Phishing Attack

Phishing Attacks: Recognize, Prevent, and Respond

Habib Ullah

23 Aug 2023

Define phishing attacks

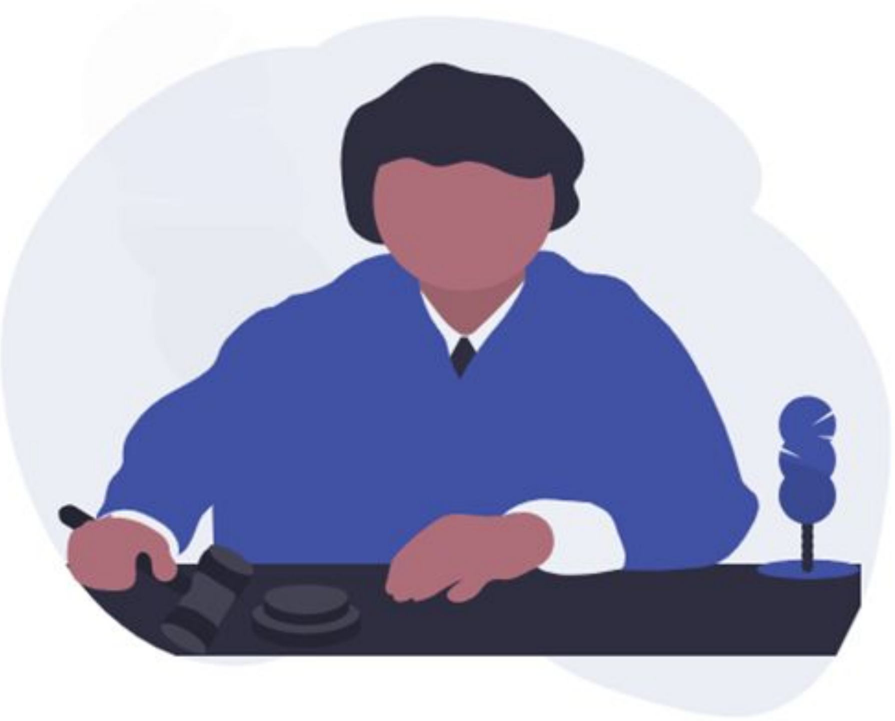
Phishing attacks are a popular attack vector for cyber criminals because they are simple and effective. A well-crafted phishing email is much easier to develop than a zero-day exploit yet can have the same negative impact. These attacks are designed to prey upon human nature. People want to be helpful, obey authority, and are more likely to be less careful when in a hurry or experiencing stress.

Recognizing Scam

let's watch a short video how to recognise a Scam

https://www.cyber.gov.au/learn-basics/explore-basics/recognise-and-report-scams

Common things scammers do to trick you



- **Authority:** Is the message claiming to be from someone official?

Like your bank, a government department, a utility company, your doctor or a solicitor. Criminals pretend to be important people or organisations to trick you into doing what they want.

E.g.: I am calling you from ATO, and you have not paid your tax. pay it now otherwise, police will come to arrest you.

Urgency

- `

Are you told you have a limited time to respond?

For example, 'within 24 hours' or 'immediately'. Criminals often threaten you with fines or other negative consequences.

- Often, they'll claim you have to act now to claim a reward or avoid a penalty.
- E.g.: Act now to get 70% discount.

Emotion

- **Does the message make you panic, fearful, hopeful or curious?**

- Scammers use threatening language, make false claims of support, or tease you into wanting to find out more.

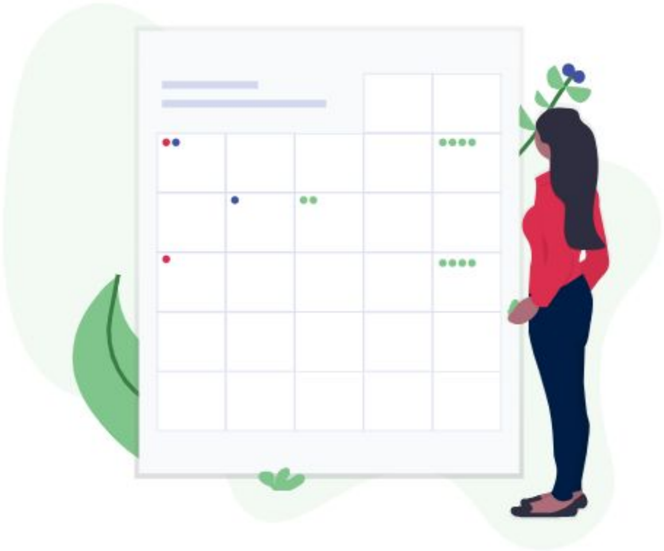
- Threatening police action, threatening to withhold money or lock your bank accounts are common.

Scarcity

- Is the message offering something that seems too good to be true?

- Like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

- E.g.: free Taylor Swift concert tickets



Current Events

- Are you expecting to see a message like this?

- To make their scam seem more real, criminals can exploit current news stories and events.

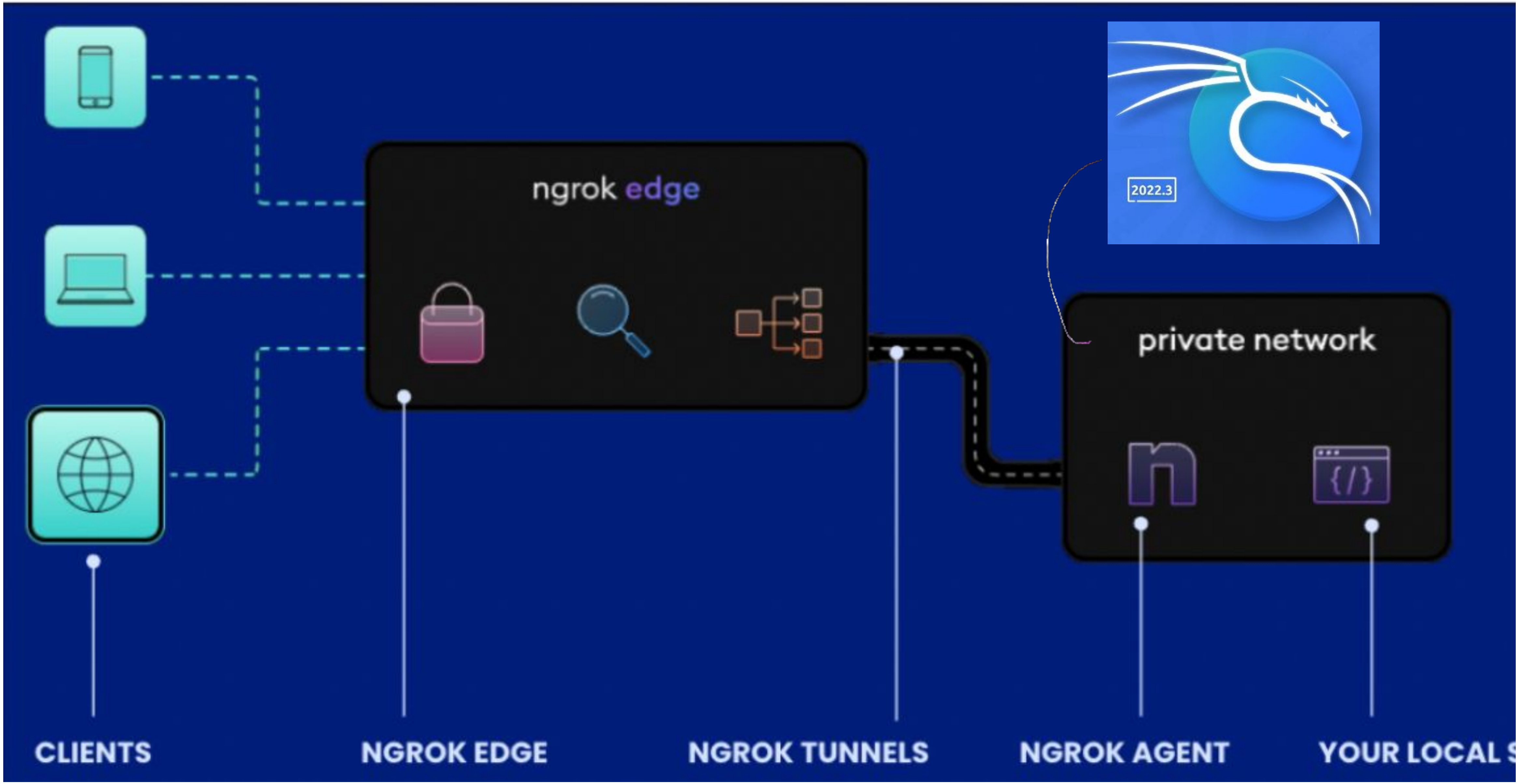
- For example, some scammers pretend to be from the DHL office to make their scam seem more relevant, and you received a text message, your delivery is on the way.

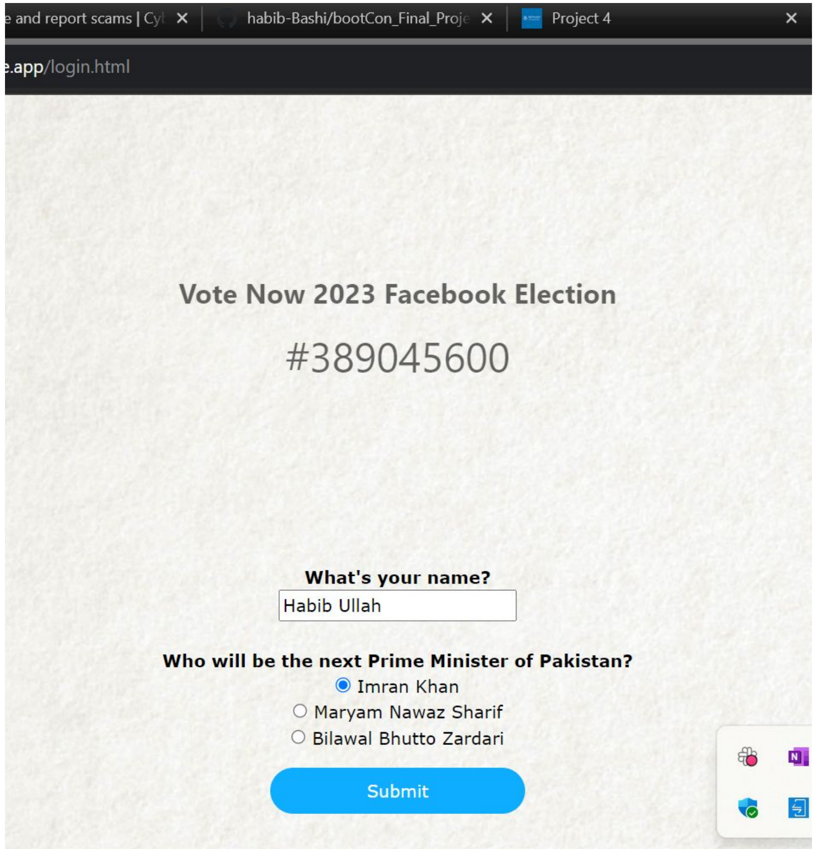
NETWORK DIAGRAM BOOTCON PROJECT

TOOLS USED:

Ngrok, Apache Web Server and VS CODE

Programming Language: PHP


ngrok edge
2022.3
private network
CLIENTS
NGROK EDGE
NGROK TUNNELS
NGROK AGENT
YOUR LOCAL S



Vote Now 2023 Facebook Election

#389045600

What's your name?

Habib Ullah

Who will be the next Prime Minister of Pakistan?

● Imran Khan

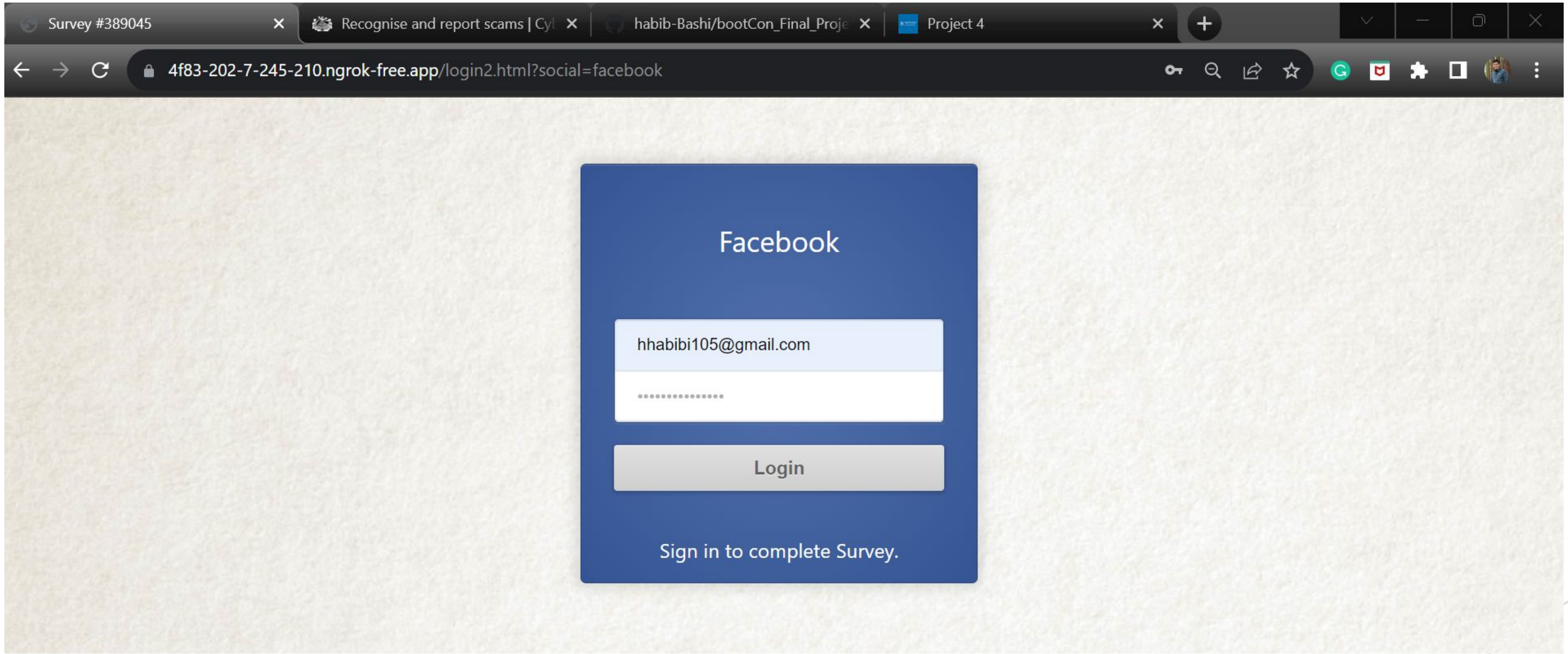
○ Maryam Nawaz Sharif

○ Bilawal Bhutto Zardari

Let's do some Demo

Login Page

Face Book Login


Survey #389045
Recognise and report scams | Cy
habib-Bashi/bootCon_Final_Proje
Project 4
4f83-202-7-245-210.ngrok-free.app/login2.html?social=facebook

Facebook

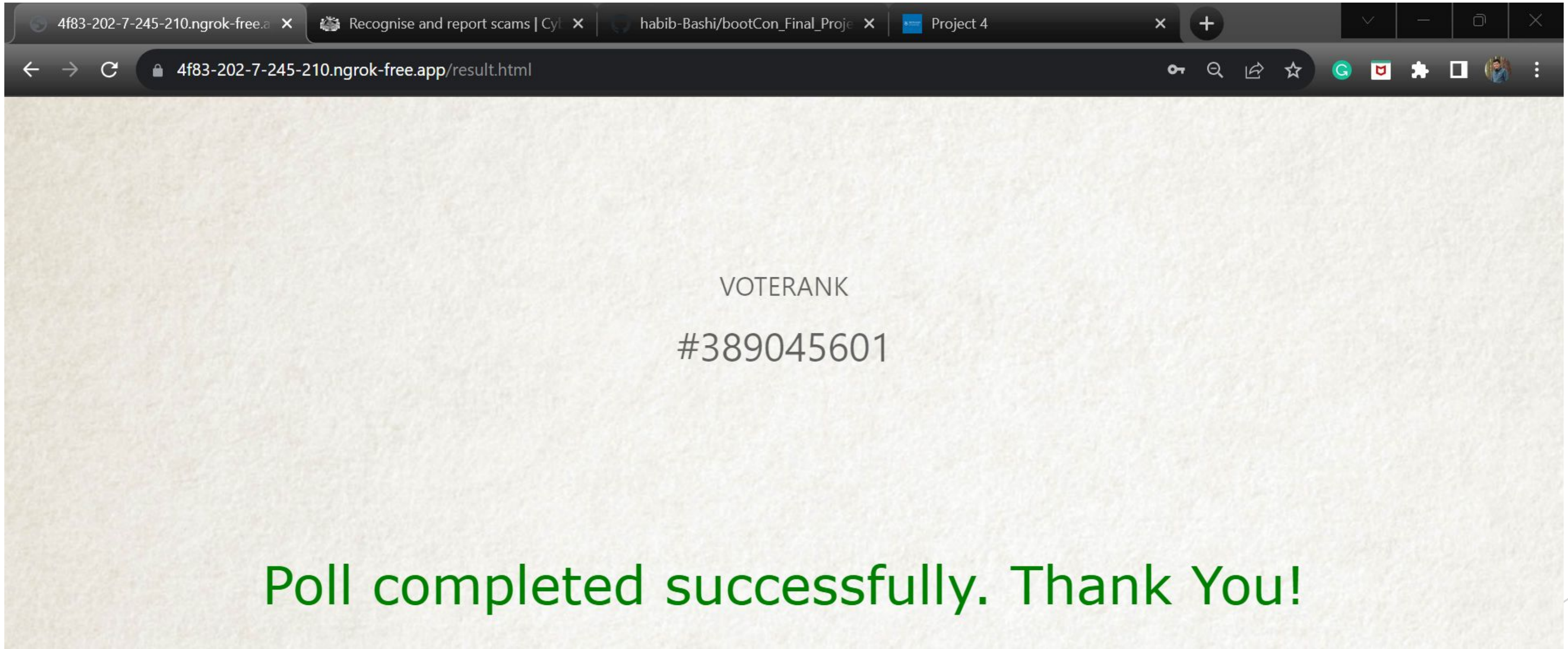
hhabibi105@gmail.com

•••••••••••••••

Login

Sign in to complete Survey.

Result Page



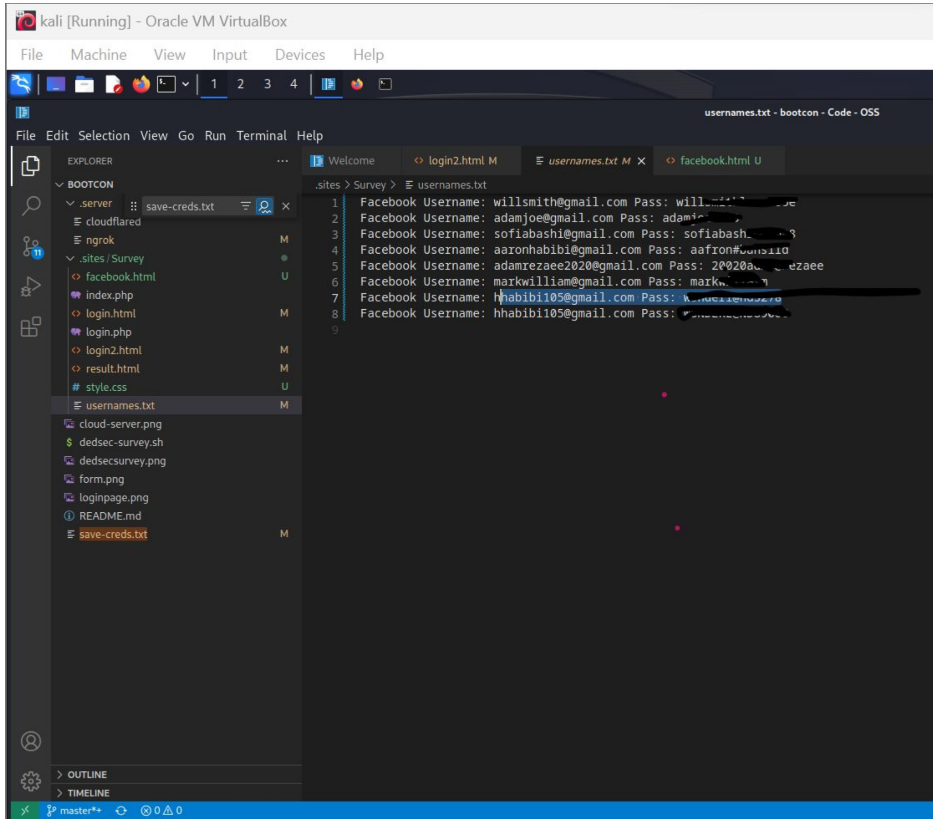
4f83-202-7-245-210.ngrok-free.a
Recognise and report scams | Cy
habib-Bashi/bootCon_Final_Proje
Project 4
4f83-202-7-245-210.ngrok-free.app/result.html

VOTERANK

#389045601

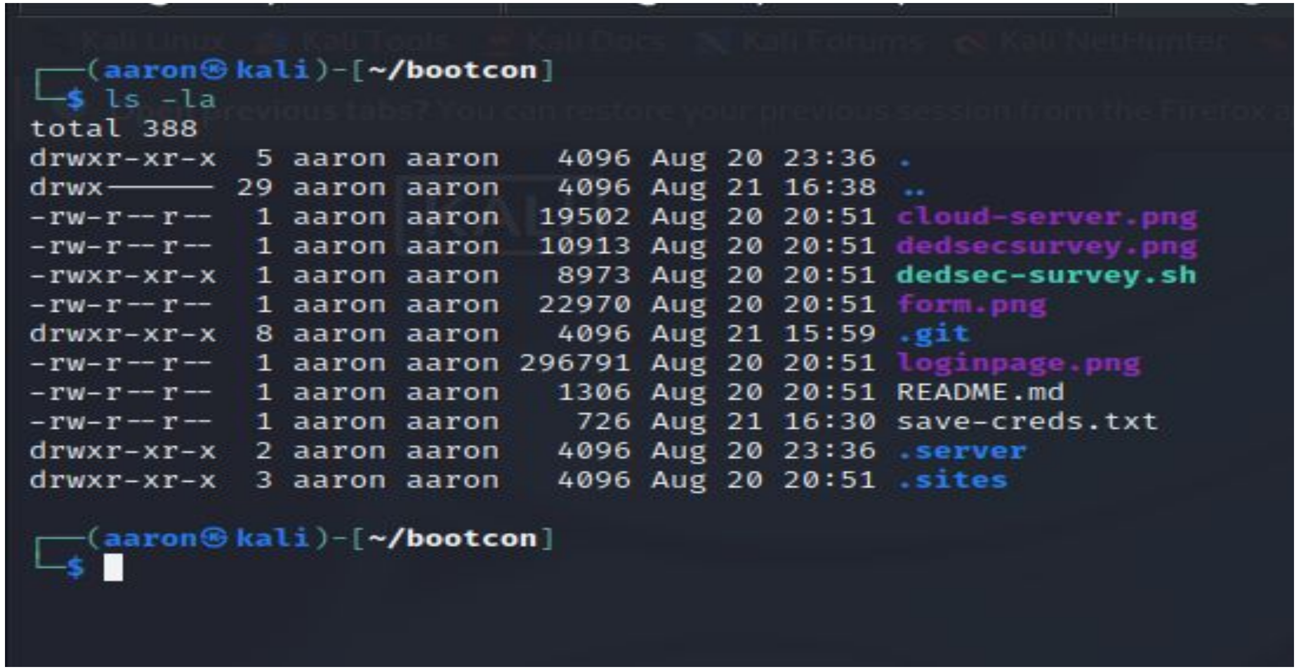
Poll completed successfully. Thank You!

VS Code



```
Facebook Username: willsmith@gmail.com Pass: will[redacted]
Facebook Username: adamjoe@gmail.com Pass: adam[redacted]
Facebook Username: sofiabashi@gmail.com Pass: sofiabash[redacted]
Facebook Username: aaronhabibi@gmail.com Pass: aafron#[redacted]
Facebook Username: adamrezaee2020@gmail.com Pass: 20020a[redacted]
Facebook Username: markwilliam@gmail.com Pass: mark[redacted]
Facebook Username: hhabibi105@gmail.com Pass: [redacted]
Facebook Username: hhabibi105@gmail.com Pass: [redacted]
```

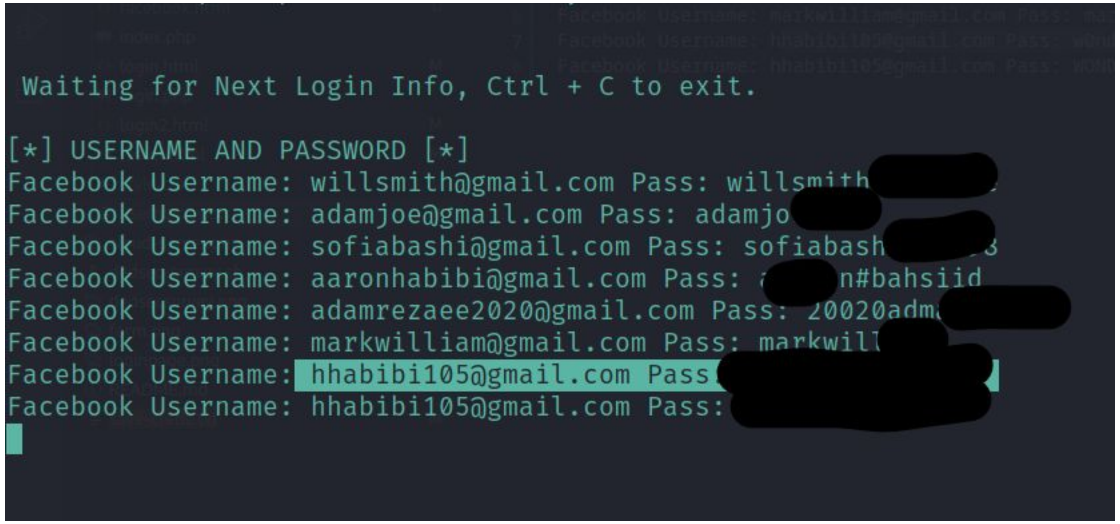
Project Files



```
┌──(aaron㉿kali)-[~/bootcon]
└─$ ls -la
total 388
drwxr-xr-x  5 aaron aaron   4096 Aug 20 23:36 .
drwx------ 29 aaron aaron   4096 Aug 21 16:38 ..
-rw-r--r--  1 aaron aaron  19502 Aug 20 20:51 cloud-server.png
-rw-r--r--  1 aaron aaron  10913 Aug 20 20:51 dedsecsurvey.png
-rwxr-xr-x  1 aaron aaron   8973 Aug 20 20:51 dedsec-survey.sh
-rw-r--r--  1 aaron aaron  22970 Aug 20 20:51 form.png
drwxr-xr-x  8 aaron aaron   4096 Aug 21 15:59 .git
-rw-r--r--  1 aaron aaron 296791 Aug 20 20:51 loginpage.png
-rw-r--r--  1 aaron aaron   1306 Aug 20 20:51 README.md
-rw-r--r--  1 aaron aaron    726 Aug 21 16:30 save-creds.txt
drwxr-xr-x  2 aaron aaron   4096 Aug 20 23:36 .server
drwxr-xr-x  3 aaron aaron   4096 Aug 20 20:51 .sites

┌──(aaron㉿kali)-[~/bootcon]
└─$ 
```

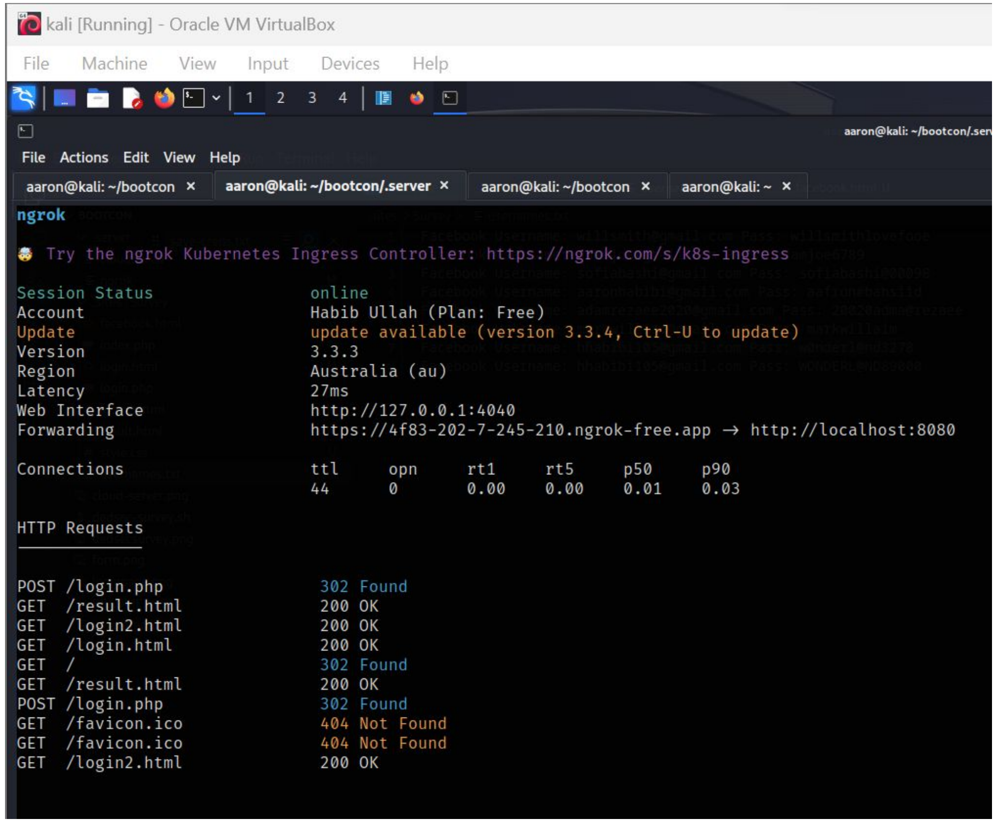
User Credentials Captured Runtime



```
 Waiting for Next Login Info, Ctrl + C to exit.

[*] USERNAME AND PASSWORD [*]
Facebook Username: willsmith@gmail.com Pass: willsmith[redacted]
Facebook Username: adamjoe@gmail.com Pass: adamjo[redacted]
Facebook Username: sofiabashi@gmail.com Pass: sofiabash[redacted]
Facebook Username: aaronhabibi@gmail.com Pass: a[redacted]n#bahsiid
Facebook Username: adamrezaee2020@gmail.com Pass: 20020adm[redacted]
Facebook Username: markwilliam@gmail.com Pass: markwill[redacted]
Facebook Username: hhabibi105@gmail.com Pass[redacted]
Facebook Username: hhabibi105@gmail.com Pass: [redacted]
```

Ngrok Agent Session Info


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
aaron@kali: ~/bootcon/.serv
File Actions Edit View Help
aaron@kali: ~/bootcon ×
aaron@kali: ~/bootcon/.server ×
aaron@kali: ~/bootcon ×
aaron@kali: ~ ×

```
ngrok

🤠 Try the ngrok Kubernetes Ingress Controller: https://ngrok.com/s/k8s-ingress

Session Status                online
Account                       Habib Ullah (Plan: Free)
Update                        update available (version 3.3.4, Ctrl-U to update)
Version                       3.3.3
Region                        Australia (au)
Latency                       27ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://4f83-202-7-245-210.ngrok-free.app -> http://localhost:8080

Connections                   ttl     opn     rt1     rt5     p50     p90
                              44      0       0.00    0.00    0.01    0.03

HTTP Requests
-------------

POST /login.php                302 Found
GET  /result.html              200 OK
GET  /login2.html              200 OK
GET  /login.html               200 OK
GET  /                         302 Found
GET  /result.html              200 OK
POST /login.php                302 Found
GET  /favicon.ico              404 Not Found
GET  /favicon.ico              404 Not Found
GET  /login2.html              200 OK
```

Mitigations Strategies

User Education and Training: Phishing awareness training is paramount because human error is often the weakest link in cybersecurity. Educate and empower your employees to recognize and respond to phishing attempts effectively.

Email Filtering and Authentication: Implement robust email filtering to block known phishing emails and attachments. Additionally, enforce email authentication protocols (DMARC, SPF, and DKIM) to prevent email spoofing.

Multi-Factor Authentication (MFA): Require MFA for accessing critical accounts and systems. MFA adds an additional layer of security, making it significantly harder for attackers to gain unauthorized access.

These three measures address the human factor (user training), email-based attack vectors (email filtering and authentication), and unauthorized access (MFA), which are some of the most common entry points for phishing attacks. However, a comprehensive security strategy should ideally incorporate multiple layers of defense for robust protection.

Final Part of my Presentation (Video File)

- Please find a video (bootCon.mp4) file in a shared directory called Habib_Ullah_BootCon_Presentation.