

Knowledge Base

# Website Hacking Techniques Most Commonly Used By Hackers



Updated on: June 27, 2023



Sovandeb

7 mins read

Do you use the internet? Guess is you do. Then you must have come across news such as hackers stealing data and bringing down services & websites. Here are some website hacking techniques hackers generally use.

**This Blog Includes** [ [show](#) ]

In fact, [according to hacking stats](#):

- 64% of companies admit to facing web attacks
- 1/131 emails contain malware in them
- Every day there are 4000+ ransomware attacks taking place
- 95% breaches happen due to human errors

These stats are startling, to say the least.

This does not mean website owners are reckless. No, they do take precautions. It's only that – this is not enough! All websites and internet services have minute vulnerabilities that could be abused by this or that website hacking technique. Unless you identify and patch these vulnerabilities on time, you remain unsecured.

After every hack, I've seen many wonder – *"If only I knew better of these hackers and the website hacking techniques, I might have successfully dodged it."*

While this has some truth to it, it isn't entirely true.

That being said, of course, peeking into the minds of hackers helps. But without [proper security equipment](#), you are only as good as a weaponless soldier.

So, with this blog post, we have created a window for you to look into the operations of a hacker and understand common web threats and the hacking techniques behind them.

Below are the nine most common website hacking techniques used by attackers.

## Top Website Hacking Techniques

### 1. Social engineering (Phishing, Baiting)

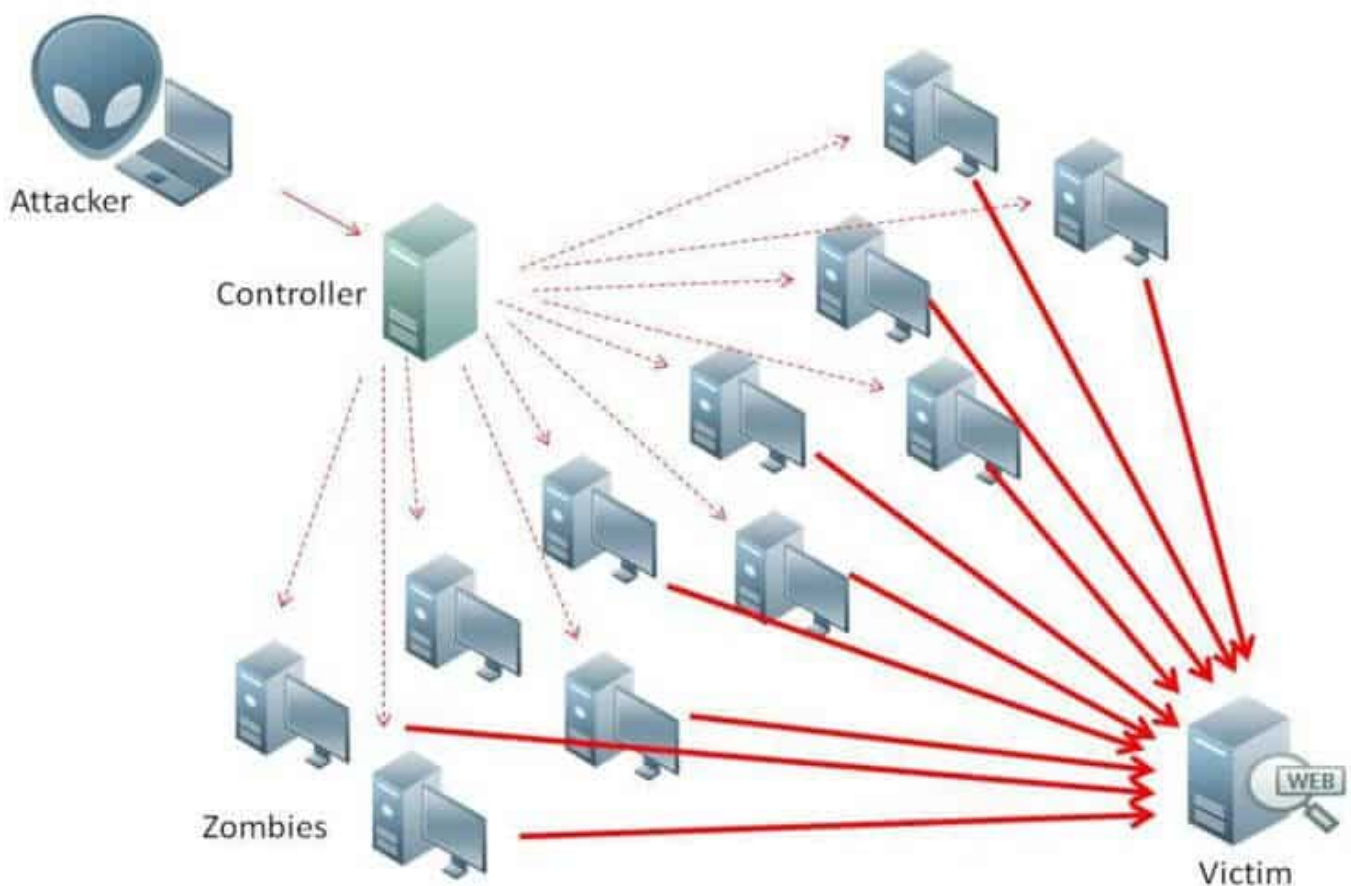
Phishing is a method where the attacker replicates the original website and then leads a victim to use this fake website rather than the original one. Once the victim enters their credentials into this website, all details are sent to the attacker. This method can be used to obtain payment information such as credit card data or personal information such as login credentials to important accounts and websites.

Another type of [social engineering](#) is the 'bait and switch' attack. In this ***hacking technique***, attackers buy advertising spots on trustworthy and popular websites and put up seemingly legit ads. Once the ads are launched, users click on it only to find themselves inside a website that is filled with malware. These malware gets

installed on the victim's system and then the attacker has a free run within their system

## 2. DDoS attacks

**Distributed Denial of Service (DDoS)** is mainly used to bring down websites by crashing their servers. Attackers flood the servers of the targeted website with the help of zombie computers or botnets. This overwhelms the resources of the servers and it crashes. In several cases, this attack was also used to steal user information by freezing the user forms. The recent **DDoS** attack on GitHub is an excellent example of how severe these attacks can be.



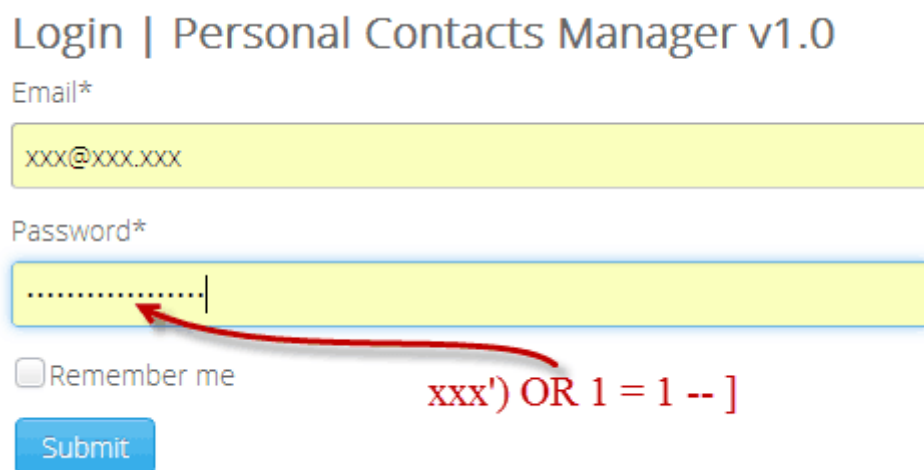
## 3. Code injection attacks

Code injection is the general term used for attacks that include injecting malicious codes into systems. Whenever there is improper handling of input data, it becomes vulnerable to code injection attacks.

These attacks are possible when input or output data is not properly validated. Once an attacker is able to inject their code into the system, they can compromise the integrity and security of the system. These attacks can also be used as a way to launch further attacks since the system is already infected and thus vulnerable.

## 4. SQL Injection

This attack majorly exploits vulnerabilities in a website's SQL libraries or databases. In case a website has any such vulnerability, hackers can use simple SQL codes to obtain information and data from the databases. These simple codes trick the system into considering them as legit queries and then give access to its database.



The image shows a login interface titled "Login | Personal Contacts Manager v1.0". It has two input fields: "Email\*" and "Password\*". The Email field contains "xxx@xxx.xxx". The Password field contains a series of dots, with a red arrow pointing to it from the text "xxx') OR 1 = 1 -- ]". Below the password field is a checkbox labeled "Remember me" and a blue "Submit" button.

## 5. XSS attacks

Also known as [Cross-Site Scripting](#) attacks, in this type of attack, hackers inject malicious code into a legit website. When a visitor enters the website and uses their credentials, all data is stored within the website, which the attacker can access anytime. These attacks can be effectively used to steal user data and private information.

There are two types of XSS attacks, stored XSS attacks and reflected XSS attacks. In stored attacks, the infected script is permanently kept in the server. And the attacker can retrieve it anytime. In reflected attacks, the scripts are bounced off web servers in the form of warnings or search results. Since this makes the request look authentic the website processes them and gets infected

## 6. Exploiting plugin vulnerabilities

If you use WordPress then you must be familiar with plugins (extensions & modules in case of Magento & Drupal respectively). Plugins are considered as the most vulnerable parts of a website. Any outdated or unsecured third-party plugins can be exploited by attackers to take control of your website or bring it down altogether. The best way to stay safe is to always use plugins from trusted sources and always keep your plugins updated

## 7. Brute force

In this hacking technique, the attackers try multiple combinations of the password until one of the combination matches. This method is simple to execute but requires huge computing power to implement. Longer the password, tougher it is to guess using brute force. Sometimes, attackers also use dictionaries to speed up the process

## 8. DNS Spoofing

By using DNS spoofing attacks, attackers can force victims to land on a fake website. This is done by changing the IP addresses stored in the DNS server to an address that leads to the attacker's website. DNS cache poisoning is the process by which the local DNS server, with the infected server. Once the victim lands on the fake website, the attacker can infect the victim's system with malware and use other website hacking techniques to cause further damage.

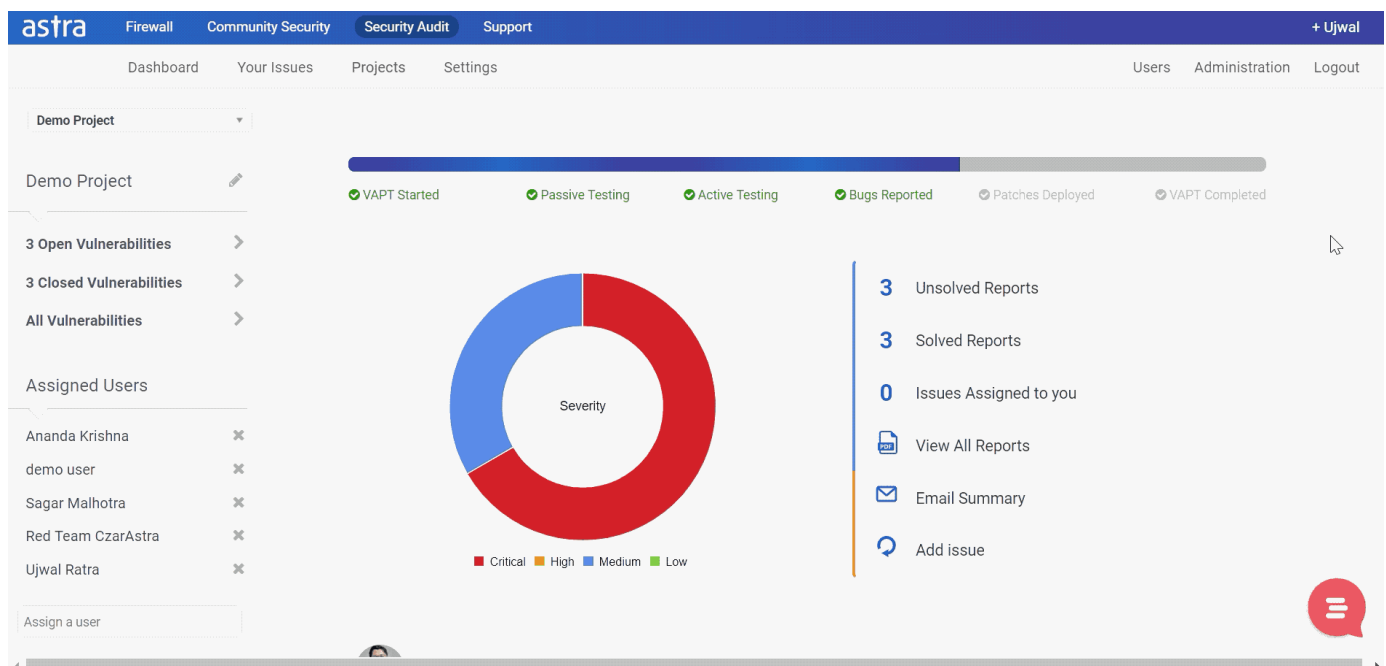
## 9. Cookie theft

As harmless as it sounds, this attack can effectively steal all your important data. During browsing sessions, websites stores tons of cookies on your computer. These cookies contain a lot of sensitive information, including your login credentials such as your passwords or even your payment data. If the attackers get their hands on

these cookies, they can either steal all this information or use it to impersonate you online.

The above attacks are generally used against some vulnerability which the attackers exploit. That is why it is crucial to keep updating your software & other systems.

Once a vulnerability is discovered it is necessary to patch it up before an attacker exploits it to cause harm. Ethical hackers and security researchers around the globe try to discover such security gaps to ensure they are fixed. [Astra's VAPT \(Vulnerability Assessment & Penetration Testing\)](#) does exactly that.



## Vulnerability Assessment & Penetration Testing by Astra

Moreover, you can look up known vulnerabilities in the system/software you are using by following this website: [cve.mitre.org](https://cve.mitre.org)

## Steps to protect yourself from getting hacked

Now we know the various ways attackers can harm you or your website. This will help us in understanding how attackers work and thus enable us to take more effective steps to protect ourselves from such attackers. Below are some basic steps to protect your data from some common website hacking techniques:

1. Use strong passwords and 2-factor authentications wherever possible
2. Keep your plugins and software updated with the latest security patches
3. Use [strong firewalls](#) to prevent DDoS attacks and block unwanted IP addresses
4. Maintaining proper code sanitization can help stop SQL injection attacks
5. Avoid clicking on any unknown links or opening attachments in [email from unknown sources](#)
6. Regular security audits to keep track of your website's security

Websites are always vulnerable to such attacks and one needs to be vigilant round the clock. To monitor your website's security, Astra's security firewall is the best option for you.

With their constant monitoring of your website and an intuitive dashboard, you will always be aware of any attempts to sabotage your website.

If you liked this post, go ahead and share this with your friends 😊

**Was this post helpful?**

Yes

27

No

10

Share this...

**Sovandeb**

Your usual nerd with an avid interest in everything tech. If not writing then following up on cyber security news and preparing for my next article. If there is something new out there you can bet I will write about it.

✉ Subscribe ▼



*Be the First to Comment!*

**B** *I* U         



This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)



0 COMMENTS



# Related Articles

Knowledge Base

## 7 Web Security Mistakes to Avoid (And How to Do So)

Knowledge Base

## Choosing a SaaS Product for your Business? 4 Things To Check Before Buying

Knowledge Base

## Blockchain Security Issues – A Complete Guide

# Psst! Hi there. We're Astra.

We make security simple and hassle-free for thousands of websites and businesses worldwide.

Our suite of security products include a vulnerability scanner, firewall, malware scanner and pentests to protect your site from the evil forces on the internet, even when you sleep.

[Get a Pentest](#)

[Protect your website](#)

We make security simple and hassle-free for thousands of websites & businesses worldwide.

See our glowing reviews on

**Trustpilot**

**Capterra**

+ Pentest

+ Website Protection

+ Company

+ Resources

Made with  in

Copyright © 2022 **ASTRA IT, Inc.** All Rights Reserved.

[Privacy Policy](#) | [Terms of Service](#) | [Report a vulnerability](#)