

Bug Hunting Methodology(Part-2)



Shankar R

Mar 14 · 10 min read

Hi I am Shankar R (@trapp3r_hat) from Tirunelveli (India). I hope you all doing good. I am a security researcher from the last one year. Yes absolutely am doing bug bounty in the part-time Because I am working as a Senior Penetration Tester at Penetolabs Pvt Ltd(Chennai).

Here is my first write up about the Bug Hunting Methodology Kindly read the first one if you really missed it to read previously.(I am not sure this write-up will be an interesting one compared to the previous.).

Sorry for the delay to make this write-up. Because I was busy with my office projects.

In this write-up I will share my some of the advice to chain vulnerabilities to increase the impact and some guidance to burp plugins which I used daily while hunting

How to make a good report !!

We can find ton of write-ups for this section but one of my favorite is





The importance of Impact:

Many researchers are looking for a bug on the target if they found a small vulnerabilities then they have reported to the target. Sometimes report will be marked as N/A even it is valid one. That will be very frustrated to the researcher(they feels like they wasted time with this target).

Always kindly think about the impact and how to increase the impact of the bug and we should explain about the real time attack scenario that should we need to concentrate while hunting.

Why N/A for valid bugs !!

If you find a valid bug(like SQLi, RCE, OS Command Injections) on the target it should be high impact as per the attacker's or researcher's perspective but the organizations are having some standards to identify and fix the bugs

For example: The bug was SQLi found on one of the domain from the target. Once the report is placed then they will start investigating the bug. If the target is not a critical asset based on their view or the business impact is very low because of that SQLi and sometimes the fixing cost is more than the impact of the SQLi. So that time SQLi will be closed as N/A(Not Applicable) You can see those types of report closed as N/A even it is a valid IDOR or Rate Limiting Bugs in facebook Bug bounty(**They closed my IDOR was closed as NA**)

Thanks to [Parthiban J](#) sir to share these of type of information with me.

How long we need to spend for recon ?(ignore this if you are getting bored in this section)

Basically I spend minimum 3 days(*Usually more than 20 hours because I am not a full time bug bounty hunter*) to collect information about my target(Based on the Target).

Don't jump to other targets before you finish your proper recon. If you jump to other targets with the minimum efforts then there is no opportunity to find a good bugs.

How to Increase the Impact

This part will help you to get an idea to increase the impact of the low hanging fruits

Scenario 1:

- If you found a private IP (Actually that is a public IP only) of the target. This time don't report to them. Try to increase the impact of the issue by doing port-scan on the IP which you found.
- Then look for vulnerable service version by doing the service scan with the Nmap tool.
- If there is a vulnerable service is running on the target then look for publicly available CVE based exploits

Note: If you are getting bored(Called as Lazy baby 😊😊) then do the Nmap script scanning on the IP which will give you some CVE based vulnerability(Based on your luck)

Scenario 2:

- Sometimes this may leads to the source code disclosure or any other sensitive informations like API key or 2FA Authentication Tokens.

Scenario 3:

- If you found a web server with the default web page, Then try to brute-force the directory which is based on the what type of server is running on the target machine that will helpful to find some default config files of a web server.

This is write-up I will explain about the following

Burpsuite Extension Series:

Burp Collaborator

How its works ! Can you understand this pictures. If no then see my description for this tool.



How Collaborator tool is detecting external service interaction:

A typical external service interaction issue can be detected as follows:

Note: Here the above highlighted field is the collaborator domain this is randomly generated by the collaborator server.

- Due to its programmed behavior (intended or otherwise), the application fetches the contents of the URL. To do this, it will first perform a DNS lookup on the random subdomain, and then perform an HTTP request.
- The DNS lookup and the HTTP request are received by the Collaborator server. Both interactions contain the random data that Burp placed into the Collaborator subdomain.
- Burp polls the Collaborator server and asks: “Did you receive any interactions for my payload?”, and the Collaborator returns the interaction details.
- Burp reports the external service interaction to the Burp user, including the full interaction messages that were captured by the Collaborator server.

The original source Link:

<https://portswigger.net/burp/documentation/collaborator>

Reference Link to know how it works and how it is very helpful to us!!



A Burp Suite Pro extension which augments your proxy traffic by injecting non-invasive headers...

github.com



Burp Macro:

This is not an Extension. This is a one of the great features by the Burp Suite

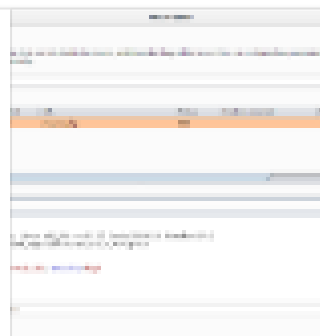
A macro is a predefined sequence of one or more requests. You can use macros within session handling rules to perform various tasks. Typical use cases for macros include:

- Fetching a page of the application (such as the user's home page) to check that the current session is still valid.
- Performing a login to obtain a new valid session.
- Obtaining a token or nonce to use as a parameter in another request.
- When scanning or fuzzing a request in a multi-step process, performing the necessary preceding requests, to get the application into a state where the targeted request will be accepted.
- In a multi-step process, after the "attack" request, completing the remaining steps of the process, to confirm the action being performed, or obtain the result or error message from the conclusion of that process.

Burp Macros and Session Handling - DigiNinja

A guide for what to writing Burp Suite macros and session handling rules

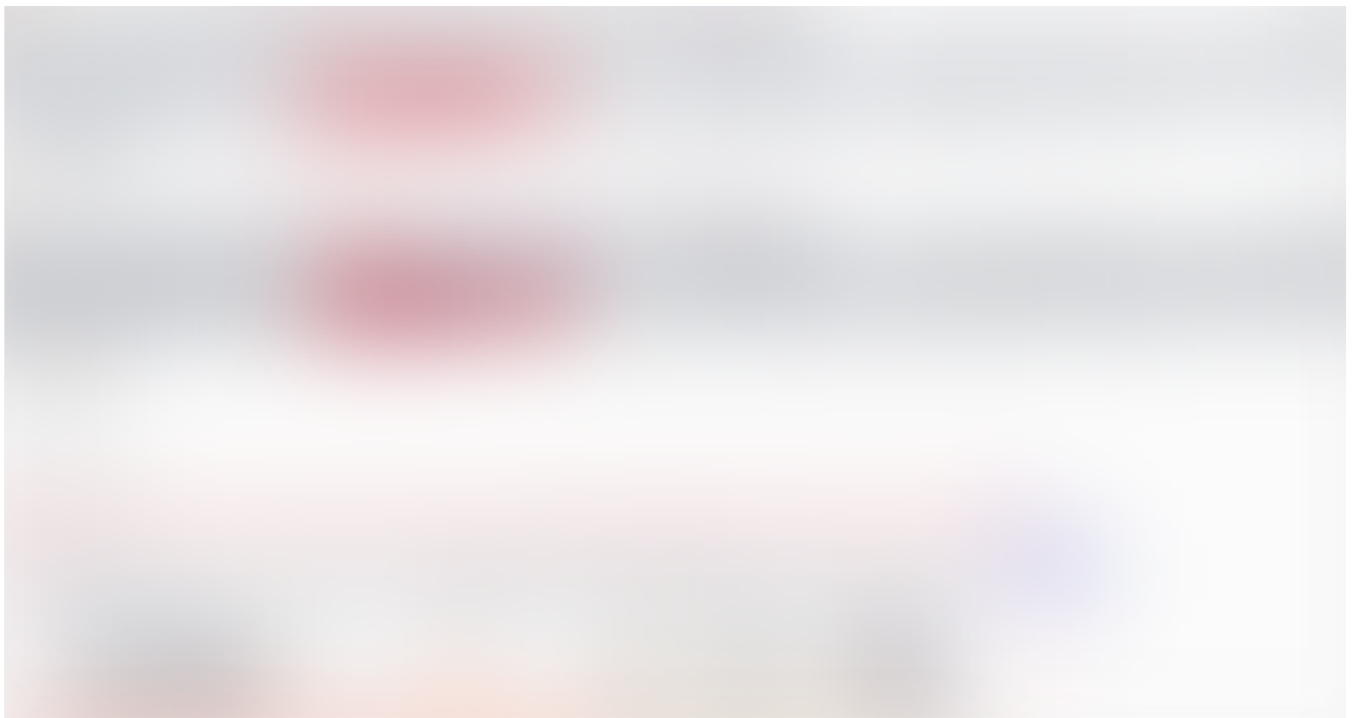
digi.ninja



BackSlash Powered Scanner

We can find lots and lots of server side vulnerabilities with this tool. But we need to understand about target application and how it's responds for different input which is done by this tool by default

Initially we need to enable the Backslash Powered scanner settings from the scanner tab. For more info checkout the below image



Extension Download Link:

PortSwigger/backslash-powered-scanner

Finds unknown classes of injection vulnerabilities
- PortSwigger/backslash-powered-scanner

github.com



AuthMatrix

AuthMatrix is an extension to Burp Suite that provides a simple way to test authorization in web applications and web services. With AuthMatrix, testers focus on thoroughly defining tables of users, roles, and requests for their specific target application upfront. These tables are structured in a similar format to that of an access control matrix common in various threat modeling methodologies.

PortSwigger/auth-matrix

AuthMatrix is a Burp Suite extension that provides a simple way to test authorization in web...

github.com



Note: We can use the Authz and Authoriz Extensions instead of AuthMatrix

PsychoPath

A Blind web root file upload and LFI detection tool

For this tool I didn't find any documentation other than this link

PortSwigger/psycho-path

psychoPATH - hunting file uploads & LFI in the dark. This tool is a customisable payload generat...




Upload Scanner

1. While uploading the file which supports formats it, use the exiftool file format meta data techniques “keywords”, “comment”, “iptc:keywords”, “xmp:keywords”, “exif:ImageDescription” and “ThumbnailImage”
2. It injects PHP, JSP, ASP, XXE, SSRF, XXS and SSI payloads on the target
- 3, It will upload with various combinations of file extensions and content- types on the target
- 4, Also it detects the issues via sleep based payloads, Burp Collaborator interactions or by downloading the file again

For tutorial kindly find the link below

https://www.modzero.ch/share/uploadscanner/UploadScanner_101_Basics.mp4

Extension Download Link:

<p>PortSwigger/upload-scanner</p> <p>HTTP file upload scanner for Burp Proxy. Contribute to PortSwigger/upload-scanner...</p> <p>github.com</p>	
--	---

DeSerialization Scanner

This extension gives Burp Suite the ability to find Java deserialization vulnerabilities.

Serialized Java objects begin with “**ac ed**” when in hexadecimal format and “**r00b**” when base64-encoded.

The content type header value will be equal to **application/x-Java-serialized-object**(It is not presented in GET request but we need to find the vulnerable endpoint and exploit with the post request)

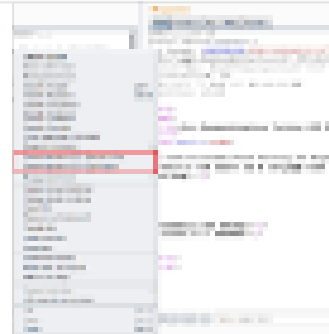
- <https://github.com/frohoff/ysoserial/releases>
- <https://github.com/joaomatosf/jexboss>

Reference Link

Reliable discovery and exploitation of Java deserialization vulnerabilities

Java deserialization vulnerabilities were discovered and disclosed in January 2015 by Gabriel Lawren...

techblog.mediaservice.net



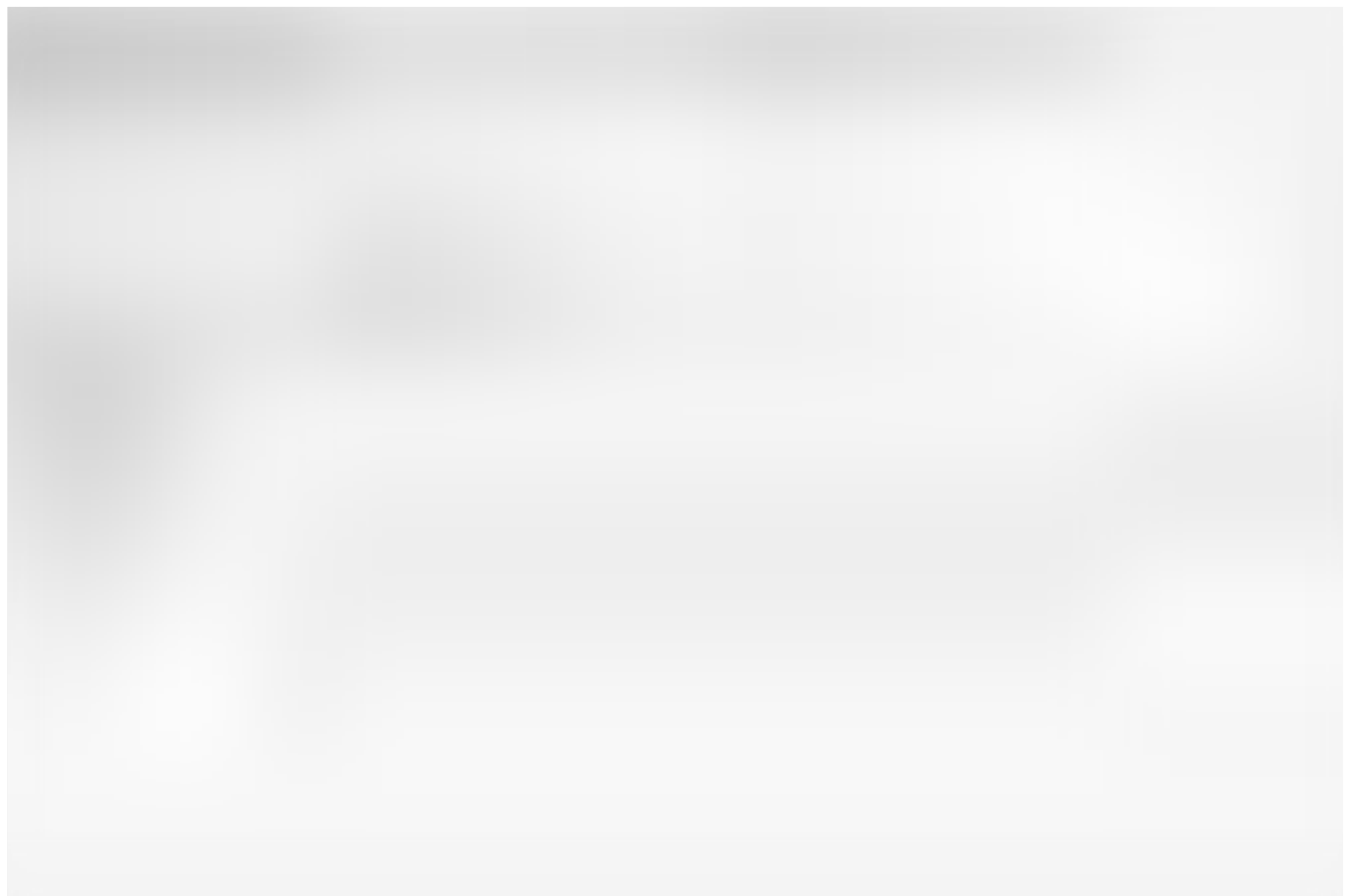
Reflector

Burp Suite extension is help us to find reflected XSS (**Sometimes SSI injection which is based on the target**)on page in real-time while browsing on web-site and include some features as:

- Content-Type white-list

How to use

After plugin install you just need to start work with the tested web-application. Every time when reflection is found, reflector defines severity and generates burp issue.

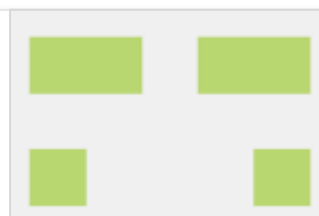


Note: Moreover you can manage content-types whitelist with which reflector plugin should work. But if you will use another types except text/html, this can lead to slowdowns in work.

Extension Download Link

elkokc/reflector

Burp plugin able to find reflected XSS on page in real-time while browsing on site - elkokc/reflector



I didn't tested yet but I was impressed with this tool. You can try at-least once to find the Race Limiting bugs

Extension Download Link

PortSwigger/turbo-intruder

Turbo Intruder is a Burp Suite extension for sending large numbers of HTTP requests and...

github.com



Burp-vulners-scanner:

It co-relate real time traffic with the exploit db. This is also similar to the extension Retire.js

Extension Download Link:

<https://github.com/vulnersCom/burp-vulners-scanner/releases/download/1.1/burp-vulners-scanner-1.1.jar>

Reference Link:

The best Burp plugin I've ever seen

Wanted to share with you what IMHO is the most promising Burp Suite plugin that just might...

medium.com



Burp ClickBandit

This tool is specifically for clickjacking only. Most of the people are confused with the clickjacking attack vector. But this tool will help us to clarify the real time attack scenario.

What is chaining of vulnerabilities ?

This is technique which the researcher can able to increase the impact of the bug or vulnerabilities using 2 or more bugs.

This is possible while some of the vulnerabilities with the low impact or self based vulnerabilities like self XSS and login CSRF and Logout CSRF, Clickjacking (Which are the out of scope bugs in many targets)etc.

How to chain vulnerabilities ?

I will share some of the great write-ups which the researcher exploits with the chaining of vulnerabilities(**Simple to Hard**)

Open Redirection to XSS

We can see ton of report for these type of chain

- <https://medium.com/@SyntaxError4/reflective-xss-and-open-redirect-on-indeed-com-subdomain-b4ab40e40c83>
- <https://hackerone.com/reports/260744>
- <https://hackerone.com/reports/196846>

Open Redirection to OAuth Token Stealing

- <https://www.arneswinnen.net/2017/06/authentication-bypass-on-airbnb-via-oauth-tokens-theft/> (This is my one of the favorite bug)
- <https://medium.com/@protector47/full-account-takeover-via-referrer-header-oauth-token-steal-open-redirect-vulnerability-chaining-324a14a1567>

- <https://winton.io/articles/uber-turning-self-xss-into-good-xss/>
- In this report Self xss is become a good XSS with the help of Clickjacking
<https://medium.com/@arbazhussain/self-xss-to-good-xss-clickjacking-6db43b44777e>
- <https://www.youtube.com/watch?v=bP6JwcDwEZE>
- <https://www.geekboy.ninja/blog/airbnb-bug-bounty-turning-self-xss-into-good-xss-2/>

LFI to RCE:

From Local File Inclusion to Remote Code Execution - Part 1 | Outpost 24 blog

Local File Inclusion - aka LFI - is one of the most common Web Application vulnerabilities. If...

outpost24.com



- <https://medium.com/bugbountywriteup/bugbounty-journey-from-lfi-to-rce-how-a69afe5a0899>
- This write up Will give you an Idea for LFI to RCE chaining
<https://resources.infosecinstitute.com/local-file-inclusion-code-execution/#gref>

SSRF to XSS

- <https://medium.com/bugbountywriteup/piercing-the-veil-server-side-request-forgery-to-niprnet-access-c358fd5e249a>
- <http://blog.orange.tw/2017/07/how-i-chained-4-vulnerabilities-on.html>
- <https://medium.com/@D0rkerDevil/how-i-convert-ssrf-to-xss-in-a-ssrf-vulnerable-jira-e9f37ad5b158>
- <https://medium.com/@adeshkolte/how-i-found-xss-via-ssrf-vulnerability-adeshkolte-873b30a6b89f>

- <https://medium.com/@hisham.mir/exploiting-a-single-parameter-6f4ba2acf523>
- <http://www.kernelpicnic.net/2017/05/29/Pivoting-from-blind-SSRF-to-RCE-with-Hashicorp-Consul.html>

SSTI to RCE:

- <https://hawkinsecurity.com/2017/12/13/rce-via-spring-engine-ssti/>

Miscellaneous:

https://medium.com/@logicbomb_1/bugbounty-how-i-was-able-to-bypass-firewall-to-get-rce-and-then-went-from-server-shell-to-get-783f71131b94

What is next (Bug Hunting Methodology Part-3) ?

Let me post some pro-tips which I collected and found from Twitter, Facebook, 1337 Suggestions and finally my own experience (which is less compared to others)

Special Thanks to **Rahul Raj**, **Velayutham SelvaRaj**, **Sreeram KL**, **Ashish Kunwar**, **John Simon**, **Sai Naik** Etc..

Kindly share your feedback with me. And let me know if there is anything wrong which I mentioned above

Thanks & Regards,

Shankar R

. . .



Noteworthy - The Journal Blog

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

Bug Hunting

Bug Bounty

Security Tool



350 claps



...



WRITTEN BY

Shankar R

Security Researcher | IBM Certified Associate Administrator
Security QRadar SIEM V7.2.8 | Penetration Tester

Follow



Noteworthy - The Journal Blog

The Official Journal Blog

Follow

[See responses \(4\)](#)

