Jurnal Kewarganegaraan
Vol. 8 No. 1 Juni 2024
P-ISSN: 1978-0184 E-ISSN: 2723-2328

Website Security Analysis Using the OWASP10 Method (Case Study: almumtazparfumebatam.store)

Bagus Surya Pradhana[1]
Informatics Engineering, STIKOM Muhammadiyah Batam, Batam, Riau islands, Indonesia[1]
Email: baguspradhana123@gmail.com

Abstract

Al Mumtaz Parfume Batam is a perfume seller who is still doing business at home. To expand the scope of its business, an online store was created with the domain almumtazparfumebatam.store. Along with technological advances, the importance of security for a website is the main thing because it prevents attacks from irresponsible outsiders that can harm the ongoing business process. To find out how secure a website is against outside attacks, it is necessary to carry out a penetration testing (pentest) process where a tester simulates himself as an outsider trying to enter the network. This study aims to analyze and test the security of the almumtazparfumebatam.store website using the OWASP10 method in 2021. This method was chosen because it is always updated with information containing 10 attacks on the web that are often found. By doing this research, it is hoped that it can find possible security holes on the almumtazparfumebatam.store website and solutions to prevent them. With this research, it is also hoped that it can fix existing gaps so as to increase the security of the almumtazparfumebatam.store website and assist the website manager in preventing attacks that could be detrimental from irresponsible parties.

Keywords: *Website, Penetration Testing,* OWASP Top 10

INTRODUCTION

In the digital era which is currently developing rapidly, websites are information media that are very commonly used, both by individuals, companies and organizations because they have very wide accessibility and can simplify a process because with a website, everything can be done online, such as It's like shopping online with the increasing number of online stores available. Websites also allow communication interactions between website owners and their users (Vermeer et al., 2020).

Apart from the benefits provided by websites, there are several factors that can endanger the function of a website, such as information leaks and various threats of cyber attacks carried out by hackers. Information security itself means how we can prevent fraud or, at least detect fraud in an information-based system, where the information itself has no physical meaning (Diwan, 2021). Based on ISO/IEC 17799:2005 which explains about information security management systems that information security is an effort to protect against various kinds of threats to ensure business continuity, minimize business risks, and increase investment and business opportunities (Taherdoost, 2022). So it can be concluded that information security is preventing and detecting malicious actions. in the form of unauthorized access, information theft, program changes or physical damage to information systems which can cause loss and damage to existing business processes.

Hacking, as defined in the Oxford dictionary, involves unauthorized access to data using computers (Oliver & Randolph, 2022). One notorious form of hacking is defacement, where hackers alter the appearance of website pages to their liking (Grimes, 2020). An example occurred on August 17, 2001, when Indonesian hackers defaced websites, sparking widespread concern. Despite differing opinions on hacker classifications, Echo-Zine 08 suggests that a hacker is someone deeply interested in computer systems, necessitating knowledge of

networking, programming, and operating systems. Hoffman et al. (2024) further delves into the intricacies, distinguishing hackers as individuals who both write and exploit programs. In the realm of ethical hacking, as elucidated in the book " CEH Certified Ethical Hacker Cert Guide" by Gregg & Santos (2022), hackers are categorized into White Hats, Black Hats, and Gray Hats. Each category delineates distinct motivations and methodologies, ranging from ethical penetration testing to illicit data theft. Additionally, hackers progress through various skill levels, from Newbies, who are novices using pre-existing tools, to Elites, who possess unparalleled expertise in system intricacies. Najera-Gutierrez & Ansari (2018) analysis in " Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux " underscores the diverse objectives of hackers, emphasizing that defacers, while not fitting neatly into predefined categories, often align with Black Hats due to their disruptive actions. Based on this intricate landscape of hacking, safeguarding website security becomes imperative to protect sensitive data, preserve website functionality, and uphold the organization's reputation.

In the context of website security, there are several methods of exploiting website vulnerabilities that are most commonly encountered, some of these methods are compiled by the Open Web Application Security Project (OWASP) Organization as the OWASP TOP 10. The list of methods created by OWASP is updated regularly to provide guidance to security managers. website about factors that need to be considered in order to improve website security (Priyawati et al., 2022). According to Bautista & Parada (2021), OWASP (Open Web Application Security Project) is an open community dedicated to creating an organization that aims to develop, purchase, and maintain trusted applications. At OWASP visitors will find everything free and open. All OWASP tools, documents, forums, and branches are free and open to anyone interested in improving security applications. OWASP supports approaching application security as a person, process, and technology issue because the most effective approach to application security requires improvements in all areas. OWASP is a new type of organization that is free from commercial pressures making it possible to provide application security related information that is unbiased, practical, and cost effective. OWASP is not affiliated with any technology company, although it supports the use of commercial security technologies (Wen & Katt, 2023). Similar to many open-source software projects, OWASP produces a wide variety of materials in an open, collaborative manner. The OWASP Foundation is a non-profit organization that ensures the long-term success of the project. Almost everyone associated with OWASP is a volunteer (Woschek, 2015).

Al Mumtaz Parfume is a perfume reseller who does not have a special place for his business such as a shophouse, kiosk, stand and so on, but still sells from home. Recently the business owner created an online store website with the domain almumtazparfumebatam.store. Previous research has extensively explored web server vulnerability testing and web application security assessment, providing valuable insights for the current study titled "Website Security Analysis Using the Owasp10 Method (Case Study: almumtazparfumebatam.store)." Studies such as "An integrated approach towards vulnerability assessment & penetration testing for a web application" by Prasad et al. and " Web Server Security Analysis Using The OWASP Mantra Method: Web Server Security Analysis Using The OWASP Mantra Method " by Subana et al. have examined the application of OWASP methodologies in assessing web server vulnerabilities. These studies, conducted at institutions like IKIP PGRI Madiun and Muhammadiyah University Faculty of Engineering Ah Ponorogo, utilized a range of tools including Whois, SSL Scan, Zenmap, Acunetix, and OWASP CSRF Tester, among others. Additionally, research such as " ZAP Proxy and OWASP Top 10 " by Ramos Flores has delved into web application vulnerability assessment, employing tools like Zed Proxy

Attack and Foundstone Sitedigger 3.0. These studies collectively contribute to the body of knowledge regarding web security assessment methodologies and tool applications, providing a foundation for the current investigation.

Moreover, investigations such as " Penetration Testing on the SISAKTI Application at Udayana University Using the OWASP Testing Guide Version 4" by Yamin et al. and " Analysis of web security using open web application security project 10" by Helmiawan et al. have focused on specific case studies, offering insights into the practical application of OWASP methodologies in real-world scenarios. These studies, conducted on web servers of Campus X Madiun and the online Thesis Management Information System (SIMSOn) at Indonesian Islam University, respectively, utilized tools like WebScrab, Brutus, Dirb, and Wireshark to assess vulnerabilities and perform penetration testing. By examining these previous research endeavors, the current study aims to build upon their findings and methodologies to analyze the security of almumtazparfumebatam.store comprehensively, utilizing the OWASP10 method as a framework for evaluation and mitigation of potential vulnerabilities.

Based on the previous explanation of the dangers that could harm a website owner, it is very necessary to carry out a security test on a website so that the website owner can understand how safe the website is and if it turns out to be less secure, what should be done to strengthen its security and prevent attacks. which can be detrimental to irresponsible parties. Based on this, an analysis was carried out to test the security of the almumtazparfumebatam.store website. The test was carried out based on the OWASP10 method as a guide to identify security and find vulnerabilities that might exist on the website so that certain steps could be taken based on the analysis results found. This research focuses on collecting information and testing by means of penetration testing based on the Open Web Application Security Project Top 10 (OWASP 10) method.

RESEARCH METHODS

The research methodology employed in this thesis involves several stages of data collection from various sources such as journals, books, and digital media available on the internet. Additionally, information is gathered through the analysis of the Lazismu web system and its management. The researcher utilized a laptop as the hardware tool and Kali Linux as the software tool, along with VirtualBox for installing Kali Linux. The software and hardware specifications include an Intel Core i7 Q720 processor, 8GB RAM, 512GB SSD storage, NVIDIA Quadro FX 880M VGA, and Kali Linux 2024.1 operating system.

In identifying the research problems, the OWASP10 method was utilized, which involves stages like footprinting, scanning, penetrating, and report generation. After identifying the issues from various sources including the Lazismu web management, the appropriate testing method was determined through discussions with the supervisor. Subsequently, the testing phase was conducted following the established procedures. To meet the application requirements, a variety of tools and technologies were employed that align with the research objectives. Comprehensive analysis was carried out to evaluate the security of the almumtazparfumebatam.store website based on the OWASP10 methodology. The analysis results were then utilized to provide recommendations aimed at enhancing the website's security level and minimizing vulnerabilities to potential attacks by malicious entities.

RESEARCH RESULTS AND DISCUSSION

Research Result

From the scanning process that has been carried out, results have been obtained that show possible security gaps on the target website, namely almumtazparfumebatam.store, including those in the following image.

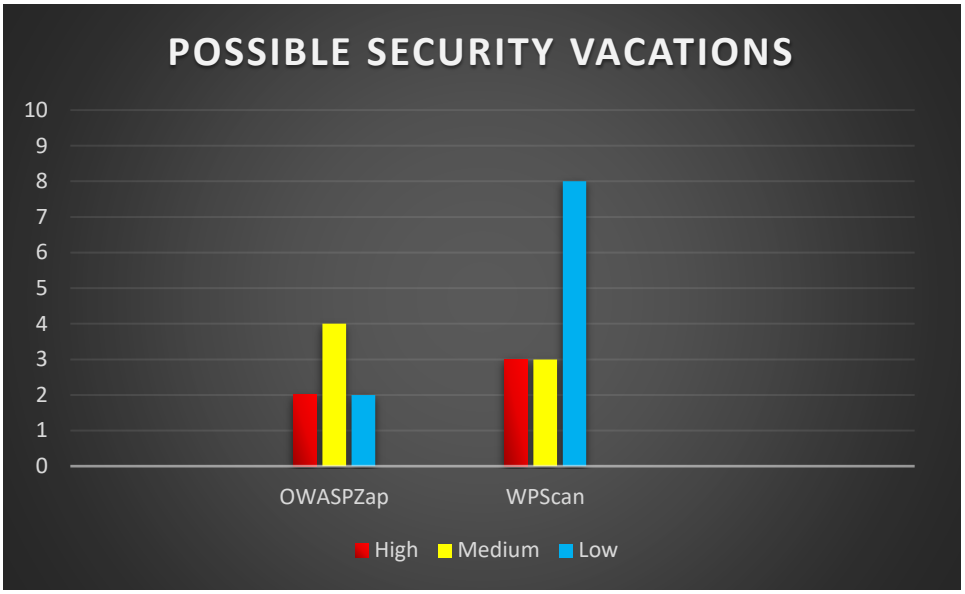


Figure 1. Graph of Possible Security Gaps

The image above shows a graph of scanning results using the OWASPZap and WPScan tools which shows the number of possible security gaps that exist on the target website based on the threat level which is divided into 3 categories, namely High, Medium and Low. For details of threats, see the table below.

Discussion

This stage explains the process of using the OWASPZap tool. The initial appearance of the OWASPZap tool is as follows.

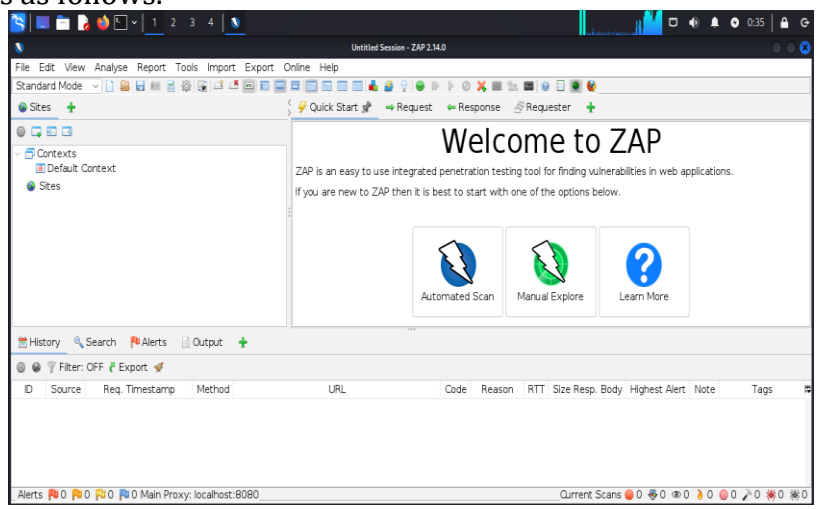


Figure 2. Initial View of OWASPZap

Next, the author uses the Automated Scan feature found in OWASPZap and enters the target URL, which can be seen as follows.

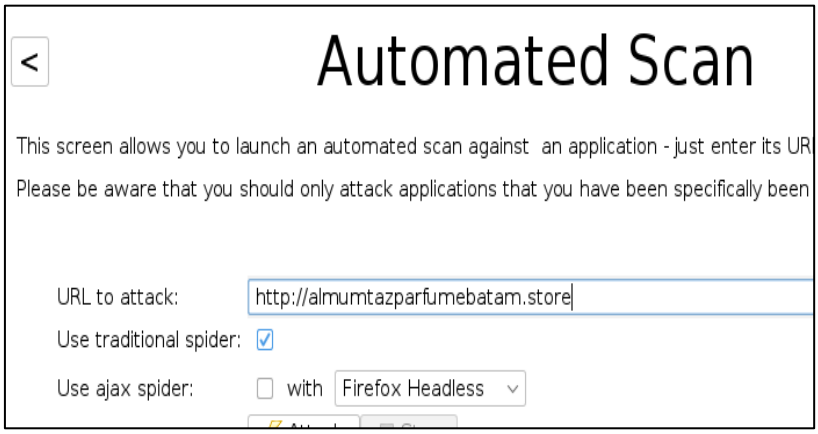


Figure 3. Input Target URL

Then the OWASPZap tool will carry out a crawling process to look for directories and indexes of the target website and after that carry out a spider scan stage as follows.

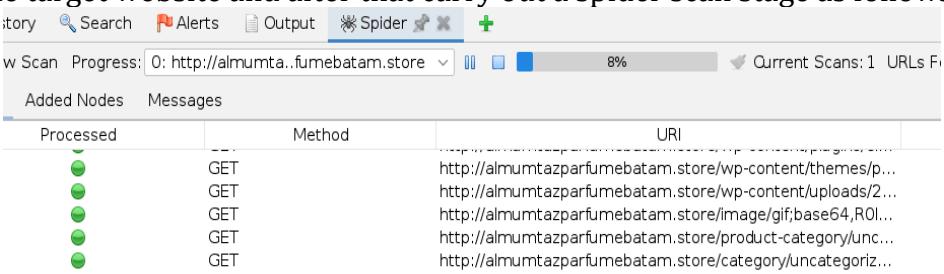


Figure 4. Crawling Process

Next is the active scanning stage to detect security gaps in the target web index as in the following image.

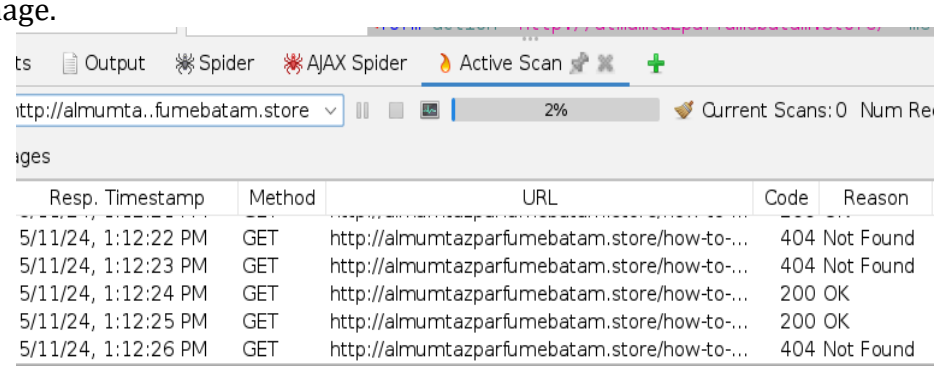


Figure 5. Active Scanning Process

After all the scanning processes are complete, you can see the alert that appears, which is a security hole that has been found as in the following image.

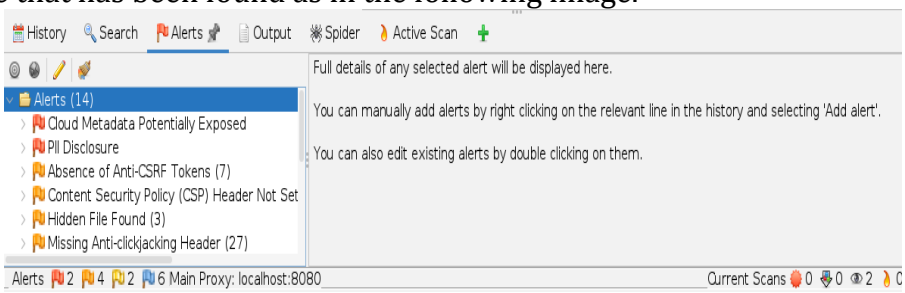
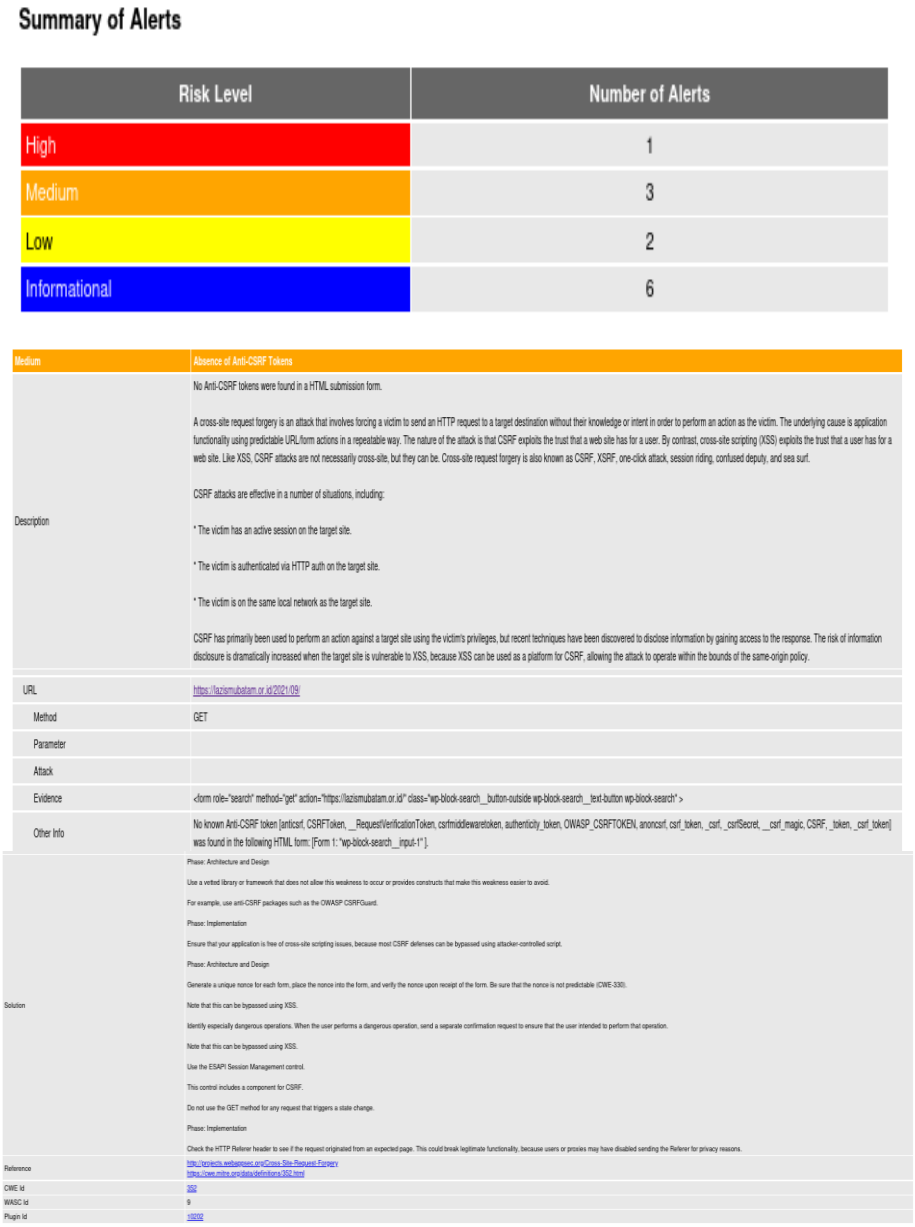


Figure 6. Alert results

Next, the author makes a report based on the alert results of security gaps detected after going through the crawling, spiderscanning and active scanning processes as shown in the following image. The report created contains the level of security gaps found which are divided into High, Medium and Low, there is also a description, category of security gaps, location of security gaps, method parameters and solutions that can be used to overcome these security gaps.



Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	3
Low	2
Informational	6

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://lazismubatam.or.id/2021/09/
Method	GET
Parameter	
Attack	
Evidence	<form role="search" method="get" action="https://lazismubatam.or.id/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "wp-block-search__input-1"].
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Figure 7. Report results from OWASPZap

At this stage the author uses several tools to start looking for sall information related to the target before the pentest is carried out. The author used the ping command on the terminal and then obtained information that almumtazparfumebatam.store has an IP address of 103.247.8.63.

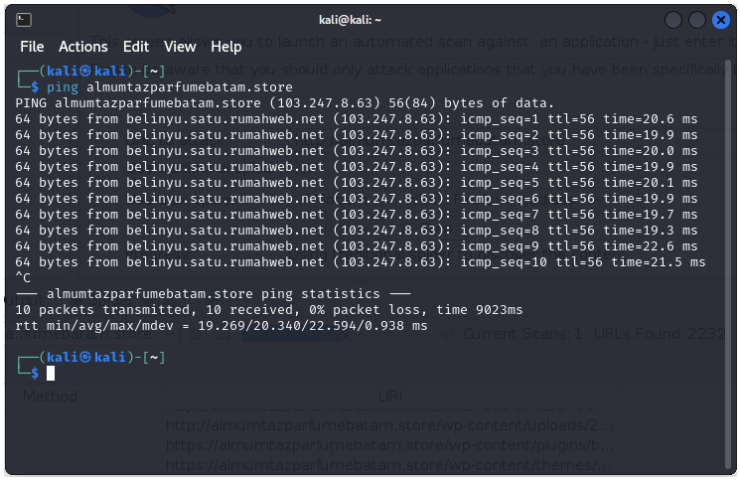


Figure 8. Target Ping Process

Next, use the whois tool to find out information that the target is in the IP address block from 103.247.8.0 to 103.247.11.255, there is also other information such as block IP address, name, email and manager contact.

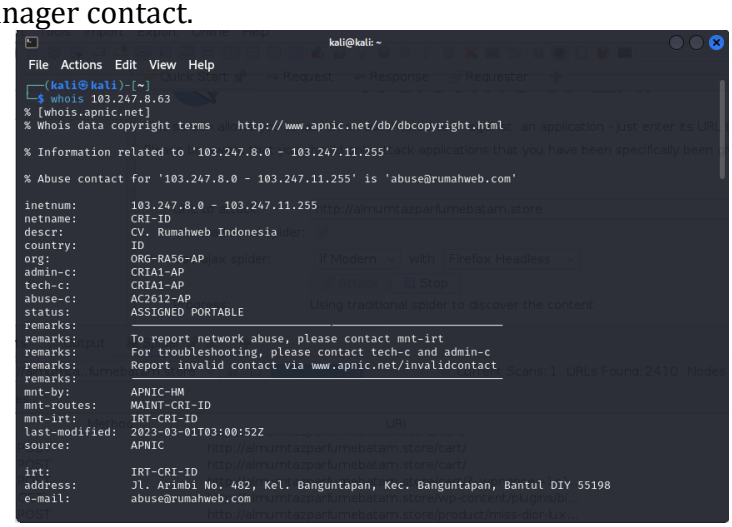


Figure 9. Use of WhoIs Tools

The next stage is to carry out port scanning to find out what TCP and UDP ports are active on the target. This test was carried out with the nmap tool using the command line "nmap almumtazparfumebatam.store" with results as in the following image.

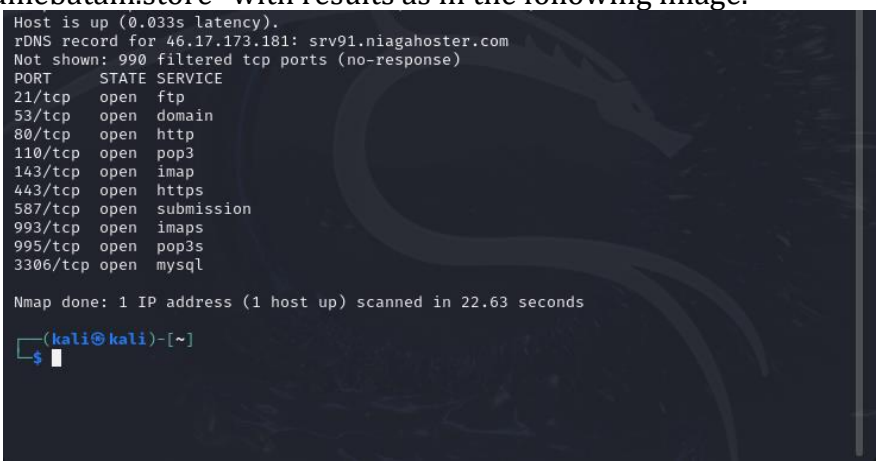


Figure 10. Scanning Using the Nmap Tool

The results obtained show a list of open TCP ports including port 21 for FTP services, port 22 for SSH services, port 80 for HTTP services, port 110 for POP3, port 143 IMAP, port 587 submission, port 443 for HTTPS, port 993 for IMAPS and port 995 .

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Pure-FTPd
✓	53	tcp	open	domain	(generic dns response: NOTIMP)
✓	80	tcp	open	http	LiteSpeed
✓	110	tcp	open	pop3	Dovecot pop3d
✓	143	tcp	open	imap	Dovecot imapd
✓	443	tcp	open	https	LiteSpeed
✓	465	tcp	open	smtp	Exim smtpd 4.96.2
✓	587	tcp	open	smtp	Exim smtpd 4.96.2
✓	993	tcp	open	imap	Dovecot imapd
✓	995	tcp	open	pop3	Dovecot pop3d
✓	2077	tcp	open	tsrmagt	
✓	2078	tcp	open	http	cPanel httpd (unauthorized)
✓	2082	tcp	open	infowave	
✓	2083	tcp	open	radsec	
✓	2086	tcp	open	gnunet	
✓	2087	tcp	open	eli	
✓	2095	tcp	open	nbx-ser	
✓	2096	tcp	open	nbx-dir	
×	2100	tcp	closed	amiganetfs	

Figure 11. Intense Scanning Zenmap

In the scanning results using Zenmap with the Intense scan configuration, all TCP ports show a greater number of ports than using Nmap. Next, testing is carried out to see if the target has a firewall using the nmap tool. The scanning type used is maimon scan using the command line "nmap -sM -p22.80 103.247.8.63", the scanning results can be seen in the following image.

```
Host is up (0.062s latency).

PORT   STATE  SERVICE
22/tcp closed ssh
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

Figure 12 Maimon Scan

The results obtained show that the target server has a port with a closed state so that this test can show the possibility that there is a firewall protecting the target. The next stage that will be carried out is OS Fingerprinting to find out what type of device and operating system the target is using. In this test the nmap and zenmap tools will be used. Nmap results show that the device used is a bridge or switch type with an unknown operating system because the target uses VirtualBox with an accuracy rate of 96% while Zenmap shows an accuracy rate of 98%, this can happen because the target uses a hosting service from a hosting provider. OS scanning is carried out using the command line "nmap -O 103.247.8.63" in the nmap tool.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 22:06 EDT
Nmap scan report for srv91.niagahoster.com (46.17.173.181)
Host is up (0.015s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql
Warning: OSScan results may be unreliable because we could not find at least 1 open and
 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86
%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), B
ay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
```

Figure 13. OS & Device Scanning

```
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Networks BayStack 450 switch
(software version 3.1.0.22) (88%)
No exact OS matches for host (test conditions non-ideal).
```

Figure 14. OS & Device Scanning Zenmap

The next stage is service fingerprinting to find out the version of a service on a particular port. The tool that will be used is nmap with the command line "nmap -sV 103.247.8.63" so that it produces results as in the following image.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 22:24 EDT
Nmap scan report for srv91.niagahoster.com (46.17.173.181)
Host is up (0.018s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        Pure-FTPd
53/tcp   open  domain     (generic dns response: NOTIMP)
80/tcp   open  http       LiteSpeed
110/tcp  open  pop3       Dovecot pop3d
143/tcp  open  imap       Dovecot imapd
443/tcp  open  ssl/https  LiteSpeed
587/tcp  open  smtp       Exim smtpd 4.96.2
993/tcp  open  ssl/imap   Dovecot imapd
995/tcp  open  ssl/pop3   Dovecot pop3d
3306/tcp open  mysql      MySQL 5.5.5-10.6.16-MariaDB-cll-lve
```

Figure 15. Port Service Scanning

To get more information, the author also tested using whatweb using the command line "whatweb 103.247.8.63" at the command prompt. From the WhatsApp results, information was also obtained that the HTTP server used was LiteSpeed as in the following image.

```
[403 Forbidden] Country[LUXEMBOURG][LU], HTML5, HTTPServer[LiteSp
iteSpeed, PoweredBy[LiteSpeed], Strict-Transport-Security[max-age
ns; preload], Title[403 Forbidden][Title element contains newline
ontent-type-options], X-Powered-By[Niagahoster], X-XSS-Protection
```

Figure 16. Results of using whatweb

Apart from using tools to carry out analysis and collect information as above, the author also carries out manual analysis such as Google Dorking and Enumeration. In this process the author managed to find out that the target website uses WordPress as in the following image.

```
<!DOCTYPE html>
<html lang="en-US">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="https://gmpg.org/xfn/11">

<meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1, max-video-preview:-1' />

    <!-- This site is optimized with the Yoast SEO Premium plugin v16.9 (Yoast SEO v22.3) - https://yoast.com/wordpress/plugins/seo/ -->
    <title>Lazismu Batam - Memberi Untuk Negeri - Lazismu Batam</title>
```

Figure 17. Page Source Target

Each testing process carried out on the targets above aims to obtain information related to the IP address and port. Service port, Operation System, and firewall can then be seen in the table as below.

Table 1. Summary of Analysis Process

IP	103.247.8.63		
Domain	almumtazparfumebatam.store		
OS	VirtualBox Unknown OS (98%)		
Ports	Service	Status	Version
21	FTP	Open	Pure-FTPd
53	Domain	Open	NOTIMP
80	HTTP	Open	LiteSpeed
110	POP3	Open	Dovecot pop3d
143	IMAP	Open	Dovecot imapd
443	SSL/HTTPS	Open	LiteSpeed
587	SMPT	Open	Exin smtpd 4.96
993	SSL/IMAP	Open	Dovecot imapd
995	SSL/POP3	Open	Dovecot pop3d
3306	MYSQL	Open	MySQL 5.5.5-10

The next stage is vulnerability identification where the author will look for security gaps in the target based on information obtained manually or using automated vulnerability scanners such as OWASPZap and WPScan. In the previous stage, information was obtained that the target uses a WordPress-based website. Based on this information, the author uses the WPScan tool to carry out vulnerability identification. The following is the scanning process carried out with WPScan.

```
[+] URL: https://almumtazparfumebatam.store/ [46.17.173.181]
[+] Started: Sat Mar 30 02:26:24 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - x-powered-by: Niagahoster
 |  - server: LiteSpeed
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://almumtazparfumebatam.store/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://almumtazparfumebatam.store/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://almumtazparfumebatam.store/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://almumtazparfumebatam.store/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 6.4.3 identified (Outdated, released on 2024-01-30).
 | Found By: Rss Generator (Passive Detection)
 |  - https://almumtazparfumebatam.store/feed/, <generator>https://wordpress.org/?v=6.4.3</generator>
 |  - https://almumtazparfumebatam.store/comments/feed/, <generator>https://wordpress.org/?v=6.4.3</generator

[+] WordPress theme in use: Phlox
 | Location: https://almumtazparfumebatam.store/wp-content/themes/Phlox/
 | Last Updated: 2024-03-21T00:00:00.000Z
 | Readme: https://almumtazparfumebatam.store/wp-content/themes/Phlox/readme.txt
 | [!] The version is out of date, the Outdated version is 2.15.8
 | Style URL: https://almumtazparfumebatam.store/wp-content/themes/Phlox/style.css
 | Style Name: Phlox
 | Style URI: https://wpPhlox.com/
 | Description: Phlox is fast, fully customizable & beautiful WordPress theme suitable for blog, personal por
 | Author: Brainstorm Force
 | Author URI: https://wpPhlox.com/about/?utm_source=theme_preview&utm_medium=author_link&utm_campaign=Phlox_
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: Phlox < 2.15.8 - Contributor+ Stored XSS
 |     Fixed in: 2.10.2
 |     References:
 |      - https://wpscan.com/vulnerability/62871f3a-c9a8-49bb-b67b-143af3caa986
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-2347
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/ed914e67-4cf7-49b1-96be-ed8c604e6dce
 |
 | [!] Title: Phlox < 2.15.8 - Editor+ Stored XSS via Theme Header/Footer
 |     Fixed in: 2.15.8
 |     References:
 |      - https://wpscan.com/vulnerability/30fd2612-91f6-4c1b-8d0c-fa607edf4717
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-29768
 |      - https://patchstack.com/database/vulnerability/Phlox/wordpress-Phlox-theme-4-6-4-cross-site-scriptin
```

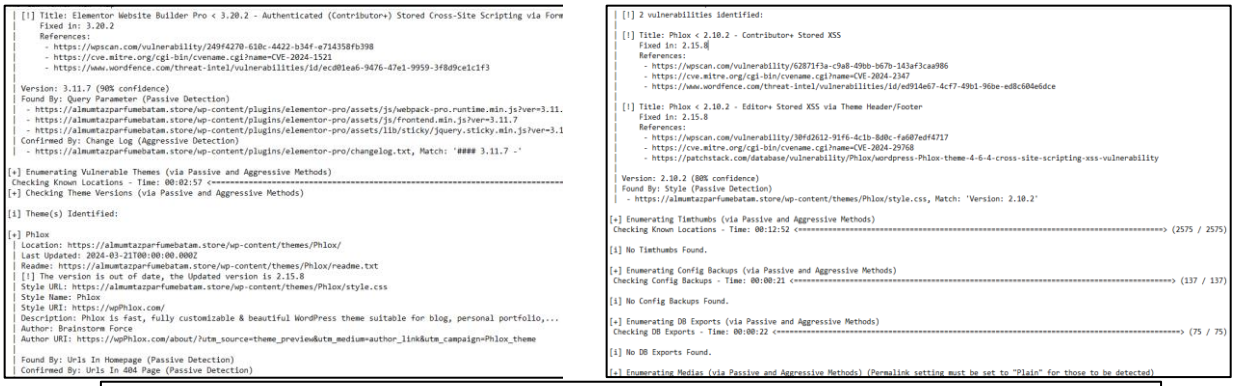
```
 | Version: 2.10.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://almumtazparfumebatam.store/wp-content/themes/Phlox/style.css, Match: 'Version: 2.15.8'

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] elementor
 | Location: https://almumtazparfumebatam.store/wp-content/plugins/elementor/
 | Last Updated: 2024-03-26T09:42:00.000Z
 | [!] The version is out of date, the Outdated version is 3.20.3
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Elementor Website Builder < 3.20.3 - Contributor+ DOM Stored XSS
 |     Fixed in: 3.20.3
 |     References:
 |      - https://wpscan.com/vulnerability/22e8d017-79f5-40c8-8a2c-e0ee42ba80c8
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-2117
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/c8d7448a-b8a6-4b0b-92df-a15272fc56
 |
 | Version: 3.20.0 (100% confidence)
 | Found By: Javascript Comment (Aggressive Detection)
 |  - https://almumtazparfumebatam.store/wp-content/plugins/elementor/assets/js/admin-feedback.js, Mat
 | Confirmed By: Style Comment (Aggressive Detection)
 |  - https://almumtazparfumebatam.store/wp-content/plugins/elementor/assets/css/admin.min.css, Match:
```

```
[+] elementor-pro
 | Location: https://almumtazparfumebatam.store/wp-content/plugins/elementor-pro/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | [!] 6 vulnerabilities identified:
 |
 | [!] Title: Elementor Pro < 3.19.3 - Authenticated (Contributor+) Information Exposure
 |     Fixed in: 3.19.3
 |     References:
 |      - https://wpscan.com/vulnerability/52195b1a-31b9-46da-bed8-7fdd2c6c8c14
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23523
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/ecc8996a-d95c-4711-ac7d-523f5100c7fc
 |
 | [!] Title: Elementor Website Builder Pro < 3.20.2 - Authenticated (Contributor+) Stored Cross-Site Scripting
 |     Fixed in: 3.20.2
 |     References:
 |      - https://wpscan.com/vulnerability/d332bb66-e69c-4d11-8ff2-2c35d7ce2808
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1364
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/531954dd-ed3f-4626-adab-c1bba8407c89
 |
 | [!] Title: Elementor Website Builder Pro < 3.20.2 - Authenticated (Contributor+) DOM-Based Stored Cross-Site Scripting
 |     Fixed in: 3.20.2
 |     References:
 |      - https://wpscan.com/vulnerability/964c149d-fb08-4f86-a9a8-34a4412b5fdd
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-2781
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/54970085-5206-45b6-adcf-11e6dd4cd633
 |
 | [!] Title: Elementor Website Builder Pro < 3.20.2 - Authenticated (Contributor+) Stored Cross-Site Scripting
 |     Fixed in: 3.20.2
 |     References:
 |      - https://wpscan.com/vulnerability/a48b0031-02f6-4871-beb3-0f61e1cd3d28
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-2121
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/8698d6dd-7376-4d29-8a5c-21c239a7aa03
```



```
[i] User(s) Identified:

[+] adminalmumtaz
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - https://almumtazparfumebatam.store/wp-json/wp/v2/users/?per_page=100&page=1
 |  Oembed API - Author URL (Aggressive Detection)
 |   - https://almumtazparfumebatam.store/wp-json/oembed/1.0/embed?url=https://almumtazparfumebatam.store/&format=json
 |  Rss Generator (Aggressive Detection)
 |  Yoast Seo Author Sitemap (Aggressive Detection)
 |   - https://almumtazparfumebatam.store/author-sitemap.xml
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 0
 | Requests Remaining: 7

[+] Finished: Sat Mar 30 02:44:25 2024
[+] Requests Done: 3608
[+] Cached Requests: 19
[+] Data Sent: 1.089 MB
[+] Data Received: 3.173 MB
[+] Memory used: 317.137 MB
[+] Elapsed time: 00:18:00
```

Figure 18. WPScan Scanning Output

From the scanning results above, we obtained several information related to WordPress that the target is using, such as the version used, plugins used, themes used, users who may have logged in, and other information leaks that could allow attacks on the target website. The author then observed and summarized this as can be seen in the following table.

Table 2. Summary of WPScan Scanning

Service Type	Service Version	Status
WordPress	6.4.3	Outdated
Phlox (Theme)	2.10.2	Outdated
Elementor (Plugin)	3.20.0	Outdated
Elementor Pro (Plugin)	3.11.7	Outdated

Next, the author carries out an analysis based on all the information that has been collected to see what possible security gaps could occur. The results of the analysis that has been carried out can be seen in the following table.

Table 3. WPScan Scanning Analysis Results

Threat Type	Amount	Username Login
Information Disclosure	1	Found(adminalmumtaz)
Information Exposure	1	
Denial of Service	1	
Cross-Site Scripting	8	

Next, the same process is carried out using the OWASPZap tool as previously when using the WPScan tool, namely carrying out vulnerability identification testing, the information collection stage and the analysis stage based on the security gap information obtained. The final

results that the author succeeded in summarizing using the OWASPZap tool are in the form of an easy-to-understand table as in the following table.

Table 4. OWASPZap Scanning Summary

Threat Level	Threat Type	Amount
HIGH	Cloud Metadata Potentially Exposed	1
HIGH	PII Disclosure	1
MEDIUM	Content Security Policy Not Set	18
MEDIUM	Absence Of Anti-CSRF Tokens	41
MEDIUM	Hidden Files Found	3
MEDIUM	Missing Anti-Clickjacking Header	41
LOW	Server Leaks Information via "X-Powered-By" Http Response Header	395
LOW	Timestamp Disclosure	135

Upon conducting analysis with previous tools, it was discovered that several false positives emerged, potentially due to queries resembling those of specific security vulnerabilities; however, manual testing revealed no impact on the target. During the scanning process using WPScan, valuable information was gleaned, including the identification of an active login user, "adminalmumtaz," albeit with an unknown password. Subsequently, the author opted to attempt penetration via the SQL Injection method on the login page form of the target. Given the utilization of WordPress services by the target, the existence of the login page on either "wp-admin" or "wp-login.php" was confirmed. Upon trying the URL "almumtazparfumebatam.store/wp-login.php," depicted in the image below, the login page was successfully accessed as anticipated.

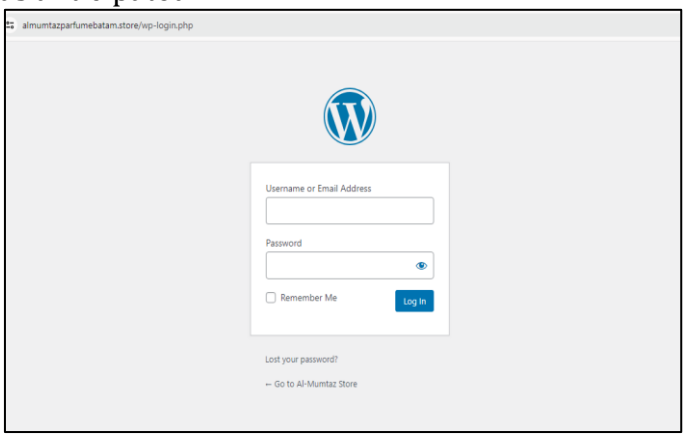


Figure 19. Target Login Page

Various syntaxes are commonly employed in SQL Injection techniques, including "OR 1=0," "OR x=x," "OR x=y," and numerous others. After numerous attempts with different syntaxes, the author successfully gained access to the admin page and obtained administrator privileges by leveraging a username obtained previously using WPScan. The specific syntax utilized by the author, "adminalmumtaz'OR'1'=1," manipulates the database by appending additional SQL syntax after the username, such as "OR'1'=1," effectively ensuring a true condition and granting the author administrator access, as depicted in the accompanying image.

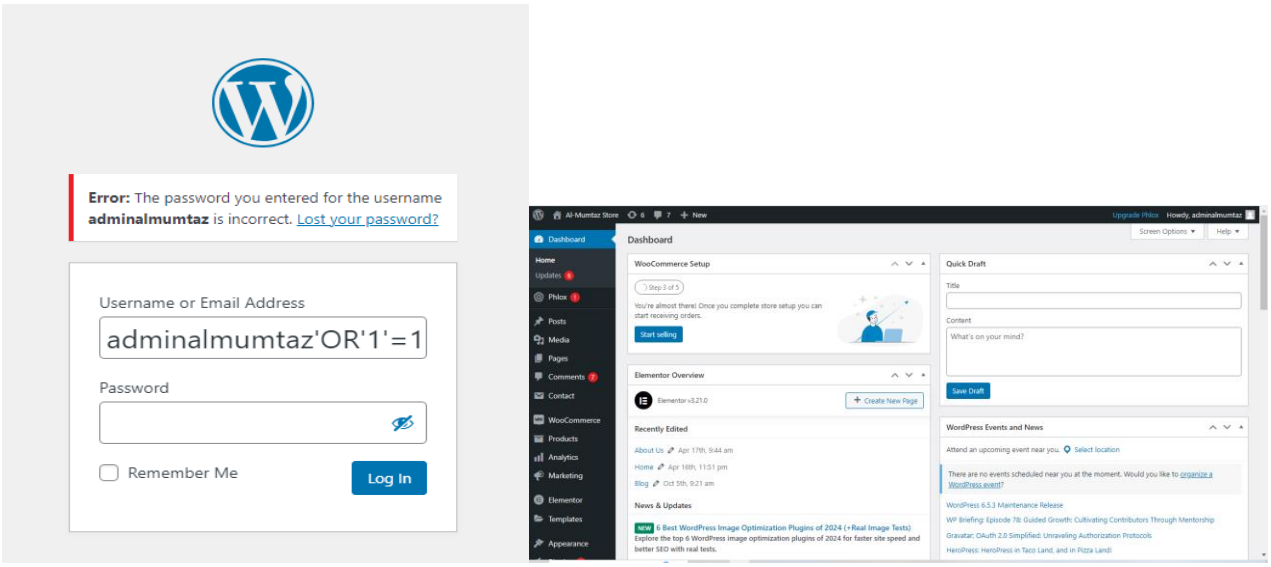


Figure 20. SQL Injection Experiment and Penetration Test

The vulnerability of the target to SQL Injection is evident due to various factors, including inadequate database security, lack of input validation, and the combination of SQL and string syntax, creating a loophole. Despite accessing the target dashboard with full privileges, the author remained unaware of the login user's password, prompting the utilization of a brute force approach. This method involves systematically attempting numerous word and number combinations until the correct one is found, with the author employing a dictionary-based approach. The efficacy of this method relies on the computer's processing speed, with the author creating and employing specific word combinations, known as payloads, tailored to potential relationships with the target and likely passwords.

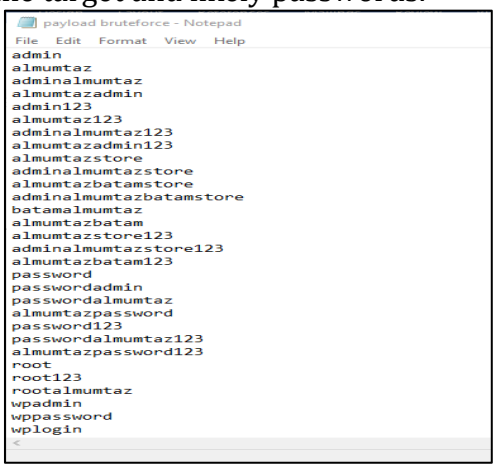


Figure 21. Bruteforce payloads

*Payloads*What has been created will be imported into tools specifically for bruteforce. The following is the first stage of testing the Bruteforce method, namely opening the Burp Suite tool as in the following image.

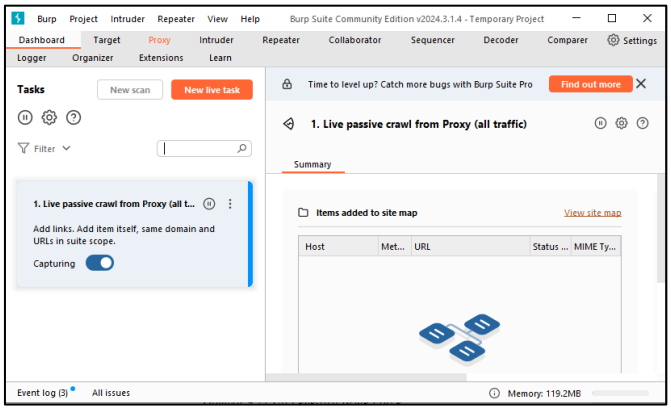


Figure 22. Initial view of Burp Suite

Next, connect the proxy from Burp Suite, namely 127.0.0.1:8080 with the browser that will be used, here the author uses the Google Chrome browser with the addition of the Foxy Proxy extension to make proxy configuration easier.

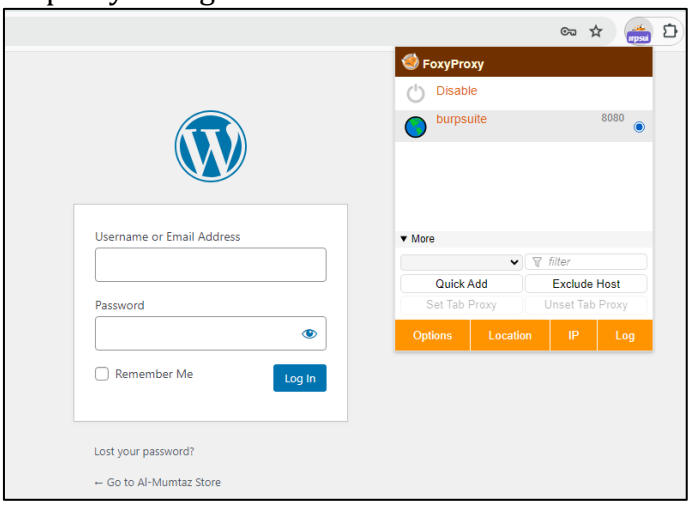


Figure 23. Changing the browser proxy

Next, the author tries to log in using the username that has been obtained, namely "adminalmumtaz" with the password "admin" which is then intercepted by Burp Suite so that the login request can be modified as in the following image.

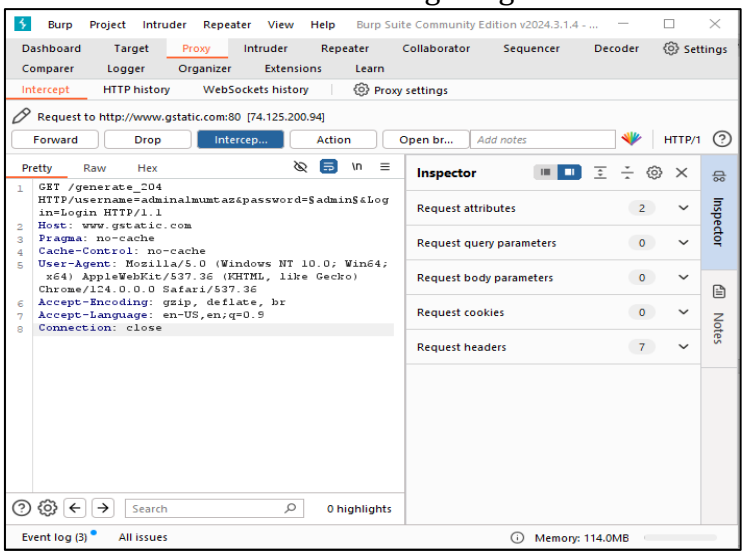


Figure 24. Intercept request

Next, move on to the intruder section to determine which syntax will be targeted in the attack. In this research, what will be attacked is the password so that the password syntax will be focused on and added to the attack target as in the following image.

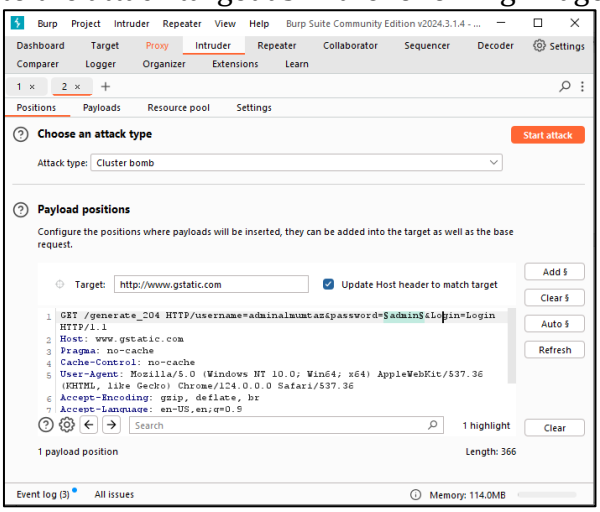


Figure 25. Payload position configuration

The next step is to configure the payloads that have previously been prepared and also configure the Gerp match as a marker for a successful login as in the following image.

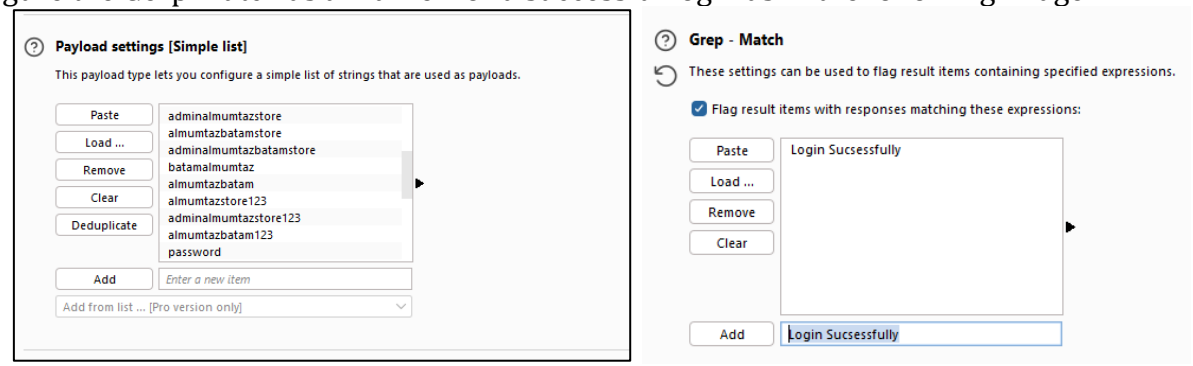
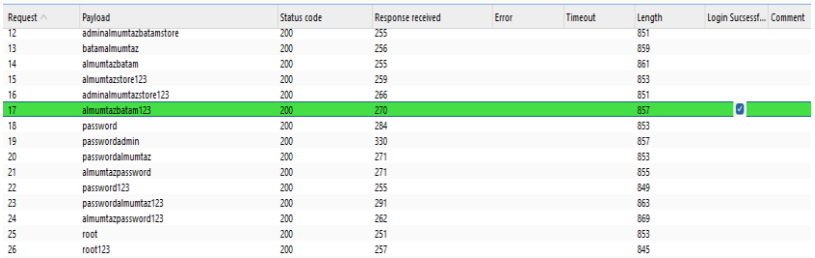


Figure 26. Load Payloads and Gerp-match Configuration

The final stage is the attack where Burp Suite will try every payload provided in the request that was intercepted previously. From this process the author succeeded in gaining login access for the password trial "almumtazbatam123" so it can be concluded that the password for the adminalmumtaz login user is "almumtazbatam123". This can be seen in the following image.



Request	Payload	Status code	Response received	Error	Timeout	Length	Login Sucsessf...	Comment
12	adminalmumtazbatamstore	200	255			851		
13	batamalmumtaz	200	256			859		
14	almumtazbatam	200	255			861		
15	almumtazstore123	200	259			853		
16	adminalmumtazstore123	200	266			851		
17	almumtazbatam123	200	270			857	✓	
18	password	200	284			853		
19	passwordadmin	200	330			857		
20	passwordalmumtaz	200	271			853		
21	almumtazpassword	200	271			855		
22	password123	200	255			849		
23	passwordalmumtaz123	200	291			863		
24	almumtazpassword123	200	262			869		
25	root	200	251			853		
26	root123	200	257			845		

Figure 27. Bruteforce results

Next, the author carried out an experiment on the target login page using the user login and password that was successfully obtained previously via the WPScan and Burp Suite tools and successfully entered the target admin dashboard with full access rights as in the following image.

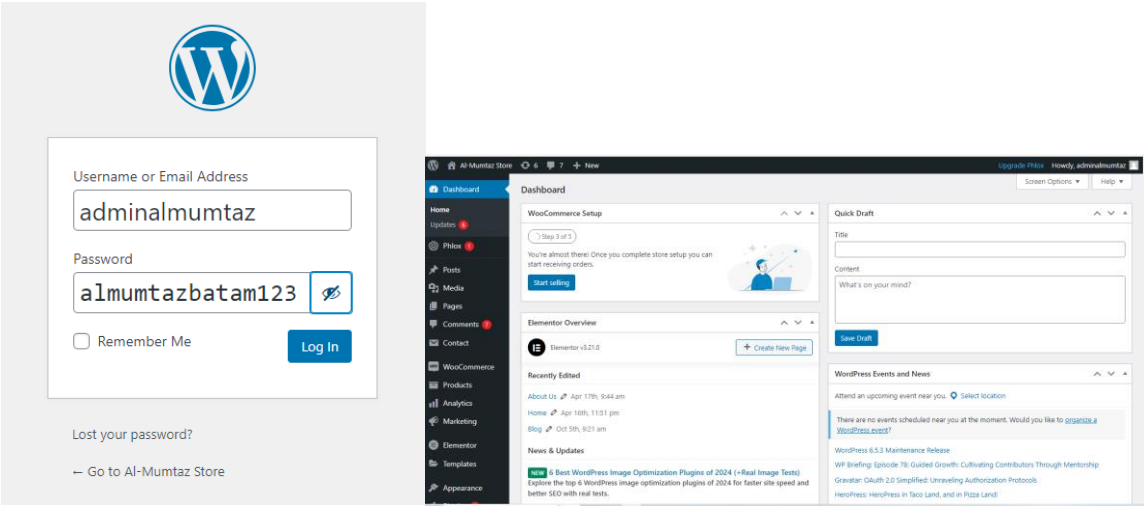


Figure 28. Login attempt

Furthermore, the author also carried out a penetration test using the DoS method where the author sent 10,000 server requests using the slowhttptest tool in the hope that this would result in the website server service being overwhelmed so that it eventually stopped functioning causing the target website to go down because it was unable to receive the large amount of incoming traffic. The DoS testing process against the target can be seen as in the following image.

Figure 29. Denial of Service Penetration Test

Upon completion of the DoS attack testing, it was observed that the target server effectively mitigates incoming traffic, with only 1,000 out of 10,000 attempts successfully accessing the server, indicating resilience against such attacks. However, Neef & Oudeh (2024) states that preceding assessments highlight several security vulnerabilities within the target website, primarily stemming from outdated plugins and themes as identified by OWASPZap and WPScan tools. These vulnerabilities, coupled with persistent risks unveiled through penetration tests like SQL Injection and Bruteforce methods, emphasize the urgency for proactive security measures. Recommendations include updating plugins and themes regularly, strengthening password configurations, and implementing encryption for login credentials to mitigate risks such as Sensitive Data Exposure. Additionally, enhancing SQL query validation and exploring hosting packages with layered firewall protection are advised steps to enhance the website's security posture against potential hacking endeavors.

CONCLUSION

In conclusion, the research conducted, including penetration testing using the OWASP10 2021 method, on the almumtazparfumebatam.store website revealed several significant findings. Firstly, the OWASP10 method proved highly suitable for identifying security

vulnerabilities within the website, highlighting areas of concern in line with the 2021 OWASP10 list. Despite efforts to secure the system, the website still exhibits notable vulnerabilities, leading to the unauthorized access of sensitive information due to successful exploits. The discovery underscores the critical importance of regularly updating plugins and themes to prevent the emergence of dangerous security gaps, as evidenced by alerts originating from outdated components. Moreover, the successful identification and exploitation of security gaps during penetration testing emphasize the necessity for the website owner to prioritize security enhancements. Moving forward, future research endeavors should consider utilizing the latest OWASP10 methodology upon its release and incorporate broader and updated exploitation techniques to reflect advancements in technology and available resources, thereby contributing to a more comprehensive understanding of web system security.

BIBLIOGRAPHY

Bautista, E. C. R., & Parada, H. D. J. (2021). Guide of principles and good practices for software security testing in web applications for a private sector company. *2021 Congreso Internacional de Innovación y Tendencias En Ingeniería (CONIITI)*, 1–7.

Diwan, T. D. (2021). An investigation and analysis of cyber security information systems: latest trends and future suggestion. *Information Technology in Industry*, *9*(2), 477–492.

Gregg, M., & Santos, O. (2022). *CEH Certified Ethical Hacker Cert Guide*. Pearson IT Certification.

Grimes, R. A. (2020). *Hacking multifactor authentication*. John Wiley & Sons.

Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., & Guntara, A. (2020). Analysis of web security using open web application security project 10. *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, 1–5.

Hoffman, C. J., Howell, C. J., Perkins, R. C., Maimon, D., & Antonaccio, O. (2024). Predicting new hackers' criminal careers: A group-based trajectory approach. *Computers & Security*, *137*, 103649.

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Neef, S., & Oudeh, M. (2024). Bringing UFUs Back into the Air With FUEL: A Framework for Evaluating the Effectiveness of Unrestricted File Upload Vulnerability Scanners. *ArXiv Preprint ArXiv:2405.16619*.

Oliver, D., & Randolph, A. B. (2022). Hacker definitions in information systems research. *Journal of Computer Information Systems*, *62*(2), 397–409.

Prasad, K. S., Sekhar, K. R., & Rajarajeswari, P. (2018). An integrated approach towards vulnerability assessment & penetration testing for a web application. *International Journal of Engineering and Technology (UAE)*, *7*, 431–435.

Priyawati, D., Rokhmah, S., & Utomo, I. C. (2022). Website vulnerability testing and analysis of website application using OWASP. *International Journal of Computer and Information System (IJCIS)*, *3*(3), 142–147.

Ramos Flores, E. (2023). ZAP Proxy and OWASP Top 10. *Computer Science;*

Subana, B., Fadlil, A., & Sunardi, S. (2020). Web Server Security Analysis Using The OWASP Mantra Method: Web Server Security Analysis Using The OWASP Mantra Method. *Jurnal Mantik*, *4*(1), 107–116.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14).

Vermeer, S., Trilling, D., Kruikemeier, S., & de Vreese, C. (2020). Online news user journeys: the role of social media, news websites, and topics. *Digital Journalism*, *8*(9), 1114–1141.

Wen, S.-F., & Katt, B. (2023). A quantitative security evaluation and analysis model for web

applications based on OWASP application security verification standard. *Computers & Security*, *135*, 103532.

Woschek, M. (2015). Owasp cheat sheets. *OWASP Foundation*, 1–315.

Yamin, R. T. N., Suarjaya, I. M. A. D., & Pratama, I. P. A. E. (2022). Penetration Testing on the SISAKTI Application at Udayana University Using the OWASP Testing Guide Version 4. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *10*(3), 155. https://doi.org/10.24843/jim.2022.v10.i03.p04