

GL03

DOKUMEN UJI PERANGKAT LUNAK

<PESONA TEGAL>

untuk:

<wisatawan>

Dipersiapkan oleh:

Ruslan Bahreisy S Hi Gafar	(2211102046)
Maulidya Indah Wulandari	(2211102098)
Novi Lailatul Faizah	(2211102110)
Juwita Wilda Pratiwi	(2211102115)

Prodi Teknik Informatika - Universitas Telkom Purwokerto

	Prodi Teknik Informatika Universitas Telkom	Nomor Dokumen		Halaman
		<i>DUPL-xxx <x: id_proyek></i>		<i><#>/<jml #</i>
		Revisi	<i><nomor revisi></i>	<i>Tgl: <isi tanggal></i>

Daftar Isi

Daftar Isi.....	2
Daftar Gambar.....	3
Daftar Tabel.....	4
Daftar Lampiran	5
1. Pendahuluan	6
1.1 Tujuan Pembuatan Dokumen	6
1.2 Ruang Lingkup Pengujian	6
1.3 Referensi.....	6
1.4 Overview Sistem & Fitur Utamanya	6
1.5 Overview Pengujian	6
1.5.1 Perangkat Keras Pengujian.....	6
1.5.2 Sumber Daya Manusia.....	7
1.5.3 Perangkat Lunak Pengujian	7
1.5.4 Material Pengujian.....	7
1.5.5 Strategi dan Metode Pengujian	7
1.5.6 Jadwal Pengujian	7
2. Pelaksanaan Pengujian	8
2.1 Pengujian Unit.....	8
2.1.1 Pengujian Black Box Method.....	8
2.1.2 Pengujian White Box Method	10
2.2 Pengujian Integrasi dan System.....	14
2.2.1 Pengujian Vulnerability	14
2.2.2 Pengujian Penetrasi.....	15
2.3 User Acceptance Test	17
2.4 Summary Pengujian Yang Masih Gagal.....	19
2.2 Lampiran	20

Daftar Gambar

Gambar 1 Hasil Security Test pada ZAP.....	11
Gambar 2 Hasil Pengujian Keamanan Web pada Nmap	12
Gambar 3 Flowchart Path Testing	13
Gambar 4 Hasil Penetration Test.....	15

Daftar Tabel

Tabel 1 Jadwal Pengujian.....	7
Tabel 2 Hasil Black Box Testing.....	8
Tabel 3 Hasil Vulnerability Testing	14
Tabel 4 Hasil Skala Likert Testing	17
Tabel 5 Hasil Usability Testing.....	18

Daftar Lampiran

Lampiran 1 Skrip Pengujian Keamanan Web pada Nmap	20
Lampiran 2 Skrip Vulnerability Testing pada Nmap.....	22
Lampiran 3 Dokumentasi Black Box Testing	26
Lampiran 4 Dokumentasi Skala Likert Test.....	27

1. Pendahuluan

1.1 Tujuan Pembuatan Dokumen

Dokumen DUPL (Dokumen Uji Perangkat Lunak) adalah dokumen yang dirancang untuk memastikan kualitas dan kelayakan perangkat lunak sebelum dirilis ke masyarakat.

1.2 Ruang Lingkup Pengujian

Ruang lingkup pengujian mencakup fungsionalitas, kinerja, dan keamanan web.

1.3 Referensi

Dokumen ini mengacu pada dokumen SKPL dan DPPL Pesona Tegal.

1.4 Overview Sistem & Fitur Utamanya

Website Pesona Tegal menyediakan berbagai informasi mengenai objek wisata unggulan, lengkap dengan deskripsi, gambar, dan lokasi. Dengan antarmuka yang sederhana dan intuitif, pengguna dapat menelusuri berbagai destinasi berdasarkan kategori tertentu seperti wisata, kuliner, dan oleh-oleh.

Fitur Utama:

1. Informasi Wisata, Kuliner, dan Oleh-oleh

- Pengguna dapat mengakses data lengkap mengenai lokasi wisata, rekomendasi kuliner, serta tempat membeli oleh-oleh khas tegal.
- Setiap destinasi dilengkapi dengan deskripsi, foto, dan ulasan pengguna.

2. Fitur ulasan dan penilaian

- Pengguna dapat memberikan ulasan dan penilaian untuk tempat yang telah dikunjungi.
- Penilaian ini berguna sebagai referensi bagi wisatawan lain.

3. Manajemen konten oleh admin

Admin memiliki akses untuk mengelola data destinasi wisata, menambah atau menghapus informasi, dan memantau ulasan pengguna.

4. Peta

Sistem dilengkapi dengan fitur peta, yang ketika di akses pengguna akan otomatis di arahkan pada web/aplikasi peta yang sudah ada.

1.5 Overview Pengujian

1. Tahap 1: *Blackbox Testing* dan *Whitebox Testing*
2. Tahap 2: *Vulnerability Testing* dan *Penetration Testing*
3. Tahap 3: *User Acceptance Testing* dan *Usability Testing*

1.5.1 Perangkat Keras Pengujian

Perangkat keras yang digunakan dalam pengujian adalah laptop.

1.5.2 Sumber Daya Manusia

Menjelaskan sumber daya manusia yang terlibat dalam pengujian perangkat lunak

1. **Tahap 1: Vulnerability Testing dan Penetration Testing**
Vulnerability dan penetration testing dilakukan oleh 4 orang tim developer web Pesona Tegal
2. **Tahap 2: Black Box Testing dan White Box Testing**
Blackbox dan White Box testing dilakukan melalui survei terhadap 10 orang pengguna.
3. **Tahap 3: User Acceptance Testing & Usability Testing**
Survei telah dilakukan terhadap 15 orang pengguna dengan kriteria berusia 20-24 tahun dengan berbagai latar pekerjaan dan pendidikan, tanpa adanya batasan jenis kelamin, dan lokasi tempat tinggal utama di wilayah Tegal dan wilayah lain dalam konteks sebagai pandangan dari wisatawan luar kota.

1.5.3 Perangkat Lunak Pengujian

Pengujian perangkat lunak dilakukan terhadap website Pesona Tegal.

1.5.4 Material Pengujian

Domain pesona tegal = <https://pesona-tegal.zedis.live/>

1.5.5 Strategi dan Metode Pengujian

1. **Black Box Testing dan White Box Testing**
Black Box test dilakukan dengan memberikan beberapa pertanyaan pada Google Form, merujuk pada keberhasilan pengguna dalam menyelesaikan tugas. White Box Test yang dilakukan, yaitu Security Test (termasuk Pengujian Keamanan Web) menggunakan software ZAP dan Nmap, serta Path Testing.
2. **Vulnerability Testing dan Penetration Testing**
Vulnerability Testing dilakukan menggunakan Nmap Scripting Engine (NSE) dan kemudian menganalisis hasil yang didapatkan. Selanjutnya, penetration testing dilakukan dengan menyerang layanan melalui software ZAP dengan mengeksploitasi port yang terbuka dan layanan yang masih rentan pada web.
3. **User Acceptance Testing dan Usability Testing**
User Acceptance Test dilakukan melalui Skala Likert Test yang hasil ditinjau melalui survei pada Google Form. Usability Testing berupa hasil analisis pada hasil survei dari Skala Likert Test.

1.5.6 Jadwal Pengujian

Tabel 1 Jadwal Pengujian

Pengujian	Kasus Data Pengujian	PIC	Jadwal pengujian
Vulnerability dan Penetration Test	Keamanan Web	Juwita Wilda Pratiwi	27 November 2024
Black Box dan White Box Test	Fungsi, Metode, dan Modul pada Kode	Juwita Wilda Pratiwi	11 Desember 2024

User Acceptance dan Usability Test	Pengalaman Pengguna	Juwita Wilda Pratiwi	18 Desember 2024
------------------------------------	---------------------	----------------------	------------------

2. Pelaksanaan Pengujian

2.1 Pengujian Unit

Pengujian terhadap unit terkecil dari perangkat lunak, seperti fungsi, metode, atau modul, untuk memastikan bahwa bagian tersebut berfungsi sebagaimana mestinya. Pengujian ini bertujuan untuk memastikan bahwa seluruh fungsi, metode, dan modul berfungsi dengan baik.

2.1.1 Pengujian Black Box Method

Black Box testing dilakukan dengan melakukan survei melalui Google Form terhadap 10 orang pengguna untuk melakukan beberapa tugas untuk menguji fitur pada web yang diberikan oleh penguji. Keberhasilan dari pengujian dilihat berdasarkan jumlah tugas yang berhasil dilakukan oleh pengguna dengan baik. Berikut tabel hasil pengujian Black Box yang telah dilakukan.

Tabel 2 Hasil Black Box Testing

Skenario Pengujian	Input Data	Prosedur Pengujian	Hasil yang diharapkan	Status									
				U-1	U-2	U-3	U-4	U-5	U-6	U-7	U-8	U-9	U-10
Pengguna akses halaman Wisata tanpa melakukan login.	-	Klik Wisata pada beranda tanpa login	Halaman Wisata ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Pengguna akses halaman Kuliner tanpa login	-	Klik Kuliner pada beranda tanpa login	Halaman Kuliner ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Pengguna akses halaman Oleh-oleh tanpa login	-	Klik Oleh-oleh pada beranda tanpa login	Halaman Oleh-oleh ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Pengguna melakukan registrasi akun	nama, asal kota, email, password Pesan: registrasi akun berhasil!	Klik Daftar pada beranda, memasukkan nama, asal, email, password, dan konfirmasi password, dan klik Daftar	Muncul pesan registrasi berhasil dan pengguna diarahkan ke beranda	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Pass
Pengguna melakukan registrasi akun melalui halaman login	Nama, asal kota, email, password Pesan: registrasi akun berhasil!	Klik Masuk, klik Buat Akun, memasukkan nama, asal, email, password, dan konfirmasi password, dan klik Daftar	Muncul pesan registrasi berhasil dan pengguna diarahkan ke beranda	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

Pengguna login setelah memasukkan email dan password yang sesuai	Email dan password Pesan: login berhasil!	Klik Masuk, memasukkan email dan password yang sesuai, klik Masuk	Muncul pesan bahwa login berhasil dan pengguna diarahkan ke beranda	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Pass
Pengguna memasukkan password yang salah ketika login	Email dan password Pesan: password anda masukkalah	Klik Masuk, memasukkan email, memasukkan password yang salah, klik Masuk, klik Ok	Muncul pesan kesalahan	Fail	Pass	Pass	Pass	Fail	Fail	Fail	Pass	Pass	Pass
Pengguna memasukkan email yang tidak sesuai ketika login	Email dan password Pesan: email tidak terdaftar	Klik Masuk, memasukkan email yang salah, memasukkan password, klik masuk, klik Ok	Muncul pesan kesalahan	Fail	Pass	Pass	Pass	Fail	Fail	Fail	Pass	Pass	Pass
Pengguna mengakses halaman Wisata setelah login	-	Klik Wisata pada header, pilih Wisata Alam, Wisata Taman, atau Wisata Sejarah	Halaman Wisata ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail
Pengguna mengakses halaman Kuliner setelah login	-	Klik Kuliner pada header, pilih Café atau Rumah Makan	Halaman Kuliner ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail
Pengguna mengakses halaman Oleh-oleh setelah login	-	Klik Oleh-oleh, pilih Makanan atau Barang	Halaman Oleh-oleh ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail
Pengguna mengakses halaman detail objek setelah klik Lihat Detail	-	Klik Lihat Detail	Halaman detail objek ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Informasi dari objek ditampilkan pada pengguna	-	Menggulir layar ke bawah	Detail objek, seperti galeri, lokasi, jam operasional, dan ulasan ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Pengguna memberikan ulasan dan rating	Ulasan dan rating	Tulis Rating atau klik up/down pada spinner	Ulasan dan rating milik pengguna ditampilkan	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Pengujian tampilan pada perangkat	url web: https://pe-sona-tegal.zed	Memasukkan url ke browser, klik tanda panah	url mengarahkan pada website	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Pass	Pass

mobile	is.live/beranda.php	(menyesuaikan perangkat mobile)	pesona tegal.										
Pengujian responsivitas pada perangkat mobile	Ukuran layar: 375px x 667px (mobile)	Akses website melalui perangkat mobile	Komponen-komponen pada website pesona tegal ditampilkan dan berfungsi dengan baik	Pass	Pass	Pass	Pass	Pass	Fail	Pass	Fail	Pass	Pass
Pengujian navigasi ke aplikasi media sosial	-	Klik icon Instagram/TikTok pada footer	Diarahkan ke aplikasi/web Instagram/TikTok	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Pass	Pass
Pengguna keluar dari akun	-	Klik Keluar	Kembali ke beranda dengan tampilan seperti sebelum login	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Pass

Analisis keberhasilan web:

Total Keberhasilan Tugas	= 162
Total Pertanyaan	= 18
Total Responden	= 10
Jumlah Responden x Jumlah Pertanyaan	= 180
Presentase Berhasil = (162/180) x 100%	= 90,00%

Jadi, persentase keberhasilan web yang didapatkan pada pengujian unit dengan Black Box Method adalah **90%**.

2.1.2 Pengujian White Box Method

Proses White box testing dilakukan dengan melakukan Security Testing (termasuk Pengujian Keamanan Web) melalui software ZAP dan Nmap, serta melakukan Path Testing dengan membuat sebuah flowchart sebagai hasil analisis dari path kode yang ada.

a. Security Test

Gambar 1 Hasil Security Test pada ZAP

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
SQL Injection	High	1 (25.0%)
SQL Injection - MySQL	High	1 (25.0%)
Parameter Tampering	Medium	5 (125.0%)
User Agent Fuzzer	Informational	435 (10,875.0%)
Total		4

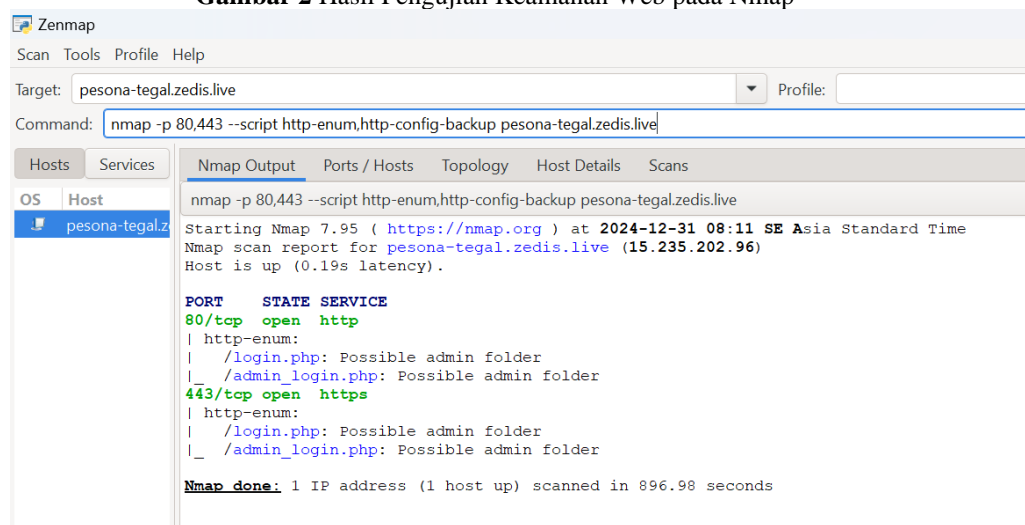
Hasil analisis:

- **SQL Injection:** Ini adalah jenis serangan yang paling umum ditemukan. Hacker dapat menyuntikkan kode SQL berbahaya ke dalam input pengguna untuk memanipulasi database. Dalam laporan Anda, terdeteksi dua jenis SQL Injection, yaitu S01 Injection dan SQL Injection-MySQL.
- **Parameter Tampering:** Serangan ini memungkinkan penyerang untuk memanipulasi parameter dalam permintaan HTTP untuk mendapatkan akses yang tidak sah atau mengubah data.
- **User Agent Fuzzer:** Serangan ini mengeksploitasi kerentanan yang terkait dengan cara aplikasi memproses informasi User-Agent.

Di mana semakin tinggi Risk atau tingkat resiko, maka akan kemungkinan dampak eksploitasi akan semakin besar dan ketika Confidence semakin tinggi, maka kemungkinan adanya kerentanan semakin tinggi. Berdasarkan hasil pemindaian yang diperoleh menunjukkan beberapa area yang perlu diperbaiki untuk mengurangi potensi kerentanannya.

b. Pengujian Keamanan Web

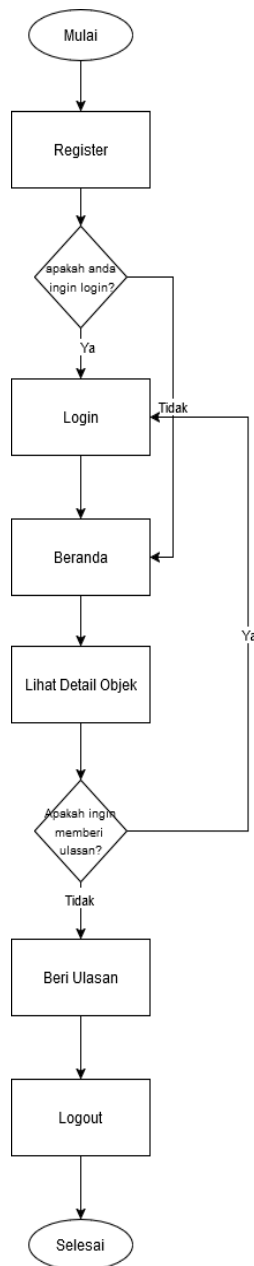
Gambar 2 Hasil Pengujian Keamanan Web pada Nmap



Hasil Analisis:

1. **Eksposur Halaman Login**, adanya file `/login.php` dan `/admin_login.php` menunjukkan bahwa URL ini bisa diakses oleh siapa saja. Jika tidak ada proteksi tambahan, ini berpotensi memudahkan brute force attack atau pencurian kredensial.
2. **Layanan HTTP Tidak Aman (Port 80)**, yaitu informasi yang dikirimkan melalui HTTP dapat disadap, terutama jika halaman login dapat diakses melalui protokol ini.
3. **Kemungkinan Data Sensitif**, skrip `http-config-backup` tidak memberikan hasil eksplisit dalam laporan ini. Namun, perlu memastikan tidak ada file konfigurasi atau cadangan yang terekspos secara publik.

c. Path Test



Gambar 3 Flowchart Path Testing

• Diagram Alur Logika

Diagram alur logika Path Testing dari website Pesona Tegal mencakup langkah-langkah berikut:

1. Pengguna dapat Register (pendaftaran pengguna baru).
2. Memutuskan apakah akan Login atau langsung menuju menu Beranda tanpa login.
3. Dari Beranda, pengguna dapat Lihat Detail Objek tanpa login.
4. Jika ingin memberikan ulasan, pengguna harus login terlebih dahulu.
5. Setelah login, pengguna dapat memberikan ulasan dan rating untuk objek yang dipilih.
6. Setelah menyelesaikan aktivitas, pengguna dapat memilih untuk logout atau kembali ke menu utama.

• Kesimpulan Path Testing

Hasil Path Testing menunjukkan, bahwa terdapat Dua Loop Utama:

1. Loop 1 (Tanpa Login): Pengguna dapat melihat rekomendasi objek di menu Beranda dan Lihat Detail Objek tanpa melakukan login.
2. Loop 2 (Setelah Login): Login diperlukan untuk memberikan ulasan dan rating. Setelah ulasan diberikan, pengguna dapat kembali ke menu utama.

Semua jalur logika yang tergambar pada diagram telah diuji dan tidak ditemukan bug pada alur utama aplikasi. Hasil Path Test menunjukkan bahwa path dari website Pesona Tegal termasuk dalam **Concatenated Loop**. Terdapat dua loop, yaitu sebelum melakukan login dan memberi ulasan.

2.2 Pengujian Integrasi dan System

Pengujian untuk memastikan bahwa beberapa unit atau komponen perangkat lunak berfungsi dengan benar. Selanjutnya, mengidentifikasi adanya masalah yang terjadi setelah seluruh kode digabungkan.

2.2.1 Pengujian Vulnerability

Vulnerability Testing dilakukan menggunakan Nmap Scripting Engine (NSE) dan kemudian menganalisis hasil yang didapatkan. Berikut adalah hasil dari pengujian yang telah dilakukan.

PENGUJIAN SISTEM OLEH : PETUGAS PELAKSANA UJIAN
TANGGAL : 27 November 2024

Tabel 3 Hasil Vulnerability Testing

Komponen Sistem	Fitur Komponen Yang Diuji	Rencana pengujiannya	Hasil Yang Diharapkan	Hasil Pengujian	Kesimpulan
Server (pesona-tegal)	Sistem operasi, layanan jaringan	- Pemindaian port terbuka dengan Nmap - Deteksi versi layanan - Deteksi sistem operasi	Tidak ada port yang tidak perlu dibuka, sistem operasi terdeteksi dan sesuai dengan konfigurasi yang diizinkan.	Banyak port terbuka termasuk FTP, HTTP, HTTPS, Node.js, dan MySQL.	Perlu menutup port yang tidak diperlukan.
Database MySQL	Keamanan koneksi dan query	- Pengujian injeksi SQL di formulir web - Pengaturan validasi input dan prepared statements	Tidak ada kerentanan injeksi SQL yang ditemukan.	Formulir tertentu seperti /register.php dan /wisata-alam.php rentan terhadap injeksi SQL.	Perlu menggunakan validasi input dan prepared statements untuk mengamankan query.
HTTP/HTTPS (Nginx)	Konfigurasi keamanan HTTP	- Pengujian terhadap cookie (httponly, secure) - Deteksi XSS dan CSRF	Tidak ada kerentanan XSS atau CSRF. Cookie harus memiliki atribut httponly dan secure.	Cookie PHPSESSID tidak memiliki atribut keamanan. Jalur sensitif seperti /admin_login.php dapat diakses publik.	Perlu menambahkan atribut keamanan pada cookie dan melindungi jalur sensitif.

Direktori web	Akses direktori sensitif	- Pengujian enumerasi direktori dan file - Uji akses kontrol direktori sensitif	Tidak ada direktori sensitif yang dapat diakses publik.	Direktori sensitif seperti /login.php dan /admin_login.php terdeteksi.	Perlu melindungi direktori dengan otentikasi tambahan atau menghapus file yang tidak digunakan.
Formulir web	Input validasi dan keamanan data	- Pengujian input user untuk injeksi SQL dan XSS - Pengujian CSRF dengan skrip otomatis	Tidak ada celah XSS, CSRF, atau injeksi SQL. Semua formulir memiliki token CSRF.	Beberapa formulir tidak memiliki perlindungan CSRF. Beberapa bidang formulir memungkinkan injeksi SQL dan XSS.	Perlu implementasi token CSRF dan pengamanan input user dengan validasi yang lebih ketat.

2.2.2 Pengujian Penetrasi

Gambar 4 Hasil Penetration Test

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	39 (354.5%)
Missing Anti-clickjacking Header	Medium	37 (336.4%)
Cookie No HttpOnly Flag	Low	1 (9.1%)
Cookie without SameSite Attribute	Low	1 (9.1%)
X-Content-Type-Options Header Missing	Low	181 (1,645.5%)
Authentication Request Identified	Informational	1 (9.1%)
Information Disclosure - Suspicious Comments	Informational	2 (18.2%)
Modern Web Application	Informational	37 (336.4%)
Session Management Response Identified	Informational	3 (27.3%)
User Agent Fuzzer	Informational	12 (109.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	52 (472.7%)
Total		11

1) Medium Risk:

- **Content Security Policy (CSP) Header Not Set** (39 kasus), yaitu CSP tidak diatur, yang meningkatkan risiko serangan seperti XSS (Cross-Site Scripting).
- **Missing Anti-Clickjacking Header** (37 kasus), yaitu header untuk mencegah clickjacking tidak diimplementasikan, memungkinkan manipulasi klik pengguna.

2) Low Risk:

- **Cookie No HttpOnly Flag** (1 kasus), yaitu cookie tidak memiliki atribut HttpOnly, meningkatkan risiko pencurian data cookie.
- **Cookie without SameSite Attribute** (1 kasus), yaitu cookie tanpa atribut SameSite, berpotensi menyebabkan CSRF (Cross-Site Request Forgery).
- **X-Content-Type-Options Header Missing** (181 kasus), tidak adanya header ini membuat aplikasi rentan terhadap MIME-type sniffing.

3) Informational (Rendah Prioritas):

- **Authentication Request Identified** (1 kasus), aktivitas otentikasi terdeteksi, tetapi tidak ada ancaman langsung yang teridentifikasi.
- **Information Disclosure - Suspicious Comments** (2 kasus), komentar mencurigakan ditemukan dalam kode, yang mungkin mengungkapkan informasi sensitif.
- **Modern Web Application** (37 kasus), indikasi aplikasi web modern tanpa ancaman spesifik.
- **Session Management Response Identified** (3 kasus), respon terkait manajemen sesi ditemukan, tanpa ancaman spesifik.
- **User Agent Fuzzer** (12 kasus), pola user-agent yang mencurigakan terdeteksi.
- **User Controllable HTML Element Attribute (Potential XSS)** (52 kasus), atribut HTML yang dapat dikontrol pengguna, berpotensi menyebabkan serangan XSS.

Total:

- Total 11 kategori alert dengan prioritas berbeda.
- Fokus utama harus diarahkan pada risiko **Medium** dan mitigasi atribut header yang hilang (**Low Risk**).

2.3 User Acceptance Test

User Acceptance Testing Pengujian ini dilakukan untuk memastikan bahwa aplikasi yang dibuat telah sesuai dengan kebutuhan pengguna dan siap untuk digunakan. Pengujian dilakukan melalui Skala Likert Testing, di mana penguji melakukan survei terhadap 15 orang dengan kriteria berikut.

Usia : 20-24 tahun
Jenis kelamin : Laki-laki & Perempuan
Jenis pekerjaan : Seluruh jenis pekerjaan
Pendidikan terakhir : Seluruh jenjang
Domisili kota : Tegal dan wilayah lain (traveller)

Pengisian survei dilakukan melalui Google Form setelah pengguna melakukan tugas untuk mengeksplorasi dan menggunakan beberapa fitur yang tersedia pada Web Pesona Tegal sesuai arahan dari penguji. Berikut hasil Skala Likert Test.

Tabel 4 Hasil Skala Likert Testing

No	Pernyataan	Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju
1	Warna dan font yang digunakan nyaman dilihat.	0	0	0	10	5
2	Tampilan antarmuka (user interface) website ini intuitif dan mudah dipahami.	0	0	0	4	11
3	Proses pendaftaran atau login mudah dilakukan.	0	0	0	2	13
4	Informasi yang disediakan oleh website ini jelas dan lengkap.	0	0	0	9	6
5	Website ini berjalan lancar di perangkat saya.	0	0	0	2	13
6	Secara keseluruhan, website ini mudah untuk digunakan.	0	0	0	4	11
7	Navigasi pada website ini mudah untuk dipahami.	0	0	0	5	10
8	Website ini memenuhi semua kebutuhan saya sebagai traveller/wisatawan.	0	0	4	4	7
9	Saya merasa website ini bermanfaat.	0	0	2	3	10
10	Saya akan merekomendasikan website ini kepada teman.	0	0	1	4	10

2.2 Pengujian Usability

Usability Testing bertujuan untuk memastikan bahwa aplikasi yang dibuat sudah memuaskan dan sesuai dengan tujuan. Pengujian ini dilakukan dengan menganalisis hasil dari Skala Likert Testing yang telah dilakukan oleh para pengguna sebelumnya,

kemudian mengetahui pengalaman penggunaan web oleh pengguna dan masalah-masalah yang dihadapi, beserta rekomendasi atau solusi yang diberikan.

Tabel 5 Hasil Usability Testing

No.	Aspek yang Diuji	Deskripsi/Instruksi	Pengamatan/Feedback dari Responden	Masalah ditemukan (Ya/Tidak)	Solusi atau Rekomendasi
1	Kemudahan Navigasi	Uji apakah pengguna dapat dengan mudah memahami navigasi pada website.	Pengguna merasa navigasi pada website mudah dipahami.	Tidak	
2	Kecepatan Loading	Uji seberapa cepat halaman website dimuat.	Pengguna merasa website ini dapat memuat halaman dengan cepat.	Tidak	
3	Keterbacaan Teks	Uji apakah teks yang ada mudah dibaca.	Pengguna merasa masih ada penggunaan font yang perlu diubah.	Ya	
4	Proses Registrasi/Login	Uji apakah proses registrasi dan login mudah dimengerti dan dilakukan.	Pengguna merasa proses registrasi dan login mudah dilakukan.	Tidak	
5	Tampilan Responsif	Uji apakah website berfungsi dengan baik di berbagai perangkat (desktop dan mobile)	Pengguna merasa website ini dapat berfungsi dengan baik.	Tidak	
6	Pemenuhan Kebutuhan	Uji apakah website telah memenuhi kebutuhan pengguna.	Pengguna merasa website ini sudah memenuhi kebutuhan.	Tidak	
7	Ketersediaan Informasi	Uji apakah informasi yang ada sesuai dengan kebutuhan pengguna.	Pengguna merasa informasi pada web ini sudah cukup sesuai dengan kebutuhan	Ya	Menambah jumlah rekomendasi tempat lebih banyak lagi

			pengguna.		dan lebih akurat.
8	Desain Visual	Uji apakah desain website menarik dan sesuai dengan tujuan produk.	Pengguna merasa desain website sudah intuitif, mudah dipahami, dan sesuai.	Tidak	
9	Error Handling	Uji penanganan ketika terjadi kesalahan/error.	Pengguna dapat mengatasi kesalahan/error dengan mudah.	Ya	Memperbaiki fungsi button yang error.
10	Kepuasan Pengguna secara Keseluruhan	Uji apakah pengguna merasa puas setelah menggunakan website.	Pengguna merasa puas terhadap website.	Tidak	

2.4 Summary Pengujian Yang Masih Gagal

2.4.1 Persentase Sukses Tugas

Jumlah tugas sukses = 6
 Jumlah total tugas = 6
Totas Success Rate = $(6 / 6) \times 100\% = 100\%$

2.4.2 Persentase Kepuasan Pengguna

Total Responden = 15
 Jumlah Pertanyaan = 10
 Jumlah setuju/sangat setuju = 143
 Presentase = $(143 / (150 \times 10)) \times 100\%$
Kepuasan Pengguna = **95,33%**

2.4.3 Persentase Error

Jumlah total interaksi = 23
 Jumlah kesalahan = 2
Error rate = $(2/23) \times 100\% = 8,70\%$

2.4.4 Waktu Penyelesaian Tugas

Rata-rata waktu penyelesaian = $(6+8+14+24+8+37+9+10+13+13+2+14+14+4+4)/15$
 = 180/15
 = **12 menit**

2.4.5 Kesimpulan

Berdasarkan pengujian yang dilakukan, didapatkan hasil, bahwa tingkat kepuasan pengguna dalam penggunaan website Pesona Tegal adalah **95,33%**. Hal ini dikarenakan pengguna merasa masih ada **8,70%** bagian yang mengalami error dan tidak berfungsi dengan baik, selain itu terdapat beberapa masukan dari pengguna terkait dengan desain dan tampilan website. Rata-rata waktu pengujian yang diperlukan adalah **12 menit** dengan persentase keberhasilan tugas **100%**.

2.2 Lampiran

1) Hasil Pengujian Keamanan Web pada White Box Method

Lampiran 1 Skrip Pengujian Keamanan Web pada Nmap

```
Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>nmap -p 1-65535 pesona-tegal.zedis.live
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-31 07:37 SE Asia
Standard Time
Nmap scan report for pesona-tegal.zedis.live (15.235.202.96)
Host is up (0.19s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    open      http
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
887/tcp   open      iclcnetsvc
888/tcp   open      accessbuilder
3000/tcp   open      ppp
3306/tcp   open      mysql
8007/tcp   open      ajp12
18972/tcp open      unknown

Nmap done: 1 IP address (1 host up) scanned in 587.39 seconds

C:\Users\LENOVO> nmap -sV pesona-tegal.zedis.live
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-31 07:51 SE Asia
Standard Time
Nmap scan report for pesona-tegal.zedis.live (15.235.202.96)
Host is up (0.19s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
21/tcp    open      ftp          Pure-FTPd
22/tcp    open      ssh          OpenSSH 9.7p1 Ubuntu 7ubuntu4 (Ubuntu
Linux; protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open      http         nginx
139/tcp   filtered  netbios-ssn
443/tcp   open      ssl/http     nginx
445/tcp   filtered  microsoft-ds
888/tcp   open      http         nginx
3000/tcp   open      http         Node.js Express framework
3306/tcp   open      mysql        MySQL 5.7.44-log
8007/tcp   open      http         Node.js Express framework
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.18 seconds

C:\Users\LENOVO>nmap -O pesona-tegal.zedis.live
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-31 07:54 SE Asia
Standard Time
Nmap scan report for pesona-tegal.zedis.live (15.235.202.96)
Host is up (0.21s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    open      http
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
888/tcp   open      accessbuilder
3000/tcp  open      ppp
3306/tcp  open      mysql
8007/tcp  open      ajp12
Device type: firewall|storage-misc|router|general purpose
Running (JUST GUESSING): Juniper JUNOS 12.X|19.X (97%), QNAP QTS 4.X
(90%), Linux 3.X (90%), FreeBSD 6.X (87%)
OS CPE: cpe:/o:juniper:junos:12 cpe:/o:qnap:qts:4.2.0
cpe:/o:linux:linux_kernel:3.16 cpe:/o:juniper:junos:19.4
cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Juniper SRX200-series firewall (JUNOS 12.1 -
12.3) (97%), QNAP QTS 4.2.0 (Linux 3.16) (90%), Juniper Networks JUNOS
19.4 (87%), FreeBSD 6.2-RELEASE (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.60 seconds

C:\Users\LENOVO>nmap -sP pesona-tegal.zedis.live
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-31 07:56 SE Asia
Standard Time
Nmap scan report for pesona-tegal.zedis.live (15.235.202.96)
Host is up (0.19s latency).
Nmap done: 1 IP address (1 host up) scanned in 18.94 seconds
C:\Users\LENOVO>nmap -p 80,443 --script http-enum,http-config-backup
pesona-tegal.zedis.live
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-31 08:31 SE Asia
Standard Time
Nmap scan report for pesona-tegal.zedis.live (15.235.202.96)
Host is up (0.19s latency).

PORT      STATE      SERVICE
80/tcp    open      http
| http-enum:
|   /login.php: Possible admin folder
|_  /admin_login.php: Possible admin folder
443/tcp   open      https
| http-enum:
|   /login.php: Possible admin folder
|_  /admin_login.php: Possible admin folder

Nmap done: 1 IP address (1 host up) scanned in 893.74 seconds

```

2) Hasil Pengujian Vulnerability

Lampiran 2 Skrip Vulnerability Testing pada Nmap

```
C:\Users\LENOVO>nmap --script vuln pesona-tegal.zedis.live
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-31 07:56 SE Asia
Standard Time
Nmap scan report for pesona-tegal.zedis.live (15.235.202.96)
Host is up (0.19s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-sql-injection:
|   Possible sqlmap for forms:
|   Form at path: /, form's action: register.php. Fields that might
be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /wisata-alam.php, form's action: register.php.
Fields that might be vulnerable:
|       name
|       origin
|   Form at path: /wisata-taman.php, form's action: register.php.
Fields that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|       name
|       origin
|   Form at path: /kulinier-rumahmakan.php, form's action:
register.php. Fields that might be vulnerable:
|       name
|       origin
|   Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
```

```

|         name
|         origin
|         Form at path: /oleh-barang.php, form's action: register.php.
Fields that might be vulnerable:
|         name
|         origin
|         Form at path: /oleh-makanan.php, form's action: register.php.
Fields that might be vulnerable:
|         name
|         origin
|         Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|         name
|         origin
|         Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|         name
|         origin
|         Form at path: /detail.php, form's action: register.php. Fields
that might be vulnerable:
|         name
|         origin
|         Form at path: /beranda.php, form's action: register.php. Fields
that might be vulnerable:
|         name
|         origin
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=pesona-tegal.zedis.live
| Found the following possible CSRF vulnerabilities:
|
|         Path: http://pesona-tegal.zedis.live:80/
|         Form id: login-popup-form
|         Form action: login.php
|
|         Path: http://pesona-tegal.zedis.live:80/
|         Form id: registration-form
|         Form action: register.php
|
|         Path: http://pesona-
tegal.zedis.live:80/detail.php?id=4&category=oleh_oleh
|         Form id: login-popup-form
|         Form action: login.php
|
|         Path: http://pesona-
tegal.zedis.live:80/detail.php?id=4&category=oleh_oleh
|         Form id: registration-form
|         Form action: register.php
|
|         Path: http://pesona-
tegal.zedis.live:80/detail.php?id=5&category=wisata
|         Form id: login-popup-form
|         Form action: login.php
|
|         Path: http://pesona-
tegal.zedis.live:80/detail.php?id=5&category=wisata
|         Form id: registration-form
|         Form action: register.php
|
|         Path: http://pesona-
tegal.zedis.live:80/detail.php?id=1&category=kuliner
|         Form id: login-popup-form
|         Form action: login.php

```

```

|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=1&category=kuliner
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-tegal.zedis.live:80/wisata-alam.php
|   Form id: login-popup-form
|   Form action: login.php
|
|   Path: http://pesona-tegal.zedis.live:80/wisata-alam.php
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-tegal.zedis.live:80/wisata-taman.php
|   Form id: login-popup-form
|   Form action: login.php
|
|   Path: http://pesona-tegal.zedis.live:80/wisata-taman.php
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=1&category=oleh_oleh
|   Form id: login-popup-form
|   Form action: login.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=1&category=oleh_oleh
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=3&category=kuliner
|   Form id: login-popup-form
|   Form action: login.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=3&category=kuliner
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=4&category=kuliner
|   Form id: login-popup-form
|   Form action: login.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=4&category=kuliner
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=3&category=wisata
|   Form id: login-popup-form
|   Form action: login.php
|
|   Path: http://pesona-
tegal.zedis.live:80/detail.php?id=3&category=wisata
|   Form id: registration-form
|   Form action: register.php
|
|   Path: http://pesona-tegal.zedis.live:80/kuliner-rumahmakan.php

```



```

|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-tegal.zedis.live:80/kuliner-rumahmakan.php
|      Form id: registration-form
|      Form action: register.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=2&category=kuliner
|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=2&category=kuliner
|      Form id: registration-form
|      Form action: register.php
|
|      Path: http://pesona-tegal.zedis.live:80/oleh-barang.php
|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-tegal.zedis.live:80/oleh-barang.php
|      Form id: registration-form
|      Form action: register.php
|
|      Path: http://pesona-tegal.zedis.live:80/oleh-makanan.php
|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-tegal.zedis.live:80/oleh-makanan.php
|      Form id: registration-form
|      Form action: register.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=2&category=oleh_oleh
|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=2&category=oleh_oleh
|      Form id: registration-form
|      Form action: register.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=2&category=wisata
|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=2&category=wisata
|      Form id: registration-form
|      Form action: register.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=6&category=wisata
|      Form id: login-popup-form
|      Form action: login.php
|
|      Path: http://pesona-
tegal.zedis.live:80/detail.php?id=6&category=wisata
|      Form id: registration-form
|      Form action: register.php
|

```

```

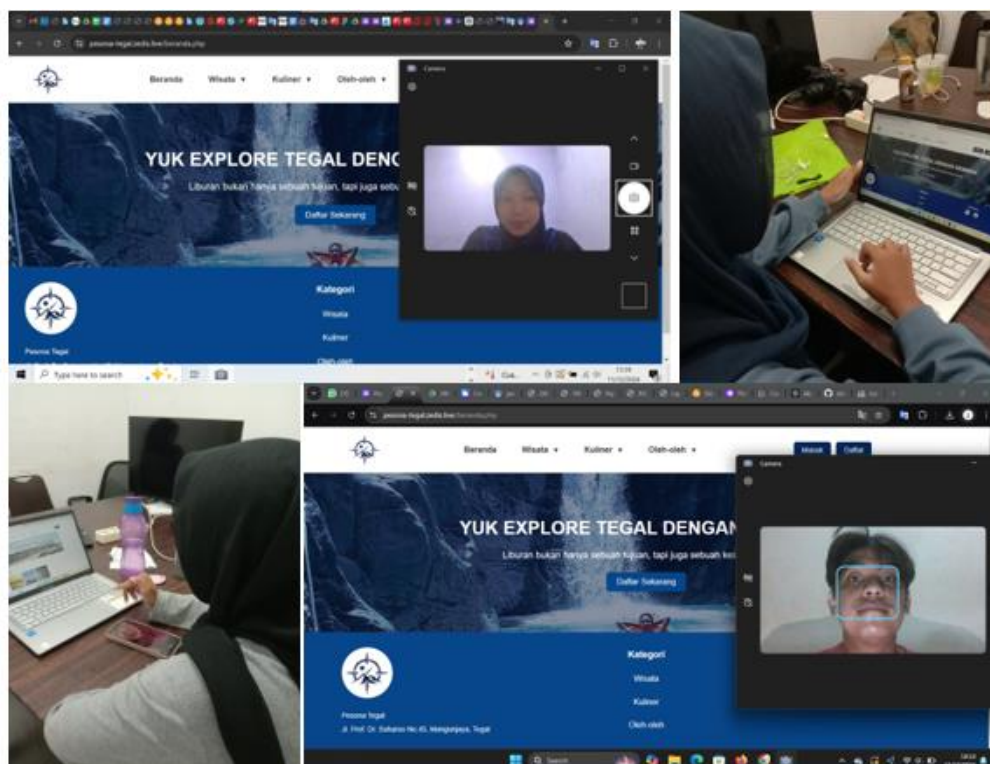
| Path: http://pesona-tegal.zedis.live:80/beranda.php
| Form id: login-popup-form
| Form action: login.php
|
| Path: http://pesona-tegal.zedis.live:80/beranda.php
| Form id: registration-form
| Form action: register.php
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|   /login.php: Possible admin folder
|_  /admin_login.php: Possible admin folder
139/tcp filtered netbios-ssn
443/tcp open      https
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|   /login.php: Possible admin folder
|_  /admin_login.php: Possible admin folder
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
445/tcp filtered microsoft-ds
888/tcp open      accessbuilder
3000/tcp open      ppp
3306/tcp open      mysql
8007/tcp open      ajp12

Nmap done: 1 IP address (1 host up) scanned in 982.80 seconds

```

3) Dokumentasi Pengujian Unit dengan Black Box Method

Lampiran 3 Dokumentasi Black Box Testing





4) Dokumentasi Skala Likert Test pada User Acceptance Test

Lampiran 4 Dokumentasi Skala Likert Test

