Pengujian Fungsionalitas dan Celah Keamanan *Website* Kampoeng Sinaoe Menggunakan *Equivalence Partition*, *Boundary Value Analysis*, *Fuzzing*, dan *Penetration Testing*

Fakhrul Alamuddin Al Zulfi[1], Dwi Fatrianto Suyatno[2]

[1,2] Sistem Informasi, Fakultas Teknik, Universitas Negeri Surabaya
[1]fakhrul.19021@mhs.unesa.ac.id
[2]dwifatrianto@unesa.ac.id

***Abstrak*— Pengujian perangkat lunak merupakan sebuah tahapan yang digunakan untuk menjamin kualitas suatu sistem dan berguna untuk mengetahui serta menemukan kesalahan-kesalahan yang terjadi setelah tahap pengembangan. Seringkali pengujian yang dilakukan untuk mengetahui kualitas sebuah sistem khususnya *website* adalah dengan menguji secara fungsionalitas dan keamanan. Menurut staf pengelola *website* Kampoeng Sinaoe, saat melakukan pembuatan *website*, hanya dilakukan pengujian sederhana menggunakan metode Black Box yakni mengamati validitas dari nilai masukan dan hasil keluaran (*Equivalence Partitioning*). *Website* tersebut juga pernah mengalami kendala pada sisi keamanan yaitu pembobolan halaman *login* admin. Hal tersebut tentunya sangat mengkhawatirkan dan dapat menyebabkan kerugian apabila data yang ada di dalam halaman admin tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab. Dalam melakukan upaya preventif sehingga tidak terjadi hal serupa pada *website* Kampoeng Sinaoe, peneliti akan melakukan pengujian fungsionalitas dan keamanan pada website tersebut menggunakan *Equivalence Partition*, *Boundary Value Analysis*, *Fuzzing*, dan *Penetration Testing*. Penelitian yang dilakukan bertujuan untuk mengetahui kualitas website dari sisi fungsionalitas dan celah keamanan. Jenis penelitian ini menggunakan pendekatan kualitatif. Penelitian kualitatif ini dijadikan landasan awal bagi peneliti untuk mengetahui bagaimana kualitas *website* Kampoeng Sinaoe. Sumber data yang didapatkan dalam penelitian ini menggunakan metode wawancara, observasi, dan studi literatur. Pelaksanaan pengujian diawali dengan menguji website dari sisi fungsionalitas dengan tahapan pembuatan daftar fitur, nilai pengujian, dan *test case*. Kemudian, dilanjut menguji *website* dari sisi keamanan dengan tahapan *pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post exploitation,* dan *reporting*. Berdasarkan kedua pengujian tersebut *website* Kampoeng Sinaoe memiliki kualitas yang kurang baik dari sisi fungsionalitas dan keamanan.**

Kata Kunci*— website, equivalence partition, boundary value analysis, fuzzing, penetration testing.

I. PENDAHULUAN

Pengujian merupakan tahapan yang sangat penting untuk menjamin kualitas suatu sistem dan juga berguna untuk mengetahui dan menemukan kesalahan-kesalahan yang terjadi setelah proses *development* dilakukan. Dengan begitu, seorang *tester/quality assurance* dapat mengetahui apakah perangkat lunak yang telah dibangun atau sedang dikembangkan sudah memenuhi kriteria dan kebutuhan pengguna [1].

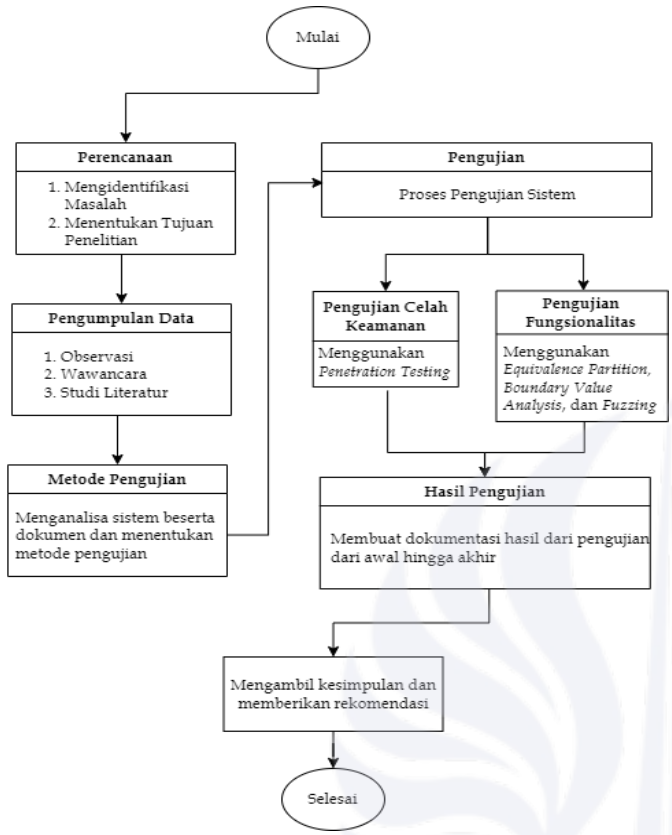
Tahapan pengujian memiliki tiga metode yang sering digunakan untuk menguji sebuah sistem, yaitu metode *white box, black box, grey box* [2]. Ketiga metode tersebut memiliki karakteristiknya masing-masing, yakni metode *white box* membutuhkan struktur internal dari sistem untuk melakukan pengujian. Lalu, metode *black box* tidak membutuhkan struktur internal dari sistem. Sedangkan metode *grey box* merupakan gabungan dari kedua metode sebelumnya yaitu *white box* dan *black box* [1]. *Black box* merupakan metode yang digunakan untuk menguji sebuah sistem yang mengacu pada sisi fungsionalitas, sehingga seorang penguji dapat mendeskripsikan bagaimana kondisi masukan dan melakukan pengujian tanpa harus mengetahui struktur internal [3]. Metode *black box* memiliki beberapa teknik pengujian yaitu *Equivalence Partition, Boundary Value Analysis, Fuzzing, Cause-Effect, Orthogonal Array Testing, All Pair Testing*, dan *State Transition* [1]. Lalu, *Penetration Testing* (Pentest) merupakan simulasi serangan *cyber* terhadap sistem untuk memeriksa kerentanan yang dapat dieksploitasi [4]. Pentest memiliki tiga teknik pengujian, yaitu *Blind Disclosure, Full Disclosure*, dan *Partial Disclosure*. Pentest memiliki kerangka kerja bernama *Penetration Testing Execution Standard* (PTES) yang dikembangkan oleh Pentest Organization, digunakan sebagai standar dalam melakukan analisis dan audit keamanan sistem [5].

Kampoeng Sinaoe merupakan Lembaga Bimbingan Belajar (LBB) yang memiliki 34 karyawan dan 250 murid, bertempat di Jalan KH. Khamdani 1, Jl. Raya Siwalanpanji No.25, Kecamatan Buduran, Kabupaten Sidoarjo. Kampoeng Sinaoe menggunakan *platform* berbasis *website* yang memiliki alamat tautan https://kampoengsinaoe.org untuk melakukan manajemen terhadap proses administrasi dan pengumpulan informasi. Menurut staf pengelola *website* Kampoeng Sinaoe, saat melakukan pembuatan *website*, hanya dilakukan pengujian sederhana menggunakan metode *Black Box* yakni mengamati validitas dari nilai masukan dan hasil keluaran (*Equivalence Partitioning*). *Website* tersebut juga pernah mengalami kendala pada sisi keamanan yaitu pembobolan halaman *login admin*. Hal tersebut tentunya sangat mengkhawatirkan dan dapat menyebabkan kerugian apabila data yang ada di dalam halaman admin tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab.

Dalam melakukan upaya preventif sehingga tidak terjadi hal serupa pada *website* Kampoeng Sinaoe, peneliti akan melakukan pengujian fungsionalitas dan keamanan pada *website* tersebut menggunakan *Equivalence Partition, Boundary Value Analysis, Fuzzing*, dan *Penetration Testing*. Pengujian tersebut bertujuan untuk mengetahui bagaimana kualitas *website* Kampoeng Sinaoe berdasarkan aspek fungsionalitas dan keamanannya.

II. METODE PENELITIAN

A. Alur Penelitian



Gbr. 1 Alur Penelitian

Berikut merupakan penjelasan mengenai alur penelitian diatas:

1) Perencanaan: Pada tahap ini peneliti melakukan identifikasi permasalahan dengan melakukan wawancara kepada staf pengelola *website* tentang insiden kebobolan. Lalu, menentukan tujuan penelitian berdasarkan identifikasi masalah tersebut.

2) *Pengumpulan Data:* Penelitian terhadap website Kampoeng Sinaoe berlangsung selama bebapa bulan, yakni mulai dari bulan Februari 2023 hingga bulan Juni 2023 dan bertempat di Jl. KH Khamdani I No. 25 Siwalanpanji, Kecamatan Buduran, Kabupaten Sidoarjo, Jawa Timur. Peneliti melakukan berbagai cara untuk mendapatkan informasi dan data yang relevan dengan objek penelitian, diantaranya adalah melakukan wawancara kepada admin pengelola *website*, melakukan observasi dengan mengamati *website*, dan mencari literatur dari sumber yang relevan. Hasil dari tahapan tersebut adalah didapatkannya informasi yang sesuai dengan keinginan peneliti.

3) Metode Pengujian: Berdasarkan hasil dari wawancara pada tahapan pengumpulan data, pihak Kampoeng Sinaoe menyatakan bahwa peneliti tidak diberikan akses *source code* dengan alasan agar keamanan tetap terjaga. Oleh karena itu, peneliti memutuskan untuk menggunakan metode *Black Box Testing* dan *Penetration Testing* sebagai metode pengujian, yang mana kedua teknik tersebut tidak membutuhkan akses ke *source code* dan konfigurasi untuk melakukan pengujiannya.

4) Pengujian: Merupakan tahapan atau proses pengujian berdasarkan aspek fungsionalitas dan keamanan yang dijabarkan pada bab II.B.

5) Hasil Pengujian: Pada tahapan ini peneliti mendokumentasikan hasil dari pengujian dari tahap awal hingga tahap akhir ke dalam bentuk laporan. Laporan tersebut diberi nama Laporan_Pengujian Fungsionalitas dan Keamanan_Kampoeng Sinaoe.

6) Mengambil Kesimpulan dan Memberikan Rekomendasi: Pada tahapan ini peneliti menganalisis, menarik kesimpulan, dan memberikan rekomendasi terhadap hasil pengujian yang telah dilakukan.

B. Proses Pengujian

Pada pengujian fungsionalitas, peneliti membuat *test case* yang berisi fitur *website* yang akan diuji dan nilai yang digunakan sebagai masukan ke dalam sistem. Berikut merupakan daftar fitur *website* yang akan digunakan sebagai objek dalam melakukan pengujian.

TABEL I
DAFTAR FITUR YANG AKAN DIUJI

No	Fitur	Kolom
1.	Manajemen Akun Admin	Nama, Username, Ganti Password
2.	Manajemen Profil Lembaga	NSM, NPSN, Nama Sekolah, Alamat, Provinsi, Kabupaten, Kecamatan, Nomor Telepon, Email, Nama Kepala Sekolah
3.	Data Pendaftar	NIK, Nama, Password, Nomor Telepon
4.	Data Master Sekolah	NPSN, Nama, Alamat
5.	Data Master Jurusan	Kode Jurusan, Nama Jurusan, Kuota
6.	Data Master Jenis Daftar	Kode Jenis, Nama Jenis
7.	Pengaturan Aplikasi	Nama Sekolah, NSM/NSS Sekolah, NPSN Sekolah
8.	Pengaturan Live Chat	Text Klik Daftar, Text Live Chat, Nomor WA Live Chat
9.	Pencarian Berita	Search
10.	Login	Username, Password

No	Fitur	Kolom
11.	Register	Nama Lengkap, Tempat Lahir, Nomor Telepon, Password, Refresh Kode
12.	Register Kontributor	Username, Password, Nama Lengkap, Email, No Telepon, Kode Keamanan

Peneliti menggunakan pengujian secara manual untuk melakukan pengujian menggunakan nilai yang berasal dari ketentuan *Boundary Value Analysis* (BVA) dan *Fuzzing* (SQLi dan XSS). Cara kerja dari pengujian manual adalah dengan memasukkan secara manual nilai yang telah ditentukan ke masing-masing kolom dari fitur yang akan diuji. Berikut merupakan tahapan yang digunakan dalam penyusunan *test case* [6].

1) *Tahap 1:* Menentukan *identifier* dan membuat deskripsi kasus uji sederhana yang berisi fitur dan penjelasan kasus uji.
2) *Tahap 2:* Memberikan data uji pada masing-masing *test case*.
3) *Tahap 3:* Membuat tindakan tertentu dan menentukan tipe partisi pada masing-masing *test case*. Terdapat penambahan kolom partisi yang berisi valid atau tidak valid, karena peneliti mengimplementasikan metode *Equivalence Partition* pada masing-masing *test case*.
4) *Tahap 4:* Menentukan hasil yang diharapkan pada masing-masing *test case* sesuai dengan ketentuan dokumen, menentukan hasil aktual pengujian, serta mengambil kesimpulan pada hasil pengujian.

Kemudian pada pengujian celah keamanan, peneliti membuat tabel pada masing-masing tahapan yang memiliki kolom deskripsi, dampak, URL/*endpoint*, *severity*, rekomendasi/solusi, dan validasi [7]. Peneliti menerapkan tahapan sistematis dari kerangka kerja *Penetration Testing Execution Standard* (PTES), yang memiliki tujuh tahapan. Berikut merupakan tahapan yang dilakukan oleh peneliti [8].

1) *Pre-engagement Interactions:* Peneliti melakukan persiapan alat dan teknik yang digunakan dalam pengujian. Alat yang digunakan oleh peneliti untuk mengumpulkan informasi adalah Nmap, Whois, Nslookup, Wappalyzer, dan OWASP ZAP.
2) *Intelligence Gathering:* Peneliti melakukan pengumpulan informasi (*gathering informations*) terhadap *website* dengan melakukan analisis menggunakan berbagai macam alat yang telah dijelaskan pada tahapan *Pre-engagement Interactions*.
3) *Threat Modeling:* Setelah mengumpulkan informasi dari *website*, selanjutnya peneliti akan membuat pemodelan untuk memudahkan peneliti dan instansi dalam memahami kerentanan. Pemodelan tersebut adalah dengan menganalisis aset/komponen dan mengidentifikasi ancaman.
4) *Vulnerability Analysis:* Setelah menemukan berbagai macam kerentanan, peneliti melakukan validasi pada setiap temuan tersebut dengan menginjeksi celah keamanan secara manual pada *website*. Hal tersebut bertujuan untuk memastikan kerentanan yang ditemukan. Jika celah keamanan tersebut memberikan *response* yang tidak semestinya, maka celah keamanan tersebut bersifat positif (rentan).
5) *Exploitation:* Setelah memvalidasi temuan kerentanan, peneliti akan memposisikan diri sebagai penyerang (*attacker*) untuk melakukan eksekusi pada setiap kerentanan bersifat Valid. Alat yang digunakan pada tahapan ini adalah Burpsuite dan SQLmap.
6) *Post-Exploitation:* Setelah melakukan eksekusi terhadap kerentanan, peneliti akan mengumpulkan hasil dari eksekusi tersebut dengan mengelompokkan berdasarkan sensitivitas data yang didapatkan. Pengelompokan tersebut menggunakan standar *Common Vulnerability Scoring System* (CVSS). CVSS merupakan sebuah standar industri yang bersifat *open-source* untuk melakukan penilaian tingkat *severity* dari celah keamanan sistem yang ditemukan. Kemudian, pengelompokan tersebut dibagi menjadi empat, yaitu *low*, *medium*, *high*, dan *critical [9]*.
7) *Reporting:* Pada tahapan ini peneliti akan membuat laporan berbentuk dokumen yang berisi tentang pengujian mulai dari tahap awal hingga akhir.

III. HASIL PENELITIAN DAN PEMBAHASAN

A. Pengujian Fungsionalitas

Pengujian fungsionalitas dilakukan dengan mengikuti skenario dan data uji yang telah dibuat pada *test case*. Hasil dari pengujian lainnya akan ditampilkan pada kolom Lulus/Gagal dengan penilaian berdasarkan kesesuaian antara hasil yang diharapkan dengan hasil pengujian. Jika hasil yang diharapkan sesuai dengan hasil pengujian, maka disimpulkan sebagai lulus. Lalu, jika hasil yang diharapkan tidak sesuai dengan hasil yang diharapkan, maka disimpulkan sebagai gagal. Total dari keseluruhan pengujian pada *test case* adalah 69 butir uji. Berikut merupakan beberapa butir uji hasil pengujian fungsionalitas.

TABEL II
HASIL PENGUJIAN FUNGSIONALITAS

ID	DESKRIPSI	LANGKAH-LANGKAH	LULUS/ GAGAL
TC-F-01	Pengujian form Login Admin	Mengisi username dan password (EP)	Lulus
TC-F-02		Hanya mengisi username (EP)	Lulus
TC-F-03		Mengisi username dan password (BVA)	Lulus
TC-F-04		Mengisi username dan password menggunakan format SQLi (Fuzzing)	Lulus
TC-F-05	Pengujian form Login User	Mengisi nisn dan password (EP)	Lulus
TC-F-06		Hanya mengisi kolom nisn (EP)	Gagal
TC-F-07		Mengisi kolom dengan format SQLi (Fuzzing)	Lulus
TC-F-08		Mengisi NISN (BVA)	Lulus

B. *Pengujian Celah Keamanan*

1) *Pre-engagement Interactions:* Peneliti melakukan instalasi perangkat lunak yang digunakan sebagai alat untuk mengumpulkan informasi, seperti Nmap, Whois, Nslookup, Wappalyzer, dan OWASP ZAP.

TABEL III
DAFTAR KOMPONEN KEBUTUHAN PENGUJIAN

NAMA KOMPONEN	INFORMASI	
Spesfikasi Perangkat Keras	Processor	Intel Core I3-5005U
	RAM	12 GB
	Hard Disk	500 GB
	OS	Linux Mint 20 (*base* Ubuntu 20.04)
	Arsitektur OS	64-bit
Spesifikasi Perangkat Lunak	Alat Scanning	OWASP ZAP
		Nmap
		Whois
		Nslookup
		Wappalyzer
		Wafw00f
	Alat Eksploitasi	Burp Suite
		SQLMap

2) *Intelligence Gathering:* Tahap awal yang dilakukan peneliti pada tahapan *intelligence gathering* adalah melakukan penggalian informasi menggunakan perintah "nslookup kampoengsinaoe.org" untuk memetakan nama *domain* menjadi alamat IP atau sebaliknya. Didapatkan IP *address* 103.152.242.2 pada *domain* kampoengsinaoe.org.

```
→  ~ nslookup kampoengsinaoe.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   kampoengsinaoe.org
Address: 103.152.242.2
```

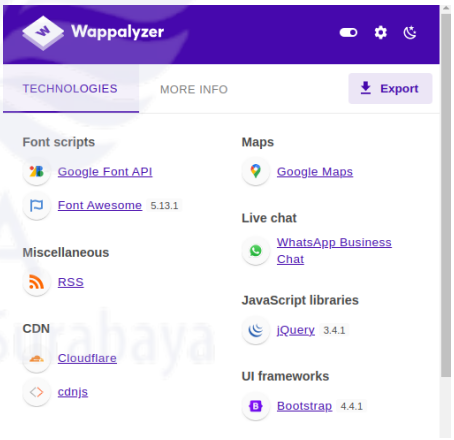
Gbr. 2 Mendapatkan IP *address* melalui NSLOOKUP

Kemudian, IP tersebut digunakan pada perintah whois "whois 103.152.242.2" untuk mendapatkan informasi tentang nama *server*, tanggal pembuatan, tanggal kadaluarsa, informasi registrasi pemilik domain, informasi kontak teknis, informasi kontak administratif, dan informasi kontak keamanan. Didapatkan informasi bahwa *website* tersebut menggunakan *hosting* dewaweb.com.

```
→  ~ whois 103.152.242.2
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '103.152.242.0 - 103.152.243.255'

% Abuse contact for '103.152.242.0 - 103.152.243.255' is 'abuse@dewaweb.com'

inetnum:        103.152.242.0 - 103.152.243.255
netname:        IDNIC-ALAMJAYA-ID
descr:          Yayasan Alam Jaya Sakti
descr:          Corporate / Direct Member IDNIC
descr:          DEWAWEB
descr:          AKR Tower - 16th Floor
descr:          Jl. Panjang no. 5, Kebon Jeruk
descr:          Jakarta Barat 11530
descr:          Jakarta 12870
country:        ID
admin-c:        EB151-AP
tech-c:         EB151-AP
abuse-c:        AA1727-AP
status:         ASSIGNED PORTABLE
mnt-by:         MNT-APJII-ID
mnt-routes:     MAINT-ID-PTAMI
mnt-irt:        IRT-ALAM-JAYA-ID
last-modified:  2020-07-17T12:55:16Z
source:         APNIC
```

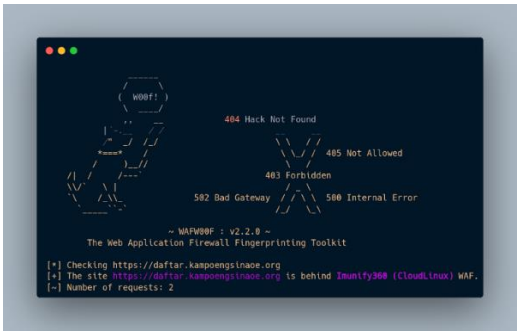
Gbr. 3 Mendapatkan informasi IP *Address*

Ketika *website* Kampoeng Sinaoe dianalisis menggunakan Wappalyzer, ditemukan teknologi Cloudflare yang berperan sebagai *web application firewall* (WAF). Hal tersebut menunjukkan bahwa IP *address* yang didapatkan oleh perintah nslookup sebelumnya adalah IP dari *firewall*.



Gbr. 4 Mendapatkan informasi *firewall* melalui Wappalyzer

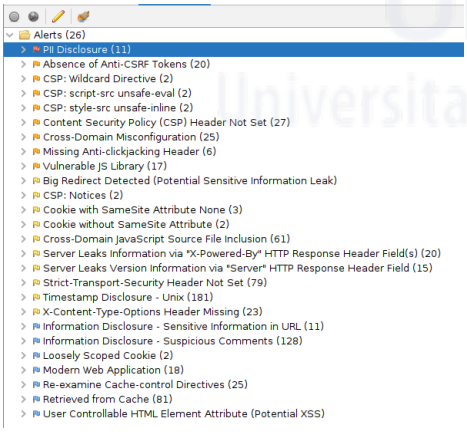
Peneliti ingin mendapatkan informasi lebih lanjut tentang tipe WAF yang digunakan oleh *website* dengan menggunakan Wafw00f. Wafw00f merupakan sebuah alat berlisensi *open source* yang digunakan untuk mendeteksi jenis *firewall*/WAF. Berikut hasil dari analisis menggunakan Wafw00f.



Gbr. 5 Mendapatkan informasi jenis WAF

Hasil dari pengujian tersebut adalah *website* Kampoeng Sinaoe menggunakan WAF Imunify360. Imunify360 merupakan sebuah WAF yang memiliki beberapa fitur utama, yaitu *malware detection* untuk mendeteksi adanya *malware* dan IPS/IDS untuk mendeteksi serta melakukan pencegahan ketika terjadi serangan dari luar. Dengan adanya proteksi dari WAF yang berasal dari Imunify360 tersebut, ketika peneliti melakukan simulasi penyerangan pada *website* Kampoeng Sinaoe, IP *address* yang berasal dari laptop peneliti diblokir oleh *server* dikarenakan terindikasi sedang melakukan penyerangan. Oleh karena itu, peneliti mengalami kesulitan dalam melanjutkan pengujian terkait celah keamanan. Setelah berkonsultasi dengan pihak Kampoeng Sinaoe, peneliti diberikan izin untuk mengakses *website* melalui server lokal dengan alamat http://localhost:8080 untuk *website* pendaftaran dan http://localhost:8081 untuk *website landing page*, dengan tujuan agar pengujian tidak terhambat oleh WAF Imunify360 yang terpasang pada *website server*.

Peneliti juga melakukan *scanning* celah keamanan menggunakan alat OWASP ZAP agar lebih efisien dan akurat. Berikut merupakan hasil dari *scanning* menggunakan alat OWASP ZAP pada alamat http://localhost:8080.



Gbr. 6 Hasil *scanning* menggunakan OWASP ZAP

Hasil dari *scanning* menggunakan alat OWASP ZAP adalah ditemukannya sebanyak 26 peringatan dengan berbagai macam tingkatan. Tingkatan tersebut dikategorikan dengan warna bendera yang berada pada sebelah kiri dengan penjelasan warna merah berarti *high*, warna *orange* berarti *medium*, warna kuning berarti *low*, dan warna biru berarti *information*.

Kemudian, peneliti melakukan analisis celah keamanan menggunakan cara manual, yakni dengan mencoba satu per satu pada setiap menu *website*. Temuan celah keamanan yang berjenis *information* tidak akan dilakukan pengujian lebih lanjut karena celah tersebut hanya bersifat informasi dan dapat ditanggulangi dengan cara menyembunyikan informasi tersebut. Hasil dari analisis celah keamanan secara manual adalah didapatkan sebanyak 9 dugaan celah keamanan.

3) *Threat Modelling:* Pada tahapan ini peneliti membuat pemodelan dari pengujian yang akan dilakukan agar memudahkan peneliti dan instansi dalam memahami kerentanan yang akan ditemukan pada pengujian ini. Berikut merupakan hasil dari tahapan pembuatan model perencanaan.

TABEL IV
HASIL THREAT MODELLING

NO.	NAMA ASET	POTENSI ANCAMAN	TINGKAT RISIKO
1.	*Website*	*Cross-Site Scripting*	Sedang
		CSRF Attack	Sedang
		Broken Authentication	Tinggi
		Takeover Account	Tinggi
		Brute Force	Rendah
		Distributed Denial of Service (DDoS)	Rendah
2.	Basis Data	*SQL Injection*	Sedang

4) *Vulnerability Analysis:* Setelah melakukan tahap perencanaan untuk melakukan penyerangan atau *threat modelling* pada celah keamanan yang telah ditemukan, tahap selanjutnya adalah melakukan validasi untuk mengetahui apakah setiap celah keamanan yang telah ditemukan tersebut bersifat positif (rentan) atau negatif (tidak rentan) menggunakan cara manual. Berikut merupakan beberapa hasil dari validasi tersebut.

TABEL V
HASIL *VULNERABILITY ANALYSIS*

NO.	DESKRIPSI	VALIDASI
1.	Big Redirect Detected, Server memberikan response yang berisi body-content, sehingga diduga bahwa body-content memiliki informasi yang sensitif	Tidak Valid
2.	CSP: Notices, Tidak ada konfigurasi CSP pada security layer untuk memproteksi adanya serangan XSS dan Data Injection	Valid

5) *Exploitation:* Setelah melakukan validasi terhadap celah keamanan yang telah ditemukan dan mengetahui celah

keamanan apa saja yang memiliki kerentanan, langkah selanjutnya adalah melakukan penyerangan atau tahap *Exploitation*.

Pada tahapan ini, peneliti melakukan penyerangan menggunakan bantuan alat/secara otomatis dan menggunakan cara manual. Alat yang digunakan untuk melakukan penyerangan adalah Burpsuite, SQLmap, dan CURL. Sedangkan untuk cara manual, peneliti melakukan penyerangan dengan cara langsung menginjeksi kerentanan melalui *inspect element*, *console browser*, dan kolom *input*. Berikut merupakan beberapa hasil dari tahapan *Exploitation* beserta dampak dan skenario penyerangan.

TABEL VI
HASIL *EXPLOITATION*

NO.	DESKRIPSI	SKENARIO	DAMPAK
1.	CSP: Notices, Tidak ada konfigurasi CSP pada security layer untuk memproteksi adanya serangan XSS dan Data Injection	1. Ketika melakukan CURL ke domain website 2. Beberapa halaman tidak memiliki konfigurasi CSP	Dapat menimbulkan bocornya informasi sensitif melalui celah XSS
5.	CSP: script-src unsafe-eval, Terdapat konfigurasi unsave-eval pada CSP	1. Melakukan injeksi script XSS yang berisi "$('body').html(' <script> alert('executed')</script>') " melalui inspect element pada tab Console 2. Maka command tersebut akan dieksekusi pada tag body di halaman website Kampoeng Sinaoe	Dapat menimbulkan bocornya informasi sensitif melalui celah XSS
10.	XSS, injeksi yang berasal dari sisi *client* dengan memasukkan kode javascript pada form input	1. Melakukan injeksi pada salah satu kolom dengan kode javascript (<audio src=1 onerror=alert(1)>) 2. Kode XSS tersebut akan tampil pada semua halaman website yang menampilkan variabel yang mengandung kode javascript	Dapat menimbulkan bocornya informasi sensitif melalui celah XSS

6) Post-Exploitation: Setelah melakukan eksploitasi atau penyerangan terhadap celah keamanan, selanjutnya adalah menentukan *severity* atau *level* dari masing-masing celah keamanan berdasarkan tipe dan dampak yang ditimbulkan. Penentuan severity tersebut dilakukan menggunakan *Common Vulnerability Scoring System* (CVSS). CVSS merupakan sebuah standar industri yang bersifat *open-source* untuk melakukan penilaian tingkat *severity* dari celah keamanan sistem yang ditemukan. Hasil dari perhitungan *severity* pada celah keamanan menggunakan CVSS akan ditampilkan pada tabel VII kolom *Severity*.

TABEL VII
HASIL TAHAPAN *POST-EXPLOITATION*

NO.	DESKRIPSI	SEVERITY
1.	CSP: Notices, Tidak ada konfigurasi CSP pada security layer untuk memproteksi adanya serangan XSS dan Data Injection	0.0 *Low*
2.	Server Leaks information via "X-Powered-By", Web server memberikan response yang berisi tentang informasi server pada HTTP response header melalui key X-Powered-By	0.0 *Low*
3.	Server Leaks version information via "Server", Web server memberikan response yang berisi tentang informasi server pada HTTP response header	0.0 *Low*
4.	CSP: Wildcard Directive, Tidak ada konfigurasi CSP pada security layer untuk memproteksi adanya serangan XSS dan Data Injection	0.0 *Low*
5.	CSP: script-src unsafe-eval, Terdapat konfigurasi unsave-eval pada CSP	0.0 *Low*
6.	CSP: style-src unsafe-inline, Terdapat konfigurasi unsave-inline pada CSP	0.0 *Low*
7.	CSP: Header Not Set, Tidak ada konfigurasi CSP pada security layer untuk memproteksi adanya serangan XSS dan Data Injection	0.0 *Low*
8.	Vulnerability JS Library, Versi JQuery yang digunakan mengandung celah keamanan, yaitu versi 4.1.3, 3.4.1, 3.3.1, 3.2.1, dan 2.2.4	0.0 *Low*
9.	Pii Disclosure, terdapat response yang mengandung informasi pribadi yang bersifat sensitif	2.7 *Low*
10.	XSS, injeksi yang berasal dari sisi *client* dengan memasukkan kode javascript pada form input	5.5 *Medium*
11.	SQLi, injeksi yang berasal dari sisi *client* dengan memasukkan simbol pada form input	3.5 *Low*
12.	Brute force, melakukan aksi *login* berulang kali dengan *payload* yang berisi *username* dan *password*	8.8 *High*
13.	Take Over Account via XSS, melakukan pencurian akun dengan trigger kerentanan XSS	8.0 *High*

Hasil dari perhitungan tingkat *severity* pada masing-masing celah keamanan yaitu didapatkan sebanyak 13 celah keamanan dengan tingkat *low*, 2 celah keamanan dengan tingkat *medium*, dan 2 celah keamanan dengan tingkat *high*.

7) Reporting

Hasil dari seluruh rangkaian pengujian fungsionalitas dan celah keamanan yang telah dilakukan menggunakan metode *equivalence partitioning*, *boundary value analysis*, *fuzzing*, dan *penetration testing execution standard* (PTES) pada *website* Kampoeng Sinaoe akan ditulis kembali dengan format laporan bernama "Laporan_Pengujian Fungsionalitas dan Keamanan_Kampoeng Sinaoe".

C. Solusi dan Rekomendasi

Setelah melakukan pengujian *website* berdasarkan fungsionalitas dan celah keamanan dengan berbagai macam alat bantu, peneliti mendapatkan hasil pada pengujian

fungsionalitas sebanyak 47 butir uji bersifat valid dan 22 butir uji bersifat tidak valid, kemudian pada pengujian celah keamanan mendapatkan 13 celah keamanan dengan tingkat *low*, 2 *medium*, dan 2 *high*. Selanjutnya adalah memberikan solusi dan rekomendasi terkait kekurangan pada sisi fungsionalitas dan kerentanan pada sisi celah keamanan. Berikut beberapa solusi dan rekomendasi tersebut.

1) Fungsionalitas

TABEL VIII
SOLUSI DAN REKOMENDASI PENGUJIAN FUNGSIONALITAS

ID	DESKRIPSI	HASIL SEBENARNYA	SOLUSI & REKOMENDASI
TC-F-06	Pengujian form Login User	Sistem tidak menampilkan pesan kesalahanan dan tidak mengalihkan ke dashboard	Memberikan pesan peringatan secara hardcode ataupun alert agar pengguna memahami ketika melakukan login
TC-F-48	Pengujian form Data Master Jenis Daftar	Sistem menampilkan pesan peringatan berhasil dan tidak menyimpan data ke database	Memberikan pesan peringatan secara hardcode ataupun alert ketika data yang dimasukkan terdapat simbol atau karakter terlarang dan tidak menyimpan data tersebut
TC-F-51	Pengujian form Pengaturan Aplikasi	Sistem menampilkan pesan peringatan berhasil dan data telah tersimpan	Memberikan validasi terhadap kolom NSM serta menampilkan pesan ketika format NSM selain angka

2) Celah Keamanan

TABEL IX
SOLUSI DAN REKOMENDASI PENGUJIAN CELAH KEAMANAN

NO.	DESKRIPSI	SOLUSI & REKOMENDASI
1.	CSP: Notices, Tidak ada konfigurasi CSP pada security layer untuk memproteksi adanya serangan XSS dan Data Injection	Melakukan konfigurasi CSP pada halaman website
2.	SQLi, injeksi yang berasal dari sisi *client* dengan memasukkan simbol pada form input	Melakukan validasi menggunakan htmlspecialchars() pada setiap kolom masukan agar tidak menerima masukan yang berisi karakter terlarang dan menggunakan prepared_statement saat melakukan query

IV. PENUTUP

A. Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan oleh peneliti pada *website* Kampoeng Sinaoe dari aspek fungsionalitas dan celah keamanan menggunakan metode pengujian *Equivalence Partition, Boundary Value Analysis, Fuzzing,* dan *Penetration Testing Execution Standard* (PTES). Hasil dari pengujian fungsionalitas adalah didapatkan sebanyak 69 butir uji dengan 47 butir uji lulus dan 22 butir uji gagal, sedangkan hasil pengujian celah keamanan didapatkan didapatkan sebanyak 13 celah keamanan dengan tingkat *low*, 2 celah keamanan dengan tingkat *medium*, dan 2 celah keamanan dengan *high severity*. Maka dari itu, dapat disimpulkan bahwa kualitas *website* Kampoeng Sinaoe berdasarkan aspek fungsionalitas adalah kurang baik, karena sistem tidak mampu memberikan *output/response* yang sesuai dengan semestinya, hal tersebut dibuktikan dengan adanya 22 butir uji gagal. Sedangkan, kualitas *website* Kampoeng Sinaoe dari aspek keamanan adalah kurang baik karena ditemukan dua celah keamanan yang memiliki *high severity*.

B. Saran

Berdasarkan kesimpulan diatas, adapun saran yang dapat disampaikan oleh penulis:

1) *Bagi pembaca:* dengan adanya penelitian ini, diharapkan pembaca mampu untuk mengetahui bagaimana cara melakukan pengujian fungsionalitas dan celah keamanan menggunakan metode Equivalence Partition, Boundary Value Analysis, Fuzzing, dan Penetration Testing Execution Standard (PTES).

2) *Bagi peneliti selanjutnya:* peneliti berharap dengan adanya penelitian ini dapat dijadikan sebagai acuan atau referensi bagi peneliti selanjutnya yang ingin meneliti lebih lanjut terkait pengujian fungsionalitas dan celah keamanan pada suatu sistem.

V. REFERENSI

[1] Uminingsih, M. Nur Ichsanudin, M. Yusuf, dan S. Suraya, "PENGUJIAN FUNGSIONAL PERANGKAT LUNAK SISTEM INFORMASI PERPUSTAKAAN DENGAN METODE BLACK BOX TESTING BAGI PEMULA," *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 1, no. 2, hlm. 1–8, Mei 2022, doi: 10.55123/storage.v1i2.270.

[2] R. Parlika, T. A. Nisaa', S. M. Ningrum, dan B. A. Haque, "Studi Literatur Kekurangan dan Kelebihan Pengujian Black Box," 2020.

[3] J. Shadiq, A. Safei, dan R. W. R. Loly, "Pengujian Aplikasi Peminjaman Kendaraan Operasional Kantor Menggunakan BlackBox Testing," *Journal of Information Management*, vol. 5, no. 2, hlm. 97, Jul 2021, doi: 10.51211/imbi.v5i2.1561.

[4] imperva.com, "What is Penetration Testing?," *Penetration Testing*. https://www.imperva.com/learn/application-security/penetration-testing/ (diakses 20 Maret 2023).

[5] B. T. K. Dewi dan M. A. Setiawan, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web".

[6] A. Saputra, "Cara Membuat Test Case: Best Practise yang dapat Anda lakukan di tahun 2022," *Cara Membuat Test Case: Best Practise yang dapat Anda lakukan di tahun 2022*, 2022. https://crocodic.com/cara-membuat-test-case-best-practise-yang-dapat-anda-lakukan-di-tahun-2022/ (diakses 1 Februari 2023).

[7] S. W. N. Nasir, A. Almaarif, dan A. Widjajarto, "Vulnerability Testing Analysis of XYZ Regional Government Site Using PTES," vol. 8, no. 3, 2021.

[8] H. Azis dan F. Fattah, "ANALISIS LAYANAN KEAMANAN SISTEM KARTU TRANSAKSI ELEKTRONIK MENGGUNAKAN METODE PENETRATION TESTING," *Ilk. J. Ilm.*, vol. 11, no. 2, hlm. 167–174, Agu 2019, doi: 10.33096/ilkom.v11i2.447.167-174.

[9] first.org, "Common Vulnerability Scoring System SIG," *Common Vulnerability Scoring System SIG*. https://www.first.org/cvss/ (diakses 7 Februari 2023).