International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON WEB APPLICATION ATTACKS

Peruru Vanaparthi Sai Likhitha[1], Prof. Raghavendra Prasad[2]

Student, Department of Information Science and Engineering, RV College of Engineering, Karnataka, India
Professor, Department of Information Science and Engineering, RV College of Engineering, Karnataka, India

---

Abstract - *Web applications are a universal way to access information in today's world. Since the number of people using the internet rises exponentially every day, along with that the attacks that can be performed on web applications also rises, so security is becoming a very serious issue in web applications in today's world. Developers and researchers have found a lot of mitigations and protective measures for web application attacks on both client side and server side, and there are also many approaches to detect attacks that can be possible on websites and prevent them also. This paper provides various web application attacks which are very popular these days like cross site scripting (XSS) attack, Commerce attacks, SQL injection attacks and Distributed Denial of Service attacks, the preventive measures and mitigations that can be taken to prevent these attacks.*

Key Words: **Web Application attacks, Cross site scripting attacks, SQL Injection, Distributed Denial of Service attacks, Commerce attacks, Web Security**

1. INTRODUCTION

Web applications are basically computer programs that allows clients to request and retrieve data from the database over the internet using their preferred web browsers. The retrieved data is presented to the user in the dynamically generated web pages which will be written in HTML and CSS. Since the number of people who uses these web applications rises exponentially, it's an active and appealing target for attackers to attack these web applications to get client sensitive data such as credit card numbers, phone numbers or making client to perform exactly how attacker wants them to. There are lot of ways to mitigate all these web application attacks. As per Open Web Application Security Project (OWASP) injection attacks are more fatal and dangerous attacks these days, basically client submits data to web applications in the form of forms or text data and submit, attackers insert SQL queries or java script code in the ongoing data to server side and web browsers just execute this queries and Java script code and provide results to the end user. So attacker can get all the information that Injection attacks he wants from these injection attacks. And one more major attack is distributed denial of service attack where the attacker just floods the server with enormous amounts of requests which are popularly known as Bots.

The top 10 vulnerabilities of OWASP according to 2020 are:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfigurations
- Cross Site Scripting
- Insecure Deserialization
- Insufficient Logging and Monitoring
- Distributed Denial of Service attacks.

Injection attacks tops the list even till today. It happens when the attacker injects any sql code and send it to the backend and backend executes the query but it the not the normal behavior of the web application and attacker gets hold of the data very easily and lot of preventive measures can be taken to prevent such injection attacks. Cross site scripting attacks involves attacker injecting script code and the end users browser have no idea to know that this script is not trusted and browser executes the script and script can contain code to access the sensitive data of end users or access the cookies or any other data and there are 3 types of XSS attacks:

- Reflected XSS
- DOM based XSS
- Stored XSS

Commerce attacks are basically done on E-commerce websites wherein attacker get hold of customer details like credit card numbers, phone numbers and any other customer information and to mitigate credit card theft web applications actually X-out the data and show only last 4 digits of credit card numbers to end users for confirmation purposes.

2. CROSS SITE SCRIPTING ATTACK

Cross site scripting attacks includes attacker injecting script in the end user data like form data or input text or comments field. But the browser has no way to know that it is not trusted and browser thinks that server might have sent that script and executes the script and script might have written to access cookies or any sensitive information about end users. If attacker gets hold of cookies he can create session with that cookie and access data from server and server has

no way to recognise the trusted end user and attacker since attacker will also be injecting cookie in every request.

There are three types of XSS attacks like stored XSS, Reflected XSS and Dom XSS. Stored XSS takes place when the injected script gets executed every time the user launches the web page and it is most dangerous XSS attack and also known as Persistent attack. Reflected XSS attacks is not permanent attack and it happens only when there is a particular event like when end user clicks on particular link or any other event and also known as Non persistent attack.

The preventive measures can be to filter the input data to server as strictly as possible and block the request if there are any java script code and to prevent XSS in HTTP responses make use of content-type headers to make sure that web browsers interpret the response in the way we intend to.

3. SQL INJECTION ATTACK

SQL Injection attack is an injection based attack which takes advantage of the security vulnerability which exists at database level of any web application. This attack occurs when attackers inserts SQL keywords or SQL queries in input which is being submitted to server. And without proper filtering of input server can execute this query can then attacker have a illegitimate access to the database and he can access any information which includes end users passwords and sensitive information.

When attacker gets holds of input source which is being used by end user, he can perform various types of SQL injection attacks

1. Piggy backed queries:

In this particular type of attacks, basically attacker adds extra query to already existing query and this extra query will be executed as part of initial query itself. For Example:

SELECT NUMBER FROM CONTACT WHERE NAME="XYZ" AND PASSWORD="ABC"; DROP TABLE NUMBER;

When above query gets executed, It will drop the table Number also. So using this type of attacks attacker can drop or add tables however attacker wants.

2. Logically Incorrect Queries:

The main important goal of this type of attacks is to get to know the most useful information and facts about the database itself like number of columns or number of tables or label and type of every column and all.

3. Union Query:

It is also known as statement injection attack. It can be accomplished by embedding union query so that when database returns, it returns the union of original query and added query. For Example:

SELECT * FROM NUMBER WHERE NAME='' UNION SELECT * FROM ADMIN AND PASSWORD="ABC"

Here query turns into union of two queries and first query doesn't return anything and second query returns all the details about the admin table in database.

The preventive measures for SQL Injection attack can be to filter the input as strictly as possible and can use web application firewalls which includes the rules to detect and block requests which contains SQL queries. And can use appropriate privileges which means not to connect to database with admin privileges unless and until it's compelling to do so.

4. COMMERCE ATTACK

All commerce attacks includes E-commerce skimming, Credit Card Fraud which is basically very difficult to trace and detect, usually detecting the fraudulent transaction itself is not an easy task since websites perform some thousands of transactions every day. There are few things based on which we can suspect about the fraud like a successful transaction after many unsuccessful attempts, Customer's IP address is not really in the same location as billing information on that particular order. To prevent credit card fraud to some extent these days web applications X-out the credit card number and show only last four digits of the credit card.

5. BROKEN AUTHENTICATION AND SESSION MANAGEMENT

This happens whenever there is session hijacking or fake authentication. And developers these days use various encryption algorithms and session management tokens to prevent these attacks and end user has to mandatorily include session token or cookie in each and very request that they send to backend server. To prevent broken authentication few requirements has to be met

Password to login must be in minimum length and it must be difficult to get by brute force attacks and must be strong to include special characters, digits and all. Number of attempts to login must also be restricted to 3 or 4 because authorized users won't try to attempt more than 3 times even though if they forget their password. User must have chance to change their password and also mechanism must require old password to change it to new password and altering phone number and email address must be strictly restricted. And

password must be stored either in encrypted or hashed form to prevent from attacking it.

When client connects to backend, server provides cookie or session ID for that particular session and requires users to include this in each and every request they make and thee tokens must be random and should not be easy to acquire and server must keep changing these tokens at particular time intervals and notify end users about the change. And session ID cannot be exposed in URL at any cost, if attacker gets hold of session ID then attacker can include that session ID in every request he makes to backend and backend will not have any idea on who is legitimate user and who is not.

The preventive measures for broken authentication and session management is to make use of very strong passwords and restrict number of attempts to login and to make use of SSL certificates to encrypt the data that does from web browser and web server. And SSL certificates which are being used by web server has to be signed by trusted certification authority.

6. DISTRIBUTED DENIAL OF SERVICE ATTACKS

Distributed Denial of service attack involves overwhelming the web server with lot of traffic and disrupt the normal traffic pattern. DDOS attacks can be performed effectively when attacker gets control of lot of computer systems and write automated script to perform attacks which are basically known as Bots. But there are both good bots and bad bots and need to block bad bots. The attacker has a control over all bots and called botnet. And attacker can send instructions and every bot in botnet, after finding out IP address of victim, every bot will start sending requests to that particular IP address.

This can be blocked by using mechanisms such as device fingerprinting which basically collects all parameters about the device and see if it is an emulator and can pose captcha to user for first request and it's very difficult for the bot to solve the captcha challenges. And one more preventive measure is to use ML model which can figure out bots by user interactions with the application.

7. CONCLUSION

SQL Injection, Cross Site Scripting attacks are the most vulnerable and dangerous attacks these days and considered most common web application attacks that attackers tend to perform to get hold of information about the end user. Most organisations and companies are providing lot of tools to prevent web application attacks like web application firewall which basically is placed between client and server to prevent all these web application attacks. With the exponential increase in web application attacks it is very important for framework and tools like web application firewall for the prevention of web application attacks so that better services and experience can be provided to the end users who uses web applications to retrieve data.

Securing end user data is very important these days so it's very important that end users to be aware of all these types of attacks and also companies to make their firewalls to be very efficient in protecting end users and blocks the attacker from attempting to do any web application attacks like injection attacks, XSS attacks, Form field consistency and CSRF attacks and encourage clients to make use of web application firewalls in case they are dealing with sending requests and retrieving sensitive data on daily basis.

8. FUTURE ENHANCEMENTS

To provide better services for the end users security of their data is very important over the web applications. The main aim of any developer is to provide their work over web but also developer has to take care in securing the end user data and the future work will include tool to actually detect these vulnerabilities and provide mitigations and block those requests.

REFERENCES

[1] Nilesh Kochre, Satish Chalukar, Santosh Kakde, "Survey On SQL Injection Attacks And Their Countermeasures ", International Journal Of Computational Engineering And Management, Vol -14, October 2011.

[2] Hossain Shaihriar and Mahammad Zulkernine, "S2XS2: A Server Side Approach To Automatically Detect XSS Attacks", Ninth International Conference on Dependable, Automatic Secure Computing, IEEE, 2011.

[3] Sruthy Mamadhan, Manesh T, Varghese Paul, "SQLStor: Blockage of Stored Procedure SQL Injection Attack Using Dynamic Query Structure Validation" 12th International Conference on Intelligent Systems Design and Applications (ISDA), IEEE, Nov. 2012, PP. 240-245.

[4] Jaskanwal Minhas, Raman Kumar, "Blocking of SQL Injection Attacks by Comparing Static and Dynamic Queries" in International Journal Computer Network and Information Security, vol.2, 2013 PP.1-9.

[5] Gao Jiao, Chang-Ming XU, JING Maohua "SQLIMW: a new mechanism against SQL-Injection" in Proc. Of 2012 International Conference on Computer Science and Service System, 2012, PP. 1178-1180.

[6] Yousra Faisal Gad Mahgoup Elhakeem , Bazara I. A. Barry," Developing a Security Model to Protect Websites from Cross-site Scripting Attacks Using Zend Framework Application", International Conference on Computing, Electrical and Electronics Engineering (ICCEEE), August 2013, PP. 624-629

[7] Takeshi Matsuda, Daiki Koizumi, "Cross Site Scripting Attacks Detection Algorithm Based on the Appearance Position of Characters", 5th International Conference on Communications, Computers and Applications, IEEE, October 2012, PP. 65-70.