



SLIIT

Discover Your Future

Systems and Network Programming - IE2012

YEAR 2 , SEMESTER 1

Bug Bounty Program

IT22315496

Chamod Anuradha

1. Contents

1. Abstract	3
2. Bug Bounty Program	4
2.1. What is bug bounty?	4
2.2. What are the bug bounty platforms?	5
2.3. Bug bounty tools	5
3. Bug hunting 01	6
3.1. Subdomain list:	7
3.2. Firewall Detection:	8
3.3. Getting information from DNS server	9
3.4. Getting information from IP Address	9
3.5. Port Scanning:	10
3.6. Host Scanning:	11
3.7. Ping :	12
3.8. Proof of concept	13
3.9. Vulnerability	15
4. Bug hunting 02	16
4.1. Subdomain list:	17
4.2. Firewall Detection:	20
4.3. Port Scanning: Required,	20
4.4. Directory Enumeration: Required,	21
4.5. Proof of concept	23
4.6. Vulnerability	25
5. Conclusion	26
6. References	27

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

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(ch@kali)-[~]
$ amass enum -passive -d skinport.com
skinport.com
blog.skinport.com
mx.skinport.com
logs-drain.skinport.com
www.skinport.com
s.skinport.com
stats.skinport.com
api.skinport.com
docs.skinport.com
grafana.skinport.com
float.skinport.com
screenshot.skinport.com
cdn.skinport.com
status.skinport.com

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

Firewall Detection:

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

```
(ch@kali)-[~]
$ wafwoof https://skinport.com
wafwoof: command not found

(ch@kali)-[~]
$ wafw00f https://skinport.com
wafw00f: command not found

The Web Application Firewall Fingerprinting Toolkit
[+] Checking https://skinport.com
[+] The site https://skinport.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

Getting information from DNS server

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

```
(cha@kali)-[~]  
$ nslookup https://skinport.com  
Server:      192.168.8.1  
Address:     192.168.8.1#53  can't find the host database  
  
** server can't find https://skinport.com: NXDOMAIN  
-> www001 https://skinport.com  
www001: command not found
```

Getting information from IP Address

Used tool with command: nslookup skinport.com

```
-> www001 https://skinport.com  
www001: command not found  
  
(cha@kali)-[~]  
$ nslookup skinport.com  
Server:      192.168.8.1  
Address:     192.168.8.1#53  
  
Non-authoritative answer:  
Name:   skinport.com  
Address: 104.18.16.19  
Name:   skinport.com  
Address: 104.18.17.19  
www001: command not found
```

Port Scanning:

Used tool with command: nmap 104.18.16.19

```
(cha@kali)-[~]
└─$ nmap 104.18.16.19
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 12:32 +0530
Nmap scan report for 104.18.16.19
Host is up (0.036s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

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

```
(cha@kali)-[~]
└─$ nmap -sV -sC -Pn 104.18.16.19
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 12:33 +0530
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 12:34 (0:00:07 remaining)
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 12:36 (0:00:30 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 12:36 (0:00:00 remaining)
Nmap scan report for 104.18.16.19
Host is up (0.042s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
|_smtp_commands: Couldn't establish connection on port 25
|_fingerprint-strings:
|_  NULL:
|_  421 4.2.1 please try again later
80/tcp    open  http         Cloudflare http proxy
|_http_title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http_server_header: cloudflare
443/tcp   open  ssl/https    Cloudflare
|_http_server_header: cloudflare
|_http_title: 400 The plain HTTP request was sent to HTTPS port
8080/tcp  open  http         Cloudflare http proxy
|_http_server_header: cloudflare
|_http_title: Site doesn't have a title (text/plain; charset=UTF-8).
8443/tcp  open  ssl/https-alt Cloudflare
|_http_title: 400 The plain HTTP request was sent to HTTPS port
|_http_server_header: cloudflare
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.93XI=7x0=9/26KTime=65128263XP=x86_64-pc-linux-gnuXr(NULL
SF:,,22,"421x204\2\1x20pleasex20tryx20againx20later\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.47 seconds
```

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

```
(cha@kali)-[~]
$ nmap -sV -sC -Pn 104.18.16.19 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 12:37 +0530
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 79.38% done; ETC: 12:37 (0:00:03 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.00% done; ETC: 12:38 (0:00:05 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.00% done; ETC: 12:39 (0:00:16 remaining)
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.00% done; ETC: 12:40 (0:00:33 remaining)
Stats: 0:02:42 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 12:40 (0:00:00 remaining)
Nmap scan report for 104.18.16.19
Host is up (0.07% latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      EMLH nmap.scanne.org: failed to receive data: connection closed
|_smtp-commands: SMTP EMLH nmap.scanne.org: failed to receive data: connection closed
|_fingerprint-strings:
|_  GenericLines, GetRequest, HTTPOptions:
|_  452 syntax error (connecting)
|_  many errors
|_  Hello, Help:
|_  452 syntax error (connecting)
80/tcp    open  http      Cloudflare http proxy
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http-server-header: cloudflare
443/tcp   open  ssl/https Cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
8888/tcp  open  tcpwrapped
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http-server-header: cloudflare
8443/tcp  open  tcpwrapped
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.93aI=720-9/26STime=65128365SP=x86_64-pc-linux-gnuXr(Hell
SF:o,1F,"452\\x20syntax\\x20error\\x20\\(connecting\\)\\r\\n")Xr(Help,1F,"452\\x20
SF:syntax\\x20error\\x20\\(connecting\\)\\r\\n")Xr(GenericLines,34,"452\\x20synta
SF:syntax\\x20error\\x20\\(connecting\\)\\r\\n421\\x20too\\x20many\\x20errors\\r\\n")Xr(Ge
SF:tRequest,34,"452\\x20syntax\\x20error\\x20\\(connecting\\)\\r\\n421\\x20too\\x20
SF:many\\x20errors\\r\\n")Xr(HTTPOptions,34,"452\\x20syntax\\x20error\\x20\\(conn
SF:ecting\\)\\r\\n421\\x20too\\x20many\\x20errors\\r\\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.52 seconds
```

Host Scanning:

Used tool with command: `host skinport.com`

```
(cha@kali)-[~]
$ host skinport.com
skinport.com has address 104.18.16.19
skinport.com has address 104.18.17.19
skinport.com mail is handled by 1 aspmx.l.google.com.
skinport.com mail is handled by 5 alt1.aspmx.l.google.com.
skinport.com mail is handled by 10 aspmx3.googlemail.com.
skinport.com mail is handled by 10 aspmx2.googlemail.com.
skinport.com mail is handled by 5 alt2.aspmx.l.google.com.
https://SKINNUEL.COM
(ch@kali)-[~]
```

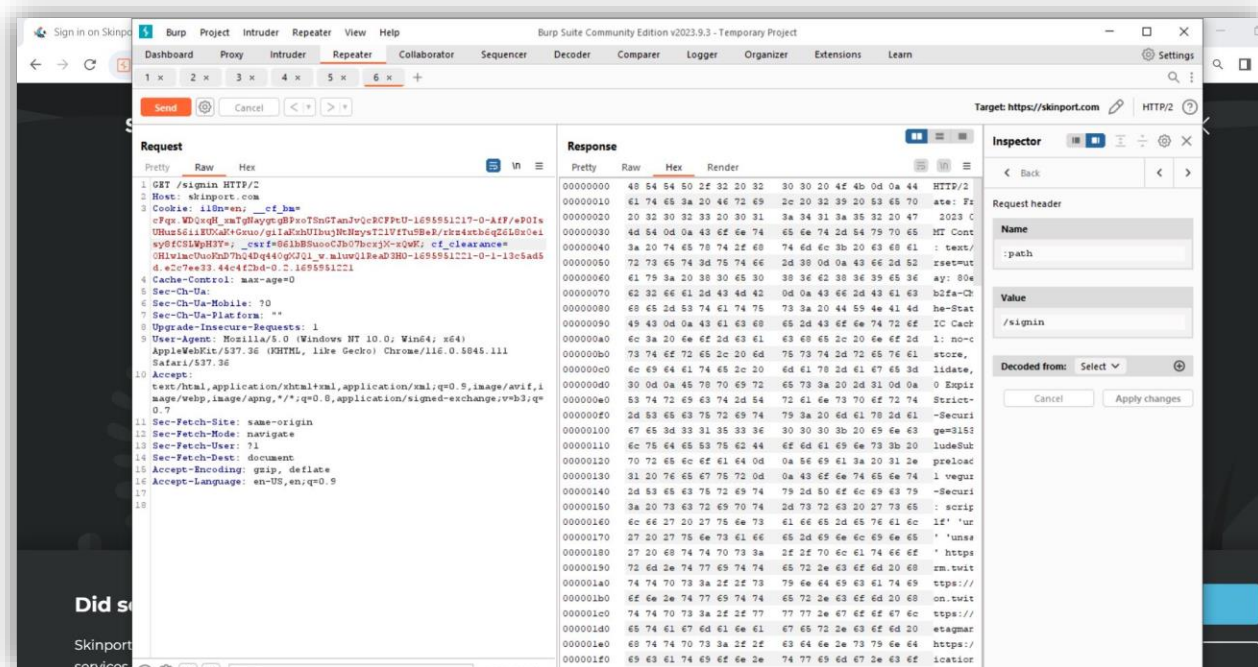
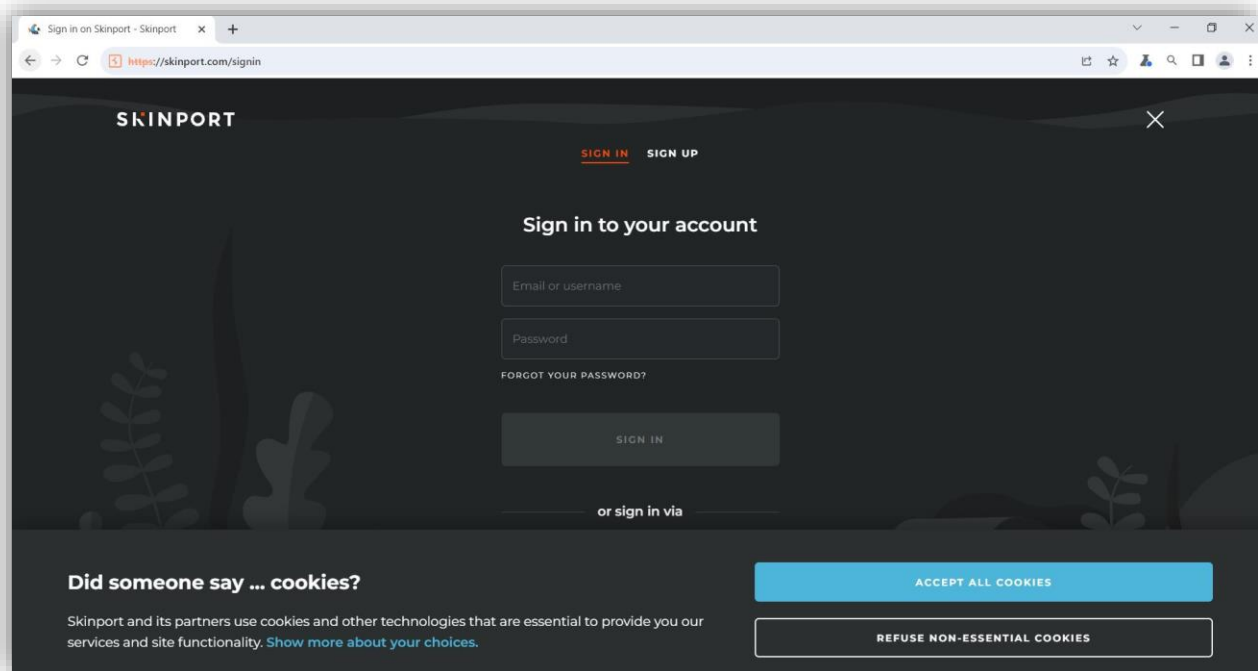
Ping :

Used tool with command: ping skinport.com

```
(cha@kali)-[~]
$ ping skinport.com
PING skinport.com (104.18.16.19) 56(84) bytes of data:
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=1 ttl=56 time=370 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=2 ttl=56 time=124 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=3 ttl=56 time=34.2 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=4 ttl=56 time=59.9 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=5 ttl=56 time=249 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=6 ttl=56 time=83.2 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=7 ttl=56 time=85.0 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=8 ttl=56 time=33.1 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=9 ttl=56 time=39.7 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=10 ttl=56 time=20.8 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=11 ttl=56 time=54.8 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=12 ttl=56 time=195 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=13 ttl=56 time=117 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=14 ttl=56 time=27.7 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=15 ttl=56 time=254 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=16 ttl=56 time=54.4 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=17 ttl=56 time=89.3 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=18 ttl=56 time=108 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=19 ttl=56 time=108 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=20 ttl=56 time=28.6 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=21 ttl=56 time=148 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=22 ttl=56 time=60.6 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=23 ttl=56 time=65.8 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=24 ttl=56 time=89.0 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=25 ttl=56 time=86.1 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=26 ttl=56 time=103 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=27 ttl=56 time=117 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=28 ttl=56 time=36.0 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=29 ttl=56 time=60.4 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=30 ttl=56 time=286 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=31 ttl=56 time=91.2 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=32 ttl=56 time=219 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=33 ttl=56 time=134 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=34 ttl=56 time=50.2 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=35 ttl=56 time=174 ms
64 bytes from 104.18.16.19 (104.18.16.19): icmp_seq=36 ttl=56 time=84.7 ms
```

Proof of concept

Used burp suite professional



Sign in on Skinfo

Burp Suite Community Edition v2023.9.3 - Temporary Project

Dashboard Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time
324	https://skinport.com	GET	/static/locales/en.80ccc2eedc2f...			200	101277	JSON	json			✓	104.18.17.19		07:05:17.29
325	https://skinport.com	GET	/api/home			200	1764	script	js			✓	104.18.17.19		07:05:19.29
326	https://skinport.com	GET	/api/home			200	26643	JSON				✓	104.18.17.19		07:05:20.29
327	https://cdn.skinport.com	GET	/images/apps/440/unusuals/fire...			404	912	HTML	png	Error		✓	104.18.17.19		07:05:21.29
368	https://skinport.com	GET	/api/browse/730?search=aaaaa...		✓	400	330	JSON				✓	104.18.17.19		07:05:24.29
369	https://skinport.com	GET	/market?search=aaaaaaaa		✓	200	2419	HTML		Skinport		✓	104.18.17.19		07:05:32.29
370	https://skinport.com	GET	/api/data/v=80ccc2eedc2f993...			200	1434	JSON				✓	104.18.17.19		07:05:45.29
371	https://skinport.com	GET	/static/locales/en.80ccc2eedc2f...			200	101277	JSON	json			✓	104.18.17.19		07:05:45.29
373	https://skinport.com	GET	/api/home			200	1764	script	js			✓	104.18.17.19		07:05:47.29
374	https://skinport.com	GET	/api/browse/730?search=aaaaa...		✓	400	330	JSON				✓	104.18.17.19		07:05:50.29
375	https://skinport.com	GET	/static/288.8fd33d81059ace.js			200	306588	script	js			✓	104.18.17.19		07:10:01.29

Request

Raw Hex

```

1 GET /market?search=aaaaaaaa HTTP/2
2 Host: skinport.com
3 Cookie: i18n=en; __cf_bm=
cFqX.WDQvGfH..._cf_bm=
861b85uocCrbO...
cf_clearance=
0H1wacUu0hD7hQ4d4qGQ1_v...
4 Cache-Control: max-age=0
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: 0
7 Sec-Ch-Ua-Platform:
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111
Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: 1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.5

```

Response

Raw Hex Render

```

1 HTTP/2 200 OK
2 Date: Fri, 29 Sep 2023 01:35:45 GMT
3 Content-Type: text/html; charset=utf-8
4 Cf-Ray: 80e07d6d8bcb303-CMB
5 Cf-Cache-Status: DYNAMIC
6 Cache-Control: no-cache, no-store, must-revalidate, max-age=0
7 Expires: -1
8 Strict-Transport-Security: max-age=31536000;
includeSubDomains; preload
9 Via: 1.1 vengur
10 Content-Security-Policy: script-src 'self' 'unsafe-eval'
'unsafe-inline' https://platform.twitter.com
https://syndication.twitter.com
https://www.googleatagmanager.com
https://cdn.syndication.twimg.com https://www.google.com
https://www.google-analytics.com https://maps.googleapis.com
https://apis.google.com https://connect.facebook.net
https://challenges.cloudflare.com
https://static.cloudflareinsights.com
https://bat.bing.com; report-uri
https://o298048.ingest.sentry.io/api/6193335/security/?sentry_key=
98577efcbca24e6daf4a099b6d11076
11 Expect-Ct: max-age=0
12 Origin-Agent-Cluster: 1
13 Pragma: no-cache
14 Referer-Policy: strict-origin-when-cross-origin
15 X-Content-Type-Options: nosniff
16 X-Download-Options: noopen
17 X-Frame-Options: SAMEORIGIN
18 X-Permitted-Cross-Domain-Policies: none
19 X-XSS-Protection: 0
20 Vary: Accept-Encoding
21 Server: cloudflare
22
23
24 <!doctype html> <html>
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width,user-scalable=no,initial-scale=1,maximum-scale=1,minimum-scale=1">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<title>
Skinport
</title>
<link rel="apple-touch-icon" sizes="180x180" href="/static/apple-touch-icon.png">
<link rel="icon" type="image/png" sizes="32x32" href="/static/favicon-32x32.png">
<link rel="icon" type="image/png" sizes="16x16" href="/static/favicon-16x16.png">
<link rel="manifest" href="/static/site.webmanifest">
<link rel="mask-icon" href="/static/safari-pinned-tab.svg"

```

Inspector

Selection 10 (Box)

Selected text

AAAAA

Request attributes 2

Request query parameters 1

Request cookies 4

Request headers 21

Response headers 21

Sign in on Skinfo

Burp Suite Community Edition v2023.9.3 - Temporary Project

Dashboard Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Proxy settings

Target: https://skinport.com HTTP/2

Send Cancel

Request

Raw Hex

```

1 GET /signin HTTP/2
2 Host: skinport.com
3 Cookie: i18n=en; __cf_bm=
cFqX.WDQvGfH..._cf_bm=
861b85uocCrbO...
cf_clearance=
0H1wacUu0hD7hQ4d4qGQ1_v...
4 Cache-Control: max-age=0
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: 0
7 Sec-Ch-Ua-Platform:
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111
Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: 1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.5
17
18

```

Response

Raw Hex Render

```

1 https://syndication.twitter.com https://www.googleatagmanager.com
https://cdn.syndication.twimg.com https://www.google.com
https://www.google-analytics.com https://maps.googleapis.com
https://apis.google.com https://connect.facebook.net
https://challenges.cloudflare.com
https://static.cloudflareinsights.com
https://bat.bing.com; report-uri
https://o298048.ingest.sentry.io/api/6193335/security/?sentry_key=
98577efcbca24e6daf4a099b6d11076
11 Expect-Ct: max-age=0
12 Origin-Agent-Cluster: 1
13 Pragma: no-cache
14 Referer-Policy: strict-origin-when-cross-origin
15 X-Content-Type-Options: nosniff
16 X-Download-Options: noopen
17 X-Frame-Options: SAMEORIGIN
18 X-Permitted-Cross-Domain-Policies: none
19 X-XSS-Protection: 0
20 Vary: Accept-Encoding
21 Server: cloudflare
22
23
24 <!doctype html> <html>
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width,user-scalable=no,initial-scale=1,maximum-scale=1,minimum-scale=1">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<title>
Skinport
</title>
<link rel="apple-touch-icon" sizes="180x180" href="/static/apple-touch-icon.png">
<link rel="icon" type="image/png" sizes="32x32" href="/static/favicon-32x32.png">
<link rel="icon" type="image/png" sizes="16x16" href="/static/favicon-16x16.png">
<link rel="manifest" href="/static/site.webmanifest">
<link rel="mask-icon" href="/static/safari-pinned-tab.svg"

```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 4

Name	Value	IS
i18n	en	
__cf_bm	cFqX.WDQvGfH...	
__cf_bm	861b85uocCrbO...	
cf_clearance	0H1wacUu0hD7hQ4d4qGQ1_v...	

Request headers 21

Name	Value	IS
ischeme	https	
method	GET	
path	/signin	
authority	skinport.com	
cookie	i18n=en	
cookie	__cf_bm=cFqX.W...	
cookie	__cf_bm=861b85uoc...	
cookie	cf_clearance=O...	
cache-control	max-age=0	
sec-ch-ua		
sec-ch-ua-mobile	0	

2,419 bytes | 408 millis

Vulnerability

02. Vulnerability title	Admin page disclosure
03. Vulnerability description	<p>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.</p> <p>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.</p> <p>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.</p>
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
safeiframe.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
l.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

```

KALI LINUX

"the quieter you become, the more you are able to hear"

```

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

```

KALI LINUX

"the quieter you become, the more you are able to hear"

```

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

```

Firewall Detection:

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

```
(cha@kali)-[~]
$ wafw00f https://judge.me/

      ( Woof! )
    ( / \ )
  ( / \ )
( / \ )

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://judge.me/
ERROR:wafw00f:Something went wrong HTTPConnectionPool(host='judge.me', port=443): Read timed out.
[+] Generic Detection results:
[*] The site https://judge.me/ seems to be behind a WAF or some sort of security solution
[~] Reason: The server header is different when an attack is detected.
The server header for a normal response is "Cowboy", while the server header a response to an attack is "",
[~] Number of requests: 6
```

Port Scanning: Required,

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

```
(cha@kali)-[~]
$ nmap -sV -sC -Pn 52.20.78.240 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-06 12:32 +0530
Nmap scan report for ec2-52-20-78-240.compute-1.amazonaws.com (52.20.78.240)
Host is up (0.28s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         heroku-router
|_ http-title: Heroku | Application Error
|_ fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Cache-Control: no-cache, no-store
|     Content-Type: text/html; charset=utf-8
|     Date: 2023-10-06 07:03:11.608754027 +0000 UTC
|     Server: heroku-router
|     Content-Length: 0
|_ GetRequest:
|   HTTP/1.0 400 Bad Request
|   Cache-Control: no-cache, no-store
|   Content-Type: text/html; charset=utf-8
|   Date: 2023-10-06 07:02:59.767621181 +0000 UTC
|   Server: heroku-router
|   Content-Length: 0
|_ HTTPOptions:
|   HTTP/1.0 400 Bad Request
|   Cache-Control: no-cache, no-store
|   Content-Type: text/html; charset=utf-8
|   Date: 2023-10-06 07:02:59.767621181 +0000 UTC
|   Server: heroku-router
|   Content-Length: 0
|_ http-server-header: heroku-router
443/tcp   open  https?
8008/tcp  open  http
|_ fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8015/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|_ GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|   HTTP/1.1 302 Found
|   Location: https://:8015
|   Connection: close
```

```
SF::\x20https://:8015\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEO
SF:RIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Option
SF:s:\x20nosniff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'\
SF:r\n\r\n")&#x20;Xr(SIPOptions,D2,"HTTP/1.1;\x20302\x20Found\r\nLocation:\x20ht
SF:tps://:8015\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r
SF:\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20n
SF:osniff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'\r\n\r\n
SF:");
```

```
----- NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY) -----
SF-Port8010-TCP:V=7.93%T=SSL%I=7%0-10/6%Time=651FB131%P=x86_64-pc-linux-gn
SF:u&#x20;(GenericLines,BBD,"HTTP/1.1;\x20200\x200K\r\nContent-Length:\x202736
SF:r\n\r\nConnection:\x20close\r\nCache-Control:\x20no-cache\r\nContent-Type:
SF:\x20text/html;\x20charset=utf-8\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-
SF:XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20nosni
SF:ff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'\r\n\r\n<IDO
SF:CTYPE>\x20html><html\x20lang=en>\x20<head>\x20<meta\x20charset=UTF
SF:-8>\x20<meta\x20http-equiv=X-UA-Compatible>\x20content=IE=8;\x20
SF:IE=EDGE>\x20<meta\x20name=viewport>\x20content=width=device-widt
SF:h;\x20initial-scale=1>\x20<style>\x20type=css>\x20body\x20{\x
SF:20height:\x20100%;&#x20font-family:\x20Helvetica,\x20Arial,\x20sans-seri
SF:f;\x20color:\x20#6a6a6a;\x20margin:\x200;\x20display:\x20flex;\x20align
SF:items:\x20center;\x20justify-content:\x20center;\x20}&#x20input[type=d
SF:ate],&#x20input[type=email],&#x20input[type=number],&#x20input[type=
SF:password],&#x20input[type=search],&#x20input[type=tel],&#x20input[ty
SF:pe=text],&#x20input[type=time],&#x20input[type=url],&#x20select,&#x20t
SF:extarea}&#x20{\x20color:\x20#262626;\x20vertical-align:\x20baseline;\x20m
SF:argin:\x20.2em;\x20border-style:\x20solid}&#x20;%(GetRequest,BBD,"HTTP/1.1
SF:\x20200\x200K\r\nContent-Length:\x202736\r\nConnection:\x20close\r\nCac
SF:he-Control:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=utf-8
SF:\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mode=b
SF:lock\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\
SF:\x20frame-ancestors\x20'self'\r\n\r\n<DOCTYPE>\x20html><html\x20lang=e
SF:n>\x20<head>\x20<meta\x20charset=UTF-8>\x20<meta\x20http-equiv=X-
SF:X-UA-Compatible>\x20content=IE=8;\x20IE=EDGE>\x20<meta\x20name=v
SF:iewport>\x20content=width=device-width,\x20initial-scale=1>\x20<st
SF:yle>\x20type=css>\x20body\x20{\x20height:\x20100%;&#x20font-fami
SF:ly:\x20Helvetica,\x20Arial,\x20sans-serif;\x20color:\x20#6a6a6a;\x20mar
SF:gin:\x200;\x20display:\x20flex;\x20align-items:\x20center;\x20justify-c
SF:ontent:\x20center;\x20}&#x20input[type=date],&#x20input[type=email],\
SF:\x20input[type=number],&#x20input[type=password],&#x20input[type=sear
SF:ch],&#x20input[type=tel],&#x20input[type=text],&#x20input[type=time\
SF:],&#x20input[type=url],&#x20select,&#x20textarea}&#x20{\x20color:\x202626
SF:26;\x20vertical-align:\x20baseline;\x20margin:\x20.2em;\x20border-styl
SF:e:\x20solid}");
```

Host script results:

|_clock-skew: 1s

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 254.19 seconds

Directory Enumeration: Required,

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

```

Processing triggers for libc-bin (2.27-6) ...

(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: 15658]
/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]

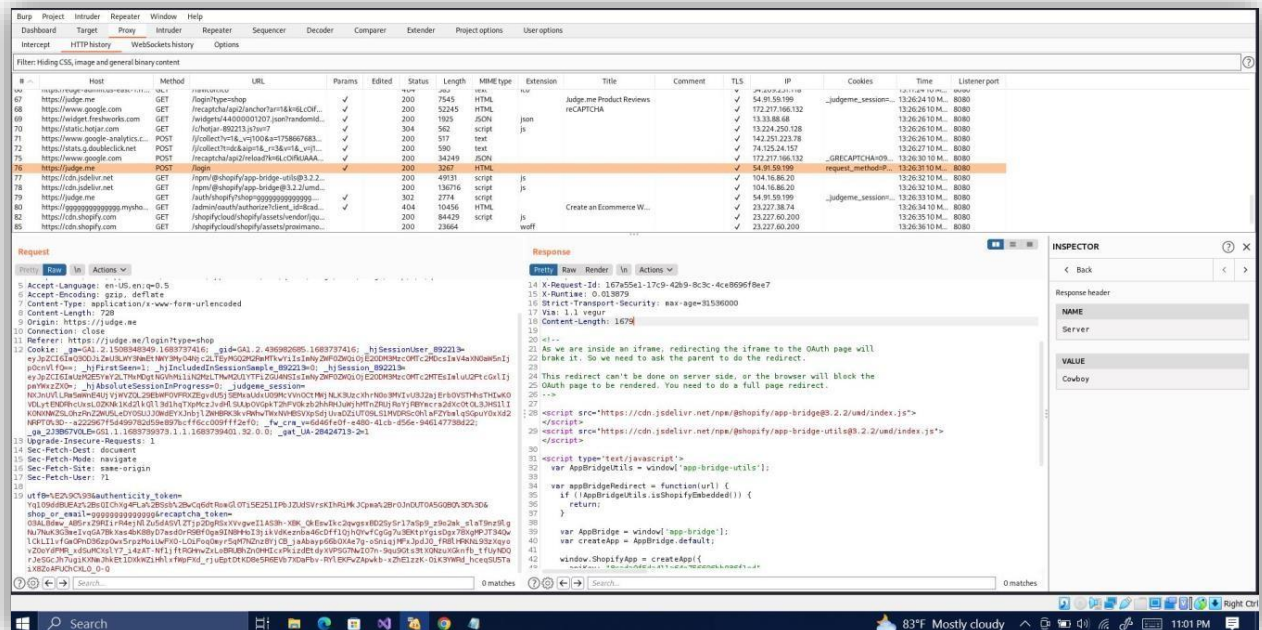
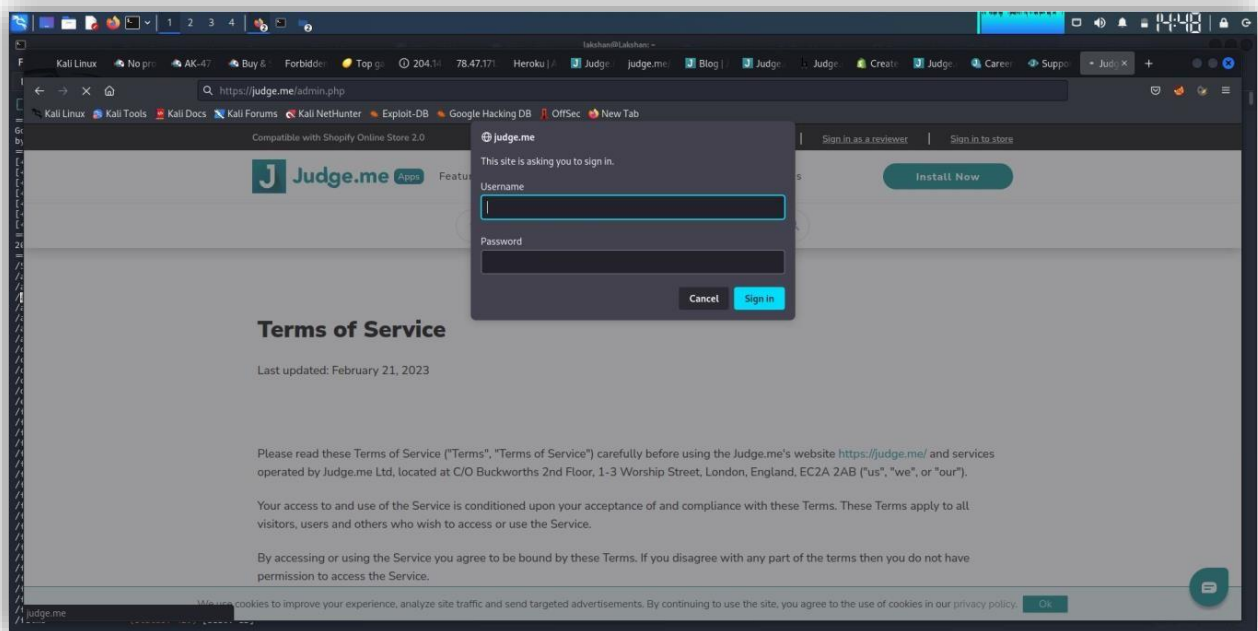
```

```

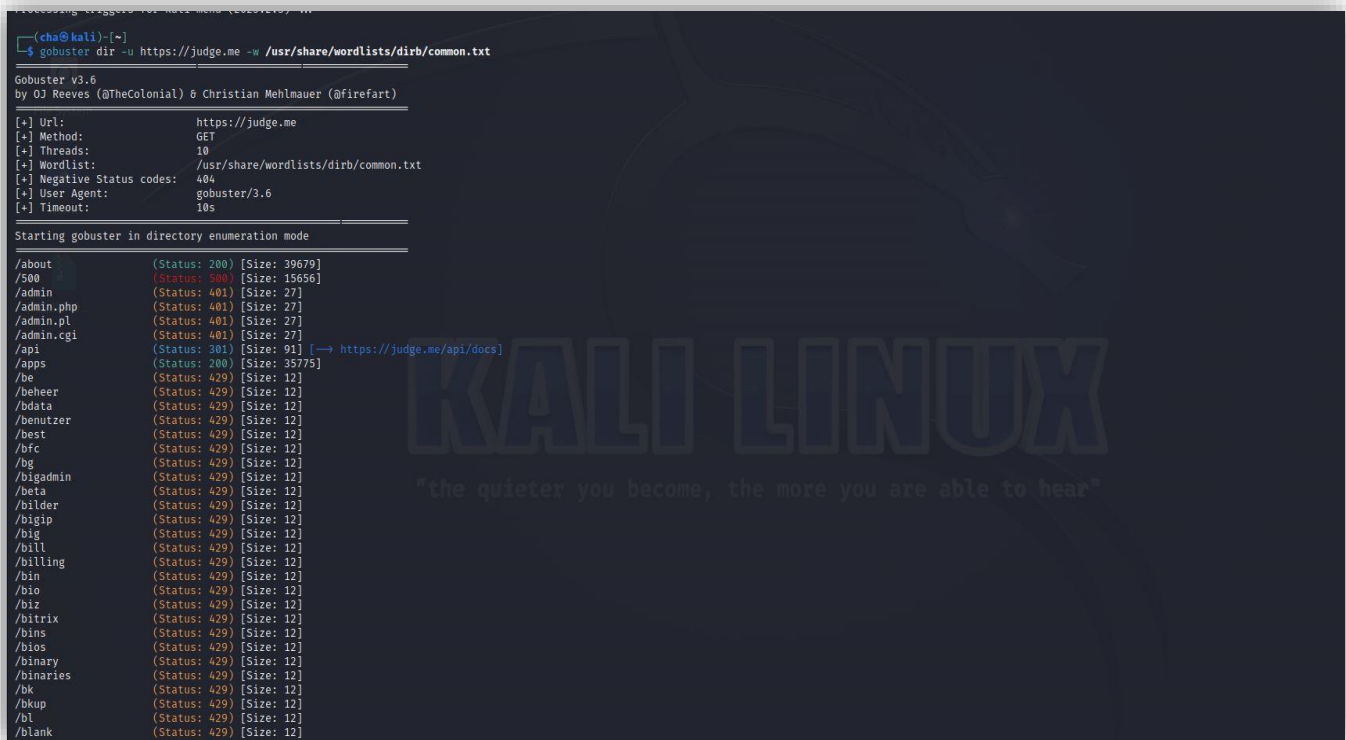
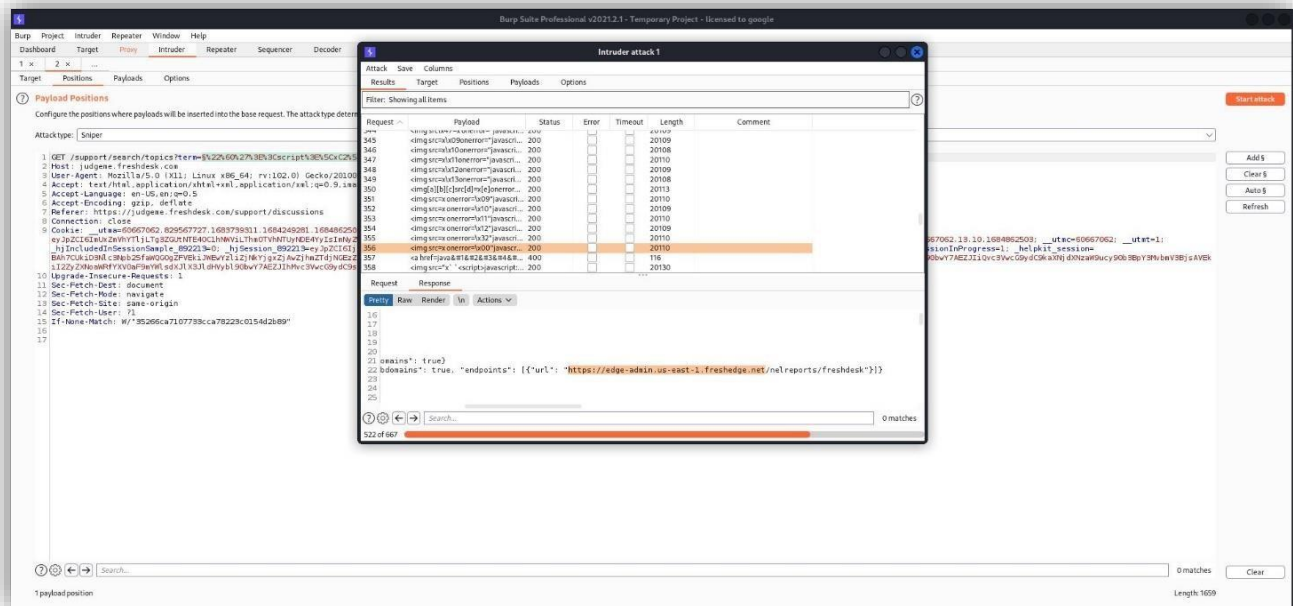
/personal    (Status: 429) [Size: 12]
/personals   (Status: 429) [Size: 12]
/pfx         (Status: 429) [Size: 12]
/pg          (Status: 429) [Size: 12]
/pgadmin     (Status: 429) [Size: 12]
/pgp         (Status: 429) [Size: 12]
/pgsql       (Status: 429) [Size: 12]
/phf         (Status: 429) [Size: 12]
/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]
/searchmx    (Status: 429) [Size: 12]
/search_results (Status: 429) [Size: 12]
/searchresults (Status: 429) [Size: 12]
/secode      (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	<p>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.</p> <p>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.</p> <p>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.</p>
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!