Security and Privacy Issues in Application from SQL Injections

Priyanka Gupta, Anupam Sharma

Abstract: Today's Web Application Attacks are very common issues. In a 2012 study, it was observed that the average web application received 4 attack campaigns per month, and retailers received twice as many attacks as other industries. Web Application Security is the branch of Information Security it deals with security of websites, web applications and web services.

Keywords: SQL Injection, Cross Site Scripting, Cross Site Request Forgery.

I Introduction

SQL injection is one of the most common factors causing serious threats to any database and application. When an unauthenticated user injects some code into our website to invade it with an intention to steal, erase or modify our database, injection occurs. It can be easily taken care of but mostly goes unnoticed.

How to prevent SQL Injection: There are many methods to fight sql injection, but the best method is to believe in a basic fundamental that no data received from any the other user can validate all our inputs.

Cross Site Scripting

XSS is a common method used by most of the malicious users to inject code in our website in order to steal our client data base, install unscrupulous softwares on our computer. A recent survey indicates that more than 80% of the users hampered were attacked by XSS only.

How to prevent XSS: First of all one must validate the inputs and avoid any malicious attempt to threaten our data base. Though whatever websites made by Wubble are properly screened and different methods are put in place to safeguard our data.

Injection through E- mail:

This is a simple method adopted by the malicious user. It is mostly over looked by us as it becomes very difficult to check the mail from the address only. In such a case the injected mail forces our website to send many emails to our contacts causing spam mails. We may become a defaulter for sending spam.

How to seek prevention from such mails: The best and the only method available to avoid such a threat is by the user himself. The user must be vigilant and has to be alert and should check the authenticity of the mail.

ISSN: 2278 – 1323

Malicious upload of a file and its execution:

The malicious user can send the data in any form to upload. Any upload on the website can cause such a harm to the database. If the malicious user is successful in uploading a malicious file, they gain full control of our database.

Prevention from such malicious uploads: The file name and the nature of the file must be validated before storing such a file on the website the harmful data sent through such an upload can be in a form of an image or a word document. So before executing such an action one needs to be watchful.

User authentication is a must:

In any database there is a certain type of data that needs protection, say credit card or bank account details. It is imperative that we should properly secure an informationwhich is private, if it is to be shown to one group and has to be hidden from the other. The highly sensitive data must be coded in some form or the other. In such cases it become highly important to keep our data in an encrypted form and make it safe. Encryption needs years to be cracked down by malicious users.

II Literature Survey

Web Application Security by SQL Injection DetectionTools, March 2012

AtefehTajpour , Suhaimi Ibrahim, Mohammad Sharifi describes the SQL injection is a type of attack which the attackeradds Structured Query Language code to a web form input box to gain access or make changes to data. SQL injection vulnerability allows an attacker to flow commands directly to a web application's underlying database and destroy functionality or confidentiality.

SQL Injections – A Hazard To Web Applications, June 2012

Neha Singh, Ravindra Kumar Purwar describes and define SQL Injections, illustrate how SQL Injections are performed. In addition we have also surveyed the various SQL Injection detection and Prevention tools and well-known attack methods. Finally, we have provided our solution to the problem and have assessed its performance.

SQL INJECTION Attacks in Web Application, January 2013

Mihir Gandhi, JwalantBariadiscuss about Advance SQL Injection (ASQLIA) first of all it identifies which type of attacks according to that prevention measures are suggested .Some New features are added to it Web Crawling ,Web Services and Advance SQL Injection (ASQLA)which will emphases more Security of Web Application. In short enhancing database security with the aspect of web developer is main aim of my paper.

IIIDiscussion on Security and Private Issue

To corrupt database content or to access the information, the attacker use application code which can be accessed by using SQL injection method. The attacker in such a case can alter, delete, read or create our data stored the database. SQL injection is one of the most widely used web application to cause peril to database.

ISSN: 2278 – 1323

XSS: CROSS SITE SCRIPTING:

Through client site, say for example, Java script, Cross Site Scripting (XSS) taps a user database by injecting a malicious code into the output of a web application. The desire then gets hold of the site and manipulate the data. XSS can divert the user to malicious sites, hijack the data or deface the site in some way.The attack leaves no evidence behind, since a forged request contains all of the information and comes from the same IP address as a real request from a victim.

BROKEN AUTHENTICATION & SESSION MANAGEMENT

The authentication details of the user and session identifiers need to be properly protected. The attacker can assume the identity of a user in case of a live session in such cases. So the Broken Authentification and Session Management caters to many security issues.

INSECURE DIRECT OBJECT REFERENCES

When a web application exposes a reference to an internal implementation object, insecure object reference takes place. Internal implementation object means database, record, files or database keys in the website. The attacker can get access to user's personal data the moment an application takes a reference to one of these objects in URL.

SECURITY MISCONFIGURATION

The lack of attention or maintenance to the web application configuration cause threat of vulnerabilities by Security Misconfiguration. There has to be a secure configuration for any framework, database server, application server and platform. It gives the attacker a chance to access your private details and corrupt the complete database.

CROSS-SITE REQUEST FORGERY (CSRF)

Cross Site Forgery (CSRF): It is a perilous attack where a user is trapped and is made to perform an action he didn't attempt to do otherwise. Hence a third party web user sends a request to a website posing that the user is already authenticated. The attacker then takes accessibility of the victim's browser. Social media, Browser E-mail chats, online banking, and web interfaces are the common victims.

Security features:

1. Check Authentication: Verify what your identification is and who you are. It makes sure that you are the authorised and person to logon to your Internet Banking account.

2. Authorization: By doing so it authorises you to manipulate your resources or accounts in a certain fashion. By this any fiddling with the funds can be checked easily.

3. Encryption: By encryption, the data in the database can be made foolproof.

4. Auditing: It keeps a record of any operation. The businessman can use it as a valid proof of any specific merchandise sale.

5. Integrity: It prevents unauthorised data modification by any third user.

6. Nonrepudiation: It is a sort of prevention against any one party from reneging on any agreement after the fact.

ISSN: 2278 – 1323

7. Availability: It is a prevention against any delay in the data or its removal.

Encryption Problems:

Encryption is another way of securing the data on the web. A 'public key' scheme is used that allows any data to be transmitted between two users who are not known to each other. In any database there is a certain type of data that needs protection, say credit card or bank account details. It is always cumbersome for the attacker to decrypt the encrypted data.

Injection: SQL, OS and LDAP are the flaws that are Injection flaws, They occur when any untrusted data is received as a part of the query or a command. The hostile command can trick the user to get trapped and become vulnerable to database threat.

Broken Authentication and Session Management: session Management and authentication method is normally defied and not implemented by the user. It allows the attacker to compromise passwords, session tokens or exploit the key information from the webmaster.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Cross-Site Scripting (XSS): It is commonly known as XSS. This error occurs the user accepts the untrusted data and makes use of it. Any uploading of pictures or the mail can cause XSS easily. It is a type of malicious exploit of a **website** where unauthorized commands are transmitted from a user that the **website** trusts. CSRF is another example of how the security industry is unmatched in its ability to come up with scary names.

Insecure Direct Object References: This happens when the user exposes a file, directory or database. In such a case the attacker can access control to the database and manipulate these references and make use of the data.

IV Result

The security settings for such headers should be strictly implemented and adhered to. Additionally the latest softwares can also be used to check any potential risks. The confidential data such as bank details or passwords for debit cards etc are mostly go unprotected during web applications. The malicious users hijack such data and cause credit card frauds, crimes and identity deface to the user. Such data should be properly protected and encrypted so that the potential invasion by any such attacker can be tackled. For such attacks a foolproof good security system is required for the frameworks, application servers, web server, database etc.

V Conclusion

A CRSF attack forces an online user to send forged HTTP request including authentication information to a vulnerable web application. This gives the attacker to force the innocent user's browser to generate requests which appear legitimate and become an easy trap. Web applications usually redirect and forward the users to other web pages and websites and in turn use untrusted data from many sources. If used, such a data can redirect threats of phising, malware etc causing serious threat to the database at the website. If a sensitive

ISSN: 2278 – 1323

and vulnerable component is exploited, such attacks are a serious threat to the data base of the victim causing harassment and humiliation.

References

[1] AtefehTajpour , Suhaimi Ibrahim, Mohammad Sharifi, "Web Application Security by SQL Injection Detection Tools", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012

[2] Neha Singh, Ravindra Kumar Purwar, "SQL Injections – A Hazard To Web Applications", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSE), Volume 2, Issue 6, June 2012

[3] Mihir Gandhi, JwalantBaria, "SQL INJECTION Attacks in Web Application", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[4] AtefehTajpour, Suhaimi Ibrahim, Maslin Masrom, "Evaluation of SQL Injection Detection and PreventionTechniques". International Journal of Advancements in Computing Technology (IJACT), 2011, Korea.

[5] DialloAbdoulayeKindy and Al-Sakib Khan Pathan,"A Survey based On Sql Injection: Vulnerabilities, Attacks, And Prevention Techniques", Department of Computer Science, International Islamic University Malaysia, Malaysia

[6] Prasant Singh Yadav,Dr pankajYadav, Dr.K.P.Yadav "A Modern Mechanism to Avoid SQL Injection Attacks in Web Applications",IJRREST: International Journal of Research Review in Engineering Science and Technology ,Volume-1 Issue-1, June 2012.

BIBLIOGRAPHY

Priyanka Gupta is Master of Computer Application and Management. She is currently working in teaching profession. She has an area of interest in Security schemes.

Anupam Sharma is Master in technology in Computer Science and Engineering. He has interest in filed of Cryptography and Information Security.

ISSN: 2278 – 1323