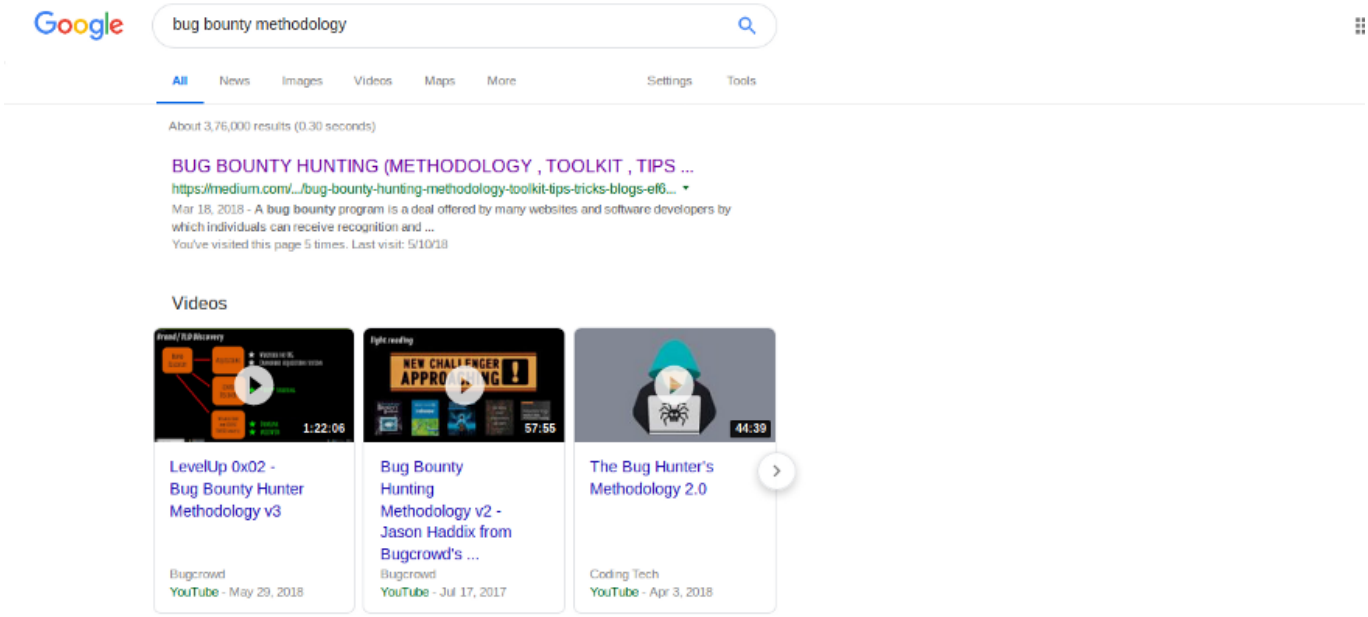
Web Application Security & Bug Bounty (Methodology, Reconnaissance, Vulnerabilities, Reporting)

Sanyam Chawla Follow
Jan 26, 2019 · 18 min read

> *Hello Folks , Hope everyone is doing good. This blog is basically for Web Security Methodology (WSM).*
>
> *Have you read my last post regarding "Bug Bounty Methodology" ? If you missed it go to this BBM link https://medium.com/@infosecsanyam/bug-bounty-hunting-methodology-toolkit-tips-tricks-blogs-ef6542301c65*

Image from Google



Bug bounty methodology (BBM) :)

Now this time i will share methodology for Web Application Security Assessment from beginning to end (Recon to Reporting/ R&R) . Try to cover most of the vulnerabilities links for web application security.

Methodology of Application Vulnerability Assessment & Pen-testing

> ***Defining a Scope***
>
> ***Reconnaissance***
>
> ***Manual Assessment (Web Security Vulnerabilities)***
>
> ***Reports***

Defining a Scope :

Each bug bounty or Web Security Project has a “scope”, or in other words, a section of a Scope of Project ,websites of bounty program’s details that will describe what type of security vulnerabilities a program is interested in receiving, where a researcher is allowed to test and what type of testing is permitted. On Bug-crowd, a bounty’s scope

can be found in the “Program Details” bounty brief section of a program page. In your web application project has give the scope which websites , subdomains, api’s links for assessment.

Reconnaissance:

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.

For Finding Web Security Vulnerabilities are not very simple . 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 Scope, as you need to look a lot deeper than you would in a regular penetration test.

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

Start a Reconnaissance

Subdomain Finding :

1. https://pentest-tools.com/

2. https://virustotal.com/

3. https://www.shodan.io/

4. https://crt.sh/?q=%25taregt.com

5. https://dnsdumpster.com/

6. https://censys.io

7. http://dnsgoodies.com

Github Open Source tools for Subdomain Finding :-

1. https://bitbucket.org/LaNMaSteR53/recon-ng
2. https://github.com/michenriksen/aquatone
3. https://github.com/aboul3la/Sublist3r
4. https://github.com/rbsec/dnscan
5. https://github.com/Cleveridge/cleveridge-subdomain-scanner

After getting all sub-domains we found two methods to scan an ip's, ports and Services:

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

2. Aquatone : https://github.com/michenriksen/aquatone

3. Nmap

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

1. https://pentest-tools.com/information-gathering/find-virtual-hosts
2. https://github.com/jobertabma/virtual-host-discovery
3. https://github.com/ChrisTruncer/EyeWitness 🙂
4. httpscreenshot https://github.com/breenmachine/httpscreenshot/
5. WAF (+ WAF type) — https://github.com/EnableSecurity/wafw00f
6. https://github.com/danielmiessler/SecLists
7. https://github.com/yasinS/sandcastle
8. https://digi.ninja/projects/bucket_finder.php

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

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

Google Dorks :

site:target.com -www
site:target.com intitle:"test" -support

site:target.com ext:php | ext:html
site:subdomain.target.com
site:target.com inurl:auth
site:target.com inurl:dev

Information Gathering Part

1. Whois Information

2. Subdomains

3. Dir info

4. S3 Buckets

5. social accounts

6. API Endpoints

7. emails

8. Vhosts

9. Backend IP address

10. Open Ports / Services running

11. Service version info (if applicable)

12. server banners

13. directory listings

14. presence security headers

> 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 developer wrote it.*

For that I would prefer

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

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

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

To look for older content that can give u ideas of site structure or maybe vulnerable endpoints 😉 For that use

1. https://web.archive.org/
2. https://gist.github.com/mhmdiaa/2742c5e147d49a804b408bfed3d32d07

> Maybe reverse whois lookup will help to discover more potential targets but make sure that they are in scope

1. 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.

> Web Application Vulnerabilities & Bug Bounty Reference

A list of bug bounty / web app security write-up that is categorized by the bug nature,

1 Sql Injection :

SQL injection is a kind of injection vulnerability in which the attacker tries to inject arbitrary pieces of malicious data(Code) into the input fields of an application, which, when processed by the application, causes that data to be executed as a piece of code by the back end SQL server, thereby giving undesired results which the developer of the application did not anticipate.

List of Database

- MySQL(Open source),
- MSSQL,
- MS-ACCESS,
- Oracle,

- Postgre SQL(open source),
- SQLite,

Type of SQL Injection

- In Band
- Out of Band
- Blind SQLI

SQLI Exploitation Technique

- Error Based Exploitation
- Union Based Exploitation
- Boolean Based Exploitation
- Time Based Delay Exploitation
- Out of Band Exploitation

Try to Identify- where the application interact with DB

- Authentication Page
- Search Fields
- Post Fields
- Get Fields
- HTTP Header
- Cookie

Based on the response received from the server

Error-based SQL injections

1. Union Query Type
2. Double Query Injection

Blind SQL Injections

1. Boolean-based blind injections.
2. Time based blind injections

Sql Injection Practice Lab

1. http://leettime.net/sqlninja.com/
2. http://hack.me/
3. http://www.sqlinjection.net/
4. https://sqlzoo.net/
5. https://github.com/Audi-1/sqli-labs

Tutorials

1. https://www.exploit-db.com/
2. https://www.hackingarticles.in/
3. http://securityidiots.com/
4. http://breakthesecurity.cysecurity.org/
5. http://lastc0de.blogspot.com/2013/07/tutorial-sql-injection-manual.html

SQL Injection Bug Bounty Writeups Written by ngalongc & @arushsinghania this is inspired by https://github.com/djadmin/awesome-bug-bounty:-

1. SQL injection in WordPress Plugin Huge IT Video Gallery in Uber by glc
2. SQL Injection on sctrack.email.uber.com.cn by Orange Tsai
3. Yahoo — Root Access SQL Injection — tw.yahoo.com by Brett Buerhaus
4. Multiple vulnerabilities in a WordPress plugin at drive.uber.com by Abood Nour (syndr0me)
5. GitHub Enterprise SQL Injection by Orange

Cross Site Scripting Tutorial & Pratical

1. https://excess-xss.com/
2. https://hackertarget.com/xss-tutorial/
3. https://xss-game.appspot.com/
4. http://leettime.net/xsslab1/chalg1.php
5. https://hack.me/t/XSS
6. https://xss-quiz.int21h.jp/
7. https://steve.fi/Security/XSS/Tutorial/
8. https://www.hacking-tutorial.com/hacking-tutorial/xss-attack-hacking-using-beef-xss-framework/#sthash.pIAyu7PF.dpbs

Cross-Site Scripting (XSS) Bug Bounty

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

21. Microsoft XSS and Twitter XSS
22. Google Japan Book XSS
23. Flash XSS mega nz — by frans
24. Flash XSS in multiple libraries — by Olivier Beg
25. xss in google IE, Host Header Reflection
26. Years ago Google xss
27. xss in google by IE weird behavior
28. xss in Yahoo Fantasy Sport
29. xss in Yahoo Mail Again, worth $10000 by Klikki Oy
30. Sleeping XSS in Google by securityguard
31. Decoding a .htpasswd to earn a payload of money by securityguard
32. Google Account Takeover
33. AirBnb Bug Bounty: Turning Self-XSS into Good-XSS #2 by geekboy
34. Uber Self XSS to Global XSS
35. How I found a $5,000 Google Maps XSS (by fiddling with Protobuf) by Marin MoulinierFollow
36. Airbnb — When Bypassing JSON Encoding, XSS Filter, WAF, CSP, and Auditor turns into Eight Vulnerabilities by Brett
37. XSSI, Client Side Brute Force
38. postMessage XSS Bypass
39. XSS in Uber via Cookie by zhchbin
40. Stealing contact form data on www.hackerone.com using Marketo Forms XSS with postMessage frame-jumping and jQuery-JSONP by frans

41. XSS due to improper regex in third party js Uber 7k XSS
42. XSS in TinyMCE 2.4.0 by Jelmer de Hen
43. Pass uncoded URL in IE11 to cause XSS
44. Twitter XSS by stopping redirection and javascript scheme by Sergey Bobrov

Brute Force

1. Web Authentication Endpoint Credentials Brute-Force Vulnerability by Arne Swinnen
2. InstaBrute: Two Ways to Brute-force Instagram Account Credentials by Arne Swinnen
3. How I Could Compromise 4% (Locked) Instagram Accounts by Arne Swinnen
4. Possibility to brute force invite codes in riders.uber.com by r0t
5. Brute-Forcing invite codes in partners.uber.com by Efkan Gökbaş (mefkan)
6. How I could have hacked all Facebook accounts by Anand Prakash
7. Facebook Account Take Over by using SMS verification code, not accessible by now, may get update from author later by Arun Sureshkumar

Stealing Access Token

1. Facebook Access Token Stolen by Jack Whitton –
2. Obtaining Login Tokens for an Outlook, Office or Azure Account by Jack Whitton
3. Bypassing Digits web authentication's host validation with HPP by filedescriptor
4. Bypass of redirect_uri validation with /../ in GitHub by Egor Homakov
5. Bypassing callback_url validation on Digits by filedescriptor

6. Stealing livechat token and using it to chat as the user — user information disclosure by Mahmoud G. (zombiehelp54)
7. Change any Uber user's password through /rt/users/passwordless-signup — Account Takeover (critical) by mongo (mongo)
8. Internet Explorer has a URL problem, on GitHub by filedescriptor.
9. How I made LastPass give me all your passwords by labsdetectify
10. Steal Google Oauth in Microsoft
11. Steal FB Access Token
12. Paypal Access Token Leaked
13. Steal FB Access Token
14. Appengine Cool Bug
15. Slack post message real life experience
16. Bypass redirect_uri by nbsriharsha
17. Stealing Facebook Messenger nonce worth 15k

Google oauth bypass

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

CSRF

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

3. Hacking PayPal Accounts with one click (Patched) by Yasser Ali
4. Add tweet to collection CSRF by vijay kumar
5. Facebookmarketingdevelopers.com: Proxies, CSRF Quandry and API Funby phwd
6. How i Hacked your Beats account ? Apple Bug Bounty by @aaditya_purani

Remote Code Execution

1. JDWP Remote Code Execution in PayPal by Milan A Solanki
2. 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
3. How I Hacked Facebook, and Found Someone's Backdoor Script by Orange Tsai
4. How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE! by Orange Tsai
5. uber.com may RCE by Flask Jinja2 Template Injection by Orange Tsai
6. Yahoo Bug Bounty — *.login.yahoo.com Remote Code Execution by Orange Tsai (Sorry its in Chinese Only)
7. How we broke PHP, hacked Pornhub and earned $20,000 by Ruslan Habalov
8. *Alert*, God-like Write-up, make sure you know what is ROP before clicking, which I don't =(
9. RCE deal to tricky file upload by secgeek
10. WordPress SOME bug in plupload.flash.swf leading to RCE in Automaticby Cure53 (cure53)
11. Read-Only user can execute arbitraty shell commands on AirOS by 93c08539 (93c08539)
12. Remote Code Execution by impage upload! by Raz0r (ru_raz0r)

13. Popping a shell on the Oculus developer portal by Bitquark
14. Crazy! PornHub RCE AGAIN!!! How I hacked Pornhub for fun and profit — 10,000$ by 5haked
15. PayPal Node.js code injection (RCE) by Michael Stepankin
16. eBay PHP Parameter Injection lead to RCE
17. Yahoo Acqusition RCE
18. Command Injection Vulnerability in Hostinger by @alberto__segura
19. RCE in Airbnb by Ruby Injection by buerRCE
20. RCE in Imgur by Command Line
21. RCE in git.imgur.com by abusing out dated software by Orange Tsai
22. RCE in Disclosure
23. Remote Code Execution by struct2 Yahoo Server
24. Command Injection in Yahoo Acquisition
25. Paypal RCE
26. $50k RCE in JetBrains IDE
27. $20k RCE in Jenkin Instance by @nahamsec

Deserialization

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

Image Tragick

1. Exploiting ImageMagick to get RCE on Polyvore (Yahoo Acquisition) by NaHamSec
2. Exploting ImageMagick to get RCE on HackerOne by c666a323be94d57
3. Trello bug bounty: Access server's files using ImageTragick by Florian Courtial
4. 40k fb rce
5. Yahoo Bleed 1
6. Yahoo Bleed 2

Insecure Direct Object Reference (IDOR)

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

10. Duo Security Researchers Uncover Bypass of PayPal's Two-Factor Authentication by Duo Labs
11. Hacking Facebook.com/thanks Posting on behalf of your friends! by Anand Prakash
12. How I got access to millions of [redacted] accounts
13. All Vimeo Private videos disclosure via Authorization Bypass with Excellent Technical Description by Enguerran Gillier (opnsec)
14. Urgent: attacker can access every data source on Bime by Jobert Abma (jobert)
15. Downloading password protected / restricted videos on Vimeo by Gazza (gazza)
16. Get organization info base on uuid in Uber by Severus (severus)
17. How I Exposed your Primary Facebook Email Address (Bug worth $4500)by Roy Castillo
18. DOB disclosed using "Facebook Graph API Reverse Engineering" by Raja Sekar Durairaj
19. Change the description of a video without publish_actions permission in Facebook by phwd
20. 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!
21. Leak of all project names and all user names , even across applications on Harvest by Edgar Boda-Majer (eboda)
22. Changing paymentProfileUuid when booking a trip allows free rides at Uber by Matthew Temmy (temmyscript)
23. View private tweet
24. Uber Enum UUID
25. Hacking Facebook's Legacy API, Part 1: Making Calls on Behalf of Any Userby Stephen Sclafani

26. Hacking Facebook's Legacy API, Part 2: Stealing User Sessions by Stephen Sclafani
27. Delete FB Video
28. Delete FB Video
29. Facebook Page Takeover by Manipulating the Parameter by arunsureshkumar
30. Viewing private Airbnb Messages
31. IDOR tweet as any user by kedrisec
32. Classic IDOR endpoints in Twitter
33. Mass Assignment, Response to Request Injection, Admin Escalation by sean

XXE (XML External Entity)

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

Unrestricted File Upload

1. File Upload XSS in image uploading of App in mopub by vijay kumar
2. RCE deal to tricky file upload by secgeek
3. File Upload XSS in image uploading of App in mopub in Twitter by vijay kumar (vijay_kumar1110)

Server Side Request Forgery (SSRF)

1. ESEA Server-Side Request Forgery and Querying AWS Meta Data by Brett Buerhaus
2. SSRF to pivot internal network
3. SSRF to LFI
4. SSRF to query google internal server
5. SSRF by using third party Open redirect by Brett BUERHAUS
6. SSRF tips from BugBountyHQ of Images
7. SSRF to RCE
8. XXE at Twitter
9. Blog post: Cracking the Lens: Targeting HTTP's Hidden Attack-Surface

Race Condition

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

Business Logic Flaw

1. Facebook simple technical hack to see the timeline by Ashish Padelkar
2. How I Could Steal Money from Instagram, Google and Microsoft by Arne Swinnen
3. How I could have removed all your Facebook notes
4. Facebook — bypass ads account's roles vulnerability 2015 by POUYA DARABI
5. Uber Ride for Free by anand praka
6. Uber Eat for Free by

Authentication Bypass

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

HTTP Header Injection

1. Twitter Overflow Trilogy in Twitter by filedescriptor
2. Twitter CRLF by filedescriptor
3. Adblock Plus and (a little) more in Google
4. $10k host header by Ezequiel Pereira

Subdomain Takeover

1. Hijacking tons of Instapage expired users Domains & Subdomains by geekboy
2. Reading Emails in Uber Subdomains
3. Slack Bug Journey — by David Vieira-Kurz
4. Subdomain takeover and chain it to perform authentication bypass by Arne Swinnen

Author Write Up

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

XSSI

1. Plain Text Reading by XSSI
2. JSON hijacking
3. OWASP XSSI
4. Japan Identifier based XSSI attacks
5. JSON Hijack Slide

Email Related

1. This domain is my domain — G Suite A record vulnerability
2. I got emails — G Suite Vulnerability
3. How I snooped into your private Slack messages [Slack Bug bounty worth $2,500]
4. Reading Uber's Internal Emails [Uber Bug Bounty report worth $10,000]
5. Slack Yammer Takeover by using TicketTrick by Inti De Ceukelaire
6. How I could have mass uploaded from every Flickr account!

Money Stealing

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

Local File Inclusion

1. Disclosure Local File Inclusion by Symlink
2. Facebook Symlink Local File Inclusion
3. Gitlab Symlink Local File Inclusion
4. Gitlab Symlink Local File Inclusion Part II
5. Multiple Company LFI
6. LFI by video conversion, excited about this trick!

CSV Injection :

1. https://hackerone.com/reports/386116
2. https://hackerone.com/reports/72785
3. https://hackerone.com/reports/223344
4. https://hackerone.com/reports/244292
5. https://payatu.com/csv-injection-basic-to-exploit/
6. https://www.owasp.org/index.php/CSV_Injection
7. https://www.we45.com/blog/2017/02/14/csv-injection-theres-devil-in-the-detail

CRLF: (Carriage Return line feed)

1. https://www.netsparker.com/blog/web-security/crlf-http-header/
2. https://hackerone.com/reports/217058
3. https://hackerone.com/reports/66391
4. https://hackerone.com/reports/237357
5. https://www.acunetix.com/websitesecurity/crlf-injection/

6. https://www.owasp.org/index.php/CRLF_Injection

Host header injection :

1. https://www.linkedin.com/pulse/host-header-injection-depth-utkarsh-tiwari

2. https://hackerone.com/reports/94637

3. https://medium.com/@rockerramg94/host-header-injection-attack-6cf4ffeb5a03

4. https://dzone.com/articles/what-is-a-host-header-attack

5. https://www.acunetix.com/vulnerabilities/web/host-header-attack/

6. https://hackerone.com/reports/235281

Cache poisoning

1. https://blog.stackpath.com/glossary/cache-poisoning/

2. https://portswigger.net/blog/practical-web-cache-poisoning

3. https://hackerone.com/reports/487

4. https://www.hackerone.com/zerodaily/2018-08-10

HTTP Response Splitting

1. https://www.owasp.org/index.php/HTTP_Response_Splitting

2.http://projects.webappsec.org/w/page/13246931/HTTP%20Response%20Splitting

3. https://hackerone.com/reports/171473

4. https://hackerone.com/reports/52042

5. https://hackerone.com/reports/53843

Web parameter tampering :

1. https://www.owasp.org/index.php/Web_Parameter_Tampering

2. https://hackerone.com/reports/141090

3. https://hackerone.com/reports/218748

Express Lang injection:

1. https://portswigger.net/kb/issues/00100f20_expression-language-injection

2. http://danamodio.com/appsec/research/spring-remote-code-with-expression-language-injection/

3. https://www.owasp.org/index.php/Expression_Language_Injection

4. https://www.scribd.com/document/212883640/Expression-Language-Injection

HTML Injection

1. https://www.acunetix.com/vulnerabilities/web/html-injection/

2. https://www.owasp.org/index.php/Testing_for_HTML_Injection_(OTG-CLIENT-003)

3. https://admin.utep.edu/Default.aspx?tabid=54090

4. https://hackerone.com/reports/328210

5. https://hackerone.com/reports/324548

6. https://hackerone.com/reports/383117

Blind XPATH Injection:-

1. https://www.owasp.org/index.php/Blind_XPath_Injection

2. https://www.scip.ch/en/?labs.20180802

3. https://www.paladion.net/blogs/xpath-injection-in-xml-databases

4. http://www.hackeone.info/2017/11/xpath-injection-tutorial-to-hack.html

LDAP Injection:-

1. http://projects.webappsec.org/w/page/13246947/LDAP%20Injection

2. https://www.owasp.org/index.php/LDAP_injection

3. https://portswigger.net/kb/issues/00100500_ldap-injection

4. https://www.synopsys.com/software-integrity/resources/knowledge-database/ldap-injection.html

OS Command Injection

1. https://www.owasp.org/index.php/Command_Injection

2.https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013)

3. https://www.checkmarx.com/knowledge/knowledgebase/OS-Command_Injection

4. https://www.hackingarticles.in/beginner-guide-os-command-injection/

5. https://hackerone.com/reports/303061

6. https://hackerone.com/reports/331032

7. https://hackerone.com/reports/340208

8. https://hackerone.com/reports/390865

9. https://hackerone.com/reports/388936

10. https://medium.com/bugbountywriteup/command-injection-poc-72cc3743f10d

SOP Bypass

1. https://resources.infosecinstitute.com/bypassing-same-origin-policy-sop/#gref

2. https://www.hackinglab.com/misc/downloads/event_2010/simon_egli_same_origin_policy_v1.0.pdf

3. https://hackerone.com/reports/164916

4. https://hackerone.com/reports/399427

5. https://hackerone.com/reports/235200

UI redressing attack & Clickjacking :

1. https://www.owasp.org/index.php/Clickjacking

2. https://www.imperva.com/Resources/Glossary/clickjacking-ui-redressing

3. https://www.geeksforgeeks.org/clickjacking-ui-redressing/

4. https://www.thesecuritybuddy.com/vulnerabilities/what-is-clickjacking-or-ui-redress-attack/

5. https://nakedsecurity.sophos.com/2008/10/09/ui-redress-attacks-aka-clickjacking/

6. https://hackerone.com/reports/85624

7. https://hackerone.com/reports/299009

8. https://medium.com/@raushanraj_65039/google-clickjacking-6a04132b918a

9. http://jasminderpalsingh.info/single.php?p=87

10. http://blog.securelayer7.net/clickjacking-vulnerability-google-cloud-print/

Session Fixation :

1. https://www.owasp.org/index.php/Session_fixation

2. https://www.owasp.org/index.php/Testing_for_Session_Fixation_(OTG-SESS-003)

3. http://projects.webappsec.org/w/page/13246960/Session%20Fixation

4. https://medium.com/white-hats/introduction-to-session-fixing-75409ffeaa5

5. https://medium.com/@grep_security/session-fixation-broken-authentication-and-session-management-c37ce0111bf5

6. https://hackerone.com/reports/135797

7. https://hackerone.com/reports/18501

8. https://hackerone.com/reports/167698

Missing http only

1. https://www.owasp.org/index.php/HttpOnly

2. https://hackerone.com/reports/239380

3. https://hackerone.com/reports/75357

4. https://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/#gref

Error Message Reveals sensitive Information/ Visible Detailed Error/Debug Page

1. https://hackerone.com/reports/304708

2. https://hackerone.com/reports/294464

3. https://hackerone.com/reports/20279

Token Leakage via Referrer

1. https://hackerone.com/reports/272379

2. https://hackerone.com/reports/342693

3. https://hackerone.com/reports/252544

4. https://hackerone.com/reports/265740

5. https://hackerone.com/reports/253448

User Enumeration:

1.https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)

2. https://blog.rapid7.com/2017/06/15/about-user-enumeration/

3. https://www.hacksplaining.com/prevention/user-enumeration

4. https://portswigger.net/blog/preventing-username-enumeration

5. https://hackerone.com/reports/282564

6. https://hackerone.com/reports/280509

7. https://hackerone.com/reports/250457

8. https://hackerone.com/reports/179701

9. https://hackerone.com/reports/223531

10. https://hackerone.com/reports/257035

11. https://hackerone.com/reports/335427

CSS Injection :

1. https://portswigger.net/kb/issues/00501300_css-injection-reflected
2. https://www.owasp.org/index.php/Testing_for_CSS_Injection_(OTG-CLIENT-005)
3. https://hackerone.com/reports/315865
4. https://hackerone.com/reports/386334

Miscellaneous

1. SAML Pen Test Good Paper
2. A list of FB writeup collected by phwd by phwd
3. NoSQL Injection by websecurify
4. CORS in action
5. CORS in Fb messenger
6. Web App Methodologies
7. XXE Cheatsheet
8. The road to hell is paved with SAML Assertions, Microsoft Vulnerability
9. Study this if you like to learn Mongo SQL Injection by cirw
10. Mongo DB Injection again by websecrify
11. w3af speech about modern vulnerability by w3af
12. Web cache attack that lead to account takeover
13. A talk to teach you how to use SAML Raider
14. XSS Checklist when you have no idea how to exploit the bug

15. CTF write up, Great for Bug Bounty
16. It turns out every site uses jquery mobile with Open Redirect is vulnerable to XSS by sirdarckcat
17. Bypass CSP by using google-analytics
18. Payment Issue with Paypal
19. Browser Exploitation in Chinese
20. XSS bypass filter
21. Markup Impropose Sanitization
22. Breaking XSS mitigations via Script Gadget
23. 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

Writing Successful Bug & Vulnerability Submission Report

What does a good report look like?

Legend has it that the best bug bounty hunters can write reports in their sleep. OK, jokes aside, while writing reports is a very important part of bug bounty hunting, we can simplify this whole process by following these basic guidelines.

Summary

The first section of your report should start with a brief summary introducing the reader to your finding. Summaries can be as simple as:

example.com is vulnerable to reflected XSS via the `q` parameter.

Or as detailed as:

> https://imgur.com/vidgif/url endpoint is vulnerable to a SSRF vulnerability which allows an attacker to craft connections originating from imgur servers to any destination on the internet and imgur internal network and craft outgoing UDP-packets / telnet-based protocol sessions (for example, to connect to SMTP servers from imgur and send spam). [1]

Vulnerability Description

This section covers all the details related to your finding. State what you found again, make the technical points clear, and explain what causes the issue. There are exceptions though where this section can be skipped. There is a popular English idiom:

> "A picture is worth a thousand words."

The same can be said about an excellent proof of concept:

> "A phenomenal security vulnerability proof of concept is worth a thousand words."
> - Probably Gandhi

Proof of concept

The proof of concept is where you really need to demonstrate the impact in the "flashiest" way possible. Make it as easy as possible for the program to see what the issue is. If your issue is cross-site scripting, then an `alert(document.domain)` can go a long way to help the program figure out where the issue lies.

Browsers verified in

Even if the issue is not browser-dependent, it is good practice to inform the program about what browser you used to trigger the vulnerability. This can help the team behind the bug bounty program reproduce your finding.

- Google Chrome: visit `chrome://version/`
- Mozilla Firefox: top-right menu icon → **?** "Help" → "About Firefox"
- Microsoft Internet Explorer: top-right cog → "About Internet Explorer"
- Microsoft Edge: **...** → "Settings" → scroll down

Mitigation

If you followed the advice in *"How do I get started with bug bounty hunting?"*, you should be capable of giving a brief description of how the bug bounty program should fix your finding. It is also a good idea to link to the relevant *OWASP Prevention* cheat sheet.

Report Writing 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/

Good Report Example :

1. https://hackerone.com/reports/73567
2. https://bugbountyguide.com/hunters/writing-reports.html

Some great resources for vulnerability report best practices are:

1. Dropbox Bug Bounty Program: Best Practices
2. Google Bug Hunter University
3. A Bounty Hunter's Guide to Facebook
4. Writing a good and detailed vulnerability report

Hope you like it , If you have any queries … Feel free to connect me through linkedin or Twitter :) If I missed something, kindly comment below so i will add to the Bug Bounty-Infosec List- If you like this blog- do clap and share with your friends :)

Whoami:- https://infosecsanyam.wixsite.com/infosecsanyam

Blog :- https://infosecsanyam.blogspot.in/

Linkedin : https://www.linkedin.com/in/infosecsanyam/

"Failure will never overtake me if my determination to succeed is strong enough." " If you don't give up , you still have a chance" :)

📝 Read this story later in Journal.

🗞️ Wake up every Sunday morning to the week's most noteworthy Tech stories, opinions, and news waiting in your inbox: Get the noteworthy newsletter >

Security Cybersecurity Web Security Bug Bounty Methodology