

ବୁଟ

BUNTY



tips

resented by ROOTBAKAR



<https://www.linkedin.com/in/r-talaohu-rootbakar-85831510a/>



<https://www.instagram.com/talaohu28/>



<https://github.com/rootbakar>



<https://www.youtube.com/channel/UC0Bx8KptT0TGAtJePOmdD7w>



@rootbakar











<https://progress28.com>

```
root@linux: ~ whoami  
R. TALAOHU
```

```
root@linux: ~ id  
ROOTBAKAR
```

# OUTLINE

-  BUG BOUNTY
-  BUG HUNTER
-  PLATFORM
-  TOOLS
-  STEP BY STEP
-  BENEFIT
-  TIPS & TRICK
-  PORTOFOLIO



# BUG BOUNTY

BUG



BUG

BUG

BUG



MONEY



CERTIFICATE



REPUTATION



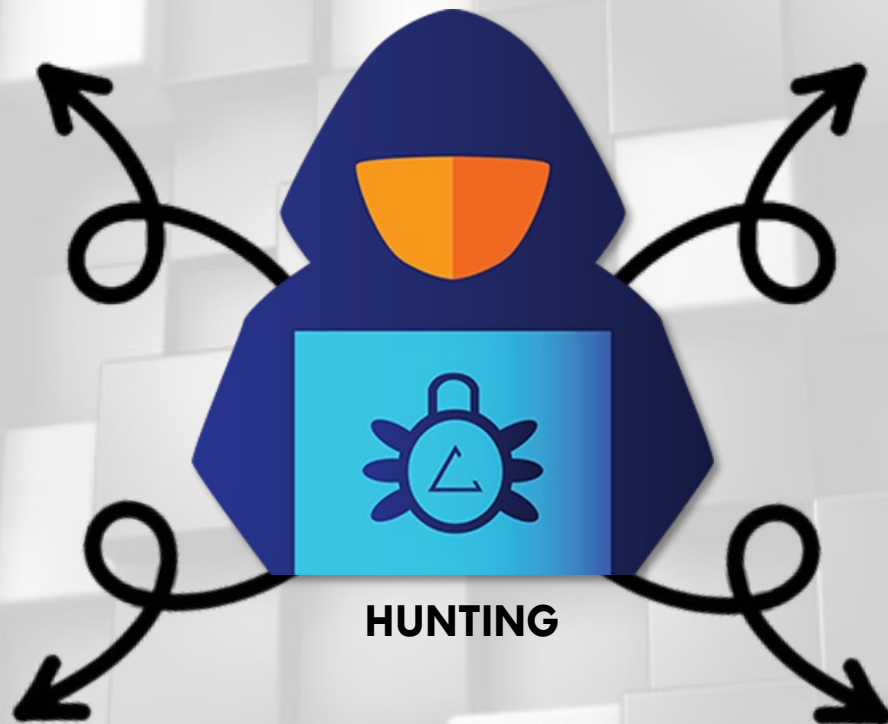
# BUG HUNTER



XSS



ATO



HUNTING



SQL



RCE



# PLATFORM



hackerone

bugcrowd



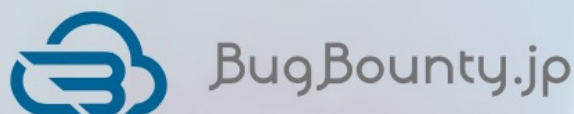
WhiteHub

YES WE H/CK

zerocopter



SecureBus



# TOOLS

## PROXY



Burp Suite Community Edition v1.7.34 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment
http://localhost	GET	/bWAPP/csrf_2.php		200	13665	HTML	bWAPP - CSRF	
http://localhost	GET	/bWAPP/csrf_2.php?...	✓	200	13668	HTML	bWAPP - CSRF	
http://localhost	GET	/bWAPP/csrf_2.php?...	✓	200	13665	HTML	bWAPP - CSRF	
http://localhost	GET	/bWAPP/js/html5.js		200	2684	script		
http://localhost	GET	/bWAPP/login.php		200	4321	HTML	bWAPP - Login	
http://localhost	GET	/bWAPP/portal.php		200	23676	HTML	bWAPP - Portal	
http://localhost	GET	/bWAPP/reset.php		200	13598	HTML	bWAPP - Reset	
http://localhost	GET	/bWAPP/sqli_7.php		200	13553	HTML	bWAPP - SQL Injection	
http://localhost	POST	/bWAPP/sqli_7.php	✓	200	13847	HTML	bWAPP - SQL Injection	
http://localhost	POST	/bWAPP/sqli_7.php	✓	200	13814	HTML	bWAPP - SQL Injection	

Request Response

Raw Params Headers Hex

GET /bWAPP/login.php HTTP/1.1  
Host: localhost  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:60.0) Gecko/20100101 Firefox/60.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-GB,en;q=0.5  
Accept-Encoding: gzip, deflate  
Cookie: security\_level=0; PHPSESSID=i6q80lthkjc13l1dn13743n3q7  
Connection: close  
Upgrade-Insecure-Requests: 1

? < + > Type a search term 0 matches

## BURP SUITE

# SUBDOMAIN



```

SUBLIST3R
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for yahoo.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..

```

SUBLIST3R

```

[17] 4.1
[<knockpy>]

+ checking for virustotal subdomains: YES
[
  "a.ns.hackerone.com",
  "b.ns.hackerone.com",
  "api.hackerone.com",
  "links.hackerone.com",
  "support.hackerone.com",
  "info.hackerone.com",
  "www.hackerone.com"
]
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scanning for subdomain...

```

KNOCKPY



DNSDUMPSTER



SUDOMY



# OSINT



SHODAN



CRT.SH



**Censys**

CENSYS



**VirusTotal**

VIRUS TOTAL



ZOOMEYE



# PARAMETER



```
  _  
 /-| -'  
( |-|/ /(/) v2.1.41  
  _/  
  _/
```

No target(s) specified

**ARJUN**

```
  _  
 /-| -'  
( |-|/ /(/) v1.2.0-git  
  _/  
  _/
```

v1.2.0-git

**FFUF**

# PORT



```
(kali@kali)-[/var/log/apache2]
$ nmap localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-26 17:37 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00032s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

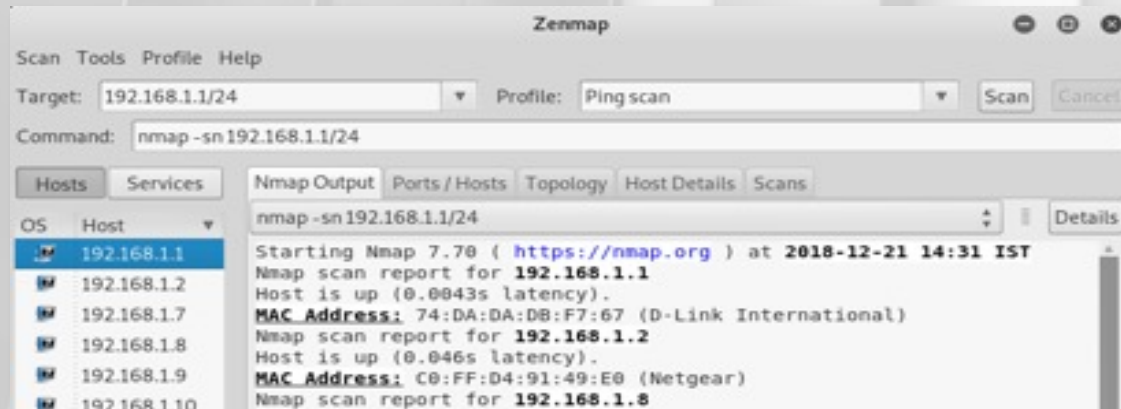
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

## NMAP

# RUSTSCAN

THE MODERN PORT SCANNER

## RUSTSCAN



## ZENMAP

```
root@b6x:~# naabu -host hackerone.com

      _ _ _ _ _
     / /   / /   / /   / /   / /   / /   / /   / /   / /   / /
    / /   / /   / /   / /   / /   / /   / /   / /   / /   / /
   / /   / /   / /   / /   / /   / /   / /   / /   / /   / /
  / /   / /   / /   / /   / /   / /   / /   / /   / /   / /
 / /   / /   / /   / /   / /   / /   / /   / /   / /   / /
/ /   / /   / /   / /   / /   / /   / /   / /   / /   / /
v1

projectdiscovery.io

[WARN] Use with caution. You are responsible for your actions
[WARN] Developers assume no liability and are not responsible for any misuse or damage.
[INF] Resolved domain hackerone.com to 104.16.100.52 for enumeration
[INF] Starting scan on host hackerone.com (104.16.100.52)
[INF] Found 4 ports on host hackerone.com (104.16.100.52) with latency 22.847935ms
hackerone.com:80
hackerone.com:443
hackerone.com:8080
hackerone.com:8443
```

## NAABU



**DORKING**



"p1.hol.es" DB\_PASSWORD



**GITHUB**

## Google Hacking Database

Filters

Reset All

Show 15

Quick Search

wordpress config

Date Added Dork

Category

Author

2019-05-06

intext:"the WordPress" inurl:wp-config ext:txt

Files Containing Juicy Info

Isaiah Puzon

**GHDB**



intext:"the WordPress" inurl:wp-config ext:txt



All



Videos



Images



News



Shopping



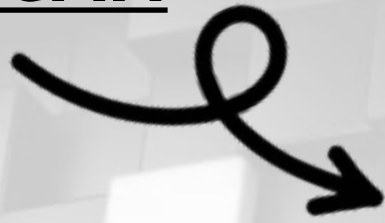
More

Tools

**GOOGLE DORK**



# VULN SCAN



**OWASP**  
Zed Attack Proxy



**acunetix**



**Nessus**  
vulnerability scanner

**netsparker**<sup>®</sup>  
web application security scanner

**Burp Suite**

for Web Application Security

**Nikto**

a Practical Website Vulnerability Scanner



**UNISCAN**

EXPLOIT

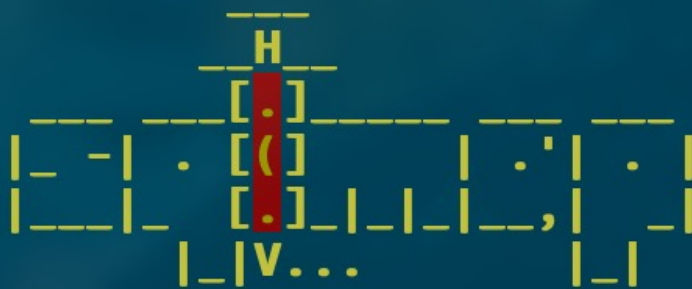


**EXPLOIT DATABASE**

WordPress Plugin IMDb Profile Widget 1.0.8 - Local File Inclusion

<b>EDB-ID:</b> 39621	<b>CVE:</b> N/A	<b>Author:</b> CRASHBANDICOT	<b>Type:</b> WEBAPPS	<b>Platform:</b> PHP	<b>Date:</b> 2016-03-27
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / 📄		<b>Vulnerable App:</b> 🇨🇭	

**EXPLOIT DB**



**{1.5.10#stable}**

<https://sqlmap.org>

Usage: python3.10 sqlmap [options]

**SQLMAP**

**READ MORE :** <https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters>



# STEP BY STEP

TARGET



SCOPES



POLICY

# FIND BUGS



**PROGRAM  
FLOW**



**XSS, SQL,  
LFI, RCE**



**REQUEST  
RESPONSE**

**TRY  
PAYLOAD/EXPLOIT**

# **SUBMIT REPORT**



**DESCRIPTION OF BUG**



**HOW TO REPRODUCE**



**IMPACT OF BUG**



**REMEDIATION**

**READ MORE :** <https://medium.com/@YoKoKho/tips-menulis-laporan-kerentanan-3deaeaf29a7d>



**SEND & REWARD**



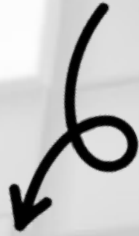
**VIA PLATFORM OR IT SUPPORT EMAIL**



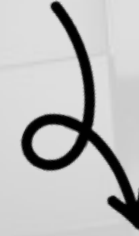
**MONEY, BTC, CERTIFICATE, SWAG, ETC**

# BENEFIT

## CERTIFICATE



## OPPORTUNITIES



[REDACTED] • 11:13 AM

btw mas. selagi nunggu hasil verifikasi laporannya  
apakah mas open for permanent work?

kami ada open position di red team



[REDACTED] • 10:43 AM

selamat pagi mas, saya [REDACTED] reporter dari  
[REDACTED], saya ingin mewawancarai mas terkait  
dengan bug hunter, apakah berkenan mas?

# NETWORK



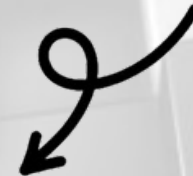
	mrdoel
	akun1337
	xASx
	batutahibnu17
	owlsec
	rootbakar
	zetc0de



	Mastur
	zetcode
	Private account
	rivi
	rifki alfaridzi
	Caesar Evan Santoso
	rootbakar
	Private account
	Danang TA



# REWARD



Bounties earned
\$380
Bounties earned
\$300
Bounties earned
\$100
Bounties earned
\$2k
Bounties earned
\$500

**Remitted payments (\$3,860.00)**

**Rp30.500.000**  
Total rewarded

€ 65,00 (Bonus)
€ 250,00 (Bonus)
€ 250,00 (Bonus)

# TIPS & TRICK

## BYPASS IDOR PROTECTION (1)



TRY TO CHANGE API VERSION



BEFORE



AFTER

READ MORE :

<https://progress28.com/2021/01/05/tips-p1-bypass-idor-protection/>



# BYPASS IDOR PROTECTION (2)



TRY TO DUPLICATE POST PARAMETER



**BEFORE**



**AFTER**

**READ MORE :**

<https://progress28.com/2020/12/25/tips-bypass-insecure-direct-object-reference-idor-protection/>



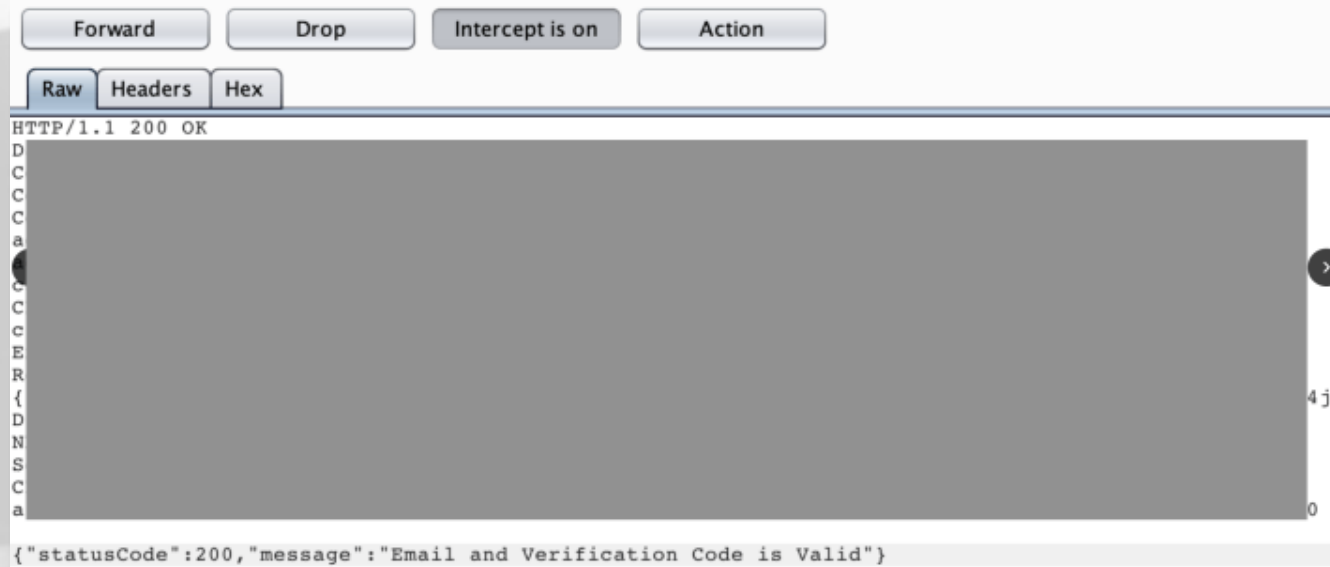
# BYPASS CODE VERIFICATION (BYPASSED SYSTEM)



TRY TO CHANGE RESPONSE (STATUS CODE)



**BEFORE**



**AFTER**

**READ MORE :**

<https://progress28.com/2021/07/14/tips-p2-bypass-code-verification-bypassed-system/>

# BYPASS FIX OPEN REDIRECT



TRY TO ADD (@) AFTER (@)

*REQUEST (GET)*

*<https://redected.com@evilzone.org>*

**BEFORE**

**READ MORE :**

<https://progress28.com/2020/09/28/tips-bypass-fix-open-redirect/>

*REQUEST (GET)*

*<https://redected.com@@evilzone.org>*

**AFTER**

# XSS VIA INSPECT ELEMENT



TRY TO ADD XSS PAYLOAD  
VIA INSPECT ELEMENT



**AFTER**

```
<label class="text-bold" for="input-detail-question" data-v-9b657988="">Data
</label>
<p class="font-14" data-v-9b657988="">...</p>
<section class="container-quill" data-v-9b657988="">
  <div class="quill-editor" data-v-9b657988="">
    <div class="ql-toolbar ql-snow">...</div>
    <div class="ql-container ql-snow" style="position: relative;">
      <div class="ql-editor" data-gramm="false" data-placeholder="
        contenteditable="true"> event
      <p>rootbakar</p>
    </div>
    <div class="ql-clipboard" tabindex="-1" contenteditable="true"></div>
    <div class="ql-tooltip ql-hidden">...</div>
  </div>
</section>
<!-->

<div class="ql-container ql-snow" style="position: relative;">
  <div class="ql-editor" data-gramm="false" data-placeholder="
    contenteditable="true"> event
  <p><iframe src=javascript:alert(document.domain)></iframe></p>
</div>
```

**BEFORE**

**READ MORE :**

<https://progress28.com/2020/09/27/tips-xss-via-inspect-element/>

# FIND ORIGIN IP VIA SHODAN OR CENSYS



TRY TO FIND ORIGIN IP FOR BYPASS WAF  
`Ssl.cert.subject.CN:"example.tld" 200`

**SSL Certificate**

Issued By:  
|- Common Name:  
**Sectigo RSA Domain Validation Secure Server CA**

Issued To:  
|- Common Name:  
**example.tld**

Supported SSL Versions:  
**TLSv1, TLSv1.1, TLSv1.2**

HTTP/1.1 **200** OK

**BEFORE**

```
Target: https://[redacted]
[00:09:10] Starting:
[00:09:38] 200 - 53B - [redacted]
[00:09:38] 200 - 147B - [redacted]
[00:09:46] 200 - 10MB - [redacted]
[00:09:49] 502 - 584B - [redacted]
[00:09:49] 502 - 584B - [redacted]
[00:09:49] 502 - 584B - [redacted]
[00:09:49] 502 - 584B - [redacted]
[00:09:55] 200 - 1KB - [redacted]
[00:10:13] 400 - 2KB - [redacted]
```

**AFTER**

```
// Your web app's Firebase configuration
```

**READ MORE :**

<http://www.firstsight.me/2022/03/from-recon-via-censys-and-dnsdumpster-to-getting-p1-by-login-using-weak-password-password/>

# OTHER REFERENCE

<https://pentester.land/list-of-bug-bounty-writeups.html>

<https://bugreader.com/reports>

<https://infosecwriteups.com>

<https://medium.com/techiepedia/tagged/bug-bounty-tips>

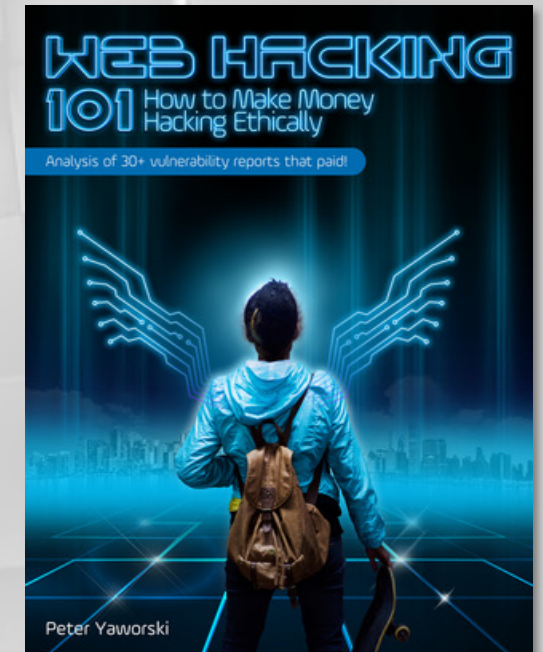
<https://github.com/KingOfBugbounty/KingOfBugBountyTips>

<https://github.com/topics/bugbountytips>

<https://www.computerfutures.com/en-jp/blog/2020/12/all-you-need-to-know-about-bug-bounty-hunting/>

<https://book.hacktricks.xyz>

<http://index-of.es>





# PORTOFOLIO

Massdrop

Google

facebook

GoPro



GITLAB

  
Alibaba Group

SONY

edmodo

DISQUS



▲ ZEIT

▲ Vercel

 Apple

Paysafe

IKEA



shopify



Telkomsel



tokopedia

traveloka



ADIRA  
FINANCE



BPJS Kesehatan  
Badan Penyelenggara Jaminan Sosial

# ACHIEVEMENTS



**BONUS**



**<https://progress28.com/2022/03/17/apple-bug-bounty-how-i-got-6000-from-apple-security-bounty/>**



pass: wimi-sec





SETIAP ORANG PUNYA JATAH GAGAL.

**HABISKAN  
JATAH GAGALMU**

KETIKA KAMU MASIH MUDA.

**-DAHLAN ISKAN-**

The background of the image is a dense, textured surface composed of numerous dark blue, three-dimensional cubes. These cubes are arranged in a somewhat irregular, staggered pattern, creating a sense of depth and movement. The lighting is soft, highlighting the edges of the cubes and giving them a matte, slightly reflective appearance. The overall color palette is monochromatic, consisting of various shades of dark blue and black.

# TERIMA KASIH

best regards ROOTBAKAR