SLIIT

Discover Your Future

Systems and Network Programming - IE2012

YEAR 2 , SEMESTER 1

Bug Bounty Program

IT22315496

Chamod Anuradha

1. Contents

Abstract

In a crowdsourced method to security testing known as "bug bounty programmes," companies pay security researchers for finding and disclosing flaws in their systems. Since bug bounty programmes have shown to be a successful means of identifying and addressing security flaws before attackers can take advantage of them, their popularity has grown in recent years.

The creation and execution of a bug bounty programme for a business using the HackerOne platform are covered in this paper. An overview of bug bounty programmes and their advantages for both organizations and security researchers is provided at the beginning of the study. The design of the company's bug bounty programme is then covered in the report, along with its scope, categories of vulnerabilities that qualify for payouts, and available prize amounts. The paper also outlines the protocols for paying security researchers rewards and for filing and reviewing bug reports.

The outcomes of the company's bug bounty programme up to this point are discussed in the report's conclusion. The report demonstrates that many high-severity vulnerabilities have been successfully found and fixed by the programme. The study also demonstrates that security experts have praised the programme and that it has contributed to the systems' increased security.

Bug Bounty Program

What is bug bounty?

A bug bounty is a monetary reward given to ethical hackers for successfully discovering and reporting a vulnerability or bug to the application's developer. Bug bounty programs allow companies to leverage the hacker community to improve their systems' security posture over time continuously. [1]

What are the bug bounty platforms?

- HackerOne
- Bugcrowd
- Synack
- YesWeHack
- HackenProof
- SafeHats
- Intigrity

Bug bounty tools

- Nmap
- Burp Suite
- Shodan
- Metapolish
- WPscan
- Nikto

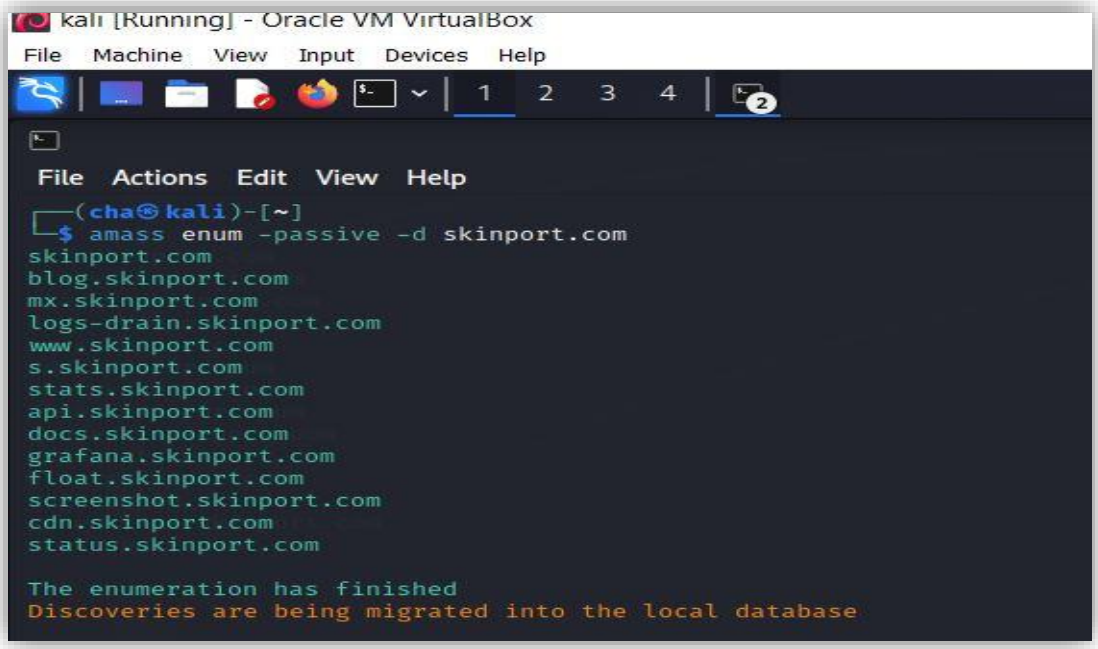
Bug hunting 01

Web site (Main)	https://skinport.com/
Hackerone URL	https://hackerone.com/skinport?type=team
IP Address	104.18.16.19
Attack Domain	skinport.com

Subdomain list:

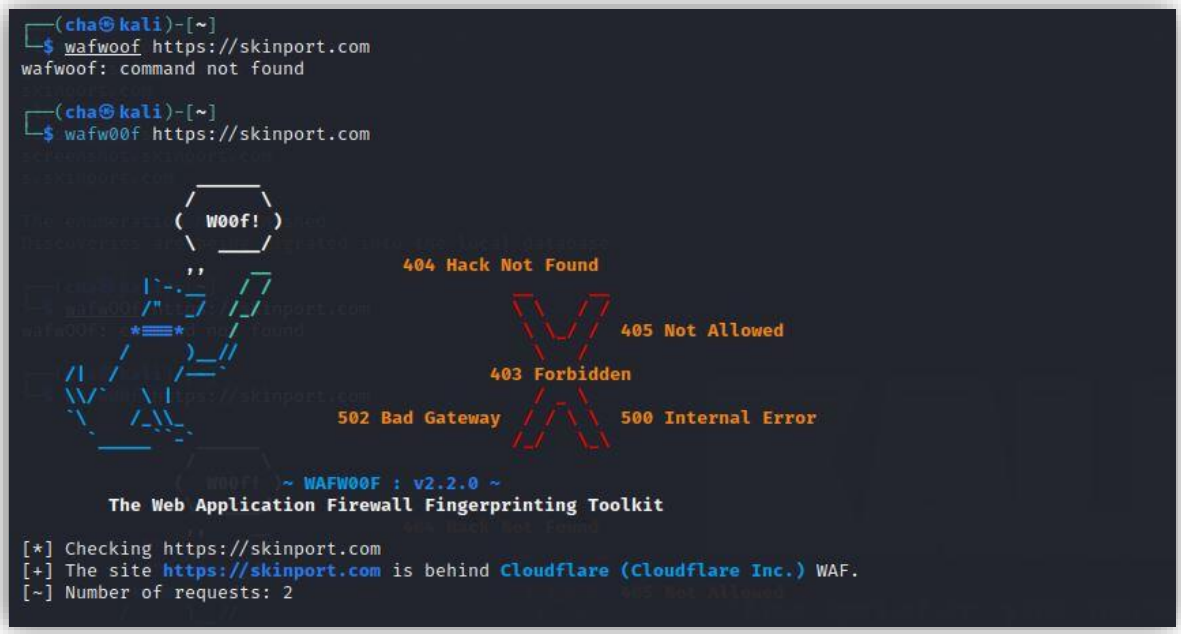
Used tool with command: amass enum -passive -d skinport.com

- stats.skinport.com
- mx.skinport.com
- cdn.skinport.com
- s.skinport.com
- blog.skinport.com
- status.skinport.com
- screenshot.skinport.com
- grafana.skinport.com
- api.skinport.com
- skinport.com
- float.skinport.com
- www.skinport.com
- logs-drain.skinport.com
- docs.skinport.com



Firewall Detection:

Used tool with command: wafw00f https://skinport.com

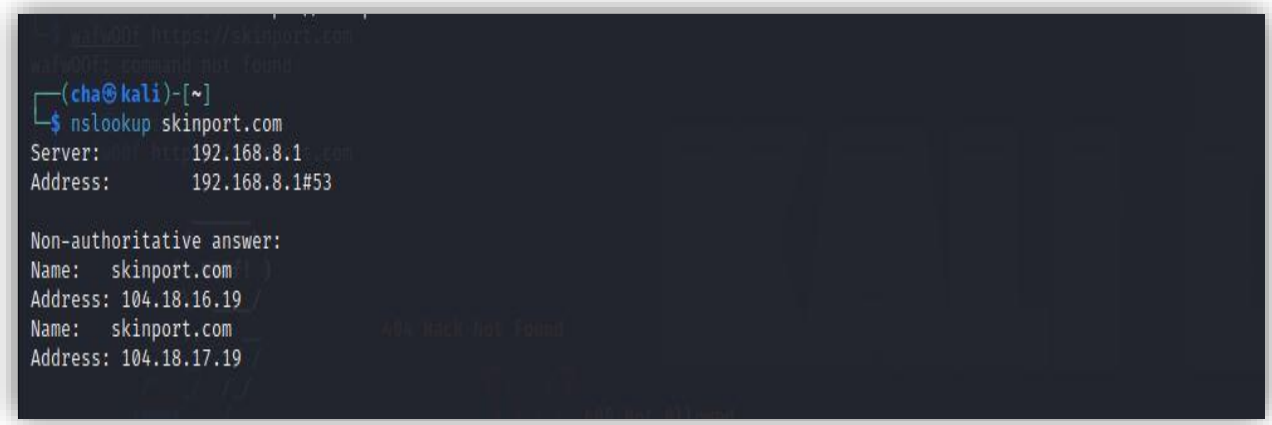


Getting information from DNS server

Used tool with command: nslookup https://skinport.com

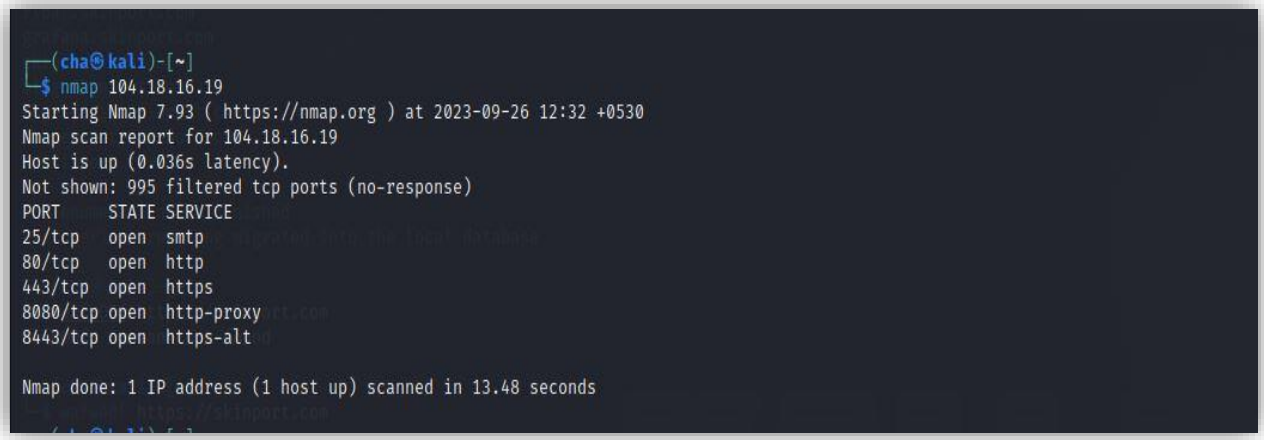
Getting information from IP Address

Used tool with command: nslookup skinport.com

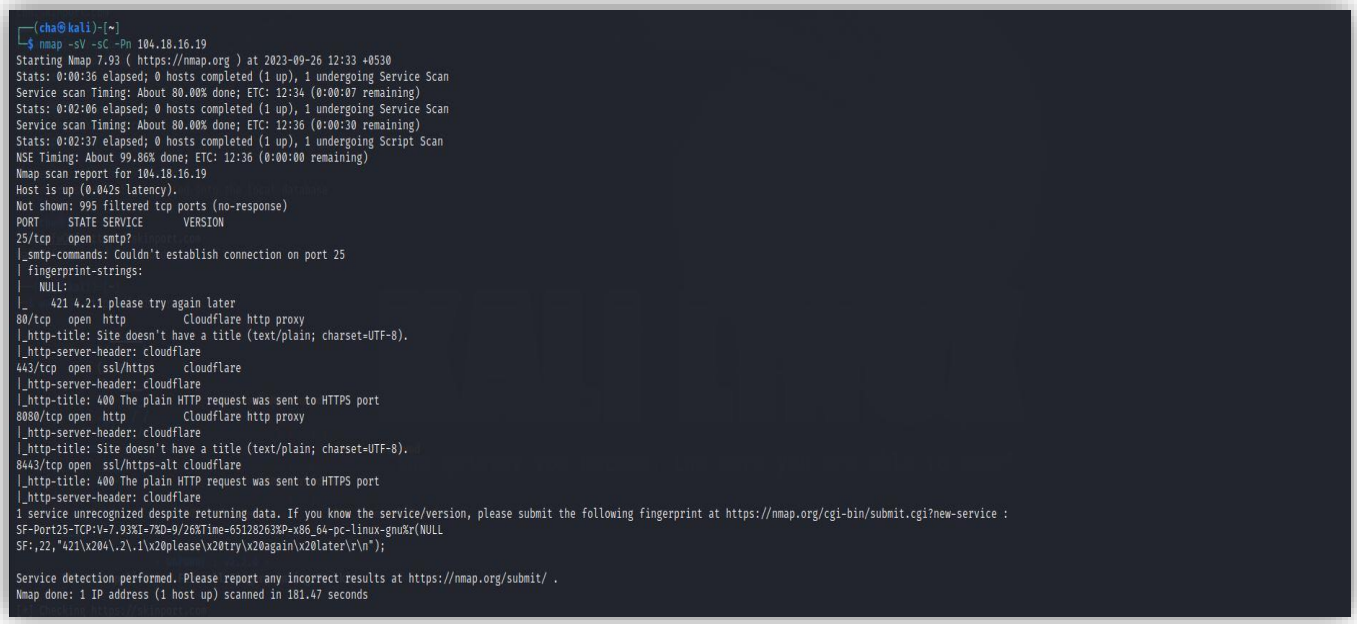


Port Scanning:

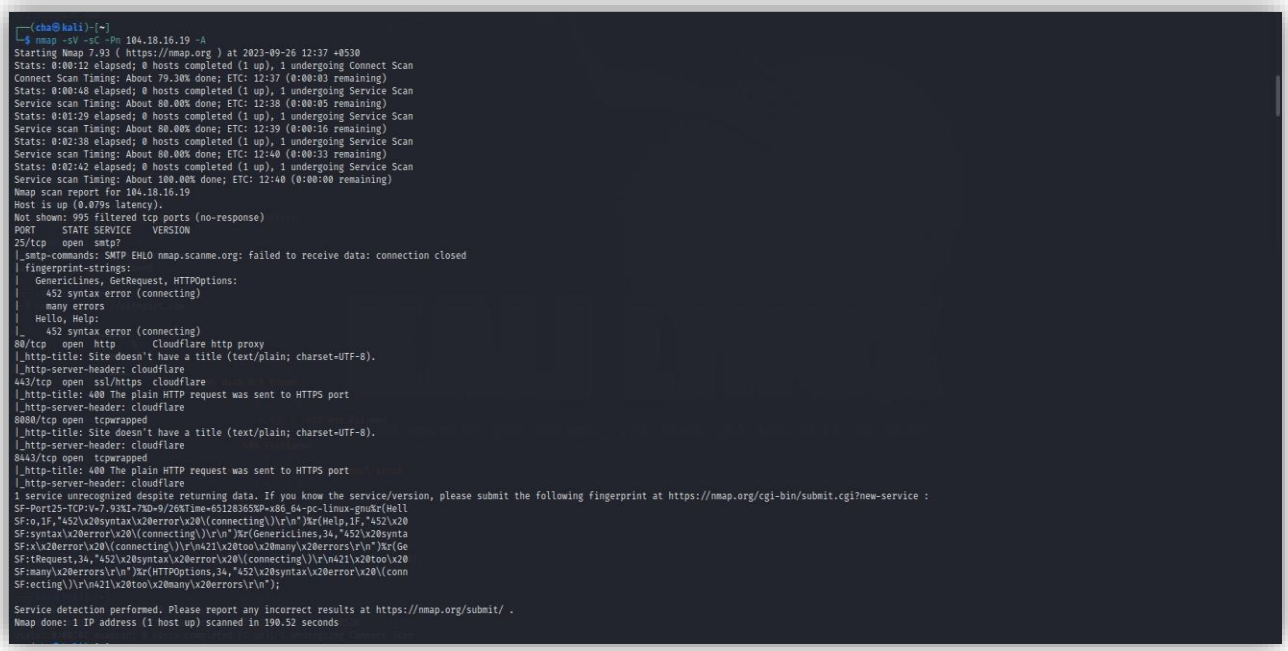
Used tool with command: nmap 104.18.16.19



Used tool with command: nmap -sV -sC -Pn 104.18.16.19

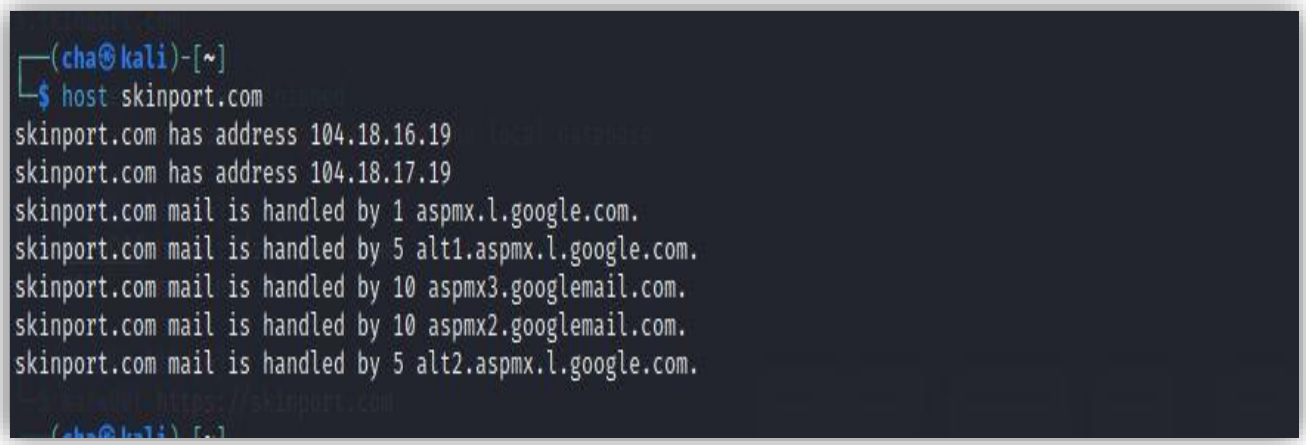


Used tool with command: nmap -sV -sC -Pn 104.18.16.19 -A



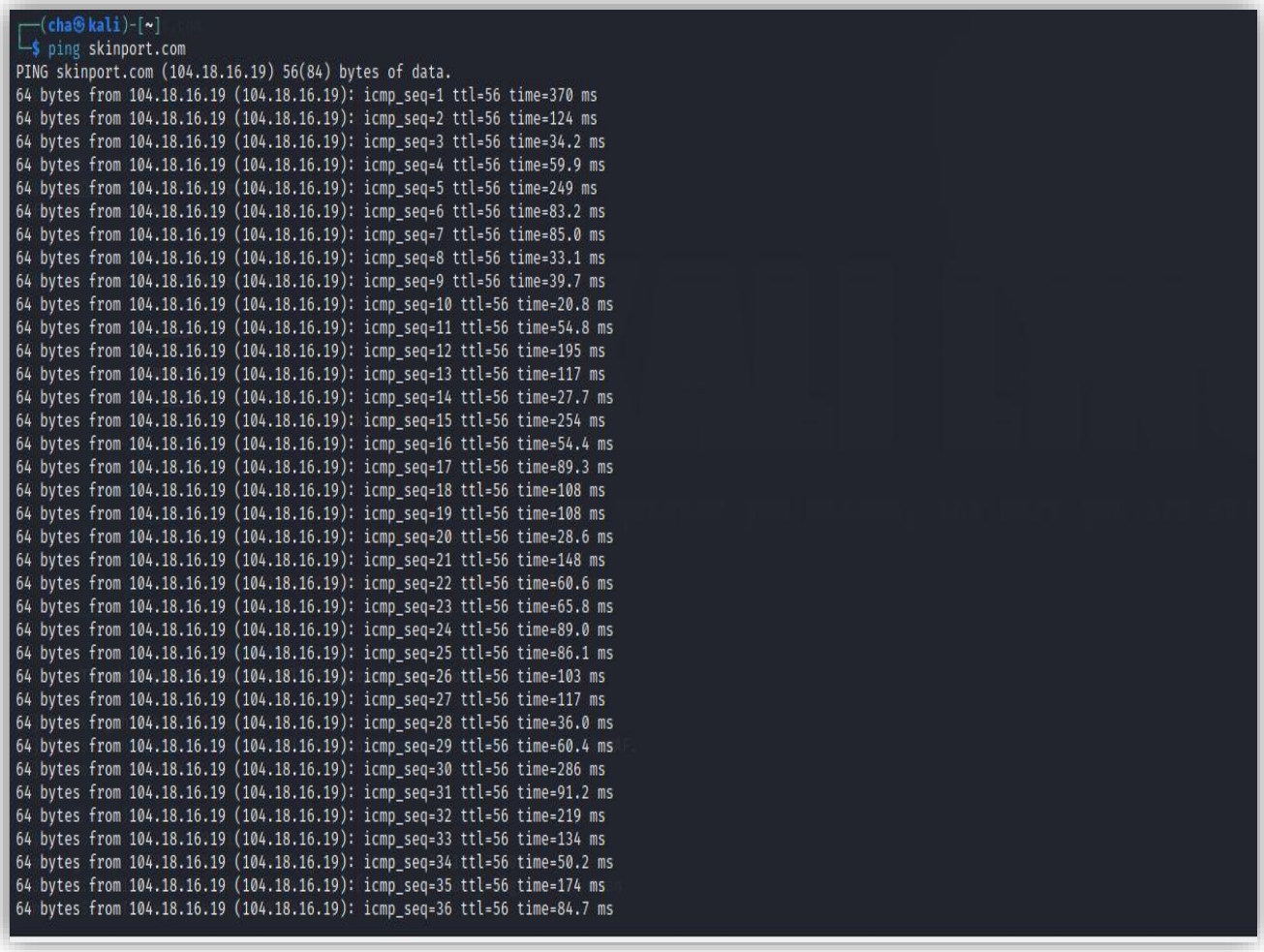
Host Scanning:

Used tool with command: host skinport.com



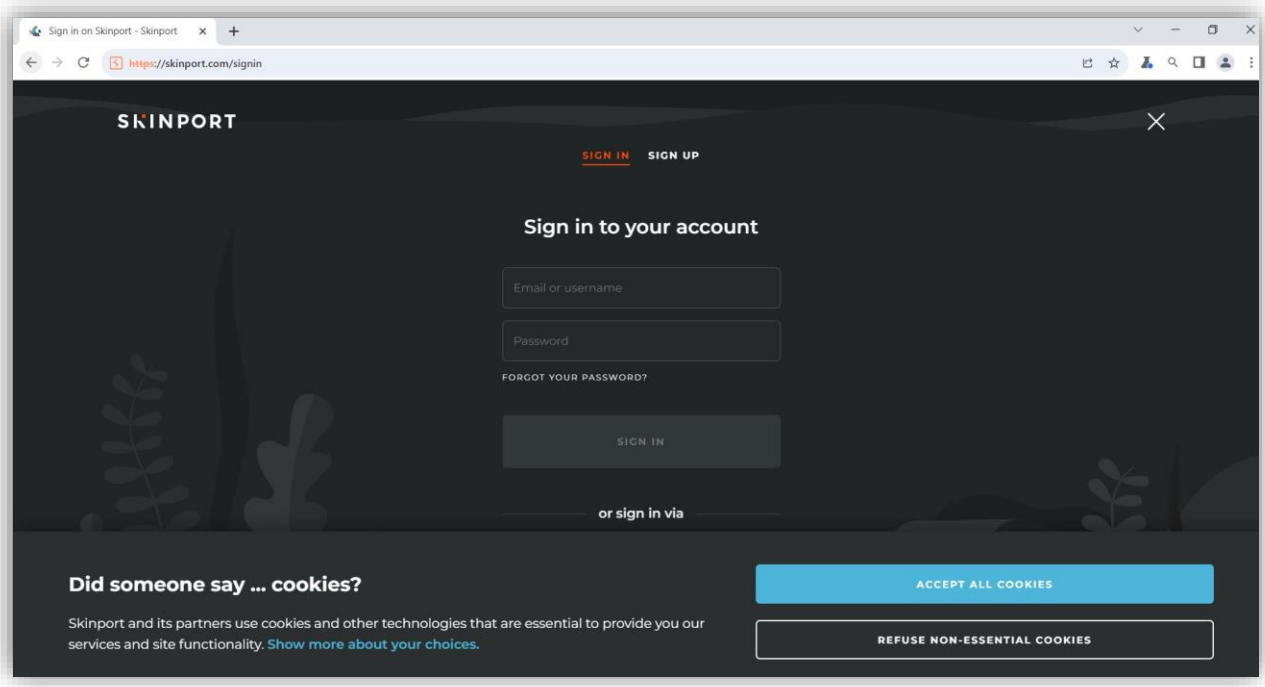
Ping :

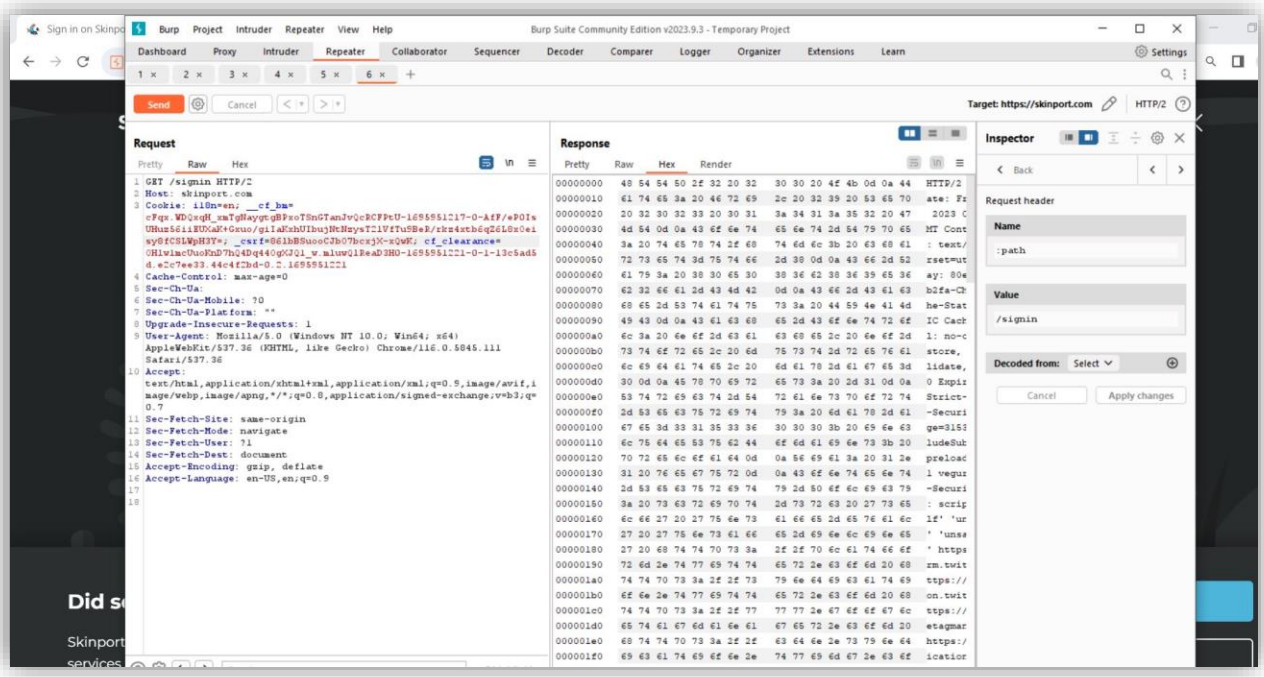
Used tool with command: ping skinport.com

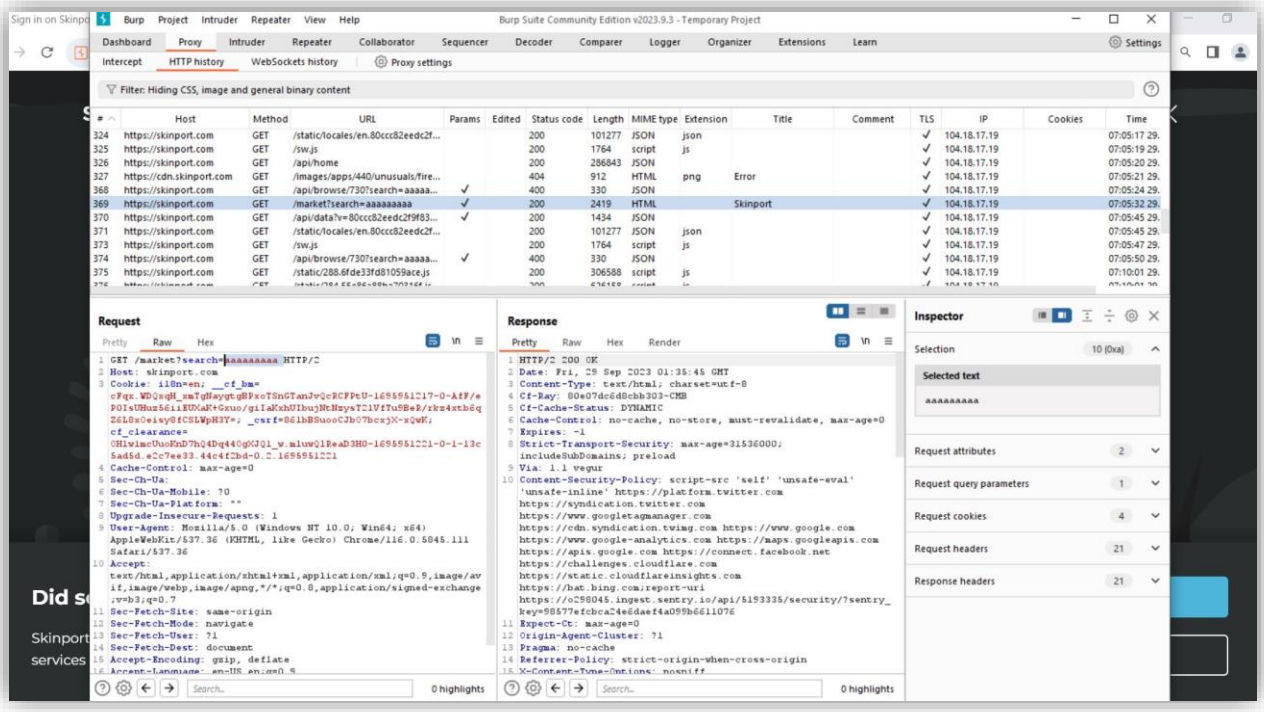


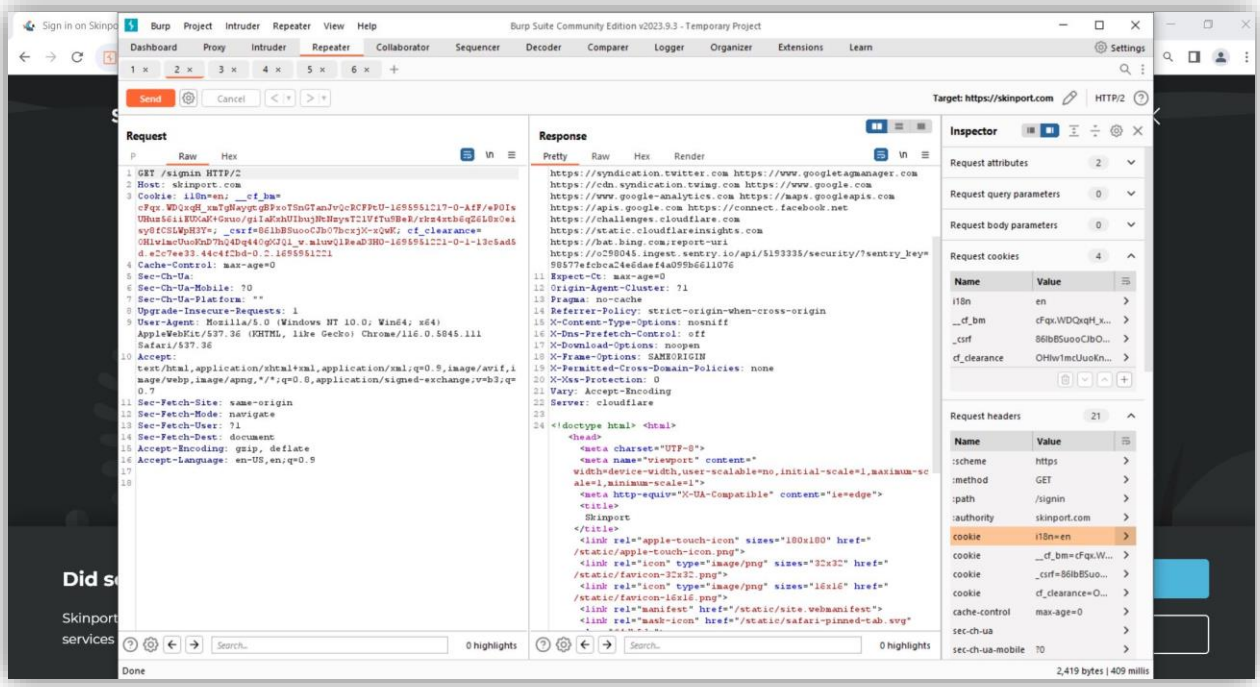
Proof of concept

Used burp suite professional






Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
Request
Response
Inspector
GET /market?search=aaaaaaaaa HTTP/2
HTTP/2 200 OK
Selection
Selected text
aaaaaaaaa
Request attributes
Request query parameters
Request cookies
Request headers
Response headers
0 highlights


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Send Cancel
Target: https://skinport.com HTTP/2
Request
Response
Inspector
GET /signin HTTP/2
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Done
2,419 bytes | 409 millis

Vulnerability

02. Vulnerability title	Admin page disclosure
03. Vulnerability description	Admin page revelation is when a management or back-end page of a website or web app is accidentally shown to the public. An admin page is usually a private place that can only be viewed by people who are allowed to run and handle the website or app. When the admin panel is revealed, people who shouldn't have permission to view it find out the URL or address of the admin page. This can happen for a number of reasons, such as the server settings not being set up correctly, weak access controls, bad handling of user input, or holes in the website's code. In this web site**, I have found a backend admin panel** which contain backend of the system. So, admin page disclosure is vulnerable to the web site individual data against protection.
04. Affected components.	Web site User Data, Web Server
05. Affected URL's	https://judge.me/admin.php https://judge.me/admin.cgi https://judge.me/admin.pl

Bug hunting 02

Web site (Main)	https://judge.me/
Hackerone URL	https://hackerone.com/judgeme?type=team
IP Address	52.20.78.240
Attack Domain	judge.me

Subdomain list:

Used tool with command: amass enum -passive -d judge.me

- https://judgeme.freshdesk.com
- https://blog.judge.me/
- https://support.judge.me/
- https://careers.judge.me/jobs
- https://status.judge.me/
- https://judgeme-pentest.myshopify.com/products/pentest
- https://judgeme-pentest.myshopify.com/
- cache.judge.me
- safeframe.judge.me
- core.judge.me
- chat.api.judge.me
- us.u.judge.me
- feedback.judge.me
- nuid.judge.me
- shopify.judge.me
- cdn-3.judge.me
- testcdn.judge.me
- tdum.judge.me
- shopifycdn.judge.me
- demo-store.judge.me
- i.judge.me
- mycars.judge.me
- k12.judge.me
- woocommerce-adapter.judge.me
- l.judge.me
- static.pub.judge.me

- fls.judge.me
- support.judge.me
- bigcommerce-adapter.judge.me
- judge.me
- cdn.judge.me
- blob.core.judge.me
- n.judge.me
- events.judge.me
- blog.judge.me
- pub.judge.me
- pub-images.judge.me
- s3.judge.me
- files.judge.me
- mail.judge.me
- sync.judge.me
- shopbasecdn.judge.me
- careers.judge.me
- u.judge.me
- shop.judge.me
- global.judge.me
- cdn1.judge.me
- shopbase.judge.me
- status.judge.me
- checkout.judge.me
- squarespacecdn.judge.me
- help.judge.me
- sites.judge.me
- s.judge.me
- images.judge.me
- api.judge.me
- en.judge.me
- www.judge.me
- assets.judge.me
- metric.judge.me

```
┌──(cha㉿kali)-[~]
└─$ amass enum -passive -d judge.me
cache.judge.me
safeframe.judge.me
core.judge.me
chat.api.judge.me
us.u.judge.me
feedback.judge.me
nuid.judge.me
shopify.judge.me
cdn-3.judge.me
testcdn.judge.me
tdum.judge.me
shopifycdn.judge.me
demo-store.judge.me
i.judge.me
mycars.judge.me
k12.judge.me
woocommerce-adapter.judge.me
l.judge.me
static.pub.judge.me
fls.judge.me
support.judge.me
bigcommerce-adapter.judge.me
judge.me
cdn.judge.me
blob.core.judge.me
n.judge.me
events.judge.me
blog.judge.me
pub.judge.me
pub-images.judge.me
s3.judge.me
files.judge.me
mail.judge.me
sync.judge.me
shopbasecdn.judge.me
careers.judge.me
u.judge.me
shop.judge.me
global.judge.me
cdn1.judge.me
shopbase.judge.me
status.judge.me
checkout.judge.me
squarespacecdn.judge.me
help.judge.me
sites.judge.me
s.judge.me
images.judge.me
```



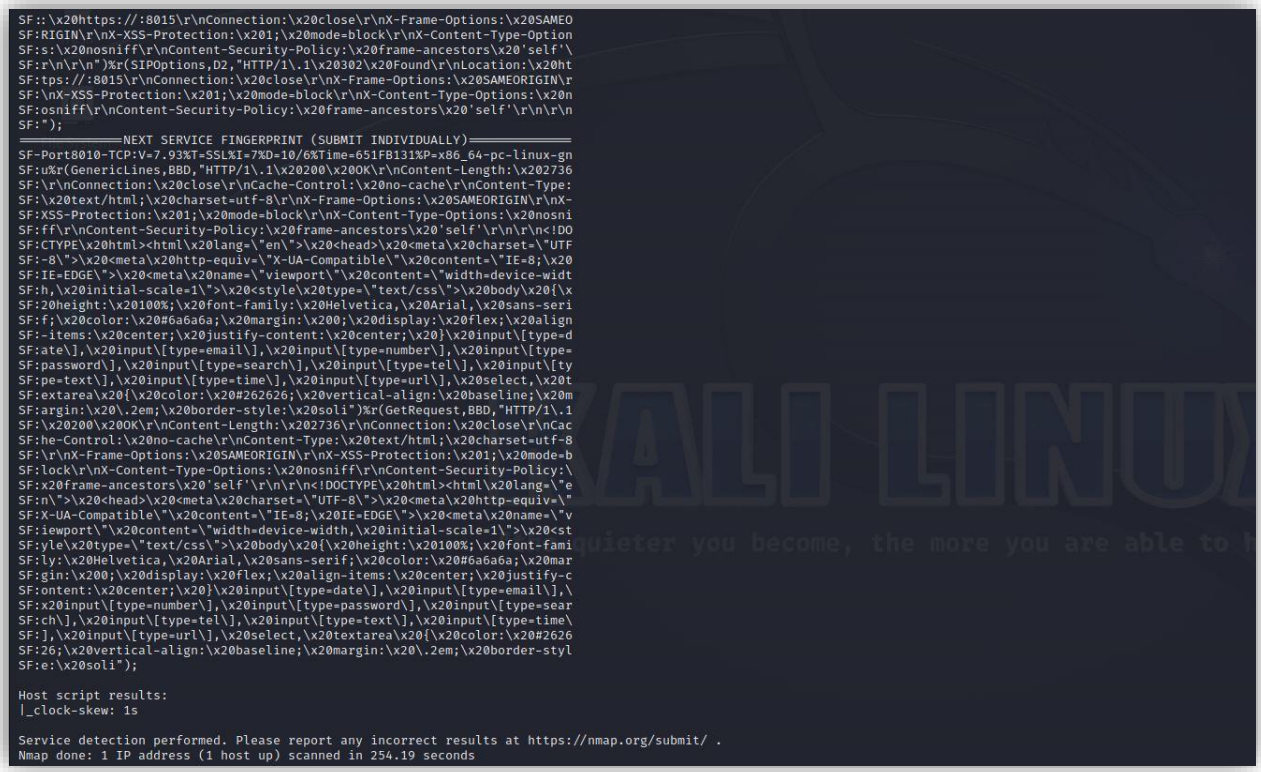
```
demo-store.judge.me
i.judge.me
mycars.judge.me
k12.judge.me
woocommerce-adapter.judge.me
l.judge.me
static.pub.judge.me
fls.judge.me
support.judge.me
bigcommerce-adapter.judge.me
judge.me
cdn.judge.me
blob.core.judge.me
n.judge.me
events.judge.me
blog.judge.me
pub.judge.me
pub-images.judge.me
s3.judge.me
files.judge.me
mail.judge.me
sync.judge.me
shopbasecdn.judge.me
careers.judge.me
u.judge.me
shop.judge.me
global.judge.me
cdn1.judge.me
shopbase.judge.me
status.judge.me
checkout.judge.me
squarespacecdn.judge.me
help.judge.me
sites.judge.me
s.judge.me
images.judge.me
api.judge.me
en.judge.me
www.judge.me
assets.judge.me
metric.judge.me

The enumeration has finished
Discoveries are being migrated into the local database
```

Firewall Detection:

Used tool with command: wafw00f https://judge.me/

Port Scanning: Required,

Used tool with command: nmap -sV -sC -Pn 52.20.78.240 -A



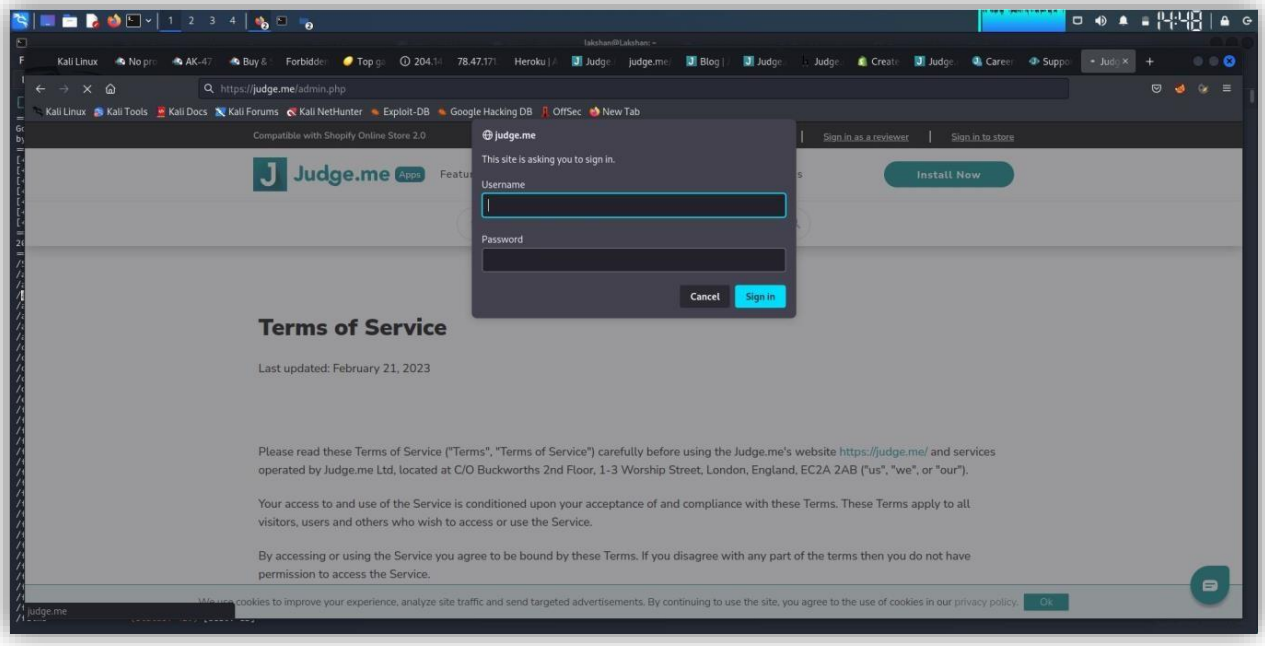
Directory Enumeration: Required,

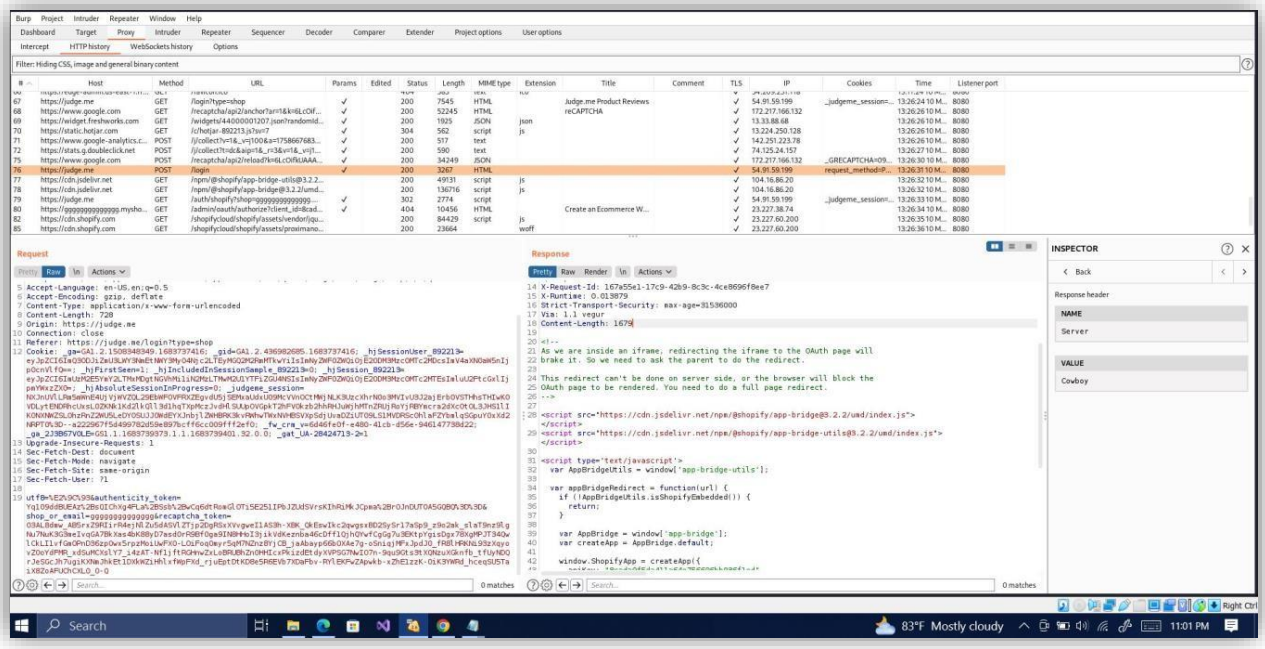
Used tool with command: gobuster dir -u https://judge.me -w /usr/share/wordlists/dirb/common.txt

```
┌──(cha㉿kali)-[~]
└─$ gobuster dir -u https://judge.me -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://judge.me
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about               (Status: 200) [Size: 39679]
/500                 (Status: 500) [Size: 15656]
/admin               (Status: 401) [Size: 27]
/admin.php           (Status: 401) [Size: 27]
/admin.pl            (Status: 401) [Size: 27]
/admin.cgi           (Status: 401) [Size: 27]
/api                 (Status: 301) [Size: 91] [--> https://judge.me/api/docs]
/apps                (Status: 200) [Size: 35775]
/be                  (Status: 429) [Size: 12]
/beheer              (Status: 429) [Size: 12]
/bdata               (Status: 429) [Size: 12]
/benutzer            (Status: 429) [Size: 12]
/best                (Status: 429) [Size: 12]
/bfc                 (Status: 429) [Size: 12]
/bg                  (Status: 429) [Size: 12]
/bigadmin            (Status: 429) [Size: 12]
/beta                (Status: 429) [Size: 12]
/bilder              (Status: 429) [Size: 12]
/bigip               (Status: 429) [Size: 12]
/big                 (Status: 429) [Size: 12]
/bill                (Status: 429) [Size: 12]
/billing             (Status: 429) [Size: 12]
/bin                 (Status: 429) [Size: 12]
/bio                 (Status: 429) [Size: 12]
/biz                 (Status: 429) [Size: 12]
/bitrix              (Status: 429) [Size: 12]
/bins                (Status: 429) [Size: 12]
/bios                (Status: 429) [Size: 12]
/binary              (Status: 429) [Size: 12]
/binaries            (Status: 429) [Size: 12]
/bk                  (Status: 429) [Size: 12]
/bkup                (Status: 429) [Size: 12]
/bl                  (Status: 429) [Size: 12]
/blank               (Status: 429) [Size: 12]
```

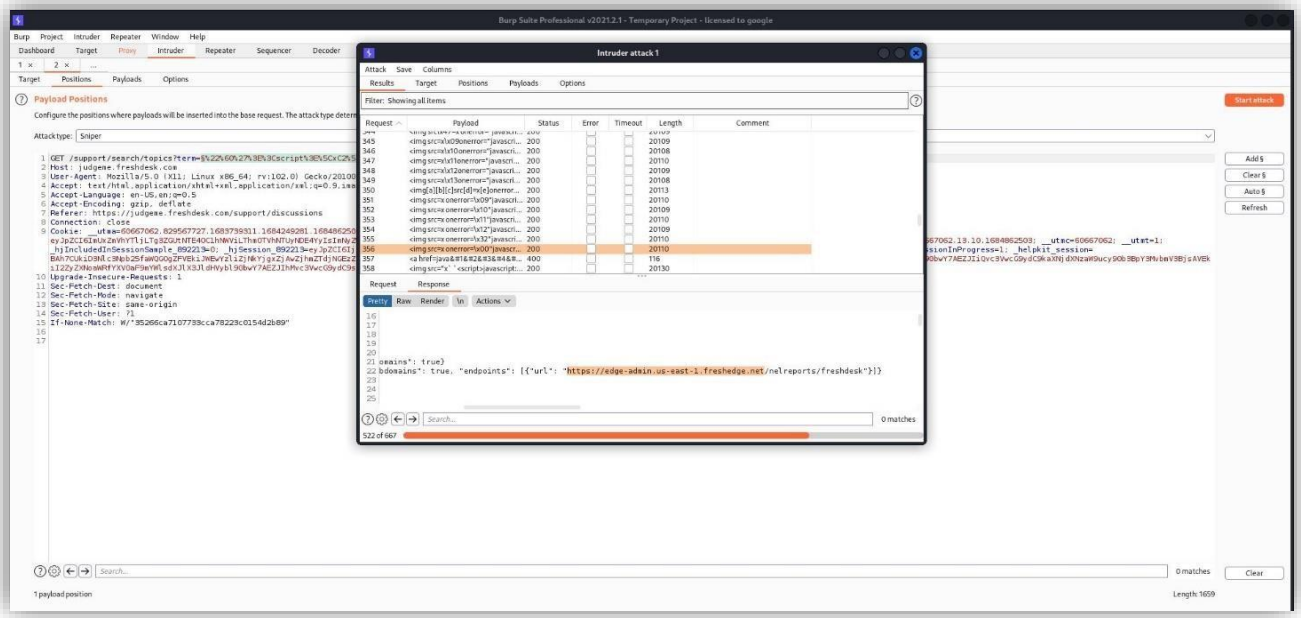
```
/personal            (Status: 429) [Size: 12]
/personals           (Status: 429) [Size: 12]
/pfx                 (Status: 429) [Size: 12]
/pg                  (Status: 429) [Size: 12]
/pgadmin             (Status: 429) [Size: 12]
/pgp                 (Status: 429) [Size: 12]
/pgsql               (Status: 429) [Size: 12]
/phf                 (Status: 429) [Size: 12]
/phishing            (Status: 429) [Size: 12]
/phone               (Status: 429) [Size: 12]
/phones              (Status: 429) [Size: 12]
/phorum              (Status: 429) [Size: 12]
/photo               (Status: 429) [Size: 12]
/photogallery        (Status: 429) [Size: 12]
/photodetails        (Status: 429) [Size: 12]
/pricing             (Status: 200) [Size: 136764]
/privacy             (Status: 200) [Size: 87748]
/products            (Status: 302) [Size: 98] [--> https://judge.me/login?type=shop]
/profile             (Status: 302) [Size: 88] [--> https://judge.me/login]
/questions           (Status: 302) [Size: 98] [--> https://judge.me/login?type=shop]
/reports             (Status: 302) [Size: 98] [--> https://judge.me/login?type=shop]
/reviews             (Status: 200) [Size: 6167]
/robots.txt          (Status: 200) [Size: 237]
/search              (Status: 200) [Size: 10423]
/Search              (Status: 429) [Size: 12]
/searchurl           (Status: 429) [Size: 12]
/search_result       (Status: 429) [Size: 12]
/sec                 (Status: 429) [Size: 12]
/search-results      (Status: 429) [Size: 12]
/searchnx            (Status: 429) [Size: 12]
/search_results      (Status: 429) [Size: 12]
/searchresults       (Status: 429) [Size: 12]
/seccode             (Status: 429) [Size: 12]
/second              (Status: 429) [Size: 12]
/secret              (Status: 429) [Size: 12]
/secrets             (Status: 429) [Size: 12]
/section             (Status: 429) [Size: 12]
/secure              (Status: 429) [Size: 12]
/sections            (Status: 429) [Size: 12]
/secure_login        (Status: 429) [Size: 12]
/secureauth          (Status: 429) [Size: 12]
```

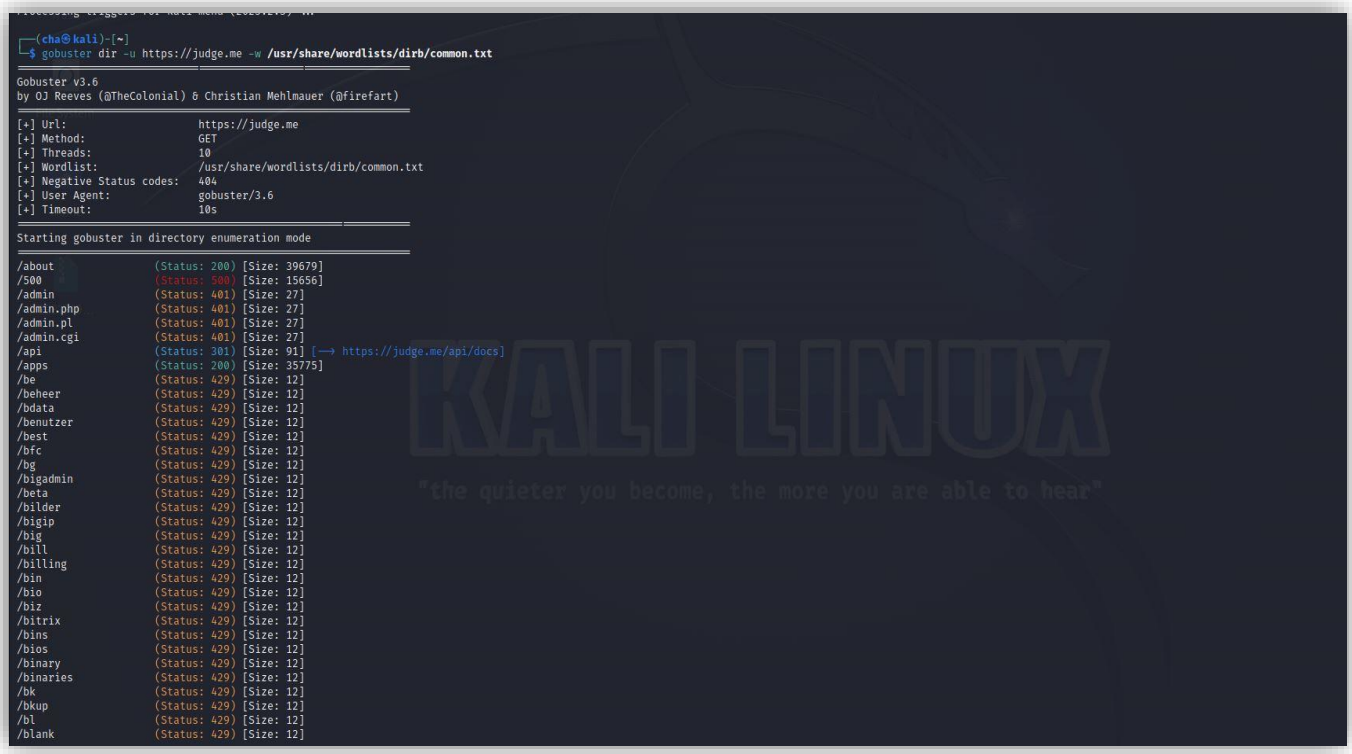
Proof of concept





Affected Endpoint





Vulnerability

02. Vulnerability title	Admin page disclosure
03. Vulnerability description	Admin page revelation is when a management or back-end page of a website or web app is accidentally shown to the public. An admin page is usually a private place that can only be viewed by people who are allowed to run and handle the website or app. When the admin panel is revealed, people who shouldn't have permission to view it find out the URL or address of the admin page. This can happen for a number of reasons, such as the server settings not being set up correctly, weak access controls, bad handling of user input, or holes in the website's code. In this web site**, I have found a backend admin panel** which contain backend of the system. So, admin page disclosure is vulnerable to the web site individual data against protection.
04. Affected components.	Web site User Data, Web Server
05. Affected URL's	https://judge.me/admin.php https://judge.me/admin.cgi https://judge.me/admin.pl

Conclusion

The firm has found success with the bug bounty programme, which has assisted in finding and fixing many high-severity vulnerabilities and enhancing the general security of the company's systems. Additionally, security experts have praised the programme and it has strengthened the bond between the organization and the security community.

The business is dedicated to keeping up the bug bounty programme and growing its future success. Additionally, the program's scope will be expanded by the corporation to include additional technologies and applications.

The business would like to express its gratitude to each and every security researcher that has taken part in the bug bounty programme so far. The increased security of the organisation is a result of your efforts.

References

[1] online - *What Are Bug Bounties? How Do They Work? [With Examples]*. (n.d.). HackerOne. https://www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples

- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Directory%20Traversal
- https://hackerone.com/skinport?type=team

https://hackerone.com/judgeme?type=team

https://www.foregenix.com/blog/the-potential-risks-of-exposed-admin-login-panels

https://kayran.io/blog/vulnerabilities/admin-panel-exposed

https://owasp.org/www-project-web-security-testing-guide/latest/4-

Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/05-Enumerate_Infrastructure_and_Application_Admin_Interfaces


THANK YOU!