact dalam skala satu sampai sembilan dibagi menjadi tiga kategori yaitu low, moderate, dan high. Pembagian nilai tiap kategori dapat dilihat pada tabel 4, kemudian tingkat keseluruhan risiko didapat dari perhitungan nilai rata – rata *likelihood* dan nilai rata – rata *impact*.

Tabel 4. Pembagian kategori likelihood dan impact

Kategori	**Nilai**
Low	0 sampai kurang dari 3
Moderate	3 sampai kurang dari 6
High	6 sampai dengan 9

Tabel 5. Klasifikasi tingkat risiko secara keseluruhan

Likelihood	***Impact***	**Tingkat Risiko**
Low	*Low*	*Note*
Low	*Moderate*	*Low*
Low	*High*	*Moderate*
Moderate	*Low*	*Low*
Moderate	*Moderate*	*Moderate*
Moderate	*High*	*High*
High	*Low*	*Moderate*
High	*Moderate*	*High*
High	*High*	*Critical*

3. Hasil dan Pembahasan (Results and Discussions)

3.1. Hasil Analisis Website

Proses *information gathering* dilakuan dengan bantuan *tool wappalyzer* dan *wpscan*. Proses *information gathering* dapat dilihat pada tabel 6. Didapatkan bahwa ketiga website dibangun dengan menggunakan bahasa pemrograman yang sama yaitu bahasa *PHP*, namun framework yang dipakai oleh ketiga website berbeda. Untuk website A menggunakan *CMS Wordpress*, website B menggunakan *codeigniter* dan website C menggunakan *laravel.* Kemudian *web server* yang dipakai oleh ketiganya adalah linux ubuntu. Daftar teknologi yang dipakai oleh ketiga website dapat dilihat pada tabel 7.

Setelah diketahui bahwa *website* A menggunakan *wordpress* maka proses pemindaian dilakukan dengan bantuan *tool wpscan*. Didapatkan bahwa versi *wordpress* yang dipakai oleh *website* A adalah versi 5.4 yang mana adalah versi lama dan memiliki beberapa kerentanan yang sudah diketahui, *website* A juga memakai beberapa *plugin* dengan versi yang memiliki kerentanan.

Tabel 6. Proses information gathering

ID	*Website* A	*Website* B	*Website* C
WSTG-INFO-01	*Pass*	*Pass*	*Pass*
WSTG-INFO-02	*Issues*	*Pass*	*Pass*
WSTG-INFO-03	*Pass*	*Pass*	*Pass*
WSTG-INFO-04	*Pass*	*Pass*	*Pass*
WSTG-INFO-05	*Pass*	*Issues*	*Pass*
WSTG-INFO-06	*Pass*	*Pass*	*Pass*
WSTG-INFO-07	*Pass*	*Pass*	*Pass*
WSTG-INFO-08	*Issues*	*Pass*	*Pass*
WSTG-INFO-10	*Pass*	*Pass*	*Pass*

Pada *website* A dapat ditemukan *issue* pada WSTG-INFO-02 atau *fingerprint web server* yaitu informasi mengenari sistem informasi pada *server* yang digunakan oleh aplikasi, pada *website* A juga ditemukan *issue* pada WSTG-INFO-08 dengan nama "*Fingerprint Web Application Framework"* yaitu *file backup* konfigurasi *wordpress*. Pada halaman *website* B terdapat *issue* pada WSTG-INFO-05 atau "*Review Webpage Content for Information Leakage"*, ditemukan kode *javascript* yang memuat informasi *url endpoint*, informasi ini dapat dimanfaatkan oleh penyerang.

Tabel 7. Daftar teknologi yang dipakai ketiga website

Aplikasi	Kategori Teknologi	Keterangan
Website A	WordPress themes	ThemeGrill ColorMag
	Operating systems	Ubuntu
	Programming languages	PHP
	Databases	MySQL
	CMS	WordPress 5.4
	*Web server*s	Apache HTTP *Server*
Website B	*Web* frameworks	CodeIgniter
	UI frameworks	Bootstrap
	Programming languages	PHP
Website C	*Web server*s	Apache HTTP *Server*
	Web frameworks	Laravel
	UI frameworks	Bootstrap

Programming languages	PHP

3.2. Pembagian Skenario Pengujian

Berdasarkan informasi dari hasil analisis website dilakukan pembagian skenario pengujian yang sesuai dengan informasi tersebut. Pengujian dengan pendekatan *black-box testing* artinya tidak ada informasi mengenai kredensial yang sah, oleh karena itu pengujian WSTG-ATHN-05, WSTG-ATHN-06 dan WSTG-ATHN-07 tidak dapat dilakukan (*Not Applicable)*. Skenario pengujian juga tidak dilakukan untuk aplikasi yang tidak memiliki fitur yang relevan terhadap skenario tersebut. Daftar skenario pengujian yang akan dilakukan pada tiap *website* dapat dilihat pada tabel 8, tabel 9 dan tabel 10. Pada *website* A dilakukan pengujian terhadap 20 skenario pengujian yang terbagi menjadi enam pengujian *authentication testing* (ATHN) dan 14 pengujian *input validation testing* (INPV), kemudian untuk *website* B dilakukan pengujian terhadap 19 skenario pengujian yang terbagi menjadi 5 pengujian ATHN dan 14 pengujian INPV, sedangkan website C dilakukan pengujian terhadap 6 skenario pengujian yang berfokus pada kategori ATHN.

3.3. Hasil Pengujian

3.3.1. Hasil Pengujian *Website* A

Dari hasil pengujian ditemukan sebanyak dua masalah keamanan (*issues*) pada website A. Satu masalah tersebut terdapat dikategori *authentication testing* dan satu masalah lainya pada kategori *input validation testing*, daftar lengkap hasil pengujian tiap skenario dapat dilihat pada tabel 8.

Pada kategori *authentication testing* kerentanan ditemukan pada skenario WSTG-ATHN-03 (*Testing for Weak Lock Out Mechanism*) ditemukan bahwa *website* A tidak memiliki mekanisme penguncian akun atau *IP device* sehingga rawan terhadap serangan *brute force.*

Kemudian pada kategori *input validation testing* ditemukan kerentanan pada skenario WSTG-IPNV-05 (*Testing for SQL Injection*). Memanfaatkan *bug* pada *plugin wordpress* berhasil melakukan serangan sql injection dan mendapatkan *user_email*, dan *user_passsword* terenkripsi.

Tabel 8. Hasil pengujian *website* A

No	ID Skenario Pengujian	Status Pengujian
1	WSTG-ATHN-01	*Pass*
2	WSTG-ATHN-02	*Pass*
3	WSTG-ATHN-03	*Issues*
4	WSTG-ATHN-04	*Pass*
5	WSTG-ATHN-09	*Pass*
6	WSTG-ATHN-10	*Pass*
7	WSTG-INPV-01	*Pass*
8	WSTG-INPV-02	*Pass*
9	WSTG-INPV-04	*Pass*
10	WSTG-INPV-05	*Issues*
11	WSTG-INPV-07	*Pass*
12	WSTG-INPV-08	*Pass*
13	WSTG-INPV-12	*Pass*
14	WSTG-INPV-13	*Pass*
15	WSTG-INPV-14	*Pass*

No	ID Skenario Pengujian	Status Pengujian
16	WSTG-INPV-15	*Pass*
17	WSTG-INPV-16	*Pass*
18	WSTG-INPV-17	*Pass*
19	WSTG-INPV-18	*Pass*
20	WSTG-INPV-19	*Pass*

3.3.2. Hasil Pengujian *Website* B

Dari hasil pengujian ditemukan sebanyak lima masalah keamanan (*issues*) pada website B. Pengujian menemukan dua masalah pada kategori authentication testing dan empat masalah pada kategori input validation testing, daftar lengkap hasil pengujian tiap skenario dapat dilihat pada tabel 9. Ditemukan kerentanan pada WSTG-ATHN-03 (*Testing for Weak Lock Out Mechanism*) dan WSTG-ATHN-04 (*Testing for Bypassing Authentication Schema*) ternyata mekanisme autentikasi pada website B dapat ditembus dengan *sql injection* tipe *blind boolean.* Setelah itu di kategori *input validation testing* ditemukan kerentanan pada skenario WSTG-INPV-02 (*Testing for Stored Cross Site Scripting*), WSTG-INPV-05 (*Testing for SQL Injection*), WSTG-INPV-14 (*Testing for Incubated Vulnerability*).

Tabel 9. Hasil pengujian *website* B

No	ID Skenario Pengujian	Status
1	WSTG-ATHN-01	*Pass*
2	WSTG-ATHN-02	*Pass*
3	WSTG-ATHN-03	*Issues*
4	WSTG-ATHN-04	*Issues*
5	WSTG-ATHN-10	*N/A*
6	WSTG-INPV-01	*Pass*
7	WSTG-INPV-02	*Issues*
8	WSTG-INPV-04	*Pass*
9	WSTG-INPV-05	*Issues*
10	WSTG-INPV-08	*Pass*
11	WSTG-INPV-11	*Pass*
12	WSTG-INPV-12	*Pass*
13	WSTG-INPV-13	*N/A*
14	WSTG-INPV-14	*Issue*
15	WSTG-INPV-15	*Pass*
16	WSTG-INPV-16	*Pass*
17	WSTG-INPV-17	*Pass*
18	WSTG-INPV-18	*Pass*
19	WSTG-INPV-19	*pass*

3.3.3. Hasil Pengujian *Website* C

Dari hasil pengujian ditemukan sebanyak satu masalah keamanan (*issues*) pada website C. Satu masalah tersebut adalah tidak adanya mekanisme penguncian pada autentikasi, daftar lengkap hasil pengujian tiap skenario dapat dilihat pada tabel 10.

Tabel 10. Hasil pengujian *website* C

No	ID Skenario Pengujian	Status
1	WSTG-ATHN-01	*Pass*

2	WSTG-ATHN-02	*Pass*
3	WSTG-ATHN-03	*Issues*
4	WSTG-ATHN-04	*Pass*
5	WSTG-ATHN-05	*Pass*
6	WSTG-ATHN-06	*Pass*
7	WSTG-ATHN-09	*N/A*
8	WSTG-ATHN-10	*N/A*

3.4. Analisis Tingkat Risiko

Untuk memudahkan pembacaan dan penulisan setiap kerentanan (issue) yang ditemukan pada saat penetration testing ataupun saat information gathering ditulis dalam kode yang disebut Reference ID. Keterangan kode Reference ID dapat dilihat pada tabel 11. daftar semua kerentanan yang telah ditemukan dengan skenario WSTG pada tabel 12.

Tabel 11. Keterangan kode *reference ID*

Kode	Keterangan
PT	*Website A*
AK	*Website B*
SP	*Website C*

Tabel 12. Daftar temuan kerentanan dan tingkat risiko

Refence ID	***Title***	***Likelihood Score***	***Impact Score***	***Risk***
PT-01	*Information of Website Configuration*	*5,5*	*3,25*	*Moderate*
PT-02	*Change WP Admin Bypass Security Page*	*5,375*	*1,125*	*Low*
PT-03	*Weak Lockout Mechanism on website A*	*5,875*	*0,625*	*Low*
PT-04	*SQL injection via Plugin Page View Count*	*6,375*	*1,75*	*Moderate*
AK-01	*Weak Lockout Mechanism on Website B*	*5,875*	*0,625*	*Low*
AK-02	*Bypass login Mechanism*	*7,625*	*4,125*	*High*
AK-03	*SQL Injection*	*7,625*	*4,125*	*High*
AK-04	*Stored XSS Can Run on Website*	*6,5*	*3,25*	*High*
SP-01	*Weak Lockout Mechanism on website C*	*5,125*	*0,625*	*Low*

Berdasarkan pengujian yang sudah dilakukan, total sembilan kerentanan keamanan berhasil diidentifikasi dengan tingkat risiko tertinggi adalah *high* dan yang terendah adalah *low*. Daftar jumlah temuan kerentanan berdsarkan tingkat risiko dapat dilihat pada tabel 13, total ada tiga kerentanan dengan tingkat risiko *high* kemudian dua kerentanan dalam tingkat risiko *moderate* dan empat kerentanan risiko *low*. Pada website A diidentifikasi total tiga kerentanan yang terdiri dari satu kerentanan *moderate* dan dua kerentanan *low*. Pada aplikasi website C hanya terdapat satu kerentanan dengan tingkat *low*. Sedangkan pada aplikasi website B berhasil diidentifikasi total enam kerentanan yang terdiri dari tiga kerentanan tingkat *high*, satu kerentanan *moderate*, dan satu kerentanan tingkat low. Tingkat risiko tertingi yang berhasil ditemukan memberikan kemungkinan bagi penyerang untuk mendapatkan informasi dari *database*, seperti *username*, *email*, *password* dalam bentuk *hash*, dsb. Namun tidak mampu melakukan modifikasi terhadap data yang berada pada database. Akan tetapi juga terdapat kemungkinan bagi penyerang menggunakan informasi tersebut untuk merusak sistem.

Tabel 13. Daftar jumlah kerentanan berdasarkan tingkat risiko

Aplikasi	***Tingkat Risiko***				***Total***
	Critical	*High*	*Moderate*	*Low*	
Website A	*0*	*0*	*1*	*2*	*3*
Website B	0	3	1	1	5
Website C	0	0	0	1	1

4. Kesimpulan (Conclusion)

Berdasarkan hasil pengujian terhadap tiga website menggunakan OWASP framework, tingkat keamanan aplikasi website PT XYZ secara keseluruhan tergolong kurang aman. Untuk menangani kerentanan terkait halaman login dan sql injection dan pada website A pihak PT XYZ dapat melakukan upgrade plugin ke versi terbaru. Lalu kerentanan terkait file backup konfigurasi cukup menghapus *file backup* yang masih tersedia pada direktori *website* atau memindahkan *file* tersebut agar tidak dapat diakses oleh semua *user*.

Kerentanan pada *website* B dapat diatasi dengan menerapkan standar prosedur pada yang sudah dibuat oleh framework codeigniter untuk kerentanan sql injection dapat menerapkan teknik query binding atau active record class sedangkan untuk kerentanan terkait cross site scripting dapat mengaktifkan konfigurasi global_xss_filtering pada codigniter untuk validasi dan sanitaze setiap input user. Pada *website* C, cara mengatasi kerentanan weack lockout dapat dilakukan dengan menerapkan *rate limit* atau *login throttling*. Untuk urutan perbaikan pihak PT XYZ perlu memperbaiki kerentanan

dengan tingkat *high* pada aplikasi *website* B terlebih dahulu karena memiliki dampak yang paling besar dibanding dengan kerentanan pada aplikasi lain. Kemudian setelah itu bisa memperbaiki kerentanan pada *website* A karena cukup mudah untuk diperbaiki. Urutan terakhir adalah aplikasi *website* C karena memiliki tingkat low dan sudah mempunyai mekanisme keamanan yang lebih baik dibanding dengan dua aplikasi lain.

Daftar Pustaka

Almeida, Fernando, Jose Duarte Santos, dan Jose Augusto Monteiro. 2020. "The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World." *IEEE Engineering Management Review* 48(3):97–103. doi: 10.1109/EMR.2020.3013206.

Armando, Rio, I. G. Ag Kom Agnam Melyantara, Rizma Elfariani, Desy Fitri Aulia Latuconsina, dan Muhammad Nasrullah. 2022. "IT Support Website Security Evaluation Using Vulnerability Assessment Tools." *Journal of Information Systems and Informatics* 4(4):949–57. doi: 10.51519/journalisi.v4i4.330.

Awad, Mohammed, Muhammed Ali, Maen Takruri, dan Shereen Ismail. 2019. "Security vulnerabilities related to web-based data." *Telkomnika (Telecommunication Computing Electronics and Control)* 17(2):852–56. doi: 10.12928/TELKOMNIKA.v17i2.10484.

Badan Siber Dan Sandi Negara. 2023. "BSSN Ungkap Lanskap Keamanan Siber Indonesia Tahun 2022 untuk Literasi Budaya Keamanan Siber." *BSSN (Badan Siber Dan Sandi Negara)*.

Florence Jaumotte, Myrto Oikonomou , Carlo Pizzinelli, Marina M. Tavares. 2023. "How Pandemic Accelerated Digital Transformation in Advanced Economies." Diambil 15 Juli 2023 (https://www.imf.org/en/Blogs/Articles/2023/03/21/how-pandemic-accelerated-digital-transformation-in-advanced-economies).

Khalaf, Osamah Ibrahim, Munsif Sokiyna, Youseef Alotaibi, Abdulmajeed Alsufyani, dan Saleh Alghamdi. 2021. "Web attack detection using the input validationmethod: Dpda theory." *Computers, Materials and Continua* 68(3):3167–84. doi: 10.32604/cmc.2021.016099.

Kristanto, Titus, Mohammad Sholik, Dewi Rahmawati, dan Muhammad Nasrullah. 2019. "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ." *JISA(Jurnal Informatika dan Sains)* 2(2):30–33. doi: 10.31326/jisa.v2i2.497.

Microsoft. 2018. "Cybersecurity threats to cost organizations in Asia Pacific." Diambil 18 Juli 2023 (https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/).

OWASP Foundation. n.d.-a. "About the OWASP Foundation." Diambil 13 Desember 2022 (https://owasp.org/about/).

OWASP Foundation. n.d.-b. "OWASP Risk Rating Methodology." Diambil (https://owasp.org/www-community/OWASP_Risk_Rating_Methodology).

Surfshark. 2022. "Data breach monitoring - Surfshark." *Surfshark*. Diambil 14 November 2022 (https://surfshark.com/research/data-breach-monitoring).

TEMPO.CO (PT INFO MEDIA DIGITAL). 2021. "Data 279 Juta Penduduk RI Diduga Bocor dan Diperjualbelikan." Diambil 20 Desember 2022 (https://bisnis.tempo.co/read/1464175/data-279-juta-penduduk-ri-diduga-bocor-dan-diperjualbelikan-ini-tanggapan-bpjs).