BASIC

BUG HUNTING

METHODOLOGY

#WHOAMI

#SHAHRUKH RAFEEQ

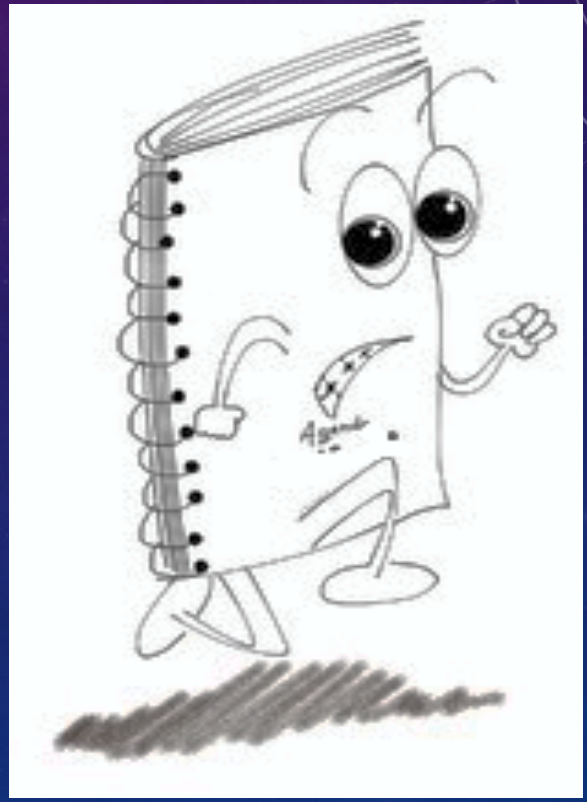
~/GRADUATE | CEH | Freelancer | Occasional Bug Hunter

logicalsrk@gmail.com | https://softwaroid.com

@d3tonator

AGENDA

- Select Target for Hunting
- How to start bug hunting
- Hunting method and Mindset
- Low Hanging Hunt
- Importance of understanding application flow
- Recon Techniques
- Report writing



BUG HUNTING

Identify the bugs or security vulnerabilities in a computer program/system or web application. Companies invite to individual to hack their assets and offer monetary rewards or swag or Hall of Fame.

Bug Hunting Program:

1. **Public Platform:** Hackerone, Bugcrowd, Intigriti, bugbounty.jp, antihack.me, yeswehack etc.
2. **Invite Only Program:** Syanck, Zerocopter, Yogasha, **Cobalt**,
3. **Self-Hosted Program:** Microsoft, Apple, Facebook, Google
4. **Non-Platform Program:** dorks…
5. **Bug Bounty Programs** https://www.bugcrowd.com/bug-bounty-list/

DORKS FOR FIND PROGRAM

- inurl : /bugbounty
- inurl : /responsible disclosure
- inurl : /whitehat
- inurl : /hall of fame
- inurl : /security/bugbounty
- inurl : /security/responsible disclosure
- inurl : /security/whitehat
- inurl : /security/hall of fame

- **My Special one:** "van de melding met een minimum van een" -site:responsibledisclosure.nl
- ”Responsible Disclosure”
- Responsible Disclosure “Reward”
- Responsible Disclosure “Bounty
- Responsible Disclosure “Swag”
- Responsible Disclosure “100$”
- ”Bug Bounty” “Reward”
- ”Powered by” Bugcrowd

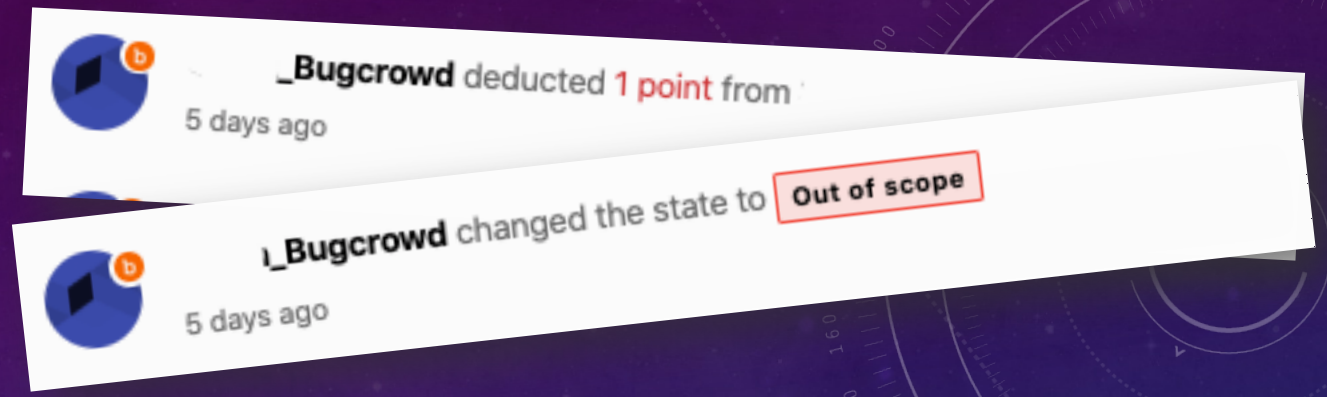
CHOOSE TO HUNT

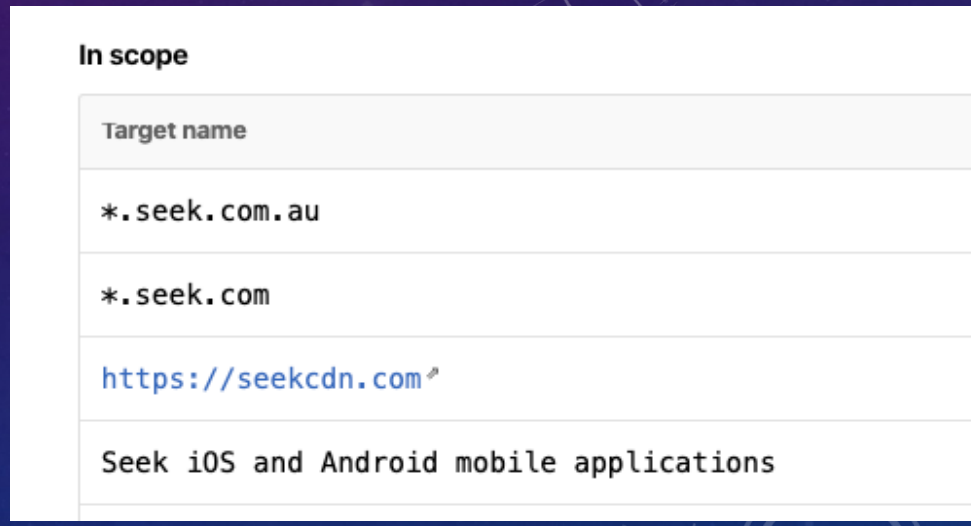
Assets in scope:

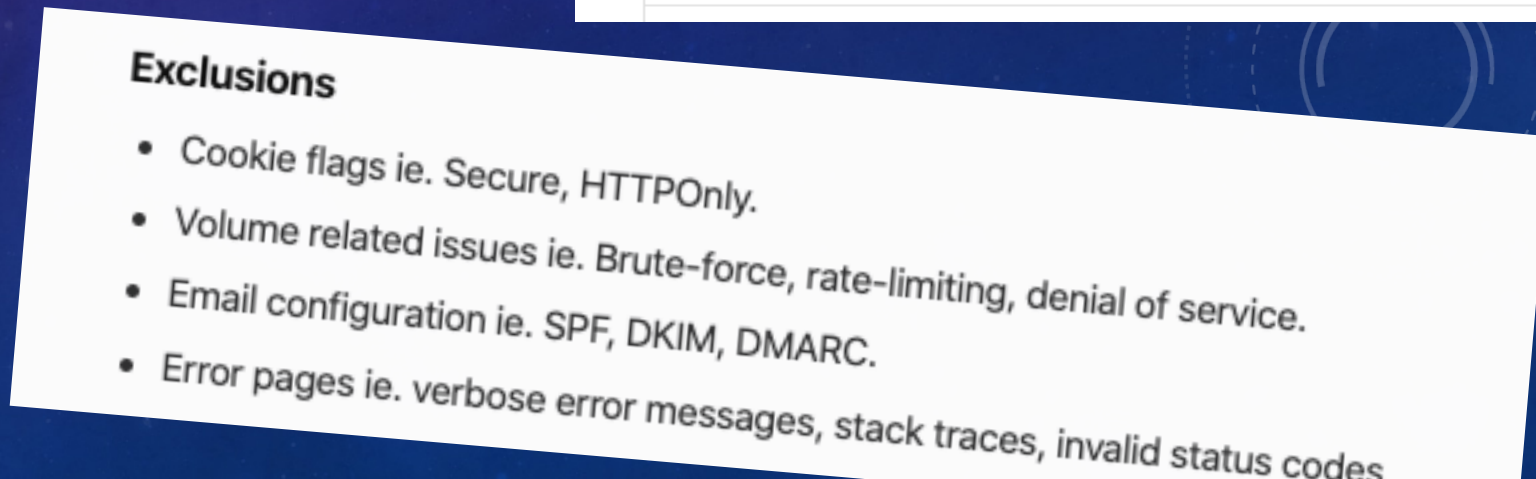
- Priority to wildcard {*.example.com}
- Mobile Apps

Paying attention to out of scope / exclusions list:

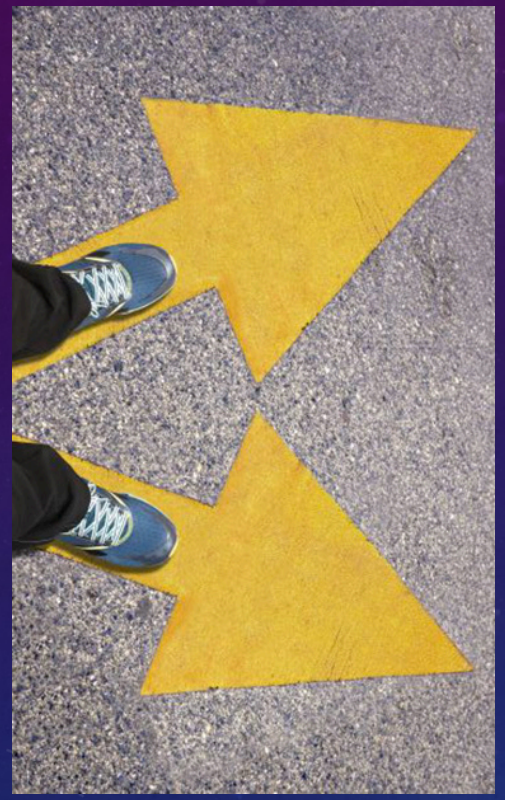
- Clickjacking
- No Rate Limit / Mail Bombing
- SPF / DMARC







LET’S START TO HUNT



Bug → Target → BOUNTY

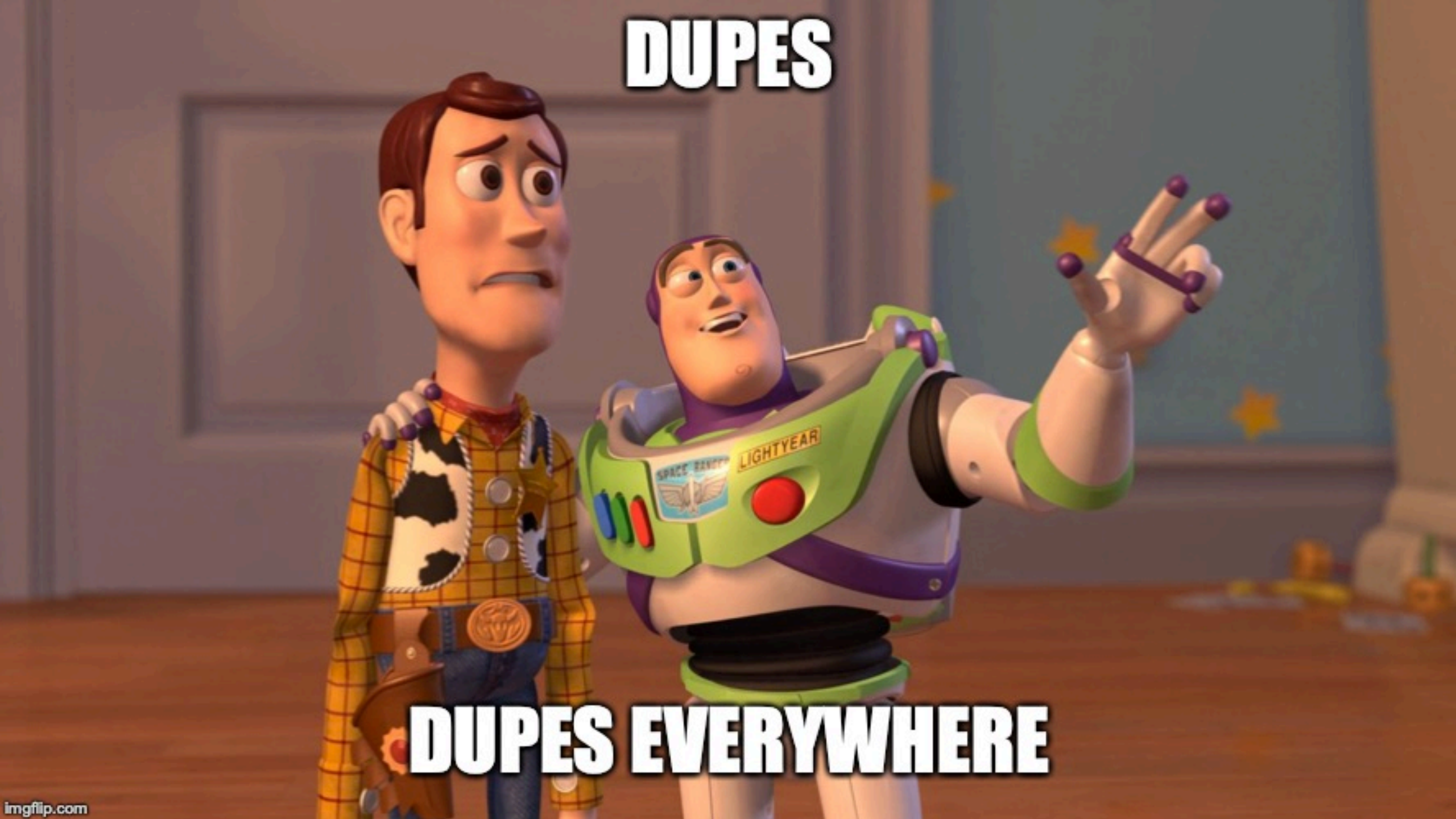
Target → Bug

BUG TO TARGET | LOW HANGS

Make your own list try these test cases everywhere:

- SPF / DMARC
- Password Reset Functionality Exploit
- Referer Token Leakage to Third party
- Session Not Invalidate after Logout
- Rate Limit on Password Reset Page/Email Triggering Form
- Lack of password confirmation while deleting account
- Open Redirection
- Host Header Injection
- Clickjacking on Payment Page
- XSS on known field
- No Password Policy
- Token not invalidate after one time use
- Long Password DOS attack
- Cross-Origin Resource Sharing (CORS)
- CSRF on authenticated Forms
- XML RPC on WordPress

Not limited ….


DUPES
LIGHTYEAR
DUPES EVERYWHERE
imgflip.com

rewarded **Lacking Permission to validate the Android scheme discloses access token to third party Apps** with $300.

Tweet this

Congratulations! has awarded **$300** for your submission **Lacking Permission discloses access token to third party Apps.**

Thanks!

Information on final processing and payment of your submission will be sent to you shortly - so stay tuned!

Failure to Invalidate Session after Password Change
(Closed) · Updated a month ago
P4 Resolved
$42
5 points
Comments 10

No Rate Limit on Forget Password Functionality Leading Huge Mail Bombing
(Closed) · Updated a month ago
P4 Resolved
$242
5 points
Comments 5

No Spoofing Protection on groundspeak.com (Main Domain)
(Closed) · Updated 21 days ago
P4 Unresolved
$168
5 points
Comments 8

Server failed to sanitize user input, Full Name convert into Hyperlink while account activation
(Private) · Updated 3 months ago
P4 Resolved Duplicate
$0
1 point
Comment 1

Lack of Password Confirmation while Account Deletion
(Private) · Updated 3 months ago
P4 Won't fix Duplicate
$0
1 point
Comment 1

Failure to Invalidate Session after Password Change
· Updated 6 months ago
P4 Unresolved Duplicate
$0
1 point
Comments 0

Session Failure to Invalidate after Logged out from Client and Server Side
· Updated 6 months ago
P4 Won't fix Duplicate
$0
1 point
Comment 1

Failure to Invalidate Session after Password Change
· Updated 6 months ago
P4 Unresolved Duplicate
$0
1 point
Comment 1


TARGET TO BUG

UNDERSTAND THE APPLICATION | RECON

Diving deep into the target, understand the application as End User. How a bad guy can harm the application

- Find all the **ASSETS** that belongs to that organization. Assets?
  - Domains & Subdomains Enumerate using: VirusTotal, Subbrute, Sublist3r, Aquatone
- IP Ranges and Port Scanning: Nmap, Masscan
- Directory Brute-force: DirBuster, dirsearch, dirb
- Run Content-Discovery in Burp Suite
- Analyze Injection Point using: Burp Spider, Reflected Parameter (Burp Plugin), Hunt-Master
- iOS / Android Apps

DOMAIN & SUBDOMAIN ENUMERATION

- Sublist3r https://github.com/aboul3la/Sublist3r

  ```
  #python sublist3r.py -d example.com
  #python sublist3r.py -d example.com -p 80,443 (Port Scanning)
  ```

- Subbrute https://github.com/TheRook/subbrute

  ```
  #./subbrute.py example.com
  ```

- Amass https://github.com/OWASP/Amass

  ```
  #amass enum -d example.com -brute -o subdomainm.txt
  ```

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

  ```
  #Aquatone-discover —d example.com
  ```

- VirusTotal https://www.virustotal.com/gui/home/search

  #https://www.virustotal.com/gui/domain/{example.com}/relations

PORT SCAN & DIRECTORY BRUTEFORCE

- **Nmap**

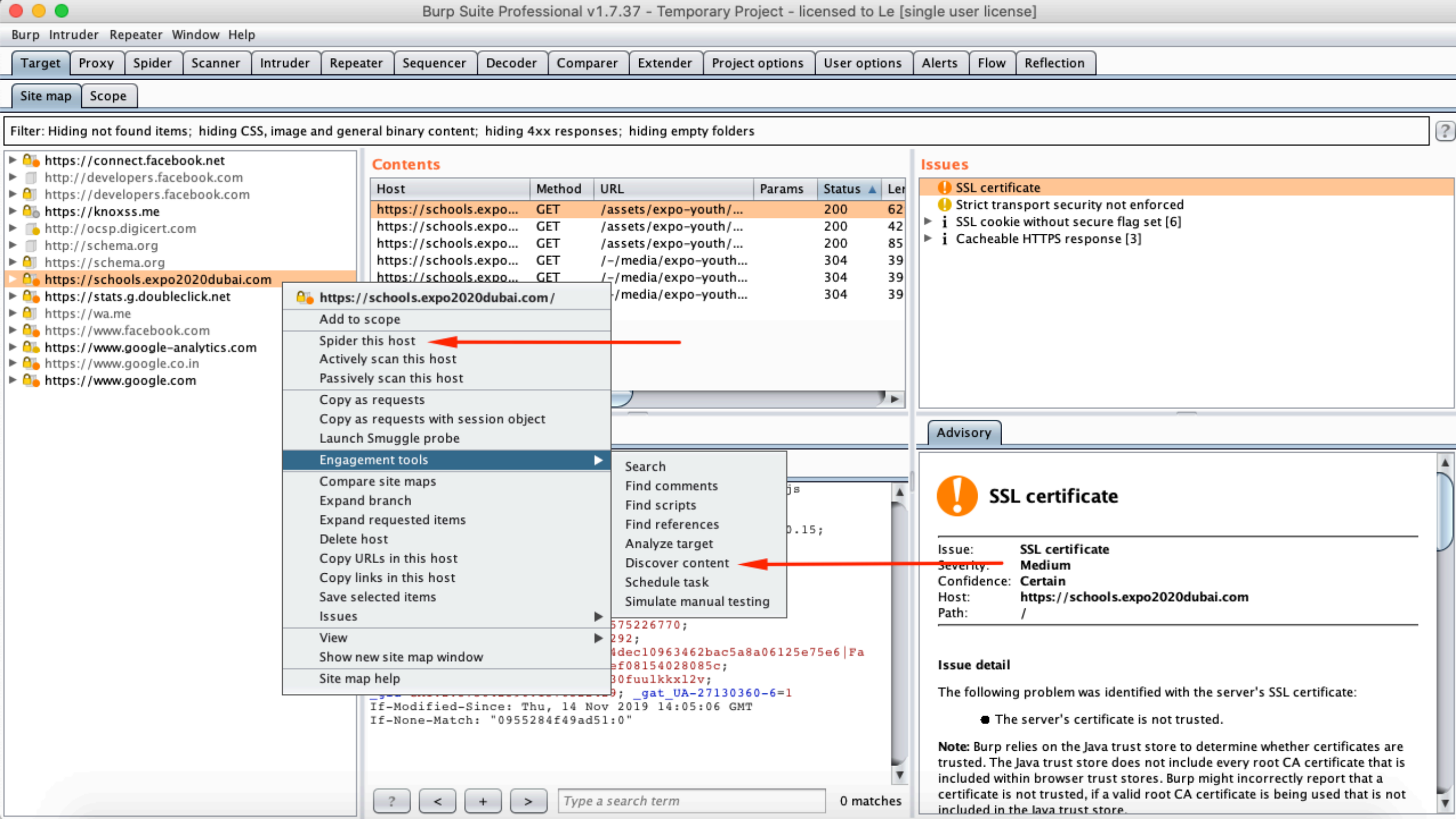
  ```
  #nmap –sC –sV 10.0.0.0

  #nmap -p 1-65535 -sV -sC -T4 target
  ```

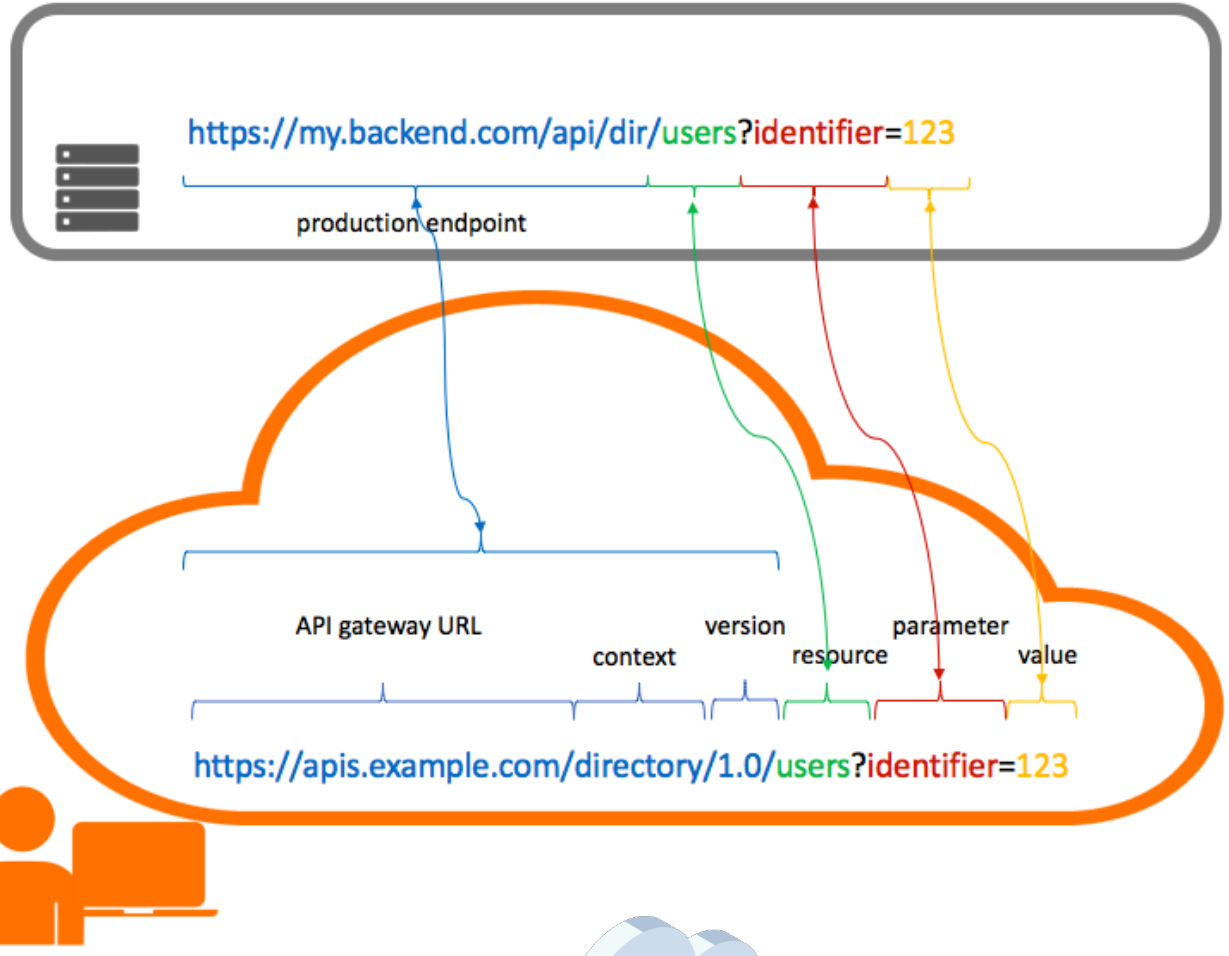
- **Mass Scan**

  ```
  #masscan -p1-65535 -iL target.txt --max-rate 10000 -oG target_output
  (Entire Port scan of List of Domain )

  #masscan –p 80,8000-8100 10.0.0.0/8 (For Specific Port)

  #masscan 0.0.0.0/0 -p0-65535 -oX scan.xml (Entire Port Scan)
  ```

- **Directory Bruteforce**

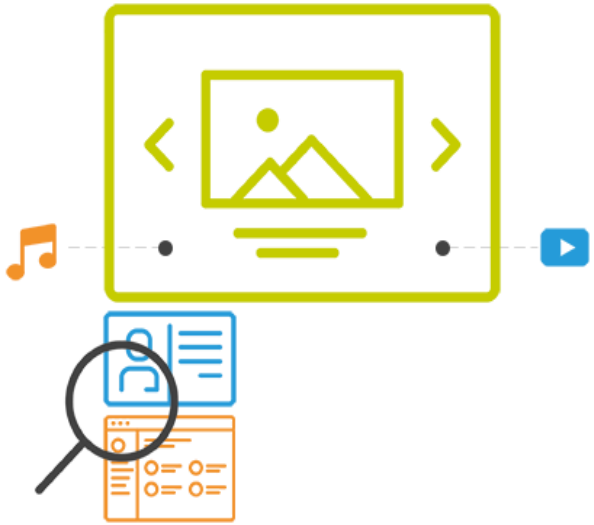
  ```
  #python dirsearch.py –d example.com/ -e .

  #dirb example.com /usr/share/wordlists/dirb/common.txt
  ```


Burp Suite Professional v1.7.37 - Temporary Project - licensed to Le [single user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Flow Reflection
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://connect.facebook.net
http://developers.facebook.com
https://developers.facebook.com
https://knoxss.me
http://ocsp.digicert.com
http://schema.org
https://schema.org
https://schools.expo2020dubai.com
https://stats.g.doubleclick.net
https://wa.me
https://www.facebook.com
https://www.google-analytics.com
https://www.google.co.in
https://www.google.com
Contents
Host Method URL Params Status Len
https://schools.expo... GET /assets/expo-youth/... 200 62
https://schools.expo... GET /assets/expo-youth/... 200 42
https://schools.expo... GET /assets/expo-youth/... 200 85
https://schools.expo... GET /-/media/expo-youth... 304 39
https://schools.expo... GET /-/media/expo-youth... 304 39
/media/expo-youth... 304 39
https://schools.expo2020dubai.com/
Add to scope
Spider this host
Actively scan this host
Passively scan this host
Copy as requests
Copy as requests with session object
Launch Smuggle probe
Engagement tools
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Issues
View
Show new site map window
Site map help
Search
Find comments
Find scripts
Find references
Analyze target
Discover content
Schedule task
Simulate manual testing
575226770;
292;
4dec10963462bac5a8a06125e75e6|Fa
ef08154028085c;
30fuulkkx12v;
; _gat_UA-27130360-6=1
If-Modified-Since: Thu, 14 Nov 2019 14:05:06 GMT
If-None-Match: "0955284f49ad51:0"
? < + > Type a search term 0 matches
Issues
SSL certificate
Strict transport security not enforced
SSL cookie without secure flag set [6]
Cacheable HTTPS response [3]
Advisory
SSL certificate
Issue: SSL certificate
Severity: Medium
Confidence: Certain
Host: https://schools.expo2020dubai.com
Path: /
Issue detail
The following problem was identified with the server's SSL certificate:
The server's certificate is not trusted.
Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

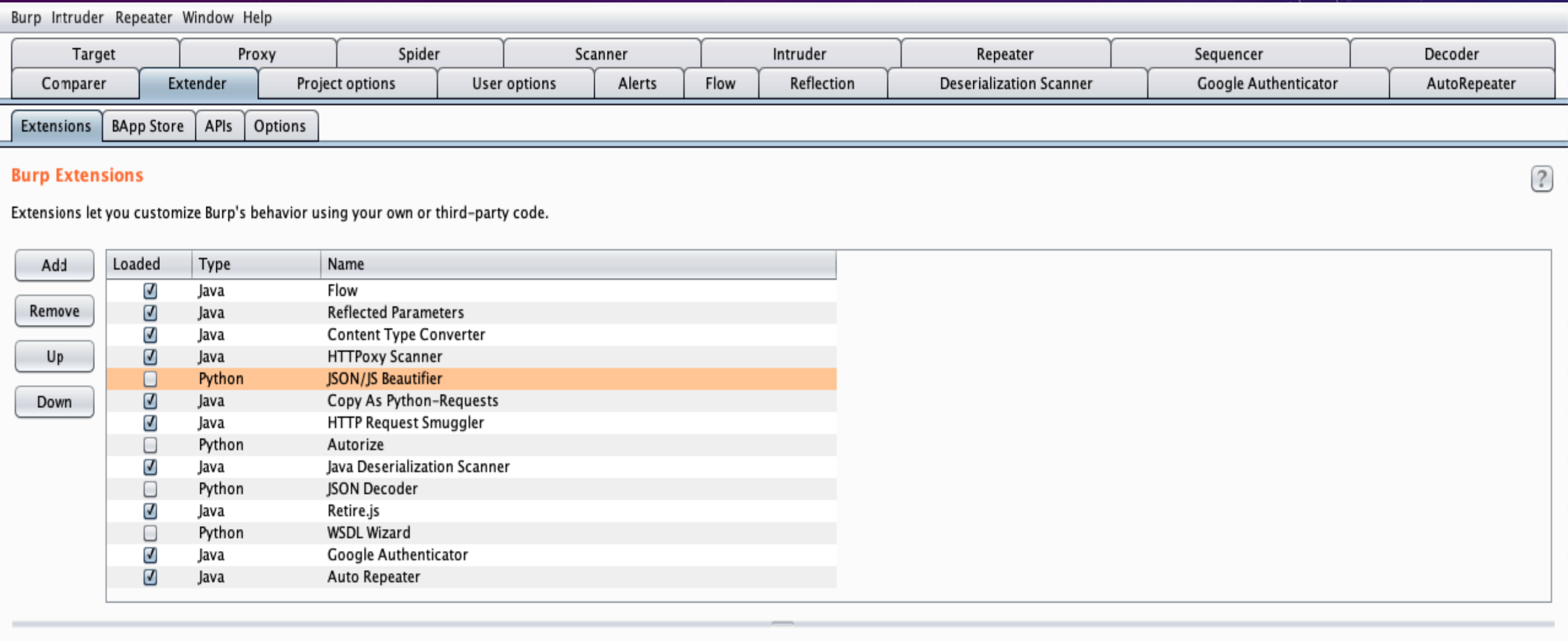

https://my.backend.com/api/dir/users?identifier=123
production endpoint
API gateway URL
context
version
resource
parameter
value
https://apis.example.com/directory/1.0/users?identifier=123


BEHIND
THE SCENES

GUI Testing



BURP USEFUL EXTENSION



REPORT WRITING

- Summary of Vulnerability
- Severity
- Tools Used
- Steps to Reproduce
- Impact
- Recommendation with Reference


It’s just the beginning