



## Anticipate Password Security with Burp Suite Using the Brute Force Attack Method

Ika Mei Lina , Gilang Ryan Fernandes

Department of Informatics Engineering, Indraprasta PGRI University, Indonesia, 12530

 [ikameilina.24@gmail.com](mailto:ikameilina.24@gmail.com)

 <https://doi.org/10.37339/e-komtek.v7i1.1162>

Published by Politeknik Piksi Ganesha Indonesia

### Artikel Info

Submitted:

02-05-2023

Revised:

20-06-2023

Accepted:

20-06-2023

Online first :

00-06-2023

### Abstract

Website is one of the information and communication media that requires internet to run. Password generation is still less aware of user security. This provokes cyber criminals to carry out attacks to retrieve user login passwords. One possible attack is a brute force attack by experimenting with all possible passwords. This research aims to discuss brute force attack techniques and how to prevent them so that users can be more careful in creating passwords and be more aware of the security of their passwords. This research shows that the brute force method can work perfectly if there is no Captcha on the web login, limiting logins that do not block accounts for a long time, and not using Two Factor Authentication.

**Keywords:** Brute Force, Burp Suite, Password, Security Analyst, Login

### Abstrak

Website merupakan salah satu media informasi dan komunikasi yang membutuhkan internet untuk menjalankannya. Pembuatan password masih kurang menyadari akan keamanan pengguna. Hal ini memancing para penjahat siber untuk melakukan serangan untuk mengambil password login milik pengguna. Salah satu serangan yang mungkin dilakukan adalah serangan brute force dengan cara bereksperimen dengan semua kemungkinan password yang ada. Penelitian ini bertujuan untuk membahas teknik serangan brute force dan cara pencegahannya agar pengguna dapat lebih berhati-hati dalam membuat password dan lebih waspada terhadap keamanan password yang dimiliki. Penelitian ini menunjukkan bahwa metode brute force dapat bekerja dengan sempurna jika tidak ada Captcha pada login web, membatasi login yang tidak memblokir akun dalam waktu yang lama, dan tidak menggunakan Two Factor Authentication.

**Kata-kata kunci:** Brute Force, Burp Suite, Password, Analis Pengamanan, Login



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

## 1. Introduction

Undeniably, the internet has contributed a lot to the convenience of human life. However, without realizing it, the internet has potential dangers behind the convenience of its use. The website is one of the information and communication media that requires the internet to run. A website is a collection of pages with information presented in text, images, sound, video, and others stored on an internet web server [1]. The website appears because of the increasing community needs in the technology field. Currently, the website is used not only as a company profile but also as a place for buying and selling transactions, discussion forums, and entertainment. With the development of the use of the website, the idea is also developing to secure access to it. One that is widely used is giving a password to log in to get full access to the website.

However, in making these passwords, many internet users still need to learn about their password security level. It can lure criminals in the cyber world to carry out attacks to retrieve the user's login password. One of the possible attacks is a brute force attack. This condition becomes even more vulnerable if internet users are unaware of the importance of password security for themselves and websites that still need to implement CAPTCHA as additional authentication for login security. CAPTCHA is a program that most humans can pass, but robots cannot pass it [2]. CAPTCHA is usually present during the account registration process or in data input to prevent bots from carrying out attacks by creating invalid data entries.

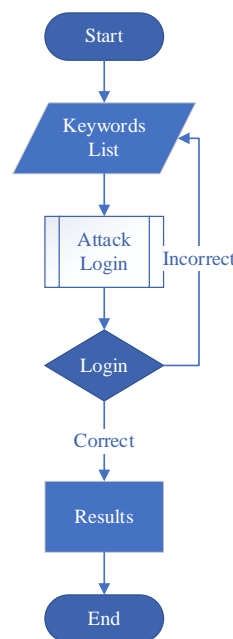
From these problems, the researcher aims to discuss brute force attack techniques and how to prevent them so that users can be more careful in making passwords and be more aware of the security of passwords. A brute force attack is a technique against a computer security system by experimenting with all possible passwords [3]. In the brute force method that will be discussed, researchers use burp suite tools to show how hackers work in carrying out their actions. Then the researcher will provide suggestions and input to create a password that is good and hard to guess using the brute force method.

## 2. Method

The researcher will use the brute force attack method to show how to get the login password so that the user can anticipate and be more aware of the password that will be created. In this study, researchers used a predetermined target, DVWA, a security vulnerability web application intended for education.

## 2.1 Brute Force Attack

A brute force attack is a method hackers use to discover someone's password to get login rights. A brute force attack is an attack that is used when there are no other weaknesses in a system and makes it easier for hackers to break into a system that has a password [4]. A brute force attack is a method used to break passwords or login access with all possible existing keywords [5]. There are various tools commonly used by hackers in this brute force method, one of which the researchers will discuss is the burp suite tool. Brute force attack flowchart is presented in **Figure 1**.



**Figure 1.** Brute Force Attack Flowchart

In the flowchart image above, you can see how brute force works: trying to log in with all the keyword lists the hacker has filtered. The keyword list contains usernames and passwords obtained through research targets. Then the keyword list is tried one by one using the sequential method, starting from the first keyword to the last keyword. The program will provide report results showing that the username and password have successfully logged in.

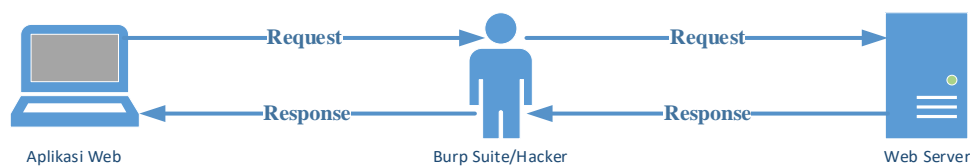
## 2.2 DVWA

In this study, the researcher used a web application called DVWA to test web vulnerabilities using the brute force method. Damn Vulnerable Web Application (DVWA) is a web application using the PHP programming language and MySQL database; this web application is very vulnerable because the primary purpose of this web is to help security professionals test their knowledge using either self-created algorithms or tools. DVWA is an open-source web application made for security and runs on localhost, which is legal. DVWA is

also intended for web developers to learn about web security and can be used as a learning medium for web application-based security systems in academic circles [6]. There is an explanation when using DVWA, where this web application is not recommended to be uploaded to a web server or hosting because it is vulnerable and only used for local servers [7].

### 2.3 Burp Suite

Burp Suite is an application used to perform penetration testing; in this application, there are several features to test the security of web applications. Penetration testing is a sub-category of ethical hacking that aims to evaluate security systems created by simulating attacks based on methods commonly used by hackers [8]. Researchers use this application to implement the attack using the brute force attack method provided by the burp suite application. Burp suite allows users to find gaps contained in a web application, and then a report can be made to the web application owner so that the bugs can be fixed [9]. This application works by utilizing a proxy and interrupting every request and response from communication with a web application [10]. Burp suite diagram is presented on Figure 2.



**Figure 2.** Burp Suite Diagram

The researcher will use the man-in-the-middle (MitM) technique to brute force using the burp suite tools. It can be seen in Figure 2 that the way burp suite works is to make requests to the server by using a proxy as an intermediary between the web application and the web server, then the server will receive the request and provide an HTTP response that is being sent to save the log. The next stage is to look at the logs that have been stored and analyzed to find loopholes or user logins.

## 3. Results and Discussion

The implementation carried out by researchers is to try to find user logins with the brute force attack method using DVWA as a web application for testing attacks and burp suite as its tools. Researchers take this action with the aim that users can anticipate and be more careful in making passwords so that irresponsible people do not easily break into them.

### 3.1 Implementation and Testing

The researcher will implement how the brute force attack method works in the discussion above. The first time researchers carried out brute force was by looking for targets to be attacked, then researching various social media to see the target's identity and other needs. Keyword list is presented in [Figure 3](#).

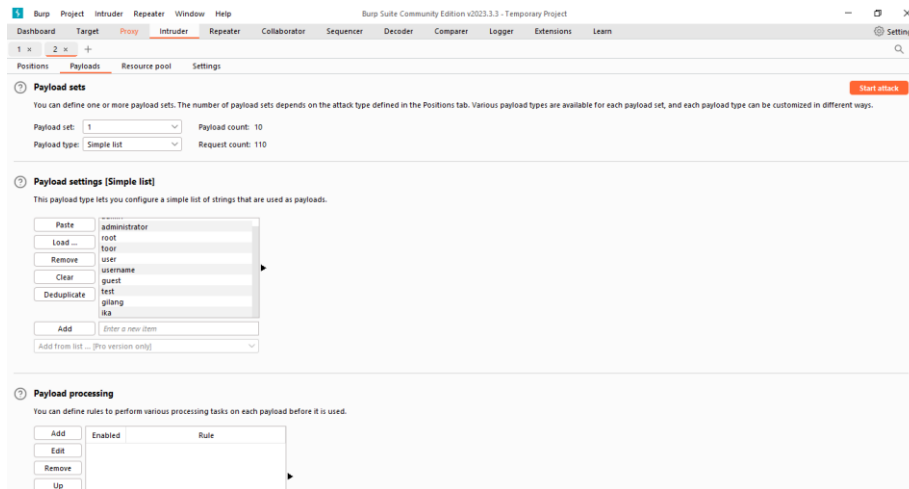


Figure 3. Keyword List

After getting information and habits from the target, the researcher will make a keyword list in the burp suite application on the intruder menu.

In the next step, the researcher will target one of the login websites owned by the target. The website used by researchers this time is DVWA. The researcher will first set up the burp suite by making an intercept on the proxy on the menu, and this step aims to see and analyze the response from the website. Intercept Burp Suite is presented on [Figure 4](#).

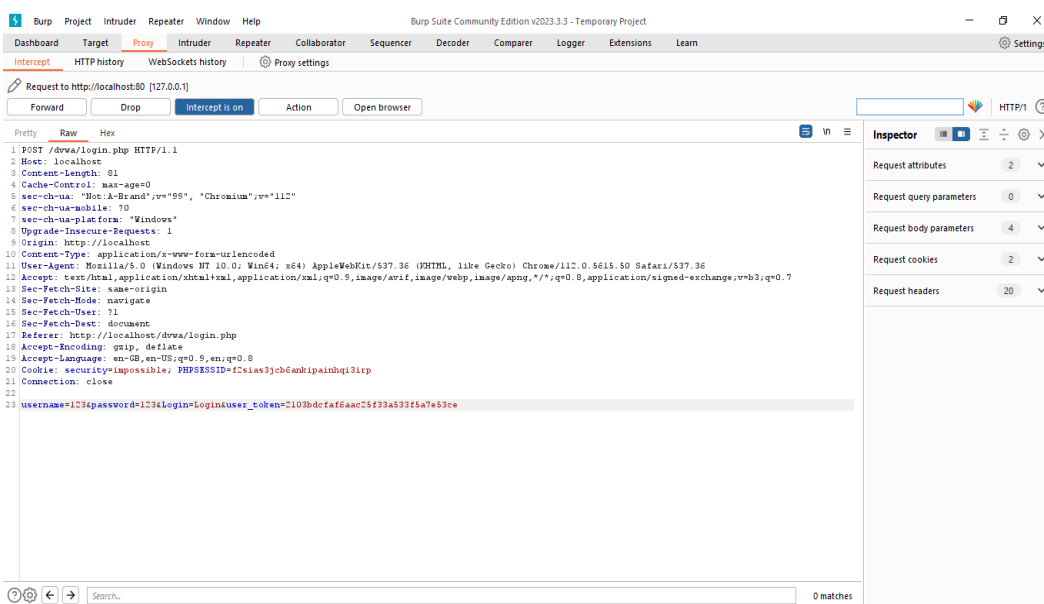
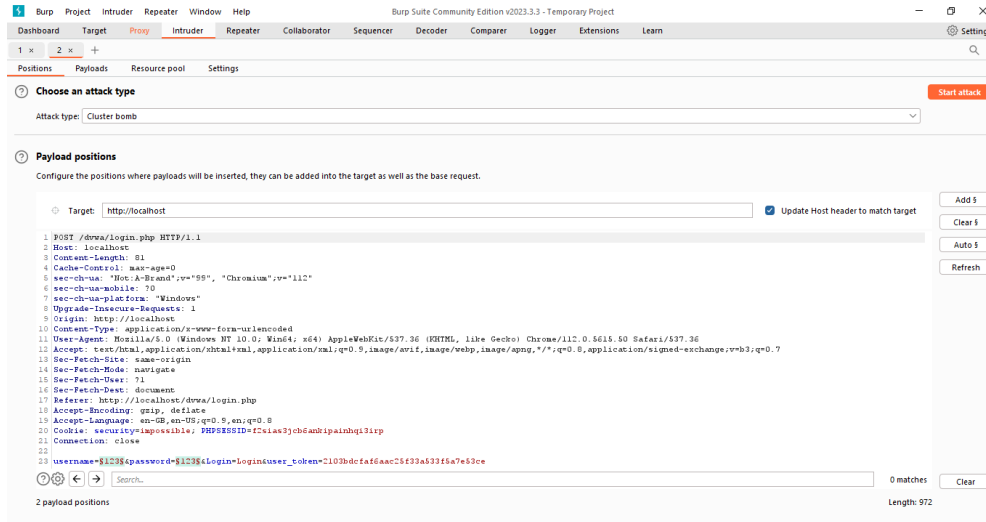


Figure 4. Intercept Burp Suite

When the intercept is activated, a response from the website will be seen, as shown in [Figure 4](#). This intercept is the first step to starting a brute force attack technique.

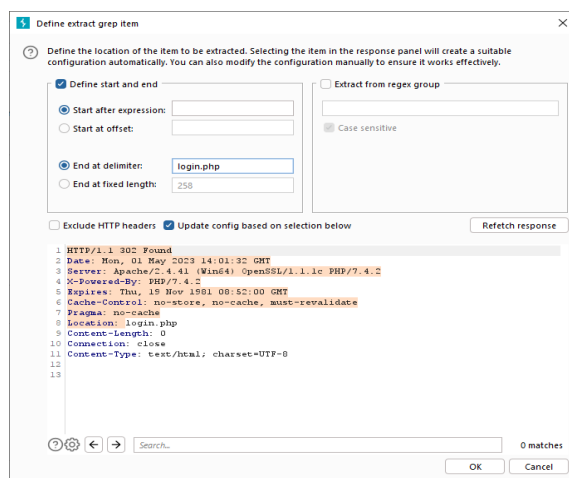
After obtaining a response from the website in raw format, the next step is to send the data to the intruder. Intruder burp suite is presented on [Figure 5](#).



**Figure 5.** Intruder Burp Suite

It can be seen in [Figure 5](#) that there are two menus, namely, attack type and payload position. For the attack type, the researcher chose cluster bomb because the researcher wanted to use the brute force attack method by using the keyword list that was obtained above and on the payload position menu, the researcher would be tagging on line 23 where there is a username and password response, this tagging aims to include keywords list that has been created.

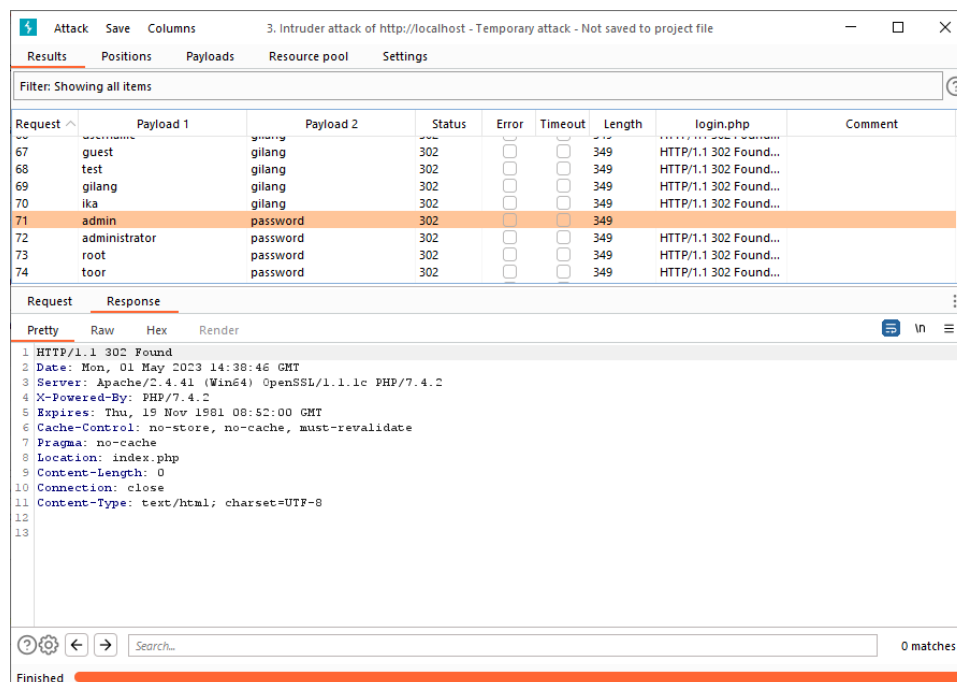
The next step is to do a grep extract contained in the intruder settings menu, and this step aims to see the website's response when carrying out a brute-force attack. Grep item burp suite is presented on [Figure 6](#).



**Figure 6.** Grep Item Burp Suite

In this menu, the researcher prefetches the response to look back at the response on the website. After the results are obtained, the researcher fills in at the end of the delimiter by targeting login.php based on the response location. Researchers use the location to see the results of the brute force attack later.

After setting up the burp suite application, the next step is to attack. When carrying out an attack, the burp suite will provide real-time response data to the website. Attack log is presented on [Figure 7](#).



Request	Payload 1	Payload 2	Status	Error	Timeout	Length	login.php	Comment
67	guest	gilang	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	
68	test	gilang	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	
69	gilang	gilang	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	
70	ika	gilang	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	
71	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	349		
72	administrator	password	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	
73	root	password	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	
74	toor	password	302	<input type="checkbox"/>	<input type="checkbox"/>	349	HTTP/1.1 302 Found...	

Request	Response
1	HTTP/1.1 302 Found
2	Date: Mon, 01 May 2023 14:38:46 GMT
3	Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.2
4	X-Powered-By: PHP/7.4.2
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT
6	Cache-Control: no-store, no-cache, must-revalidate
7	Pragma: no-cache
8	Location: index.php
9	Content-Length: 0
10	Connection: close
11	Content-Type: text/html; charset=UTF-8
12	
13	

**Figure 7.** Attack Log

In the picture above, it can be seen that the burp suite has started to attack with the keyword list that was created before. There is a response from the website as follows HTTP/1.1 302 Found, and it can be inferred that the response was a failed login because researchers are targeting login.php. On line 71, there is an empty response, whereas if the response is analyzed in the response menu, there is line 8 in a different location, namely index.php. It indicates that the keyword list with the username "admin" and the password "password" was successfully logged in. target website (DVWA).

### 3.2 Anticipate Brute Force Attacks

In the discussion above, the researcher has implemented how a brute force attack is carried out. On this occasion, researchers will discuss handling brute force attacks for users and web application developers.

On the user side, you can handle it by not providing detailed information on social media or other website applications, and users can use usernames and passwords that are hard to guess. Passwords that are hard to guess usually combine uppercase letters, lowercase letters, symbols, and numbers. A good password also consists of a minimum of 8 combination characters. The researcher will give an example of how to make a good password that is hard to guess.

## **Gilang Dosen Universitas Indraprasta**

Figure 8. Creating Password

As seen in Figure 8, the researcher uses a sentence that is easy to remember, and then the researcher will take the letters in the preamble of the sentence. From the picture, the researcher has marked in red which words you want to take to create a password so that it becomes "GilDosUnindra."

The next step is to replace vowels with numbers and also add symbols. The following is the result of the password combination that was created. Password combination is presented **Figure 9**.

**G1lD0s\*n1ndr@**

**Figure 9.** Password Combination

As seen in the picture above, researchers replace several letters with numbers and symbols. It aims to make passwords difficult to guess and attack using brute force.

On the web application developer side, you can anticipate this attack by limiting logins so that when you fail 3 to 5 times, it will be blocked, and it will take time to try to log in again. This technique aims to stop brute force attack attempts. The next step developers can take is to use a captcha (Completely Automated Public Test to Tell Computers and Humans Apart), so that login can only be done by the user and not a program or tool used by hackers to carry out brute force attacks. Developers can also use Two Factor Authentication, where this method can avoid brute force techniques carried out by hackers by confirming from other devices and the OTP code.

These methods can avoid brute force attacks so that users can secure their accounts more optimally, and the developer can also help protect accounts from this technique in their web applications.



#### 4. Conclusion

In the explanation above, it can be concluded that every website has weaknesses. Therefore password security from the user side is critical because the more difficult the password is to guess, the more difficult the password is to crack. The burp suite application can make it easier for hackers to carry out brute force attack techniques by combining all the possibilities in the keyword list to find the target username and password.

Besides that, awareness of account security from the user and developer side is needed because this burp suite tool is straightforward to use even for ordinary people. The brute force method can work perfectly without Captcha in the web login. The login limit does not block the account long enough and does not use Two Factor Authentication. Therefore it is essential to implement various security measures in using the web to avoid any possible losses.

#### References

- [1] D. F. Murad, N. Kusniawati, and A. Asyanto, "Aplikasi Intelligence Website Untuk Penunjang Laporan Paud Pada Himpaudi Kota Tangerang," *CCIT J.*, vol. 7, no. 1, pp. 44–58, 2013, doi: 10.33050/ccit.v7i1.168.
- [2] M. Fikry and M. Iskandarsyah, "Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) Menggunakan Pendekatan Drag and Drop," *J. Sains, Teknol. dan Ind.*, vol. 2, no. 1, pp. 64–70, 2016.
- [3] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 52–55, 2016.
- [4] M. R. Sampurna, "Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA: Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA," *J. Netw. Comput. Appl. ...*, vol. 1, no. 2, pp. 25–33, 2022.
- [5] K. Daya *et al.*, "Pengamanan File Gambar Menggunakan," *TECHSI - J. Tek. Inform.*, vol. 10, no. 1, pp. 155–162, 2018.
- [6] M. Affandi and S. Setyowibowo, "Implementasi Snort sebagai alat pendeteksi intrusi menggunakan Linux," *Teknol. Inf. Teor. Konsep, dan Implementasi J. Ilm.*, vol. 4, no. 2, pp. 98–112, 2013.
- [7] Digininja, "GitHub - digininja/DVWA: Damn Vulnerable Web Application (DVWA)." <https://github.com/digininja/DVWA> (accessed Apr. 28, 2023).
- [8] A. Hidayat and I. P. Saputra, "Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia.Net, Tanjung Harapan Lampung Timur)," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 118–124, 2018.
- [9] A. Subari, S. Manan, E. Ariyanto, and A. Fauzi, "Pemanfaatan Metode Wavs (Web Application Security Scanners) Menggunakan Burp Suite Tools Dalam Audit Teknis

Keamanan Sistem Informasi Surat Tugas Sekolah Vokasi Undip,” *Gema Teknol.*, vol. 21, no. 4, pp. 125–130, 2022.

- [10] E. Listartha, G. Arna, J. Saskara, D. Gede, and S. Santyadiputra, “Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications,” *Sci. Comput. Sci. Informatics J.*, vol. 4, no. 2, pp. 1–14, 2021.