Website Hacking: SQL Injection Method And Its Prevention

U.Nanaji¹, K.T.Mahesh Babu², P.Sai Sampath³

¹Associate Professor, Dept. of CSE, KL University, Vaddeswaram, AP, India
²Final Year B. Tech, Dept. of ECM, KL University, Vaddeswaram, AP, India
³Final Year B. Tech, Dept. of ECM, KL University, Vaddeswaram, AP, India

Abstract— In the Internet, the websites has an important role to fulfill user requirements. These websites are maintained to be secure. The third person may hack a website without knowledge of developer and they may do any fraudulent activities on the website. The websites can be hacked by using any one of the hacking mechanisms such as SQL Injection, Command Injection, Local File Inclusion injection, and etc... The website may use personal details of it's users in online environment. These personal details must be secured. There are many types of mechanisms are available to secure the websites and user's data. This paper makes a survey about such types of protection mechanism and makes awareness to the people.

Keywords—Hacking, SQL Injection, Website.

I. INTRODUCTION

The Art of exploring various security breaches is termed as Hacking. Computer Hackers have been around for so many years. Since the Internet became widely used in the World, We have started to hear more and more about hacking. Only a few Hackers, such as Kevin Mitnick, are well known. In a world of Black and White, it's easy to describe the typical Hacker. A general outline of a typical Hacker is an Antisocial, Pimple-faced Teenage boy. But the Digital world has many types of Hackers. Hackers are human like the rest of us and are, therefore, unique individuals, so an exact profile is hard to outline. The best broad description of Hackers is that all Hackers aren’t equal. Each Hacker has Motives, Methods and Skills. But some general characteristics can help you understand them. Not all Hackers are Antisocial, Pimple-faced Teenagers. Regardless, Hackers are curious about Knowing new things, Brave to take steps and they are often very Sharp Minded.

Ethical Hacking is testing the resources for a good cause and for the betterment of technology. Technically Ethical Hacking means penetration testing which is focused on Securing and Protecting IT Systems. SQL Injection is one of the most common vulnerability in web applications today. It allows attacker to execute database query in url and gain access to some confidential Information etc...( In shortly). SQL injection refers to the act of someone inserting a MySQL statement to be run on your database without your knowledge. Injection usually occurs when you ask a user for input, like their name, and instead of a name they give you a MySQL statement that you will unknowingly run on your database.

SQL Injection [1] is a type of web application security vulnerability in which an attacker is able to submit a database SQL command which is executed by a web application, exposing the back-end database. A SQL Injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. The specially crafted user data tricks the application into executing unintended commands or changing data. SQL Injection allows an attacker to create, read, update, alter, or delete data stored in the back-end database. In its most common form, a SQL Injection attack gives access to sensitive information such as social security numbers, credit card number or other financial data. According to Vera code’s State of Software Security Report SQL Injection is one of the most prevalent types of web application security vulnerability.

II. About Website Hacking

Hacking website means altering or manipulating the website content or database i.e. manipulate website contents say CSS or Java scripts , leak its users database,
corrupt its database, deface the website's index page, exploit the anonymous login and much more... Hacking websites is nowadays became a fashion among the Hackers. They hack the website and deface its index page to display their own custom defaced page, mostly for popularity. There are several website Hacking techniques like Injection attacks i.e. SQL Injection, Command Injection, Local File Inclusion injection, X Path Injection, arc injection, Cross site scripting attacks, Cross site scripting forgery attacks, Header manipulation, hackingrootdirectories, bypassing registratio n, unblocking websites , Hacking premium accounts, Cookie based attacks, domain hijacking and much more involved in achieving the abovementioned.

The files of your website are stored on a computer somewhere. The computer, called a "server" or "web server",[2] is not too much different from your home PC, except that its configuration is specialized for making files available to the world wide web, so it has a lot of hard drive capacity and a very high speed internet connection. It probably doesn’t have its own monitor or keyboard because everyone who communicates with it does so through its internet connection, just like you do.

Your website and server have several security systems that determine what kind of access each person has. You are the owner, so you have passwords that give you read/write access to your site. You can view files (read) and you can also change them (write). Everybody else only has read access. They can view your files, but they are never, ever supposed to be able to change them, delete them, or add new ones.

A hack occurs when somebody gets through these security systems and obtains write access to your server, the same kind you have. Once they obtain that, they can change, add, or delete files however they want. If you can imagine someone breaking into your home and sitting down at your PC with a box of installation CD's, that’s what a website hack is like. They might do only a little damage, or a lot. The choice is up to them. Altering the page was simply the thing they chose to do after they got in. Once they get in, they can do ANYTHING, including alter your pages that are pure HTML. That is the reason why, after a hack, the most important thing isn’t repairing the damage they did (which most people focus on), but finding out how they got in. Website hacking is one of the modern enterprises of organized crime, but if you think that means it’s being done amateurishly by a bunch of elderly mobsters who took night classes in Computer ABC’s to learn what "this Internet Explore thing is", think again. These organizations have professional programmers. Their campaigns to take control of thousands of the world's computers are well planned and sophisticated, drawing on an in-depth knowledge of operating system software, browser vulnerabilities, programming, and even psychology, and their attacks are almost always automated. Strangely enough, if your site was hacked, it probably wasn’t done by a person, but by another computer, which was hacked by another computer, which was hacked by yet another, and somewhere way back in the chain is a programmer who initially unleashed the sequence of events that set all these computers to attacking each other and building a giant network, a "botnet", a massively parallel virtual supercomputer whose purpose is to suck up all of the world's information that the criminals can efficiently turn into money. They need to have as many computers as possible recruited into the enterprise, and that’s why they wanted to hack your little website.

III. SQL Injection

A SQL injection attack exploits vulnerabilities in a web server database that allow the attacker to gain access to the database and read, modify, or delete information. SQL Injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command which is executed by a web application, exposing the back-end database. A SQL Injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. The specially crafted user data tricks the application into executing unintended commands or changing data. SQL Injection allows an attacker to create, read, update, alter, or delete data stored in the back-end database. In its most common form, a SQL Injection attack gives access to sensitive information such as social security numbers, credit card number or other financial data. According to Vera code’s State of Software Security Report SQL Injection is one of the most prevalent types of web application security vulnerability.

Input validation on the SQL Injection:

There are measures that can be applied to mitigate SQL injection attacks. Web developer can check whether some suspicious characters are sent from the Login Page like ‘’, ‘‘, ‘‘, ‘‘, ‘‘, etc. Always store the Passwords in the Database server in the Encrypted Form. Use of these practices does not guarantee that SQL injection can be completely eliminated, but they will make it more difficult for Hackers to conduct these attacks.
Fig. 1. Attacks input validation can help prevent.

Prevention:

SQL injection can be prevented if you adopt an input validation technique in which user input is authenticated against a set of defined rules for length, type, and syntax and also against business rules. You should ensure that users with the permission to access the database have the least privileges. Additionally, do not use system administrator accounts like “sa” for Web applications. Also, you should always make sure that a database user is created only for a specific application and this user is not able to access other applications. Another method for preventing SQL injection attacks is to remove all stored procedures that are not in use. Use strongly typed parameterized query APIs [4] with placeholder substitution markers, even when calling stored procedures. Show care when using stored procedures since they are generally safe from injection. However, be careful as they can be injectable (such as via the use of exec () or concatenating arguments within the stored procedure).

IV. Proposed Technology

For quite some time now hackers have used SQL injection attack methods to quickly find and exploit website vulnerabilities and effectively spread malware. In order to prevent SQL injections, enterprise information security teams must go above and beyond the old SQL defense of testing and patching Web application code.

We can prevent hacking a website through sql injection by patching the code developed by the programmers.

V. Conclusion

Even though the Usage of internet had become essential now a day. The Security issues are not that much convincing, so the website developers must take care by patching the code thoroughly during the development stage only.

REFERENCES

[1] SQL INJECTION:
[3] Input Validation: Referred from the text “Hacking for Beginners”.
[5] SQL INJECTION BASICS:
[6] SQL Injection Walkthrough
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
[7] Sql injection What is It?
http://www.acunetix.com/websitesecurity/sql-injection/
[8] Stop SQL Injection Attacks Before They Stop You