Jurnal E-Komtek
Vol. 8 No. 2 (2024) pp. 286-293
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Website Penetration Testing with SQL Injection Technique Using SQLMAP on Termux

Gilang Ryan Fernandes[1], Ika Mei Lina[2]

[1,2]Informastics Engineering, Universitas Indraprasta PGRI, Indonesia, 12530

gilang.fernandes@gmail.com

https://doi.org/10.37339/e-komtek.v8i2.2074

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
02-10-2024
Revised:
23-12-2024
Accepted:
24-12-2024
Online first :
26-12-2024

Abstract

Websites make it easier for us to find information or do our daily work. Almost all companies have websites, be it company profiles or application websites. With the development of technology, some programmers forget about website security. Websites with security weaknesses can be easily hacked, such as changing appearance to taking essential data. One thing to watch out for is external factors in the form of attacks carried out by hackers using the SQL Injection technique. This technique can find and take all databases stored on the website server. The purpose of this study is so that programmers and companies, in general, can be more careful with this attack so as not to experience losses from both the company and the consumer side. The results obtained in this study show that SQL injection attacks can cause significant losses because they can modify and take over the database on the attacked website. This tool also runs automatically so that laypeople without an understanding of hacking can carry out this attack. Thus, programmers can secure their websites using techniques to secure SQL Injection attacks.

Keywords: *SQL Injection; Hacking; SQLMap; Website; Termux*

Abstrak

Website memudahkan kita dalam mencari informasi maupun mengerjakan pekerjaan kita sehari-hari. Saat ini sudah hampir semua perusahaan mempunyai website, baik itu web company profile maupun web aplikasi. Dengan berkembangnya teknologi membuat beberapa programmer melupakan keamanan pada website. Website yang memiliki kelemahan keamanan bisa sangat mudah diretas, seperti merubah tampilan, hingga pengambilan data-data penting. Salah satu yang perlu diwaspadai yaitu faktor eksternal berupa serangan yang dilakukan oleh hacker dengan teknik SQL Injection. Teknik tersebut dapat mengetahui serta mengambil semua database yang tersimpan pada server website. Tujuan dari penelitian ini agar programmer dan perusahaan pada umumnya dapat lebih berhati-hati dengan serangan ini agar tidak mengalami kerugian baik dari sisi perusahaan maupun konsumen. Hasil yang didapat pada penelitian ini adalah serangan SQL Injection dapat memberikan kerugian besar, dikarenakan serangan ini dapat memodifikasi dan mengambil alih database pada website yang diserang. Tools ini juga berjalan secara otomatis sehingga orang awam tanpa pemahaman hacking bisa dapat melaukan serangan ini. Dengan demikian programmer dapat mengamankan websitenya dengan cara melakukan teknik-teknik untuk pengamanan serangan SQL Injection.

Kata-kata kunci: *SQL Injection; Hacking; SQLMap; Website; Termux*

1. Introduction

Websites today can also be called windows to the world, where all the information we need can be searched and read via the internet. Websites can make it easier for us to find information or do our daily work. A website makes it easier to do anything mobile because we don't need to carry laptops and computers everywhere. Almost all companies have websites, be it company profiles or application websites, as a need for their company. With the increasing development of technology, some programmers sometimes forget about website security. Data is a valuable asset significantly impacting various sectors, from government business to people's daily lives [1].

Websites with security weaknesses can be quickly taken over by irresponsible people, such as the appearance of the website that can be changed or the taking of essential data. This will cause various negative impacts on the company, including data taken and the loss of user or consumer trust. Therefore, its security is necessary in creating and building a website. Internal or external factors can cause weaknesses in a system or website [2]. One thing to watch out for is external factors in the form of attacks often carried out by hackers using the SQL Injection technique. This attack allows hackers to create SQL queries that can be used to retrieve and change databases [3]. This technique is one of the methods used to hack a website. With this technique, a hacker can find and take all the databases on the target website server. By using a framework such as Laravel or Codeigniter that already has security in it, it is possible that this attack can be carried out because the latest version of SQLmap installed on Termux Android can have advantages in scanning the framework. The website server stores various files and website components [4]. Data taken with this attack technique can harm companies and website users. Therefore, researchers will discuss in detail how this technique can work and how to prevent it. The purpose of this study is so that the public, especially programmers and companies in general, can be more careful with this attack so as not to experience losses from both the company and the user.

2. Method

In this study, the author uses SQL injection techniques to find security holes in a website. With the SQLMap tool, the author will conduct security testing on the Acunetix Acuart website, where this test aims to learn and provide a way to handle it. Thus, we can find out how dangerous the technique is on the website. SQL injection method can be presented in **Figure 1**.

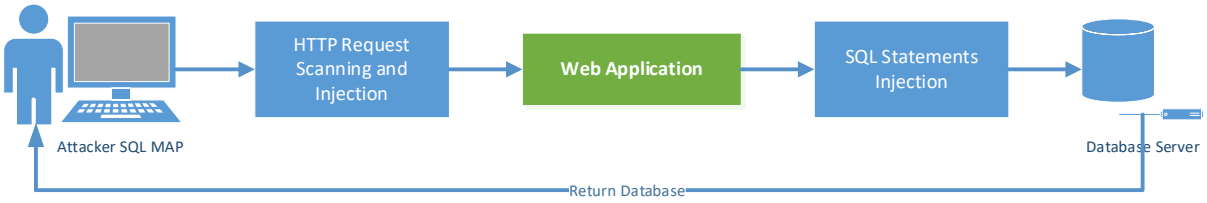

Figure 1. SQL Injection Method

The image above shows the SQL Injection method used in this research to take over a website's database.

2.1. SQL Injection

SQL Injection is an attack method that targets web servers by utilising SQL code to manipulate databases [5]. This technique is a way to check database vulnerabilities on a website. This SQL injection is one of the attacks or crime threats in the digital world. This technique works by entering a parameter or query statement on the website to find errors and get the user or website database.

2.2. Website

A website is a collection of web pages used to share information in the form of writing, videos, images, and other information that can be accessed by anyone using the Internet. A website can also be interpreted as a form of communication through mass media with an internet network that can provide specific information and can be accessed by many people. [6]. Currently, websites are developing rapidly and are a step for companies to introduce their business to everyone. Websites have many types, ranging from static to dynamic websites; even now, creating a website can be done without coding using a Content Management System (CMS). A Content Management System (CMS) is a system that contains a collection of programming languages and is made into one to manage the content of a website. [7].

2.3. Termux

Termux is a Linux terminal emulator that runs on the Android operating system. This application can be installed and run directly without rooting the Android smartphone. [8]. Termux is popular among Android fans because it can run scripts based on Python, C, Bash, and others.

2.4. SQLMap

This tool is the most famous tool and functions to help hackers search and find website security holes, especially database holes. This tool can automatically detect database security holes on a website. This SQLmap uses Python, so it runs very lightly and quickly. SQLMap is

an open-source application with the best algorithm to exploit SQL Injection weaknesses and can take over the database server. [9].

2.5. Acunetix Acuart

Acunetix Acuart's website is owned by Acunetix and is used to test cyber attacks. This website is intentionally made to have many security holes so that people can learn system security legally. The Acunetix Acuart website is used for security testing or cyber-attacks. [10]. Acuart has several holes, including the Sql Injection XSS security hole.

3. Results and Discussion

When implementing, the researcher used a method that did not violate the law and was legal because the website that tried to perform SQL Injection was the Acunetix Acuart website, which is specifically for security testing and learning. Implementing SQL Injection is a learning and awareness of the website we create to avoid hacker attacks, especially SQL Injection attacks.

3.1. Implementation and Testing

Based on the discussion above, the researcher will implement penetration testing on the Acuart website using the SQL injection technique. When carrying out a SQL Injection attack, the first thing to do is to find a security hole on the website. Acuart website is presented in **Figure 2**.

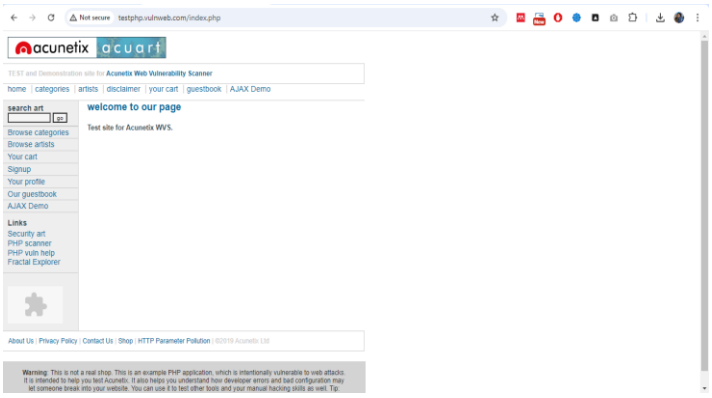

Figure 2. Acuart Website

The image above shows the Acuart website that will be targeted for SQL Injection attacks. The website's appearance is minimalist, with no visible security holes. This is where penetration testing or hackers analyse the targeted website to find security holes or bugs. Finding bugs is presented in **Figure 3**.

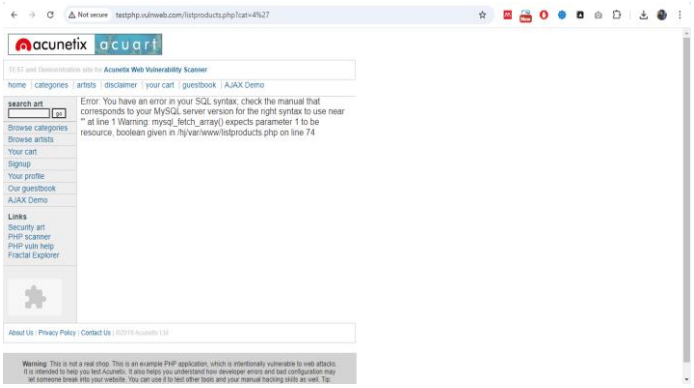

Figure 3. Finding Bugs

During further investigation regarding security or bugs on the website, a security gap was found, marked by an error message on the product list page. The error occurred because the author entered an exploit parameter on the website domain, so a gap was found, which led to an SQL database error.

To ensure the error was a security hole or bug, the researcher conducted further exploitation using Termux. SQLMap on Termux is presented in Figure 4.

Figure 4. SQLMap on Termux

In Figure 3, the termux layer that has installed the SQLMap tool is visible, whereas in the figure, SQLMap activity is testing and searching for security from the Acuart website. SQLMap is a powerful tool for carrying out SQL injection attacks, and it automatically finds targeted SQL security holes.

When running the SQLMap tool, the database results from the Acuart website, namely the Acuart database and information_schema, are displayed. It should be noted that information_schema is a default database from SQL, so our target is the accurate database. The Exploit database is presented in Figure 5.

Figure 5. Exploit Database

The researcher exploited the database with the name Acuart to see the tables in the database. After exploiting the database with SQLMap, there are 8 tables: artists, carts, categ, featured, guestbook, pictures, products, and users. Because the researcher wants the username and password to log in to the website, the researcher chooses the user's table as the next table exploitation to get the columns in the table. Exploit tables are presented in Figure 6**.**

Figure 6. Exploit Tables

In the image above, the author exploits the user's table to see its columns. After exploitation using SQLMap, several columns and their data types exist. It can also be seen in image 5 that in the user's table, the columns name, email, pass, and uname are the next targets to be exploited so that the contents of each column can be displayed.

The next step is to enter parameters into SQLMap to find the users' column table contents. The exploit column is presented in Figure 7.

Figure 7. Exploit Column

After entering the parameters in SQLMap, the user column results are obtained. This data is very important and valuable and must be protected because it includes data such as name, email, username, and password, which can also be accessed on the Accuart website to log in. This website has weaknesses besides SQL Injection, one of which is that password data has no data encryption protection. That way, hackers can log in to the website very easily.

3.2. Anticipate SQL Injection

There are several ways to handle the SQL injection security gap itself. The first is to validate data input, where the programmer ensures that all data received by the website or application is validated before being sent to the database. This validation can be done by checking the data type and removing special characters and input length. The second step can use the prepared statement by separating the SQL query from the input data. The third is the SQL Escape String, which ensures that the input data cannot be interpreted as part of the SQL query. The fourth step is to turn off error notifications. Next, to avoid SQL Injection attacks, you can secure the database by granting access rights according to the user's role. The sixth step is to use the Web Application Firewall (WAF) and Intrusion Prevention System (IPS), which can help detect and prevent these attacks by filtering suspicious requests. Next, when creating a website application, make it a habit to encrypt crucial data such as usernames, passwords, and other vital data.

The steps above can help to anticipate hacker attacks with SQL Injection techniques. Programmers can also choose a framework if they want to build a website-based application because it already has features to help programmers solve security holes that can endanger websites and companies hacked by hackers.

4. Conclusion

Based on the discussion and analysis above, it can be concluded that this SQL Injection attack has a significant impact on the company because, with this attack, hackers can easily take the database on the attacked website. It can be seen above that attacks with the SQL Injection technique can be done with an Android smartphone. SQLMap is a hacking tool that can run automatically according to the desired command, so finding gaps on the targeted website does not take long. The many data leak incidents experienced by several companies have made researchers want to provide knowledge about website attack techniques, one of which is SQL Injection. Researchers conducted this penetration testing to instil the importance of securing data on the website application that was created so that there would be no more data loss experienced by several companies recently.

References

[1] R. Al Ihsan and B. A. Sekti, "Pentingnya Keamanan Data Dalam Era Digital : Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia," pp. 2–6, 2023.

[2] W. Wahyudin, H. Kuswara, R. Resti, and S. Dalis, "Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales," *Comput. Sci.*, vol. 4, no. 1, pp. 44–52, 2024, doi: 10.31294/coscience.v4i1.2978.

[3] N. Bhateja, S. Sikka, and A. Malhotra, "A Review of SQL Injection Attack and Various Detection Approaches," *Smart Sustain. Intell. Syst.*, no. November 2017, pp. 481–489, 2021, doi: 10.1002/9781119752134.ch34.

[4] Fatul Faatihah *et al.*, "Analisis dan Evaluasi Terkait Keamanan pada Web Server," *J. Ilm. Sains dan Teknol.*, vol. 2, no. 7, pp. 73–77, 2024.

[5] A. Riyanti, B. M. Rahmanto, D. R. Hardianto, R. D. A. Yuristiawan, and A. Setiawan, "Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 9, 2024, doi: 10.47134/pjise.v1i4.2623.

[6] Y. Z. Surentu, D. M. D. Warouw, and M. Rembang, "Pentingnya Website Sebagai Media Informasi Destinasi Wisata Di Dinas Kebudayaan Dan Pariwisata Kabupaten Minahasa," *Acta Diurna Komun.*, vol. 2, no. 4, pp. 1–17, 2020, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/actadiurnakomunikasi/article/view/31117/29843

[7] A. A. A. Ushud, I. Novita, and N. Juliasari, "Pelatihan Pemanfaatan CMS Untuk Pembuatan Website Bagi OrangTua Siswa Sekolah Alam Tangerang," *JAM-TEKNO (Jurnal Pengabdi. Kpd. Masy. TEKNO)*, vol. 2, no. 1, pp. 20–25, 2021.

[8] Andria and I. Mubarok, "Pengujian Keamanan Basis Data Sistem Informasi Berbasis Web," *Semin. Nas. Apl. Sains Teknol.*, no. Prosiding SNAST 2021, pp. 66–74, 2021, [Online]. Available: https://ejournal.akprind.ac.id/index.php/snast/article/view/3392/2459

[9] B. Damele A. G. and M. Stampar, "SQLmap: automatic SQL injection and database takeover tool." https://sqlmap.org/ (accessed 1 November 2024).

[10] Z. A. Anwari, I. G. P. Wedana, J. Deva, K. D. D. Widyaputra, G. A. J. Saskara, and I. M. E. Listartha, "Analisis Kerentanan Pada Suatu Website Menggunakan Tools Xspear, Xsscon, Dan Pwnxss," *J. Inform. Teknol. dan Sains*, vol. 4, no. 4, pp. 406–412, 2022, doi: 10.51401/jinteks.v4i4.2104.