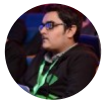
How To Do Your Reconnaissance Properly Before Chasing A Bug Bounty



Hussnain Fareed Follow

Nov 25, 2017 · 17 min read

Today I am writing about the love story between bug bounties & reconnaissance, but before I do I should say that i'm not much of an expert and this article reflects me sharing my personal opinion.

This blog post will be focusing on recon & where to look for bugs In a Bug Bounty Program, this is not a guide on how to find bugs in a tech sense, but rather a case of tactics you can use to find bugs.

I am assuming you already know about penetration testing, therefore I will not be explaining how to test for vulnerabilities, but rather **where** to test for them & the tools you can use. This is mainly just a general overview of how someone would map out a target site and efficiently perform

reconnaissance to gain as much info on the site as possible before beginning their audit.

Recon is an essential element of any penetration testing.

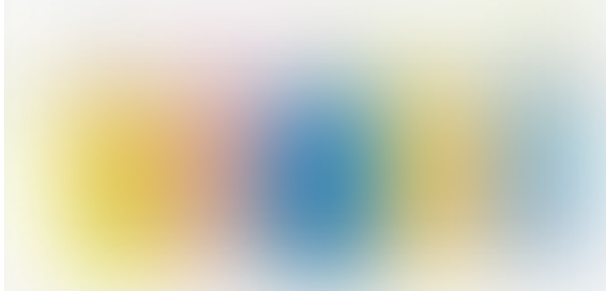
Competition?

Bug Bounty programs are not very simple, the thing you need to remember about bug bounty programs is that there is a lot of competition. When you're taking part in a bug bounty program, you're competing against both

the security of the site, and also against the thousands of other people who are taking part in the program. For this reason, it's important to think critically.

This is why passive and active reconnaissance is especially important for bounty programs, as you need to look a lot deeper than you would in a regular penetration test.

Importance of Reconnaissance in Pentesting?



Extracting relevant information can play a game changing role in many situations. Extracting this information is pretty simple and somewhat easy. Sometimes recon can go beyond collecting basic information to understand the system and can also identify information which might straight away

lead to exploitation, sometimes without actually touching the entity being tested.

Even after having such significance this phase is not given enough importance and most of the tests focus straight away on exploitation. The key point here is that exploitation is certainly important but performing a thorough recon could prove very helpful in it and also make it easier, faster and stealthier.

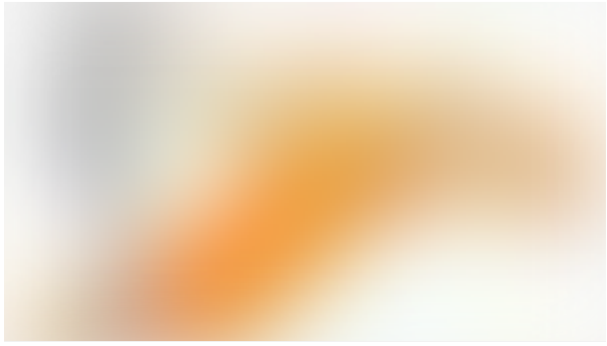
Determining the Target?

Ideally you're going to be wanting to choose a program that has a wide scope. You're also going to be wanting to look for a bounty program that has

a wider range of vulnerabilities within scope. The wider attack surface for the bounty program, and the wider range of vulnerabilities considered valid, then the higher the chance would be of getting a valid payout.

After choosing which bounty program you're going to attempt, the next basic step that would be to map out your attack surface to know more about it.

Time to Map out the target!



Rule No#1 (That I mostly forgot to follow 😛 and Ended Up messing the day completely) That is properly reading the terms for the bounty and

clearly understand which domains are in scope and which forms of vulnerabilities are considered valid reports.

Sometimes I forgot to do That and Shit happens Submitting things that aren't within scope of the bounty program, tells the people running the program that you haven't properly read the terms, and it will lead to them not taking your future reports seriously. I mean Seriously

So Now Before doing any Attack or testing you really need to actively/passively person reconnaissance on your target to effectively map out most of the things you can do to get to know more about your target !

> **"Keep your friends close and your enemies closer?"**

So following this phrase i always keep the target closer to my heart and map it out as much as i can ☺ it always give me an idea of how everything is structured & how everything works on the target.

I start every program by mining information about the domains, email servers and social network connections. The larger the scope, the higher the

chance of finding a bug. let's assume all subdomains are within scope, then one of the first steps would be to enumerate valid subdomains.

I use different tools for that.

The List:

- https://pentest-tools.com/
- https://virustotal.com/
- https://www.shodan.io/
- https://crt.sh/?q=%25taregt.com
- https://dnsdumpster.com/
- https://censys.io
- http://dnsgoodies.com

These are the webs that I Use Everyday ☺

- https://bitbucket.org/LaNMaSteR53/recon-ng

- https://github.com/michenriksen/aquatone
- https://github.com/aboul3la/Sublist3r
- https://github.com/rbsec/dnscan
- https://github.com/Cleveridge/cleveridge-subdomain-scanner

So now after getting all of the subdomains we should go towards 2nd Step that is in my opinion is port scanning. We have two methods to that the old fashioned way (but OLD IS GOLD lol) that is Running a scan through nmap for limited ports, selected one or maybe 1–50000 God knows what u gonna do 😛

Masscan can also help https://github.com/robertdavidgraham/masscan

The second method that i used many times is using aquatone to scan the subdomains and then use it for scanning the ports you have options to Scan ports like common/large/huge.

It would be best to use aquatone, but ideally you want to be scanning each individual IP address associated with their subdomains and having the

output saved to a file, after this look for any services running on unusual ports or any service running on default ports which could be vulnerable (FTP, SSH, etc). You're also going to want to look for the version info on services running in order to determine whether anything is outdated and potentially vulnerable. it takes Time but it also gives results ☺

Also Just don't get limited to Subdomains Try extracting vhosts ☺ tools like

- https://pentest-tools.com/information-gathering/find-virtual-hosts
- https://github.com/jobertabma/virtual-host-discovery

Planing to Move faster try https://github.com/ChrisTruncer/EyeWitness ☺

or maybe

httpscreenshot https://github.com/breenmachine/httpscreenshot/

You should make notes during the recon to avoid confusion. Take them in whatever manner you want, but since participation in bug bounty programs involves mainly black box testing, it is really important to get a feel of how

the site is structured and to map it all out in order to be able to efficiently find bugs.

Well that's just the basic you might want to look at the headers to see which security options are in place, for example looking for presence of X-XSS-Protection: or X-Frame-Options: deny. Knowing what security measures are in place means you know your limitations. also look out for WAFs and i suggest you can use WafW00f for that

- https://github.com/sandrogauci/wafw00f (WAFW00F identifies and fingerprints Web Application Firewall (WAF) products.)

Also u should also be looking for any information disclosure and laso sometimes for Dir listing or maybe dir scanning can help for other stuff you can use Dirbuster

- https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Burp Suite, spider is going to be your best friend. Just make sure that your scope is set correctly so that you're not wasting time spidering unneeded domains. Also, intruder is completely necessary for directory brute-forcing. Download the https://github.com/danielmiessler/SecLists repository, which has plenty of lists to discover content across multiple platforms. If you have Burp Suite Pro, I highly recommend utilizing the Reflector extension. This will show you any parameters that are reflected into the responses as Burp is spidering.

use robots.txt to determine the directories which may contain useful info, look for the disallow rules.

Also spider the host for API endpoints 😉 and Make notes lol

wappalyzer can be good to use for Checking CMS ☺

extracting S3 buckets during recon is Really nice idea, look for them manually or use Tools Like.

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

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

Well Basically when i'm done with this stuff, I make Notes with name of subdomain/IP or domain.

Mostly My stepwise notes typically contains:

- Whois Information
- Subdomains
- Dir info
- S3 Buckets
- social accounts
- API Endpoints
- emails
- Vhosts
- Backend IP address
- Open Ports / Services running

- Service version info (if applicable)
- server banners
- directory listings
- presence security headers
- WAF (+ WAF type)

Well After this I start Making and capturing requests and responses of all types, accepted user inputs (GET/POST/COOKIES), and Other Points.

Also Don't forget your best friend Google :p Use google Dorks U can make your own or use make by others ☺

Try it out

- https://pentest-tools.com/information-gathering/google-hacking
- https://github.com/1N3/Goohak/
- https://github.com/ZephrFish/GoogD0rker/

wanna construct your own? Have a Look at https://support.google.com/websearch/answer/2466433?hl=en

Make sure to spend as much time as possible performing recon, until you have a pretty good feel of how the site operates,

There are even occasions where passive recon can lead to some important information Disclosure. i.e. searching github or pastebin for the company name and stumbling across some random source that ended up online after some sloppy dev wrote it.

For that I would prefer

- https://github.com/1N3/Sn1per (for web)
- https://github.com/michenriksen/gitrob (for github)
- https://github.com/dxa4481/truffleHog
- https://github.com/IOActive/RepoSsessed
- https://github.com/anshumanbh/git-all-secrets

I got some good reports payouts using these ☺

Don’t forget to look deep into Js files well manually you will love it But time saving is the goal so try using tools like

- https://github.com/jobertabma/relative-url-extractor

also One of the best thing is To look for older content that can give u ideas of site structure or maybe vuln endpoints ☺ For that use

- https://web.archive.org/
- https://gist.github.com/mhmdiaa/2742c5e147d49a804b408bfed3d32d07
- https://gist.github.com/mhmdiaa/adf6bff70142e5091792841d4b372050

maybe reversewhois lookup will help to discover more potential targetes but make sure that they are in scope

- http://viewdns.info/reversewhois/?q=

Alright, so then there's this thing called **PunkSpider**. (https://www.punkspider.org) "It is a **global web application vulnerability search engine**. Don't get too excited though.

PunkSpider is pretty cool to play around with, but it's not much in-depth. You also can't use wildcards in your searches, making it a pain to search for multiple sub-domains. But there's no harm in taking a few minutes to look around. Who knows, maybe you'll get lucky?

Well That's almost everything I do During recon & before starting actual Bug Bounty hunting! So Hope i didn't missed anything for the basic recon i perform… But to help a Bit more Look into these Bug Bounty reference. Sometimes u got lucky enough to Find the same bug that has been reported before in different Bug Bounty Program.

Bug Bounty Reference

A list of bug bounty write-up that is categorized by the bug nature, Written by ***ngalongc*** this is inspired by https://github.com/djadmin/awesome-bug-

bounty

My intention is to make a full and complete list of common vulnerability that are publicly disclosed bug bounty write-up, and let Bug Bounty Hunter to use this page as a reference when they want to gain some insight for a particular kind of vulnerability during Bug Hunting, feel free to submit pull request. Okay, enough for chit-chatting, let's get started.

- XSSI
- Cross-Site Scripting (XSS)
- Brute Force
- SQL Injection (SQLi)
- External XML Entity Attack (XXE)
- Remote Code Execution (RCE)
- Deserialization
- Image Tragick
- Cross-Site Request Forgery (CSRF)

- Insecure Direct Object Reference (IDOR)
- Stealing Access Token
- Google Oauth Login Bypass
- Server Side Request Forgery (SSRF)
- Unrestricted File Upload
- Race Condition
- Business Logic Flaw
- Authentication Bypass
- HTTP Header Injection
- Email Related
- Money Stealing
- Miscellaneous

Cross-Site Scripting (XSS)

- 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
- 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
- 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

Brute Force

- Web Authentication Endpoint Credentials Brute-Force Vulnerability by Arne Swinnen
- InstaBrute: Two Ways to Brute-force Instagram Account Credentials by Arne Swinnen
- How I Could Compromise 4% (Locked) Instagram Accounts by Arne Swinnen
- Possibility to brute force invite codes in riders.uber.com by r0t
- Brute-Forcing invite codes in partners.uber.com by Efkan Gökbaş (mefkan)
- How I could have hacked all Facebook accounts by Anand Prakash

- Facebook Account Take Over by using SMS verification code, not accessible by now, may get update from author later by Arun Sureshkumar

SQL Injection

- SQL injection in WordPress Plugin Huge IT Video Gallery in Uber by glc
- SQL Injection on sctrack.email.uber.com.cn by Orange Tsai
- 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

Stealing Access Token

- Facebook Access Token Stolen by Jack Whitton –
- Obtaining Login Tokens for an Outlook, Office or Azure Account by Jack Whitton

- Bypassing Digits web authentication's host validation with HPP by filedescriptor
- Bypass of redirect_uri validation with /../ in GitHub by Egor Homakov
- Bypassing callback_url validation on Digits by filedescriptor
- Stealing livechat token and using it to chat as the user — user information disclosure by Mahmoud G. (zombiehelp54)
- Change any Uber user's password through /rt/users/passwordless-signup — Account Takeover (critical) by mongo (mongo)
- Internet Explorer has a URL problem, on GitHub by filedescriptor.
- How I made LastPass give me all your passwords by labsdetectify
- Steal Google Oauth in Microsoft
- Steal FB Access Token
- Paypal Access Token Leaked
- Steal FB Access Token
- Appengine Cool Bug
- Slack post message real life experience

- Bypass redirect_uri by nbsriharsha
- Stealing Facebook Messenger nonce worth 15k

Google oauth bypass

- Bypassing Google Authentication on Periscope's Administration Panel By Jack Whitton

CSRF

- Messenger.com CSRF that show you the steps when you check for CSRF by Jack Whitton
- Paypal bug bounty: Updating the Paypal.me profile picture without consent (CSRF attack) by Florian Courtial
- 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

Remote Code Execution

- 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 (Sorry its in Chinese Only)
- 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

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

Image Tragick

- 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)

- 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
- 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

XXE

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

Unrestricted File Upload

- 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)

Server Side Request Forgery (SSRF)

- 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

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

Subdomain Takeover

- 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

Author Write Up

- 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

XSSI

- Plain Text Reading by XSSI
- JSON hijacking
- OWASP XSSI
- Japan Identifier based XSSI attacks
- JSON Hijack Slide

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

2017 Local File Inclusion

- 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!

Miscellaneous

- 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

10 rules of Bug Bounty

Following “**10 rules of Bug Bounty**”

1. Targeting the Bug Bounty Program
2. How do you Approach the Target?
3. Don’t Expect Anything!
4. Less Knowledge about Vulnerabilities and Testing Methodologies
5. Surround yourself with Bug Bounty Community to keep yourself Updated

6. AUTOMATION
7. GET BOUNTY or GET EXPERIENCE
8. FIND THE “BUG” or FIND A “BUG’S CHAIN”
9. FOLLOW MASTER’S PATH
10. RELAX & ENJOY LIFE

Well that’s all Folks Hopefully my way of doing basic recon can help you to properly Select the target-Map it out properly-Hunt it down using the information you have gathered and At the end Writing a Report suggestion is to read the blog https://blog.bugcrowd.com/advice-for-writing-a-great-vulnerability-report/

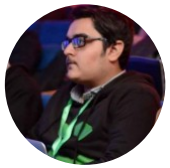
There is a whole list of resources I have created for your help ☺ (***https://github.com/husnainfareed/Resources-for-learning-ethical-hacking/***)

#NOTE all references taken from the Internet and shared on internet xD
Thanks to those who shared their opinion before that helped me learn ☺

If you enjoyed this story, please click the 👏 button and share to help others find it. Feel free to leave a comment.

Security | Ethical Hacking | Pentesting | How To

2.7K claps



WRITTEN BY

Hussnain Fareed

Follow

Interested in Computers, Hacking, Machine Learning and Web Development 👨‍💻

InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Maintained by Hackrew

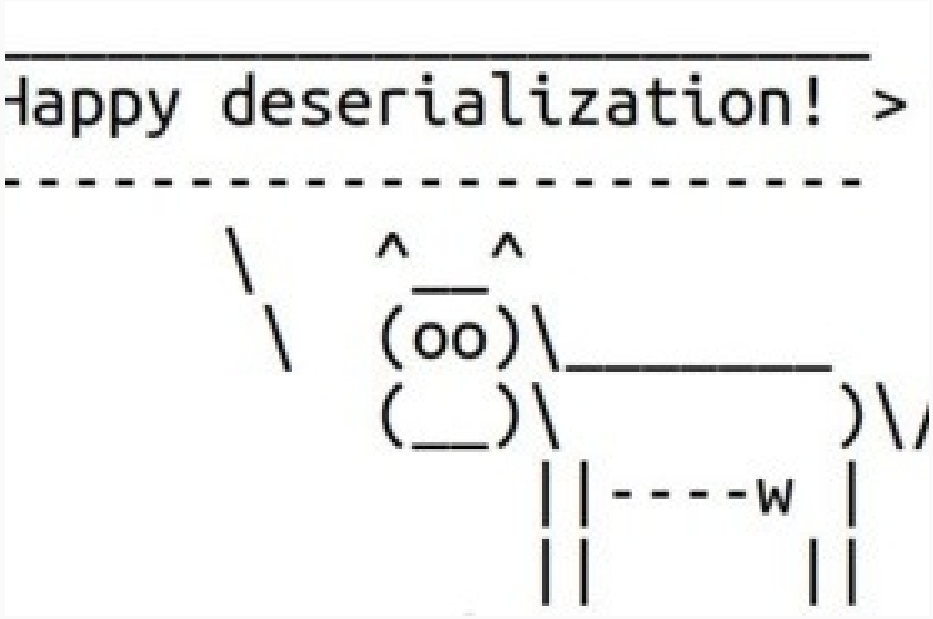
See responses (10)

More From Medium

More from InfoSec Write-ups

Safer deserialization in Spring Security OAuth2

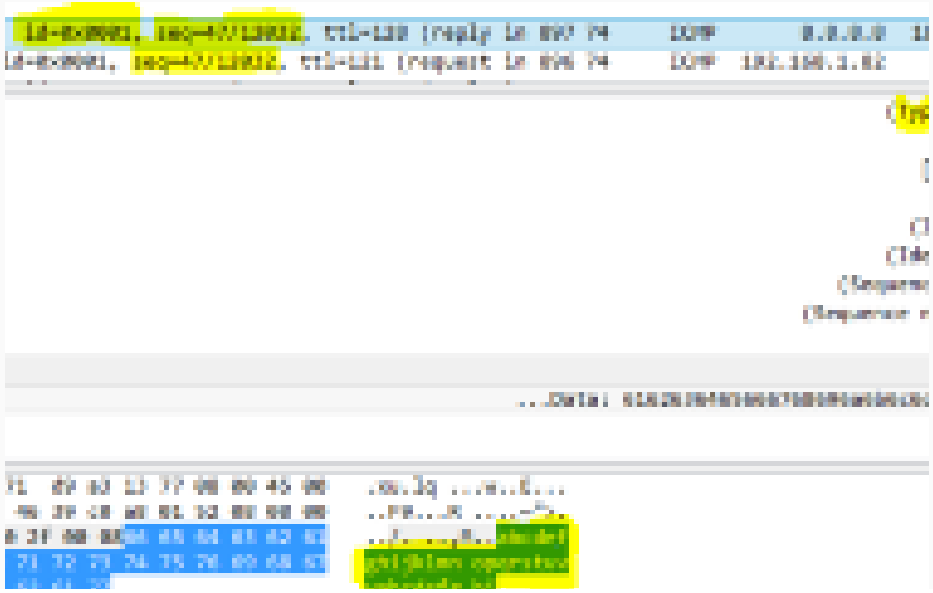
Artem Smotrakov in InfoSec Write-ups
Nov 16 · 5 min read ★



More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako in InfoSec Write-ups
Dec 17, 2018 · 8 min read



More from InfoSec Write-ups

Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups

Jun 11 · 6 min read ★

848