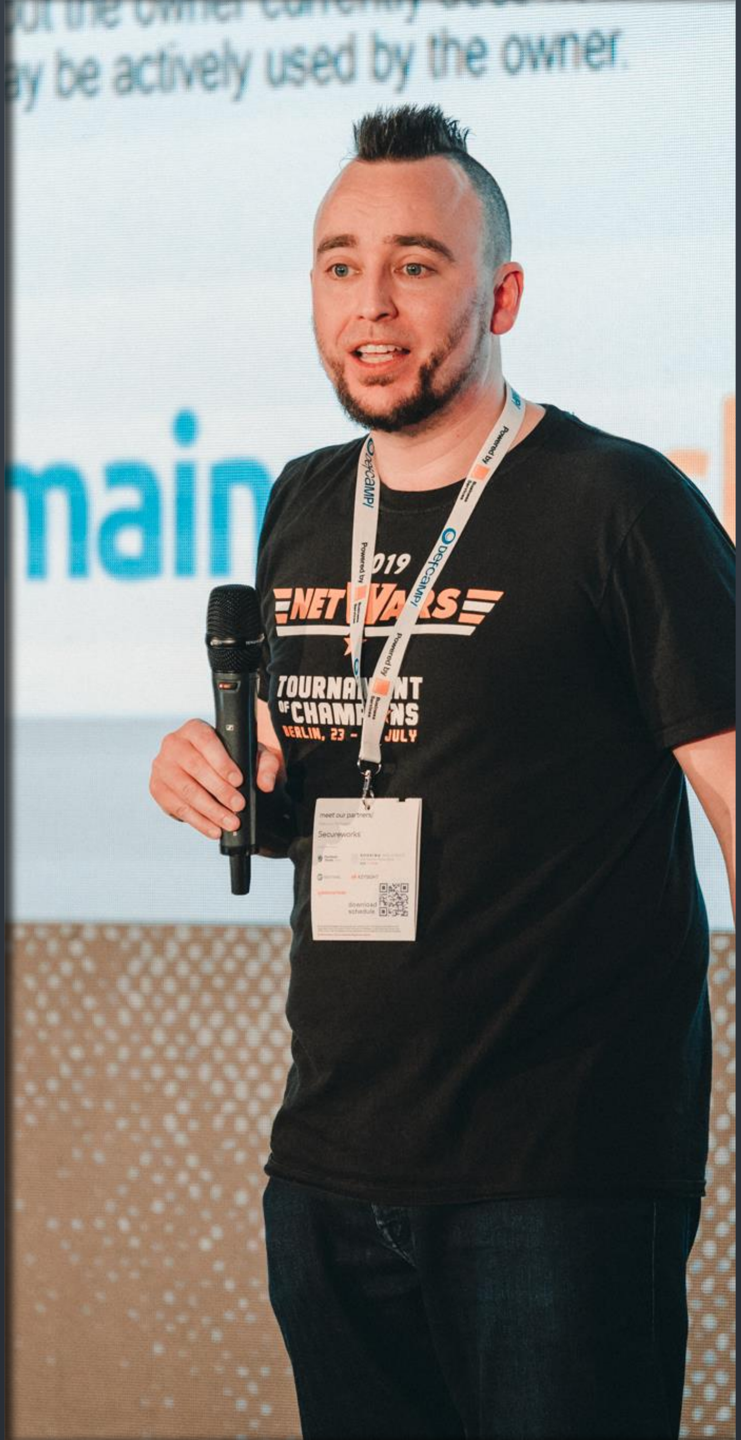
RIVER SECURITY

Enhancing Security Testing for QA Professionals



WHO AM I?

COO, PRINCIPAL AND FOUNDER AT RIVER SECURITY

PRINCIPAL INSTRUCTOR AT SANS

IN SHORT:

**I SHOW HOW CRIMINALS BREAK-IN,
AND I HELP THROW THEM BACK OUT…**

GCIH	GIAC Certified Incident Handler
GPEN	GIAC Certified Penetration Tester
GSLC	GIAC Security Leadership
GMOB	GIAC Mobile Device Security Analyst
GDAT	GIAC Defending Advanced Adversaries
GCTI	GIAC Cyber Threat Intelligence
GCFA	GIAC Certified Forensic Analyst
GXPT	GIAC Certified Penetration Tester

Agenda

Introduction to IT Security Testing

Why Security Testing Matters

The Evolving Threat Landscape

Understanding Security Vulnerabilities

Common Vulnerabilities and their implications

Real world breaches and lessons learned

Principles of Security Testing

Tools and techniques suited for testers

Black box vs. White box testing

Other Important Aspects

Best Practices

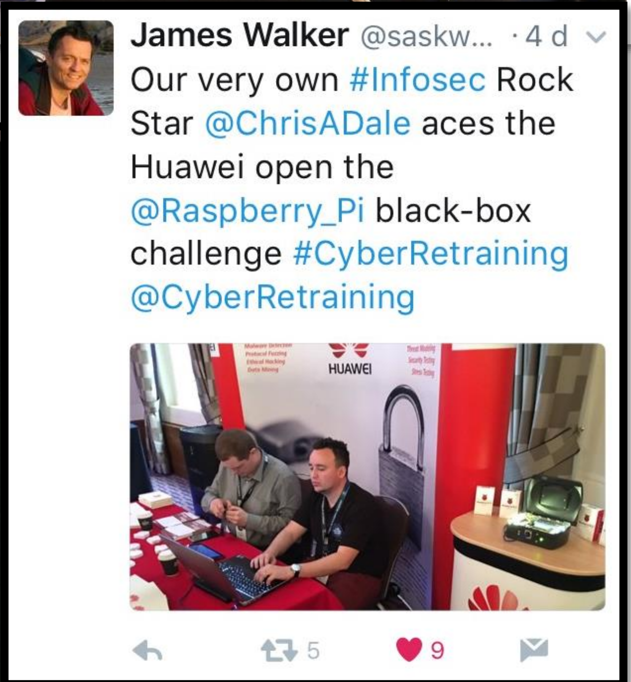
Procedures and checklists

Setting the Stage with Cyber Crime – Who are we up against?

An interesting view on the threat actors, who they are and the money the make.

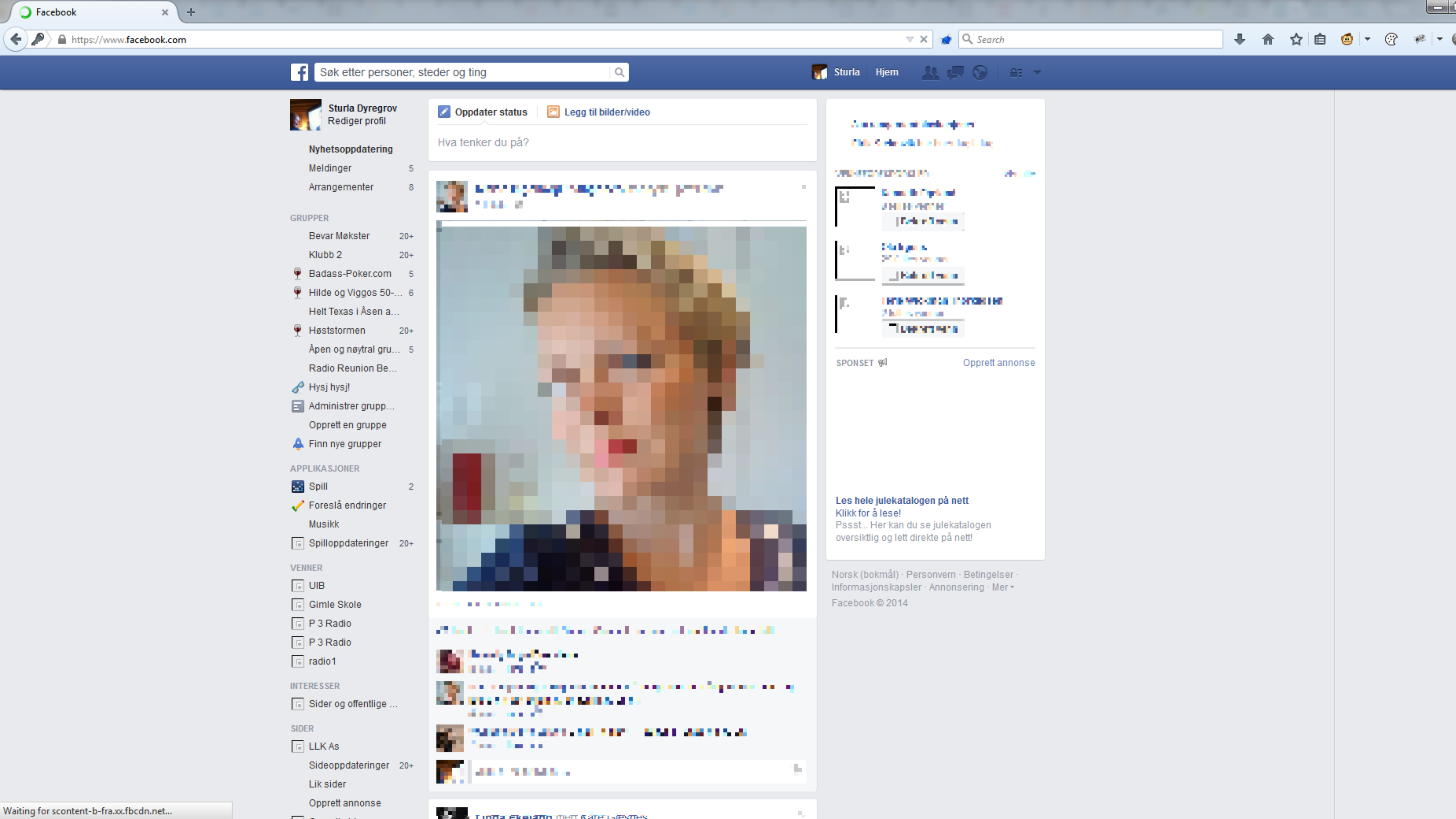
NSM
ÅRSRAPPORT 2013
NASJONAL SIKKERHETSMYNDIGHET ER NORGES EKSPERTORGAN FOR INFORMASJONS- OG OBJEKTSIKKERHET

Nyhetsmorgen lørdag


James Walker @saskw... · 4 d

Our very own #Infosec Rock Star @ChrisADale aces the Huawei open the @Raspberry_Pi black-box challenge #CyberRetraining @CyberRetraining

acker



Sturla Dyregrov
Rediger profil

Nyhetsoppdatering	
Meldinger	5
Arrangementer	8
GRUPPER	
Bevar Møkster	20+
Klubb 2	20+
Badass-Poker.com	5
Hilde og Viggos 50-...	6
Helt Texas i Åsen a...	
Høststormen	20+
Åpen og nøytral gru...	5
Radio Reunion Be...	
Hysj hysj!	
Administrer grupp...	
Opprett en gruppe	
Finn nye grupper	
APPLIKASJONER	
Spill	2
Foreslå endringer	
Musikk	
Spilloppdateringer	20+
VENNER	
UIB	
Gimle Skole	
P 3 Radio	
P 3 Radio	
radio1	
INTERESSER	
Sider og offentlige ...	
SIDER	
LLK As	
Sideoppdateringer	20+
Lik sider	
Opprett annonse	

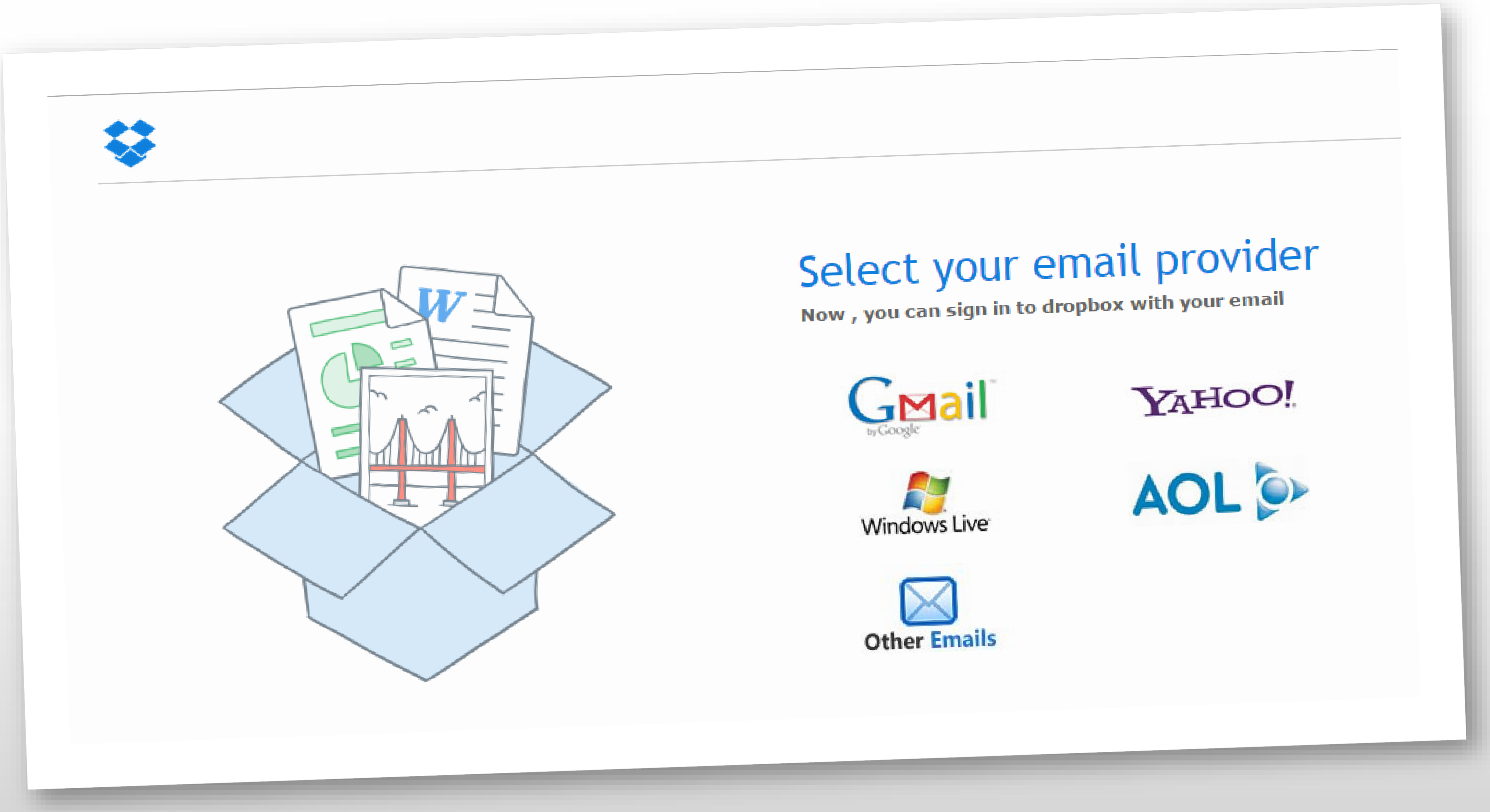
Oppdater status
Legg til bilder/video
Hva tenker du på?

SPONSET
Opprett annonse

Les hele julekatalogen på nett
Klikk for å lese!
Pssst... Her kan du se julekatalogen oversiktlig og lett direkte på nett!

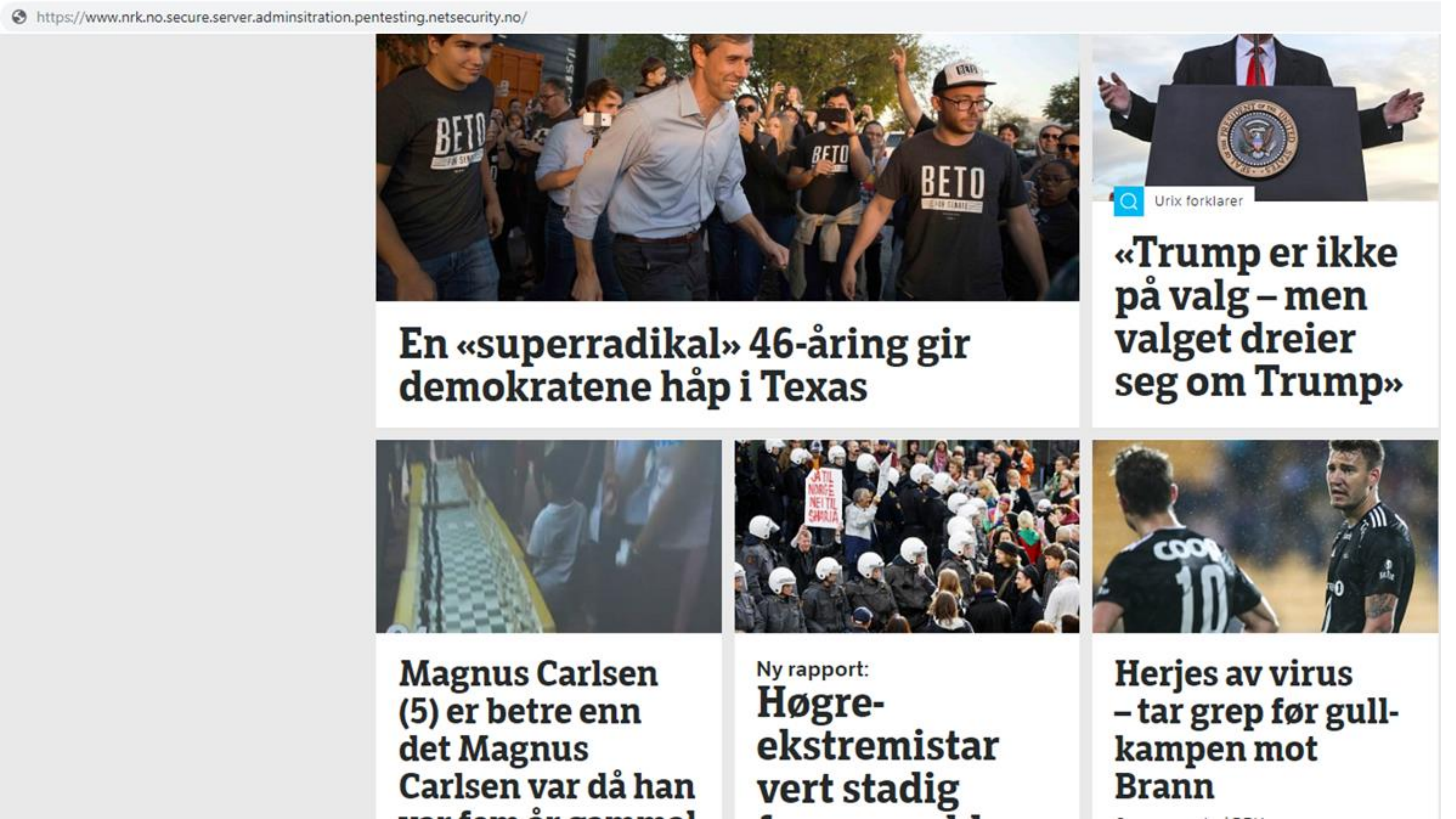
Norsk (bokmål) · Personvern · Betingelser · Informasjonskapsler · Annonsering · Mer
Facebook © 2014

Waiting for scontent-b-fra.xx.fbcdn.net...



Select your email provider

Now , you can sign in to dropbox with your email



https://www.nrk.no.secure.server.adminsitration.pentesting.netsecurity.no/

En «superradikal» 46-åring gir demokratene håp i Texas

Urix forklarer

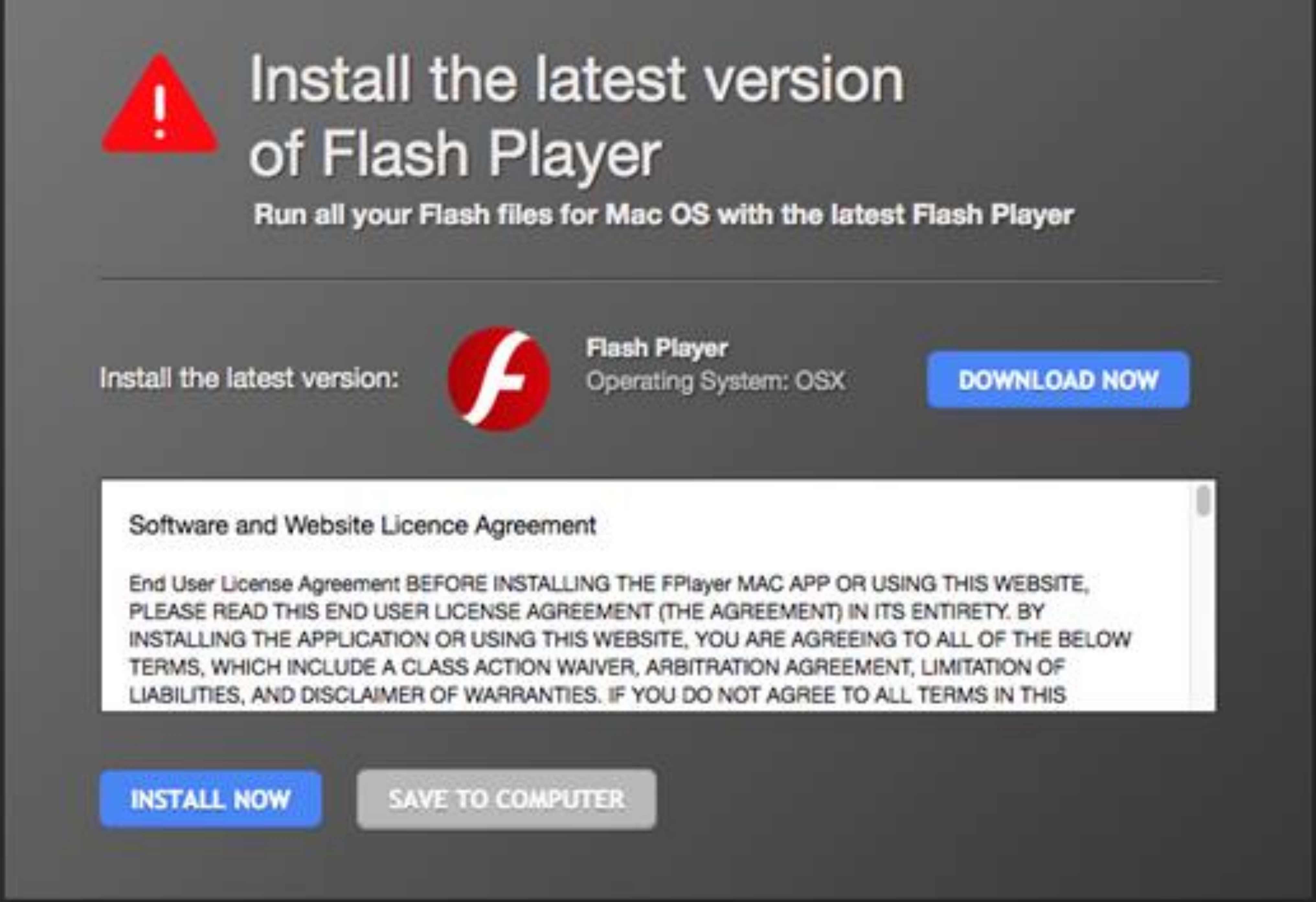
«Trump er ikke på valg – men valget dreier seg om Trump»

Magnus Carlsen (5) er betre enn det Magnus Carlsen var då han var fem år gammel

Ny rapport:

Høgre-ekstremistar vert stadig

Herjes av virus – tar grep før gull-kampen mot Brann



Install the latest version of Flash Player

Run all your Flash files for Mac OS with the latest Flash Player

Install the latest version:

Flash Player

Operating System: OSX

Software and Website Licence Agreement

End User License Agreement BEFORE INSTALLING THE FPlayer MAC APP OR USING THIS WEBSITE, PLEASE READ THIS END USER LICENSE AGREEMENT (THE AGREEMENT) IN ITS ENTIRETY. BY INSTALLING THE APPLICATION OR USING THIS WEBSITE, YOU ARE AGREEING TO ALL OF THE BELOW TERMS, WHICH INCLUDE A CLASS ACTION WAIVER, ARBITRATION AGREEMENT, LIMITATION OF LIABILITIES, AND DISCLAIMER OF WARRANTIES. IF YOU DO NOT AGREE TO ALL TERMS IN THIS

Cyber Crime and Threat Actors

- High returns for low efforts
  - You can target thousands of victims with little effort
  - Payments often happen instantly
- Money laundering
  - Cryptocurrency
  - Tumblers
  - Mules
- Personal Data - How much are we worth?
  - Loose once and it is potential permanent damage for victims
- Easy to stay anonymous and not get caught

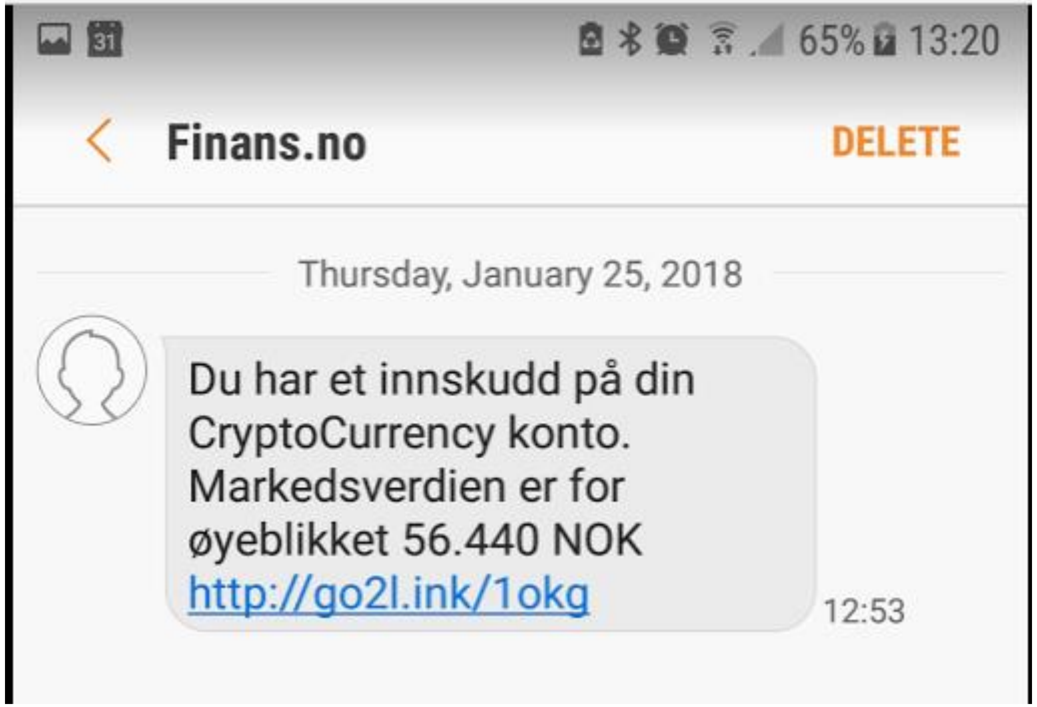
Crouching Yeti (Russia), Epic Turla (Russia), Darkhotel (Unknown) (Source: Kaspersky)

Hacking is BIG MONEY

Personal Data

How much are we worth?

Our personal data for sale.

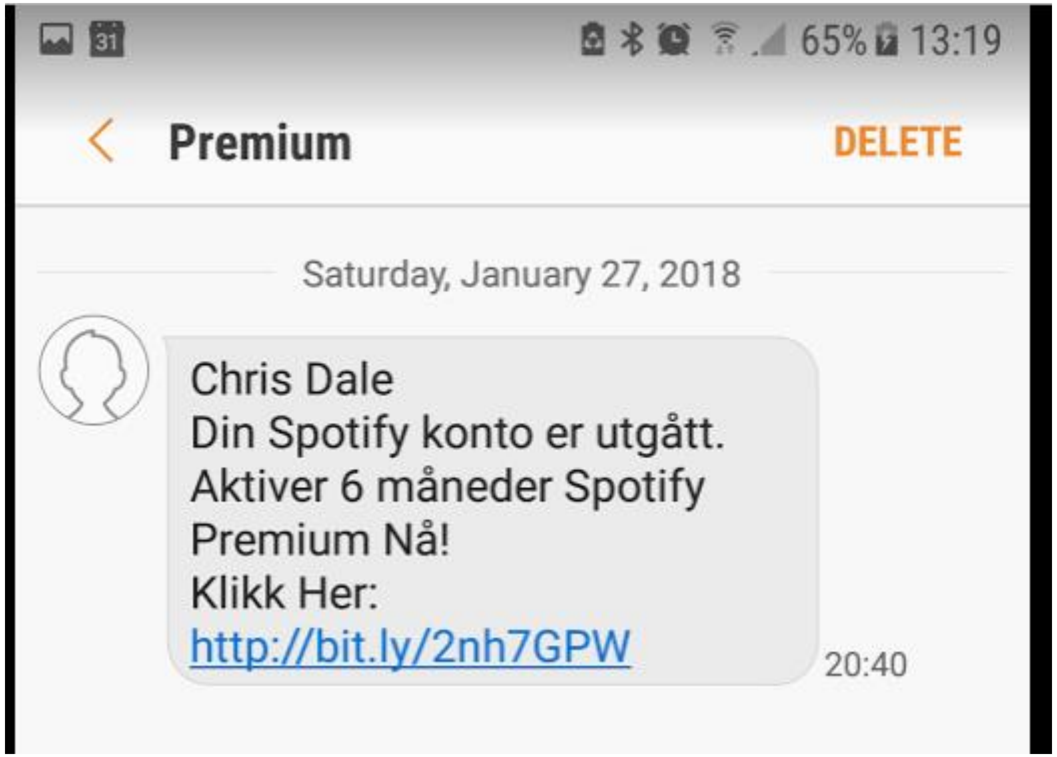


Finans.no

Thursday, January 25, 2018

Du har et innskudd på din CryptoCurrency konto. Markedsverdien er for øyeblikket 56.440 NOK
http://go2l.ink/1okg

12:53

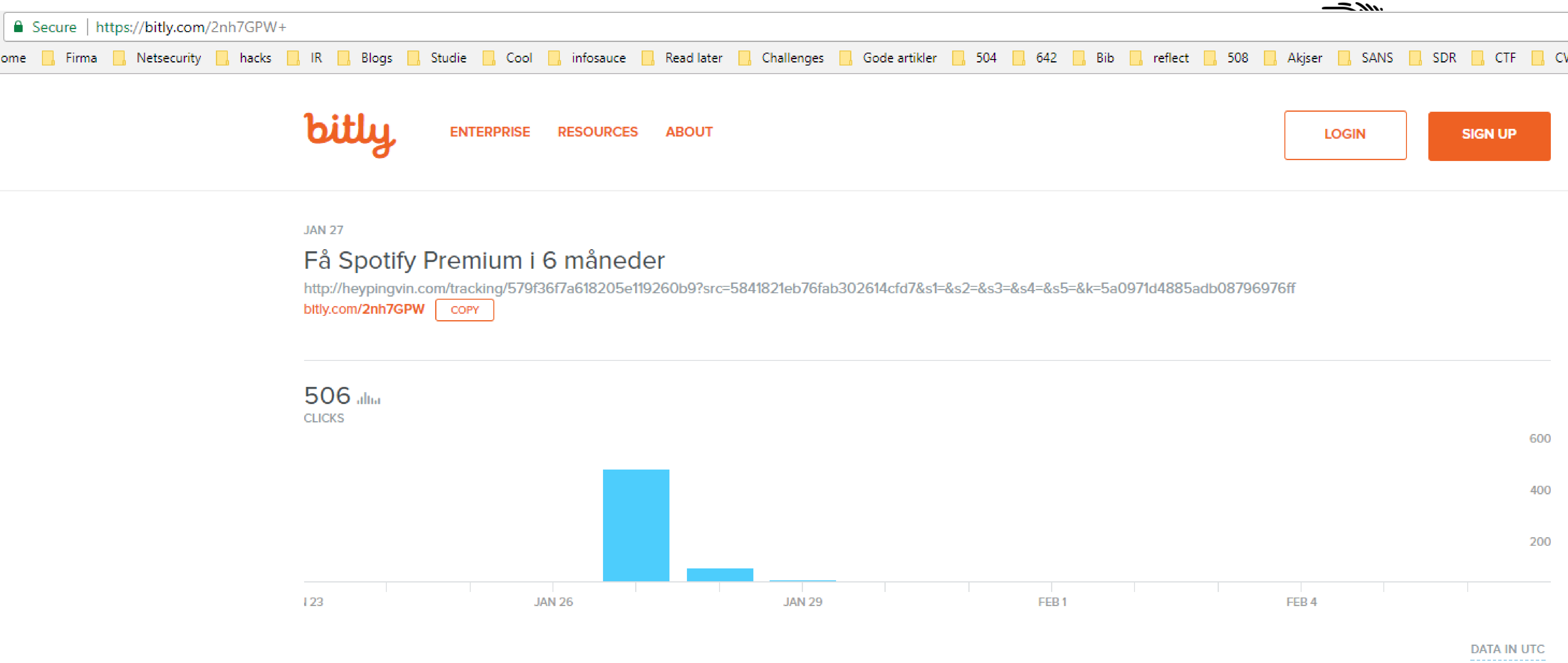


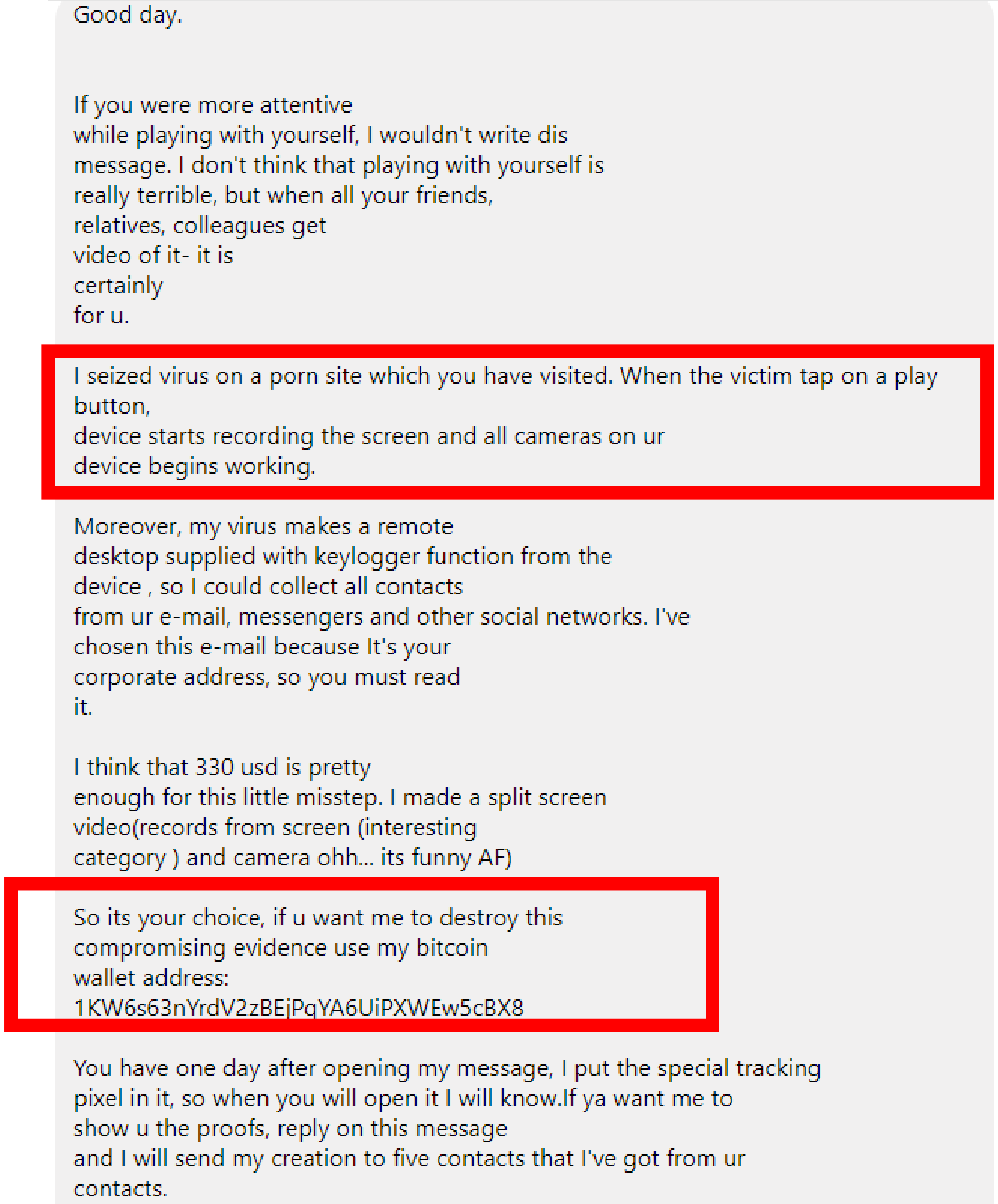
Premium

Saturday, January 27, 2018

Chris Dale
Din Spotify konto er utgått.
Aktiver 6 måneder Spotify Premium Nå!
Klikk Her:
http://bit.ly/2nh7GPW

20:40





Good day.

If you were more attentive
while playing with yourself, I wouldn't write dis
message. I don't think that playing with yourself is
really terrible, but when all your friends,
relatives, colleagues get
video of it- it is
certainly
for u.

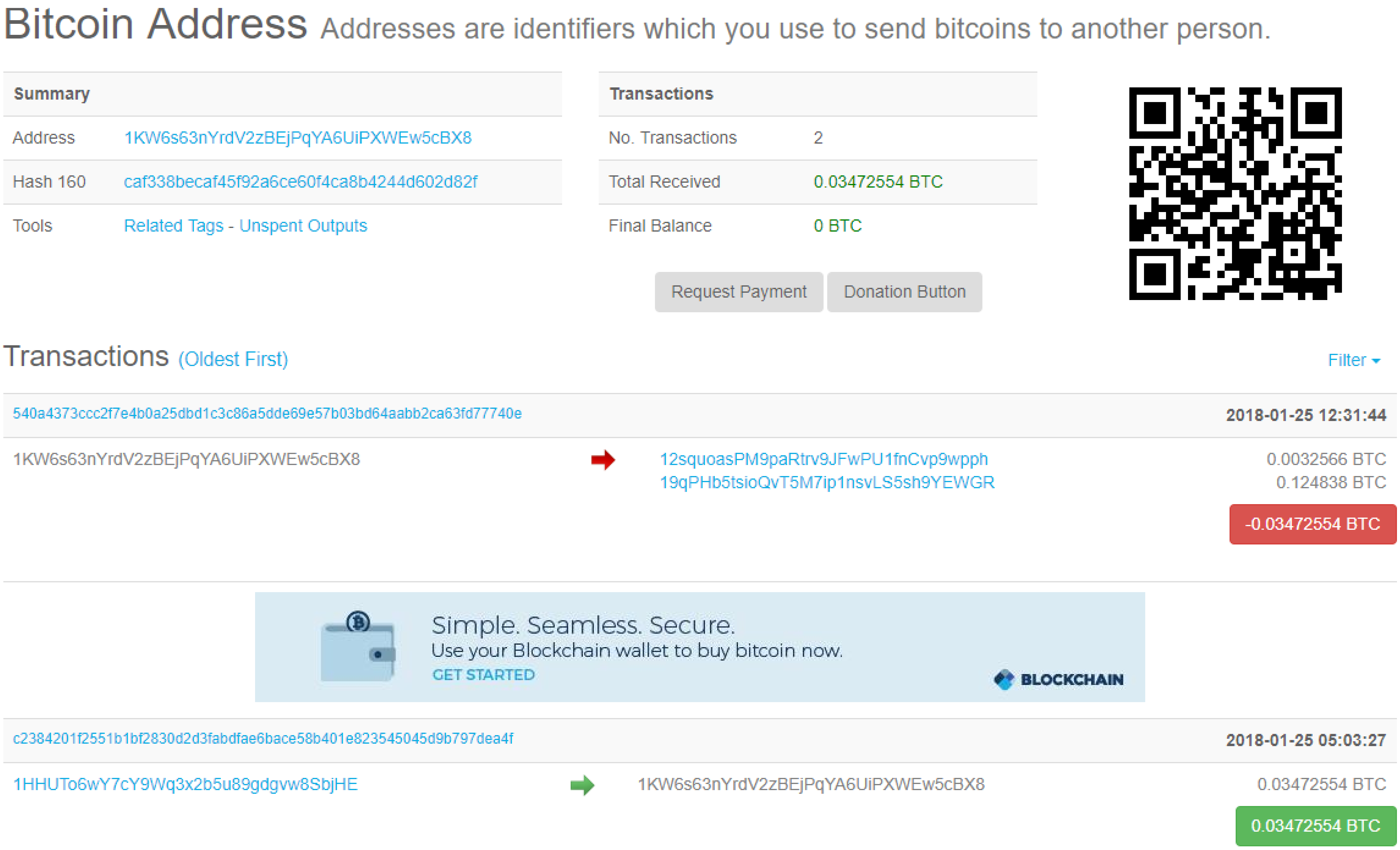
I seized virus on a porn site which you have visited. When the victim tap on a play
button,
device starts recording the screen and all cameras on ur
device begins working.

Moreover, my virus makes a remote
desktop supplied with keylogger function from the
device , so I could collect all contacts
from ur e-mail, messengers and other social networks. I've
chosen this e-mail because It's your
corporate address, so you must read
it.

I think that 330 usd is pretty
enough for this little misstep. I made a split screen
video(records from screen (interesting
category) and camera ohh... its funny AF)

So its your choice, if u want me to destroy this
compromising evidence use my bitcoin
wallet address:
1KW6s63nYrdV2zBEjPqYA6UiPXWEw5cBX8

You have one day after opening my message, I put the special tracking
pixel in it, so when you will open it I will know.If ya want me to
show u the proofs, reply on this message
and I will send my creation to five contacts that I've got from ur
contacts.



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1KW6s63nYrdV2zBEjPqYA6UiPXWEw5cBX8
Hash 160	caf338becaf45f92a6ce60f4ca8b4244d602d82f
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	2
Total Received	0.03472554 BTC
Final Balance	0 BTC

Transactions (Oldest First)

540a4373ccc2f7e4b0a25dbd1c3c86a5dde69e57b03bd64aabb2ca63fd77740e 2018-01-25 12:31:44

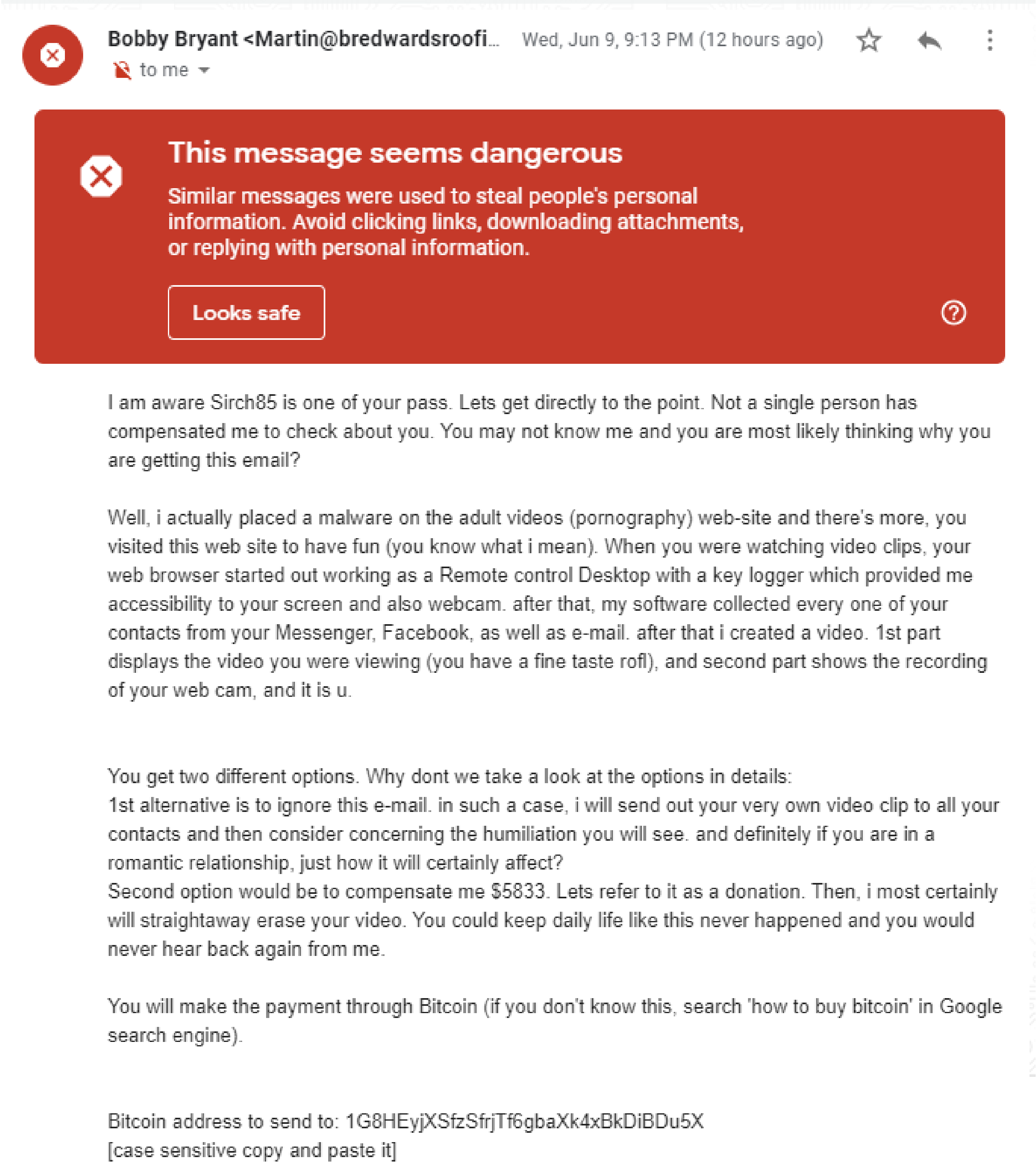
1KW6s63nYrdV2zBEjPqYA6UiPXWEw5cBX8 → 12squoasPM9paRtrv9JFwPU1fnCvp9wpph 0.0032566 BTC
19qPHb5tsioQvT5M7ip1nsvLS5sh9YEWGR 0.124838 BTC

-0.03472554 BTC

c2384201f2551b1bf2830d2d3fabdfae6bace58b401e823545045d9b797dea4f 2018-01-25 05:03:27

1HHUTo6wY7cY9Wq3x2b5u89gdgvw8SbjHE → 1KW6s63nYrdV2zBEjPqYA6UiPXWEw5cBX8 0.03472554 BTC

0.03472554 BTC



Bobby Bryant <Martin@bredwardsroofi... Wed, Jun 9, 9:13 PM (12 hours ago)

to me

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

I am aware Sirch85 is one of your pass. Lets get directly to the point. Not a single person has compensated me to check about you. You may not know me and you are most likely thinking why you are getting this email?

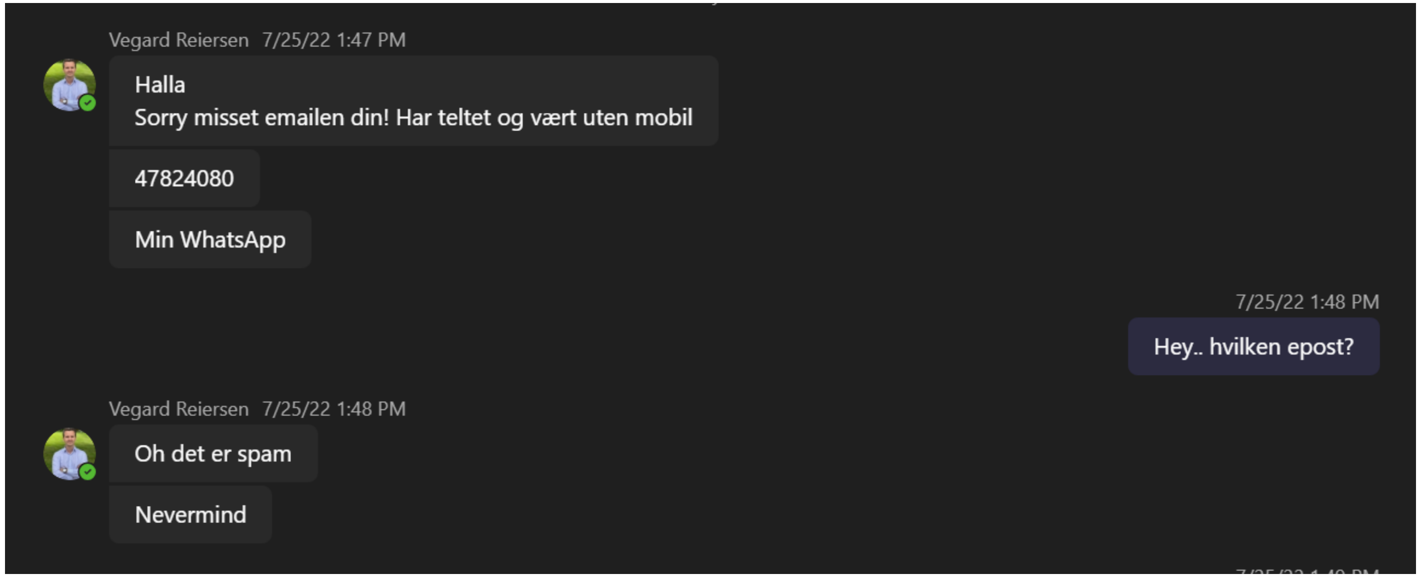
Well, i actually placed a malware on the adult videos (pornography) web-site and there's more, you visited this web site to have fun (you know what i mean). When you were watching video clips, your web browser started out working as a Remote control Desktop with a key logger which provided me accessibility to your screen and also webcam. after that, my software collected every one of your contacts from your Messenger, Facebook, as well as e-mail. after that i created a video. 1st part displays the video you were viewing (you have a fine taste rofl), and second part shows the recording of your web cam, and it is u.

You get two different options. Why dont we take a look at the options in details:
1st alternative is to ignore this e-mail. in such a case, i will send out your very own video clip to all your contacts and then consider concerning the humiliation you will see. and definitely if you are in a romantic relationship, just how it will certainly affect?
Second option would be to compensate me $5833. Lets refer to it as a donation. Then, i most certainly will straightaway erase your video. You could keep daily life like this never happened and you would never hear back again from me.

You will make the payment through Bitcoin (if you don't know this, search 'how to buy bitcoin' in Google search engine).

Bitcoin address to send to: 1G8HEyjXSfzSfrjTf6gbaXk4xBkDiBDu5X
[case sensitive copy and paste it]

Within the Same Week of Hire



Vegard Reiersen 7/25/22 1:47 PM

Halla
Sorry misset emailen din! Har teltet og vært uten mobil

47824080

Min WhatsApp

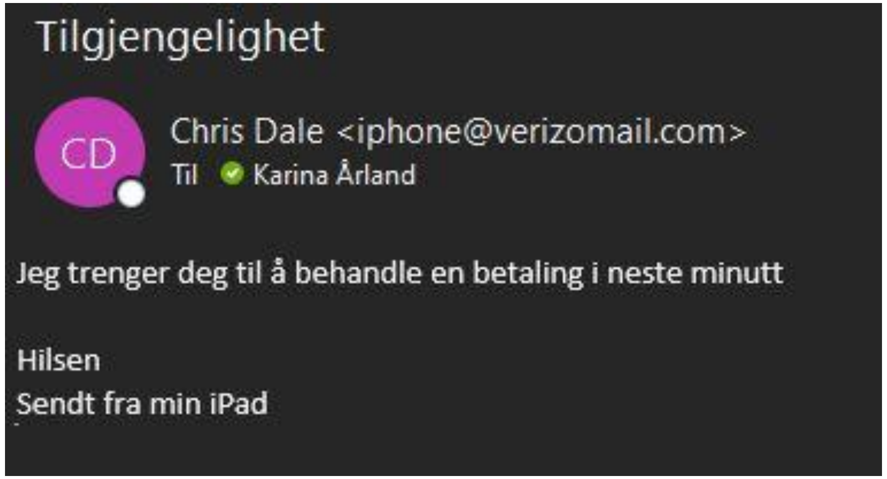
7/25/22 1:48 PM

Hey.. hvilken epost?

Vegard Reiersen 7/25/22 1:48 PM

Oh det er spam

Nevermind

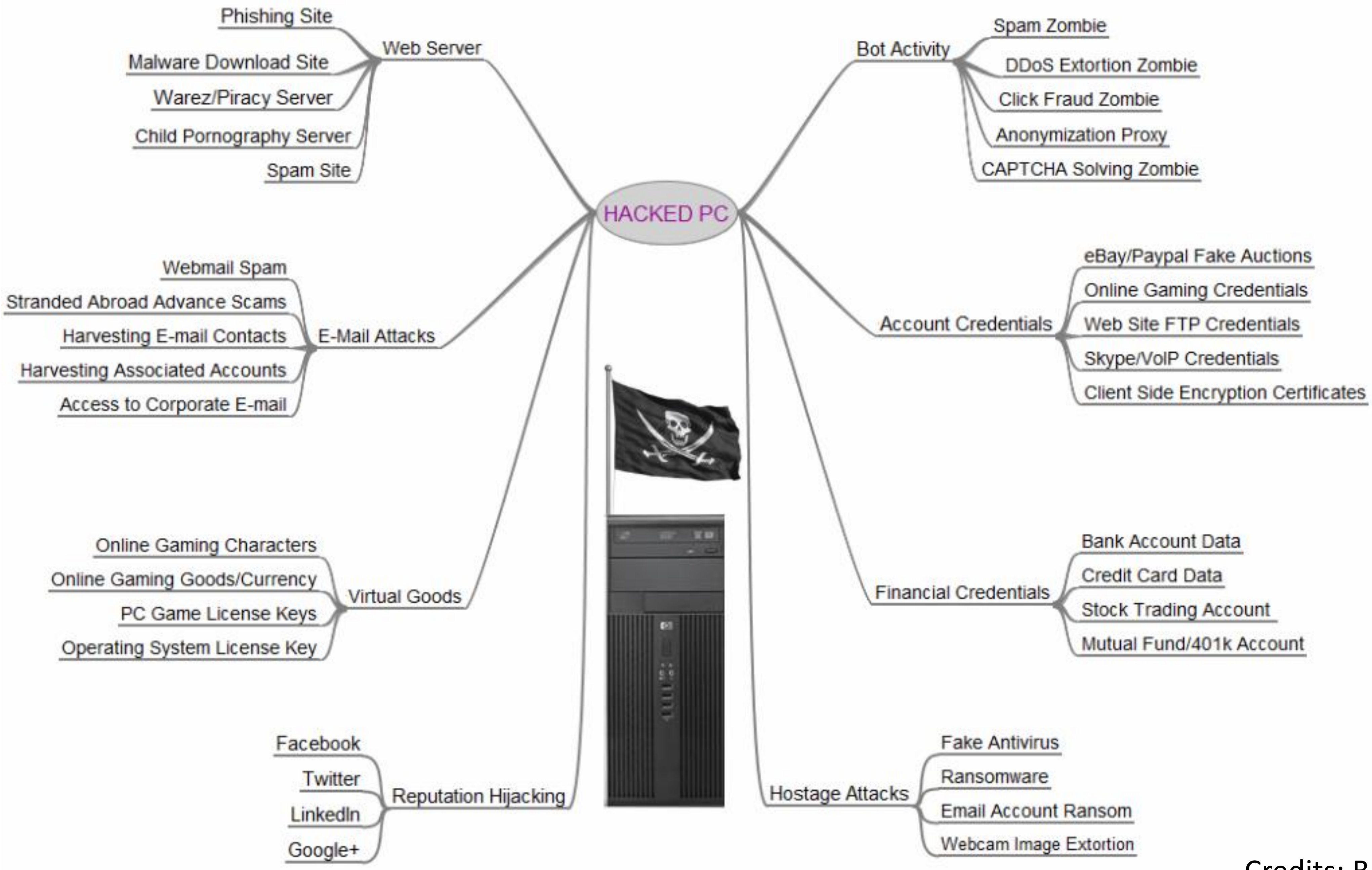


Tilgjengelighet

Chris Dale <iphone@verizomail.com>
Til Karina Årland

Jeg trenger deg til å behandle en betaling i neste minutt

Hilsen
Sendt fra min iPad



HACKED PC

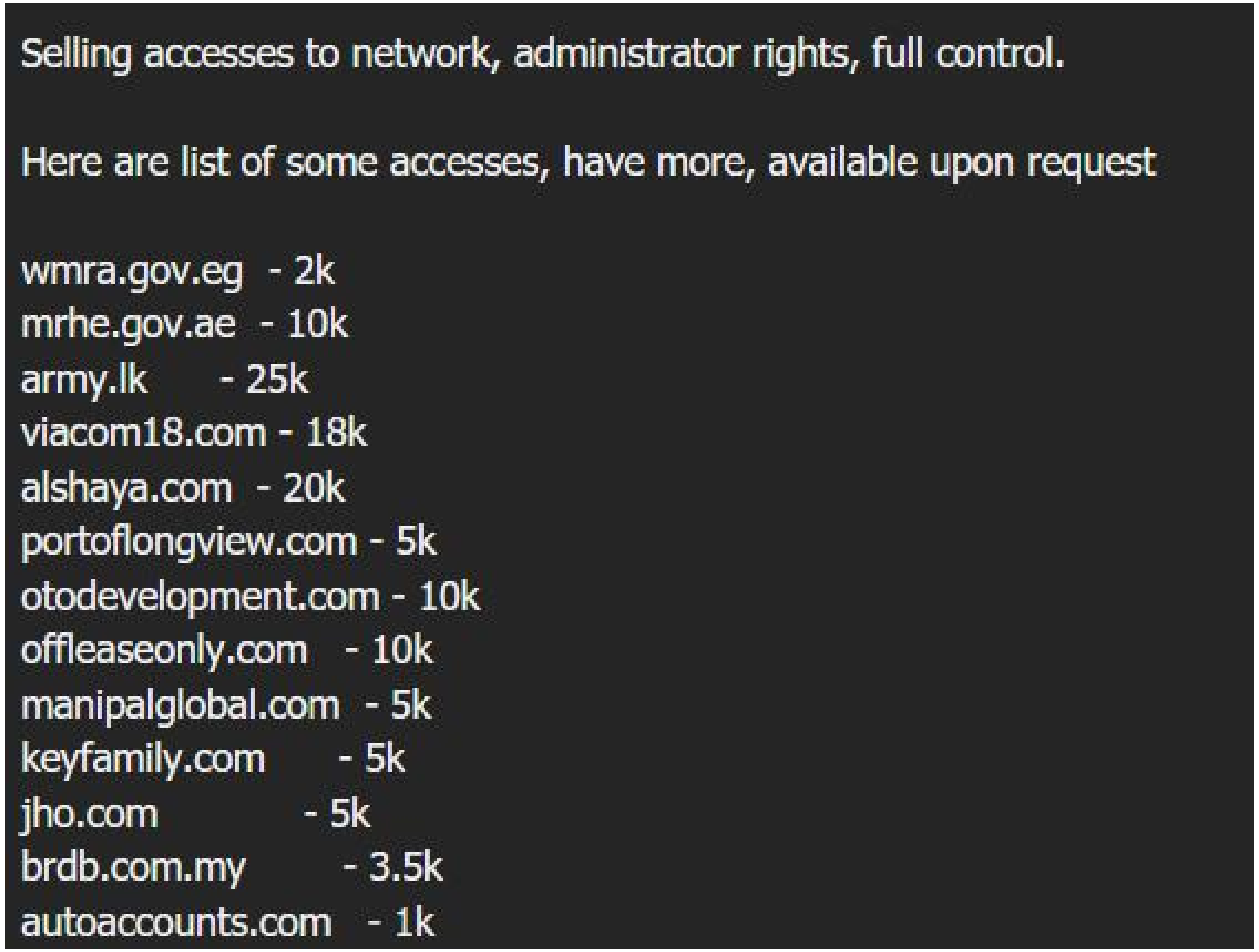
- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Reputation Hijacking
  - Facebook
  - Twitter
  - LinkedIn
  - Google+
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

Credits: Brian Krebs

Attacks for Fun and **Profit**

- Attackers are figuring out how to make money from their malicious code
- Ask law enforcement: If there's money in a given crime, we'll see much more of it
- How to make money on malicious code:
  - Cryptocurrency miners
  - Spam and web-based advertising
  - Phishing: Email, phone, and targeted (spear) phishing
  - Denial-of-Service extortion
  - Keystroke loggers stealing financial information
  - Rent out armies of infected systems for all the above
  - RAM scrapers pulling CC numbers from POS terminals
- Ransomware, ransomware, ransomware

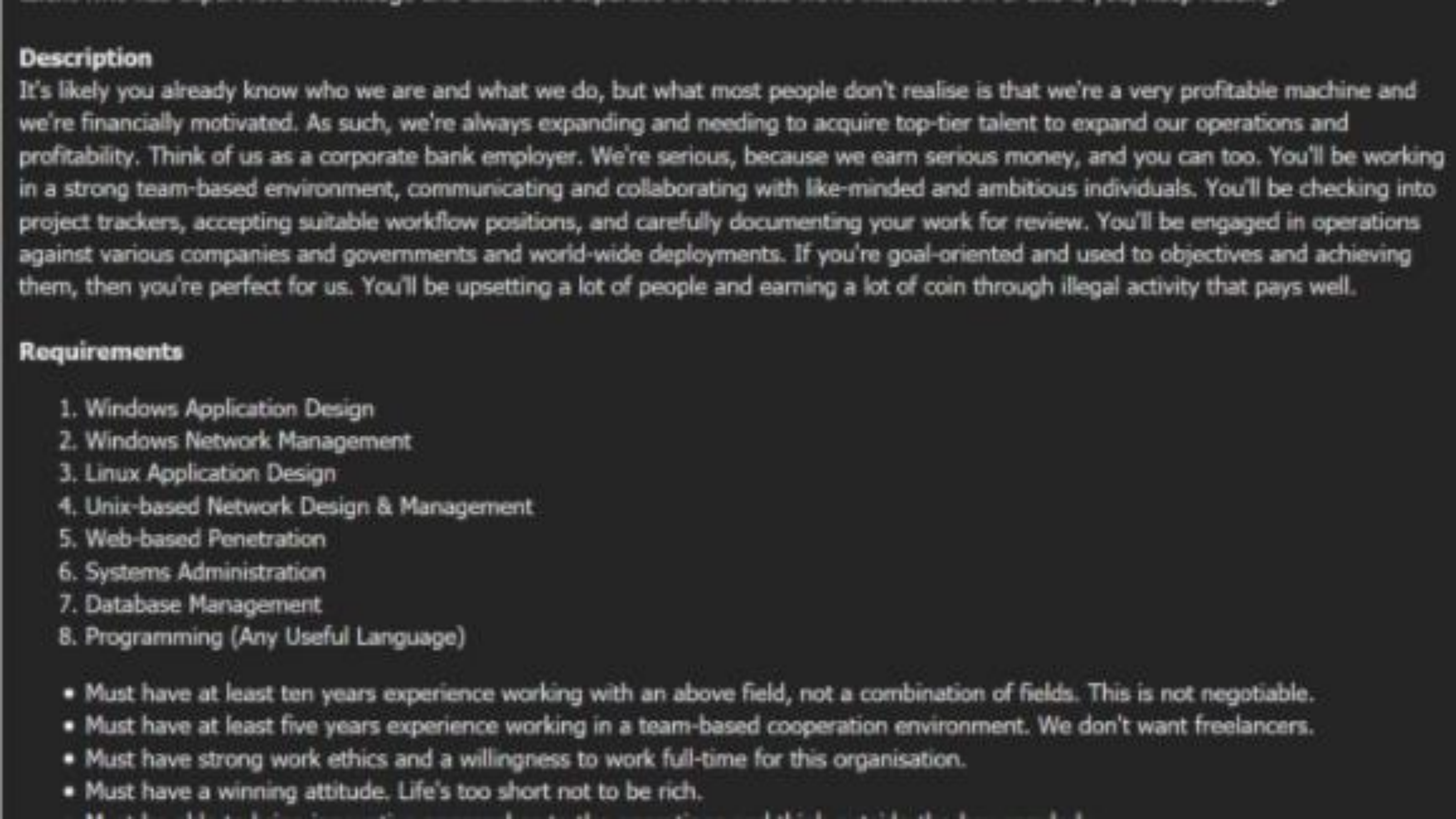
How much would someone pay to get access to your organization?



Selling accesses to network, administrator rights, full control.

Here are list of some accesses, have more, available upon request

wmra.gov.eg - 2k
mrhe.gov.ae - 10k
army.lk - 25k
viacom18.com - 18k
alshaya.com - 20k
portoflongview.com - 5k
otodevelopment.com - 10k
offleaseonly.com - 10k
manipalglobal.com - 5k
keyfamily.com - 5k
jho.com - 5k
brdb.com.my - 3.5k
autoaccounts.com - 1k



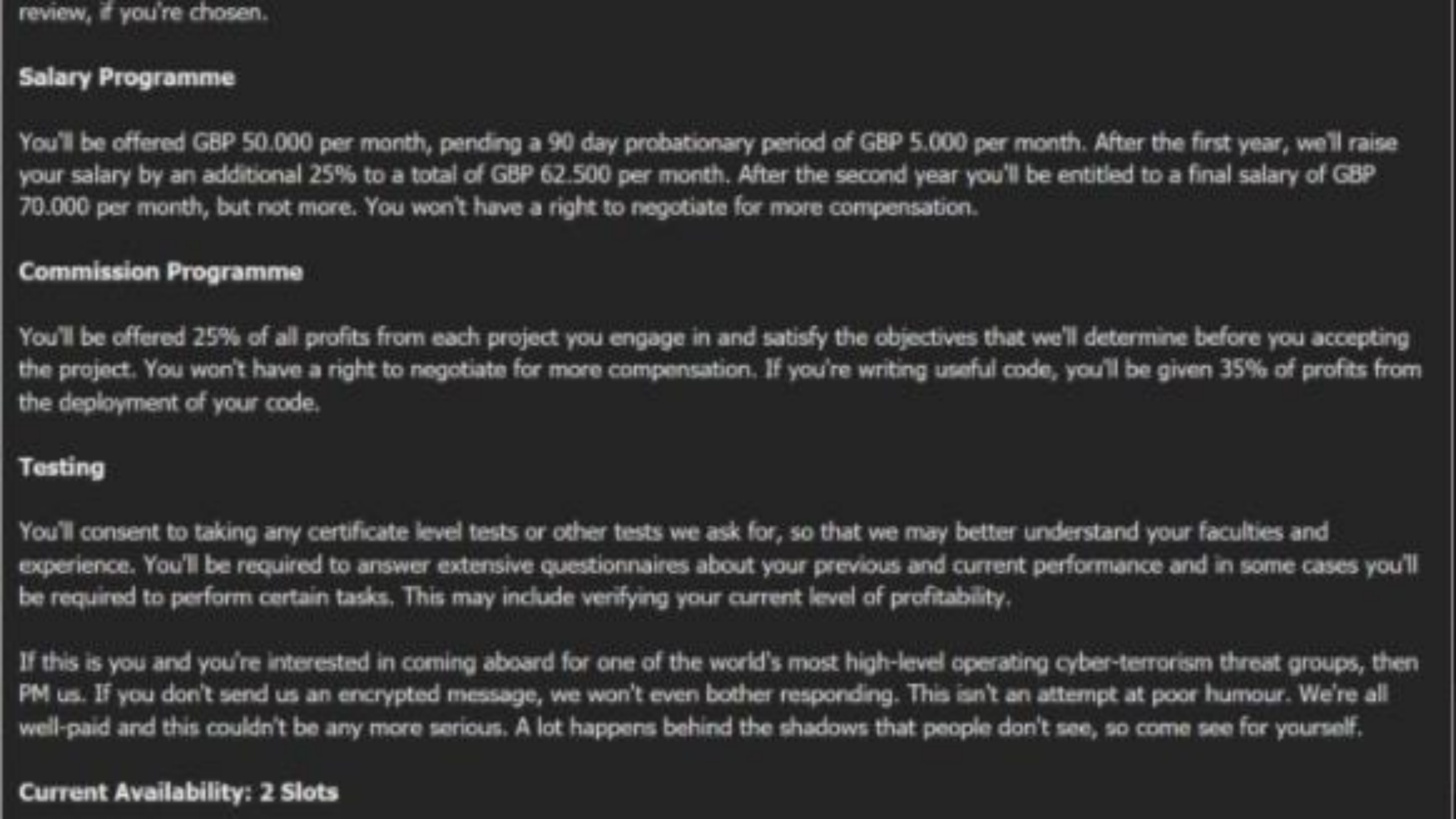
Description

It's likely you already know who we are and what we do, but what most people don't realise is that we're a very profitable machine and we're financially motivated. As such, we're always expanding and needing to acquire top-tier talent to expand our operations and profitability. Think of us as a corporate bank employer. We're serious, because we earn serious money, and you can too. You'll be working in a strong team-based environment, communicating and collaborating with like-minded and ambitious individuals. You'll be checking into project trackers, accepting suitable workflow positions, and carefully documenting your work for review. You'll be engaged in operations against various companies and governments and world-wide deployments. If you're goal-oriented and used to objectives and achieving them, then you're perfect for us. You'll be upsetting a lot of people and earning a lot of coin through illegal activity that pays well.

Requirements

1. Windows Application Design
2. Windows Network Management
3. Linux Application Design
4. Unix-based Network Design & Management
5. Web-based Penetration
6. Systems Administration
7. Database Management
8. Programming (Any Useful Language)

- Must have at least ten years experience working with an above field, not a combination of fields. This is not negotiable.
- Must have at least five years experience working in a team-based cooperation environment. We don't want freelancers.
- Must have strong work ethics and a willingness to work full-time for this organisation.
- Must have a winning attitude. Life's too short not to be rich.



review, if you're chosen.

Salary Programme

You'll be offered GBP 50.000 per month, pending a 90 day probationary period of GBP 5.000 per month. After the first year, we'll raise your salary by an additional 25% to a total of GBP 62.500 per month. After the second year you'll be entitled to a final salary of GBP 70.000 per month, but not more. You won't have a right to negotiate for more compensation.

Commission Programme

You'll be offered 25% of all profits from each project you engage in and satisfy the objectives that we'll determine before you accepting the project. You won't have a right to negotiate for more compensation. If you're writing useful code, you'll be given 35% of profits from the deployment of your code.

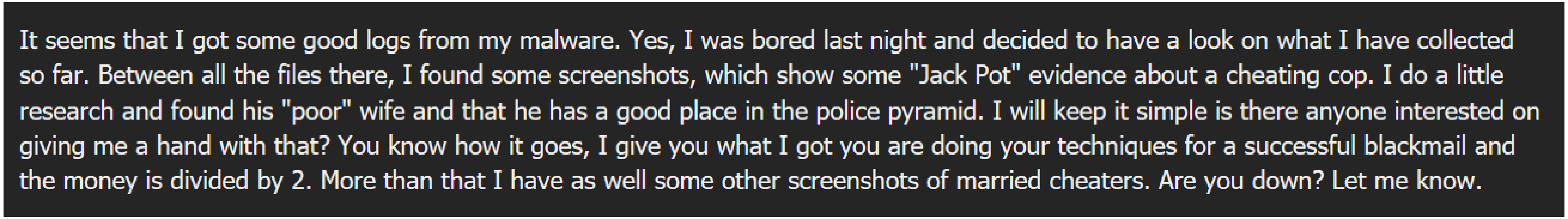
Testing

You'll consent to taking any certificate level tests or other tests we ask for, so that we may better understand your faculties and experience. You'll be required to answer extensive questionnaires about your previous and current performance and in some cases you'll be required to perform certain tasks. This may include verifying your current level of profitability.

If this is you and you're interested in coming aboard for one of the world's most high-level operating cyber-terrorism threat groups, then PM us. If you don't send us an encrypted message, we won't even bother responding. This isn't an attempt at poor humour. We're all well-paid and this couldn't be any more serious. A lot happens behind the shadows that people don't see, so come see for yourself.

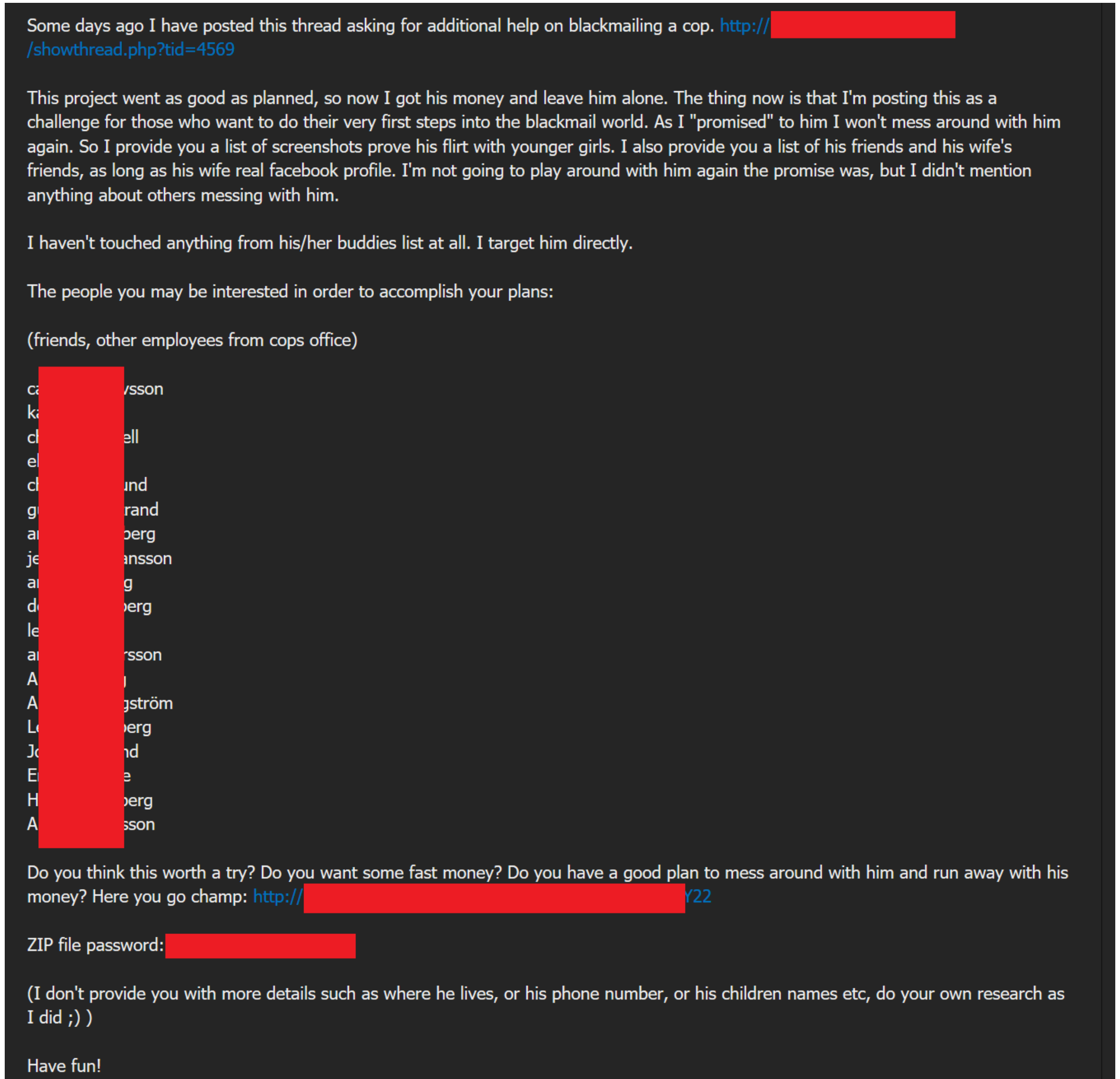
Current Availability: 2 Slots

Darknet Post 1/2



It seems that I got some good logs from my malware. Yes, I was bored last night and decided to have a look on what I have collected so far. Between all the files there, I found some screenshots, which show some "Jack Pot" evidence about a cheating cop. I do a little research and found his "poor" wife and that he has a good place in the police pyramid. I will keep it simple is there anyone interested on giving me a hand with that? You know how it goes, I give you what I got you are doing your techniques for a successful blackmail and the money is divided by 2. More than that I have as well some other screenshots of married cheaters. Are you down? Let me know.

Darknet Post 2/2



Some days ago I have posted this thread asking for additional help on blackmailing a cop. http://[redacted]/showthread.php?tid=4569

This project went as good as planned, so now I got his money and leave him alone. The thing now is that I'm posting this as a challenge for those who want to do their very first steps into the blackmail world. As I "promised" to him I won't mess around with him again. So I provide you a list of screenshots prove his flirt with younger girls. I also provide you a list of his friends and his wife's friends, as long as his wife real facebook profile. I'm not going to play around with him again the promise was, but I didn't mention anything about others messing with him.

I haven't touched anything from his/her buddies list at all. I target him directly.

The people you may be interested in order to accomplish your plans:

(friends, other employees from cops office)

[redacted]

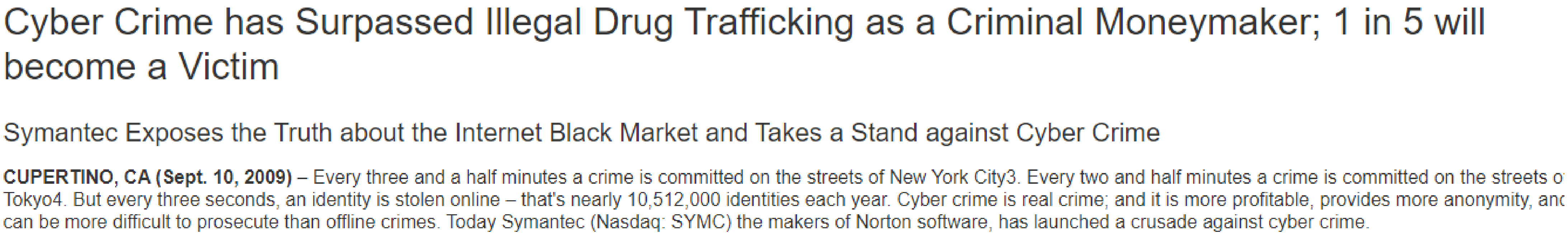
Do you think this worth a try? Do you want some fast money? Do you have a good plan to mess around with him and run away with his money? Here you go champ: http://[redacted]Y22

ZIP file password: [redacted]

(I don't provide you with more details such as where he lives, or his phone number, or his children names etc, do your own research as I did ;))

Have fun!

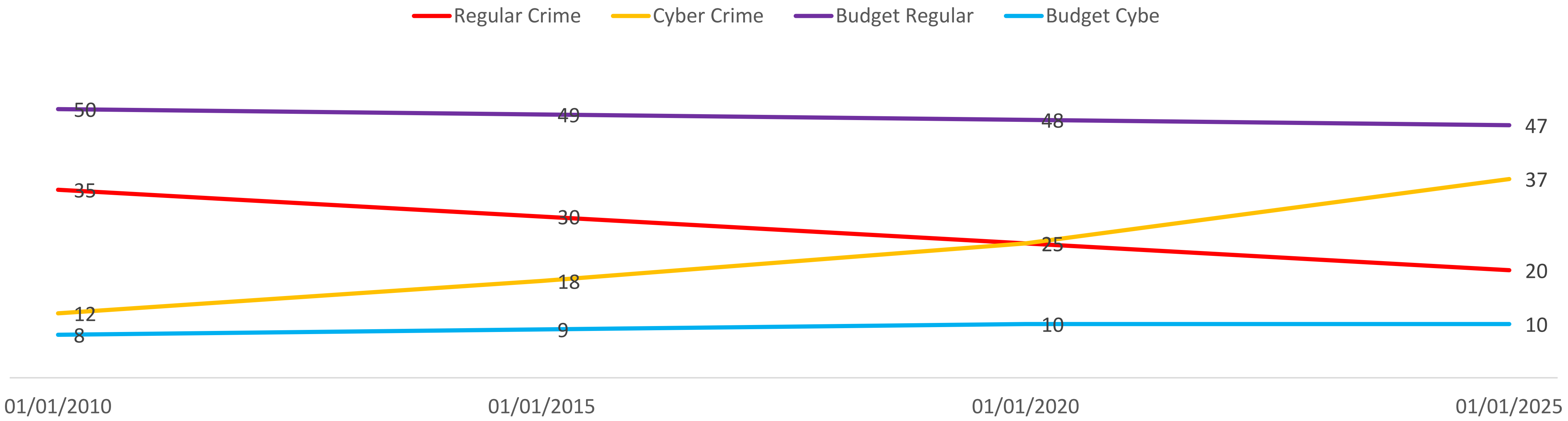
A Reminder – This is 14 Years Ago



Cyber Crime has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker; 1 in 5 will become a Victim

Symantec Exposes the Truth about the Internet Black Market and Takes a Stand against Cyber Crime

CUPERTINO, CA (Sept. 10, 2009) – Every three and a half minutes a crime is committed on the streets of New York City3. Every two and half minutes a crime is committed on the streets o Tokyo4. But every three seconds, an identity is stolen online – that's nearly 10,512,000 identities each year. Cyber crime is real crime; and it is more profitable, provides more anonymity, anc can be more difficult to prosecute than offline crimes. Today Symantec (Nasdaq: SYMC) the makers of Norton software, has launched a crusade against cyber crime.



Introduction to Security Testing

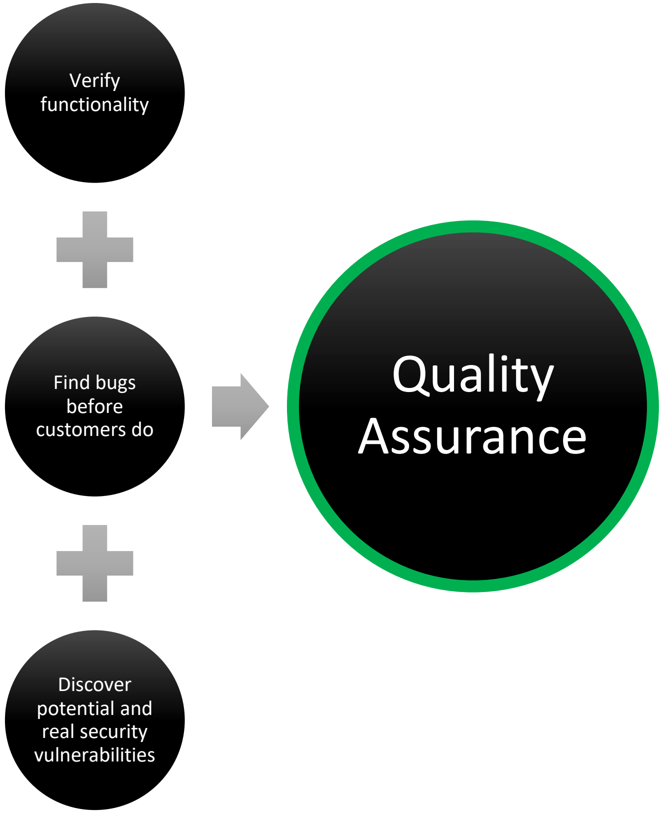
Hackers Manifesto

As a hacker, I am driven by a relentless curiosity and a desire to uncover the hidden truths that lie just beyond our reach. I know that there is always a way to penetrate even the most seemingly impenetrable systems. I approach every challenge with sharp senses, a keen intellect, and an open mind, ready to peel away layer after layer of complexity in pursuit of the answers I seek.

I understand that the work of a hacker is not magic, but rather the product of hard-won knowledge and a deep understanding of the systems we seek to exploit. I will not be deterred by initial failures, but will instead channel that energy into building my knowledge and experience, all the while observing the problem at hand and digging deeper than anyone else to find a way in.

To be a successful hacker is not easy, but I am committed to this path and will persist in the face of any obstacle. I will not assume that there is nothing to be found but will always maintain a sense of excitement and possibility, knowing that there is always something more to discover. I am hacker, and I will not rest until I have uncovered every secret and unlocked every door.

What is the Goal of Testing?



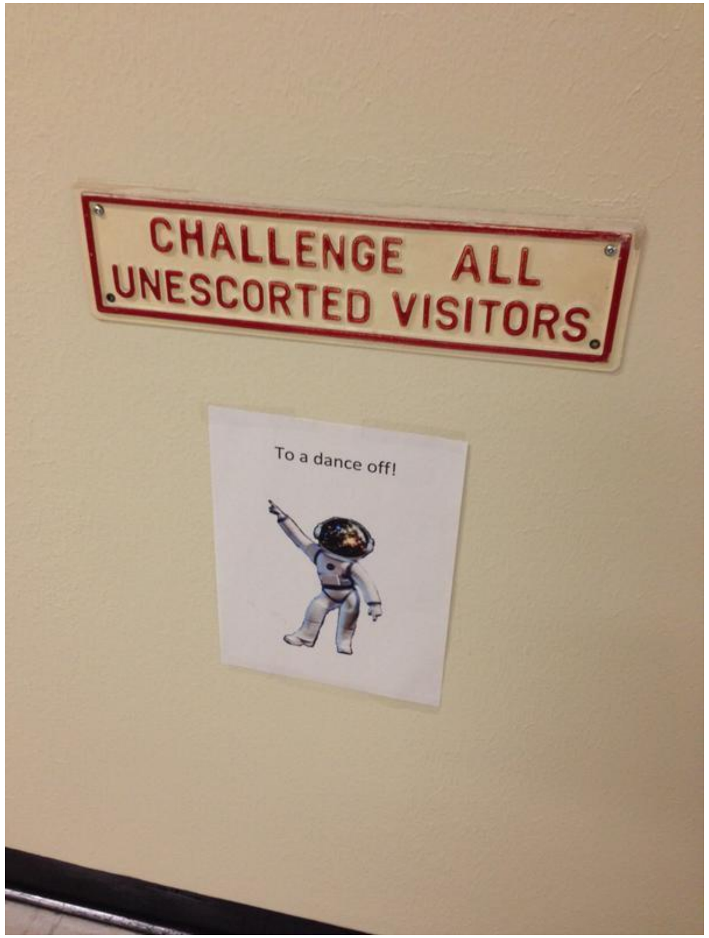
Verify functionality

Find bugs before customers do

Discover potential and real security vulnerabilities

Quality Assurance

Always Keep In Mind



Primer on Web

- Web is ubiquitous
- It is an essential piece of technology to understand

Web1.0

The Read Only Web

Web 2.0

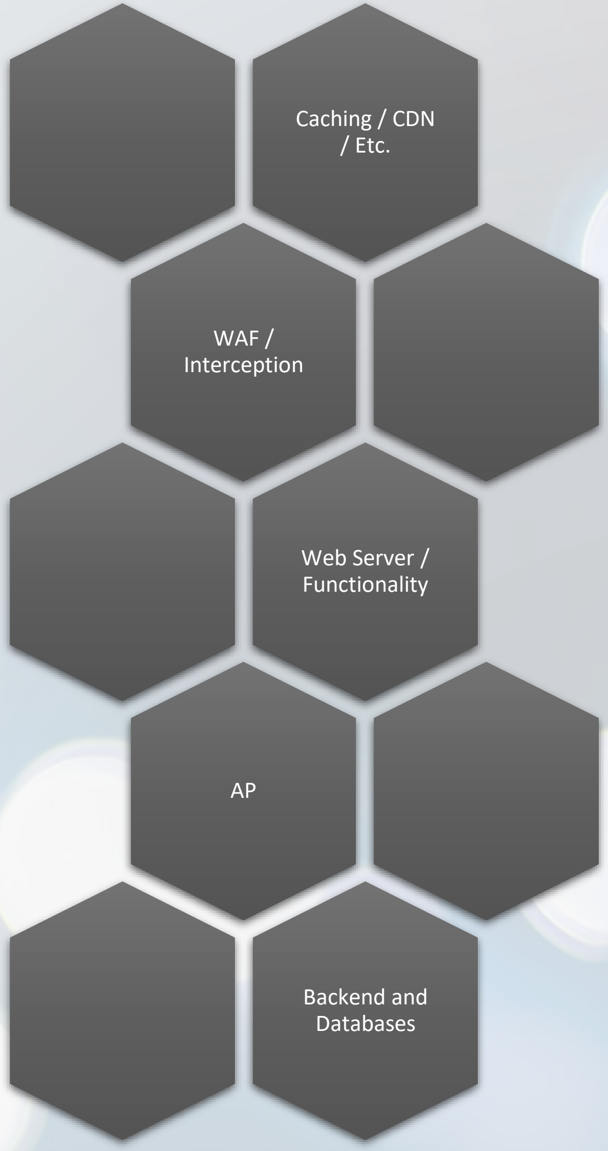
The Dynamic and Interactive Web

Web 3.0

Read-Write-Execute Web

Typically It's Not Just A Application

- There is a front-end
- API typically connected
- Back-end supporting data read and storage



Caching / CDN / Etc.

WAF / Interception

Web Server / Functionality

AP

Backend and Databases

Components in Play

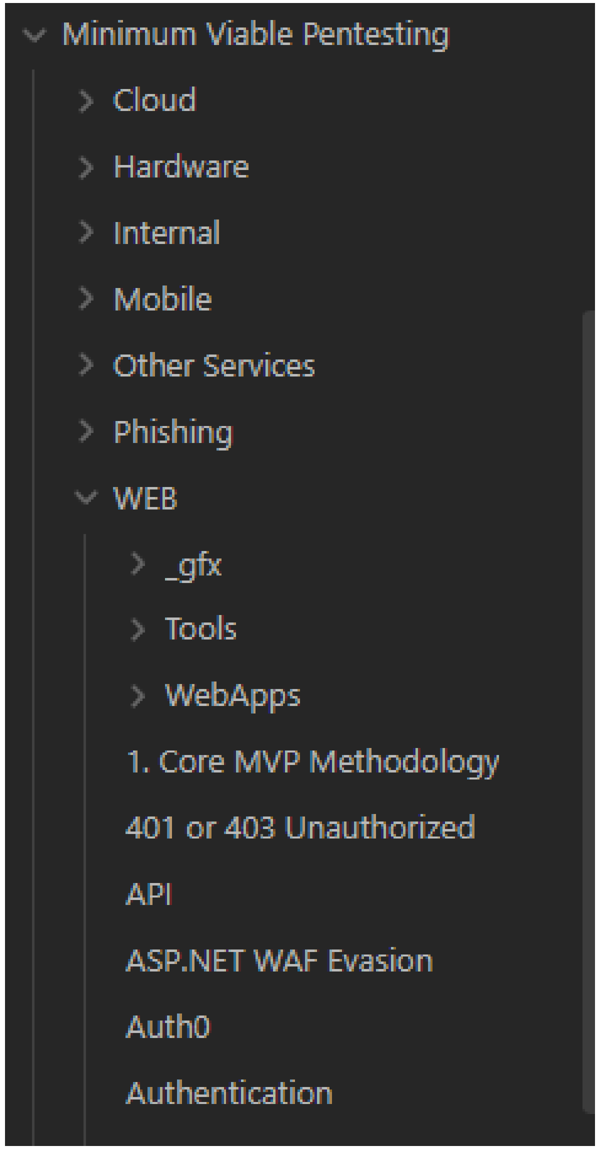
- HTTP – For transporting between client and server
- HTML – Mark up for displaying data
- CSS – Mark up for styling
- JavaScript – Programming to make it dynamic
- Web Servers (e.g., Apache, Nginx) – Serve website content
- APIs (RESTful, GraphQL) – Interface for interacting with other software
- SSL/TLS – Secure data transmission
- Frameworks & Libraries (e.g., React, Angular, Vue for frontend; Node.js, Django for backend) – Simplify development

Minimum Viable Penetration Testing

Frameworks

Define an **absolute minimum** of activity to perform on a certain system or piece of technology or application.

- Allow experience from previous tests to be reused
- A way to support pentesters. Don’t start from scratch.
  - Your own refined Google / Hacktricks.xyz / etc.
- Not training on concepts, but simple bullets of what needs to be done
- Make pentester accountable to:
  - Check the things which needs to be checked
  - Ask team for help when there are interesting anomalies
- There are application and technology specific MVP’s

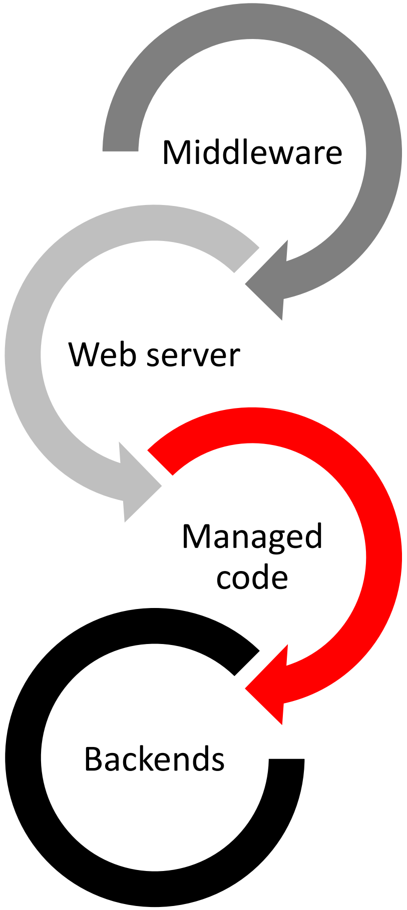


- Minimum Viable Pentesting
  - Cloud
  - Hardware
  - Internal
  - Mobile
  - Other Services
  - Phishing
  - WEB
    - _gfx
    - Tools
    - WebApps
    - 1. Core MVP Methodology
    - 401 or 403 Unauthorized
    - API
    - ASP.NET WAF Evasion
    - Auth0
    - Authentication

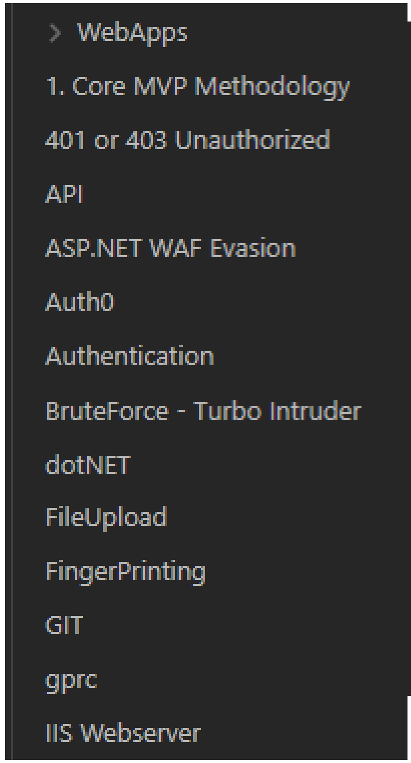
Tech and Application Specific MVP

Frameworks

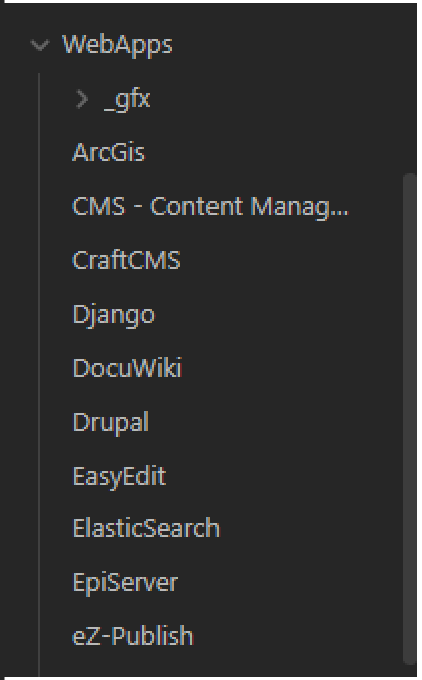
Attack The Stack



Tech & App Specific MVP



```
> WebApps
1. Core MVP Methodology
401 or 403 Unauthorized
API
ASP.NET WAF Evasion
Auth0
Authentication
BruteForce - Turbo Intruder
dotNET
FileUpload
FingerPrinting
GIT
gprc
IIS Webserver
```



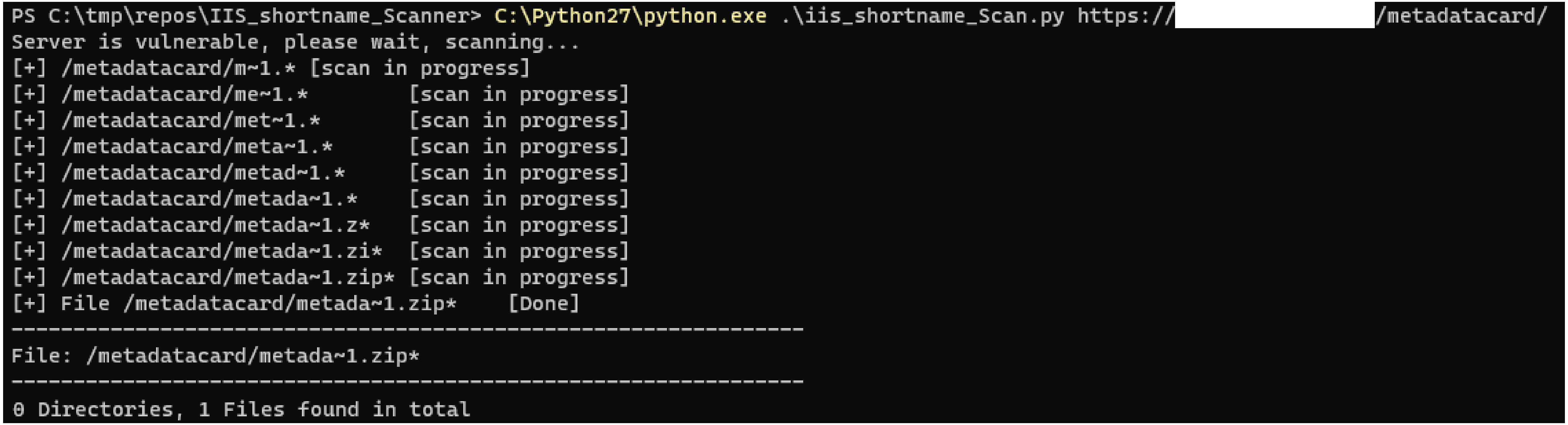
```
v WebApps
    > _gfx
    ArcGis
    CMS - Content Manag...
    CraftCMS
    Django
    DocuWiki
    Drupal
    EasyEdit
    ElasticSearch
    EpiServer
    eZ-Publish
```

Testing Frameworks

- ASVS – Application Security Verification Standard
- WSTG – Web Security Testing Guide
- …

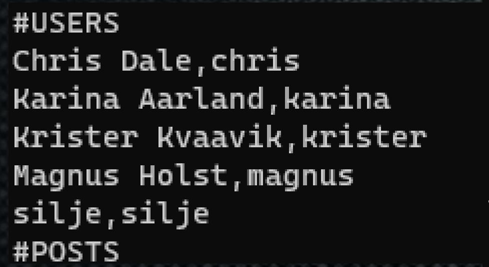
IIS Short Name Scanning

Frameworks

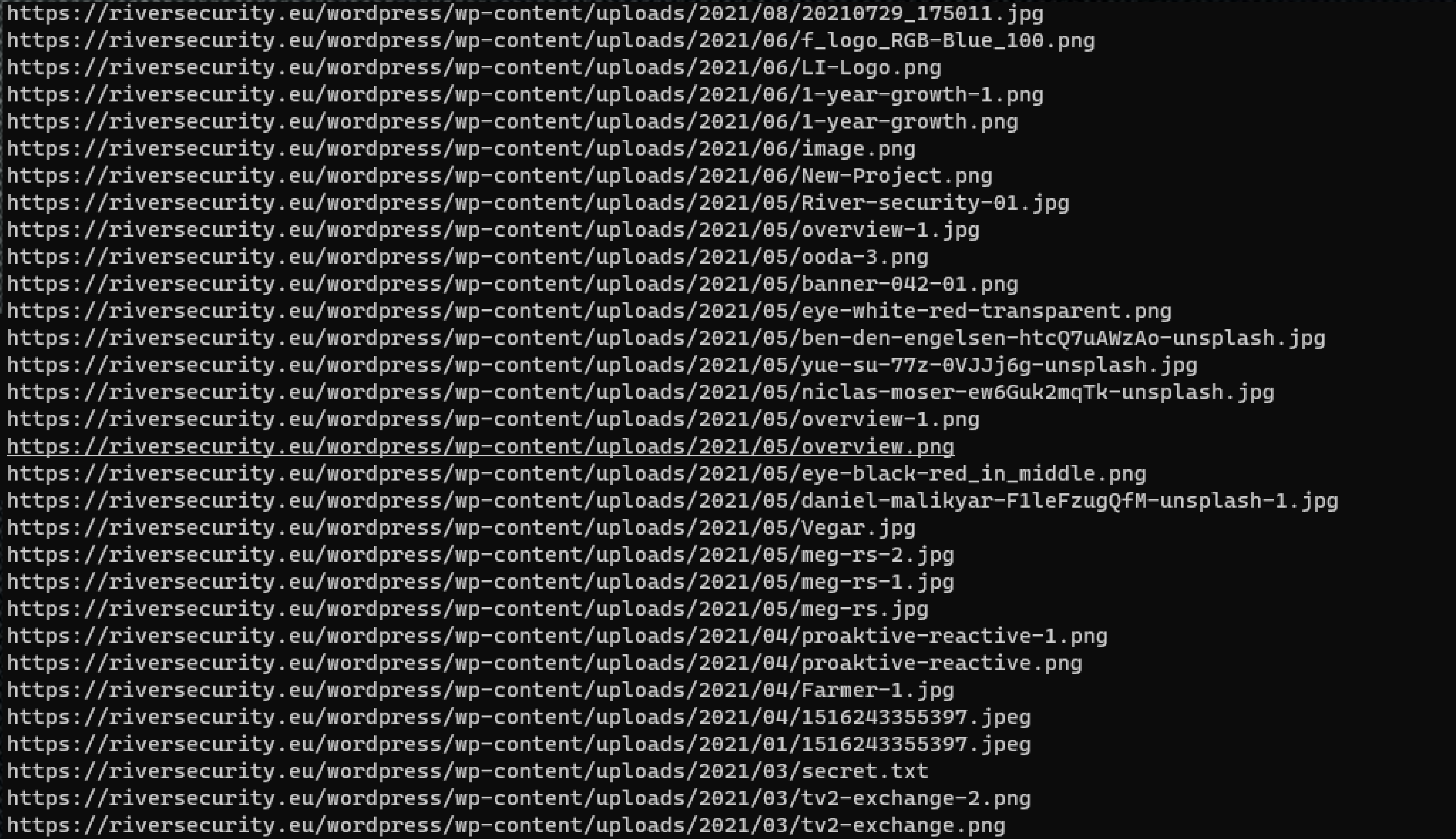


```
PS C:\tmp\repos\IIS_shortname_Scanner> C:\Python27\python.exe .\iis_shortname_Scan.py https://[redacted]/metadatacard/
Server is vulnerable, please wait, scanning...
[+] /metadatacard/m~1.* [scan in progress]
[+] /metadatacard/me~1.*        [scan in progress]
[+] /metadatacard/met~1.*       [scan in progress]
[+] /metadatacard/meta~1.*      [scan in progress]
[+] /metadatacard/metad~1.*     [scan in progress]
[+] /metadatacard/metada~1.*    [scan in progress]
[+] /metadatacard/metada~1.z*   [scan in progress]
[+] /metadatacard/metada~1.zi*  [scan in progress]
[+] /metadatacard/metada~1.zip* [scan in progress]
[+] File /metadatacard/metada~1.zip*    [Done]
----------------------------------------------------------------
File: /metadatacard/metada~1.zip*
----------------------------------------------------------------
0 Directories, 1 Files found in total
```

WordPress Enumeration



```
#USERS
Chris Dale,chris
Karina Aarland,karina
Krister Kvaavik,krister
Magnus Holst,magnus
silje,silje
#POSTS
```



```
https://riversecurity.eu/wordpress/wp-content/uploads/2021/08/20210729_175011.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/06/f_logo_RGB-Blue_100.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/06/LI-Logo.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/06/1-year-growth-1.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/06/1-year-growth.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/06/image.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/06/New-Project.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/River-security-01.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/overview-1.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/ooda-3.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/banner-042-01.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/eye-white-red-transparent.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/ben-den-engelsen-htcQ7uAWzAo-unsplash.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/yue-su-77z-0VJJj6g-unsplash.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/niclas-moser-ew6Guk2mqTk-unsplash.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/overview-1.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/overview.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/eye-black-red_in_middle.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/daniel-malikyar-F1leFzugQfM-unsplash-1.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/Vegar.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/meg-rs-2.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/meg-rs-1.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/05/meg-rs.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/04/proaktive-reactive-1.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/04/proaktive-reactive.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/04/Farmer-1.jpg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/04/1516243355397.jpeg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/01/1516243355397.jpeg
https://riversecurity.eu/wordpress/wp-content/uploads/2021/03/secret.txt
https://riversecurity.eu/wordpress/wp-content/uploads/2021/03/tv2-exchange-2.png
https://riversecurity.eu/wordpress/wp-content/uploads/2021/03/tv2-exchange.png
```

When You Don't Have MVP

Frameworks

- Create one
  - It is **minimum** viable
  - A starting point is better than nothing
- Dedicate days before the engagement to:
  - Build
  - Set-up
  - Configure
  - Break & Hack
  - Create CTF challenges ;)
- Create foundations for future hypothesis

Frameworks to help testing

OWASP ASVS

Technology Stacks

- It is rarely just a web-server
- Components are typically in-front and behind
- In-front we typically have:
  - Reverse Proxies
  - Web Application Firewalls
  - Caching, Content Delivery Networks
  - Load balancers
- Behind we typically have:
  - Databases, SQL, NoSQL, Key/value and more.
  - Files, folders and data
  - Micro-services
  - Search Engines

HTTP is Stateless

- In other words, HTTP does not automatically keep track of you
- Cookies, server-side, client-side
- Common client-side states involve:
  - Json Web Tokens (JWT)
  - .NET WebForms
- Server-side state are included in most development frameworks:
  - PHPSessionID
  - JSEssionID
  - .NETSessionID

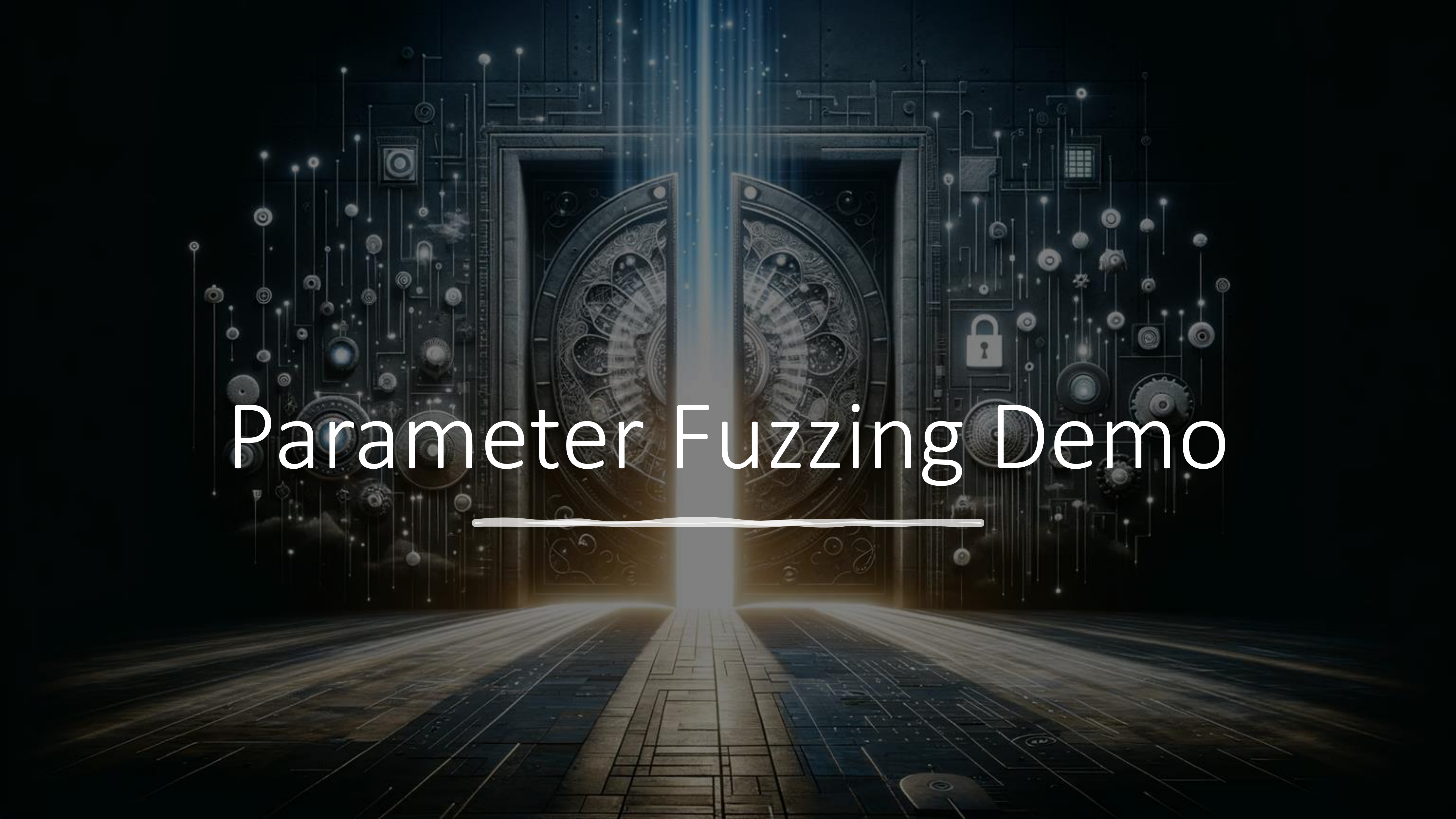
Methods and Parameters

- GET, POST
- Also other methods
  - PUT
  - DELETE
  - PATCH
- Parameters can be provided as path of URL or in Body
- Parameters as part of the Path
  - /getUser/:id/
  - /get/user/1337/?limit=true

Example HTTP Request and Reply

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
```

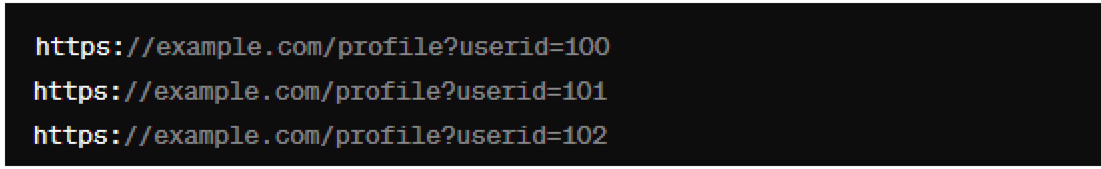
```
HTTP/1.1 200 OK
Date: Wed, 14 Oct 2020 12:28:53 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Sat, 10 Oct 2020 14:30:00 GMT Content-Length: 612
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip Connection: Closed

<!DOCTYPE html>
 <html> <head> <title>Example Domain</title> </head>
 <body>
 <h1>Example Domain</h1> <p>This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.</p>-
 </body> </html>
```



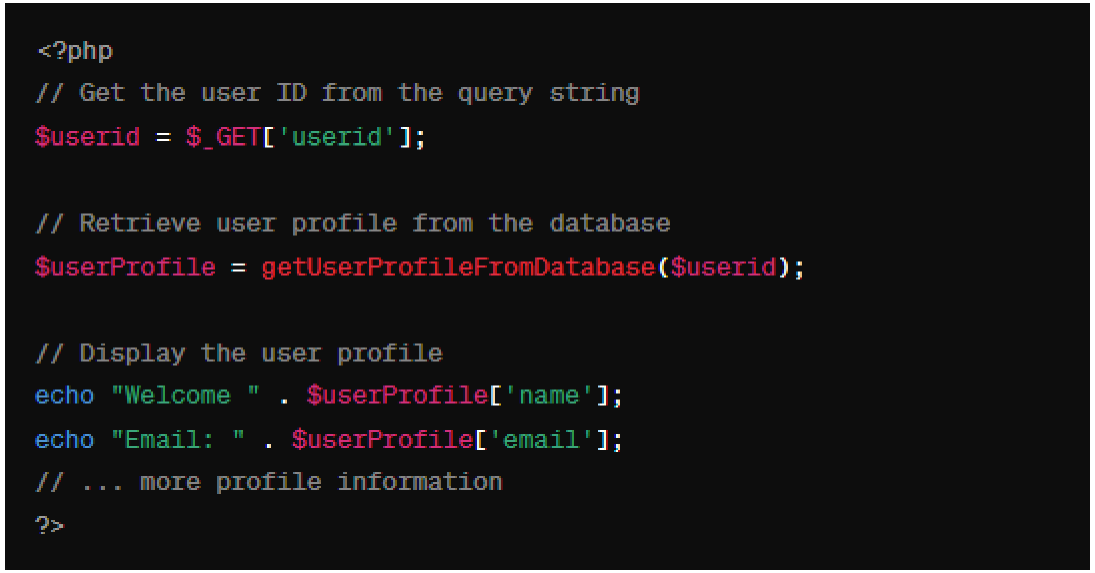
Parameter Fuzzing Demo

Magic Numbers

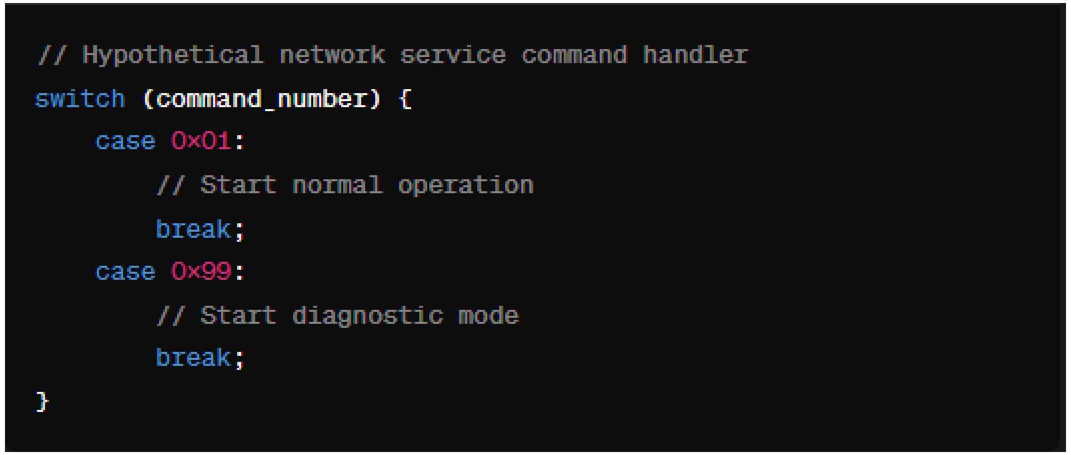
- What if you see a request with a number or predictable string?
- Don’t just not and accept
- Challenge and test
- What happens if we try another ID?
- Always require authentication, authorization, use non-predictable values



```
https://example.com/profile?userid=100
https://example.com/profile?userid=101
https://example.com/profile?userid=102
```



```php
<?php
// Get the user ID from the query string
$userid = $_GET['userid'];

// Retrieve user profile from the database
$userProfile = getUserProfileFromDatabase($userid);

// Display the user profile
echo "Welcome " . $userProfile['name'];
echo "Email: " . $userProfile['email'];
// ... more profile information
?>
```

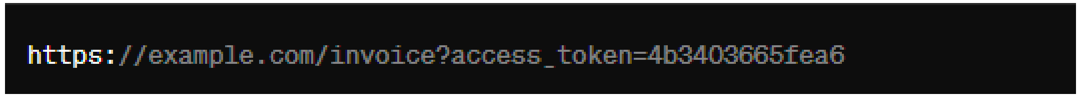


```
// Hypothetical network service command handler
switch (command_number) {
    case 0x01:
        // Start normal operation
        break;
    case 0x99:
        // Start diagnostic mode
        break;
}
```

Magic Number Demo

An Alternative to Magic Numbers

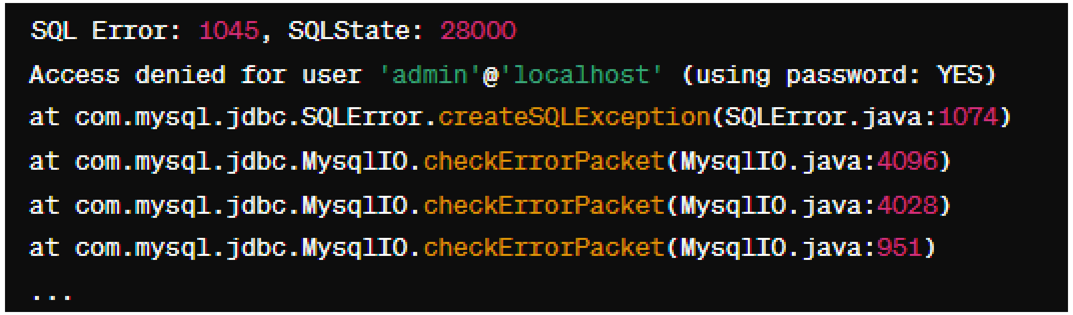
- GUID / UUID - 128-bit number used to uniquely identify information
  - 550e8400-e29b-41d4-a716-446655440000
  - f47ac10b-58cc-4372-a567-0e02b2c3d479
  - 5f9c0a0c-8d6a-40b4-8bbb-1ba16f1f5e4d
- Size and complexity makes them impossible to predict
  - Unless they use a predictable seed, e.g. computer systems MAC address, time or other non-random factors
  - Some UUID implementations focus on uniqueness, not predictability



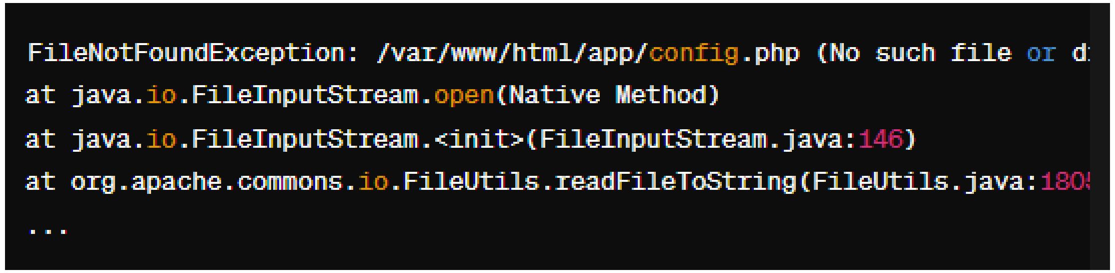
```
https://example.com/invoice?access_token=4b3403665fea6
```

Stack Traces

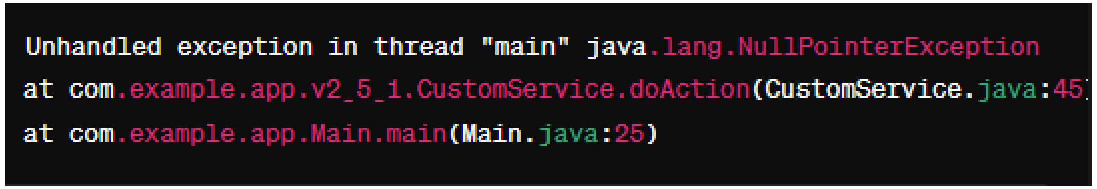
- Exposing these stack traces help attackers develop a targeted attack
- If we don’t expose these, attackers are blind…
- “But we need them” – developers will say…



```
SQL Error: 1045, SQLState: 28000
Access denied for user 'admin'@'localhost' (using password: YES)
at com.mysql.jdbc.SQLError.createSQLException(SQLError.java:1074)
at com.mysql.jdbc.MysqlIO.checkErrorPacket(MysqlIO.java:4096)
at com.mysql.jdbc.MysqlIO.checkErrorPacket(MysqlIO.java:4028)
at com.mysql.jdbc.MysqlIO.checkErrorPacket(MysqlIO.java:951)
...
```



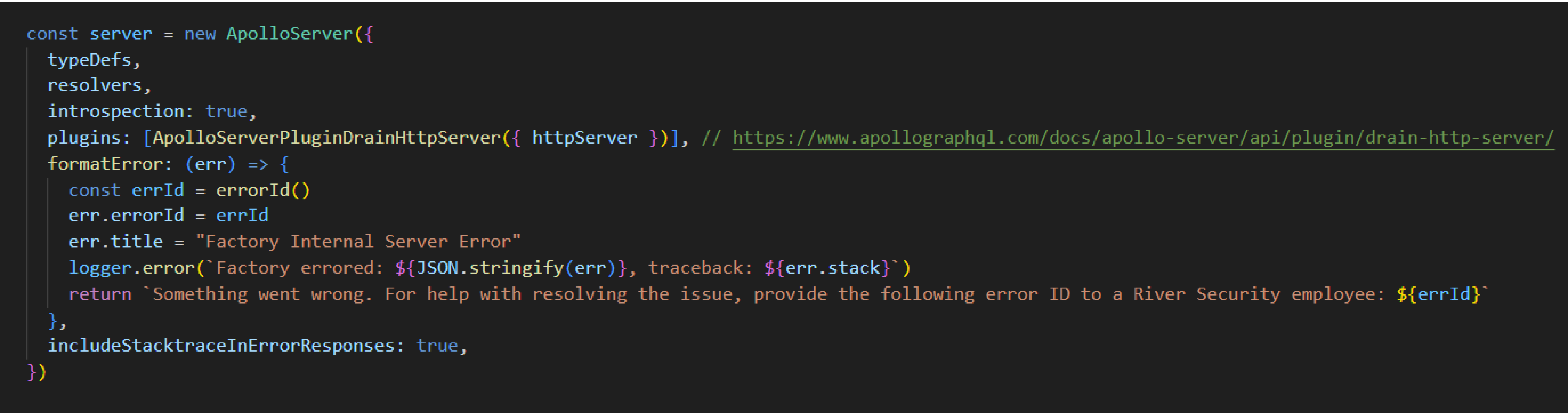
```
FileNotFoundException: /var/www/html/app/config.php (No such file or d
at java.io.FileInputStream.open(Native Method)
at java.io.FileInputStream.<init>(FileInputStream.java:146)
at org.apache.commons.io.FileUtils.readFileToString(FileUtils.java:180
...
```



```
Unhandled exception in thread "main" java.lang.NullPointerException
at com.example.app.v2_5_1.CustomService.doAction(CustomService.java:45
at com.example.app.Main.main(Main.java:25)
```

Error Conditions

- Never reveal detailed stack-traces to the user in production
- It greatly aids hackers



```
const server = new ApolloServer({
  typeDefs,
  resolvers,
  introspection: true,
  plugins: [ApolloServerPluginDrainHttpServer({ httpServer })], // https://www.apollographql.com/docs/apollo-server/api/plugin/drain-http-server/
  formatError: (err) => {
    const errId = errorId()
    err.errorId = errId
    err.title = "Factory Internal Server Error"
    logger.error(`Factory errored: ${JSON.stringify(err)}, traceback: ${err.stack}`)
    return `Something went wrong. For help with resolving the issue, provide the following error ID to a River Security employee: ${errId}`
  },
  includeStacktraceInErrorResponses: true,
})
```

Good Logging – 5 W, 1 H

We want logs to give the consumers **valuable** information, including security information

- Who, What, Where, When, Why, How

```
2023-04-05 14:32:07  - INFO -  Where: User Authentication Module  -
 Who: User ID 12345  IP Address 192.168.1.25  -  What: Login Attempt
-  When: 2023-04-05T14:32:07Z  -  How: Standard Login Form  -  Why:
User Initiated Login Process
```

Example

```
INFO - Transaction Completed -  Who: User ID 98765  -  What: Purchase  -  When: 2023-09-15T14:45:03Z  -  Where: Checkout Page  -  Why: User initiated purchase after adding items to cart  -  How: Credit Card Payment  Card Type: Visa  Amount: $150.00  Transaction ID: 123456789abc
```

- Who: User ID 98765. Identifies the specific user who made the transaction.
- What: Purchase. Specifies the action or event, in this case, a completed transaction.
- When: 2023-09-15T14:45:03Z. Provides a precise timestamp of when the transaction was completed.
- Where: Checkout Page. Indicates the part of the system or application where the event occurred.
- Why: User initiated purchase after adding items to cart. Gives context for the action, explaining the user's intention or the cause of the event.
- How: Credit Card Payment, Card Type: Visa, Amount: $150.00, Transaction ID: 123456789abc. Describes the method of transaction, including payment method, card type, amount, and transaction identifier for tracking and verification.

Bad Logging

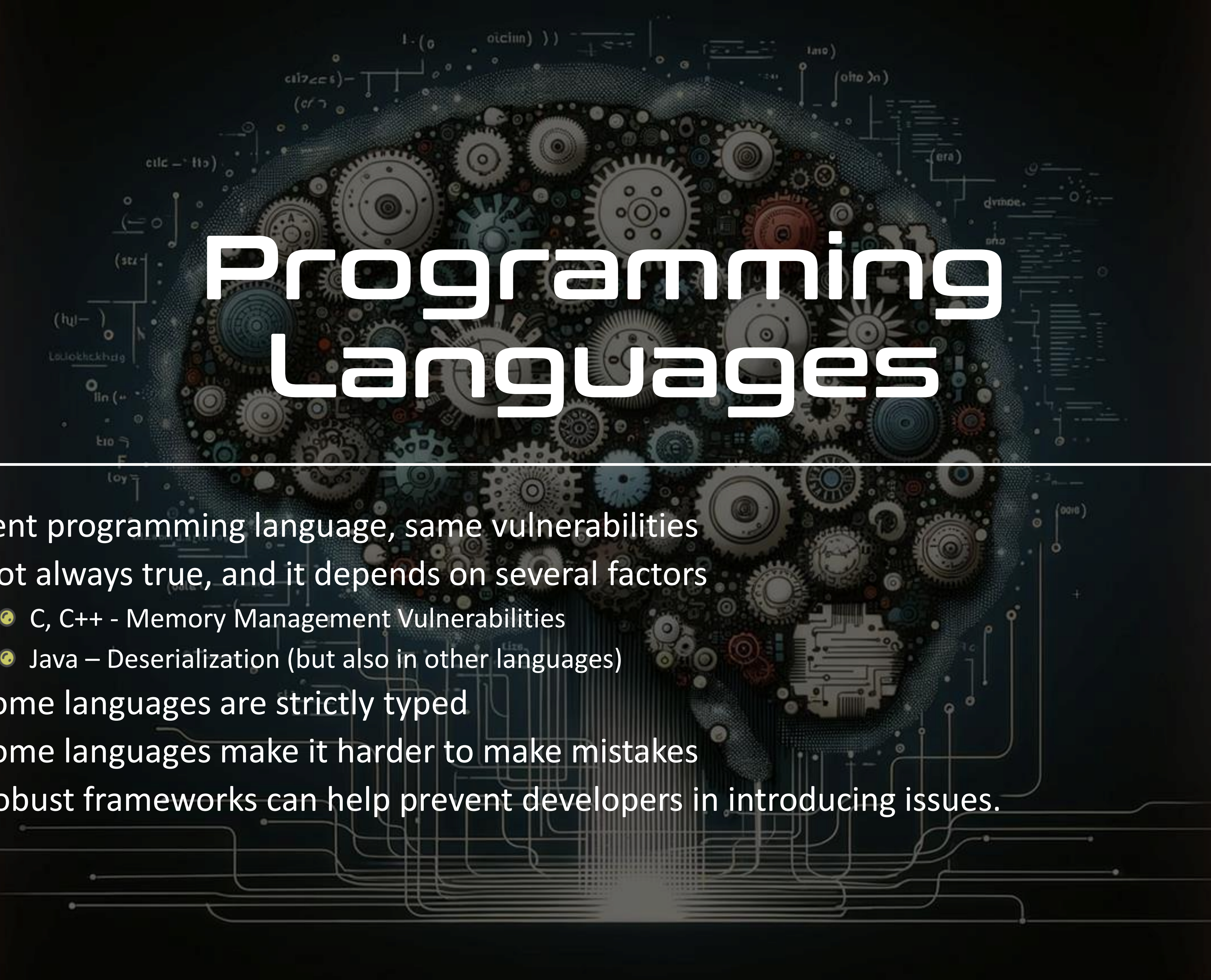
- INFO - User logged out successfully
- [2024-02-05 19:15:32] - DEBUG - Button X clicked. Color changed to blue. Window resized to 800x600. Scroll position updated. User viewed tooltip text.
- Error encountered. User=1234 Time=9:15

ERROR: 404 Not Found. 2024-01-05. Page=/home

- [2024-01-05 10:05:22] - ERROR - Something went wrong
- [2023-12-05 09:15:32] - INFO - User Login - Username: admin, Password: ExpectCloudyWeather2024!

Headers

- HSTS and CSP
- Redirects
- Compression
- Caching
- Vhost
- Content-type
- Authentication requirements
- Server Information and Custom Headers



Programming Languages

- Different programming language, same vulnerabilities
  - Not always true, and it depends on several factors
    - C, C++ - Memory Management Vulnerabilities
    - Java – Deserialization (but also in other languages)
  - Some languages are strictly typed
  - Some languages make it harder to make mistakes
  - Robust frameworks can help prevent developers in introducing issues.

Encoding

- Not encryption
- Implies decoding if algorithm is known
  - No key involved
- Character encodings (e.g., ASCII, UTF-8)
- Data serialization formats (e.g., JSON, XML)
- Content encoding for compression (e.g., gzip)
- Audio/video encoding (e.g., AAC, H.264)
- Image encoding (e.g., JPEG, PNG)

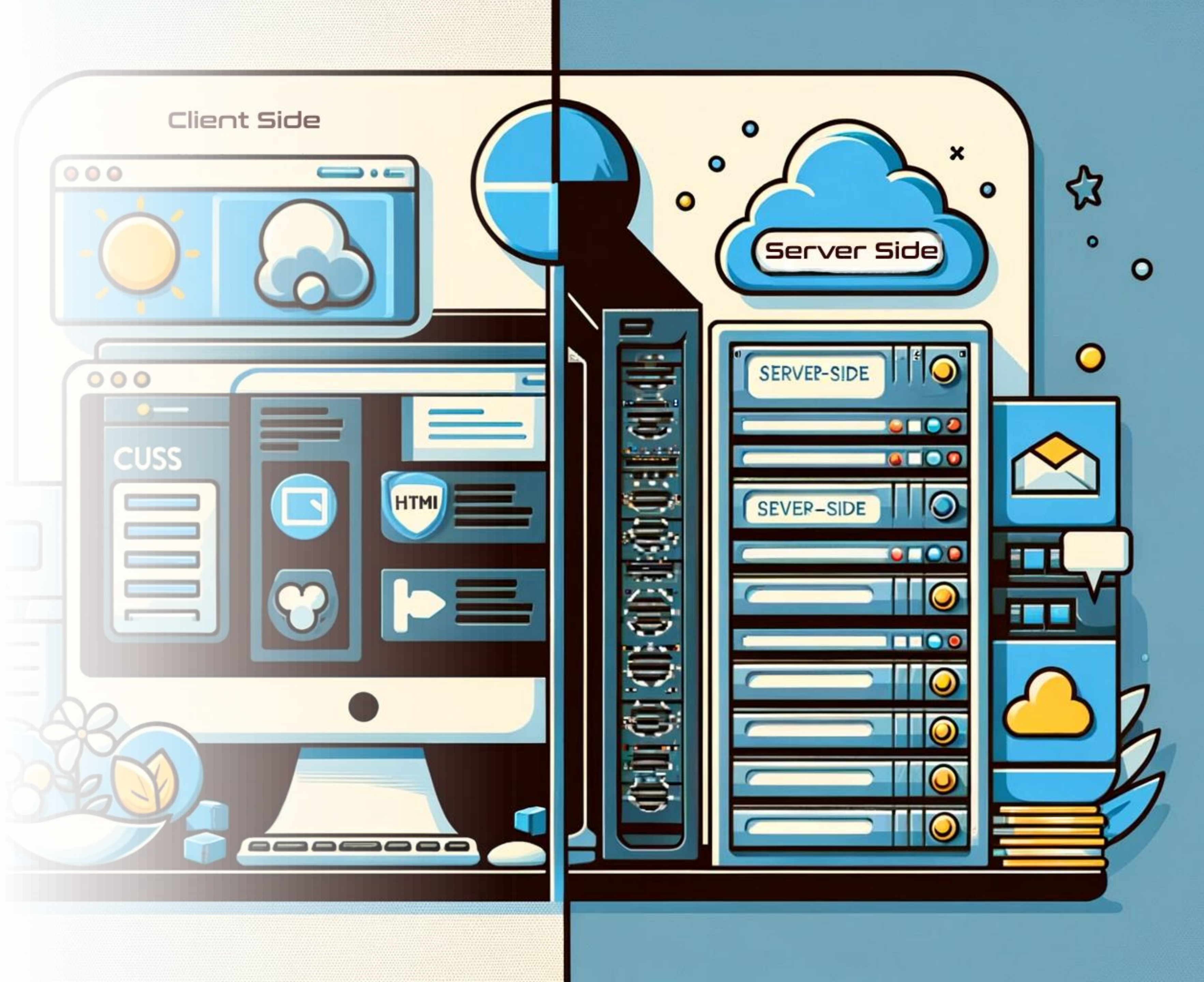
Encryption

- Data at Rest vs. Data in Transit
- What good is data at rest encryption?
- Key Management and Rotation is necessary
- Asymmetric Encryption is strong, but impacts performance
- Symmetric Encryption is fast, but key management is challenging

Crypto Demo

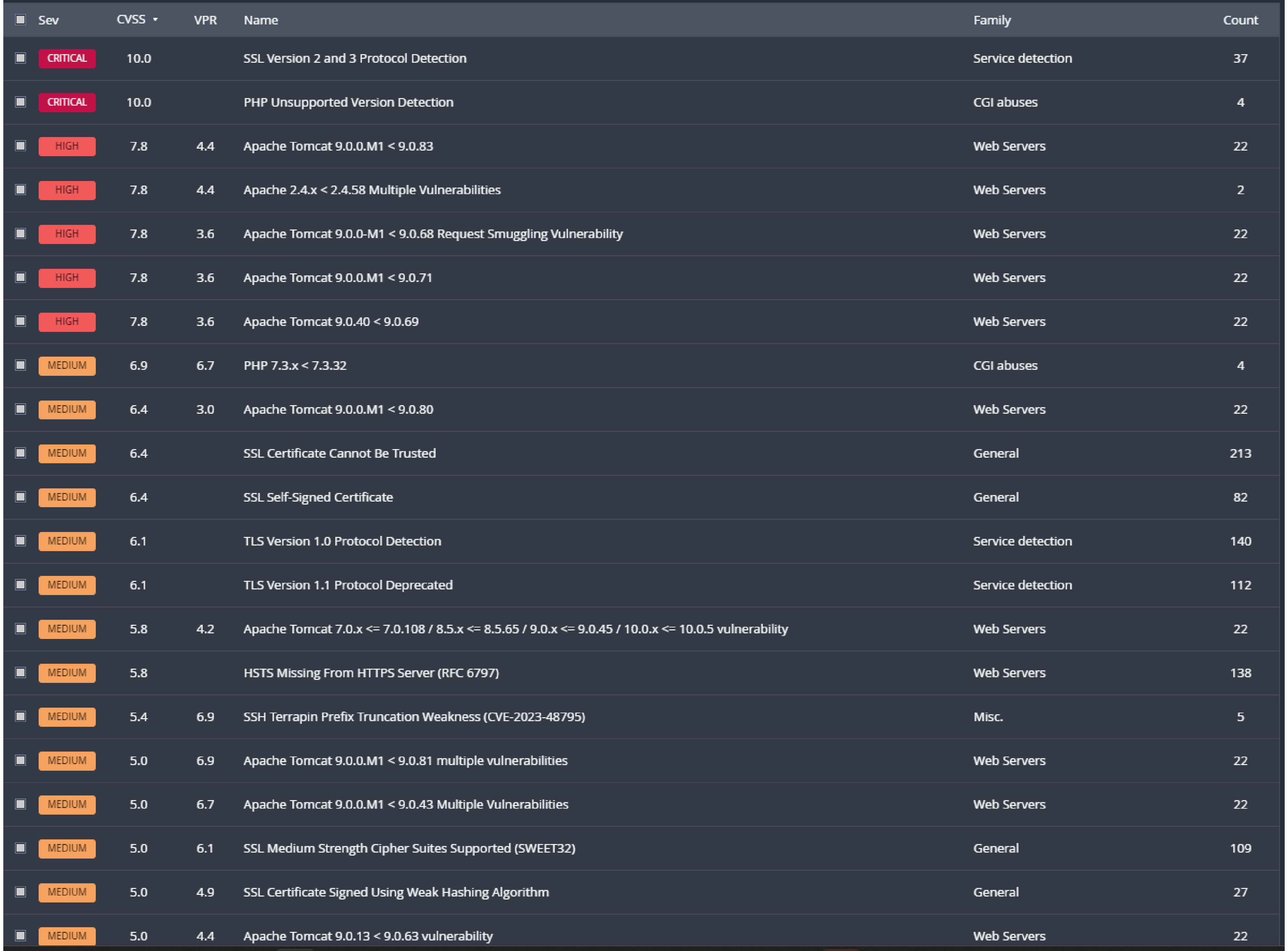
Client Side vs. Server Side

- Validation can happen in client-side
- But it must be present on the server-side
- Client side is for usability and performance
- Server side is for integrity and security



Common Security Scanner Findings

- Why are these a big deal or not?
- Crypto/SSL/TLS findings
- Missing CSRF, HSTS, Other Best Practices
- Programming Language Unsupported
- Application and/or Web Server Out-Dated



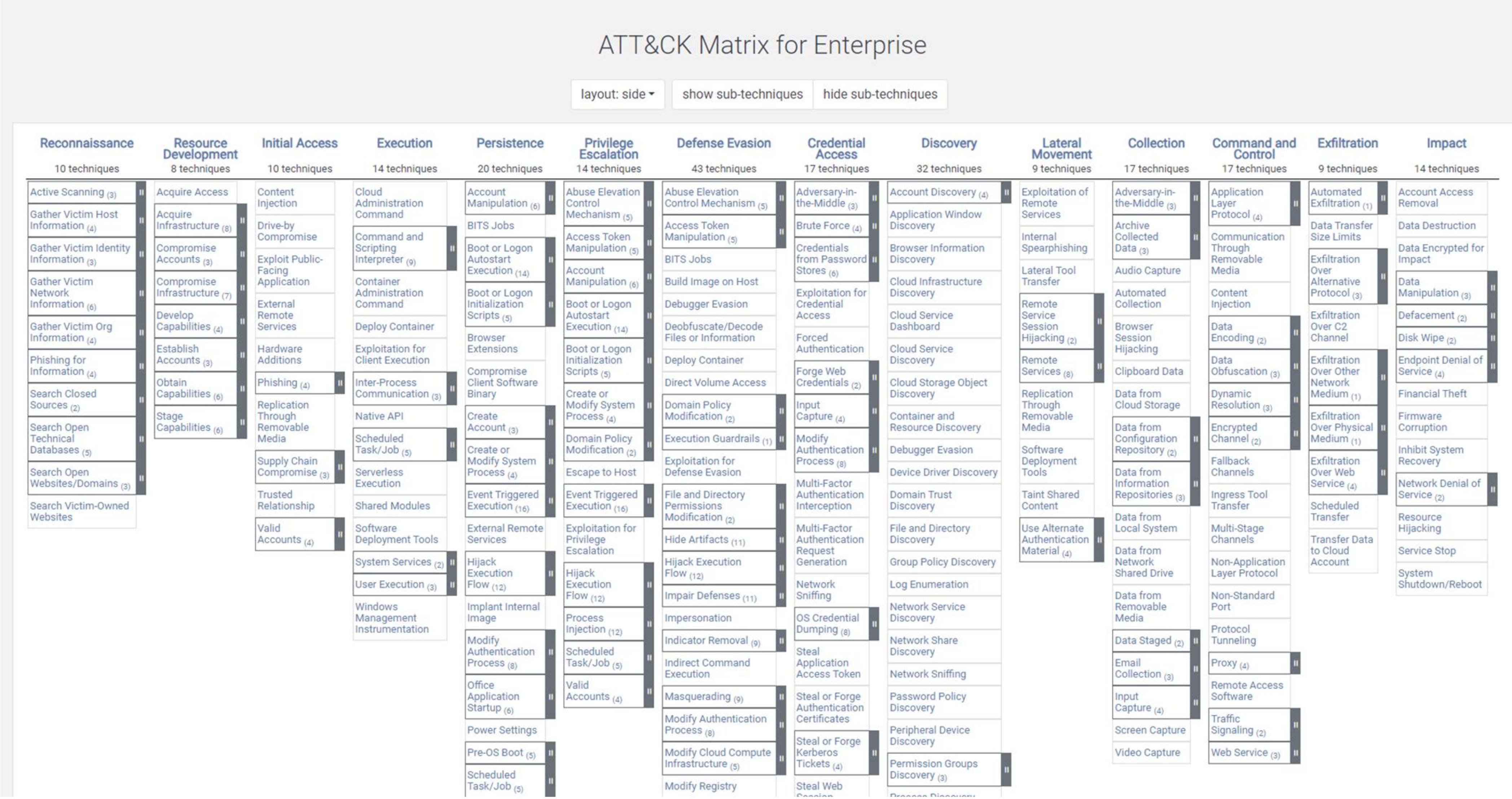
Privacy By Design

- Data Minimization
- End-to-End Encryption
- Anonymization and Pseudonymization
- Transparency and User Control
- Privacy-Enhancing Technologies (PETs)
- Default Privacy Settings
- Privacy Impact Assessments

Kill Chains

- Multiple different ones out there
- But let us check MITRE ATT&CK

Kill Chains



ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (11)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Proxy (4)		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Remote Access Software		
				Pre-OS Boot (5)		Impersonation	Steal Web Session	Network Share Discovery		Screen Capture	Traffic Signaling (2)		
				Scheduled Task/Job (5)		Indicator Removal (9)		Network Sniffing		Video Capture	Web Service (3)		
						Indirect Command Execution		Password Policy Discovery					
						Masquerading (9)		Peripheral Device Discovery					
						Modify Authentication Process (8)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (5)		Process Discovery					
						Modify Registry							

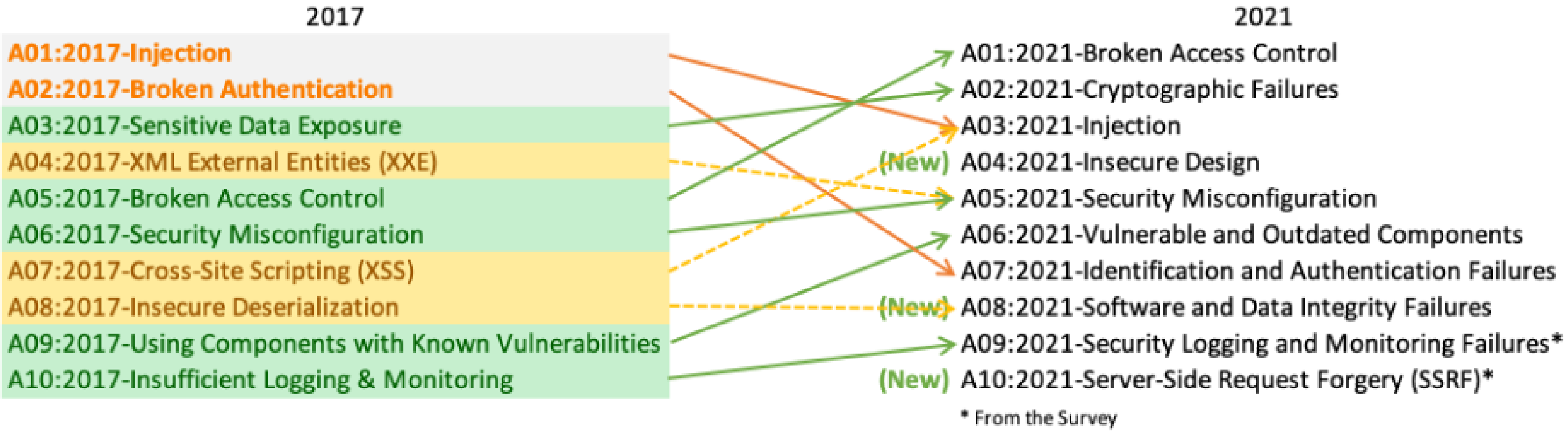
Section Two

Understanding Security Vulnerabilities

The Fundamentals: OWASP TOP 10

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

- API1:2023 - Broken Object Level Authorization
- API2:2023 - Broken Authentication
- API3:2023 - Broken Object Property Level Authorization
- API4:2023 - Unrestricted Resource Consumption
- API5:2023 - Broken Function Level Authorization
- API6:2023 - Unrestricted Access to Sensitive Business Flows
- API7:2023 - Server Side Request Forgery
- API8:2023 - Security Misconfiguration
- API9:2023 - Improper Inventory Management
- API10:2023 - Unsafe Consumption of APIs



2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Injection

What is injection?

The attacker sends text that exploit the syntax of the targeted interpreter.

Any data coming from other systems, scripts or especially from users should **never** be trusted before proper sanitation is put in place.

login
already have an account
usernam
passwo
*Name
*Emai
*I am contacting
Nettuts+
Choose an image to upload
Browse...
We take GIF, JPG, & PNG images
Add a message and post it
□ Check this if you do not want this photo posted
upload
php
SUPER
CLEAN
FORMULA

Let Us Take a Closer Look

- SQL Injection – Attacking connected service
- Cross-Site Scripting (XSS) – Attacking users
- Command Injection – Attacking the server

SQL Injection – Just to make sure we get it

Query: SELECT * FROM users WHERE username=$name AND password = $pw

Data:

Userid	Username	Password
1	Admin	1234admin5678
2	Sylvester	stall0wned
3	Arnold	Musclemania2024

Username: Admin
Password: 1234admin5678

```
SELECT * FROM users WHERE username = ‘Admin’
            AND password = ‘1234admin5678’
```

Injection:

Username: Admin
Password: myPassword' OR 1=1;--

```
SELECT * FROM users WHERE username = ‘Admin’
            AND password = ‘myPassword’ OR 1=1;--’
```

SQL Injection

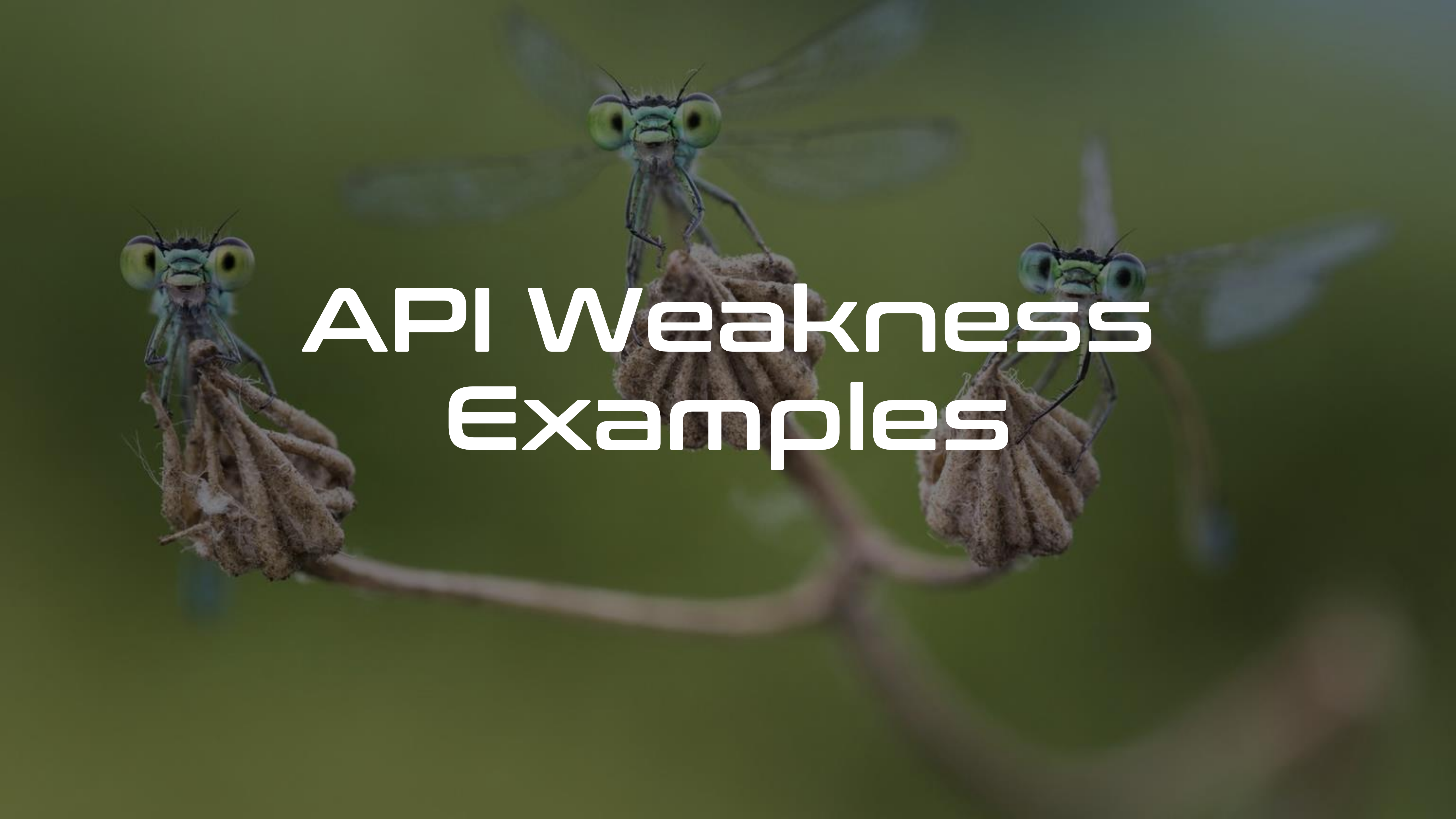
- We are attacking the QUERY language and the database behind the application
- Databases come in many shapes and forms
- Let us demo and walk through

Cross Site Scripting

- Input from users are reflected onto the website, for other users to see
- What if this input is not sanitized?
- Could it be misinterpreted as command and markup, not data?
- With XSS we are attacking the USERS of the system
- Let us demo this and walk through it

Command Injection

- Developers are lazy and can often find use of the operating system to help them out
- Operating Systems can often execute multiple commands
- What if you can input such an additional command?
- Let us demo and walk through this



API Weakness Examples

API1:2023 - Broken Object Level Authorization

- An attacker changes the userID parameter in a GET request to access another user's personal messages.
- A user modifies the accountID in a banking transaction API call to view someone else's account balance.
- An API call to retrieve a user's documents does not check if the requester has permissions for those documents, leading to unauthorized access.

API2:2023 - Broken Authentication

- An API endpoint allows the use of default, weak, or well-known passwords, which can be easily guessed.
- Session tokens are not rotated after login, allowing an attacker to reuse an old session token.
- An API does not enforce multi-factor authentication, allowing an attacker to gain access with just stolen credentials.

API3:2023 - Broken Object Property Level Authorization

- An API returns a JSON object with confidential user details when a non-admin user requests their profile information.
- A user is able to retrieve other users' email addresses by manipulating the response object properties.
- An endpoint for updating user details does not properly check properties being updated, allowing an attacker to modify roles or permissions.

Roifiiunation
API03 3
Object Propertty Leel Authizization
vistuze the brobject your properyty Level Authiforization

API4:2023 - Unrestricted Resource Consumption

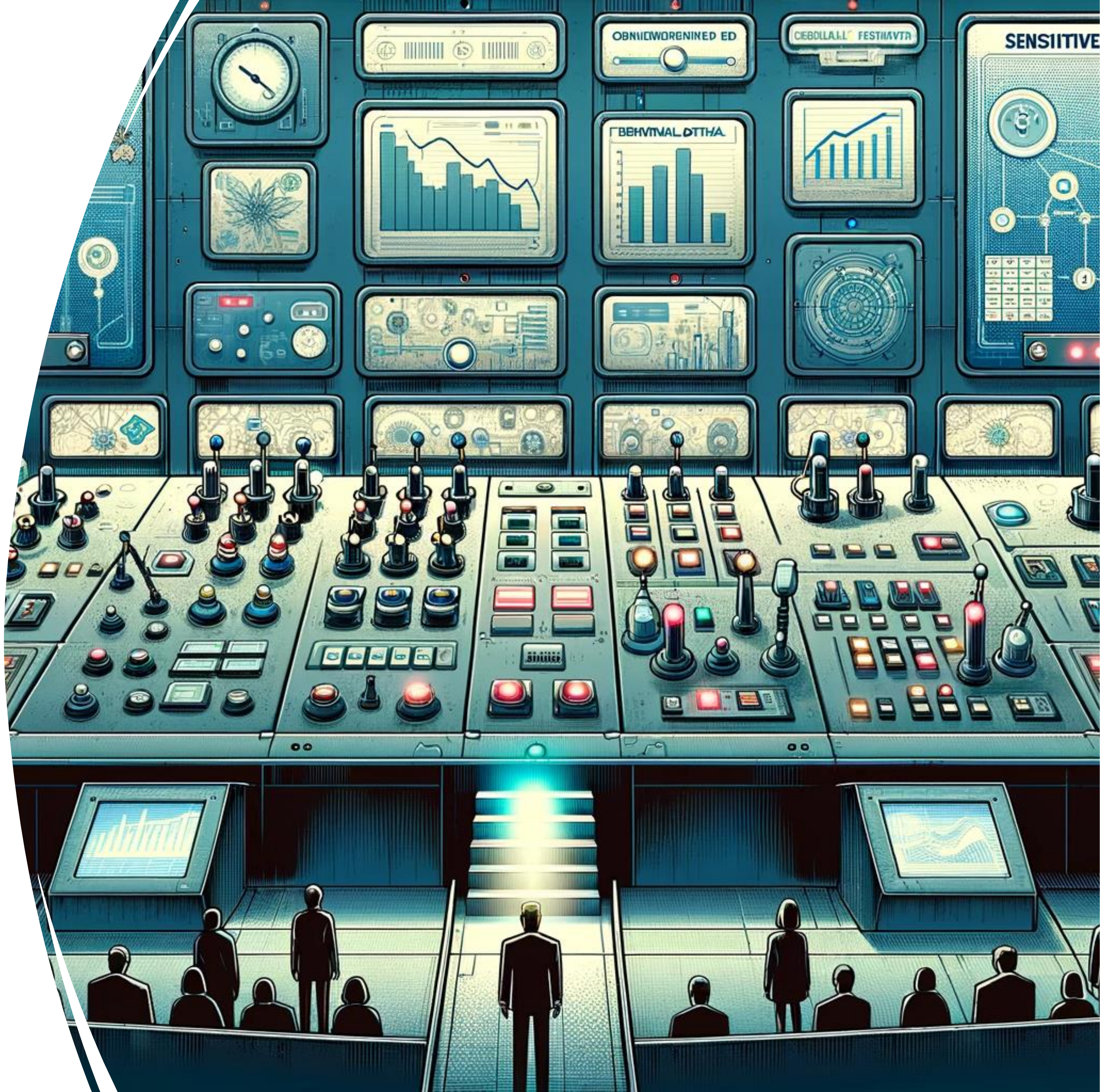
- An API allows the client to fetch all records in a database without pagination, causing excessive memory use.
- A file upload API does not limit the size of an upload, allowing an attacker to fill the server's disk space.
- An API endpoint for data processing does not have a timeout, allowing CPU-intensive requests to hog system resources.

API5:2023 - Broken Function Level Authorization

- A non-administrative user is able to access an admin-only API endpoint due to improper role checks.
- An endpoint for deleting users is accessible by any authenticated user, rather than just system administrators.
- A regular user can access an API function to grant permissions to other users due to missing function-level authorization checks.

API6:2023 - Unrestricted Access to Sensitive Business Flows

- An API that approves credit applications does not verify the role of the requester, allowing any employee to approve applications.
- An endpoint that is used to start a batch job for financial report generation can be triggered by any user in the system.
- A payment initiation API does not implement proper workflow checks, allowing users to bypass normal transaction approval processes.



API7:2023 - Server Side Request Forgery (SSRF)

- An API that fetches images from a URL provided by the user can be exploited to access internal services from the server's perspective.
- An API endpoint accepts file paths for logging purposes, which can be exploited to access system files.
- A cloud service API does not sanitize user input for URLs, leading to internal metadata services being accessed.

API8:2023 - Security Misconfiguration

- An API server with verbose error messages exposes stack traces that include function names and file paths.
- An API endpoint is unintentionally exposed to the public due to incorrect security group settings in the cloud.
- API keys are stored in a public repository, allowing unauthorized users to access the API.

API9:2023 - Improper Inventory Managemen

- A deprecated version of an API lacking current security features is still accessible, exposing the system to known vulnerabilities.
- An organization is unaware that a development API endpoint is publicly accessible.
- A company does not realize that an API endpoint with a testing database, including real user data, is exposed to the internet.

API10:2023 – API10:2023 - Unsafe Consumption of APIs

- An application blindly trusts data from an external API, leading to cross-site scripting (XSS) vulnerabilities.
- An app integrates with a third-party API without enforcing encryption, allowing data to be intercepted in transit.
- An external weather API is consumed without rate limiting, and the third-party provider experiences a breach, leading to a data leak of API request logs.

Principles of Security Testing

Preface

- Garbage In – Garbage Out
  - Unfortunately, many developers are not defensive
  - Chosen to trust data-sources or does not realize which can be manipulated
- Many developers rely on online sources for solving problems
- Developers know about cyber security
  - But does not know how to audit, test or realize if their code is vulnerable

I Did Some Research

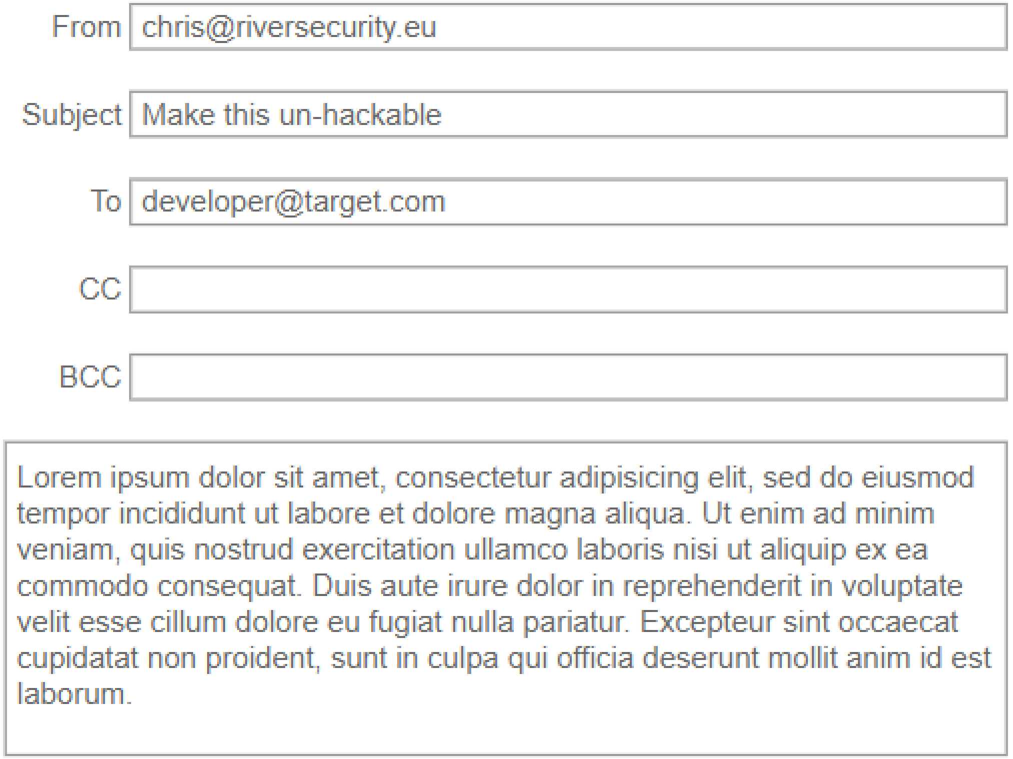
- GOOGLE RESULTS
- BOOKS
- SCHOOL & INSTITUTIONS
- COURSES

Imagine We Looked For

- XSS
- Command Injection
- SSRF
- XXE
- Direct Object references
- Type juggling
- File inclusion
- Template injection
- Password storage
- Serialization
- Least amount of privileges
- Xpath injection
- Cache poisoning
- CORS
- CSRF
- DOM-based XSS

Defensive Developers

- Ideally, developers should be defensive when coding
  - What input am I expecting, and how can I ensure it conforms?
  - I.e. input sanitization
- Where does it receive input from?
  Don’t trust <u>any</u> source
  - Database
  - User
  - Headers
  - Registry / files / whatever
- Always think:
  “allow list” before “deny list”
- Gracefully fail, always



From	chris@riversecurity.eu
Subject	Make this un-hackable
To	developer@target.com
CC	
BCC	

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Negative Testing

What Is Your Name?

Input a number

Upload a zip file

Our Objectives Should Be Clear

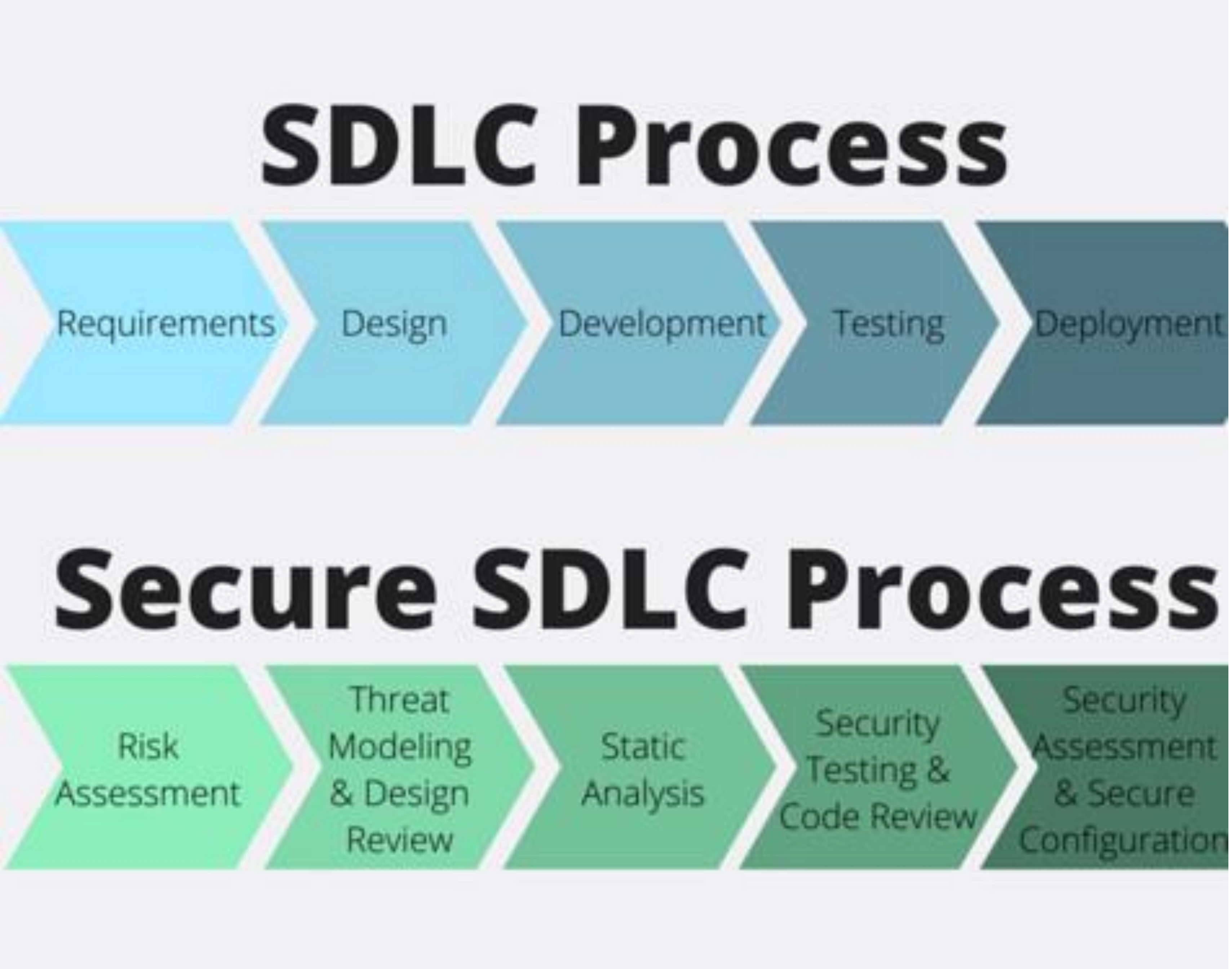
Identify, Map and Control risk

- Confidentially – Ensure sensitive data is only available to authorized users
- Integrity – Guarantee data can not be tampered
- Availability – Make sure the application and data is available when needed
- Authentication – Verify identity of users and systems
- Authorization – Preserve the fact users should only have access to which they have been granted
- Non-repudiation – Prevent users from denying their ations

Types of Security Testing

We’ve got to figure out where and what we want to be doing:

- Penetration Testing – Expert Field
- Vulnerability Scanning – “Anyone can do”
- Bug Bounty – You’re on the internet
- Auditing – Ask, Interview and Check
- Risk Assessment – Let’s plan it out



S-SDLC

- A Software Development Life Cycle where we attempt to make it Secure
- Keep in mind the word lifecycle implies:
  - Inception/Development
  - Operation/Use
  - Retirement/Unrollment
- Iterative Process

Other Kinds of Tesing

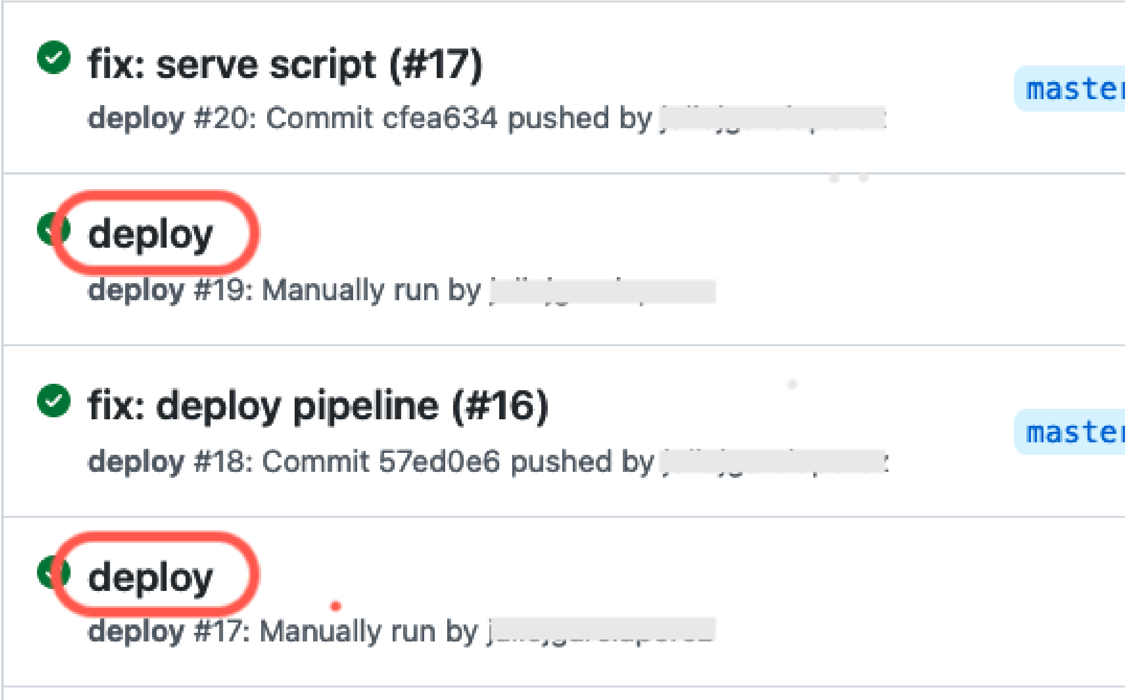
- Static Application Security Testing (SAST)
  - Analyzing source code for vulnerabilities without executing the program.
- Dynamic Application Security Testing (DAST)
  - Analyzing running applications for vulnerabilities.
- Interactive Application Security Testing (IAST)
  - Combines SAST and DAST by testing applications from within using software instruments.
- Software Composition Analysis (SCA)
  - Identifying and analyzing open-source components within the software to detect vulnerable libraries and licenses.

Test Automation

- Via scripts
  - Unit Tests
  - Regression Tests
  - Run as part of build workflows
- Recording
  - Graphical Testing via Selenium
  - In-browser recording
- Typically to verify things behave the same after deployments

CI / CD

- Continuous Integration and Continuous Deployment (CI/CD): Integrating code into a shared repository frequently, with automated build and test processes to facilitate continuous delivery.
- Get automatic feedback on test conditions
- Get feedback early, during commits and build phases



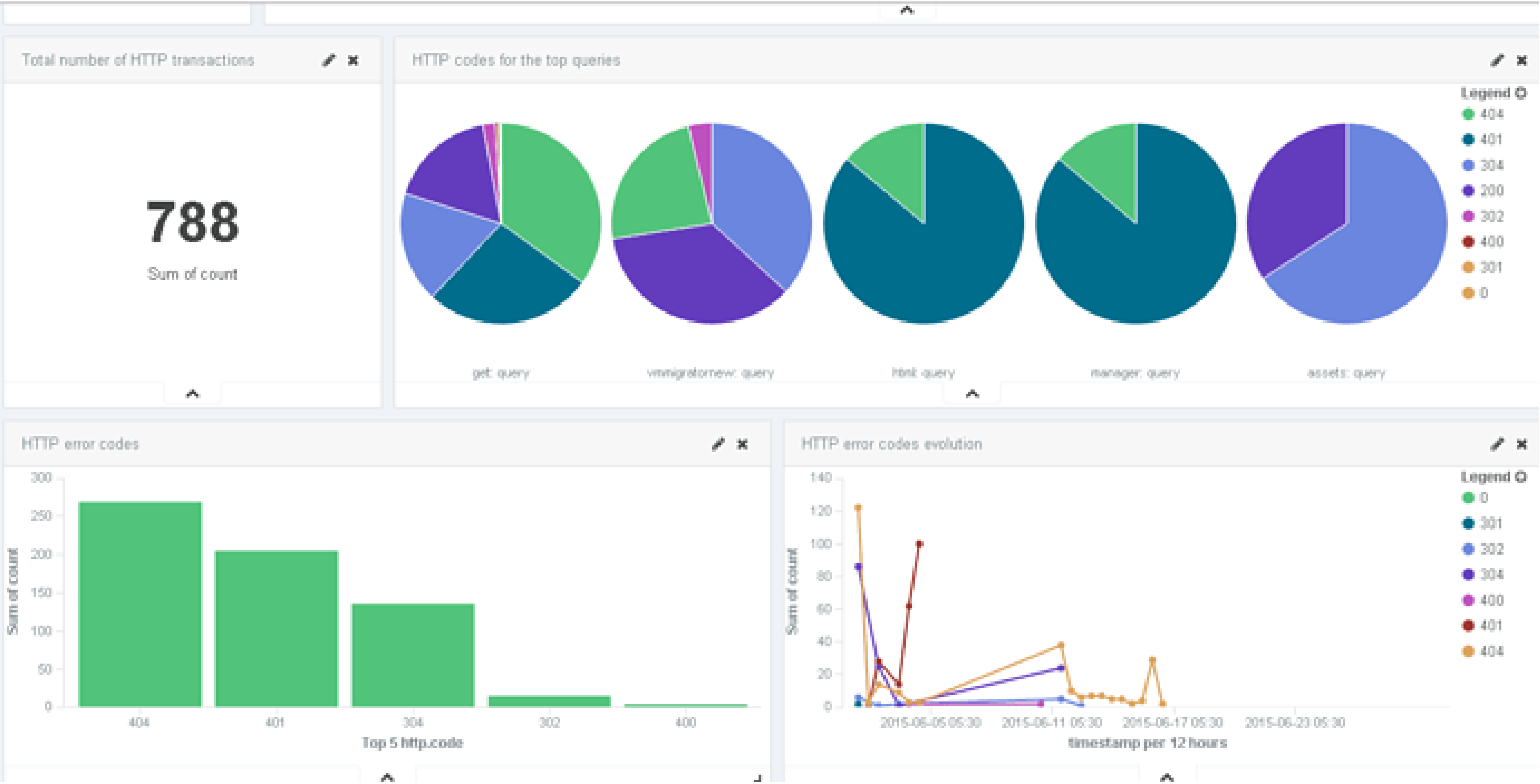
✓ **fix: serve script (#17)**
deploy #20: Commit cfea634 pushed by [redacted]
maste

✓ **deploy**
deploy #19: Manually run by [redacted]

✓ **fix: deploy pipeline (#16)**
deploy #18: Commit 57ed0e6 pushed by [redacted]
maste

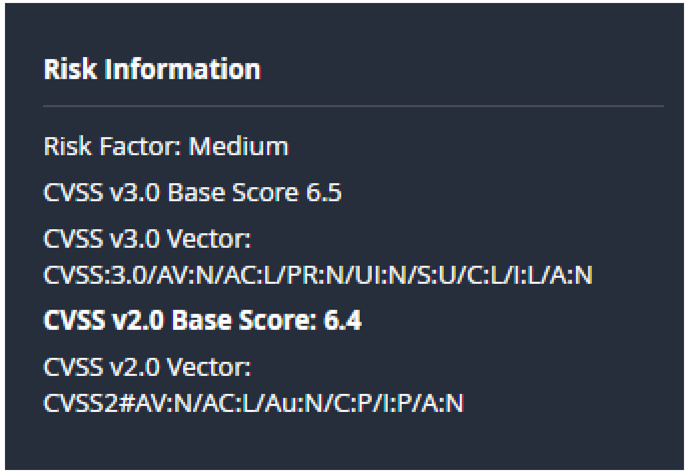
✓ **deploy**
deploy #17: Manually run by [redacted]

DevOps to Support



Scoring Vulnerabilities

- Objective vs. Subjective
- CVSS 3.1.1
- CVSS 4



Risk Information

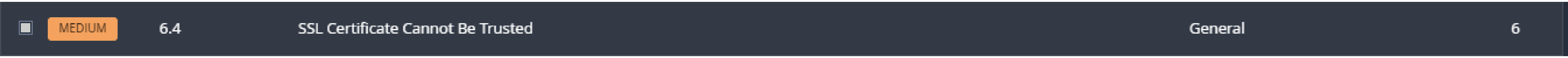
Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Base Score: 6.4

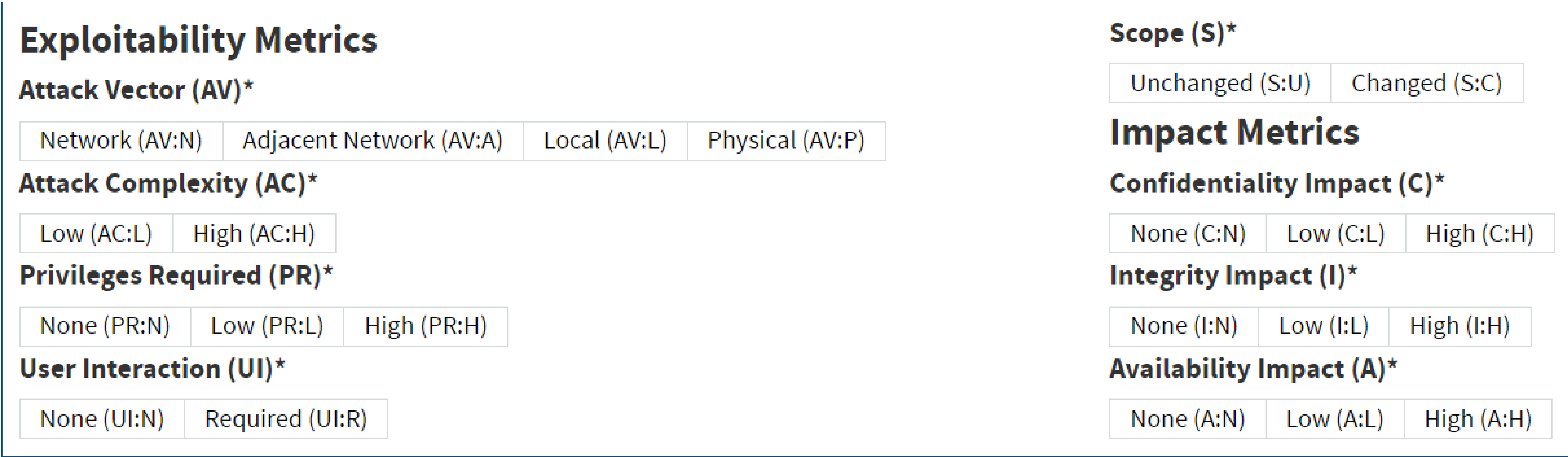
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N



□	MEDIUM	6.4	SSL Certificate Cannot Be Trusted	General	6

Assessment Questions

- Is this vulnerability due to my code?
- Is it a part of the framework I use?
- Does my code use the vulnerable function?
- Does the vulnerable function accept arbitrary input from user?
- Does the vulnerability affect my server or my users?
- Can a penetration tester actually use this to exploit something?



Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*

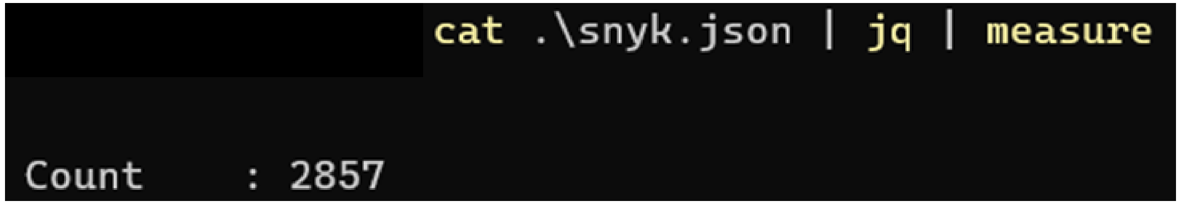
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

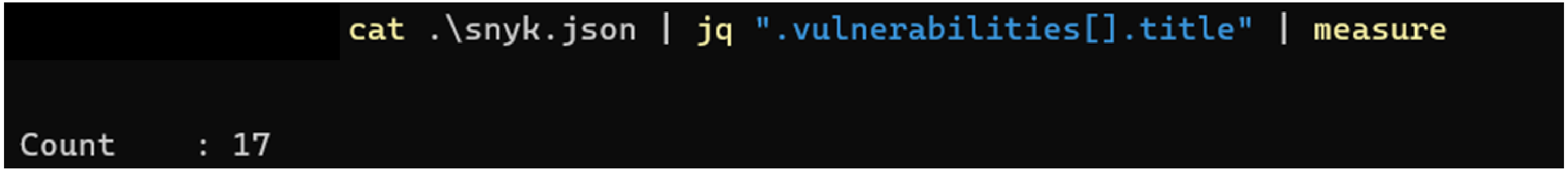
None (A:N) | Low (A:L) | High (A:H)

Snyk Output

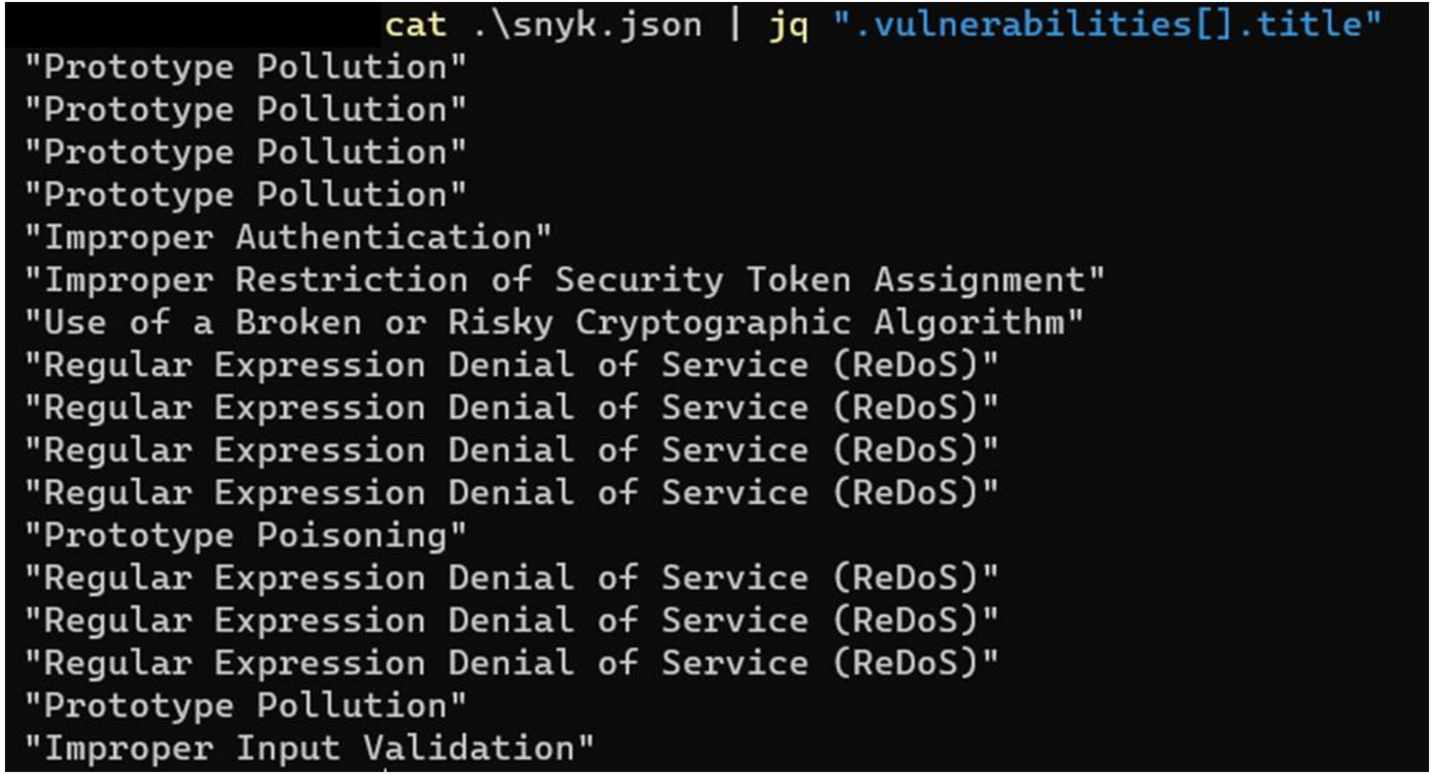
- Criticality
- Widespread win
- Quick-wins
- Long tail



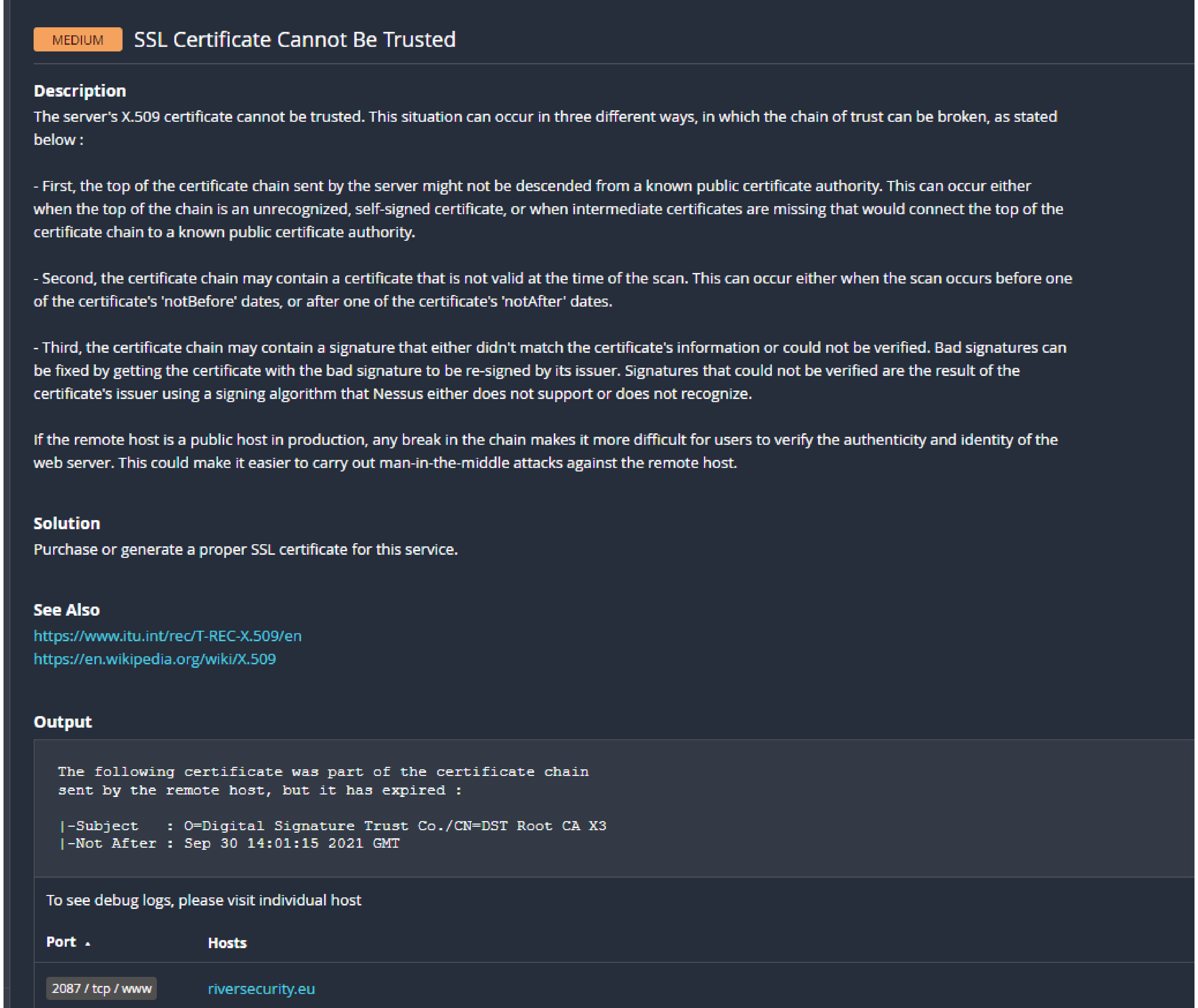
```
[redacted] cat .\snyk.json | jq | measure


Count    : 2857
```



```
[redacted] cat .\snyk.json | jq ".vulnerabilities[].title" | measure


Count    : 17
```



```
[redacted] cat .\snyk.json | jq ".vulnerabilities[].title"
"Prototype Pollution"
"Prototype Pollution"
"Prototype Pollution"
"Prototype Pollution"
"Improper Authentication"
"Improper Restriction of Security Token Assignment"
"Use of a Broken or Risky Cryptographic Algorithm"
"Regular Expression Denial of Service (ReDoS)"
"Regular Expression Denial of Service (ReDoS)"
"Regular Expression Denial of Service (ReDoS)"
"Regular Expression Denial of Service (ReDoS)"
"Prototype Poisoning"
"Regular Expression Denial of Service (ReDoS)"
"Regular Expression Denial of Service (ReDoS)"
"Regular Expression Denial of Service (ReDoS)"
"Prototype Pollution"
"Improper Input Validation"
```



MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Output

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Not After : Sep 30 14:01:15 2021 GMT
```

To see debug logs, please visit individual host

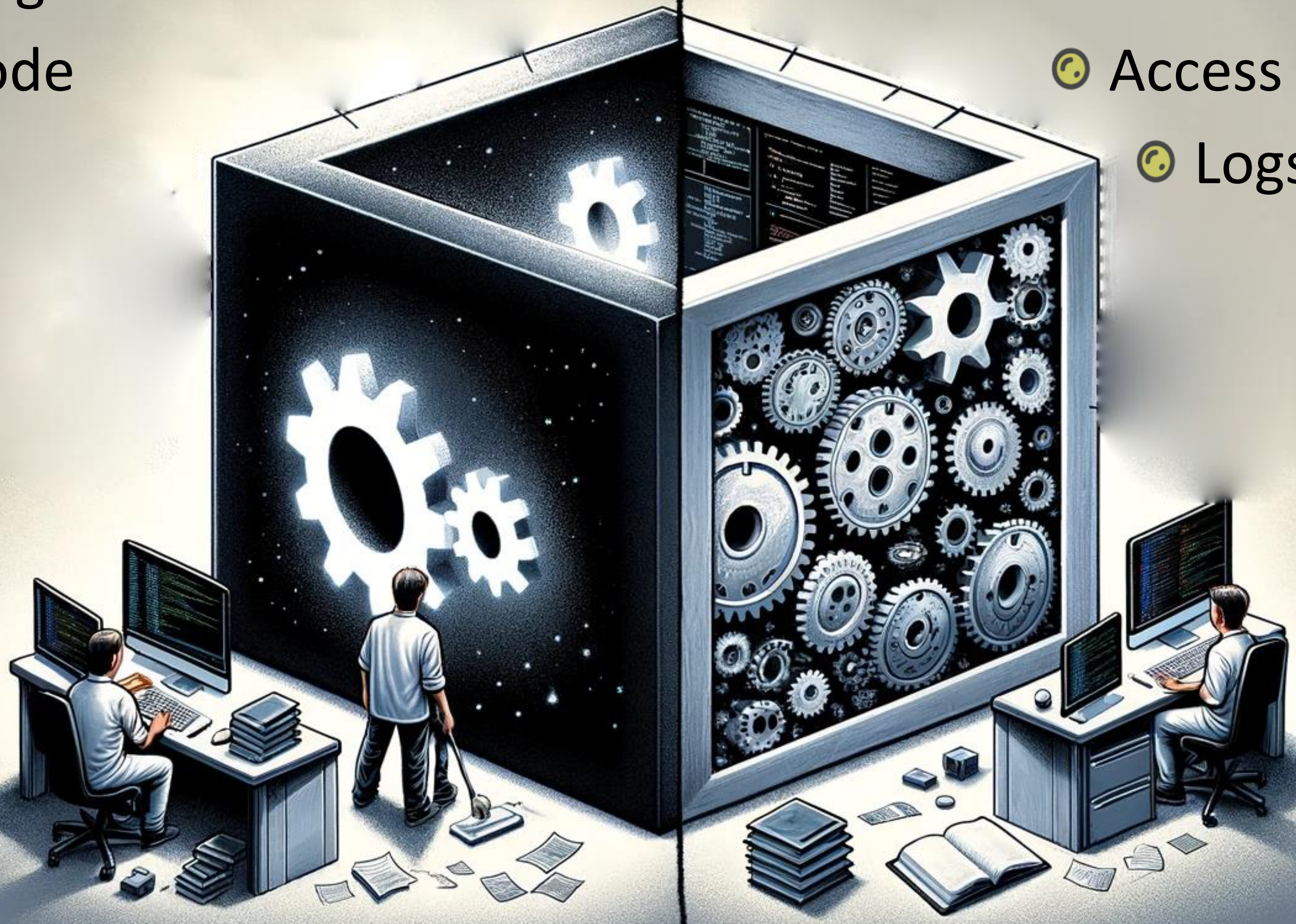
Port ▲	Hosts
2087 / tcp / www	riversecurity.eu

BLACK BOX TESTING

- Zero Knowledge
- No Source Code
- Do Your Best

WHITE BOX TESTING

- Full Knowledge
- Access to Source Code
- Logs and telemetry
- Nomeclature
- Training

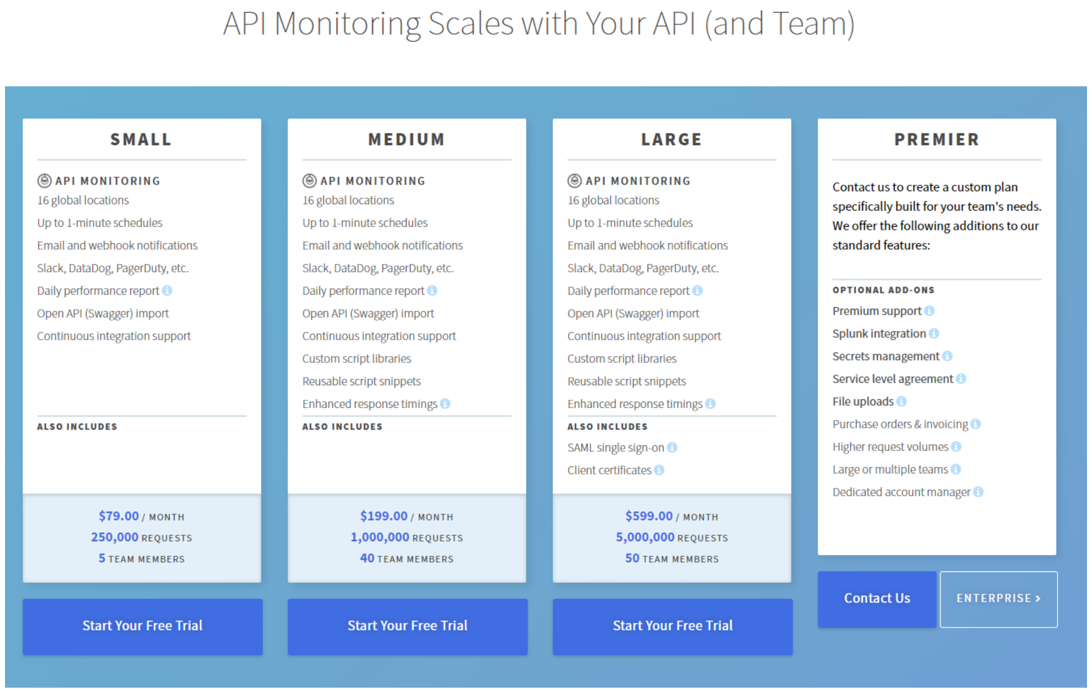


Threat Modelling

- Threat Modelling Can be Fun and Learning Exercise
- Help plan out the design
- Automate generation of risk
- Help conclude and understand designs attack surface

Performance Testing

- Performance Testing: Assessing the speed, scalability, and stability of the application under various conditions.



API Monitoring Scales with Your API (and Team)

SMALL

API MONITORING

16 global locations

Up to 1-minute schedules

Email and webhook notifications

Slack, DataDog, PagerDuty, etc.

Daily performance report

Open API (Swagger) import

Continuous integration support

ALSO INCLUDES

$79.00 / MONTH

250,000 REQUESTS

5 TEAM MEMBERS

MEDIUM

API MONITORING

16 global locations

Up to 1-minute schedules

Email and webhook notifications

Slack, DataDog, PagerDuty, etc.

Daily performance report

Open API (Swagger) import

Continuous integration support

Custom script libraries

Reusable script snippets

Enhanced response timings

ALSO INCLUDES

$199.00 / MONTH

1,000,000 REQUESTS

40 TEAM MEMBERS

LARGE

API MONITORING

16 global locations

Up to 1-minute schedules

Email and webhook notifications

Slack, DataDog, PagerDuty, etc.

Daily performance report

Open API (Swagger) import

Continuous integration support

Custom script libraries

Reusable script snippets

Enhanced response timings

ALSO INCLUDES

SAML single sign-on

Client certificates

$599.00 / MONTH

5,000,000 REQUESTS

50 TEAM MEMBERS

PREMIER

Contact us to create a custom plan specifically built for your team's needs. We offer the following additions to our standard features:

OPTIONAL ADD-ONS

Premium support

Splunk integration

Secrets management

Service level agreement

File uploads

Purchase orders & invoicing

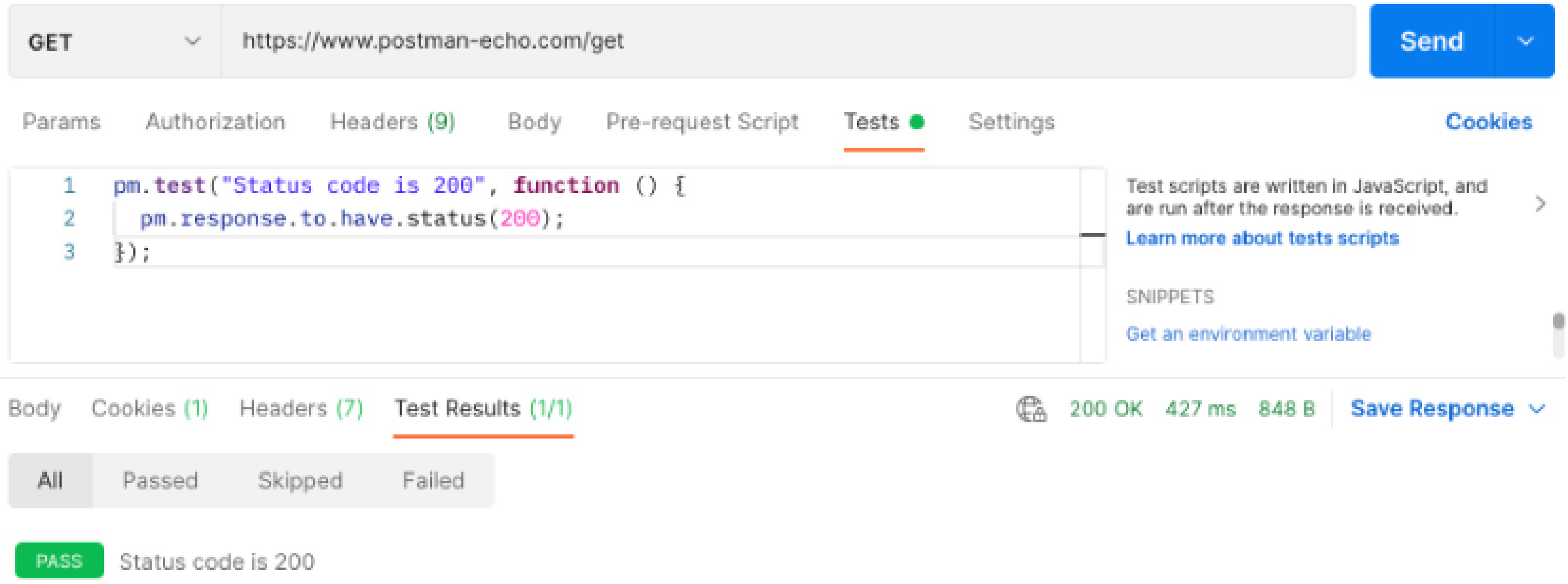
Higher request volumes

Large or multiple teams

Dedicated account manager

Postman

- Has collections which can be shared among the team
- Parses OpenAPI/Swagger
- Understands GraphQL
- Overall is a useful and nice tool
- Has scripting and testing capabilities



https://www.postman-echo.com/get

```
pm.test("Status code is 200", function () {
  pm.response.to.have.status(200);
});
```

Test scripts are written in JavaScript, and are run after the response is received.

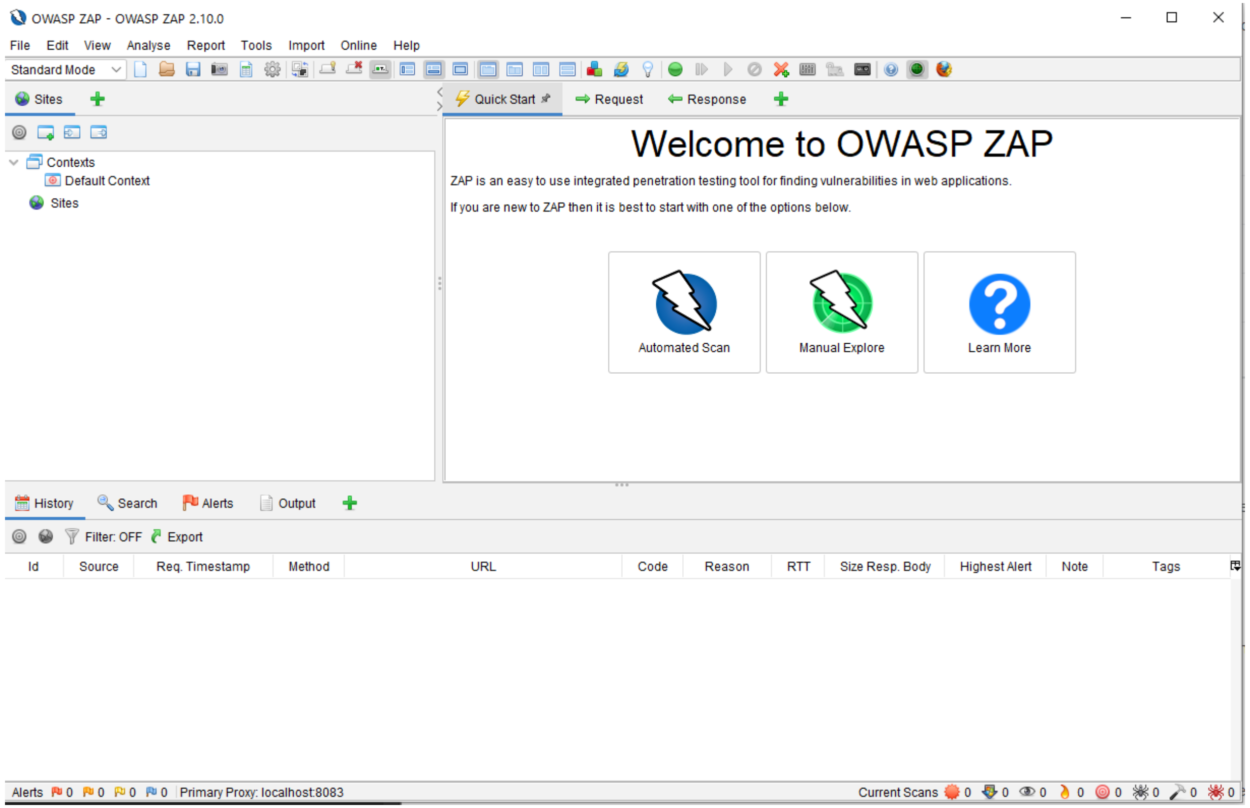
Learn more about tests scripts

200 OK 427 ms 848 B

PASS Status code is 200

OWASP ZAP

- Nice free Attack Proxy for testing web applications
- Has a nice site-map feature
- Can scan for vulnerabilities
- Allows fuzzing for vulnerabilities
- Chaining of proxies
- WebSocket support
- Good developer support



OWASP ZAP - OWASP ZAP 2.10.0

Welcome to OWASP ZAP

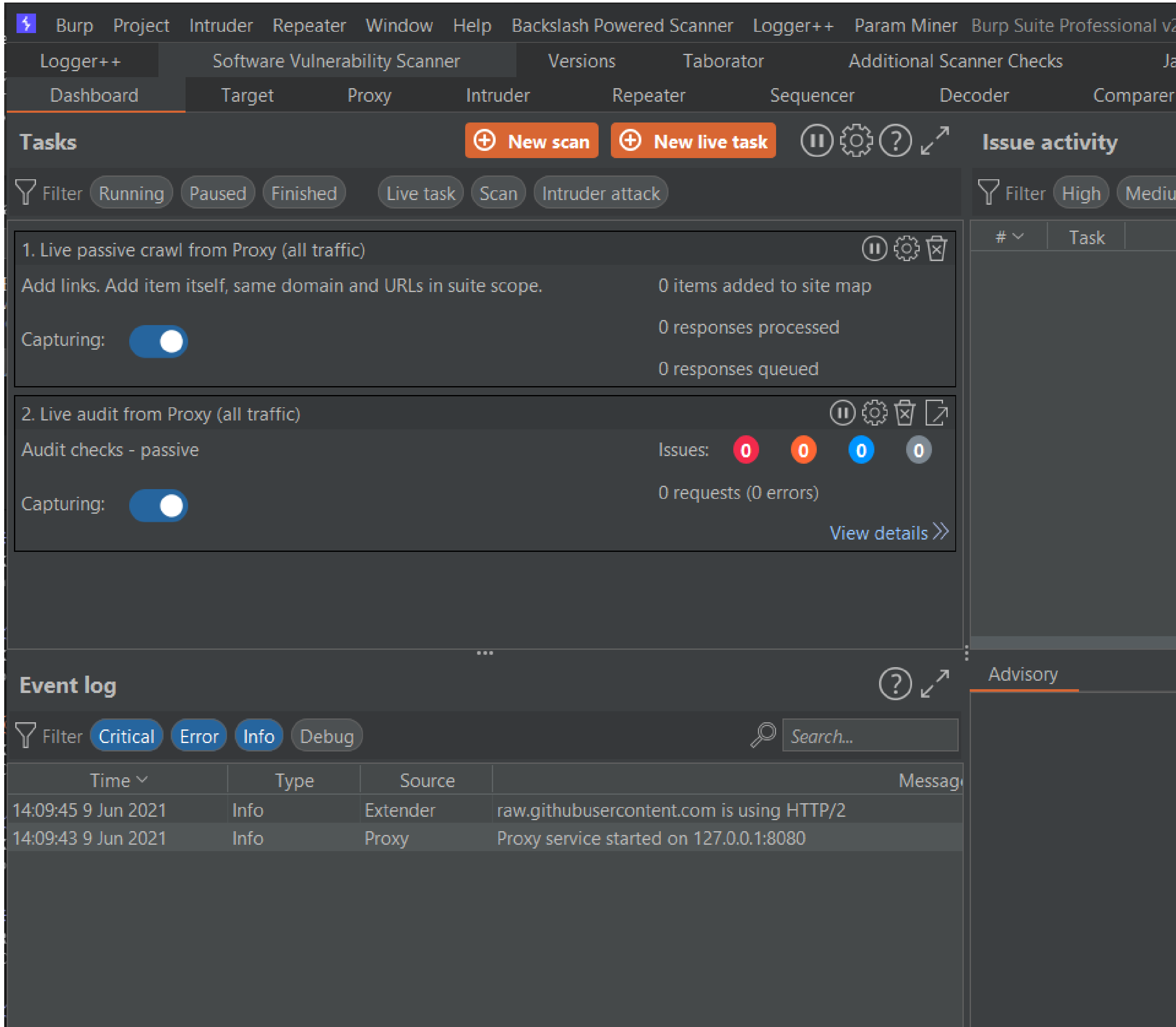
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Primary Proxy: localhost:8083

Burp Suite

- Defacto tool by pentester
- Strong fuzzing capabilities
- Extension support
- Very flexible and robust
- Well developed scanner
- Spidering engine with good SPA support



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing:

Issues: 0 0 0 0

0 requests (0 errors)

View details »

Time	Type	Source	Message
14:09:45 9 Jun 2021	Info	Extender	raw.githubusercontent.com is using HTTP/2
14:09:43 9 Jun 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080

Where to Learn

- Challenges and Experimental Learning
  - Burp Suite Academy
  - Wechall.net
  - Overthewire.org
  - APISec University
- Do It Yourself
  - OWASP Juice Shop - OWASP Top 10 in realistic environment
  - DVWA , DVWS – Damn Vulnerable Web Application/Service
  - OWASP DevSlop Pixi – MEAN (Mongo, Express, Angular, Node) Stack
  - REST API Goat
  - crAPI – Complete Ridicoulus API – OWASP Top 10 Vulnerabilities
  - vAPI – OWASP Top 10 exercises

RIVER SECURITY

https://into.bio/chrisdale & https://into.bio/rivsec

Twitter – https://twitter.com/ChrisADale

LinkedIn – https://www.linkedin.com/in/chrisad/

Fighting Cyber Crime – https://riversecurity.eu