GAJABAAR

An InfoSecurity Mentorship: Design To Deployment

Presenter: Prasant Adhikari

FAQ: Is it …

गाँजाबार? (weed-bar?)

✗

FAQ: Is it …

गाँजाबार? (weed-bar?)

✗

गजबार?

✓

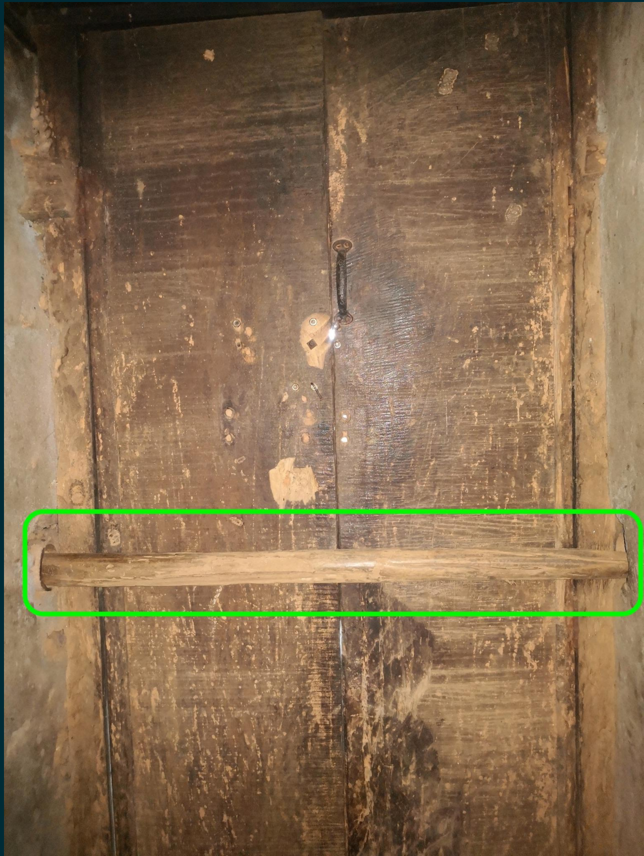
FAQ: Is it ...

गाँजाबार? (weed-bar?)

✗

गजबार?

✓



Part I: All About Gajabaar

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

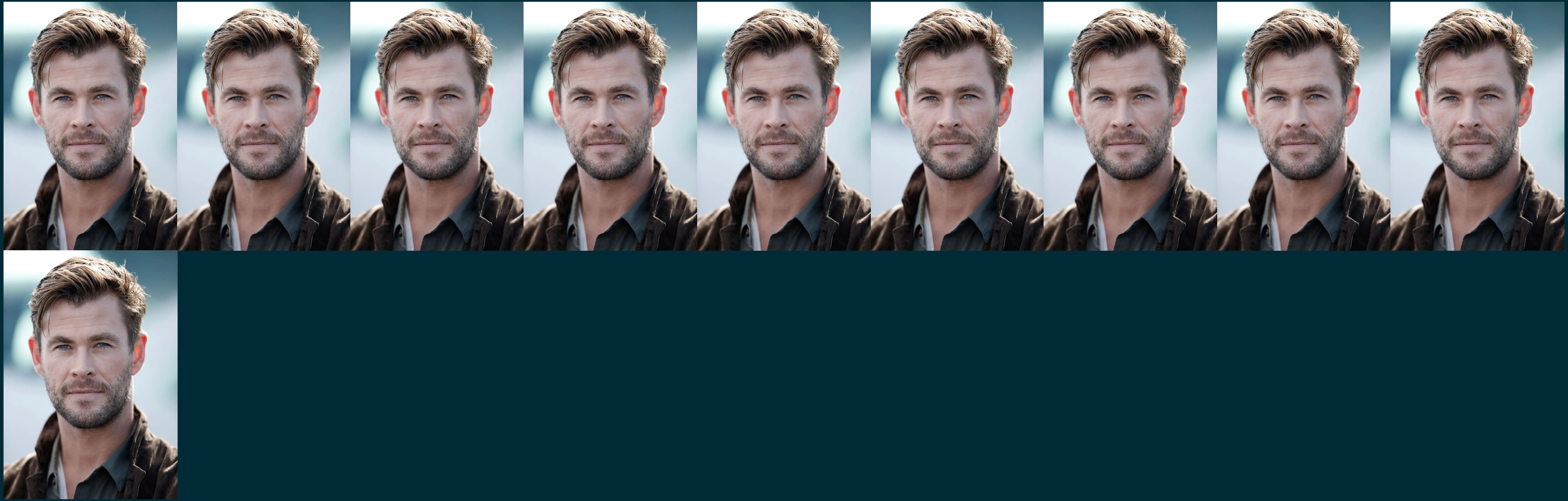
Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

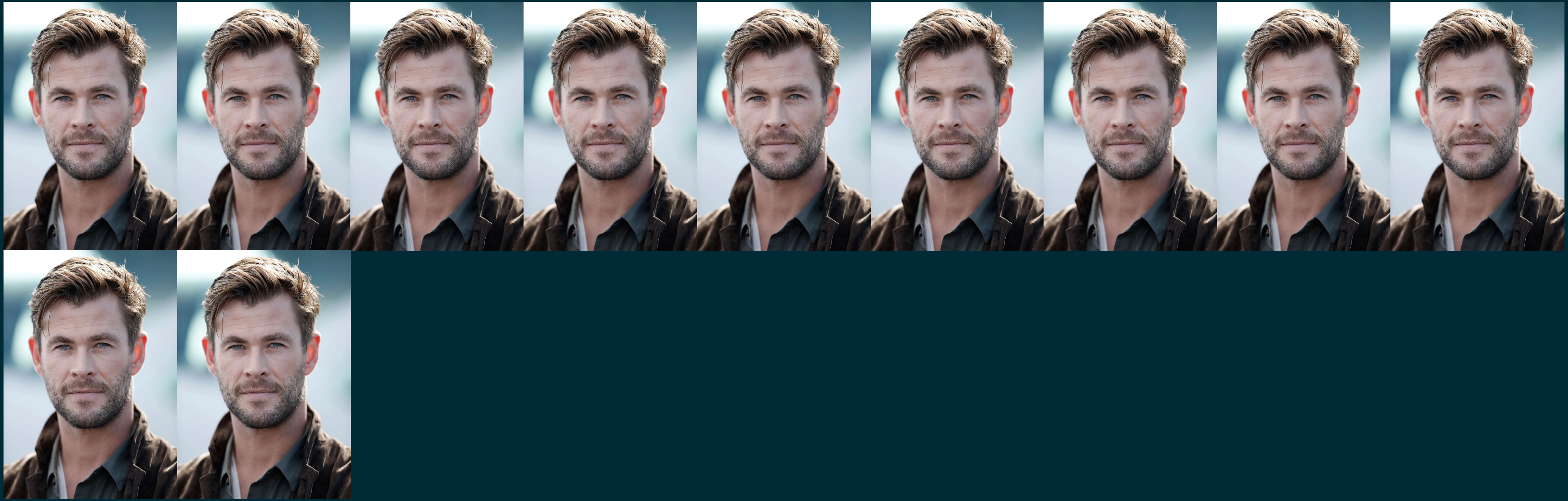
Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

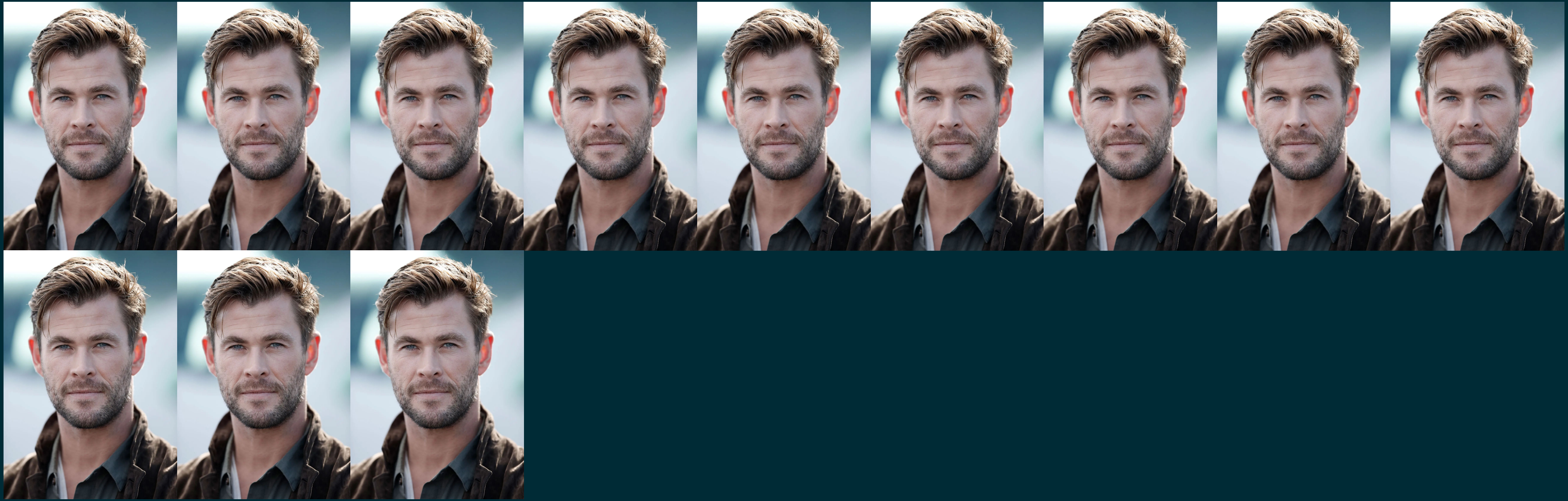
Origins: Jan 2020 - Wordcamp Butwal



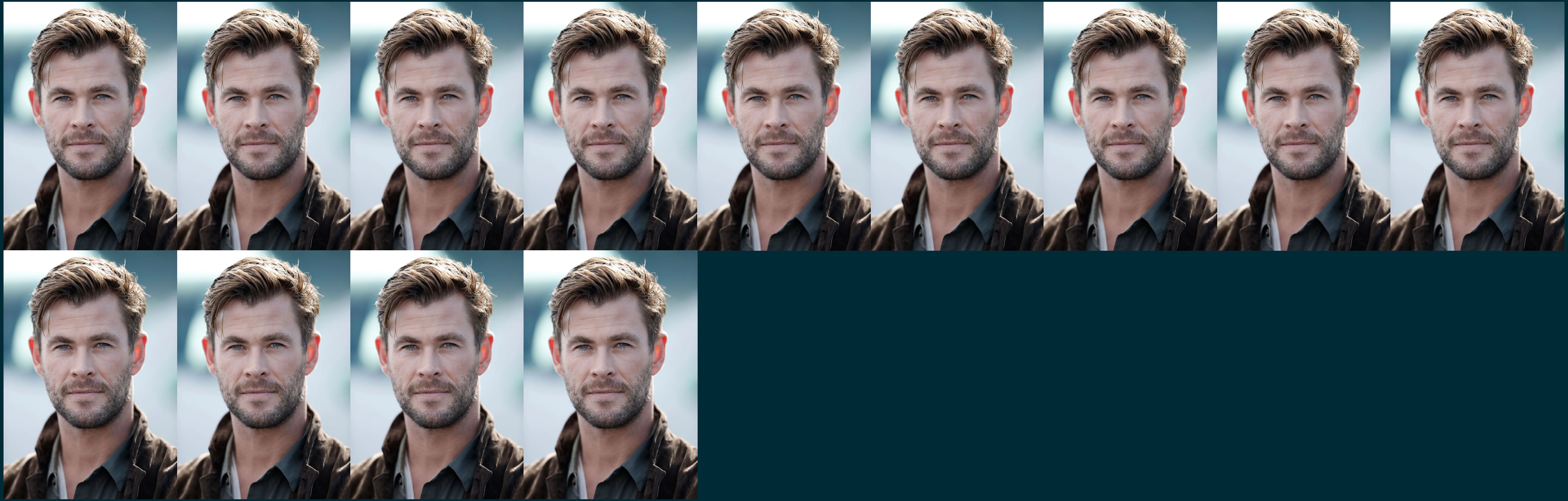
Origins: Jan 2020 - Wordcamp Butwal



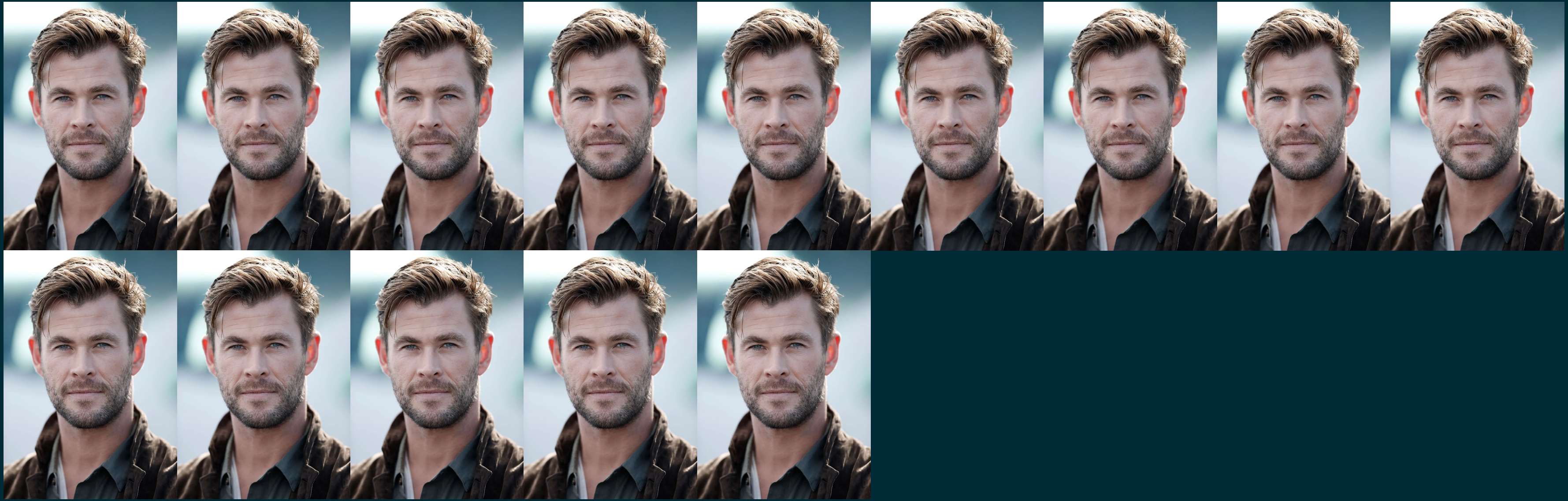
Origins: Jan 2020 - Wordcamp Butwal



Origins: Jan 2020 - Wordcamp Butwal



Origins: Jan 2020 - Wordcamp Butwal



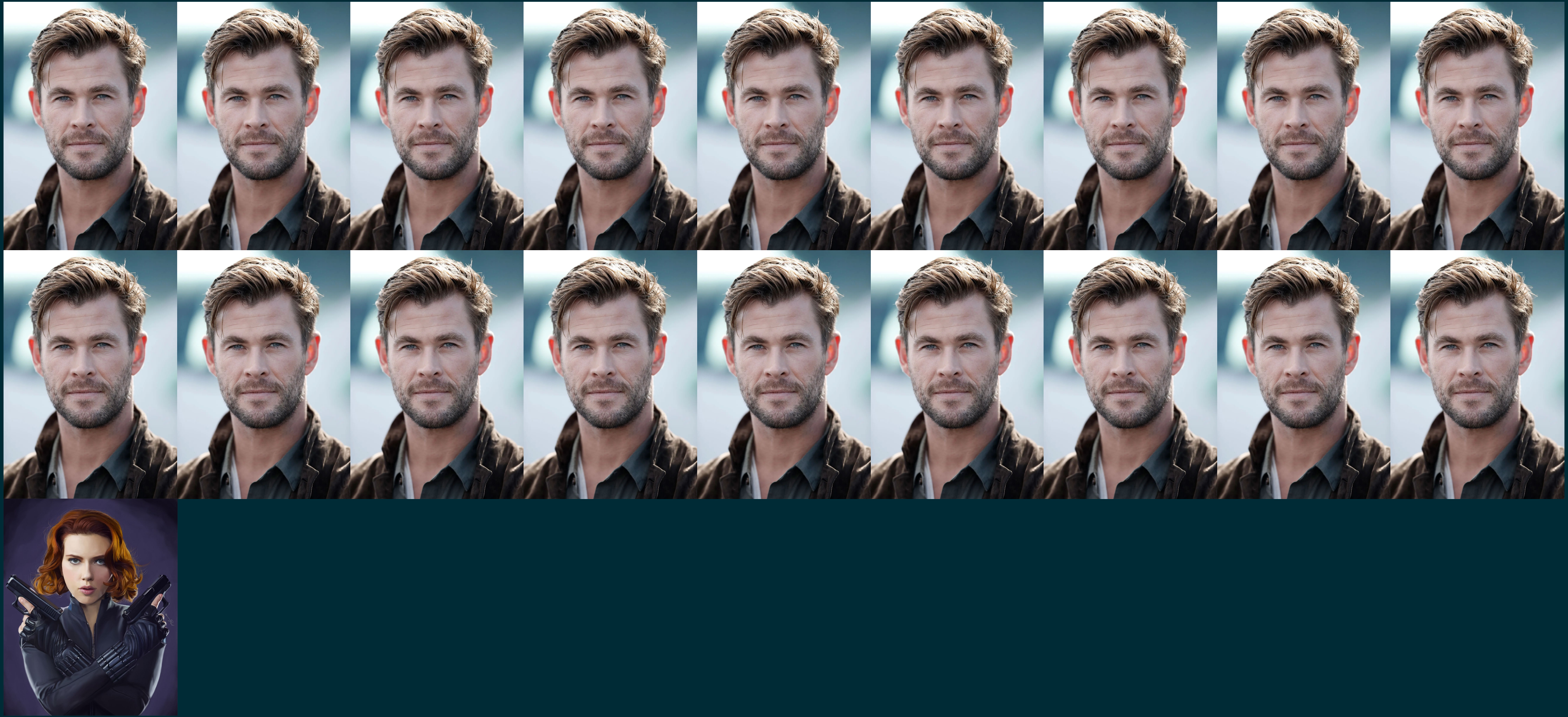
Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

Origins: Jan 2020 - Wordcamp Butwal

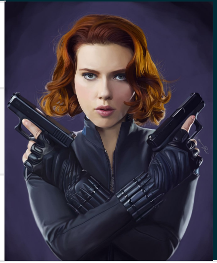
Origins: Jan 2020 - Wordcamp Butwal



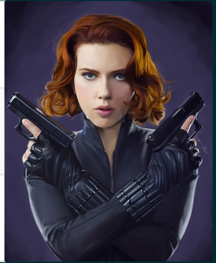
ASM: Feb 2022

Prasant Adhikari
likes language and literature
PhD student @NYU Center For Cybersecurity

Pratima Sharma
writer, story-teller and entrepreneur
CEO @Mandala IT Solutions



Rashmi Lamichhane
likes drawing and sports
Analyst @DB Schenker



whois gajabaar.io

```
. . .
# whois.namecheap.com

Domain name: gajabaar.io
Registry Domain ID: 20a2e9db176a48719495a327664c54bc-DONUTS
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2022-02-02T15:02:26.33Z
Creation Date: 2020-02-21T13:49:40.09Z
. . .
```

git commit-ed

```
commit 4b6d99fc60be873cf499681ca57587bdc1cb8ffe
Author: Prasant Adhikari <pa1038@nyu.edu>
Date:   Fri Feb 21 20:11:22 2020 -0500

    Initial commit


. . .
+++ b/README.md
@@ -0,0 +1,2 @@
+# gajabaar
+An Information Security Mentorship Program
```

Peer Selection: Non-Technical Q1

`Tell us about a time when you learned something on your own. (300 words max.)`

It might help you to think about the following while answering:

- How did you find the resources?
- What were the challenges?
- What would have made it easier?

As long as your answer shows your approach to learning, do not worry about answering each sub-question.

Peer Selection: Non-Technical Q2

Tell us how you retain information that you have learned. (300 words max.)

The mentors agree that we tend to forget what we have learned in the past. Going into the program, we would like to know how you would keep track of things you have learned and things you would like to explore further.

Instead of a text response, you may also choose to send us a picture/screenshot of your notes on a particular topic you have learned (about computers or otherwise) or send links to your blog/vlog.

Do not fret about the form of submission as long as it shows the way you track your own knowledge-base. (example: a picture of a page from your notebook does not have a disadvantage over a blog submission from another application.)

Peer Selection: Technical Q1

Capture the Flag (CTF) is a competition that puts together a set of security puzzles that you can solve to get points. Here's an excellent introduction to CTF by LiveOverflow. You do not need to know everything in the video, just a sense of what a CTF is.

Headover to CTFTIME.org. The site hosts information about CTFs happening around the world, the challenges designed for those CTFs and the solutions after the CTF is over.

Pick any challenge (one) from CTFTIME.org. Readup on the challenge and its solution (also called a write-up).

`In your own words, summarize the challenge and its solution.`

It might help to think about the following while answering:

- Name/Category/Link of the challenge
- What did the authors of the challenge want participants to learn/notice
- What did you learn in the process
- What are ideas you are still unclear about in the challenge

Do not worry about the sophistication of the challenge you pick or not knowing everything in the solution. Just walk us through your thought-process/understanding.

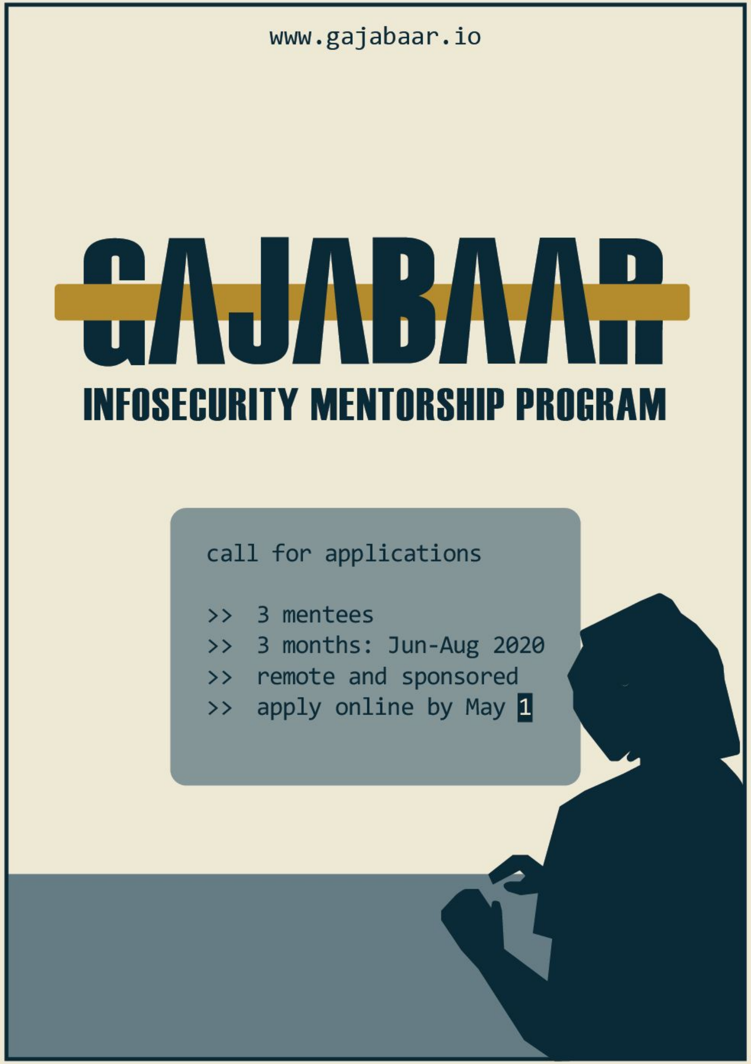
Peer Selection: Technical Q2

Nmap is a tool commonly used to map a network and find vulnerable hosts. An output from nmap looks like the following:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-22 13:26 EST
. . .
Scanning localhost (127.0.0.1) [65535 ports]
Discovered open port 4330/tcp on 127.0.0.1
Discovered open port 9050/tcp on 127.0.0.1
Discovered open port 902/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 4000/tcp on 127.0.0.1
Discovered open port 43435/tcp on 127.0.0.1
Discovered open port 18083/tcp on 127.0.0.1
Discovered open port 44321/tcp on 127.0.0.1
Discovered open port 44322/tcp on 127.0.0.1
Discovered open port 43291/tcp on 127.0.0.1
```

Write a program in a programming language of your choice that takes the above output (in a file or as a string) and prints out the port numbers separated by a comma.

Call for Application: March 2020



www.gajabaar.io

GAJABAAR

INFOSECURITY MENTORSHIP PROGRAM

call for applications

```
>>  3 mentees
>>  3 months: Jun-Aug 2020
>>  remote and sponsored
>>  apply online by May 1
```

Call for Application: 2021

GAJABAAR

INFOSECURITY MENTORSHIP

Remote. Tailored. Sponsored.

Apply online @ gajabaar.io

Call for Application: 2022

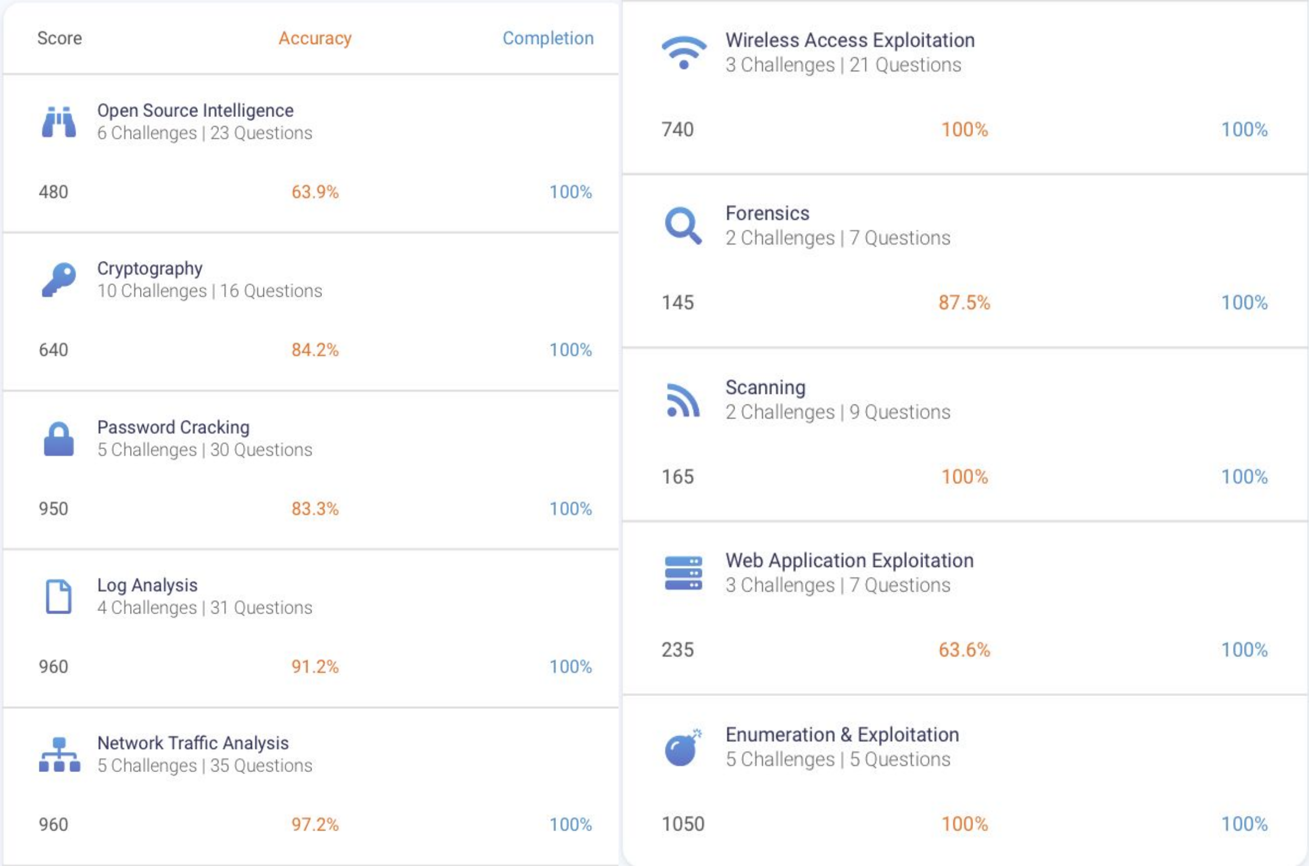
Peer Selection: Interview

- *(Find a quick-unintrusive way of indicating I will be taking notes, hence typing, during the interview)*
- Introduce myself . The most relevant bits are probably name, hometown, education, current position. ~2 min (x2)
- Introduce the program. Focus on the FAQ bits. CyberSecurity, BeginnerFriendly, Responsive, Sponsored. ~2 min
- Tell us a little about yourself. ~3 min
- How did you find out about the program? ~1 min
    - Ask about the interest in security. ~1 min
- How does the program align with your current-interest/future-goals? Or What are your hopes from the program? (Check which one sounds better and go with it) ~5 min
    - Try to get a sense of how much time they are willing/able to commit
- We will also ask this later. We want to ask you a few questions with specifics about your application. Do you have any questions for us at this point?
    - . . .

Curriculum I: The Summer

- OverTheWire bandit
- OverTheWire redtiger
- OverTheWire natas
- Cryptopals
- TryHackMe Advent Of Cyber
- picoCTF
- googleCTF

Curriculum II: National Cyber League

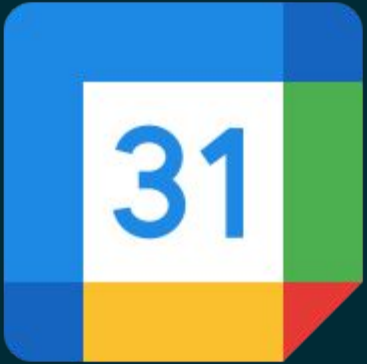


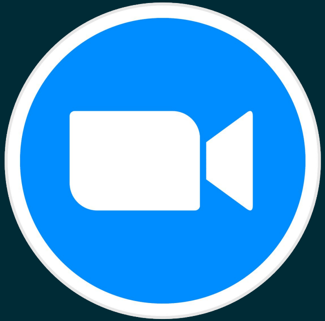
<table>
<tr><th></th><th>Score</th><th>Accuracy</th><th>Completion</th></tr>
<tr><td>Open Source Intelligence
6 Challenges | 23 Questions</td><td>480</td><td>63.9%</td><td>100%</td></tr>
<tr><td>Cryptography
10 Challenges | 16 Questions</td><td>640</td><td>84.2%</td><td>100%</td></tr>
<tr><td>Password Cracking
5 Challenges | 30 Questions</td><td>950</td><td>83.3%</td><td>100%</td></tr>
<tr><td>Log Analysis
4 Challenges | 31 Questions</td><td>960</td><td>91.2%</td><td>100%</td></tr>
<tr><td>Network Traffic Analysis
5 Challenges | 35 Questions</td><td>960</td><td>97.2%</td><td>100%</td></tr>
<tr><td>Wireless Access Exploitation
3 Challenges | 21 Questions</td><td>740</td><td>100%</td><td>100%</td></tr>
<tr><td>Forensics
2 Challenges | 7 Questions</td><td>145</td><td>87.5%</td><td>100%</td></tr>
<tr><td>Scanning
2 Challenges | 9 Questions</td><td>165</td><td>100%</td><td>100%</td></tr>
<tr><td>Web Application Exploitation
3 Challenges | 7 Questions</td><td>235</td><td>63.6%</td><td>100%</td></tr>
<tr><td>Enumeration &amp; Exploitation
5 Challenges | 5 Questions</td><td>1050</td><td>100%</td><td>100%</td></tr>
</table>

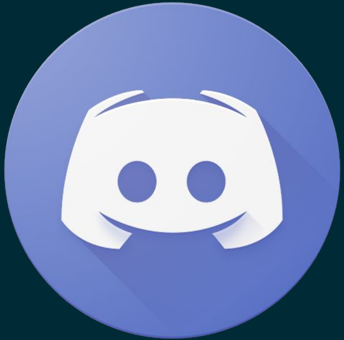
The Extra Curricular: Ad Hoc Support

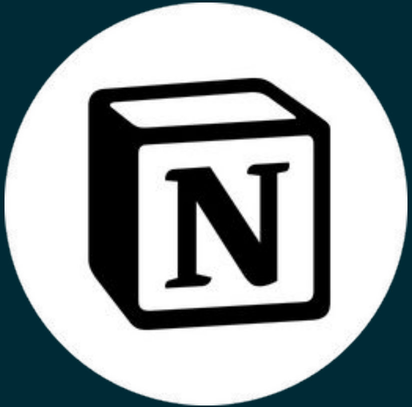
- BurpSuite Academy
- PentesterLab
- CryptoHack
- HackTheBox
- pwn.college
- The Missing Semester
- Subscriptions for Online Community
- Threatcon Tickets

The Internals









The Outcome: Testimonials I

In just a span of two odd months, I have learnt so much more about not just cyber-security but also computer science in general, about research, about self-studying, about analysis, and most importantly, about community.

The Outcome: Testimonials II

Throughout the journey, the mentors guided us as per our requirements and caliber. They knew what would be difficult for me and what would make my path easier.

The Outcome: Testimonials III

The concepts which might take you take months to get properly; Gajabaar makes it possible to learn within some weeks provided that you put the required effort.

The Outcome: By the numbers

- A total of 75 applications have been received. 100% applicants accepted.

The Outcome: By the numbers

- A total of 75 applications have been received. 100% applicants accepted.

- A total of 15 mentees have completed all labs. (2022 excluded)

The Outcome: By the numbers

- A total of 75 applications have been received. 100% applicants accepted.

- A total of 15 mentees have completed all labs. (2022 excluded)

- At least 7 of our alumni went on to have cyber-security jobs in at least four different companies around the Kathmandu Valley

The Cost

- 160 mentor hours per year
  - Includes material design, prep time for lecture meetings, office hours and feedback on submissions.

- 250$ per year
  - Includes THM/HTB/NCL subscriptions along with an attack server and DNS renewals.

The Future

- Certification Mentorship
  - OSCP (CEH, CRTP)
  - Funding

The Future

- Certification Mentorship
  - OSCP (CEH, CRTP)
  - Funding
- Connecting Mentees with Jobs
  - Connecting with companies on what the market needs are

The Future

- Certification Mentorship
  - OSCP (CEH, CRTP)
  - Funding
- Connecting Mentees with Jobs
  - Connecting with companies on what the market needs are
- Finding a local anti-harassment module

Part II: The Macro Picture

Word to the Mentors: Define the Scope

Word to the Mentors: Define the Scope

- Studying Abroad

Word to the Mentors: Define the Scope

- Studying Abroad
- Career Counseling

Word to the Mentors: Define the Scope

- Studying Abroad
- Career Counseling
- Software Engineering/ Machine Learning/ Artificial Intelligence

Word to the Mentors: Expect a Wide Range of Exposure

- SSH (?) / Terminal (?)
- CTF (?)
- Inspect Element (?)
- Linux (?)

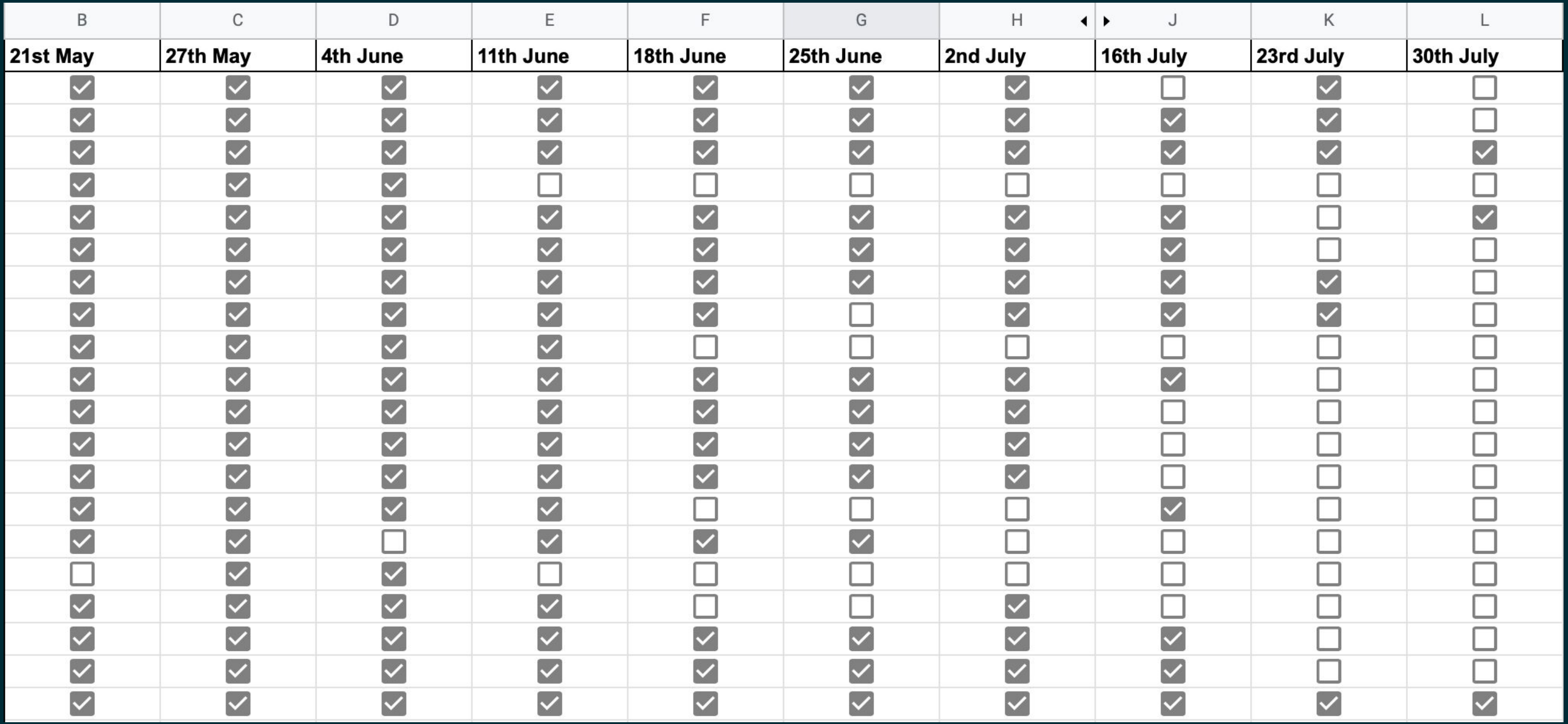
Word to the Mentors: Trust the Application

- The ones who accomplished the most were the ones who put in the work into the application.

Word to the Mentors: Have One-on-One Interview

- The mentees engagement during the program is heavily influenced by the initial interaction we had with them.

Word to the Mentors: Avoid the Exams



B	C	D	E	F	G	H	J	K	L
21st May	**27th May**	**4th June**	**11th June**	**18th June**	**25th June**	**2nd July**	**16th July**	**23rd July**	**30th July**
☑	☑	☑	☑	☑	☑	☑	□	☑	□
☑	☑	☑	☑	☑	☑	☑	☑	☑	□
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☑	☑	☑	□	□	□	□	□	□	□
☑	☑	☑	☑	☑	☑	☑	☑	□	☑
☑	☑	☑	☑	☑	☑	☑	☑	□	□
☑	☑	☑	☑	☑	☑	☑	☑	☑	□
☑	☑	☑	☑	☑	□	☑	☑	☑	□
☑	☑	☑	☑	□	□	□	□	□	□
☑	☑	☑	☑	☑	☑	☑	☑	□	□
☑	☑	☑	☑	☑	☑	☑	□	□	□
☑	☑	☑	☑	☑	☑	☑	□	□	□
☑	☑	☑	☑	☑	☑	☑	□	□	□
☑	☑	☑	☑	□	□	□	☑	□	□
☑	☑	□	☑	☑	☑	□	□	□	□
□	☑	☑	□	□	□	□	□	□	□
☑	☑	☑	☑	□	□	☑	□	□	□
☑	☑	☑	☑	☑	☑	☑	☑	□	□
☑	☑	☑	☑	☑	☑	☑	☑	□	□
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

A word to the Mentees

A word to the Mentees

Welcome

Questions / Comments / Concerns . . .

Questions / Comments / Concerns . . .

Thank you!