TECHNIQUES FOR ATTACKING WEB APPLICATION SECURITY

Rutvi Pradipkumar Adhyaru

Faculty of Computer Science & Applications, CHARUSAT, Changa, Gujarat

ABSTRACT

The web is absolutely necessary part of our lives. It is wide platform which is used for information sharing and service over internet. They are used for the financial, government, healthcare, education and many critical services. Everyday billions of user purchase items, transfer money, retrieve information and communicate over web with each other. Although the web is best friend of users because it provide anytime anywhere access to information and services at the same time. All things are created by human in the world so its reality that the things created by man are little bit problematic. So web applications are also created by human so it contains too many loopholes. The popularity of applications allure hackers towards them. Now a Days Securing and maintaining the websites against attack is very hard and challenging task. Finding loopholes in Web application, Computer system or network and exploiting them called hacking. New approaches for web attacks are invented day to day so the study of detect and prevent against web application attack and finding solution is important part in internet world. In this paper we introduced all web application based attack including two major attacks like XSS (Cross Site Scripting) and SQLI.

KEYWORDS

Web Application Attacks, Web Security, Vulnerability.

1. INTRODUCTION

Web application security and cyber security is Current, demandable and hot career field subject. The World Wide Web becomes most important and global information medium in the world. It quickly becomes most dominant way to provide access to online services. User use web based applications to search data, exchange message, interact with each other, conduct business, and perform financial operation and many more. For many users the web is very easy to use and convenient because it provide 24 – hour anytime, anywhere access to information and service for all concerned the stakes are high: A)business : that derive increasing income from internet commerce. B) Users: Those who trust web application with sensitive information. C) Criminals: Those who can make big money by stealing payment details or compromising bank accounts.

2. PROBLEM OF WEB SECURITY

An important security research problem is how to enable user who is running a client on an untrusted platform to securely communicate with the web application. Because some people want to do business with insecure site. Some organization or companies don't want to give the information about their own security holes. So, it's very hard task to get the reliable information about the state of web security today. Too many sites are there that did not authenticate users

DOI : 10.5121/ijist.2016.6205

because there was no need. Each user treated in a same way and was presented in same information [4]. Any security threats arising from hosting a website were related largely to vulnerabilities in web server software. If an attacker compromises a web server he would not gain access to any sensitive information because the information held on the server was already open to public view. An attacker typically would modify the files on the server to deface the website's contents. No user want to use web application if she believes her information will be disclosed with unauthorized parties.

3. WORKING OF WEB APPLICATION

Web applications are computer program allowing website visitors to submit and retrieve data to database over the internet using their preferred web browser. The World Wide Web consists of websites and websites were collection of web pages [16]. There are mainly two types: 1) Static: a web page is one that does not change when a user request it. The web server sends the page to

the requesting web browser without modifying it. 2) Dynamic: It's modified by server before it

is sent to the requesting browser. Web browsers were invented as a means of retrieving and displaying these documents. Web page contain HTML, images, script code and become more user friendly but also exploits security loopholes. Each web application is different and may contain unique vulnerability. Web application is mainly created to perform practically useful functions you could possibly implement like,

- Web mail services : Gmail, yahoo, Hotmail
- Interactive information : Wikipedia
- Social networking : Facebook, Myspace, hi5.com, twitter, LinkedIn, classmates
- Shopping : Amazon, flip kart
- Weblogs : blogger
- Online calendars : Google calendar, o2 calendar, yahoo calendar
- Online telephone directory : yellow.com, whitepages.com, anywho.com

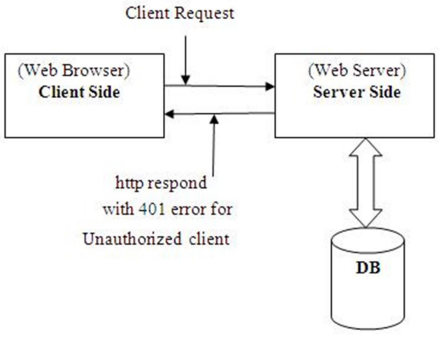

Figure 1: Working of Web Application

At client side, client sends request to particular task than at server side, client's request processed with web server using dynamic HTML pages through execution or interpretation[6]. If user is authorized then server provides appropriate response to the client request otherwise it responds with 401 errors for non-authorized client. It's called http authentication and then web application interact with backend database for storing and retrieving data. The programming language, state maintenance, logic implementation and design differentiate web application from others. Generally attacker attacks via Application Layer. Attacker sends attack inside valid http request. Firewall, patching, IDS and SSL cannot detect or stop attack inside http request.

4. MISCONCEPTIONS REGARDING SECURITY

Some security misunderstandings are there,

- Firewall protects my web server and database.
- The IDS protects my server and database.
- IDS configured to detect attacks.
- Honey pot catches the attackers.
- SSL secure my site.
- SSL secure transaction of data between web server and browser of user.

These all misconceptions are wrong. SSL does not protect against the server and applications but SSL is the hacker's best friend due to false sense of security. There is one beautiful sentence said by John Viegel and Gary McGraw that "Malicious hackers don't create security holes; they simply exploit them. Security holes and vulnerabilities – the real root cause of the problem – are the result of bad software design and implementation."

5. REASONS FOR ATTACKING WEB APPLICATIONS

Currently there are many privacy risks in web applications. Today too many websites are hacked by anonymous. They target website because of different types of reasons. They are mentioned in table 1.

Attack Goal	%
Stealing Sensitive Information	42%
Defacement	23%
Planning Malware	15%
Unknown	08%

Deceit	03%
Blackmail	03%
Link Spam	03%
Worm	01%
Phishing	01%
Information Warfare	01%

Table 1: Reasons for Attacks [12]

6. WEB APPLICATION VULNERABILITY

There are several different types of attacks used by hackers. These types of attacks and its usage are mentioned in following Table 2.

Attack/Vulnerability Used	**% of use**
SQL Injection	**20%**
Unintentional Information Disclosure	**17%**
Known Vulnerability	**15%**
Cross Site Scripting (XSS)	**12%**
Insufficient Access Control	**10%**
Credential/Session Prediction	**08%**
OS Commanding	**03%**
Security Misconfiguration	**03%**
Insufficient Ant automation	**03%**
Denial Of Service	**03%**

Redirection	**02%**
Insufficient Session Expiration	**02%**
Cross Site Request Forgery(CSRF)	**02%**

Table 2: types of Attacks [12]

This all are the Vulnerability types and how much it's usage. The SQL Injection and Cross Site

Scripting are the most famous vulnerabilities in web application. Generally web servers, application servers, and web application environment are affected to following types of vulnerabilities. The OWASP (Open Web Application Security Project) listed all security vulnerability at [12].There are two types of attacks which are frequently used by hackers namely SQL Injection attack and XSS (Cross Site Scripting) Attack. The following are the brief explanation of each type of attack.

6.1 SQL Injection Attack

Injection means tricking an application into including unintended commands in the data sent to an interpreter. Here what interpreter do. They take strings and interpret them as command. (SQL, OS Shell, XPath, LDAP etc.) Any web application which accepts the user input as a basis of performing database query may be vulnerable to SQL Injection. It use loopholes in the web application that interact with database. In this attacker exploits input vulnerability and attempt to send incorrect command or SQL query to the web application. These queries can fraud the interpreter to display unauthorized data to hacker [11]. By this attack hacker can Read the important information related to user (user name, password, email) from database. Access admin account and perform all the operation which is done by only admin. Hacker can also modify data by passing query. He run operating systems command on database server. There are also some parts in SQL Injection;

- ❖ Union Based SQL Injection
- ❖ String Based SQL Injection
- ❖ Error Based SQL Injection

6.2 Cross Site Scripting (XSS)

XSS is also one of the danger attack. In this attack hacker simply inject script in Webpages. These pages are returned to client and malicious code will be executed in the browser of client with alert popup. And by simply responding the web application hacks. (Ex. Attacker sets the trap – update my profile then victim views page – see Attacker profile and script silently sends attacker victim's session cookie) . Hacker can Access cookies, session tokens, do remote code execution and get sensitive data. We can classify xss into two classes' server xss and client xss. There are three types of xss;

- o Stored XSS
- o Reflected XSS
- o Dom based XSS

Stored xss also known as persistent xss .This occur when hacker stored malicious script permanently in target server like database, visitor log, and comment field or in URL. Reflected xss occur when hacker insert inject script into some input field [13]. This is not permanent by

refreshing page it will lost. And Dom base xss occur on client side when hacker enters malicious script.

6.3 Broken Authentication / Session Management

This attack also like bypass authentication. Authentication is method utilized by web application to verify that whether the user is authorize or not. Valid user's password and username stored in to database. This is a most frequent system for web application. Various action can broke the authentication no matter its strong [11]. If the user authentication system of website is weak then Hacker can take full advantage he can change the password, modify account information, and get sensitive information.

6.4 Cross site request forgery (CSRF) :

This attack also like a XSS but there is one difference that is here attacker create forged http request (e.g. Update account, login – logout, purchase process) and forced victim in to submitting malicious action via image tags, XSS, or other techniques. In which he is authenticated such as submitting http request through alert box or with other techniques [11]. If the user is authenticated the attack succeeds. By this attack attacker can steal all the information or get the password or username.

6.5 Insecure Direct Object References

When developer expose references to initial implementation object like file, dictionary, database key. Without access control check or other protection attacker can manipulate these references to access an authorized data hacker who is unauthorized simply changes a parameter value that directly refers to the system object to another object the user isn't authorized for [12].

6.6 Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server and platform. In these types of attack hacker accesses default accounts, unused pages, unpatched flaws, unprotected files and dictionaries to gain unauthorized access or for the knowledge of the system.

6.7 Sensitive Data Exposure

Many applications do not properly protect important information like credit card, tax ID's, authentication Ids. Hacker may steal or change such weekly protected data to conduct credit card fraud, id theft or other crimes. Hacker generally does not break cryptography. They break something else such as steal keys, do man in middle attacks or steal clear text data of the server while transit or from user's browser.

6.8 Using Components with Known Vulnerability

Components like frameworks or software module always run with full privileges. If vulnerable component exploited then attack can facilitate important data loss. In this hacker search a weak component by scanning. He customizes the exploit as need and executes the attack. It gets more danger if used component is deep in application.

6.9 Invalidated Redirects and Forwards

Generally web application redirects users to another page or website and use untrusted data to consider designation pages without proper validation. Hacker can redirect victim to phishing site. Hacker links to redirect and forced victim to click. Since the link is to a valid site. Attacker targets unsafe forward to bypass authentication.

6.10 Missing Function Level Access Control :

Mostly web applications verify function level rights before making that visible in the UI. Application need to perform the same access control checks on the server when each function is accessed. If request are not verified hacker, it will be able to forge requests in order to access functionality without proper authorization. Hacker who is authorized user simply changes the URL or a parameter to privileged system. He can also access private functions that aren't protected.

7. CONCLUSIONS

This paper presents an overview about the web application security area. It explains the different types of attacks used by hackers and mainly focuses on SQL Injection and XSS types of danger attack. Web security is required because Information is asset of any organization. Any breach in information security can affect image of organization. Only 10% of people are aware about hacking and hackers. Many techniques have been proposed to secure web application and browser from attackers, but even so this technique still poor.

Future work will be on the SQL Injection in web security area because it's a common but still latest attack.

REFERENCES

[1] Allen Harper, Jonathan Ness, Gideon Lenkey. "Gray Hat Hacking – Third Edition" – 2011.
[2] Ashwani Garg and Shekhar Singh. "A Review on Web Application Security Vulnerabilities". International journal of advanced research in computer science and software engineering", Volume 3, Issue 1, January - 2013.
[3] Bhavani Thurais Ingham, Chris Clifton, Amar Gupta, Elisa Bertino, Elena Ferrari. "Directions
[4] Dafydd Stuttard and Marcus Pinto. "The Web Application Hacker's Handbook – Second Edition" – 2014 for Web and E-Commerce Applications Security. http://ssrn.com/abstract_id=333682 October 2002.
[5] Gary Wasserman and Zhendong Su. "Sound and Precise Analysis of Web Applications for Injection Vulnerabilities*, University of California, Davis.
[6] Gopal R. Chaudhary and Prof. Madhav V. Vaidya. "A Survey on Security and Vulnerabilities of Web Application". International Journal of Computer Science and Information Technology, Volume 5(2), 2014.
[7] Hesham Abusaimeh and Mohammad Shkoukani. Survey of Web Application and Internet Security Threats", International journal of computer science and network security, Volume.12, No.12,December – 2012.
[8] Katkar Anjali S. and Kulkarni Raj B."Web Vulnerability Detection and Security Mechanism",International Journal Of Soft Computing and Engineering, Volume 2, Issue 4, September – 2012.
[9] Martin Szydlowsi, Christopher Kruegel and Engin Kirda. "Secure Input for Web Applications"
[10] Mr. K.Naveen Durai and K.Priyadharsini. "A Survey on Security Properties and Web Application Scanner", International journal of computer science and mobile computing, Vol.3.Issue.10, October – 2014.

[11] Nadya EIBachir EI Moussaid and Ahmed Toumanari. “Web Application Detection: A Survey and Classification. International Journal of Computer Applications”, Volume 103 – No.12, October – 2014.
[12] Open Web Application Security Project. http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[13] Rahul Johari and Pankaj Sharma.”A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection, International Conference on Communication System and Network Technologies. 2012
[14] Swarnaprabha Patil, Prof. Nitin Agrawal. “Web Security Attack and Injection- A Survey* International Journal of Advancements in Research & Technology, Volume 4, Issue 2 February – 2015.
[15] Ulfar Erlingsson a, Benjamin Livshits and Yinglian Xie. “End-to-end Web Application Security”
[16] Xiaowei Li & Yuan Xue. “A Survey on Web Application Security”. Vanderbilt University.

Author

Rutvi Pradipkumar Adhyaru
Faculty of Computer Science and Application
Charotar University of Science & Technology