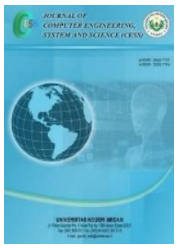
CESS e-ISSN: 2502-714x
(Journal of Computing Engineering, System and Science) 8(2) July 2023 518-528 p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess



Implementasi Penetration Testing Pada Website Menggunakan Metode Penetration Testing Execution Standard (PTES)

Implementation of Penetration Testing on the Website Using the Penetration Testing Execution Standard (PTES) Method

Bagus Kurniawan[1*], Ikhwan Ruslianto[2], Syamsul Bahri[3]

[1,2,3] Program Studi Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura
Jalan Prof. Dr. H. Hadari Nawawi Pontianak
email: [1]kurniawanbagus55@gmail.com, [2] ikhwanruslianto@siskom.untan.ac.id, [3]syamsul.bahri@siskom.untan.ac.id

A B S T R A K

Indonesia merupakan salah satu negara yang memiliki tingkat kejahatan siber yang sangat tinggi di dunia. Masalah tersebut timbul akibat sumber daya manusia yang kurang memadai dan kurangnya perawatan berkala pada sistem digital di Indonesia. Salah satu perawatan yang dapat dilakukan adalah *Penetration Testing* sebagai evaluasi sistem digital agar lebih baik dan terhindar dari serangan siber. Metode yang dapat membantu dalam melakukan *Penetration Testing* adalah dengan metode *Penetration Testing Execution Standard (PTES)*. Hasil yang didapatkan dari penelitian ini bahwa *website* https://k*****.go.id memiliki tiga belas kerentanan. Sehingga dari tiga belas kerentanan yang didapatkan dilakukan dengan tiga jenis serangan yang berbeda yaitu *Clickjacking, SQL Injection,* dan *Cross Site Scripting (XSS)*. Ketiga jenis serangan tersebut hanya serangan *Clickjacking* yang berhasil dilakukan pada *website* https://k*****.go.id. Diperoleh kesimpulan bahwa *website* memiliki risiko kerentanan dan terjadinya serangan bernilai sedang dilihat berdasarkan *OWASP ZAP Risk Rating Methodology*.

Kata Kunci: *Penetration Testing, Cyber Security, Clickjacking, SQL Injection, Cross Site Scripting (XSS), Website, Kerentanan.*

A B S T R A C T

Indonesia is a country that has a very high cybercrime rate in the world. This problem arises due to inadequate human resources and a lack of regular maintenance of digital systems in Indonesia. One of the treatments that can be done is Penetration Testing as an evaluation of digital systems to make them better and avoid cyber attacks. A method that can assist in

Penulis Korespondensi: Bagus Kurniawan
email: kurniawanbagus55@gmail.com

carrying out Penetration Testing is the Penetration Testing Execution Standard (PTES) method. The results obtained from this research are that the website https://k*****.go.id has thirteen vulnerabilities. So that the thirteen vulnerabilities found were carried out with three different types of attacks, namely Clickjacking, SQL Injection, and Cross Site Scripting (XSS). The only three types of attacks are clickjacking attacks that were successfully carried out on the https://k*****.go.id website. It is concluded that the website has a risk of vulnerability and the occurrence of attacks is worth being seen based on the OWASP ZAP Risk Rating Methodology.

Keywords: *Penetration Testing, Cyber Security, Clickjacking, SQL Injection, Cross Site Scripting (XSS), Website, Vulnerability.*

1. PENDAHULUAN

Lembaga Pemerintahan Indonesia yaitu Badan Penyelenggara Jaminan Sosial (BPJS) seperti yang dikutip pada portal berita CNN Indonesia menjelaskan rentetan kasus kebocoran data yang dialami oleh Badan Penyelenggara Jaminan Sosial (BPJS). Pada bulan Mei 2021 BPJS mengklaim 279 juta data penduduk Indonesia diperjualbelikan di forum *hacker*. Data tersebut mencangkup data kependudukan anggota Tentara Nasional Indonesia (TNI) dan Polisi Republik Indonesia (POLRI) terdiri dari data nama lengkap, Kartu Tanda Penduduk (KTP), nomor telepon, email, dan alamat [1].

Masalah tersebut timbul karena *website* Pemerintahan yang ada di Indonesia tidak memiliki parameter keamanan yang memadai hingga kurangnya *maintenance* dan jarang melakukan test keamanan pada *website*. Kurangnya Sumber Daya Manusia (SDM) di bidang *Cybersecurity* yang memiliki peranan penting dalam pengembangan *website* menjadi faktor lain terjadinya serangan siber. Untuk itu sangat perlu dipertimbangkan dan dipersiapkan guna mencegah terjadinya serangan hacker pada *website* [2]

Penelitian terkait tentang "Analisis Keamanan *Website* Menggunakan Metode *Penetration Testing Execution Standard (PTES)"*. Hasil dari penelitian tersebut dengan menggunakan metode *Penetration Testing Execution Standard (PTES)* dan mampu membantu sekolah dalam meningkatkan keamanan *website* SMKN 1 Cibatu dan mendapatkan rekomendasi perbaikan pada *website* [3].

Penelitian lainnya tentang "Analisis Perbandingan Metode Web Security PTES, ISSAF dan OWASP Di Dinas Komunikasi dan Informasi Kota Bandung". Hasil dari penelitian ini metode *Penetration Testing* yaitu *Penetration Testing Execution Standard (PTES)* dan *Open Web Application Security Project (OWASP)* dinilai tepat dalam melakukan *Penetration Testing* [4].

Solusi yang dapat dilakukan dari permasalahan diatas dengan melakukan *Penetration Testing* dengan metode *Penetration Testing Execution Standard (PTES)*. Penelitian yang dilakukan dengan judul "*Implementasi Penetration Testing Pada Website* https://k*****.go.id *Menggunakan Metode Penetration Testing Execution Standard (PTES)"*. Penelitian ini diharapkan dapat membantu dalam meminimalisir terjadinya serangan oleh *attacker* agar administrator suatu sistem dapat mengetahui kerentanan yang ada pada *website* sehingga dapat mengevaluasi dan meningkatkan *website* lebih baik dari sebelumnya.

2. DASAR/TINJAUAN TEORI

2.1. Penetration Testing

Penetration testing merupakan salah satu cara dalam melakukan pengujian terhadap keamanan *website*, kegiatan *penetration testing* lebih cenderung untuk memiliki suatu tujuan yang spesifik, misalnya seperti dapat tidaknya suatu target diambil alih. Banyak metode yang bisa dilakukan dalam melakukan *penetration testing* salah satunya yang dilakukan adalah metode *Penetration Testing Execution Standard (PTES)*. dalam metode ini diterapkan tujuh tahapan untuk mencari celah keamanan pada *website* Pemerintah yang saling berhubungan [5].

2.2. Penetration Testing Execution Standard (PTES)

Metode *Penetration Testing Execution Standard (PTES),* metode ini berisi uji penetrasi yang terdiri dari tujuh tahap yaitu tahap pra interaksi (*Pre-Engagement Interactions*), pengumpulan informasi (*Intelligence Gathering*), pemodelan ancaman (*Threat Modelling*), analisis kerawanan (*Vulnerability Analysis*), eksploitasi (*Exploitation*), pasca eksploitasi *(Post Exploitation*) dan pelaporan *(Reporting*) [6].

2.3. OWASP Risk Rating Methodology

OWASP Risk Rating Methodology adalah suatu metode untuk menilai risiko keamanan pada aplikasi web, yang dikembangkan oleh organisasi OWASP *(Open Web Application Security Project)*. *OWASP Risk Rating Methodology* membantu organisasi untuk mengevaluasi risiko keamanan pada aplikasi web dan menentukan tindakan mitigasi yang sesuai untuk mengurangi risiko [7]. Dalam penerapannya terbagi menjadi beberapa factor untuk mengukur tingkat risiko keamanan *website* yaitu *Threat Agent Factors, Vulnerability Factors,* dan *Technical Impact*.

Dalam melakukan penilaian resiko terdapat beberapa rumus dalam berdasarkan 3 faktor *Threat Agent Factors* pada persamaan 1*, Vulnerability Factors* pada persamaan 2*,* dan *Technical Impact* pada persamaan 3.

$$TA = \frac{Skill\ level+Motive+Opportunity+Size}{4} \quad (1)$$

$$Vuln = \frac{EoD+EoE+AW+ID}{4} \quad (2)$$

$$TI = \frac{Loc+LoI+LoA+LoAV}{4} \quad (3)$$

2.4. Determining the Severity of the Risk

Pada langkah ini dilakukan dengan mencari tahu apakah kemungkinannya rendah, sedang, atau tinggi. Skala 0 sampai 9 dibagi menjadi tiga bagian sesuai *standar OWASP Risk Rating Methodology* pada Tabel 1 [7]. Untuk menentukan nilai *Risk Value* dapat menggabungkan nilai dari *Likelihood* dan *Impact Levels* dengan klasifikasi pada Tabel 2 [7].

Tabel 1. Likelihood and Impact Levels

0 to <3	Rendah
3 to <6	Sedang
6 to 9	Tinggi

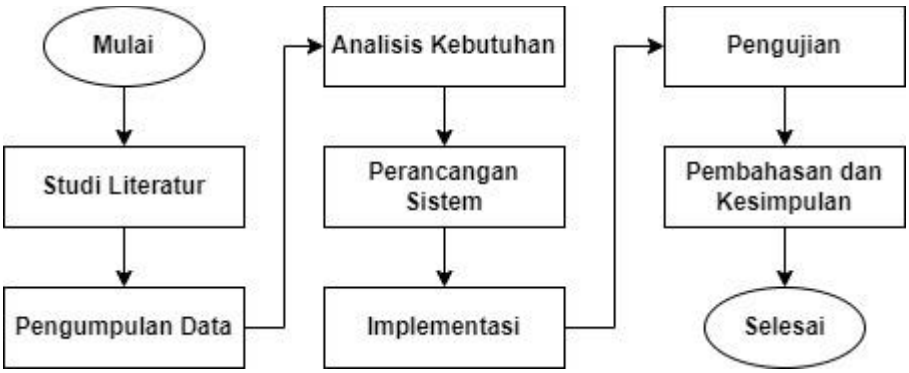
Tabel 2. Overall Risk Severity

Overall Risk Severity				
Impact	Tinggi Sedang Rendah	Sedang Rendah - Rendah	Tinggi Sedang Rendah Sedang	Kritikal Tinggi Sedang Tinggi
Likelihood				

3. METODE

3.1. Metode Penelitian

Penelitian ini dilakukan dengan beberapa tahapan metode penelitian yang dapat dilihat pada Gambar 1.



Gambar 1. Diagram Alir Metode Penelitian

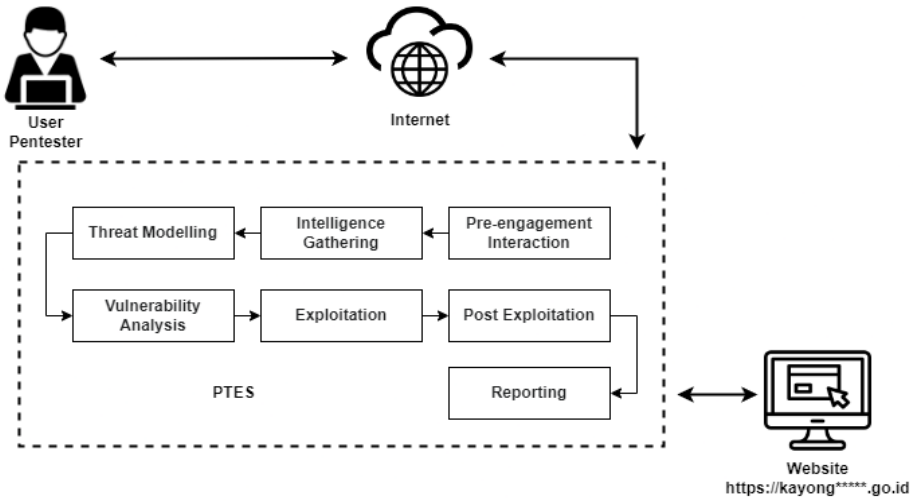
Keterangan:

1. Studi Literatur, pada tahapan ini mencari informasi berfokus terhadap topik *Penetration Testing* dengan metode *Penetration Testing Execution standard (PTES)* sehingga banyak ditemukan jurnal terkait dengan apa yang dinginkan.
2. Pengumpulan Data, pada tahapan ini dilakukan dengan dua metode pasif dan aktif pada website.
3. Analisis Kebutuhan, Analisis kebutuhan terbagi menjadi dua yaitu analisis kebutuhan perangkat keras dan analisis kebutuhan perangkat lunak.
4. Perancangan Sistem, Perancangan dimulai dengan merancang kegiatan *penetration testing* yang dilakukan.
5. Implementasi, melakukan implementasi tahapan *Penetration Testing Execution Standard (PTES)* pada *website* Pemerintah dengan menerapkan tujuh tahapan.
6. Pengujian, pengujian dilakukan untuk menilai keberhasilan dari perancangan sistem yang telah dibuat.
7. Pembahasan dan Kesimpulan, membahas hasil dari pengujian dan mendapatkan simpulan dari pengujian.

3.2. Gambaran Umum Sistem

Gambaran dimulai dari penguji melakukan implementasi tahapan *Penetration Testing Execution Standard (PTES)* pada *website* https://k*****.go.id dengan menerapkan tujuh tahapan. Pertama *Pre-engagement Interaction* tahap persiapan yang bertujuan untuk

menyepakati objek atau target *website*, kedua *Intelligence Gathering* tahapan mencari informasi terkait *website* https://k*****.go.id, ketiga *Threat Modeling* tahapan bertujuan untuk menentukan perlakuan terhadap *website,* keempat *Vulnerability Analysis* tahapan mulai mencari celah keamanan dengan menggunakan aplikasi owasp zap, kelima *Exploitation* tahapan melakukan pengujian serangan berdasarkan hasil dari celah keamanan *website,* keenam *Post Exploitation* perlakuan kepada *website* setelah dilakukan eksploitasi, *Reporting* tahapan terakhir untuk melaporkan hasil dari *penetration testing* kepada pihak dari *website* https://k*****.go.id. Pada Gambar 2 menunjukkan bagaimana mekanisme gambaran umum sistem.



Gambar 2. Gambaran Umum Sistem

4. HASIL DAN PEMBAHASAN

Penetration Testing yang dilakukan dengan metode *Penetration Testing Execution Standard (PTES).* Setiap tahapan berisikan implementasi yang dilakukan berdasarkan perancangan yang sudah dirancang sebelumnya. Implementasi menjelaskan cara atau teknis melakukan *Penetration Testing* sehingga didapatkan hasil.

4.1. Implementasi Pre-Engagement Interaction

Pada tahapan *Pre-Engagement Interaction* terdapat beberapa kegiatan yang dilakukan dalam melakukan *penetration testing*, sebelumnya dilakukan pembicaraan dan diskusi untuk mencapai kesepakatan yang merupakan tujuan dari tahapan awal ini. Hasil tersebut dapat dijelaskan pada Tabel 4.

Tabel 3. Kegiatan Pre-Engagement Interaction

No	Kegiatan	Status	Hasil
1	Identifikasi Lingkup	Terlaksana	Target *penetration testing website* Pemerintah dengan metode PTES
2	Menentukan tujuan penetration testing	Terlaksana	- Tujuan Premier: Melakukan *penetration testing* untuk menemukan kerentanan pada *website* Pemerintah. - Tujuan Sekunder: Objek penelitian yang dilakukan.

3	Menyusun ROE *(Roles Of Engagement)*	Terlaksana	- Penetration testing dilakukan diluar jam kerja agar tidak mengganggu kinerja *website* - Menyajikan hasil *penetration testing* dalam *soft file* maupun *hard file* - Lokasi: Indonesia
4	Mempermudah jalur komunikasi	Terlaksana	Komunikasi dengan administrator dari *website* Pemerintah

4.2. Implementasi Intelligence Gathering

Dalam mengimplementasikan tahapan *Intelligence Gathering* digunakan metode *Open Source Intelligence (OSINT)* yang terbagi menjadi dua buah metode pasif dan aktif. Pada metode pasif dimulai dengan melakukan pencarian informasi menggunakan *tools* Shodan. Metode kedua yang dilakukan adalah dengan metode aktif dengan menggunakan *tools* Nmap yang dijalankan pada sistem operasi Kali Linux, *scanning* pertama yang dilakukan adalah *Service Detection* (-sV). Untuk Hasil Intelligence Gathering dapat dilihat pada Tabel 5.

Tabel 4. Hasil Intelligence Gathering

Alamat URL *Website*	https://k*****.go.id
Alamat IP	103.***.***.**
Lokasi	Indonesia
Kota	Jakarta
Pemilik Layanan	Direktorat E-Government Kementerian KOMINFO
Penyedia ISP	Direktorat E-Government Kementerian KOMINFO
Autonomous System Number	AS132634
Tipe Server	nginx
Algoritma kunci publik	RSA
Daftar *port* terbuka	- 80/tcp: http; Imunify360 Webshield 1.18 firewall - 443/tcp: ssl/http; nginx - 53/tcp: domain; PowerDNS Autoritative Server 4.4.1 - 110/tcp: pop3; Dovecot pop3d - 465/tcp: ssl/smtp; Exim smtpd 4.95 - 993/tcp: imaps - 995/tcp: pop3s - 2000/tcp: cisco-sccp - 5060/tcp: sip - 8008/tcp: http

4.3. Implementasi Thread Modelling

Threat Modelling atau Pemodelan ancaman menggunakan model STRIDE dengan mengelompokkan jenis ancaman *menjadi S/spoofing, T/tampering, R/repudiation, I/information disclosure, D/ denial of service, E/elevation of privilege*. Pemodelan ancaman

dilakukan untuk acuan dalam melakukan eksploitasi. Pemodelan ancaman dapat dijabarkan pada poin berikut sesuai metode STRIDE.

1. *Spoofing*, serangan yang dilakukan dengan menggunakan proxychains agar IP yang digunakan untuk akses *website* bersifat random dan anonim. Proxychains dilakukan dengan memasukan perintah pada setiap menjalankan aplikasi nmap, sqlmap, dan OWASP ZAP.
2. *Tampering,* serangan dilakukan dengan teknik SQL Injection pada sistem *database*. Serangan SQL Injection menggunakan aplikasi sqlmap pada Kali Linux. Untuk menjalankan sqlmap dibutuhkan parameter URL yang mengarah ke *index database website*.
3. *Repudation,* serangan yang dilakukan dengan menggunakan proxychains agar IP yang digunakan untuk akses *website* bersifat *random* dan anonim. Proxychains dilakukan dengan memasukan perintah pada setiap menjalankan aplikasi nmap, sqlmap, dan OWASP ZAP.
4. *Information Disclosure,* serangan dilakukan dengan teknik SQL Injection pada sistem *database*. Serangan *SQL Injection* menggunakan aplikasi sqlmap pada Kali Linux. Untuk menjalankan sqlmap dibutuhkan parameter URL yang mengarah ke *index database website*.
5. *Denial of Service,* serangan dilakukan *port scanning* dengan Nmap, dan *vulnerability scanning* dengan OWASP ZAP. Aplikasi nmap akan mengirimkan paket SNY ke ribuan semua *port website* sehingga akan memperlambat kinerja *website.*
6. *Elevation of Privilege,* serangan yang akan dilakukan dengan teknik *Cross Site Scripting (XSS).* Memberikan inputan kode injeksi pada belakang URL agar melihat *respon* dari *website.*

4.4. Implementasi Vulnerability Analysis

Tahapan *Vulnerability Analysis* dilakukan dengan menggunakan aplikasi OWASP ZAP, hal yang dilakukan adalah dengan memasukkan URL *website* https://k*****.go.id pada kolom *attack* OWASP ZAP. Setelah dilakukan *scanning* didapatkan hasil menunjukkan bahwa *website* memiliki risiko kerentanan berdasarkan aplikasi OWASP ZAP yang ditunjukkan pada Tabel 6.

Tabel 5. Hasil Vulnerability Analysis

No	Kerentanan	Risiko
1	*Cloud Metadata Potentially Exposed*	Tinggi
2	*SQL Injection - Hypersonic SQL - Time Based*	Tinggi
3	*SQL Injection - SQLite*	Tinggi
4	*Content Security Policy (CSP) Header Not Set*	Sedang
5	*Missing Anti-clickjacking Header*	Sedang
6	*Absence of Anti-CSRF Tokens*	Sedang
7	*Hidden File Found*	Rendah
8	*Server Leaks Version Information via "Server" HTTP Response Header Field*	Rendah
9	*Strict-Transport-Security Header Not Set*	Rendah
10	*Cookie No HttpOnly Flag*	Rendah
11	*Cookie Without Secure Flag*	Rendah
12	*Cookie without SameSite Attribute*	Rendah
13	*X-Content-Type-Options Header Missing*	Rendah

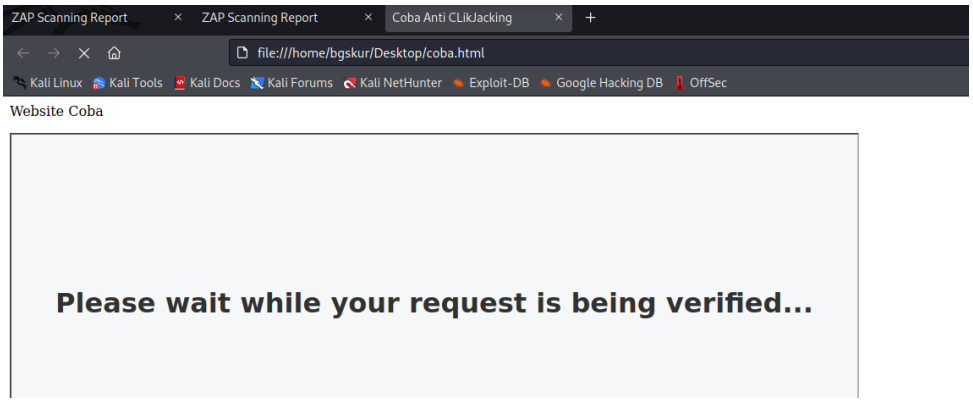
14	*User Agent Fuzzer*	Informasi
15	*Modern Web Application*	Informasi

4.5. Implementasi Exploitation

Setelah didapatkan kerentanan dari tahapan *Vulnerability Analysis*, untuk menguji apakah benar ada kerentanan pada *website* dilakukan tahapan selanjutnya yaitu *Exploitation*. Tetapi tidak semua serangan yang didapatkan dari hasil *scanning* bisa dilakukan eksploitasi karena ada beberapa kerentanan yang bersifat informasi dan beberapa faktor yang menyebabkan kerentanan tidak dapat di eksploitasi.

4.5.1. Clickjacking

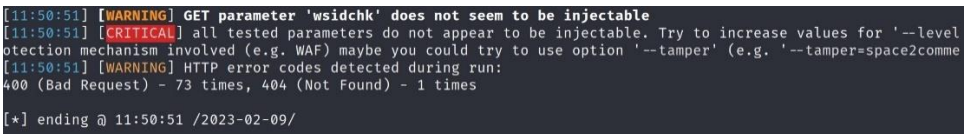
Serangan Clickjacking memanfaatkan kerentanan *Missing Anti-clickjacking Header.* Cara kerja Clickjacking adalah dengan menambahkan lapisan transparan pada halaman *website* sehingga pengguna lain tidak mengetahui apa yang telah dilakukan. Pada Gambar 2 menunjukkan hasil *website* https://k*****.go.id yang berhasil dibuka di halaman lain dengan serangan *Clickjacking.*



Gambar 3. Serangan Clickjacking

4.5.2. SQL Injection

Serangan SQL injection yang dilakukan memanfaatkan kerentanan *SQL Injection - Hypersonic SQL - Time Based* dan *SQL Injection – SQLite.* Cara kerja serangan *SQL Injection* dengan menyuntikkan kode program pada terhadap suatu celah keamanan. Serangan SQL tidak berhasil dilakukan karena parameter yang digunakan tidak bisa dibuka dan sesuai yang ada pada *website* https://k*****.go.id. Gambar 3 menunjukkan hasil serangan *SQL Injection* yang gagal dilakukan dengan *tool* SQLMap.

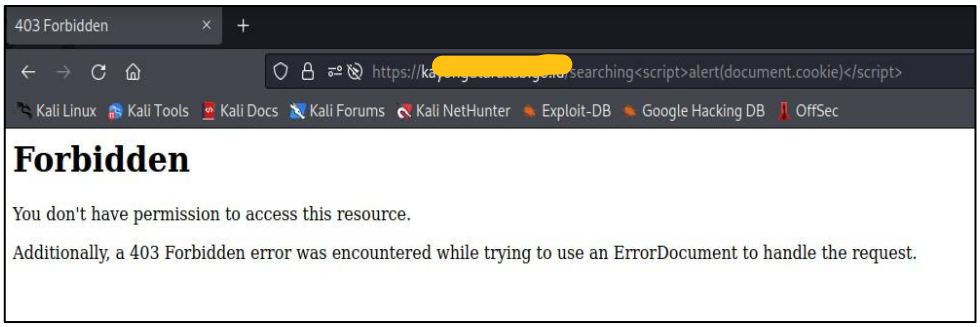


Gambar 4. Serangan SQL Injection

4.5.3. Cross Site Scripting

Serangan ini merupakan serangan dengan memanfaatkan kerentanan *Content Security Policy (CSP) Header Not Set,* cara kerja serangan dengan menyuntikkan kode berupa *JavaScript*

tujuan untuk mendapatkan *cookie* korban. Pada Gambar 4 Hasil yang didapatkan 403 *Forbidden* artinya *website* tidak mengizinkan dan memberi *respon* dari *request* yang diminta seperti.



Gambar 5. Serangan Cross Site Scripting (XSS)

4.6. Post Exploitation

Setelah dilakukan tahapan eksploitasi pada *website* https://k*****.go.id dengan memanfaatkan kerentanan kemudian tahapan selanjutnya adalah *Post Exploitation* atau setelah eksploitasi. Pada tahapan ini dilakukan penilai risiko berdasarkan *OWASP Risk Rating Methodology.* Pada metode tersebut dilihat berdasarkan ketiga faktor. Setiap faktor memiliki kriteria nilai masing-masing sesuai kerentanan *website* yang didapatkan, nilai kriteria bisa dilihat pada metode *OWASP Risk Rating Methodology.* Dari ketiga faktor tersebut maka didapatkan masing-masing nilai pada Tabel 7.

Tabel 6. Nilai Faktor OWASP Risk Rating Methodology

Threat Agent	Vulnerability	Technical Impact
4	4.51	3.76

Setelah didapatkan masing-masing dari nilai faktor kemudian dilakukan klasifikasi penilaian untuk mencari tahu apakah kemungkinannya rendah, sedang, atau tinggi dari kerentanan, Tabel 8 adalah hasil dari nilai nilai *Likelihood* didapatkan dari penjumlahan hasil nilai *Threat Agent* dan *Vulnerability Factor* kemudian dibagi 2 dan didapatkan nilai *Likelihood*. Nilai *Likelihood* digabungkan dengan nilai *Technical Impact* barulah mendapatkan nilai risiko kerentanan *website* https://k*****.go.id berdasarkan *OWASP Risk Rating Methodology*.

Tabel 7. Nilai Risiko Kerentanan

Nilai Likelihood	Nilai Technical Impact	Risiko
$4 + 4.51/2 = 4.255$ (Sedang)	3.76 (Sedang)	Sedang

Kemudian untuk nilai risiko serangan dilihat dari nilai faktor kemudian dilakukan klasifikasi penilaian untuk mencari tahu apakah kemungkinannya rendah, sedang, atau tinggi dari setiap masing-masing eksploitasi. Tabel 9 adalah hasil dari nilai *Likelihood* didapatkan dari penjumlahan hasil nilai *Threat Agent* dan *Vulnerability Factor* kemudian dibagi 2 dan didapatkan nilai *Likelihood*. Nilai *Likelihood* digabungkan dengan nilai *Technical Impact* barulah mendapatkan nilai risiko serangan *website* https://k*****.go.id.

Tabel 8. Nilai Risiko Serangan

Jenis Serangan	Nilai Likelihood	Nilai Technical Impact	Risiko
Clickjacking	4.5 (Sedang)	4.5 (Sedang)	Sedang
SQL Injection	3.625 (Sedang)	2.75 (Rendah)	Rendah
Cross Site Scripting	3.625 (Sedang)	2.75 (Rendah)	Rendah

4.7. Implementasi Reporting

Tahapan *Reporting* atau pelaporan disajikan menjadi dua bentuk laporan yaitu *executive summary* dan laporan teknis. Dalam *executive summary* terbagi menjadi beberapa bagian latar belakang dan tujuan, temuan umum, profil risiko, dan rekomendasi. Sedangkan untuk laporan teknis memuat lingkup uji penetrasi, teknik pengumpulan informasi, teknik analisis kerawanan, dan teknis eksploitasi. Laporan tersebut akan diserahkan kepada pihak *website* https://k*****.go.id.

4.8. Pembahasan

Setelah dilakukan pengimplementasian metode *penetration testing* dengan menggunakan metode *Penetration Testing Execution Standard (PTES)* dari setiap tahapan memiliki hasil masing-masing yang saling berhubungan, hasil yang didapatkan *website* https://k*****.go.id memiliki 13 kerentanan berdasarkan hasil dari *Vulnerability Analysis* pada Tabel 9.

Tabel 9. Hasil Kerentanan

No	Kerentanan	Risiko
1	*Cloud Metadata Potentially Exposed*	Tinggi
2	*SQL Injection - Hypersonic SQL - Time Based*	Tinggi
3	*SQL Injection - SQLite*	Tinggi
4	*Content Security Policy (CSP) Header Not Set*	Sedang
5	*Missing Anti-clickjacking Header*	Sedang
6	*Absence of Anti-CSRF Tokens*	Sedang
7	*Hidden File Found*	Rendah
8	*Server Leaks Version Information via "Server" HTTP Response Header Field*	Rendah
9	*Strict-Transport-Security Header Not Set*	Rendah
10	*Cookie No HttpOnly Flag*	Rendah
11	*Cookie Without Secure Flag*	Rendah
12	*Cookie without SameSite Attribute*	Rendah
13	*X-Content-Type-Options Header Missing*	Rendah
14	*User Agent Fuzzer*	Informasi
15	*Modern Web Application*	Informasi

Ketiga belas kerentanan tersebut termasuk kategori risiko sedang yang dinilai oleh laporan dari aplikasi OWASP ZAP. Setelah didapatkan kerentanan serangan yang dilakukan terhadap *website* https://k*****.go.id terbagi menjadi 3 serangan yaitu *Clickjacking, SQL Injection,* dan *Cross Site Scripting (XSS).* Untuk serangan *Clickjacking* memiliki nilai risiko sedang, serangan *SQL Injection* bernilai rendah, dan serangan *Cross Site Scripting (XSS)* bernilai rendah dihitung berdasarkan *OWASP Risk Rating Methodology*.

Tabel 10. Nilai Resiko Serangan

Jenis Serangan	Nilai Likelihood	Nilai Technical Impact	Risiko
Clickjacking	4.5 (Sedang)	4.5 (Sedang)	Sedang
SQL Injection	3.625 (Sedang)	2.75 (Rendah)	Rendah
Cross Site Scripting	3.625 (Sedang)	2.75 (Rendah)	Rendah

5. KESIMPULAN

Website https://k*****.go.id memiliki 13 kerentanan yang ditemukan, nilai *Likelihood* adalah 4.255 kategori sedang didapatkan dari nilai *Threat Agent Factor* dan *Vulnerability Factor*, untuk nilai Technical Impact adalah 3.76 kategori sedang, nilai didapatkan dari *OWASP Risk Rating Methodology* sehingga tingkat risiko *website* https://k*****.go.id bernilai sedang dilihat dari standar Open World Application Standard Project (OWASP). Pada *website* https://k*****.go.id serangan Clickjacking memiliki nilai *Likelihood* 4.5 kategori sedang dan nilai *Technical Impact* 4.5 artinya risiko dari serangan *Clickjacking* adalah sedang. Serangan *SQL Injection* nilai *Likelihood* 3.625 kategori sedang dan nilai *Technical Impact* 2.75 artinya risiko dari serangan *SQL Injection* adalah rendah. Serangan *Cross Site Scripting (XSS)* nilai *Likelihood* 3.625 kategori sedang dan nilai *Technical Impact* 2.75 artinya risiko dari serangan *Cross Site Scripting (XSS)* adalah rendah sehingga ditemukan nilai resiko yang berfungsi dalam membantu mitigasi dalam perbaikan *website* yang diserang.

REFERENSI

[1] "CNN Indonesia," "Rentetan Kasus Dugaan Kebocoran Data Kesehatan Pemerintah Baca artikel CNN Indonesia "Rentetan Kasus Dugaan Kebocoran Data Kesehatan Pemerintah," 3 September 2021. https://www.cnnindonesia.com/teknologi/20210903142047-185-689370/rentetan-kasus-dugaan-kebocoran-data-kesehatan-pemerintah/2 (diakses 3 Oktober 2022).

[2] Kominfo, "Indonesia kekurangan Bakat Cyber Security," 27 Desember 2016. https://www.kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media (diakses 4 Juni 2023).

[3] S. Utoro *dkk.*, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," 2020.

[4] T. Revolino Syarif dan D. Andri Jatmiko, "Analisis Perbandingan Metode Web Security PTES, ISSAF dan Owasp di Dinas Komunikasi Dan Informasi Kota Bandung," 2019.

[5] A. Arbi, "Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web Menggunakan Standar OWASP 10 pada domain Web Perusahaan," Nov 2020.

[6] S. U. Sunaringtyas, D. Surya Prayoga, J. K. Siber, P. Siber, dan S. Negara, "Edu Komputika Journal Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On," 2021. [Daring]. Tersedia pada: http://journal.unnes.ac.id/sju/index.php/edukom

[7] ZAP Dev Team, "OWASP Risk Rating Methodology," 2023.