

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Popular Ways Hackers Hack Websites Explained.](#)

Mr. Robot - December 2, 2015, 4:54 am

Hi everyone! Recently I created a thread helping users discover if their passwords have been leaked due to database hacking and now I will tell you about some of the most popular methods hackers use.

Full credit to the original author - I will be adding videos later and adding information as I work through to cover as many end points as possible

Author is Shritam Bhowmick and can be found at <http://defencely.com>

Symlinking

Spoiler ([Click to View](#))A symlink is basically a special file that “points to” a hard link on a mounted file system. 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.

In different variations of a symlinking attack a hacker may be able to control the changes to a file, grant themselves advanced access, insert false information, expose sensitive information or corrupt or destroy vital system or application files.

Injection Attacks

Spoiler ([Click to View](#))Injection Attacking occurs when there are flaws in your SQL Database, SQL libraries, or even the operating system itself. Employees open seemingly credible files with hidden commands, or “injections”, unknowingly.

In doing so, they’ve allowed hackers to gain unauthorized access to private data such as social security numbers, credit card number or other financial data.

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.

Clickjacking Attacks

Spoiler ([Click to View](#))Clickjacking Attacks

Clickjacking, also called a UI Redress Attack, is when a hacker uses multiple opaque layers to trick a user into clicking the top layer without them knowing.

Thus the attacker is “hijacking” clicks that are not meant for the actual page, but for a page where the attacker wants you to be.

For example, using a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password for their bank account, but are actually typing into an invisible frame controlled by the attacker.

DNS Cache Poisoning

Spoiler ([Click to View](#)) DNS Cache Poisoning involves old cache data that you might think you no longer have on your computer, but is actually “toxic”.

Also known as DNS Spoofing, hackers can identify vulnerabilities in a domain name system, which allows them to divert traffic from legit servers to a fake website and/or server.

This form of attack can spread and replicate itself from one DNS server to another DNS, “poisoning” everything in it’s path.

In fact, in 2010, a DNS poisoning attack completely compromised the Great Firewall of China (GFC) temporarily and censored certain content in the United States until the problem was fixed.

Social Engineering Attacks

Spoiler ([Click to View](#)) A social engineering attack is not technically a “hack”.

It happens when you divulge private information in good faith, such as a credit card number, through common online interactions such as email, chat, social media sites, or virtually any website.

The problem, of course, is that you’re not getting into what you think you’re getting into.

A classic example of a social engineering attack is the “Microsoft tech support” scam.

This is when someone from a call center pretends to be a MS tech support member who says that your computer is slow and/or infected, and can be easily fixed – at a cost, of course.

Cross Site Scripting Attacks

Spoiler ([Click to View](#)) Cross Site Scripting, also known as an XSS attack, occurs when an application, url “get request”, or file packet is sent to the web browser window and bypassing the validation process. Once an XSS script is triggered, it’s deceptive property makes users believe that the compromised page of a specific website is legitimate.

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

Remote Code Execution Attacks

Spoiler ([Click to View](#)) 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.

The following vulnerable components were downloaded 22 million times in 2011:

Apache CXF Authentication Bypass (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3451>)

By failing to provide an identity token, attackers could invoke any web service with full permission.

Cross Site Request Forgery Attacks

Spoiler ([Click to View](#)) A Cross Site Request Forgery Attack happens when a user is logged into a session (or account) and a hacker uses this opportunity to send them a forged HTTP request to collect their cookie information.

In most cases, the cookie remains valid as long as the user or the attacker stays logged into the account. This is why websites ask you to log out of your account when you're finished – it will expire the session immediately.

In other cases, once the user's browser session is compromised, the hacker can generate requests to the application that will not be able to differentiate between a valid user and a hacker.

Broken Authentication and Session Management Attacks Spoiler ([Click to View](#)) If the user authentication system of your website is weak, hackers can take full advantage.

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).

If a hacker exploits the authentication and session management system, they can assume the user's identity.

Scary indeed.

Ask yourself these questions to find out if your website is vulnerable to a broken authentication and session management attack:

- Are user credentials weak (e.g. stored using hashing or encryption)?

- Can credentials be guessed or overwritten through weak account management functions (e.g. account creation, change password, recover password, weak session IDs)?

- Are session IDs exposed in the URL (e.g. URL rewriting)?

- Are session IDs vulnerable to session fixation attacks?

- Do session IDs timeout and can users log out?

If you answered "yes" to any of these questions, your site could be vulnerable to a hacker.

If you are reading this - This is far from finished, my computer is having issues and I have to post this thread now to avoid losing this.

Pictures to come and details on who to contact for support and where, plus video guides and a help desk.

Closing till complete as users from the group NULL are sending my PM's attacking my work and threatening me.

reacts - December 2, 2015, 5:10 am

Your post is very interesting. I'm looking forward for more content like this from you.

Wireless Network - December 2, 2015, 7:18 am

Nice post buddy. Could be useful for beginners

Im gone brah - December 2, 2015, 8:11 am

Really poor 'tutorial', you didn't even state how someone would go on about utilizing these attacks. You didn't provide any code snippets, you didn't mention how to bypass different IDS's or WAF's. You didn't explain anything at all.

The fact you took your time to write this shit makes me lose hope.

-Elusive- - December 2, 2015, 8:14 am

"The reason for copying most of the below information is - I couldn't have written better even if I tried"
I lol'd.

GewooE - December 2, 2015, 8:19 am

Great post, pretty helpful I hope you update the thread as you said it!

Mr. Robot - December 2, 2015, 8:29 am

(Dec 2, 2015 09:11 AM)Zayne Wrote: [\[CITE\]](#) Really poor 'tutorial', you didn't even state how someone would go on about utilizing these attacks. You didn't provide any code snippets, you didn't mention how to bypass different IDS's or WAF's. You didn't explain anything at all.

The fact you took your time to write this shit makes me lose hope.
If you took the time to read the entire thread you would see it is incomplete - I merely needed to post it due to current computer issues.

The fact the thread is currently titled - [TUTORIAL] Popular Ways Hackers Hack Websites Explained.

And I have given popular examples and explained how they are used - if you are looking for a pre-written code to go hack facebook or some stupid shit - you should just stop while you are ahead- I am trying to contribute something and people like you are discouraging. I completely and fully accept your apology for not reading the entire thread as it's obvious you didn't do so, but don't you dare come to someones thread to flame when they are just trying to help.

Im gone brah - December 2, 2015, 8:57 am

(Dec 2, 2015 09:29 AM)Mr. Robot Wrote: [\[CITE\]](#) If you took the time to read the entire thread you would see it is incomplete - I merely needed to post it due to current computer issues.

The fact the thread is currently titled - [TUTORIAL] Popular Ways Hackers Hack Websites Explained.

And I have given popular examples and explained how they are used - if you are looking for a pre-written code to go hack facebook or some stupid shit - you should just stop while you are ahead- I am trying to contribute something and people like you are discouraging. I completely and fully accept your apology for not reading the entire thread as it's obvious you didn't do so, but don't you dare come to someones thread to flame when they are just trying to help. And what makes your 'tutorial' different compared to anything else on this forum? I've seen multiple tutorials cover each and everything in your thread so far.

I am tired of visiting this section, seeing all useless threads over and over. Don't tell me what I can, and cannot do. If someone just want to know the principles of the method explained, they could go to any other tutorial here or head straight to OWASP or Wikipedia.

edit:

Quote:An Injection Attack could have this command line:

String query = "SELECT * FROM accounts WHERE custID=" + request.getParameter("id") +"";
You know a command line is basically a text interface? What you wrote there (I mean copy) was

just a query which is vulnerable.

Vellichor - December 2, 2015, 1:02 pm

Quote:Injection Attacking occurs when there are flaws in your SQL Database, SQL libraries, or even the operating system itself. Employees open seemingly credible files with hidden commands, or "injections", unknowingly. TIL flaws in Linux Kernel causes SQLi

?A?O - December 2, 2015, 2:22 pm

(Dec 2, 2015 09:29 AM)Mr. Robot Wrote: [\[CITE\]](#) If you took the time to read the entire thread you would see it is incomplete - I merely needed to post it due to current computer issues.

The fact the thread is currently titled - [TUTORIAL] Popular Ways Hackers Hack Websites Explained.

And I have given popular examples and explained how they are used - if you are looking for a pre-written code to go hack facebook or some stupid shit - you should just stop while you are ahead- I am trying to contribute something and people like you are discouraging. I completely and fully accept your apology for not reading the entire thread as it's obvious you didn't do so, but don't you dare come to someones thread to flame when they are just trying to help.

1. This thread has no detail at all and lacks everything needed in a solid tutorial thread.
2. Learn how to take criticism from people and don't be on such a high horse.
3. Don't make threats to people you don't know. It'd be wise on your part.

harnemo - December 2, 2015, 2:34 pm

Without intention to hijack the OPs thread I recently created a thread on how to protect your Wordpress site from hackers. It is not some ultimate guide, but I believe it can be helpful against some basic hacking attempts. Link to the thread:

<https://hackforums.net/showthread.php?tid=5079411>