

Forum:[Hack Forums](#)

Thread: [How to hack website and top 10 website hacking tools.](#)

bpnrockstar - December 27, 2019, 5:38 am

TOPICS COVERED IN THIS TUTORIAL

What is a web application? What are Web Threats?

Top 10 web haking tools

WHAT IS A WEB APPLICATION? WHAT ARE WEB THREATS?

A web application (website) is an application based on the client-server model. The server provides database access and the business logic. It is hosted on a web server. .

SQL Injection – the goal of this threat could be to bypass login algorithms, sabotage the data, etc.

Denial of Service Attacks – the goal of this threat could be to deny legitimate users access to the resource

Cross-Site Scripting XSS – the goal of this threat could be to inject code that can be executed on the client-side browser.

Cookie/Session Poisoning – the goal of this threat is to modify cookies/session data by an attacker to gain unauthorized access.

Form Tampering – the goal of this threat is to modify form data such as prices in e-commerce applications so that the attacker can get items at reduced prices.

Code Injection – the goal of this threat is to inject code such as PHP, Python, etc. that can be executed on the server. The code can install backdoors, reveal sensitive information, etc.

Defacement – the goal of this threat is to modify the page been displayed on a website and redirecting all page requests to a single page that contains the attacker's message.

TOP 10 WEBSITE HACKING TOOLS.

BURP SUITE. :-

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Source: <http://portswigger.net/burp/>

NIKTO NIKTO DARKWEBSOLUTIONS.COM

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against

web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

Source:

METASPLOITMETASPLOIT :-

The Metasploit Framework (MSF) is far more than just a collection of exploits. It's an infrastructure that you can build upon and utilize for your custom needs. This allows you to concentrate on your unique environment, and not have to reinvent the wheel. I consider the MSF to be one of the single most useful auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

Source: <https://www.offensive-security.com/metasploit-unleashed/introduction/>

NMAP :-

NMAP ("NETWORK MAPPER") IS A FREE AND OPEN SOURCE (LICENSE) UTILITY FOR NETWORK DISCOVERY AND SECURITY AUDITING. MANY SYSTEMS AND NETWORK ADMINISTRATORS ALSO FIND IT USEFUL FOR TASKS SUCH AS NETWORK INVENTORY, MANAGING SERVICE UPGRADE SCHEDULES, AND MONITORING HOST OR SERVICE UPTIME. NMAP USES RAW IP PACKETS IN NOVEL WAYS TO DETERMINE WHAT HOSTS ARE AVAILABLE ON THE NETWORK, WHAT SERVICES (APPLICATION NAME AND VERSION) THOSE HOSTS ARE OFFERING, WHAT OPERATING SYSTEMS (AND OS VERSIONS) THEY ARE RUNNING, WHAT TYPE OF PACKET FILTERS/FIREWALLS ARE IN USE, AND DOZENS OF OTHER CHARACTERISTICS. IT WAS DESIGNED TO RAPIDLY SCAN LARGE NETWORKS, BUT WORKS FINE AGAINST SINGLE HOSTS. NMAP RUNS ON ALL MAJOR COMPUTER OPERATING SYSTEMS, AND OFFICIAL BINARY PACKAGES ARE AVAILABLE FOR LINUX, WINDOWS, AND MAC OS X. IN ADDITION TO THE CLASSIC COMMAND-LINE NMAP EXECUTABLE, THE NMAP SUITE INCLUDES AN ADVANCED GUI AND RESULTS VIEWER (ZENMAP), A FLEXIBLE DATA TRANSFER, REDIRECTION, AND DEBUGGING TOOL (NCAT), A UTILITY FOR COMPARING SCAN RESULTS (NDIFF), AND A PACKET GENERATION AND RESPONSE ANALYSIS TOOL (NPING). SOURCE: [HTTPS://NMAP.ORG/](https://nmap.org/)

WIRESHARK:-

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Source: <https://www.wireshark.org/>

6 – NESSUS

Nessus is the most trusted vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, use wizards to easily and quickly create

policies, schedule scans and send results via email. Nessus supports more technologies than any other vendor, including operating systems, network devices, hypervisors, databases, tablets/phones, web servers and critical infrastructure.

Source: <https://www.tenable.com/products/nessus-vulnerability-scanner>

7 – THC HYDRA

Number one of the biggest security holes are passwords, as every password security study shows. Hydra is a parallized login cracker which supports numerous protocols to attack.

New modules

are easy to add, beside that, it is flexible and very fast. Hydra was tested to compile on Linux, Windows/Cygwin, Solaris 11, FreeBSD 8.1, OpenBSD, OSX, QNX/Blackberry, and is made available under GPLv3 with a special OpenSSL license expansion.

Source: <https://www.thc.org/thc-hydra/>

8. SQL MAP:-

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Source: <http://sqlmap.org/>

9. WPS SCAN:-

WPS is an open source penetration testing tool that automates the process of detecting and exploiting wordpress websites. It comes with a powerful detection engine, many niche features for the ultimate penetration tester. we need kali linux or termux to use this tool. we will discuss later how to use wpscan to enumerate the username and how to hack wordpress website using bruteforce.

source:- <https://wpscan.org/>

10. RED HAWK:-

Red Hawk is an open source web applications tool that can be used for web information gathering

and vulnerability scanning purpose

HOW TO USE :- <https://darkwebsolutions.com/what-is-red-hawk/>

HOW TO HACK WEBSITES:-

For more visit :- <https://darkwebsolutions.com/how-to-hack-websites/>

nslookup103 - January 2, 2020, 11:13 am

your best friend is ping, nslookup, and tracert

creatine - January 27, 2020, 6:58 am

Found this on torrent site (Udemy (warez disallowed)-Burp-Suite-Bug-Bounty-Web-Hacking-from-Scratch) is this same as the burp suite tool tip nr 1 ?

Dotexe - January 27, 2020, 7:04 am

(Jan 27, 2020 07:58 AM)creatine Wrote: [\[CITE\]](#) Found this on torrent site (Udemy (warez disallowed) (warez disallowed)-Burp-Suite-Bug-Bounty-Web-Hacking-from-Scratch) is this same as the burp suite tool tip nr 1 ?

If that's the one i think of its totally not worth it, they are covering only the basics, you literally pay 20 bucks for 5 folders with 4-5 videos of 6mins each and covering only the basics. In fact back then when i needed networking i bought one course and the lecturer was explaining very well, also the folder consists of 68 other and each video was 35 to 45 minutes. So before you buy a course, make sure the content is worth it, and to answer your question, yes it is exactly the same tool.

creatine - January 27, 2020, 7:08 am

(Jan 27, 2020 08:04 AM)Dotexe Wrote: [\[CITE\]](#) If that's the one i think of its totally not worth it, they are covering only the basics, you literally pay 20 bucks for 5 folders with 4-5 videos of 6mins each and covering only the basics. In fact back then when i needed networking i bought one course and the lecturer was explaining very well, also the folder consists of 68 other and each video was 35 to 45 minutes. So before you buy a course, make sure the content is worth it, and to answer your question, yes it is exactly the same tool.

its free cracked version from torrent site and you are wright the are only video's but free anyway

Dotexe - January 27, 2020, 7:10 am

(Jan 27, 2020 08:08 AM)creatine Wrote: [\[CITE\]](#) its free cracked version from torrent site
Still, the content inside the course can be found on youtube, its up to you if you want to watch it. But if i were you i'd totally avoid downloading such torrents, already know the website you're talking about.

creatine - January 27, 2020, 7:14 am

found Burp Suite pro v2.1.0.7 plus keygen from haxnode

Dotexe - January 27, 2020, 7:19 am

(Jan 27, 2020 08:14 AM)creatine Wrote: [\[CITE\]](#) found Burp Suite pro v2.1.0.7 plus keygen from

haxnode

Let me tell you something,if you want to be a pentester, you can do bounties without the pro version. After few bounties (depends on the severity of course) you can afford pro license. Obviously you can download cracked version but what would be the point ? Pro version won't help you get more money just like that. It just gives you more functionality over the tool.

microdri72 - January 29, 2020, 8:39 pm

Dating logins is needs asap...

Zoosk/Ourtime/match.com/christianmingles.com/chemistry.com/seniormatch.com e.t.c

Cryptograph - February 3, 2020, 4:17 am

(Jan 2, 2020 12:13 PM)nslookup103 Wrote: [\[CITE\]](#) your best friend is ping, nslookup, and tracert
You seem pretty dovoted to nslookup by the looks of your username.

LordDragon - July 2, 2020, 8:03 am

Thanks for sharing this mate.

linkinpork - July 2, 2020, 11:42 am

(Jan 27, 2020 08:19 AM)Dotexe Wrote: [\[CITE\]](#) Let me tell you something,if you want to be a pentester, you can do bounties without the pro version. After few bounties (depends on the severity of course) you can afford pro license. Obviously you can download cracked version but what would be the point ? Pro version won't help you get more money just like that. It just gives you more functionality over the tool.

This. Just find a good persistent XSS and you already have 500 USD at very the least. Bonus points if you chain it to something more severe.

Even a low-severity (exploitable) bug can get you 100 bucks for sure.

Grats on losing exile mode lol (Btw I thought I was dying of corona so I got my original closed). Also I'm ditching the Tifa mascot because too much Rule 34.