10 MOST COMMON WEBSITE HACKING TECHNIQUES YOU SHOULD KNOW

Post Views: 49,135

We been talking a lot about cleaning and protecting websites from attacks. But what about knowing how exactly your website can be hacked? That is an interesting and useful information we would like to share with you. So let us go through the most popular hacking techniques for you.

1. Phishing

One of the most insidious techniques used today is Phishing.It's hard to find the person that doesn't know what phishing is. However a lot of users are still getting tricked by hackers on a daily basis.

Phishing implies the replication of the website with the aim of stealing money or personal information. And once a user enters his credit card details,for example, a hacker will have access to that data and will be able to use the received information for his own benefit.

2. Viruses and malicious code

Hackers can crawl almost into any website and leave in its' database malware or insert code into the website's files. There is a huge variety of viruses, and each may impact the infected site differently. But there should be no doubt that a virus, regardless of its type, will not benefit your business.

interface. Once the a user clicks the button with an intention of to proceed to a certain page, he will find himself on an unfamiliar website, usually with an inappropriate content.

4. Cookie Theft

With the help of a malicious software hackers can steal your browser's cookies. And those cookies contain a lot of important information: browsing history, usernames and passwords. As you understand,that data can also contain logins and password to your website's administrator's panel.

5. Denial of Service (DoS\DDoS)

DDOS stands for Distributed Denial of Service. DDOS attack is a way to make a certain server unavailable or, in other words, a way to crash the server.

To interrupt or crash the server a hackers would use bots. Those bots soul purpose is to send requests to the website, a lot of requests. As a result, a server unable to process all of the received requests will simply crash. The most hazardous thing about this technique is that a hacker can crash the server in a relatively small amount of time

6. DNS spoofing

This malware is also known as DNS cache poisoning. It engages that old cache data you might have forgotten about.
Vulnerabilities in the domain name system allow hackers to redirect traffic from your website to a malicious one. Moreover, hackers can program this attack so the infected DNS server will infect another DNS and so on.

7. SQL injection

If your website has vulnerabilities in its SQL database or libraries, hackers can get access to your confidential information by deceiving the system.So there is no surprise that SQL injections can also be a simple tool. But this simple tool can allow a hacker to access vital information of your website.

The malware records keystrokes , captures all of the user's actions on the keyboard, and to send all that has been recorded to the hackern ; it also installs a malicious script that produces an in-browser cryptocurrency miner.
If a hacker succeeds in obtaining data, then the result of the hacking will be stolen admin credentials that can allow hackers to easily log into your website

9. Non-targeted website hack

In most cases, hackers don't target a specific website. They are more interested in massive hacking.
It is easy to suffer from a non-targeted attack – you just need to overlook any CMS, plugin or template vulnerability. Any gap is a chance to get into the hacker's sight and become a victim during the next attack.
Hackers can find websites with similar weaknesses easily. They can always use Google's Hacking Database to receive a list of vulnerable websites that have the same properties. For example, hackers can find all indexed websites that have a vulnerable plugin installed. Or websites with unhidden catalogues.

10. Brute force

A Brute Force Attack is the simple method to gain access to a website. It tries various combinations of the passwords again and again until it gets in. This repetitive action is like an army attacking a fort.

Conclusion

It is hard for website owners to believe that anyone can find and hack a vulnerable website in literally minutes without any specific instruments. Everything a hacker needs is to find the desired criteria in Google's Hacking Database and run a search with those parameters. Then, depending on the criteria a hacker chose, he can take the needed actions to hack a website. Experienced hackers will spend less than two minutes on it. And they will spend even less time if the attack is automated.

from all types of hacker’s attacks, find existing viruses and malicious codes.

Think about the security of your website in advance, then you will significantly lower the probability of being hacked

8 COMMENTS

Jstash

October 25th 2018, 2:59 am

nice one

REPLY

E

March 13th 2019, 9:22 pm

yes

REPLY

Amit Saini Machine Never Die

January 15th 2019, 1:23 pm

Nice and Informative this article.

REPLY

Patrachar

February 12th 2019, 1:01 pm

Really nice information. Thanks for sharing.

REPLY

Patterson

May 28th 2019, 10:05 pm

Nice article

REPLY

Hridoy Hasan

REPLY

Faceless

June 23rd 2019, 10:54 am

Oh my GooooooooD

REPLY

Dhaneshwaer

June 25th 2019, 8:52 am

Nice

REPLY

ADD COMMENT

Name *

Email *

Website

POST COMMENT

SEARCH ON COBWEB SECURITY BLOG

Search...

MAKE SAFE YOUR WEBSITE

SOCIAL LINKS

MAKE SAFE YOUR WEBSITE WITH WEBDEFENDER

MOST VIEWED POSTS

Why eCommerce Websites Are The Main Target For Hackers (4,999)

CWIS antivirus for Cpanel/WHM – PHP website security (4,352)

CATEGORIES

- Drupal vulnerabilities
- Magento vulnerabilities
- Phishing sites
- Uncategorised
- Vulnerability
- Web Security
- Website Malware
- Website Security
- WordPress Hack
- WordPress Security

ARCHIVES

- February 2019
- August 2018
- May 2018
- April 2018
- March 2018
- February 2018
- January 2018
- December 2017
- November 2017
- October 2017

CWIS
COBWEB SECURITY

- May 2017
- April 2017
- February 2017
- January 2017
- December 2016

‹ ›

FREE PRODUCTS

- FREE WEBSITE ANTIVIRUS
- WORDPRESS PLUGIN

SOLUTIONS

- FREE MALWARE SCANNER
- WEBSITE UNDER ATTACK ?
- PROTECT YOUR WEBSITE
- MALWARE REMOVAL
- WEBSITE SECURITY

SUPPORT

- WEB SECURITY ACADEMY
- WEB DEFENDER FEATURES

CWIS
COBWEB SECURITY

ABOUT US

- ABOUT
- OUR TEAM
- CUSTOMER TESTIMONIALS
- PRIVACY POLICY
- TERMS OF SERVICE

BUSINESS WEBSITE PRODUCT

- PLANS & PRICES
- PREMIUM PLAN – 100% SECURITY
- PROFESSIONAL ANTIVIRUS

WEB SERVER ANTIVIRUS

- CPANEL/WHM CWIS ANTIVIRUS
- WEB SERVER PREMIUM SECURITY