International Journal of Multidisciplinary Research and Growth Evaluation.

Website vulnerability analysis PT. Sadikun Niaga Mas Raya Uses the Owasp Penetration Testing Method

Muhammad Fiqri Fachrezi Ikhsan [1*], Erick Irawadi Alwi [2], Tasrif Hasanuddin [3]
[1-3] Program Study Informatics Engineering, Faculty of Computer Science, Indonesian Muslim University, Makassar, Indonesia

* Corresponding Author: **Muhammad Fiqri Fachrezi Ikhsan**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 01
January-February 2024
Received: 26-11-2023
Accepted: 28-12-2023
Page No: 418-425

Abstract
The development of the world of computers, the internet and web technology is so rapid that it has penetrated all areas of people's lives. The increasing number of internet service users means that more and more information can be found online. Many individuals are aware of how the information they provide can be used, and organizations are increasingly aware of information security risks that can have negative impacts. Losing important documents can affect business processes, an organization's image, customer trust, and relationships with their business partners. This incident also occurred at PT. Sadikun Niagamas Raya as a subsidiary of PT. Pertamina.
The purpose of this research is to test the security of the www.sadikun.com web domain against attacks from outside parties and convert the penetration testing results into an understandable report.
The method used in this research is the Penetration Testing method with several steps starting from Star, searching for information, scanning, testing possible security gaps, creating a test report until completion.
The results obtained from this research are that 3 security gaps were found, including scripts that can be inserted and executed in the search column, usernames and passwords that can be accessed in the database due to the ID parameter in the URL being vulnerable to sqlinjection attacks, the database can be downloaded via the URL caused by a configuration error on the server side. Based on the OWASP framework which lists the 10 most common web application security vulnerabilities that have the potential to harm PT. Sadikun Niagamas Raya.

Keywords: Vulnerability Analysis, Penetration Testing, OWASP

Introduction

The development of the world of computers, the internet and web technology is so rapid that it has penetrated all areas of people's lives. Currently, people are more dependent on computer network services. With the increasing number of internet service users, more and more information can be found online. This information has become invaluable in the digital era for organizations, businesses and individuals. However, the more information a person provides about themselves on the internet, the less private they become. Recently, many individuals have become aware of how the information they provide can be used, and organizations are increasingly aware of information security risks that can have negative impacts. Losing important documents can affect business processes, organizational image, customer trust, and relationships with their business partners (Herfiedhantya, 2014) [8]. The incident that occurred at PT. Sadikun Niagamas Raya is a SQL injection attack that causes the attacker to retrieve information about the database. One of the basic rules in determining the security of a network is 3, namely Confidentiality (confidentiality) maintaining the confidentiality of information from unauthorized people, Integrity (integrity) protecting changes to information from unauthorized people and Availability (availability) ensuring that information is always available for use. Accessed or abbreviated as CIA TRIAD.

If the 3 basic factors in network security cannot be met then a network can be categorized as unsafe and prone to being compromised by irresponsible parties (Goolsby, 2020) [7]. In overcoming this problem, one of the steps that can be taken is to carry out an analysis of the systems and networks at PT. Sadikun Niagamas Raya from an outside perspective or public network. This research focuses on collecting information and testing existing systems using the penetration testing (pentest) method based on the 2022 Open Web Application Security Project (OWASP) framework.

The objectives to be achieved in this research are

1. Security testing of the web domain www.sadikun.com against external attacks carried out by irresponsible people which could harm PT. Sadikun Niagamas Raya.
2. Turn penetration testing results into reports that everyone can understand.

Research Methodology

A. Research Stages

Penetration testing research on the www.sadikun.com domain using the OWASP10 method, there are several steps that need to be carried out, as shown in the flow depicted in Figure 1.

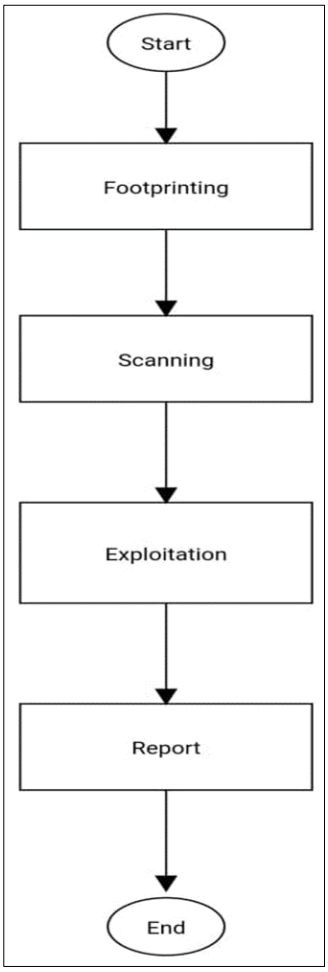

Fig 1: Flow of penetration testing on the website www.sadikun.com

In the initial stage, it is necessary to identify problems based on information obtained from various sources or PT network management. Sadikun Niaga Mas Raya. Identification of this problem can also be based on other sources such as final dissertations or dissertations similar to this research, as well as other supporting information.

After identifying the problem, the next step is to conduct a literature review related to the concept of information security, pentest testing, and networks. Research is carried out by searching for books, theses, scientific research, and various other sources of information available on the internet. The purpose of this literature review is to obtain theories that are relevant to the research being conducted.

The next step is to determine the testing method. At this stage, discussions were held with the supervisor based on the literature review that had been carried out previously. This discussion aims to find a testing method that is appropriate to the research being carried out. After a suitable method has been found, the next step is to carry out the testing phase on a previously determined target.

After the test is carried out, the results will produce data and logs that will be used for further analysis. This analysis aims to find final results and appropriate solutions related to previously identified problems. Next, the final stage is creating a final report which includes all research stages, starting from problem identification, literature review, testing methods, analysis, to final results and recommended solutions.

B. Research Design

Research design is a framework used to plan and carry out penetration testing with clear objectives and structured

methods. This research design helps ensure that testing is carried out in a systematic, consistent, and repeatable manner. The penetration testing research design must be tailored to the specific needs and context of the system or network to be tested. Penetration testing research design involves several stages and components that need to be carefully considered. The following is a more detailed explanation of each component in the penetration testing research design in Figure 2.

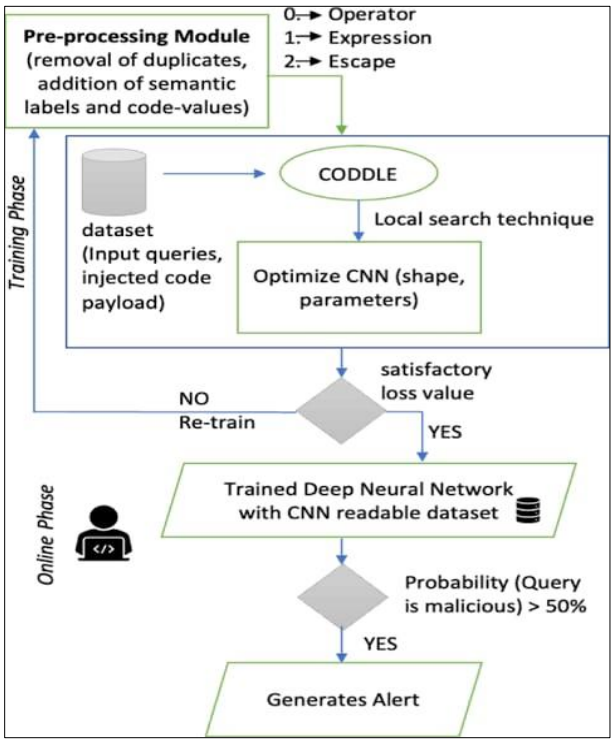

Fig 2: Flowchart of Penetration Testing Stages

C. Research Methods

In conducting pentest research on a website with the subdomain www.sadikun.com, data collection is carried out through several steps. The steps involved in collecting this data include several sources, especially through documents such as journals, books, scientific papers, final assignments, or digital sources such as the internet. Apart from that, information is also obtained through analysis of PT's network infrastructure and systems. Sadikun Niaga Mas Raya, as well as through discussions with the network management of PT. Sadikun Niaga Mas Raya and expert in the field of information security or pentest testing.

1. Research Needs Tools

In this research, several tools were used consisting of hardware and software. The hardware used is a laptop, while the software used is Kali Linux and Python 2.7. Kali Linux is a Debian-based Linux distribution that has various features and tools that are very suitable for conducting pentest testing. Meanwhile, Python is a versatile interpretive programming language, with a focus on code readability making it easier to understand the syntax.

2. Research Flow

This research has a well-arranged flow to ensure that the testing carried out remains focused and in accordance with the plan in order to achieve the expected goals. The following are the steps applied in this research:

1. Foot printing

The first step to mastering the system includes collecting all forms of information about the website with the domain www.sadikun.com. This will be carried out by pentesting by analyzing the website technology used to detect parameters that make it possible to provide vital information in the header.

2. Scanning

After getting information about the target website, the next step is to scan to look for other possible security holes on the website that can be exploited. To carry out this scanning, tools such as the OWASPZap tool are used to analyze security in the header and API Service.

3. Penetration test

Carrying out testing on the website with the domain www.sadikun.com by manual testing using help from HACKBAR and SQLMap to exploit the database.

4. Preparation of test results reports

The process of describing and interpreting test results carried out with the OWASP framework involves determining solutions that are appropriate to the test method.

Results and Discussion

Results

1. Foot printing

The initial stages carried out for penetration testing activities include collecting all forms of information regarding the website with the domain www.sadikun.com, this will be done by analyzing the technology used on the target website, website www. sadikun.com was created with pure PHP

version 7.3.16, the web server used is nginx version 1.14.2, name server jktns1.biz.net.id, jktns2.biz.net.id, ns3.biz.net.id, ns4.biz.net.id and website IP 182.253.0.29.

2. Scanning

The next stage is a scanning process to analyze information on possible security gaps on the target website, from the scanning process (Herfiedhantya *et al.*, 2014) [8] which has been carried out using the OWASPZap automation tool (Pratama, 2019) [10] providing information containing vulnerability alerts on the website consisting of Vulnerable JS Library, Absence of Anti -CSRF Tokens, Application Error Disclosure, Cookie No HttpOnly Flag, Cookie Without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Server Leaks Information via "X-Powered-By" HTTP, X-Content-Type-Options Header Missing, contained The security gap is in the form of XSS on the target website with the domain www.sadikun.com whose vulnerability level is "Medium" as shown in Figure 3.

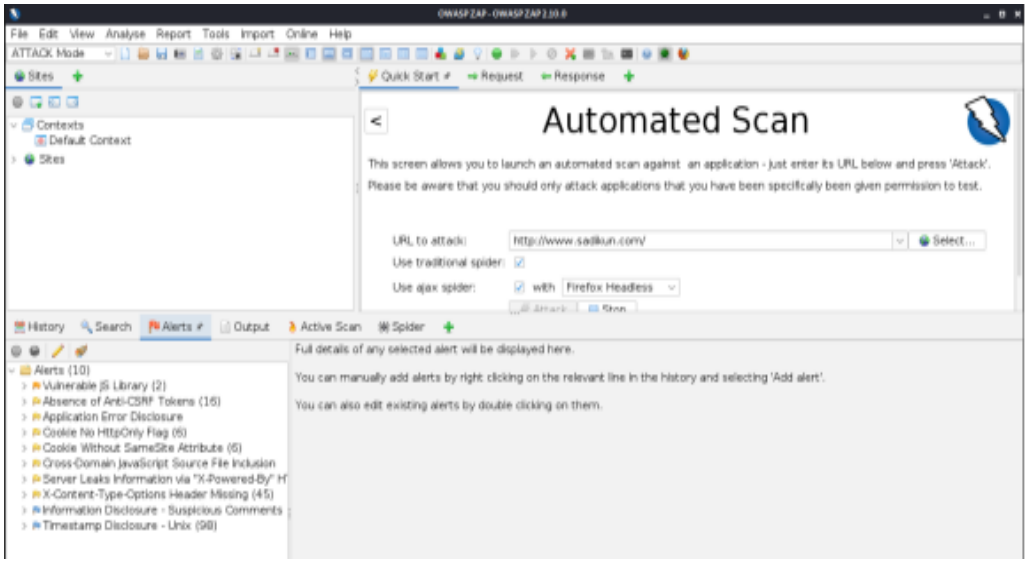

Fig 3: OWASPZap Scanning tool process

The next stage is scanning using NIKTO tools to analyze security gaps that allow access to sensitive files on the web taget that can be accessed freely. Figure 4.

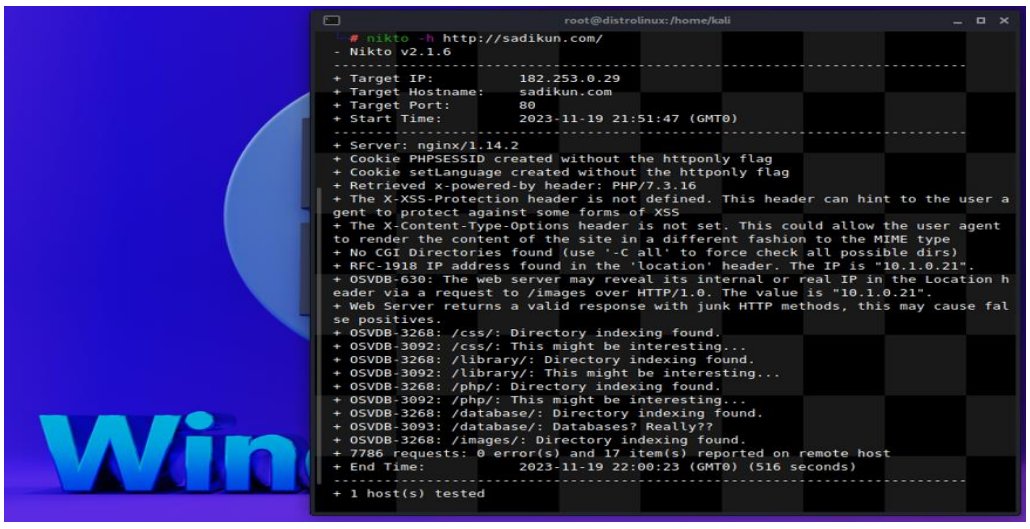

Fig 4: Scanning process using NIKTO tools

Based on Figure 4. Information provided from the NIKTO tool (Dirgahayu, 2015) [3] that there is an error on the target website which results in the attacker being able to freely access files in the server directory such as using the path in the URL in the form of /css/, /php/, / library/ , /images/ , /database/.

3. Test for possible security gaps

The test stage for possible security gaps plays an important role in maintaining information security. The primary function of a security gap test is to identify and evaluate potential security gaps in systems or infrastructure used to store, transmit, or process sensitive information. The results of the Security Vulnerability Test which was carried out manually were that an XSS (Cross Site Scripting) type vulnerability was found which made it possible to insert malicious scripts to be executed on the target website using scripts from JavaScript (Fathur, 2020) presented in Figure 5.

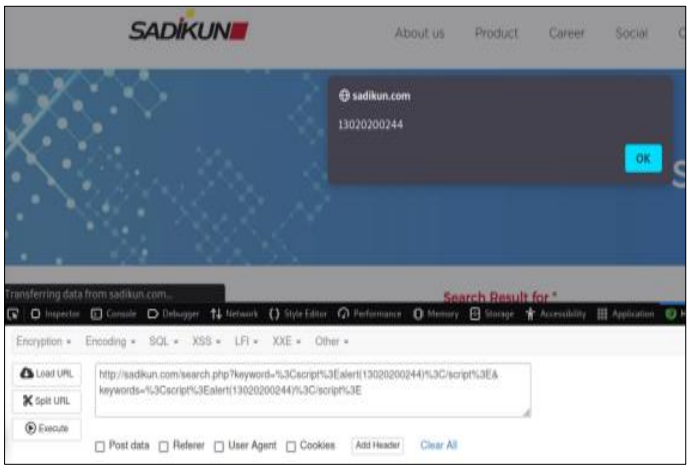

Fig 5: XSS attack injection process

The next stage, namely testing possible SQLinjection attack vulnerabilities, is carried out by infecting the parameters in the target web URL using single quote characters to detect that the target web is vulnerable to SQLinjection attacks (Dirgahayu, 2015) [3] as in Figure 6.

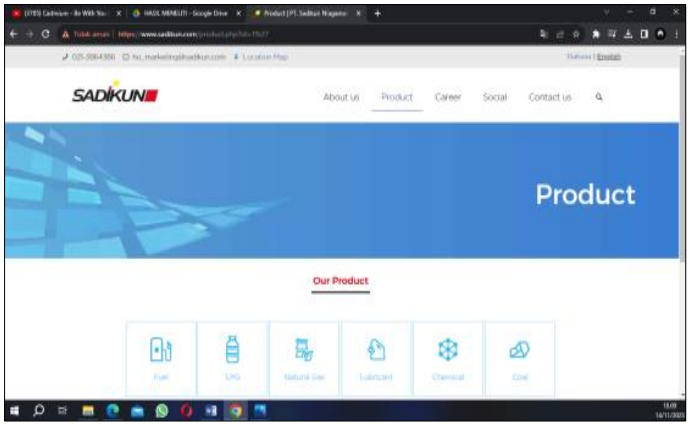

Fig 6: SQL attack injection process

The next process is checking to find out the position of the database on the target web and how many columns the target web database has using the Payload Tools HACKBAR Figure 7.

Fig 7: Checking database columns

The next process is checking the database version on the target website using the payload in the HACKBAR Tools Figure 8.

Fig 8: Checking database version

The process of checking the database name on the target website uses the payload in the HACKBAR Tools Figure 9.

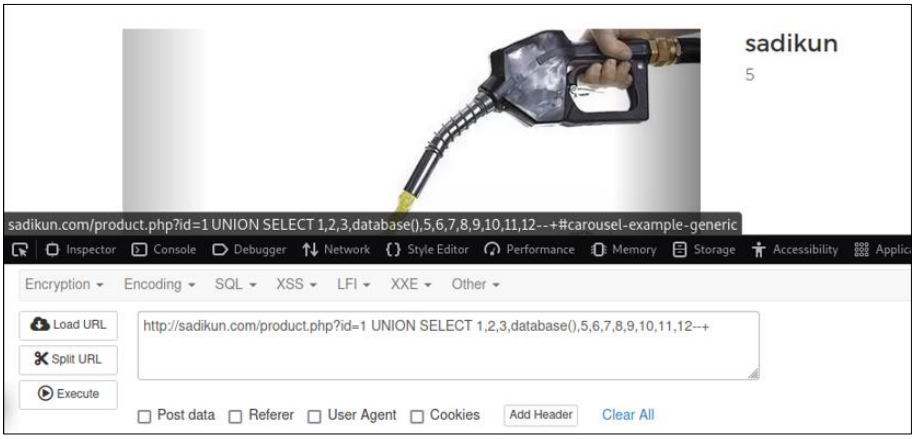

Fig 9: Checking database names

At this stage, we will explain the use of the sqlmap (Dahlan *et. al*, 2013) application which is used to attack the target web database using the syntax of sqlmap –u for parameters that point to the target URL or host and –dbs for enumerating the name of the target web database which will be explained in Figure 10.

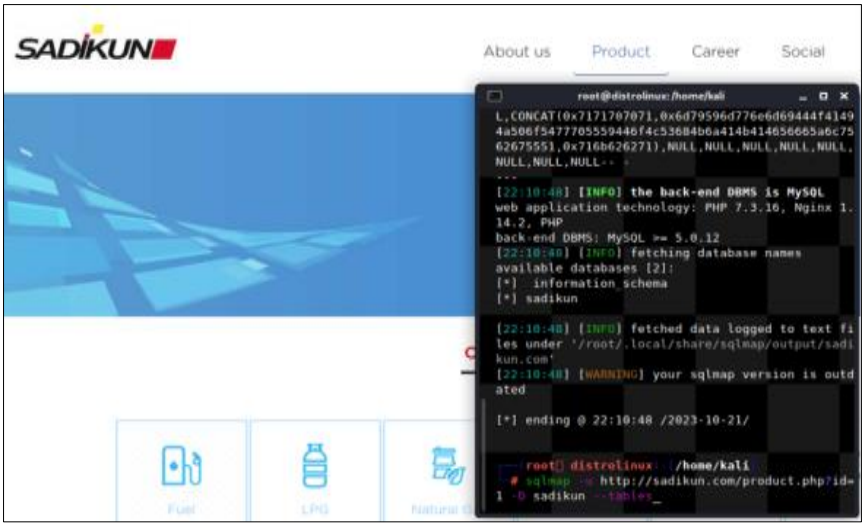

Fig 10: SQLinjection process using SQLMap

From Figure 10, it can be seen that there are two databases, namely information_schema and sadikun. SQLmap provides information that the www.sadikun.com database can be infected with the id parameter using the payload UNION SELECT 1,2,3,database(),5,6,7,8,9,10,11,12--+ The next stage displays a list of database tables on the target website using the syntax sqlmap –u https://www.sadikun.com/product.php?id=1 -D sadikun –tables . SQLmap provides information on a list of tables in the Sadikun database including the tables sdkn_about, sdkn_about_achievment, sdkn_about_achievment_category, sdkn_business_unit, sdkn_career, sdkn_contact, sdkn_footer, sdkn_home, sdkn_navigation, sdkn_product, sdkn_pages, sdkn_product_images, sdkn_slider, sdkn_social, sdkn_top_header, sdkn_user. Figure 11.

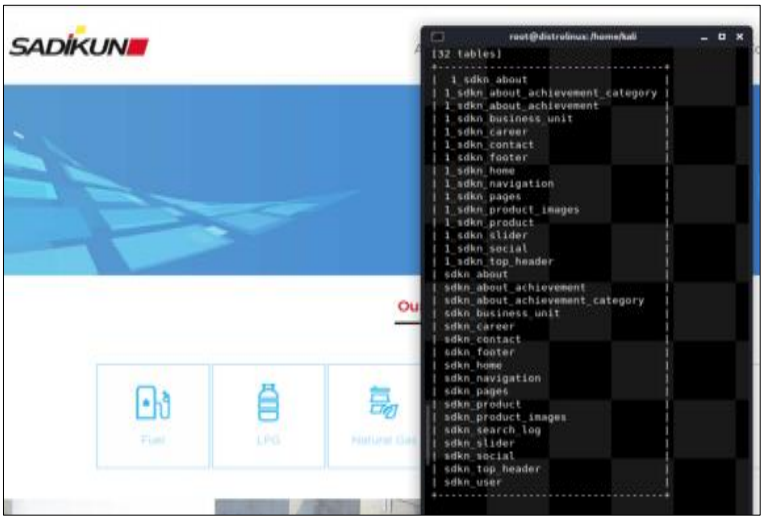

Fig 11: Displays a list of tables in the database

The next stage takes the contents of the user table using the syntax sqlmap –u https://www.sadikun.com/product.php?id=1 –D sadikun –T sdkn_user –dump. SQLmap provides information from the user table which contains username and password Figure 12.

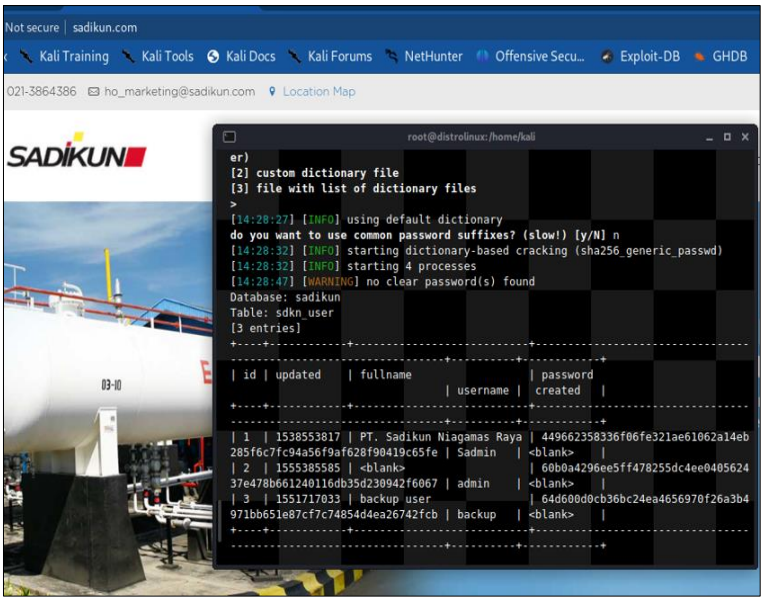

Fig 12: Displays the contents of the user table

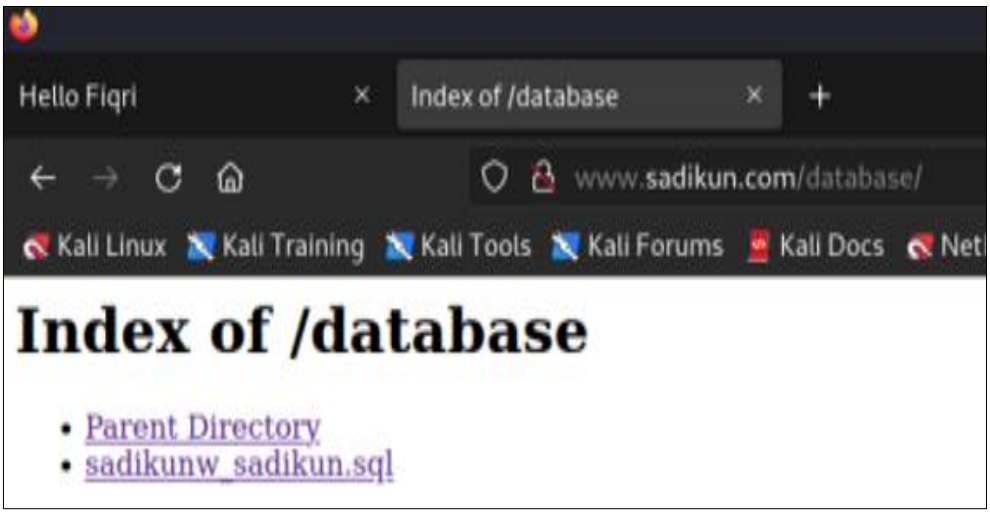

Fig 13: Accessing the database via URL

In Figure 13. The database can be accessed and downloaded on the user's side by using the path /database/ in url (Dirgahayu, 2015) [3]. Attackers can download the database on the website www.sadikun.com by clicking sadikunw_sadikun.sql then the database will be automatically downloaded.

Discussion

The results of the vulnerability analysis that has been carried out using the penetration testing method on the www.sadikun.com domain, there are 3 security gaps, including scripts that can be inserted and executed in the search column, usernames and passwords that can be accessed in the database due to the ID parameters in the The URL is vulnerable to SQL injection attacks, the database can be downloaded via the URL due to a configuration error on the server side (Mustaqbal, 2015) [9].

Based on the OWASP framework which lists the 10 most common and potentially detrimental web application security vulnerabilities. The following is a brief explanation of the vulnerabilities, risks, and recommendations found based on the OWASP Top 10 vulnerabilities framework in Table 1.

Table 1: Types of Vulnerabilities

No	Type of Vulnerability	Risk	Recommendation
1	Cross-Site Scripting (XSS)	This vulnerability occurs when the application does not properly validate or filter user input and allows injection of malicious script code. XSS attacks can allow an attacker to steal user data or run malicious scripts in a user's browser.	Always properly validate and sanitize user input in search input fields. Make sure only expected characters are accepted, and avoid accepting or executing input that contains script code.
2	Injection	This vulnerability occurs when user input is not properly filtered and malicious data can be inserted into commands or queries executed by the application. This could result in SQL, LDAP, or other system command injection attacks	Use parameterized statements or prepared statements to separate SQL statements from user data in the id parameter in the url. By using parameter placeholders, the database can treat input data as values rather than as part of an SQL statement, thereby reducing the risk of SQL Injection attacks.
3	Broken Acces Control	These vulnerabilities occur when access controls are not properly implemented, resulting in users gaining unauthorized access to resources that they should not have access to. This may allow access to sensitive data or functionality that would otherwise be limited.	Always perform authorization checks on the server side before granting access to certain resources or features. Don't just rely on client-side access controls, as this can be circumvented by attackers so they can access sensitive files via the URL path.

Conclusion

The conclusions obtained from this vulnerability testing research are

1. Security testing has been successfully carried out on the web domain www.sadikun.com against external attacks by irresponsible people which could harm PT. Sadikun Niagamas Raya.
2. Has converted penetration testing results into reports that can be understood by everyone.

References

1. Abidin AZ. Penetration Testing Using the Owasp Method (Open Web Application Security Project; c2015.
2. Dahlan M. Testing and Analysis of Website Security against SQL Injection Attacks (Case Study: UMK Website), Research Report, Informatics Technology Study Program, Muria Kudus University, Kudus; c2013.
3. Dirgahayu T, Prayudi Y, Fajaryanto A. Application of the ISSAF and OWASP version 4 methods for testing web server vulnerabilities. NERO Scientific Journal. 2015;1(3):190-197.
4. Dirgahayu RT, Prayudi Y, Fajaryanto A. Application of the ISSAF and OWASP version 4 Methods for Web Server Vulnerability Testing; c2015.
5. Djamalilleil A, Muslim M, Salim Y, Alwi EI, Azis H, Herman. Modified Transposition Cipher Algorithm for Images Encryption. 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), Makassar, Indonesia; c2018. p. 1-4, DOI: 10.1109/EIConCIT.2018.8878326.
6. Fathur M. Tokopedia's Responsibility for Consumer Personal Data Leaks. 2020;2(1):43-60.
7. Goolsby R. Developing a new approach to cyber diplomacy. Future Force. 2020;6(2):8-15.
8. Herfiedhantya. Penetration Test of Gadjah Mada University's Network Security System Using the Information Systems Security Assessment Framework (ISSAF). Yogyakarta; c2014.
9. Mustaqbal. Theoretical Basis for Understanding Black Box Testing; c2015.
10. Pratama IP, Wiradarma AA. Open source intelligence testing using the owasp version 4 framework at the information gathering stage (Case study: X company). International Journal of Computer Network and Information Security. 2019;11(7):8-12.