iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** II **Month of publication:** February 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Vol. 2 Issue II, February 2014
ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Is your website protected: a quick study to know "unknown doors to your websites?"

Seema Agarwal[1], Manjeet Singh[2], Navneet Kumar[3]

[1]*Associate Professor, JIMS, New Delhi*
[2]*Assistant Professor, JIMS, New Delhi*
[3] *System Administrator, JIMS, New Delh*

Abstract: ***Website and its related technology started to play a vital role in our life. Infect it has become most important representative of business and provide significant improvements in business operations, banking system, education system, communication system and in the entire human life. Websites has not only brought the world closer together, but it has allowed the world's to access any part of the world in easiest way. It's provide a smooth and easiest platform through which our prospective client or customer also interacts with our business and huge number of sales happen through this only. But good and bad things always fly together. Same is with websites also. Developers always try to develop best websites and hackers try to destroy it or damage vital information. So, there is a need of extraordinary attention towards protection of websites, especially if we are transferring vital information through it. There is lot of loopholes or we can say that unknown doors by which hackers try to enter in websites and try to damage it. Such as SQL injection, cross site scripting, session management, click jacking, dns caching, symbolic linking etc. So, through this article we want to describe some loopholes by which hackers try to enter in any websites or hacked it. Hence we suggest all website owner to take almost care for making their website as secured as possible. Always tries to secure your database, validate all inputs, encrypt all user name and passwords, end sessions properly and close all possible doors to keep hackers out.***

Keywords: ***website protection, website safety, is your website protected, hacker's tools, website hacking technique.***

I. INTRODUCTION

Website and its related technology started to play a vital role in our life and became most important thing. Infect it has become most important representative of business and provide significant improvements in business operations, banking system, education system, communication system and in the entire human life. If we talking about globalization, websites has not only brought the world closer together, but it has allowed the world's to access any part of the world in easiest way. It brings down the barriers of linguistic and geographic boundaries. But most common things are that for all purpose we have needs an online medium which is being possible through websites and its related technology. Suppose if we want socially connected with globe then we have to use social websites as a platform, if we want to try any banking or financial works then respective websites help us. That means from music to rocket science, from banking to knowledge gathering in online medium we are dependent to websites. It's provide a smooth and easiest platform through which our prospective client or customer also interacts with our business and huge number of sales happen through this only. As we know there are always two side of a coin. Same is with websites also. Developers always try to develop best websites and hackers try to destroy it. Nowadays websites are at top priority of hackers list who try to steal or damage vital information. So, there is a need of extraordinary attention towards protection of websites, especially if we are transferring vital information through it. Hence websites must be protected in best possible manner.

II. OBJECTIVE

Through this topic (i.e. "Is your website protected: a quick study to know "unknown doors to your websites") we try to focus on loopholes of websites and online communication medium which affected by the hacker and crackers. We also summaries some tools by which online website crimes can be taken and some safety jacket to save your websites in effective manner.

Vol. 2 Issue II, February 2014
ISSN: 2321-9653

III. UNKNOWN DOORS TO YOUR WEBSITES WHICH AFFECTED IN MANY WAYS

Websites are the platform of online medium and backbone of online business, knowledge and communication. So, it must be protected through below mention threads.[1]

1. SQL Injection Attacks
2. Cross Site Scripting Attacks
3. Man-in-the-middle attack
4. Broken Authentication and Session Management Attacks
5. Click jacking Attacks
6. DNS Cache Poisoning
7. Social Engineering Attacks
8. Symlinking – An Insider Attack
9. Cross Site Request Forgery Attacks
10. Remote Code Execution Attacks
11. DDoS Attack – Distributed Denial Of Service Attack

SQL Injection Attacks
Generally, this attack occur when there are flaws in website SQL Database, its libraries, or even the operating system itself. Attackers inject some hidden query through webpage's or websites loopholes. Users open such files with hidden query unknowingly and fill there details, credit card numbers, private information etc. In doing so, they have allowed hackers to gain unauthorized access to private data.

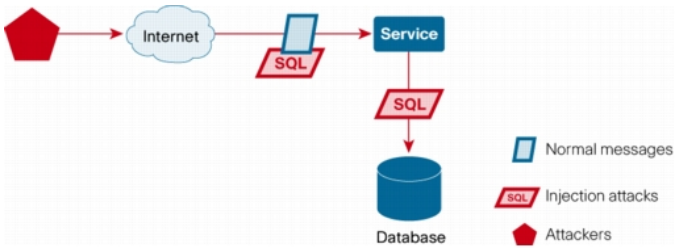


Fig.1- SQL Injection Attacks [2]

Technical Injection Attack Example:
An Injection Attack could have this command line:
String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") +"'";The hacker modifies the 'id' parameter in their browser to send: ' or '1'='1. This changes the meaning of the query to return all the records from the accounts database to the hacker, instead of only the intended customers.

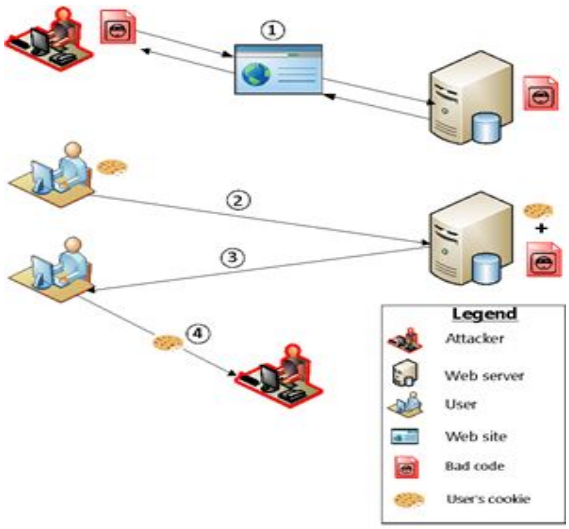
Cross Site Scripting Attacks
These attacks have become the most prevalent and dangerous security issue affecting web applications. XSS vulnerabilities occur whenever an application takes data that originated from a user and sends it to a web browser without first properly validating or encoding it. XSS attacks can be used to hijack user sessions, deface websites, conduct port scans on victims' internal networks, conduct phishing attacks, and take over users' browsers.[3]

For example, if www.ebank.com/info.html has XSS script in it, the user might see a popup window asking for their credit card and other sensitive info.

Technical Cross Site Scripting Example:
(String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>";

The attacker modifies the 'CC' parameter in their browser to:
'><script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'

This causes the user's session ID to be sent to the attacker's website, allowing the hacker to hijack the user's current session. That means the hacker has access to the website admin credentials and can take complete control over it.[4]



Vol. 2 Issue II, February 2014
ISSN: 2321-9653

Fig.2- Basic Description of stored XSS attack to steal cookies [5]

Man-in-the-middle attack

This attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in below figure.
Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.

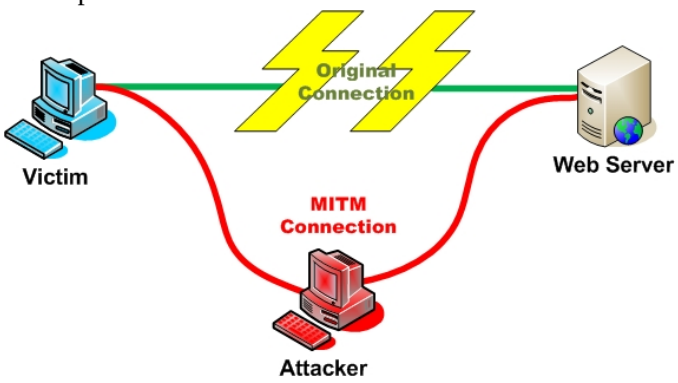


Fig.3- Illustration of man-in-the-middle attack [6]
Broken Authentication and Session Management Attacks

Authentication systems involve passwords, key management, session IDs, and cookies that can allow a hacker to access your account from any computer (as long as they are valid). So, if authentication system and session management is weak then hackers definitely take advantage of this.

For Example

Scenario #1: Airline reservations application supports URL rewriting, putting session IDs in the URL:

```
http://example.com/sale/saleitems
jsessionid=2P00C2JSNDLPSKHCJUN2JV
?dest=Hawaii
```

An authenticated user of the site wants to let his friends know about the sale. He e-mails the above link without knowing he is also giving away his session ID. When his friends use the link they will use his session and credit card.
Scenario #2: Application's timeouts aren't set properly. User uses a public computer to access site. Instead of selecting "logout" the user simply closes the browser tab and walks away. Attacker uses the same browser an hour later, and that browser is still authenticated.

Scenario #3: Insider or external attacker gains access to the system's password database. User passwords are not properly hashed, exposing every user's password to the attacker.[7]

Click jacking Attacks

It is also known as (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function. The term "clickjacking" was coined by Jeremiah Grossman and Robert Hansen in 2008.[8]

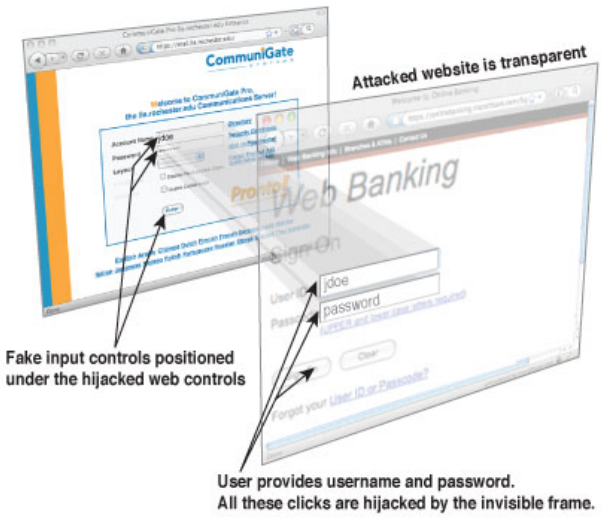


Fig.4- Illustration of man-in-the-middle attack [9]

Social Engineering Attacks

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

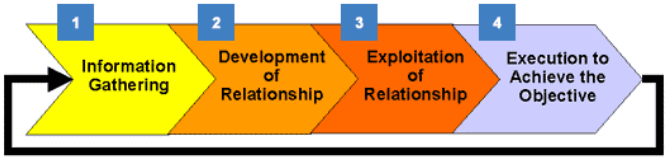


Fig.5- Social Engineering attack cycle [10]

Symlinking – An Insider Attack

In computing, a symbolic link (also symlink or soft link) is a special type of file that contains a reference to another file or directory in the form of an absolute or relative path and that affects pathname resolution.

A symlinking attack occurs when a hacker positions the symlink in such a way that the user or application that access the endpoint thinks they're accessing the right file when they're really not.

If the endpoint file is an output, the consequence of the symlink attack is that it could be modified instead of the file at the intended location. Modifications to the endpoint file could include appending, overwriting, corrupting, or even changing permissions.

Cross Site Request Forgery Attacks

CSRF is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated. With a little help of social engineering (like sending a link via email/chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.[12]

Technical Example

In this case the hacker creates a request that will transfer money from a user's account, and then embeds this attack in an image request or iframe stored on various sites under the attacker's control.

Remote Code Execution Attacks

A Remote Code Execution attack is a result of either server side or client side security weaknesses.
Vulnerable components may include libraries, remote directories on a server that haven't been monitored, frameworks, and other software modules that run on the basis of authenticated user access. Applications that use these components are always under attack through things like scripts, malware, and small command lines that extract information.[13]

DDoS Attack – Distributed Denial Of Service Attack

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet
[14]

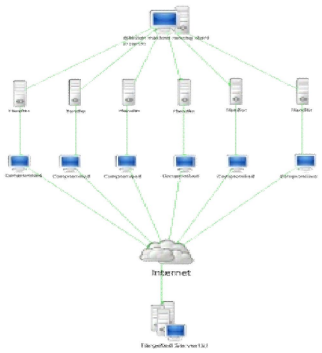


Fig.6- DDoS Stacheldraht Attack diagram. [14]

Vol. 2 Issue II, February 2014
ISSN: 2321-9653

IV. PROTECTION FROM UNKNOWN DOORS OF WEBSITE

- Installed software updates and patches of operating system regularly.
- Actually hackers see the weakness of system and take advantages so, always use recent version of software's.
- Make your database fully authenticated and validated.
- Always close your session after working with website or try to delete history from web browser.
- Never click on seemingly innocuous web pages which save you from Click jacking Attacks.
- See path of the pages before clicking on symbolic link.
- Update your browser also on regular basis.
- Make sure firewall must be installed on your pc and update it regularly.
- Personalize your firewall setting during the setup process which show how much data you want to allow into your system from internet.
- Change your password regularly.
- Always use proper antivirus and scan regularly your pc.
- Make sure anti-virus software updates automatically.
- Install anti-spyware programs onto your system.
- Delete emails from unknown sources.
- Network must be managed with appropriate firewall.
- Check your system software and make sure not any unknown software installed you pc.
- Make your pc password protected.

V. DIFFERENT METHODOLOGIES USED FOR SAFETY FOR WEBSITES

- Keep your operating system updated/patched. Set it to "auto update".
- Use anti-virus and anti-spyware software and keep them updated.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Secure your transactions. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.
- Be cautious about all communications you receive including those purported to be from "trusted entities" and be careful when clicking links contained within those messages.
- Do not respond to any unsolicited (spam) incoming e-mails.
- Do not open any attachments contained in suspicious emails.
- Do not respond to an email requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password."
- Beware of emails that threaten any dire consequences should you not "verify your information".
- Do not enter personal information in a pop-up screen. Providing such information may compromise your identity and increase the odds of identity theft.
- Have separate passwords for work related and non-work related accounts.
- Be educated with modern technology.

VI. CONCLUSIONS

At the end of "Is your website protected: a quick study to know unknown doors to your websites" we want to suggest that this type of attack generally done by hacker and cyber criminals. So, there is a need of extraordinary attention towards protection of websites, especially if we are transferring vital information through it. Hence websites must be protected in best possible manner. Hence we suggest all website owner to take almost care for making their website as secured as possible. Always tries to secure your database, validate all inputs, encrypt all user name and passwords, end sessions properly and close all possible doors to keep hackers out.

REFERENCES

[1] http://defencely.com/blog/10-popular-ways-hackers-hack-website/

[2] Cisco Review http://www.cisco.com/en/US/prod/collateral/con netw/ps5719/ps7314/prod_white_paper0900aecd80661 ca6.html

[3] Microsoft.com http://www.microsoft.com/security/sir/trategy/default.aspx#!cross_site_scripting

[4] http://defencely.com/blog/10-popular-ways-hackers-hack-website/

[5] http://www.microsoft.com/security/sir/trategy/default.aspx#!cross_site_scripting

[6] https://www.owasp.org/index.php/Man-in-the-middle_attack

[7] https://www.owasp.org/index.php/Top_10_2013-A2 Broken_Authentication_and_Session_Management

[8] http://en.wikipedia.org/wiki/Clickjacking

[9] http://hackingtech.in/clickjacking-attack-things-you-should-know/

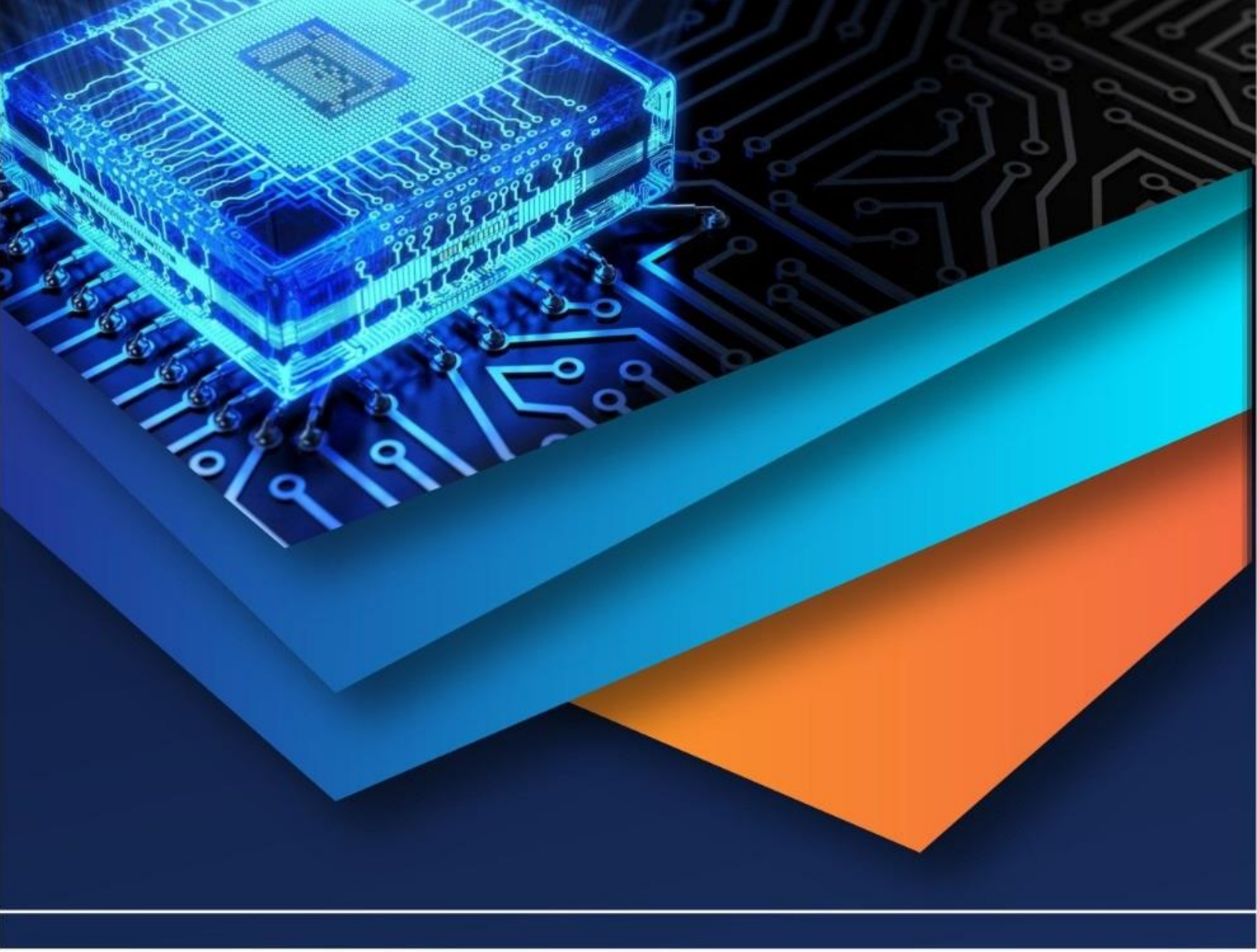
[10] copyright 2002 Gartner G2

[11] http://en.wikipedia.org/wiki/Symbolic_link

[12] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

[13] http://defencely.com/blog/10-popular-ways-hackers-hack-website/

[14] http://en.wikipedia.org/wiki/Denial-of-service_attack



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY