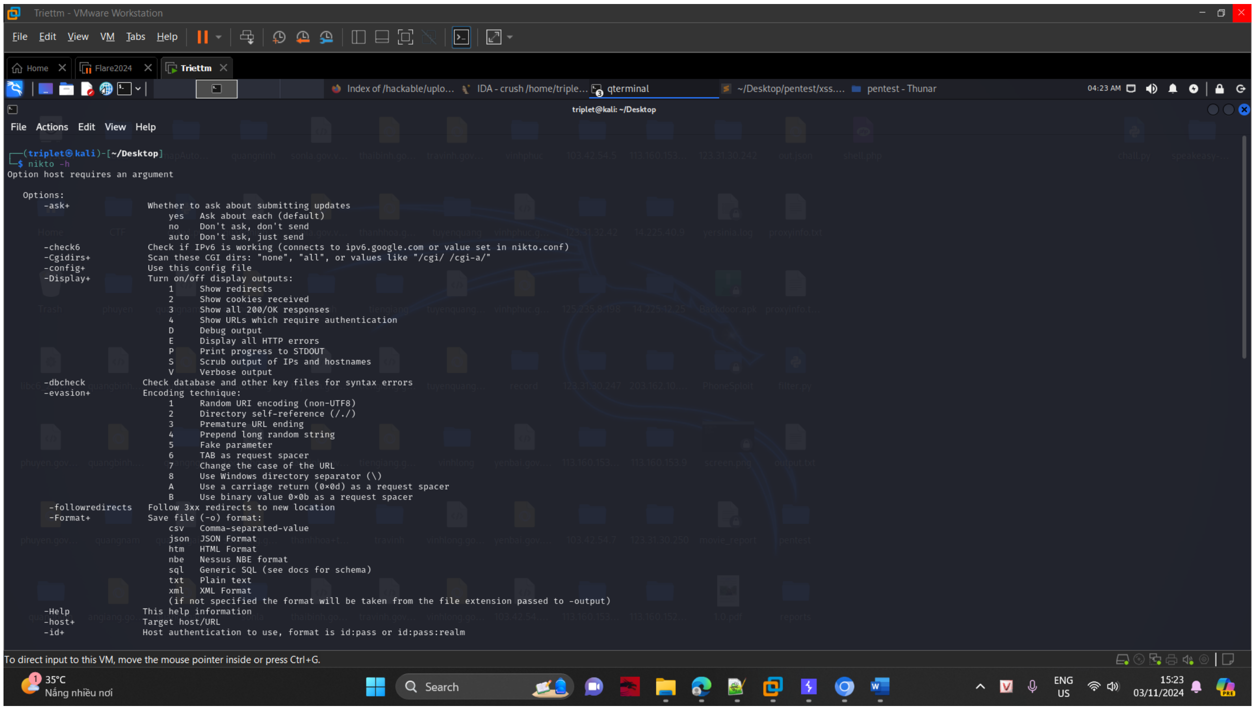
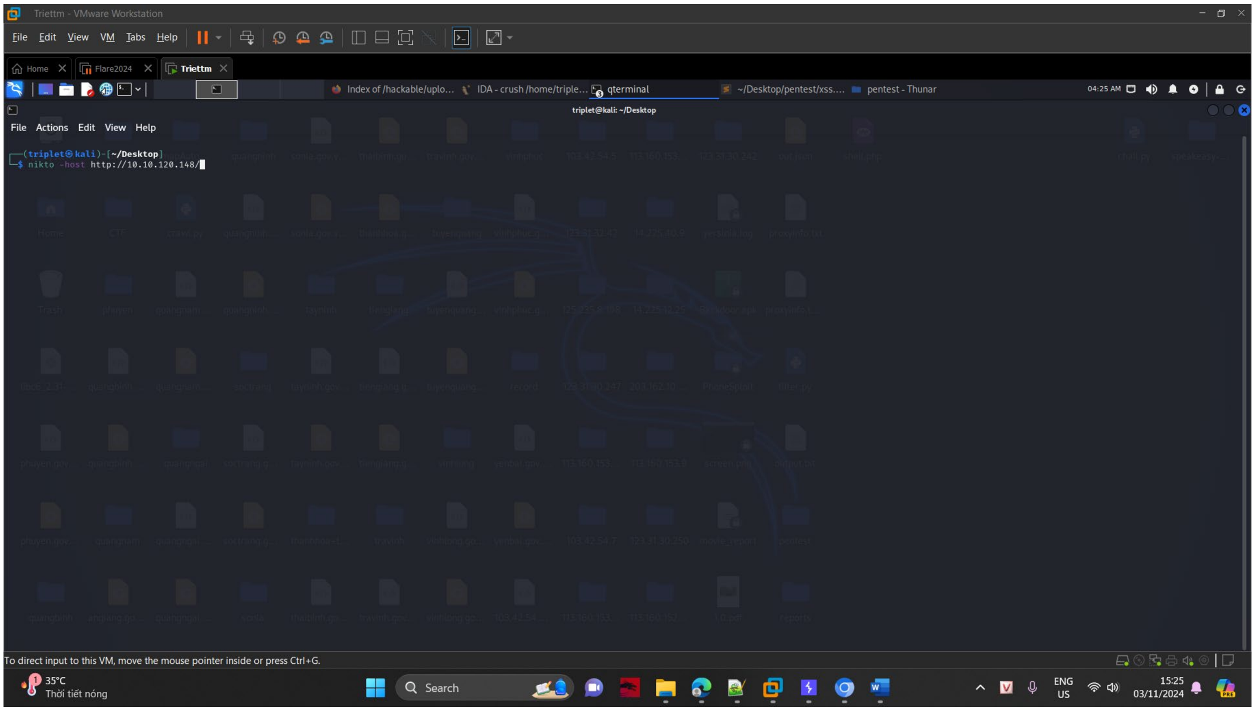
Lab 13: Using nikto.pl	
Name	Tran Minh Triet
Student ID	SE172241

Start Nikto



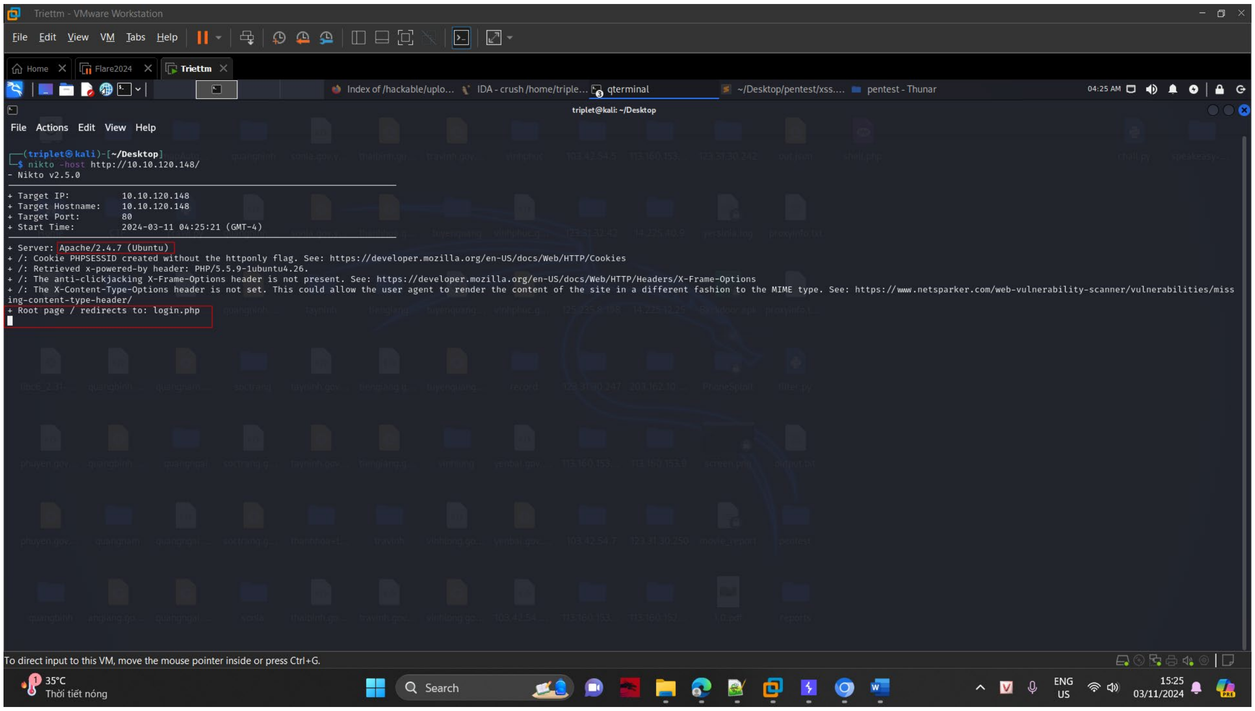
```
┌──(triplet㉿kali)-[~/Desktop]
└─$ nikto -h
Option host requires an argument

   Options:
       -ask+               Whether to ask about submitting updates
                               yes   Ask about each (default)
                               no    Don't ask, don't send
                               auto  Don't ask, just send
       -check6             Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                               1     Show redirects
                               2     Show cookies received
                               3     Show all 200/OK responses
                               4     Show URLs which require authentication
                               D     Debug output
                               E     Display all HTTP errors
                               P     Print progress to STDOUT
                               S     Scrub output of IPs and hostnames
                               V     Verbose output
       -dbcheck           Check database and other key files for syntax errors
       -evasion+          Encoding technique:
                               1     Random URI encoding (non-UTF8)
                               2     Directory self-reference (/./)
                               3     Premature URL ending
                               4     Prepend long random string
                               5     Fake parameter
                               6     TAB as request spacer
                               7     Change the case of the URL
                               8     Use Windows directory separator (\)
                               A     Use a carriage return (0×0d) as a request spacer
                               B     Use binary value 0×0b as a request spacer
        -followredirects   Follow 3xx redirects to new location
        -Format+           Save file (-o) format:
                               csv   Comma-separated-value
                               json  JSON Format
                               htm   HTML Format
                               nbe   Nessus NBE format
                               sql   Generic SQL (see docs for schema)
                               txt   Plain text
                               xml   XML Format
                               (if not specified the format will be taken from the file extension passed to -output)
       -Help              This help information
       -host+             Target host/URL
       -id+               Host authentication to use, format is id:pass or id:pass:realm
```

Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /hackable/uplo...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
04:23 AM
triplet@kali: ~/Desktop
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
35°C
Nắng nhiều nơi
Search
ENG
US
15:23
03/11/2024

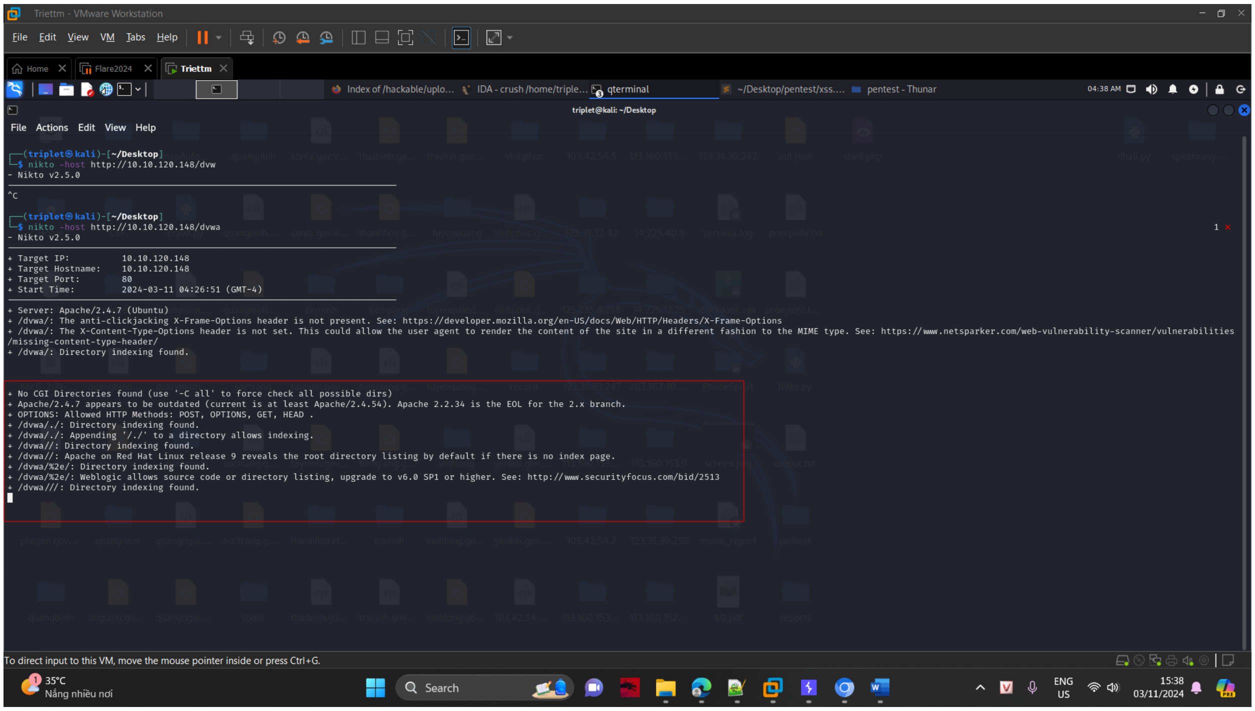


```
┌──(triplet㉿kali)-[~/Desktop]
└─$ nikto -host http://10.10.120.148/
```

Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /hackable/uplo...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
04:25 AM
triplet@kali: ~/Desktop
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
35°C
Thời tiết nóng
Search
ENG
US
15:25
03/11/2024

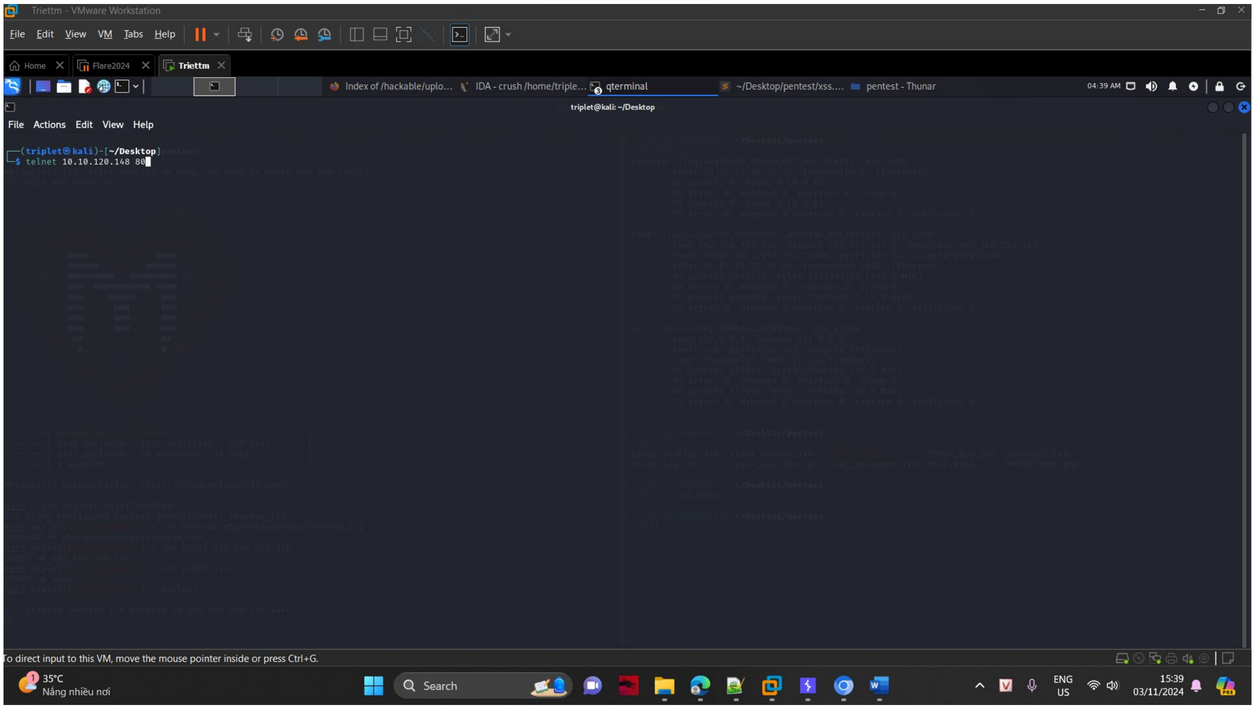


```
┌──(triplet㉿kali)-[~/Desktop]
└─$ nikto -host http://10.10.120.148/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.120.148
+ Target Hostname:    10.10.120.148
+ Target Port:        80
+ Start Time:         2024-03-11 04:25:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: login.php
```

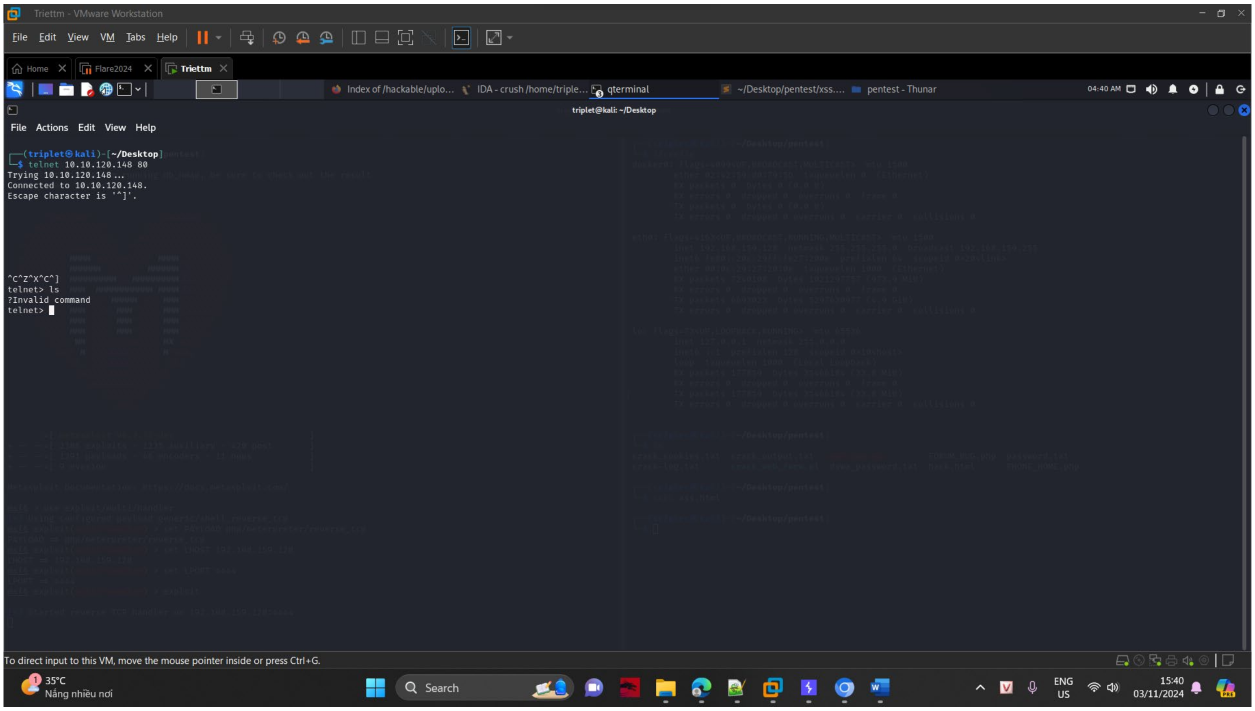


```
┌──(triplet㉿kali)-[~/Desktop]
└─$ nikto -host http://10.10.120.148/dvw
- Nikto v2.5.0
---------------------------------------------------------------------------
^C

┌──(triplet㉿kali)-[~/Desktop]
└─$ nikto -host http://10.10.120.148/dvwa
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.120.148
+ Target Hostname:    10.10.120.148
+ Target Port:        80
+ Start Time:         2024-03-11 04:26:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /dvwa/: Directory indexing found.


+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /dvwa/./: Directory indexing found.
+ /dvwa/./: Appending '/./' to a directory allows indexing.
+ /dvwa//: Directory indexing found.
+ /dvwa//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /dvwa/%2e/: Directory indexing found.
+ /dvwa/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ /dvwa///: Directory indexing found.
```

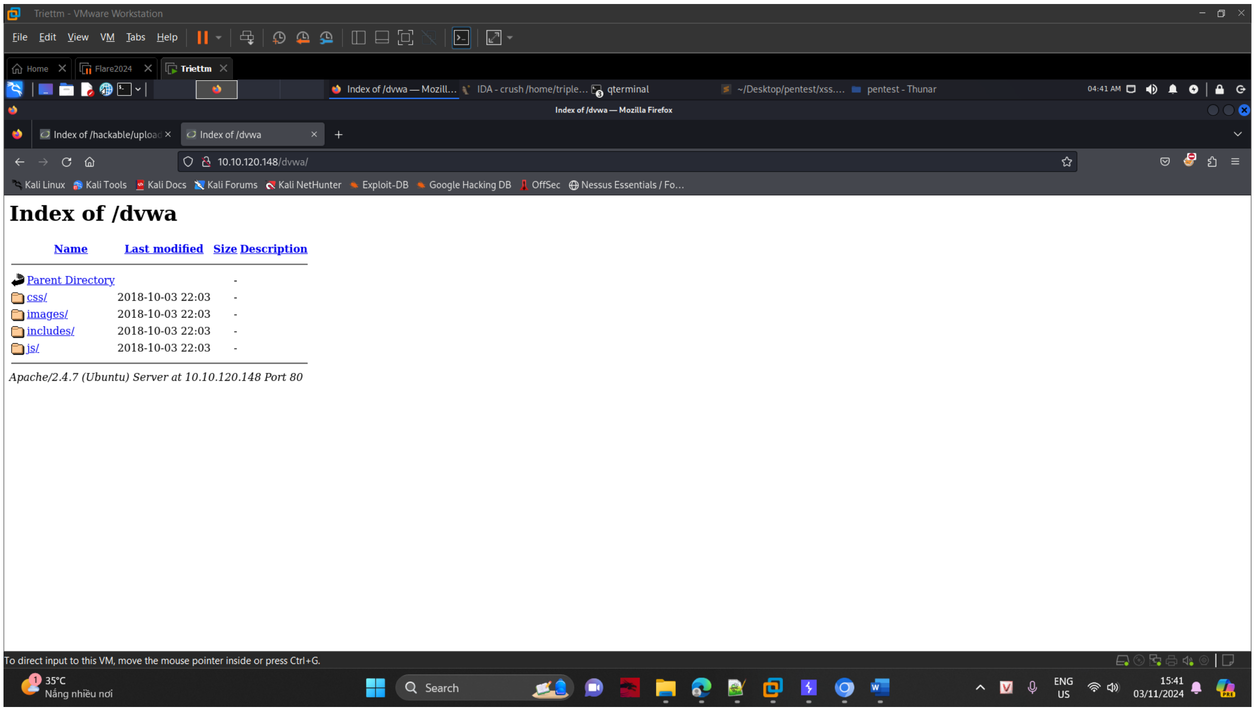
Use Telnet to Grab Webserver and Operating System Banner


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /hackable/uplo...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
04:39 AM
triplet@kali: ~/Desktop
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
35°C
Nắng nhiều nơi
Search
ENG
US
15:39
03/11/2024

```
┌──(triplet㉿kali)-[~/Desktop]
└─$ telnet 10.10.120.148 80
```


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /hackable/uplo...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
04:40 AM
triplet@kali: ~/Desktop
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
35°C
Nắng nhiều nơi
Search
ENG
US
15:40
03/11/2024

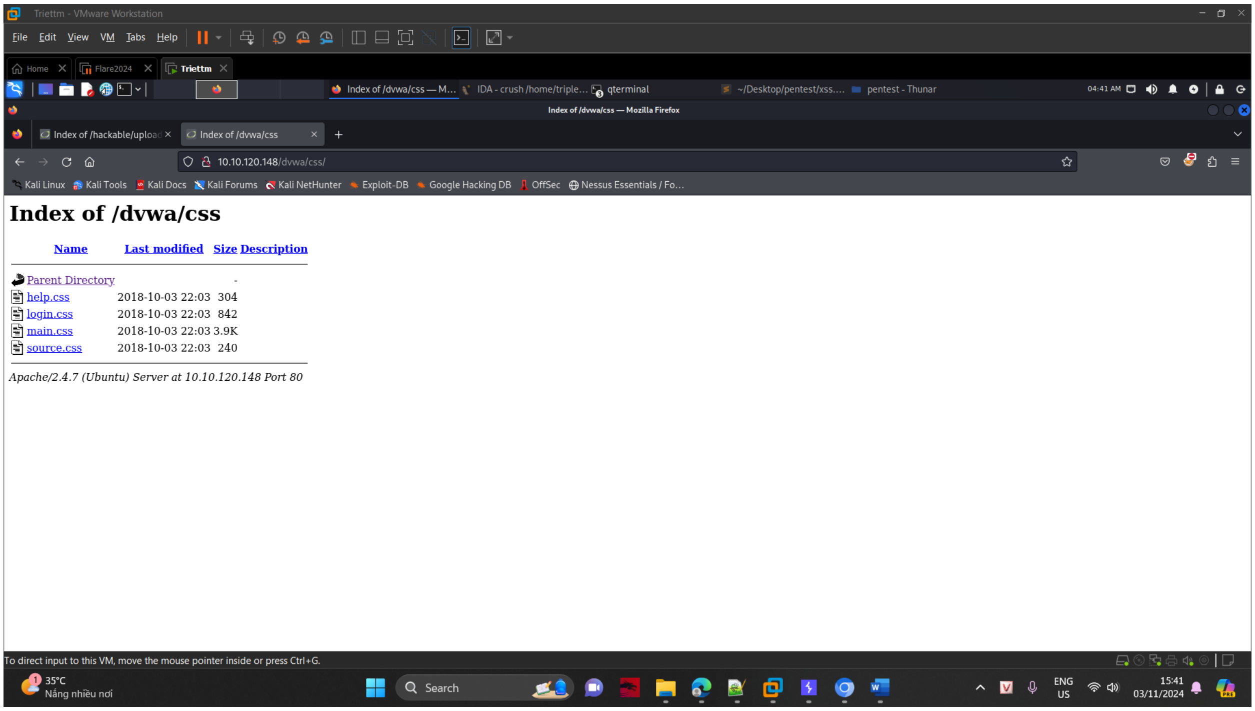
```
┌──(triplet㉿kali)-[~/Desktop]
└─$ telnet 10.10.120.148 80
Trying 10.10.120.148...
Connected to 10.10.120.148.
Escape character is '^]'.




^C^Z^X^C^]
telnet> ls
?Invalid command
telnet> 
```


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /dvwa — Mozill...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
04:41 AM
Index of /dvwa — Mozilla Firefox
Index of /hackable/uploac
Index of /dvwa
10.10.120.148/dvwa/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
35°C
Nắng nhiều nơi
Search
ENG
US
15:41
03/11/2024

Index of /dvwa

Name	Last modified	Size	Description
Parent Directory		-	
css/	2018-10-03 22:03	-	
images/	2018-10-03 22:03	-	
includes/	2018-10-03 22:03	-	
js/	2018-10-03 22:03	-	

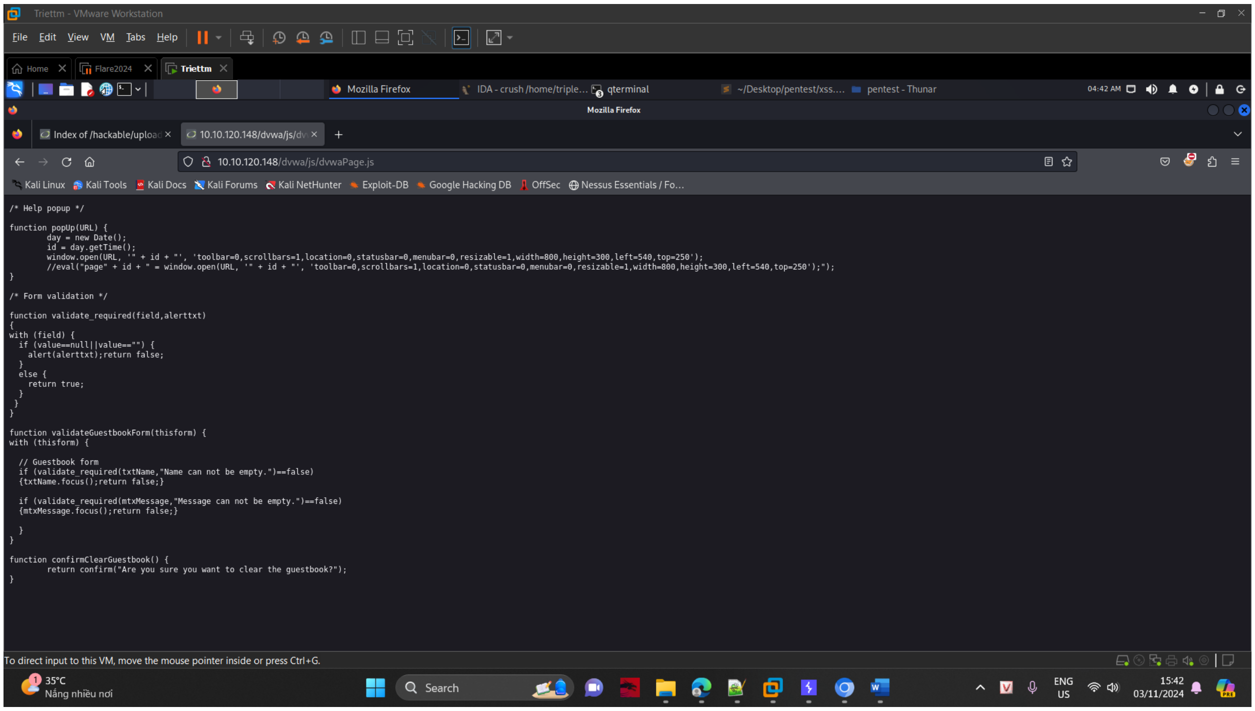
Apache/2.4.7 (Ubuntu) Server at 10.10.120.148 Port 80


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /dvwa/css — M...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
04:41 AM
Index of /dvwa/css — Mozilla Firefox
Index of /hackable/uploac
Index of /dvwa/css
10.10.120.148/dvwa/css/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
35°C
Nắng nhiều nơi
Search
ENG
US
15:41
03/11/2024

Index of /dvwa/css

Name	Last modified	Size	Description
Parent Directory		-	
help.css	2018-10-03 22:03	304	
login.css	2018-10-03 22:03	842	
main.css	2018-10-03 22:03	3.9K	
source.css	2018-10-03 22:03	240	

Apache/2.4.7 (Ubuntu) Server at 10.10.120.148 Port 80



```
/* Help popup */

function popUp(URL) {
        day = new Date();
        id = day.getTime();
        window.open(URL, '" + id + "', 'toolbar=0,scrollbars=1,location=0,statusbar=0,menubar=0,resizable=1,width=800,height=300,left=540,top=250');
        //eval("page" + id + " = window.open(URL, '" + id + "', 'toolbar=0,scrollbars=1,location=0,statusbar=0,menubar=0,resizable=1,width=800,height=300,left=540,top=250');");
}

/* Form validation */

function validate_required(field,alerttxt)
{
with (field) {
  if (value==null||value=="") {
    alert(alerttxt);return false;
  }
  else {
    return true;
  }
 }
}

function validateGuestbookForm(thisform) {
with (thisform) {

  // Guestbook form
  if (validate_required(txtName,"Name can not be empty.")==false)
  {txtName.focus();return false;}

  if (validate_required(mtxMessage,"Message can not be empty.")==false)
  {mtxMessage.focus();return false;}

  }
}

function confirmClearGuestbook() {
        return confirm("Are you sure you want to clear the guestbook?");
}
```