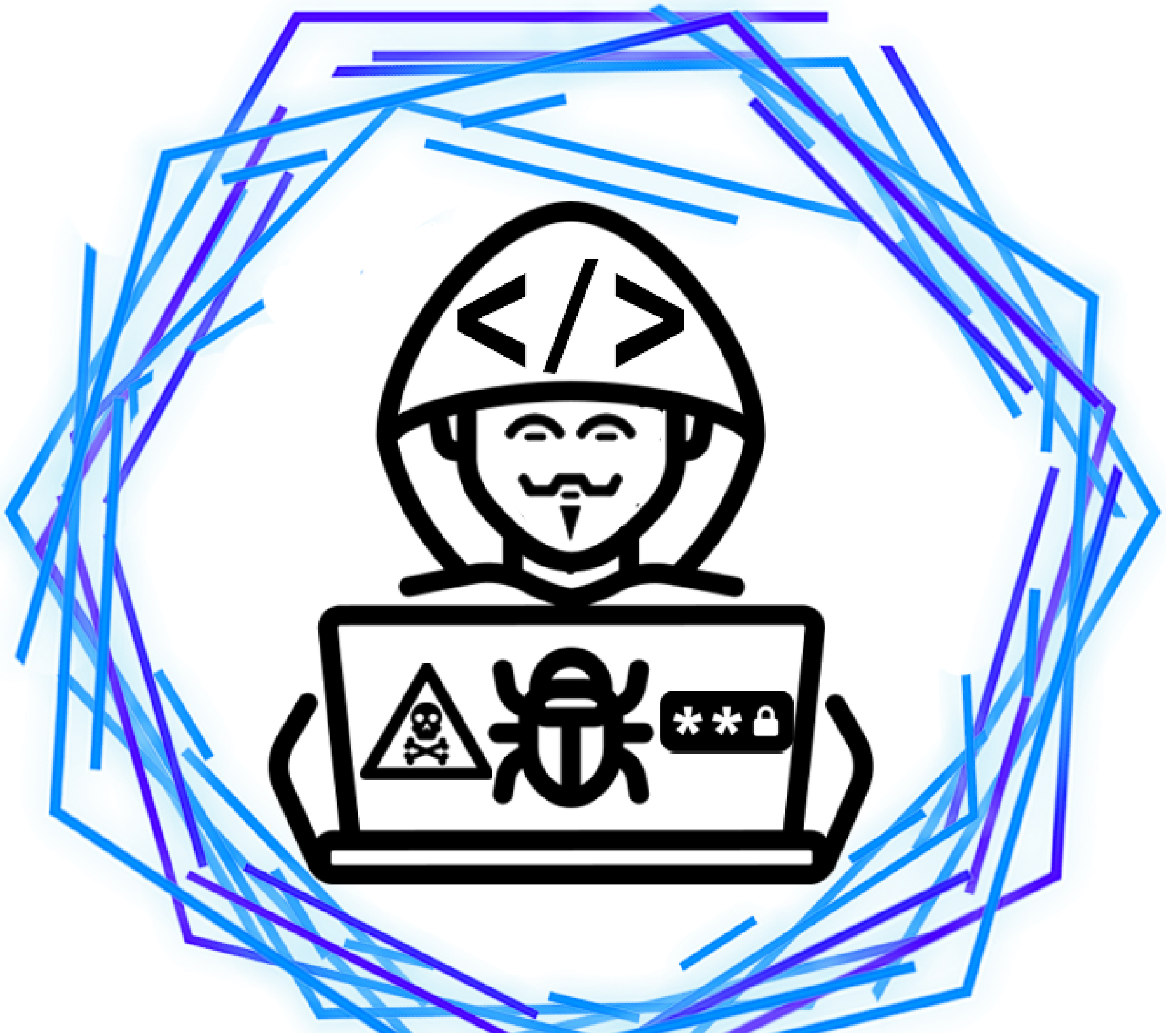


SecurityBreached
Cyber security Solutions.

Guide 001 |Getting Started in Bug Bounty Hunting..

June 3, 2019 / 14 Comments

A Noobs Guide to Getting Started in Bug Bounty Hunting | Muhammad Khizer Javed, whoami.securitybreached.org | aslicybersecurity.com | @KHIZER_JAVED47

> **“*No one will tell you anything or everything about this field, It’s a long strange path but you have to travel it alone with little help from others.*”**

> *“ I am still learning more about Bug Bounty Hunting and writing about this as I am learning, is my way of retaining the knowledge. and sharing what i learned so far and from internet.*

Bug Bounty Hunting is an exciting field to be in today, To define Bug Bounty in simple wording I'll day “**Bug Bounty is a reward paid to an Ethical Hacker for identifying and disclosing a potential security bug found in a participant's Web, Mobile or System.**”. But i hope as you're here already you know enough about bug bounty hunting that i don't need to define it to get into usual basics.

Now who am i? i already wrote a note like this in 2017 at **WHO AM I? And My Experiments with Hacking?** It contains some information about me and my experience and a basic guide but it's all mixed up and not really in details so i decided to write a new one read it if you like to know a bit about me otherwise i'll be moving the resources i shared there to this note with some details. I hope this blog will be helpful to you guys do let me know in comments if i missed something and you would like to add something or have any questions. This Blog contains Resources i have collected from all over the internet and adding them here to make a blog that contains 0-100 about getting started in Bug Bounty i'll try my best to mention each place i managed to get the resources from if somethings missed you know how to write a comment under a blog post. peace.\!

> First of all I want you guys to Read The article by Eric Raymond http://www.catb.org/esr/faqs/hacker-howto.html
> For Me It has become standard guideline for Starters.
> As Mentioned In This Article One of The Most Important Thing You Need to Have If You want Become a Hacker is Attitude!
>
> **To be a hacker, you have to develop some of these attitudes. But copping an attitude alone won't make you a hacker, any more than it will make you a champion athlete or a rock star. Becoming a hacker will take intelligence, practice, dedication, and hard work.Therefore, you have to learn to distrust attitude and respect competence of every kind. Hackers won't let posers waste their time, but they worship competence — especially competence at hacking, but competence at anything is valued. Competence at demanding skills that few can master is especially good, and competence at demanding skills that involve mental acuteness, craft, and concentration is best.If you revere competence, you'll enjoy developing it in yourself — the hard work and dedication will become a kind of intense play rather than drudgery. That attitude is vital to becoming a hacker.**

What You Should Know Before Starting to learn about Bug Bounty Hunting?

It’s Actually a Rough Road Ahead… ~Khizer

> **I’ll be writing this blog in 3 Major Phases were i’ll break down things to be as easy as possible, because the major audience in my mind right now is absolute beginners, or ones who have already tried learning or working but failed for some reason…**

Phase #01

- **Phase 01 is Based on Basics of Networks communication stuff, Programming & Automation.**

Well first of all to work on anything you need to know some very basic thing, that includes how a system works and how can you can make changes to it. Now let's start from very basics…

Web, HTTP & Network Basics:

Web:
Just for overview you should give a read to one of these

>https://www.tutorialspoint.com/web_developers_guide/web_basic_concepts.htm
>https://developers.google.com/web/fundamentals/security/
>http://www.alphadevx.com/a/7-The-Basics-of-Web-Technologies
>http://www.cs.kent.edu/~svirdi/Ebook/wdp/ch01.pdf

HTTP:

Communication is the key to success thus in order to learn something works on in our case how an application works and what it's flow is we need to learn how it communicates with you. and the Most basic thing i can think of is knowing about HTTP. Mentioning a few places you should definitely visit to get an idea about HTTP.

> https://www.w3.org/Protocols/
> https://www.w3schools.com/whatis/whatis_http.asp
> https://www.tutorialspoint.com/http/http_status_codes.htm
> https://www.tutorialspoint.com/http/http_url_encoding.htm
> https://www.tutorialspoint.com/http/http_requests.htm
> https://www.tutorialspoint.com/http/http_responses.htm
> https://www.hacker101.com/sessions/web_in_depth

What You'll basically learn from these is about HTTP Protocols, HTTP Requests, Response, Status Codes, Encoding/Decoding, and From the last URL you'll get to learn it under security perspective so you'll get to learn SOP, Cookie, MIEM & HTML Pharising. These will definitely help you later with Web app testing and stuff.

Networking:

A basic understanding of networking is important for anyone who's into computer. So a few resources to learn the basics of Networking.

>https://commotionwireless.net/docs/cck/networking/learn-networking-basics/
> https://commotionwireless.net/docs/cck/networking/learn-networking-basics/
> https://www.slideshare.net/variwalia/basic-to-advanced-networking-tutorials
> https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html
> http://www.penguintutor.com/linux/basic-network-reference

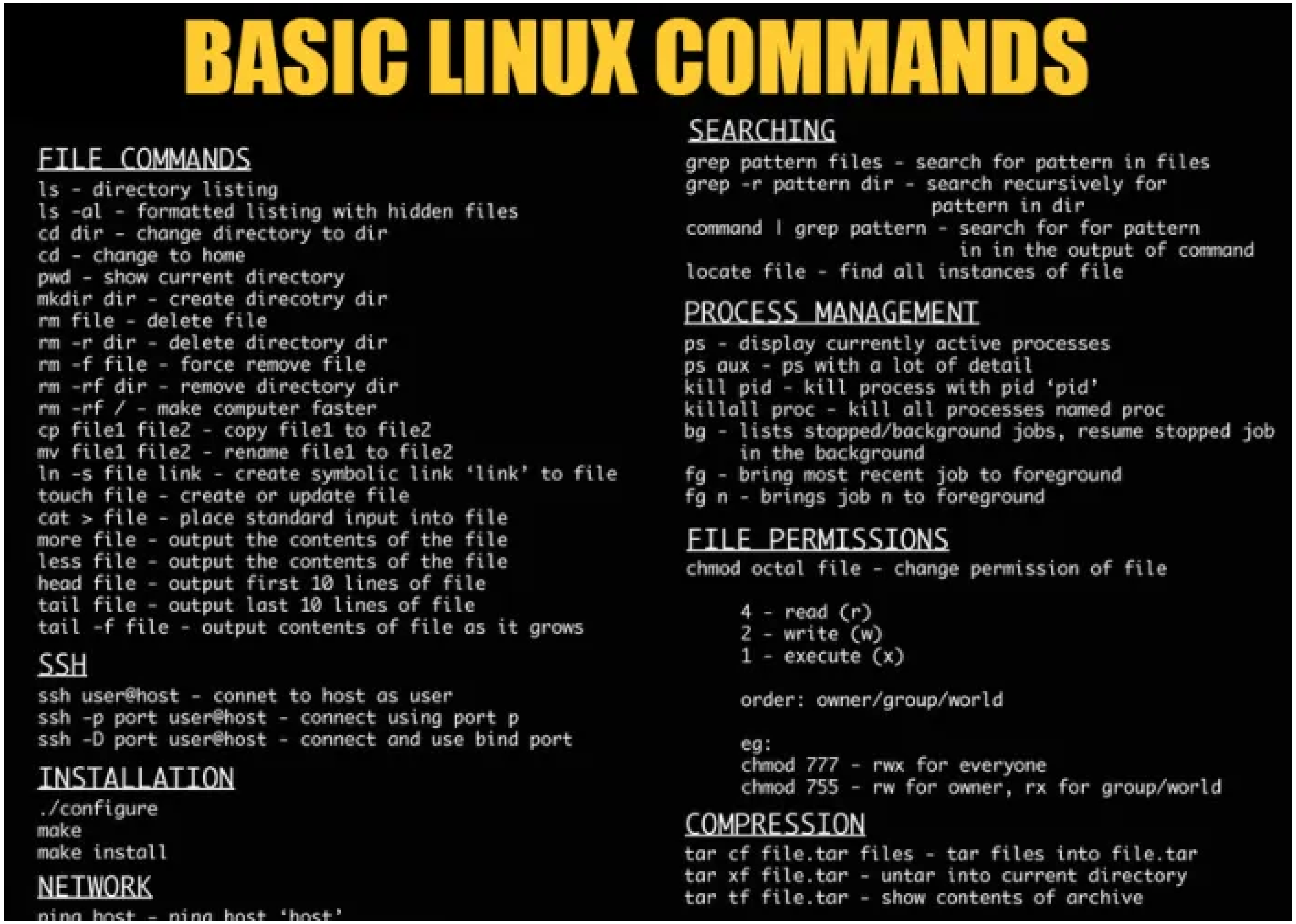
> https://www.utilizewindows.com/list-of-common-network-port-numbers/

> https://code.tutsplus.com/tutorials/an-introduction-to-learning-and-using-dns-records–cms-24704

> https://www.digitalocean.com/community/tutorials/an-introduction-to-networking-terminology-interfaces-and-protocols

Linux Commands:

>http://linuxcommand.org/



BASIC LINUX COMMANDS

FILE COMMANDS

```
ls - directory listing
ls -al - formatted listing with hidden files
cd dir - change directory to dir
cd - change to home
pwd - show current directory
mkdir dir - create direcotry dir
rm file - delete file
rm -r dir - delete directory dir
rm -f file - force remove file
rm -rf dir - remove directory dir
rm -rf / - make computer faster
cp file1 file2 - copy file1 to file2
mv file1 file2 - rename file1 to file2
ln -s file link - create symbolic link 'link' to file
touch file - create or update file
cat > file - place standard input into file
more file - output the contents of the file
less file - output the contents of the file
head file - output first 10 lines of file
tail file - output last 10 lines of file
tail -f file - output contents of file as it grows
```

SSH

```
ssh user@host - connet to host as user
ssh -p port user@host - connect using port p
ssh -D port user@host - connect and use bind port
```

INSTALLATION

```
./configure
make
make install
```

NETWORK

```
ping host - ping host 'host'
```

SEARCHING

```
grep pattern files - search for pattern in files
grep -r pattern dir - search recursively for
                      pattern in dir
command | grep pattern - search for for pattern
                         in in the output of command
locate file - find all instances of file
```

PROCESS MANAGEMENT

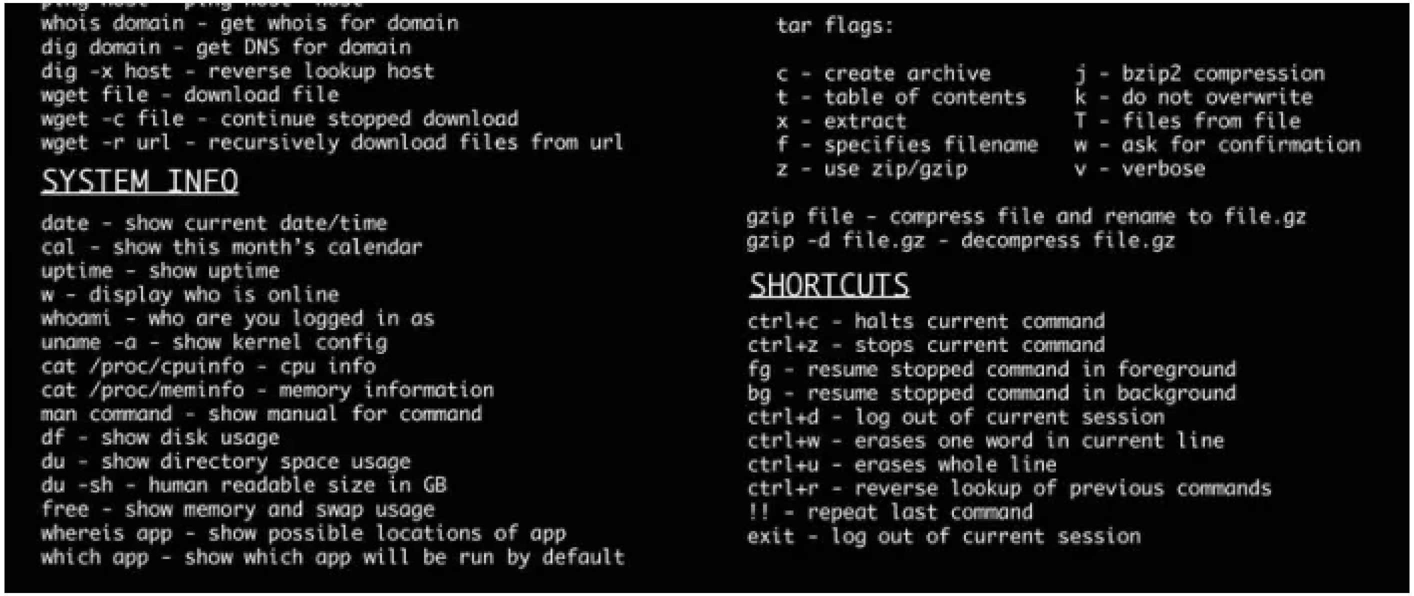
```
ps - display currently active processes
ps aux - ps with a lot of detail
kill pid - kill process with pid 'pid'
killall proc - kill all processes named proc
bg - lists stopped/background jobs, resume stopped job
     in the background
fg - bring most recent job to foreground
fg n - brings job n to foreground
```

FILE PERMISSIONS

```
chmod octal file - change permission of file

     4 - read (r)
     2 - write (w)
     1 - execute (x)

     order: owner/group/world

     eg:
     chmod 777 - rwx for everyone
     chmod 755 - rw for owner, rx for group/world
```

COMPRESSION

```
tar cf file.tar files - tar files into file.tar
tar xf file.tar - untar into current directory
tar tf file.tar - show contents of archive
```



```
whois domain - get whois for domain
dig domain - get DNS for domain
dig -x host - reverse lookup host
wget file - download file
wget -c file - continue stopped download
wget -r url - recursively download files from url
SYSTEM INFO
date - show current date/time
cal - show this month's calendar
uptime - show uptime
w - display who is online
whoami - who are you logged in as
uname -a - show kernel config
cat /proc/cpuinfo - cpu info
cat /proc/meminfo - memory information
man command - show manual for command
df - show disk usage
du - show directory space usage
du -sh - human readable size in GB
free - show memory and swap usage
whereis app - show possible locations of app
which app - show which app will be run by default
```

```
  tar flags:

  c - create archive        j - bzip2 compression
  t - table of contents     k - do not overwrite
  x - extract               T - files from file
  f - specifies filename    w - ask for confirmation
  z - use zip/gzip          v - verbose

gzip file - compress file and rename to file.gz
gzip -d file.gz - decompress file.gz
SHORTCUTS
ctrl+c - halts current command
ctrl+z - stops current command
fg - resume stopped command in foreground
bg - resume stopped command in background
ctrl+d - log out of current session
ctrl+w - erases one word in current line
ctrl+u - erases whole line
ctrl+r - reverse lookup of previous commands
!! - repeat last command
exit - log out of current session
```

What You'll learn from these are basics of Networking, TCP/ID, DNS, Network terminologies & Linux commands etc. These will definitely help you later with Recon Process.

> *"Learn to make it; then break it!*

Programming/Coding:

To be a Good Hacker you don't really need to be a Good Programmer but it's always Good to cover this before going in Any form of Computer Hacking or Bug Bounty in general. Also Sometimes It increases your chances of successfully identifying and exploiting a vulnerability and also you may need code to escalate a bug with a low/medium severity to high/critical.
I Personally suffered for two year in bug bounties because in many cases i couldn't really understands what the particular code means, couldn't exploit an issue properly or couldn't even code in general, and I'm, still trying my best to catch up to speed so i'll suggest you

guys not to skip these parts and go directly towards Bug Bounties.
Now I'll suggest a few languages that one should properly have basic to medium level knowledge about and keep advancing it.

HTML:

> https://www.w3schools.com/html/
> https://www.codecademy.com/learn/learn-html
> https://learn.shayhowe.com/advanced-html-css/
> https://htmldog.com/guides/html/advanced/

PHP:

> https://www.w3schools.com/php/
> https://stackify.com/learn-php-tutorials/
> https://www.codecademy.com/learn/learn-php
> https://www.guru99.com/php-tutorials.html
> https://www.codecademy.com/learn/paths/web-development

JavaScript:

> https://www.youtube.com/watch?v=PkZNo7MFNFg
> https://www.codecademy.com/learn/introduction-to-javascript
> https://learnjavascript.today/
> https://www.thebalancecareers.com/learn-javascript-online-2071405

SQL(Structured Query Language):

> https://www.youtube.com/watch?v=HXV3zeQKqGY
> https://www.w3schools.com/sql/
> https://www.codecademy.com/learn/learn-sql

> http://www.sqlcourse.com/

C/C++
>https://www.youtube.com/watch?v=vLnPwxZdW4Y
>https://www.learncpp.com/
>https://www.codecademy.com/learn/learn-c-plus-plus
>https://www.sololearn.com/Course/CPlusPlus/
>https://www.learn-c.org/
>https://www.youtube.com/watch?v=KJgsSFOSQv0

Java:
>https://www.codecademy.com/learn/learn-java
>https://www.geeksforgeeks.org/java-how-to-start-learning-java/
>https://www.learnjavaonline.org/
>https://www.youtube.com/watch?v=grEKMHGYyns

What You'll learn from them is not just Programming languages but the proper way of web and systems to communicate that you gonna test, I'm no expert or even a starter i'm just a learner in Programming so sharing the resources i'm currently following. Like you know XSS, HTML injections, PHP Injections, SQLi etc and Many other vulnerabilities you can't exploit properly unless you know the code that runs behind and knows exactly how to communicate so that's why is learning them are important to get a good start.

Adding Automation to your work:

"Never send a human to do a machine's job"

Well As you know sometimes you need to so your work faster and more efficiently so the best way i think for it is Automating your work not gonna get to much into depth of it as it's something i myself is just getting familiar about.. so You can read more about Importance of Automation for a Bug Bounty Hunter at
https://pentester.land/conference-notes/2018/07/25/bug-bounty-talks-2017-automation-for-bug-hunters.html
I'll just share here my notes for what languages i'm following and looking forward to be good at..

Python:
> https://realpython.com/
> https://docs.python.org/3/tutorial/
>https://drive.google.com/drive/u/0/folders/0ByWO0aO1eI_MT1E1NW91VlJ2TVk?fbclid=IwAR35WNZwBQudINaZ10I5ZA2YDQdtNXSEwRyEiLEK91_csJ7ekN1ut7AQNeQ

Bash:
> https://www.tutorialspoint.com/unix/shell_scripting.htm
> https://www.learnshell.org/
> https://medium.com/quick-code/top-tutorials-to-learn-shell-scripting-on-linux-platform-c250f375e0e5

Ruby:
> https://www.learnrubyonline.org/
> https://www.codecademy.com/learn/learn-ruby

Golang:
> https://tour.golang.org/welcome/1
> https://www.udemy.com/learn-go-the-complete-bootcamp-course-golang/

What You'll learn from these is to code your own tools and understand many other common tools and modify them according to your needs. Ofc one can't learn all these but should try to get grip on one he likes and get to understand others.

So Till Here I'll say you already knew all the basics, was good around PHP, JS & HTML stuff & also was good around Scripting & SQL or maybe learned a bit or these and gave it a good time i'll say a fews weeks maybe… Then Congrats you have already gone through **Phase #01** This means that You have done 39% Of Learning Work towards being a good Bug Hunter/ Ethical Hacker.. Just keep a practicing i myself is still learning this phase because 4 years ago when i started i skipped this part for no reason and then had to see many things differently so i hope you guys won't have an issue if you go through the First Phase easily.

Phase #02

- **Phase 02 is Based on Learning about Vulnerabilities, Resources to follow to learn them, Places to practice & Tools etc**.

> ***"Being a hacker is lots of fun, but it's a kind of fun that takes lots of effort. The effort takes motivation."***

Now let's start with basic learning about InfoSec the first and really most important step would be to choose a proper initial path that you are going to start learning. Choosing a right path to start in Bug Bounty is very important. It totally depends upon your interest, like some people choose Web Application path first coz it's easy to learn and go through than mobile and others… (***Some of the resources are moved here from my old blog that's i'm going to remove but these are updated and properly arranged by my experience***)

I'll focus on Web, & Mobile Here coz this is what my interest is.

Before I add anything else i'll suggest You to actually go through

Hacker101 By HackerOne https://www.hacker101.com/
And
Bugcrowd University https://www.bugcrowd.com/hackers/bugcrowd-university/

Both of these contains Huge list of resources and lectures that can help you in even a better way than many of us can't but as you guys are following this as well so i decided to add them here also.

Web App Security:

Before I Suggest you what to Learn first if you follow my suggested path I'll like to tell you some ways you can practice your skills..

CTF(Capture The Flag):
Now to practice for Bug Bounties you can participate in CTF challenges. Just like the name suggests "Capture The Flag" there are several challenges for you to solve which deals with real-world vulnerabilities. The more you practice on these challenges the more you will learn about the different technologies required to break into an application or a system.

For Web App I'll suggest you guys to read the following books & guides first

>https://www.packtpub.com/networking-and-servers/mastering-modern-web-penetration-testing
>https://www.amazon.com/Hackers-Underground-Handbook-secure-systems/dp/1451550189
>https://leanpub.com/web-hacking-101
>https://www.amazon.com/gp/product/1593275641/
>https://www.amazon.com/gp/product/1512214566/
>https://www.amazon.com/Tangled-Web-Securing-Modern-Applications-ebook/dp/B006FZ3UNI/

By Reading these books you will get a good knowledge about Web App pentesting & Security testing in general and in depth.

In addition to these Books i'll suggest you guys should really give good time reading and understanding OWASP Testing Guide & OWASP Top 10 Vulnerabilities from 2010-2017

OWASP Testing project:
>https://www.owasp.org/index.php/OWASP_Testing_Project

OWASP Top 10 Project:
>https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2010
>https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013
>https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Adding a Few basic Pdfs for you guys to go though and save locally to you can keep it revised and keep learning from them.. i'll say they gonna help you almost a hundred percent of the time. So do give these a good time

> **Kali linux Revealed** https://docs.kali.org/pdf/kali-book-en.pdf

> **Nmap Cheat Sheet** https://s3-us-west-2.amazonaws.com/stationx-public-download/nmap_cheet_sheet_0.6.pdf
> **Metasploit Cheat Sheet:** https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

Now by this point i'll say You have done Good enough research and given good time to practice and learn that you can jump into a Bug Bounty Program to test in real life environment outside CTF, or test environments.
So you can happily jump to the pages at

https://bugcrowd.com/programs
https://hackerone.com/directory

And Select a Program But I'll suggest you to read till the end.

Following all of them books, testing guides you might have an idea of vulnerabilities so i'll name a few common ones and try to give good reference to learn them easily.

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

References to read:

>https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/?utm_campaign=Incapsula-moved
>https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
>https://www.netsparker.com/blog/web-security/csrf-cross-site-request-forgery/

Some POCs:

- CSRF Account Takeover famebit by Hassan Khan
- Hacking PayPal Accounts with one click (Patched) by Yasser Ali
- Add tweet to collection CSRF by vijay kumar
- Facebookmarketingdevelopers.com: Proxies, CSRF Quandry and API Fun by phwd
- How i Hacked your Beats account ? Apple Bug Bounty by @aaditya_purani
- Paypal bug bounty: Updating the Paypal.me profile picture without consent (CSRF attack) by Florian Courtial
- CSRF Account Takeover by Vulnerables
- Uber CSRF Account Takeover by Ron Chan
- Messenger.com CSRF that show you the steps when you check for CSRF by Jack Whitton

Cross-Site Scripting (XSS)

XSS enables attackers to inject client-side scripts into web pages viewed by other users.

References to read:

>https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
>https://portswigger.net/web-security/cross-site-scripting
>https://excess-xss.com/

Some POCs:

- AirBnb Bug Bounty: Turning Self-XSS into Good-XSS #2 by geekboy

- Uber Self XSS to Global XSS
- How I found a $5,000 Google Maps XSS (by fiddling with Protobuf) by Marin MoulinierFollow
- Airbnb – When Bypassing JSON Encoding, XSS Filter, WAF, CSP, and Auditor turns into Eight Vulnerabilities by Brett
- XSSI, Client Side Brute Force
- postMessage XSS Bypass
- XSS in Uber via Cookie by zhchbin
- Stealing contact form data on www.hackerone.com using Marketo Forms XSS with postMessage frame-jumping and jQuery-JSONP by frans
- XSS due to improper regex in third party js Uber 7k XSS
- XSS in TinyMCE 2.4.0 by Jelmer de Hen
- Pass uncoded URL in IE11 to cause XSS
- Twitter XSS by stopping redirection and javascript scheme by Sergey Bobrov

- Microsoft XSS and Twitter XSS
- Google Japan Book XSS
- Flash XSS mega nz – by frans
- Flash XSS in multiple libraries – by Olivier Beg
- xss in google IE, Host Header Reflection
- Years ago Google xss
- xss in google by IE weird behavior
- xss in Yahoo Fantasy Sport
- xss in Yahoo Mail Again, worth $10000 by Klikki Oy
- Sleeping XSS in Google by securityguard
- Decoding a .htpasswd to earn a payload of money by securityguard
- Google Account Takeover

- Sleeping stored Google XSS Awakens a $5000 Bounty by Patrik Fehrenbach
- RPO that lead to information leakage in Google by filedescriptor
- God-like XSS, Log-in, Log-out, Log-in in Uber by Jack Whitton
- Three Stored XSS in Facebook by Nirgoldshlager
- Using a Braun Shaver to Bypass XSS Audit and WAF by Frans Rosen
- An XSS on Facebook via PNGs & Wonky Content Types by Jack Whitton
    - he is able to make stored XSS from a irrelevant domain to main facebook domain
- Stored XSS in *.ebay.com by Jack Whitton
- Complicated, Best Report of Google XSS by Ramzes
- Tricky Html Injection and Possible XSS in sms-be-vip.twitter.com by secgeek
- Command Injection in Google Console by Venkat S
- Facebook's Moves – OAuth XSS by PAULOS YIBELO
- Stored XSS in Google Docs (Bug Bounty) by Harry M Gertos
- Stored XSS on developer.uber.com via admin account compromise in Uber by James Kettle (albinowax)
- Yahoo Mail stored XSS by Klikki Oy
- Abusing XSS Filter: One ^ leads to XSS(CVE-2016-3212) by Masato Kinugawa
- Youtube XSS by fransrosen
- Best Google XSS again – by Krzysztof Kotowicz
- IE & Edge URL parsin Problem – by detectify
- Google XSS subdomain Clickjacking

SQL Injection

SQL injection, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

References to read:

>https://www.owasp.org/index.php/SQL_Injection
>https://portswigger.net/web-security/sql-injection
>https://www.imperva.com/learn/application-security/sql-injection-sqli/
>https://www.w3schools.com/sql/sql_injection.asp

Some POCs:

- SQL Injection Vulnerability nutanix by Muhammad Khizer Javed
- Yahoo – Root Access SQL Injection – tw.yahoo.com by Brett Buerhaus
- Multiple vulnerabilities in a WordPress plugin at drive.uber.com by Abood Nour (syndr0me)
- GitHub Enterprise SQL Injection by Orange
- SQL injection in WordPress Plugin Huge IT Video Gallery in Uber by glc
- SQL Injection on sctrack.email.uber.com.cn by Orange Tsai

Remote Code Execution (RCE)

In RCE an attacker's able to execute arbitrary commands or code on a target machine or in a target Machine.

References to read:

>https://www.netsparker.com/blog/web-security/remote-code-evaluation-execution/
>https://en.wikipedia.org/wiki/Arbitrary_code_execution

Some POCs:

- How we broke PHP, hacked Pornhub and earned $20,000 by Ruslan Habalov
    - *Alert*, God-like Write-up, make sure you know what is ROP before clicking, which I don't =(
- RCE deal to tricky file upload by secgeek
- WordPress SOME bug in plupload.flash.swf leading to RCE in Automatic by Cure53 (cure53)
- Read-Only user can execute arbitraty shell commands on AirOS by 93c08539 (93c08539)
- Remote Code Execution by impage upload! by Raz0r (ru_raz0r)
- Popping a shell on the Oculus developer portal by Bitquark
- Crazy! PornHub RCE AGAIN!!! How I hacked Pornhub for fun and profit – 10,000$ by 5haked
- PayPal Node.js code injection (RCE) by Michael Stepankin
- eBay PHP Parameter Injection lead to RCE
- Yahoo Acqusition RCE
- Command Injection Vulnerability in Hostinger by @alberto__segura
- RCE in Airbnb by Ruby Injection by buerRCE
- RCE in Imgur by Command Line
- RCE in git.imgur.com by abusing out dated software by Orange Tsai
- RCE in Disclosure
- Remote Code Execution by struct2 Yahoo Server
- Command Injection in Yahoo Acquisition
- Paypal RCE
- $50k RCE in JetBrains IDE
- $20k RCE in Jenkin Instance by @nahamsec

- JDWP Remote Code Execution in PayPal by Milan A Solanki
- XXE in OpenID: one bug to rule them all, or how I found a Remote Code Execution flaw affecting Facebook's servers by Reginaldo Silva
- How I Hacked Facebook, and Found Someone's Backdoor Script by Orange Tsai

- How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE! by Orange Tsai
- uber.com may RCE by Flask Jinja2 Template Injection by Orange Tsai
- Yahoo Bug Bounty – *.login.yahoo.com Remote Code Execution by Orange Tsai (in Chinese)
- Google App Engine RCE by Ezequiel Pereira

- Exploiting ImageMagick to get RCE on Polyvore (Yahoo Acquisition) by NaHamSec
- Exploting ImageMagick to get RCE on HackerOne by c666a323be94d57
- Trello bug bounty: Access server's files using ImageTragick by Florian Courtial
- 40k fb rce
- Yahoo Bleed 1
- Yahoo Bleed 2

Insecure Direct Object Reference (IDOR)

In IDOR an application provides **direct** access to **objects** based on the user-supplied input. As a result of this vulnerability, attackers can bypass authorization and access resources in the system directly.

References to read:

>https://www.bugcrowd.com/blog/how-to-find-idor-insecure-direct-object-reference-vulnerabilities-for-large-bounty-rewards/
>https://www.owasp.org/index.php/Testing_for_Insecure_Direct_Object_References_(OTG-AUTHZ-004)
>https://www.secjuice.com/idor-insecure-direct-object-reference-definition/

Some POCs:

- DOB disclosed using "Facebook Graph API Reverse Engineering" by Raja Sekar Durairaj

- Change the description of a video without publish_actions permission in Facebook by phwd
- Response To Request Injection (RTRI) by ?, be honest, thanks to this article, I have found quite a few bugs because of using his method, respect to the author!
- Leak of all project names and all user names , even across applications on Harvest by Edgar Boda-Majer (eboda)
- Changing paymentProfileUuid when booking a trip allows free rides at Uber by Matthew Temmy (temmyscript)
- View private tweet
- Uber Enum UUID
- Hacking Facebook's Legacy API, Part 1: Making Calls on Behalf of Any User by Stephen Sclafani
- Hacking Facebook's Legacy API, Part 2: Stealing User Sessions by Stephen Sclafani
- Delete FB Video
- Delete FB Video
- Facebook Page Takeover by Manipulating the Parameter by arunsureshkumar
- Viewing private Airbnb Messages
- IDOR tweet as any user by kedrisec
- Classic IDOR endpoints in Twitter
- Mass Assignment, Response to Request Injection, Admin Escalation by sean

- Trello bug bounty: The websocket receives data when a public company creates a team visible board by Florian Courtial
- Trello bug bounty: Payments informations are sent to the webhook when a team changes its visibility by Florian Courtial
- Change any user's password in Uber by mongo
- Vulnerability in Youtube allowed moving comments from any video to another by secgeek
  - It's *Google* Vulnerability, so it's worth reading, as generally it is more difficult to find Google vulnerability
- Twitter Vulnerability Could Credit Cards from Any Twitter Account by secgeek
- One Vulnerability allowed deleting comments of any user in all Yahoo sites by secgeek
- Microsoft-careers.com Remote Password Reset by Yaaser Ali
- How I could change your eBay password by Yaaser Ali

- Duo Security Researchers Uncover Bypass of PayPal’s Two-Factor Authentication by Duo Labs
- Hacking Facebook.com/thanks Posting on behalf of your friends! by Anand Prakash
- How I got access to millions of [redacted] accounts
- All Vimeo Private videos disclosure via Authorization Bypass with Excellent Technical Description by Enguerran Gillier (opnsec)
- Urgent: attacker can access every data source on Bime by Jobert Abma (jobert)
- Downloading password protected / restricted videos on Vimeo by Gazza (gazza)
- Get organization info base on uuid in Uber by Severus (severus)
- How I Exposed your Primary Facebook Email Address (Bug worth $4500) by Roy Castillo

Unrestricted File Upload

As in name unrestricted file upload allows user to upload malicious file to a system to further exploit to for Code execution

References to read:

>https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/unrestricted-file-upload/
>https://www.owasp.org/index.php/Unrestricted_File_Upload
>https://www.hackingarticles.in/5-ways-file-upload-vulnerability-exploitation/

Some POCs:

- File Upload XSS in image uploading of App in mopub by vijay kumar
- RCE deal to tricky file upload by secgeek
- File Upload XSS in image uploading of App in mopub in Twitter by vijay kumar (vijay_kumar1110)
- Unrestricted File Upload to RCE by Muhammad Khizer Javed

XML External Entity Attack (XXE)

XXE is an attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.

References to read:

>https://portswigger.net/web-security/xxe
>https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet
>https://phonexicum.github.io/infosec/xxe.html

Some POCs:

- XXE through SAML
- XXE in Uber to read local files
- XXE by SVG in community.lithium.com
- How we got read access on Google's production servers by detectify
- Blind OOB XXE At UBER 26+ Domains Hacked by Raghav Bisht

Local File Inclusion (LFI)

The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation.

References to read:

>https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion
>https://www.netsparker.com/blog/web-security/local-file-inclusion-vulnerability/
>https://medium.com/@Aptive/local-file-inclusion-lfi-web-application-penetration-testing-cc9dc8dd3601

Some POCs:

- SSRF to LFI
- Disclosure Local File Inclusion by Symlink
- Facebook Symlink Local File Inclusion
- Gitlab Symlink Local File Inclusion
- Gitlab Symlink Local File Inclusion Part II
- Multiple Company LFI
- LFI by video conversion, excited about this trick!

Subdomain Takeover

A process of registering a non-existing domain name to gain control over another domain.

References to read:

>https://blog.securitybreached.org/2017/10/11/what-is-subdomain-takeover-vulnerability/
>https://0xpatrik.com/subdomain-takeover-basics/
>https://github.com/EdOverflow/can-i-take-over-xyz

Some POCs:

- Hijacking tons of Instapage expired users Domains & Subdomains by geekboy
- Reading Emails in Uber Subdomains
- Slack Bug Journey – by David Vieira-Kurz
- Subdomain takeover and chain it to perform authentication bypass by Arne Swinnen
- UBER Wildcard Subdomain Takeover by Muhammad Khizer Javed
- Lamborghini Subdomain Takeover Through Expired Cloudfront Distribution by Muhammad Khizer Javed
- Subdomain Takeover via Unsecured S3 Bucket Connected to the Website by Muhammad khizer Javed

Server Side Request Forgery (SSRF)

by SSRF the attacker can abuse functionality on the server to read or update internal resources.

References to read:

>https://medium.com/@madrobot/ssrf-server-side-request-forgery-types-and-ways-to-exploit-it-part-1-29d034c27978
>https://www.owasp.org/index.php/Server_Side_Request_Forgery
>https://www.netsparker.com/blog/web-security/server-side-request-forgery-vulnerability-ssrf/
>https://blog.detectify.com/2019/01/10/what-is-server-side-request-forgery-ssrf/

Some POCs:

- ESEA Server-Side Request Forgery and Querying AWS Meta Data by Brett Buerhaus
- SSRF to pivot internal network
- SSRF to LFI
- SSRF to query google internal server
- SSRF by using third party Open redirect by Brett BUERHAUS

- SSRF tips from BugBountyHQ of Images
- SSRF to RCE
- XXE at Twitter
- Blog post: Cracking the Lens: Targeting HTTP's Hidden Attack-Surface

Some Other Interesting POCS:

A huge collection at https://github.com/djadmin/awesome-bug-bounty

Deserialization

- Java Deserialization in manager.paypal.com by Michael Stepankin
- Instagram's Million Dollar Bug by Wesley Wineberg
- (Ruby Cookie Deserialization RCE on facebooksearch.algolia.com by Michiel Prins (michiel)
- Java deserialization by meals

Race Condition

- Race conditions on Facebook, DigitalOcean and others (fixed) by Josip Franjković
- Race Conditions in Popular reports feature in HackerOne by Fábio Pires (shmoo)

Business Logic Flaw

- Facebook simple technical hack to see the timeline by Ashish Padelkar
- How I Could Steal Money from Instagram, Google and Microsoft by Arne Swinnen
- How I could have removed all your Facebook notes

- Facebook – bypass ads account's roles vulnerability 2015 by POUYA DARABI
- Uber Ride for Free by anand praka
- Uber Eat for Free by

Authentication Bypass

- OneLogin authentication bypass on WordPress sites via XMLRPC in Uber by Jouko Pynnönen (jouko)
- 2FA PayPal Bypass by henryhoggard
- SAML Bug in Github worth 15000
- Authentication bypass on Airbnb via OAuth tokens theft
- Uber Login CSRF + Open Redirect -> Account Takeover at Uber
- [http://c0rni3sm.blogspot.hk/2017/08/accidentally-typo-to-bypass.html?m=1](Administrative Panel Access) by c0rni3sm
- Uber Bug Bounty: Gaining Access To An Internal Chat System by mishre

HTTP Header Injection

- Twitter Overflow Trilogy in Twitter by filedescriptor
- Twitter CRLF by filedescriptor
- Adblock Plus and (a little) more in Google
- $10k host header by Ezequiel Pereira

Email Related

- This domain is my domain – G Suite A record vulnerability
- I got emails – G Suite Vulnerability
- How I snooped into your private Slack messages [Slack Bug bounty worth $2,500]

- Reading Uber's Internal Emails [Uber Bug Bounty report worth $10,000]
- Slack Yammer Takeover by using TicketTrick by Inti De Ceukelaire
- How I could have mass uploaded from every Flickr account!

Money Stealing

- Round error issue -> produce money for free in Bitcoin Site by 4lemon

Others

- Payment Flaw in Yahoo
- Bypassing Google Email Domain Check to Deliver Spam Email on Google's Behalf
- When Server Side Request Forgery combine with Cross Site Scripting

- SAML Pen Test Good Paper
- A list of FB writeup collected by phwd by phwd
- NoSQL Injection by websecurify
- CORS in action
- CORS in Fb messenger
- Web App Methodologies
- XXE Cheatsheet
- The road to hell is paved with SAML Assertions, Microsoft Vulnerability
- Study this if you like to learn Mongo SQL Injection by cirw
- Mongo DB Injection again by websecrify
- w3af speech about modern vulnerability by w3af

- Web cache attack that lead to account takeover
- A talk to teach you how to use SAML Raider
- XSS Checklist when you have no idea how to exploit the bug
- CTF write up, Great for Bug Bounty
- It turns out every site uses jquery mobile with Open Redirect is vulnerable to XSS by sirdarckcat
- Bypass CSP by using google-analytics
- Payment Issue with Paypal
- Browser Exploitation in Chinese
- XSS bypass filter
- Markup Impropose Sanitization
- Breaking XSS mitigations via Script Gadget
- X41 Browser Security White Paper

So these were some common issues that one should get a grip on and learn more and more about Following is a list of some Attacks Topics that You Should do some research and read the Blogs/reports on them..

- **Sql Injection Attack**
- **Hibernate Query Language Injection**
- **Direct OS Code Injection**
- **XML Entity Injection**
- **Broken Authentication and Session Management**
- **Cross-Site Scripting (XSS)**
- **Insecure Direct Object References**
- **Missing Function Level Access Control**
- **Cross-Site Request Forgery (CSRF)**
- **Using Components with Known Vulnerabilities**

- Unvalidated Redirects and Forwards
- ClickJacking Attacks
- DNS Cache Poisoning
- Symlinking
- Remote Code Execution Attacks
- Remote File inclusion
- Local file inclusion
- Denial oF Service Attack
- PHPwn
- NAT Pinning
- XSHM
- HTTP Parameter Pollution
- Tabnabbing
- LDAP injection
- Log Injection
- Path Traversal
- Reflected DOM Injection
- Repudiation Attack
- Resource Injection
- Server-Side Includes (SSI) Injection
- Session fixation
- Session hijacking attack
- Session Prediction
- Setting Manipulation
- Special Element Injection
- SMTP injection

- **Traffic flood**
- **XPATH Injection**

BLOGS! You should read.

Lets Get Towards Blogs!There are Plenty of Blogs Shared By Hackers on Daily Basis That You can read to learn More and More……….

- https://blog.it-securityguard.com/
- https://blog.innerht.ml/
- http://brutelogic.com.br/blog/
- https://klikki.fi/
- http://philippeharewood.com/
- https://seanmelia.wordpress.com/
- https://respectxss.blogspot.com/
- https://www.gracefulsecurity.com/
- https://whitton.io/
- https://tisiphone.net/
- http://archive.nahamsec.com/
- https://www.hackerscreed.org/
- http://danlec.com/blog
- https://wehackpeople.tumblr.com/
- https://bitquark.co.uk/blog/
- https://www.arneswinnen.net/
- http://bugbountypoc.com/
- https://medium.com/@arbazhussain/
- http://www.shawarkhan.com/

- https://blog.detectify.com/
- http://www.rafayhackingarticles.net/...
- https://forum.bugcrowd.com/
- https://securitywall.co/
- https://www.hackerone.com/blog
- http://www.securitytube.net/
- https://hackasia.org/
- http://www.gangte.net/
- https://mukarramkhalid.com/
- https://securitytraning.com/
- https://jubaeralnaziwhitehat.wordpress.com/...
- http://hackaday.com/
- http://www.securityfocus.com/
- https://packetstormsecurity.com/
- http://www.blackhat.com/
- https://www.metasploit.com/
- http://sectools.org/
- https://labs.detectify.com/
- https://blog.rubidus.com/
- http://www.securityidiots.com/
- https://hackernoon.com/
- https://sqli-basic.blogspot.com/
- https://bugbaba.blogspot.in/
- https://vulnerability-lab.com/
- https://medium.com/@know.0nix/
- https://medium.com/@codingkarma/

These are some Of the Websites That I like to Visit regularly to b updated and Read Their Articles………. There are Plenty of Other Blogs, Websites That are Missing from This List so be sure to add them In comments.

YouTube Channels! You should follow.

Now Lets get Towards YouTube Channel Links… These Channels are Shared By Hackers where They Upload their Video POCs.. Watching them u can actually understand how to demonstrate these type of attacks …

https://www.youtube.com/channel/UCP…
https://www.youtube.com/channel/UCJ…
https://www.youtube.com/channel/UCR…
https://www.youtube.com/channel/UCY…
https://www.youtube.com/channel/UCw…
https://www.youtube.com/channel/UCa…
https://www.youtube.com/channel/UCt…
https://www.youtube.com/channel/UC5…
https://www.youtube.com/channel/UCM…
https://www.youtube.com/channel/UC_…
https://www.youtube.com/channel/UCq…
https://www.youtube.com/channel/UCV…
https://www.youtube.com/channel/UCs…
https://www.youtube.com/channel/UCa…
https://www.youtube.com/channel/UCP…
https://www.youtube.com/channel/UCX…
https://www.youtube.com/channel/UC4…
https://www.youtube.com/channel/UCs…

https://www.youtube.com/channel/UCo...
https://www.youtube.com/channel/UCy...
https://www.youtube.com/channel/UCS...
https://www.youtube.com/channel/UCO...
https://www.youtube.com/channel/UCh...
https://www.youtube.com/channel/UCo...
https://www.youtube.com/channel/UC9...
https://www.youtube.com/channel/UCe...
https://www.youtube.com/channel/UC2...
https://www.youtube.com/channel/UCP...
https://www.youtube.com/channel/UCz...

Any Channel Link Missing? Kindly add it in Comments

Another advice…… Regularly follow http://h1.nobbd.de/ to b updated with HackerOne Public Bug reports You can learn alot from them

Alternatively You can Join Slack Community for Hackers
https://bugbounty-world.slack.com/
https://bugbountyforum.com/

Tools! You should try out.

dnscan https://github.com/rbsec/dnscan
Knockpy https://github.com/guelfoweb/knock
Sublist3r https://github.com/aboul3la/Sublist3r
massdns https://github.com/blechschmidt/massdns

nmap https://nmap.org

masscan https://github.com/robertdavidgraham/masscan

EyeWitness https://github.com/ChrisTruncer/EyeWitness

DirBuster https://sourceforge.net/projects/dirbuster/

dirsearch https://github.com/maurosoria/dirsearch

Gitrob https://github.com/michenriksen/gitrob

git-secrets https://github.com/awslabs/git-secrets

sandcastle https://github.com/yasinS/sandcastle

bucket_finder https://digi.ninja/projects/bucket_finder.php

GoogD0rker https://github.com/ZephrFish/GoogD0rker/

Wayback Machine https://web.archive.org

waybackurls https://gist.github.com/mhmdiaa/adf6bff70142e5091792841d4b372050 Sn1per https://github.com/1N3/Sn1per/

XRay https://github.com/evilsocket/xray

wfuzz https://github.com/xmendez/wfuzz/

patator https://github.com/lanjelot/patator

datasploit https://github.com/DataSploit/datasploit

hydra https://github.com/vanhauser-thc/thc-hydra

changeme https://github.com/ztgrace/changeme

MobSF https://github.com/MobSF/Mobile-Security-Framework-MobSF/ Apktool https://github.com/iBotPeaches/Apktool

dex2jar https://sourceforge.net/projects/dex2jar/

sqlmap http://sqlmap.org/

oxml_xxe https://github.com/BuffaloWill/oxml_xxe/

XXE Injector https://github.com/enjoiz/XXEinjector

The JSON Web Token Toolkit https://github.com/ticarpi/jwt_tool

ground-control https://github.com/jobertabma/ground-control

ssrfDetector https://github.com/JacobReynolds/ssrfDetector

LFISuit https://github.com/D35m0nd142/LFISuite
GitTools https://github.com/internetwache/GitTools
dvcs-ripper https://github.com/kost/dvcs-ripper
tko-subs https://github.com/anshumanbh/tko-subs
HostileSubBruteforcer https://github.com/nahamsec/HostileSubBruteforcer Race the Web https://github.com/insp3ctre/race-the-web
ysoserial https://github.com/GoSecure/ysoserial
PHPGGC https://github.com/ambionics/phpggc
CORStest https://github.com/RUB-NDS/CORStest
retire-js https://github.com/RetireJS/retire.js
getsploit https://github.com/vulnersCom/getsploit
Findsploit https://github.com/1N3/Findsploit
bfac https://github.com/mazen160/bfac
WPScan https://wpscan.org/
CMSMap https://github.com/Dionach/CMSmap
Amass https://github.com/OWASP/Amass

Any Import Tool Missing Add in comments…

This was as much as i can think about sharing with you guys related to Web app Security in tools and vulns i have added a few things about mobile apps but the following sections contains some references you should definitely go through if you gonna join the mobile app security gang as well..

Mobile App Security.

So hello to Mobile App Security section now let me clear this first i'm a complete noob at this section so it won't be as detailed as the web app one.

Now The best and the very first thing i would suggest is to actually learn about Development phase of an app mainly my focus is Android APPs (doesn't necessarily means that you should go for learning to develop an android but at least get to know. For this You can go through the following Android App development tools. (My suggestion is you should actually give basic time to these)

Android SDK ~ The Android software development kit (SDK) includes a comprehensive set of development tools. These include a debugger, libraries, a handset emulator based on QEMU, documentation, sample code, and tutorials

ADT Bundle ~ The Android Developer Tools(ADT) bundle is a single download that contains everything for developers to start creating Android Application

Root Tools ~ RootTools provides rooted developers a standardized set of tools for use in the development of rooted applications.

Now if you have gone through them let's get towards Mobile app security vulnerabilities For this i'll suggest you to first go towards OWASP Mobile Top 10 Giving them a good overview will definitely worth it.

I'll also Highly suggest these two Books specifically for Android & IOS app testing

The Mobile Application Hacker's Handbook
iOS Application Security: The Definitive Guide for Hackers and Developers

For Mobile Applications i'll share Two of the Best places i'm currently following to learn and i would highly recommend you guys to have a look at them and giving them a proper read will definitely help you

Application Security Wiki:

Application Security Wiki is an initiative to provide all Application security related resources to Security Researchers and developers at one place.

https://appsecwiki.com/#/

Learn IOS Security:

IOS Security Guide to learn and test by Prateek

http://damnvulnerableiosapp.com/#learn

owasp-workshop-android-pentest:

Learning Penetration Testing of Android Applications

Mobile Application Penetration Testing Cheat Sheets

The Mobile App Pentest cheat sheet

Mobile penetration testing android command cheatsheet

Summing up the Phase #02 of this blog i think by following these resources at and giving them good time one can get pretty good at Bug Hunting..

Here are some Websites or Places where you can play CTF Challenges and practice your skills that you have learned.

- **Hacker 101** https://ctf.hacker101.com/
- **Hack the box** https://www.hackthebox.eu/
- **OvertheWire wargames** http://overthewire.org/wargames/
- **Pwnable.tw** https://pwnable.tw/
- **Vulnhub** https://www.vulnhub.com/
- **Troy Hunt “*Hack Yourself* First”** https://hack-yourself-first.com/
- **Hack.Me** https://hack.me/
- **Hacksplaining** https://www.hacksplaining.com/lessons
- **Penetration Testing Practice Labs** https://www.amanhardikar.com/mindmaps/Practice.html

Other Resources:

I saw a few friends of mine shared some really interesting and important tools, & resources so i decided to add them here as well because I’m giving some good time to them nowadays.

Tools used for Penetration testing / Red Teaming.

List-pentest-tools: A curated list of network penetration testing tools.

Password lists for use in penetration testing situations, broken up by TLD.

Penetration tests cases, resources and guidelines.

Penetration Testing notes, resources and scripts

A collection of hacking / penetration testing resources to make you better!

RedTeam-Pentest-Cheatsheets

Collection of OSCP study material && tools.

Kali Linux Offensive Security Certified Professional Survival Exam Guide

Penetration Testing / OSCP Biggest Reference Bank / Cheatsheet

An archive of everything related to OSCP

GitBook: OSCP RoadMap

OSCP Cheatsheets, Pentesting / Red Teaming Tools and Techniques

How to prepare for OSCP complete guide

OSCP All Tools are Here ...!!

I hope the Path Guide i'm trying to share here clears doubts for many newcomers in Bug Bounty Hunting. Let's move to Phase #03

Phase #03

- **Phase 03 is All about Selecting a target, getting started to test and after finishing testing writing a good report about the issue you have found**.

Hey so Now the Final Phase i have in my mind is for People who have gone through all the good important stuff and now are testing.. so i'll like to give my advice about a few things and then will sum up this blog.

Selecting and Approaching a Target?

One of the most import things in Bug bounty Hunting is to Select a target that you're going to test. This basically depends on ones mood, experience and skills one can take a look at a target with a huge scope having 4-5 websites will all subdomains inscope and a few mobile apps and test start testing them or just one domain & one app with a good app having a lot of features to test.

One can go to https://bugcrowd.com/programs or https://hackerone.com/directory and look for a program accordingly or either individual programs like Google, Facebook or ebay.

Approaching a target to Hunt is an easy task you just need to be careful with what you're doing it all depends on you.. for me i usually do recon at first by going through domain history, links, IPs, & WayBack Info of the site. **Don't forget to keep notes of everything you do**,

now basically after the basic recon process thats i used tools and stuff for or somethings have to done manual.. I start hunting, i take a particular functionality/workflow in the application and start digging deep into it. I do look for low hanging fruits or surface bugs. There is no point focussing your efforts on those but keeping track of them is really helpful. I Observe this workflow/requests via a proxy tool such as Burp or Zap. Burp is actually the only tool I use for we or android app pentesting I mainly .Create multiple accounts because I want to test the functions being sent from one user to another. If you haven't been provided multiple accounts, ask for it. Till date, I have not been refused a second account whenever I have asked for it. or sometimes create them easily. Just work with the app flow and keep testing look for weird behaviours of the app try changing things in them but remember finding an app working weirdly isn't necessarily means you have found a bug worth reporting but i would suggest you to keep digging and try to actually find a basic security impact of that… then i usually go for major listed security vulnerabilities i use the methods to achieve them nothing much special just all depends on an app you can't find a PHP code injection in a static web lol so that's why i usually give good time on learning the web flow. for this i go got reading API docs and stuff. After spending a few hours on this stuff, if i can't get anything on a particular point of the app i usually stop and move on.
Getting hung up on something is the biggest motivation killer but that doesn't mean i gave up. I do get back to it later if something else comes up. That's why i always make notes and save them for later use.

That's basically all i do lol looks basic and easy but for me it's hell time spent…

Reporting a Vulnerability?

So i'll say after all this effort you have put into learning, practicing, & actually successfully finding an vulnerability, writing a report will be one of the most difficult tasks. Because one mistake can make the team reviewing them annoyed or maybe increase their workflow. for me Writing a simple but effective report with proper headings and giving as much details as possible with POC images or videos can actually make your work fun and the teams work easy. to Write a report i follow these guides.

WRITING SUCCESSFUL BUG SUBMISSIONS – BUG BOUNTY HUNTER METHODOLOGY

Writing a good and detailed vulnerability report

What does a good report look like?

Well i guess this is where i'll end this Blog and i hope these resources i'm sharing here help answer the questions i basically get in my DMs about teaching them. I myself is a student right now and learning is a huge part of my life also, i consider myself a beginner and sharing this is basically a way for me to learn more.. As Mentioned before this Guide is basically for people who are absolutely new or are still looking for a proper way about what to learn first and from where.

Ending Note!

Being a security researcher, it is really tough to keep yourself up to date. I'd ask the beginners to focus on self study and learn things by themselves as everything is possible all you need is the passion of taking a step after that you can achieve anything. Nothing is impossible to achieve. All i achieved was by doing self-study and self motivation and without any certifications and i'm still learning and trying my best to share what i can so others can also learn something.

> "
>
> ***You are never a perfect person, but you are still better than the rest of the people.***

For a security researcher, all it takes is the passion to achieve something. I hope this article helped you motivate to take a positive step in life..   Well Thanks for reading that's All I can Share With you Guys For Now I'll Make sure to Keep this Article Updated for More People to read.

./THANKS

Share this:

Like this:

Loading...

Posted in: Tips | Tagged: AsliCyberSecurity, BUG BOUNTY HUNTING, Bug Hunting, BugBounties, Bugbountyhunting, Bugcrowd, Cyber Security, Guide to BugBounty, HackerOne, InfoSec

← WHO AM I? And My Experiments with Hacking?

14 Comments

malav/Wolfdroid
June 3, 2019 at 8:26 am

Great blog …. Try a tool by yourself and if you find it cool and useful , you can add it to your list . The name of the tool is GOOHAK

Here is the link
https://github.com/1N3/Goohak

Reply

Sadiq West
June 3, 2019 at 8:31 pm

I recommend this blog to both pro’s and newbies. Thanks bro awesome article

Reply

axyz
June 4, 2019 at 5:45 am

kadak bhai 😁 i mean amazing but the drive link is not opening will you allow me??

Reply

thenewbhaxor
June 4, 2019 at 10:24 am

Thanks a lot for this brief writing and it is a gold mine for me as I want to start my journey in bugbounty!

Reply

negro1337
June 4, 2019 at 4:52 pm

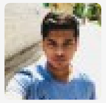
Just awsome negro

Reply

Ed Carlos
June 6, 2019 at 4:17 pm

Just one thing.
Your linux commands list contains this:
“rm -rf / – make computer faster”
And that really shouldn’t be there

Reply



babayaga47
June 6, 2019 at 4:18 pm

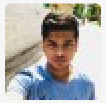
😂 i hope if someone is trying to learn this he/She knows what that is

Reply

Ed Carlos
June 6, 2019 at 4:38 pm

i really hope so.
But this is the internet, you never know hahaha

Reply



babayaga47
June 6, 2019 at 4:55 pm

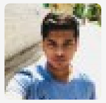
Hahaha 😂

Reply

Anonymois
June 13, 2019 at 6:14 am

Many thanks u just saved me hours of researching
Great job amd good luck in your journey

Reply



babayaga47

June 13, 2019 at 6:15 am

Thanks 🧡

Reply

Ejaz Hussain

June 15, 2019 at 3:42 pm

i think you should review the yt channel links section because they are same as the last your whoami post which contained some gaming and terminated channel which is not helpful. thanks

Reply

babayaga47

June 15, 2019 at 3:45 pm

Thanka for that I actually mentioned that some of them are moved from previous post and also have a good new list will update it

Reply

Aurangzaib Pario
June 18, 2019 at 11:00 pm

wow …. what a post man … !! LONG LIVE … 😍😍 … publish your own PDF and you can get bucks from it man … Go on 😊

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

Subscribe to Blog via Email

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Join 44 other subscribers

Email Address

Subscribe

Social

Security Breached

Blog Stats

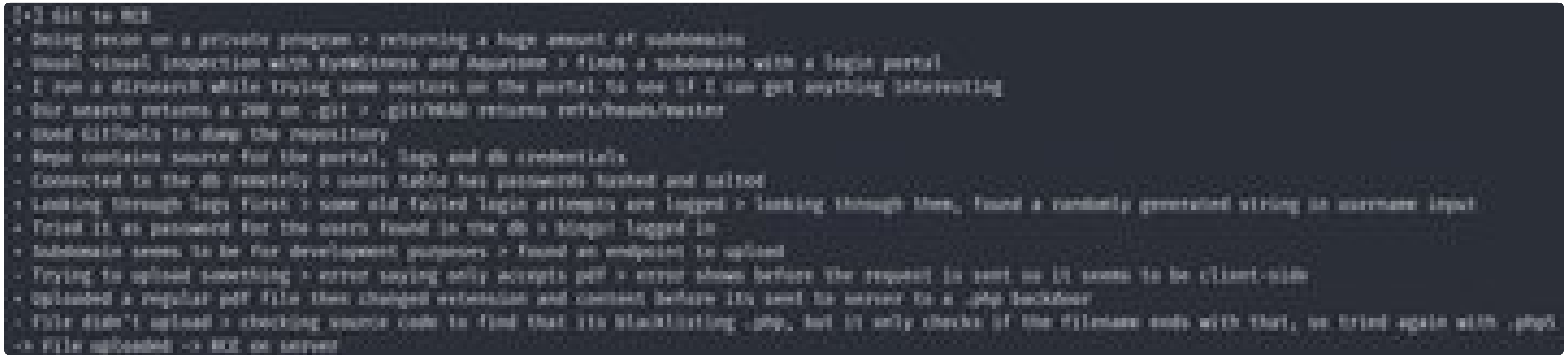
30,421 hits

Follow me on Twitter

M. Khizer Javed Retweeted

Kei0x
@Kei0x

As promised, posting the next lazy write-up, this is how I went from Git to RCE.
Bounty: $3500#bug #bughunter #bugbounty #bounty
If you enjoy these and want to see more, I will be posting others soon again.



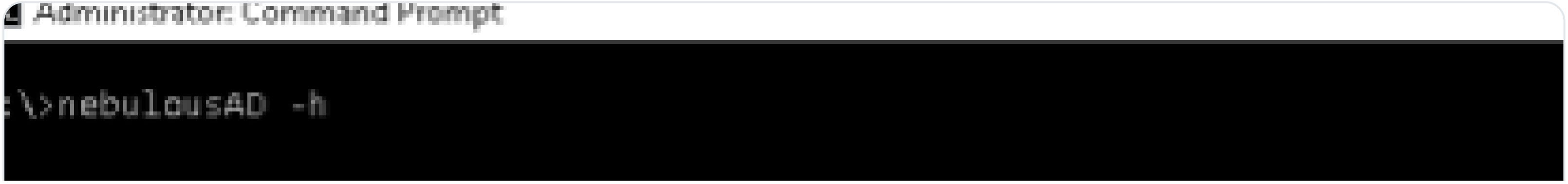
```
[+] Git to RCE
- Doing recon on a private program > returning a huge amount of subdomains
- Usual visual inspection with EyeWitness and Aquatone > finds a subdomain with a login portal
- I run a dirsearch while trying some vectors on the portal to see if I can get anything interesting
- Dir search returns a 200 on .git > .git/HEAD returns refs/heads/master
- Used GitTools to dump the repository
- Repo contains source for the portal, logs and db credentials
- Connected to the db remotely > users table has passwords hashed and salted
- Looking through logs first > some old failed login attempts are logged > looking through them, found a randomly generated string in username input
- Tried it as password for the users found in the db > bingo! logged in
- Subdomain seems to be for development purposes > found an endpoint to upload
- Trying to upload something > error saying only accepts pdf > error shows before the request is sent so it seems to be client-side
- Uploaded a regular pdf file then changed extension and content before its sent to server to a .php backdoor
- File didn't upload > checking source code to find that its blacklisting .php, but it only checks if the filename ends with that, so tried again with .php5
-> File uploaded -> RCE on server
```

Sep 14, 2019

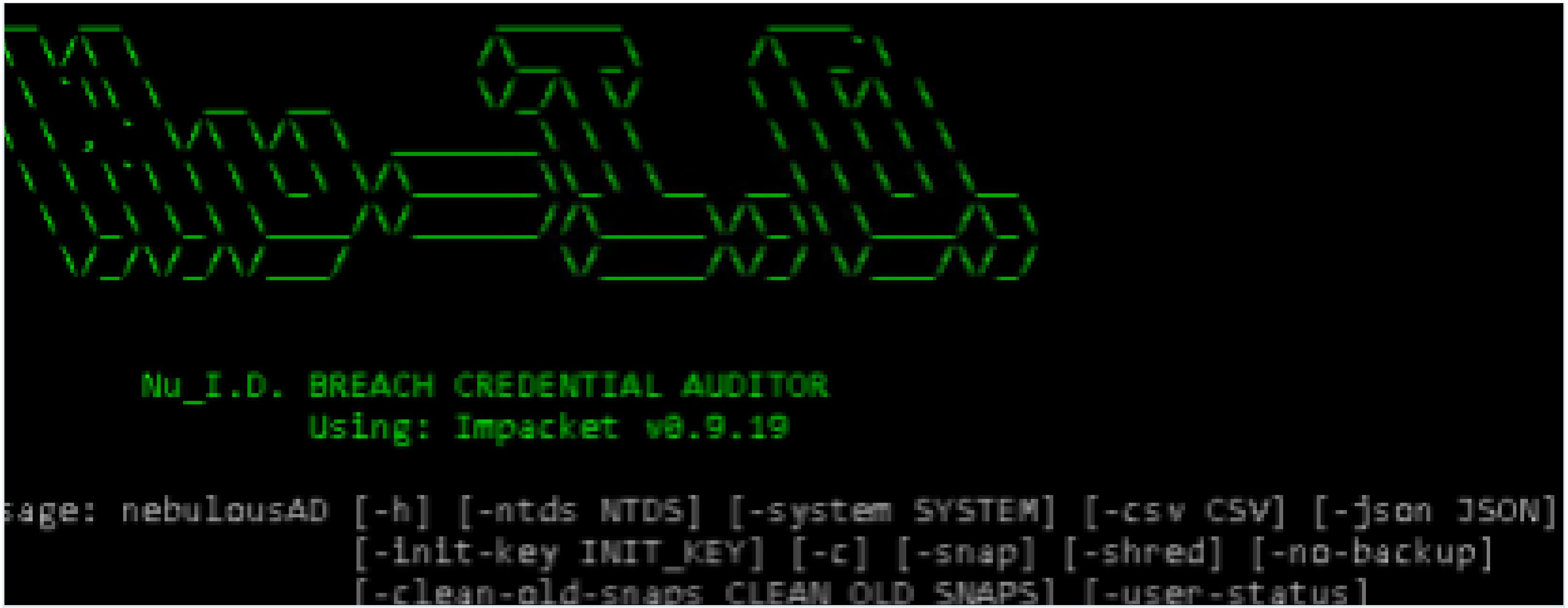
M. Khizer Javed Retweeted

NuID
@_NuID

Check passwords in Active Directory against 2.5 billion breached passwords—for free—now with more privacy! NebulousAD v1.1 has been released 🔒 buff.ly/2UO72Kd



```
:\>nebulousAD -h
```



```
      Nu_I.D. BREACH CREDENTIAL AUDITOR
              Using: Impacket v0.9.19

sage: nebulousAD [-h] [-ntds NTDS] [-system SYSTEM] [-csv CSV] [-json JSON]
                 [-init-key INIT_KEY] [-c] [-snap] [-shred] [-no-backup]
                 [-clean-old-snaps CLEAN_OLD_SNAPS] [-user-status]
```

NebulousAD v1.1 with k-Anonymity

NebulousAD is a free tool to audit passwords in Active Directory against 2.5 billion breached passwords.

blog.nuid.io

Sep 11, 2019

M. Khizer Javed Retweeted

Hossam Sec
@HossamSec

instead of buying udemy course for 20$~200$ and just have very basic course with a great titles and low content i suggest for you to buy a subscription in @PentesterLab which you will learn from a good level to a very advanced level with a video , course and lab of all new 1/n

Sep 14, 2019

M. Khizer Javed Retweeted

caseyjohnellis
@caseyjohnellis

“Everybody who’s a bug hunter is an entrepreneur.” — Casey Ellis, CEO and founder, Bugcrowd. the-parallax.com/2019/09/12/bug… <<< this is one of my *very* favorite sub-stories of the growth of #bugbounty, vdp, and crowdsourcing

How bug bounties are fueling hacker entrepreneurs - The Parallax

As the bug bounty business matures, the bounties themselves present opportunities for hacker entrepreneurs to pocket profits while developing