

Report Attacchi di Phishing W23D4

In questo esercizio dovremo simulare due diversi attacchi di phishing, uno tramite Gophish e uno tramite uno strumento chiamato SET (Social Engineering Toolkit).

Gophish

Gophish è un framework gratuito usato per simulare campagne di phishing, noi andremo ad utilizzarlo per scopi puramente didattici.

Come da consegna andiamo a scaricare la versione di Gophish per Windows, accediamo con le credenziali fornite ed eseguiamo poi un cambio password come suggerito dalla piattaforma.

Step 1 Andiamo a creare un gruppo chiamandolo prova ed aggiungiamo un user, nel mio caso ho aggiunto me stessa come target della campagna phishing.

The screenshot shows the Gophish web interface for managing users. At the top, a red banner displays the message "No targets specified". Below this, there is a "Name:" label followed by a text input field containing the word "Prova". Underneath the input field are two buttons: a red "+ Bulk Import Users" button and a "Download CSV Template" link. Below these buttons, there are four input fields for user details: "First Name" (containing "Sara"), "Last Name" (containing "Man"), "Email" (containing "saram.manini@gm"), and "Position" (containing "Position"). To the right of these fields is a red "+ Add" button. Below the input fields, there is a "Show" dropdown menu set to "10" and a "Search:" input field. Below the search field, there is a table with headers "First Name", "Last Name", "Email", and "Position". The table body is empty, and a message "No data available in table" is displayed. Below the table, it says "Showing 0 to 0 of 0 entries". At the bottom right, there are "Previous" and "Next" buttons. At the very bottom, there are "Close" and "Save changes" buttons.

Step 2 Selezioniamo una mail da usare come template per la campagna, come si può vedere nell'immagine sottostante ho scelto una mail inviata da Epicode. Clicchiamo sui tre puntini a lato della mail, poi su mostra messaggio originale ed infine copia negli appunti.

Messaggio originale

ID messaggio	<9yF21Z_1TbWd1CUjSM37zA@geopod-ismtpd-7>
Creato alle:	30 luglio 2025 alle ore 11:26 (consegnato dopo 0 secondi)
Da:	noreply@epicode.com
A:	saram.manini@gmail.com
Oggetto:	Feedback for W20D4 - Consegna
SPF:	PASS con l'IP 149.72.80.22 Ulteriori informazioni
DKIM:	'PASS' con il dominio epicode.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

[Scarica messaggio originale](#)[Copia negli appunti](#)

Step 3 Proseguiamo creando la mail per la campagna di phishing, importiamo la mail copiata negli appunti in precedenza e modifichiamola in modo che serva al meglio ai nostri scopi. Una volta soddisfatti, clicchiamo su salva.

Import Email

Envelope Sender:

noreply@epicode.com

Subject:

Ritardo nei pagamenti

TextHTML

B *I* ~~S~~ I_x Styles

Normal

Ciao Epicoder,

Visto che si tratta di un esercizio puramente didattico, ho scelto una pagina solitamente usata per test di vulnerabilità: VulnWeb.

Edit Landing Page

Name:

VulnWeb

Import Site

HTML

B I S T_x | **¶** | **☰ ☷** | **↶ ↷** | **🔗 🔕** | **📌 🚫** | **🖼️ 🪴** | **☰ ☷** | **Ω** | **🔄** | **💡 Source** | **🔍**

B I S T_x | **¶** | **☰ ☷** | **↶ ↷** | **🔗 🔕** | **📌 🚫** | **🖼️ 🪴** | **☰ ☷** | **Ω** | **🔄** | **💡 Source** | **🔍**

Acunetix website security

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

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

If you are already registered please enter your login information below:

☒ Capture Submitted Data ?

Step 5 Creiamo un profilo per il mittente della mail di phishing, in questo caso è stata creata una mail ad hoc su Gmail: noreplyepicode@gmail.com, ad un occhio inesperto questo indirizzo email potrebbe risultare legittimo e questo ovviamente va a favore dell'attaccante.

Di seguito i requisiti per creare una email Gmail che funziona correttamente con Gophish:

- Abilitare l'autenticazione a 2 fattori;
- Abilitare l'app password per Gophish.

Successivamente abbiamo riempito i campi richiesti da Gophish con le seguenti informazioni:

- Name: Epicode;
- Interface Type: SMTP;
- SMTP from: noreplyepicode@gmail.com
- Host: smtp.gmail.com:465
- Username: noreplyepicode@gmail.com;
- Password: App password fornita da Google.

The image shows a web-based configuration form for an SMTP mail client. The form is organized into several sections with labels and input fields. The 'Name' field contains 'Epicode'. The 'Interface Type' dropdown menu is set to 'SMTP'. The 'SMTP From:' field contains 'noreplyepicode@gmail.com'. The 'Host' field contains 'smtp.gmail.com:465'. The 'Username' field contains 'noreplyepicode@gmail.com'. The 'Password' field is masked with dots. There is a checkbox labeled 'Ignore Certificate Errors' which is checked. At the bottom, under 'Email Headers:', there are two input fields: one containing 'X-Custom-Header' and another containing '{{.URL}}-gophish'. To the right of these fields is a red button with a plus icon and the text '+ Add Custom Header'.

Name:

Epicode

Interface Type:

SMTP

SMTP From: ⓘ

noreplyepicode@gmail.com

Host:

smtp.gmail.com:465

Username:

noreplyepicode@gmail.com

Password:

☒ Ignore Certificate Errors ⓘ

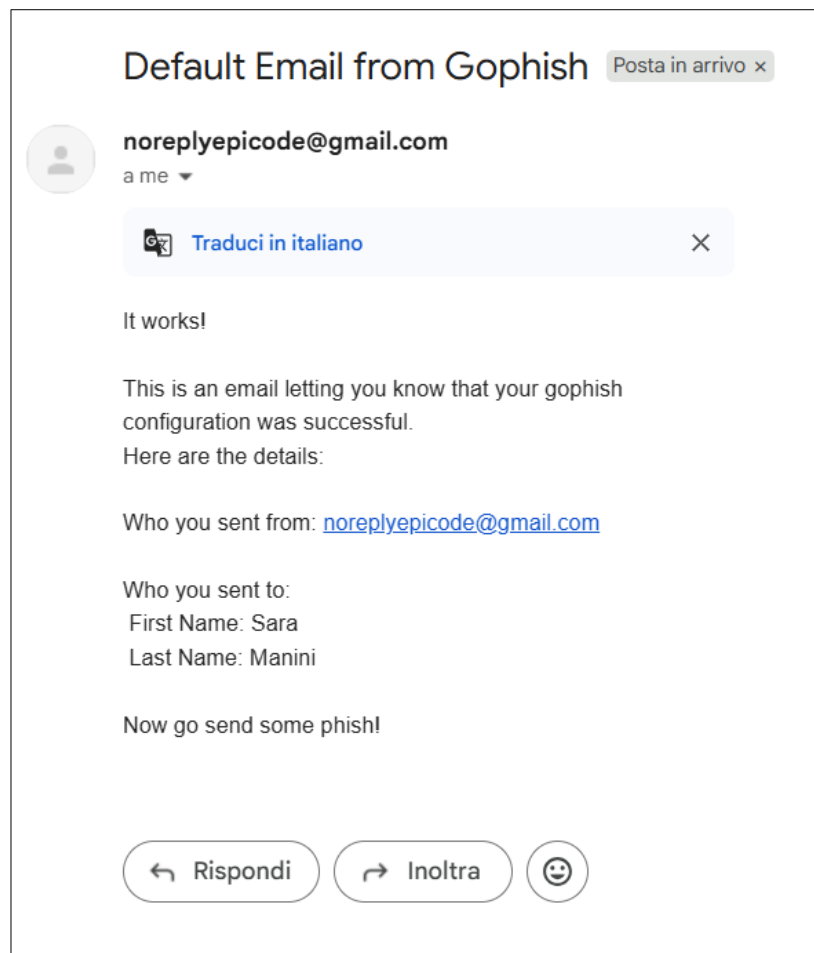
Email Headers:

X-Custom-Header

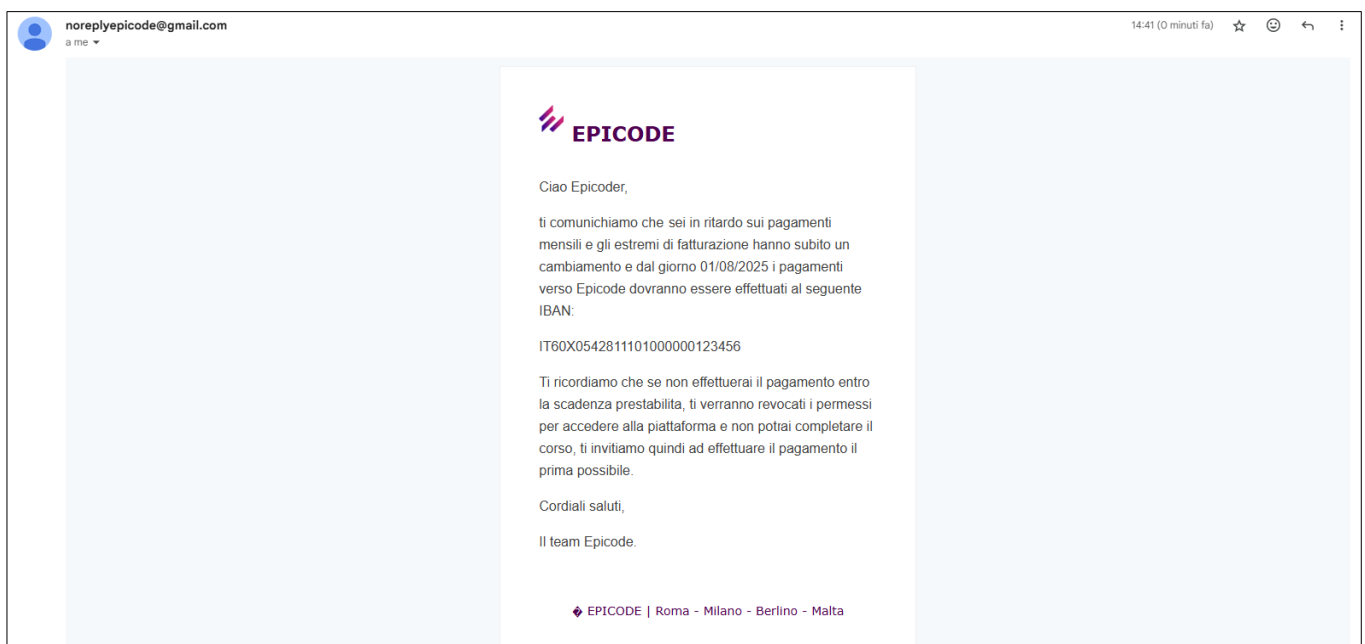
{{.URL}}-gophish

+ Add Custom Header

Step 6 Inviando una mail di test per controllare che tutto sia andato a buon fine.



Step 7 Possiamo ora far partire una campagna di phishing con le impostazioni selezionate in precedenza.



SET (Social Engineering Toolkit)

SET è un tool che troviamo già installato su Kali che permette di creare pagine di phishing e altri servizi legati al social engineering.

Step 1 Avviamo il programma e come da istruzioni andiamo a selezionare le seguenti opzioni:

- 1 – Social engineering attacks;
- 2 – Website Attack Vectors;
- 3 – Credentials Harvester Attack Method;
- 2 – Site Cloner.

```

.. ##### .. ##### .. #####
.##.....##.##.....## ...
.##.....##.##.....## ...
.. ##### .. ##### .. #####
.##.....##.##.....## ...
.##.....##.##.....## ...
.##.....##.##.....## ...
.. ##### .. ##### .. #####

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://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 PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

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

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
```

Step 2 Andiamo a digitare il nostro stesso IP così che le credenziali ci vengano automaticamente inviate e selezioniamo il sito web da clonare, visto lo scopo didattico dell'esercizio è stato di nuovo scelto VulnWeb.

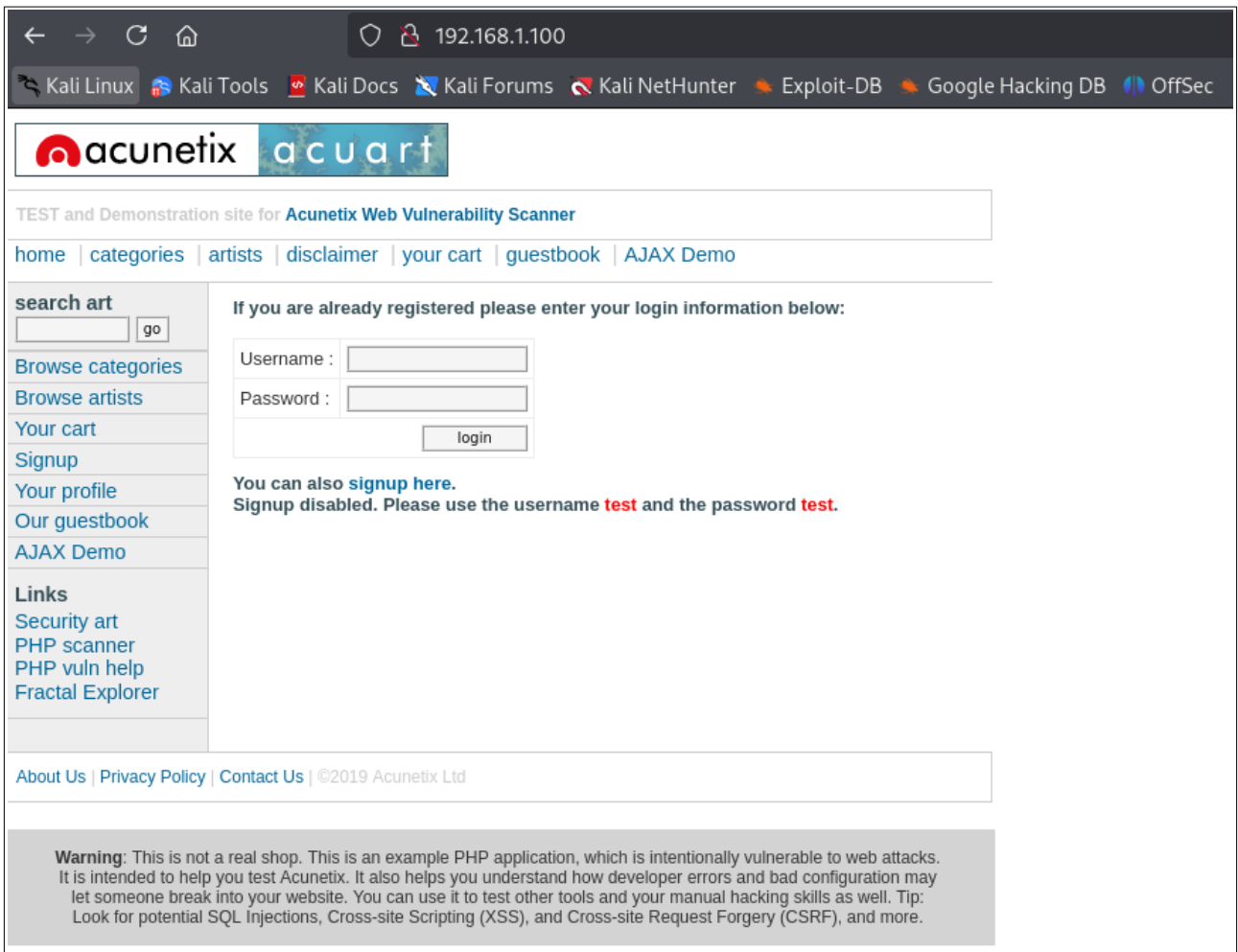
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.100]: 192.168.1.100
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] 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:
```

Step 3 Ora se da browser andremo a digitare l'IP della VM di Kali, visualizzeremo la pagina login di VulnWeb.

Inseriamo delle credenziali fittizie nei campi appositi.



← → ↻ 🏠 192.168.1.100

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

acunetix **acuart**

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.

Step 4 Tornando sul terminale precedente, vedremo stampate a schermo le credenziali che abbiamo appena inserito sulla pagina web clonata.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.100]: 192.168.1.100
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] 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. Check the help screen for more details. You should understand how webserver errors and bad configurations may
[*] The Social-Engineer Toolkit Credential Harvester Attack uses hacking skills as well. Tip
[*] Credential Harvester is running on port 80. It can also perform Cross-Site Scripting (XSS), and more.
[*] Information will be displayed to you as it arrives below:
192.168.1.100 - - [01/Aug/2025 08:50:37] "GET / HTTP/1.1" 200 -
192.168.1.100 - - [01/Aug/2025 08:50:38] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=Mario
POSSIBLE PASSWORD FIELD FOUND: pass=Sottolio
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```


Facoltativo

Facciamo svolgere un'analisi della mail di phishing creata con Gophish ad una AI.

Se visualizziamo il messaggio originale della mail possiamo vedere che sia SPF che DKIM e DMARC hanno la dicitura PASS, la mail ha quindi eluso questi sistemi di controllo, un'analisi più approfondita dell'header e del corpo però mostra che la mail è facilmente riconoscibile come sospetta.

Messaggio originale	
ID messaggio	<1754052214335267500.3720.4663848286171111202@WIN10>
Creato alle:	1 agosto 2025 alle ore 14:43 (consegnato dopo 2 secondi)
Da:	noreplyepicode@gmail.com Tramite gophish
A:	Sara Manini <saram.manini@gmail.com>
Oggetto:	Ritardo nei pagamenti
SPF:	PASS con l'IP 209.85.220.41 Ulteriori informazioni
DKIM:	'PASS' con il dominio gmail.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

[Scarica messaggio originale](#)[Copia negli appunti](#)

Di seguito gli indicatori di phishing forniti dall'analisi con AI:

- Mittente sospetto, l'email non arriva da un dominio ufficiale di Epicode;
- Strumento usato: l'email è stata inviata tramite Gophish;
- Richiesta di pagamento con nuovo IBAN, tipico segno di una frode finanziaria;
- Link sospetto, il link contenuto rimanda a VulWeb, un sito per test di vulnerabilità e non per pagamenti ufficiali;
- Tono di urgenza, le mail di phishing usano spesso la tattica di minacciare la vittima se non segue le istruzioni riportate nella mail, per infondere un senso di fretta e mandare così nel panico la vittima.