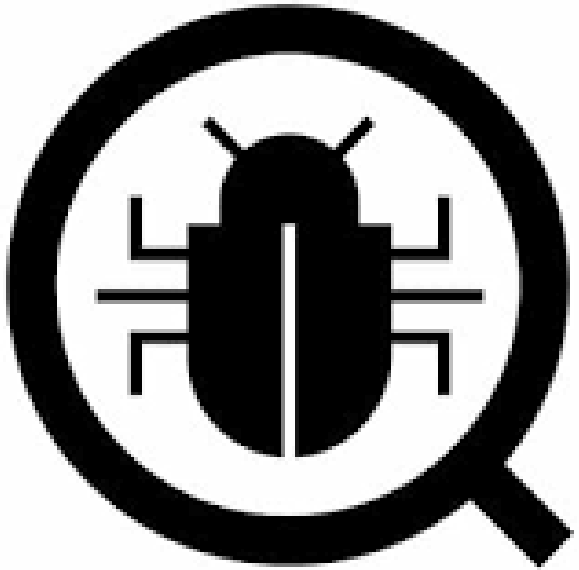
defend Denmark



Bug Bounty

Crowdsourced sikkerhed anno 2026

HVORDAN VENLIGE HACKERE HJÆLPER MED AT STYRKE VIRKSOMHEDERS IT-SIKKERHED

HVEM ER JEG ?

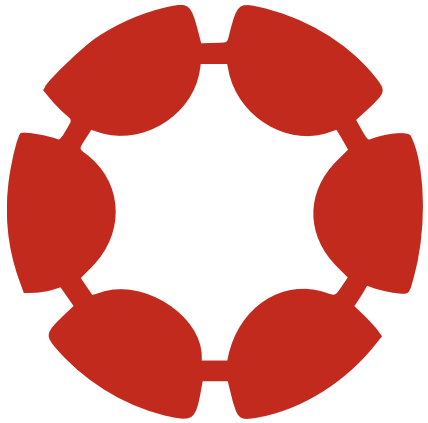
- ***Emil Christian Hørning***
- Uddannet inden for cybersikkerhed
- White-hat hacker med 10 års erfaring
- Moderne dusørjæger – Finder fejl og bliver betalt for at finde dem
- CEO i Defend Denmark – virksomhed der forbinder danske organisationer med danske etiske hackere

Hvad er bug bounty?

- En tilgang til aktiv/offensiv test af sikkerhed
- En byttehandel
  - Dusører gives af virksomheder, for ny viden om reelle sårbarheder
  - Ingen dusør hvis man kender til problemet i forvejen
  - Ingen dusør for ”ligegyldige” sårbarheder
- Resultatsorienteret tilgang til hacking
- Virksomheder eksponerer deres systemer, hackere arbejder ”freelance” i deres egen tid

Dansk platform til at arbejde med danske freelance etiske hackere

1. Danske freelance etiske hackere finder sårbarheder I vores kunder
2. Rapporterer det til Defend Denmark
3. Defend Denmark verificererer og er I kontakt med kunden
4. Kunden får information om sårbarheden
5. Kunden betaler en ***dusør*** alt efter hvor slem sårbarheden er



defend Denmark

Bug bounty er ikke nyt

- **Bugcrowd** startede som den første platform i 2011
- Siden da er der kommet en del nye spillere på markedet
- Oftest brugt af større virksomheder
- Eller virksomheder med en væsentlig digitalisering

hackerone

bugcrowd

YesWeHack

GO BUGFREE

Synack

INTIGRITI

defend Denmark

Meta

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.

Submit a report

Bug Bounty rewards

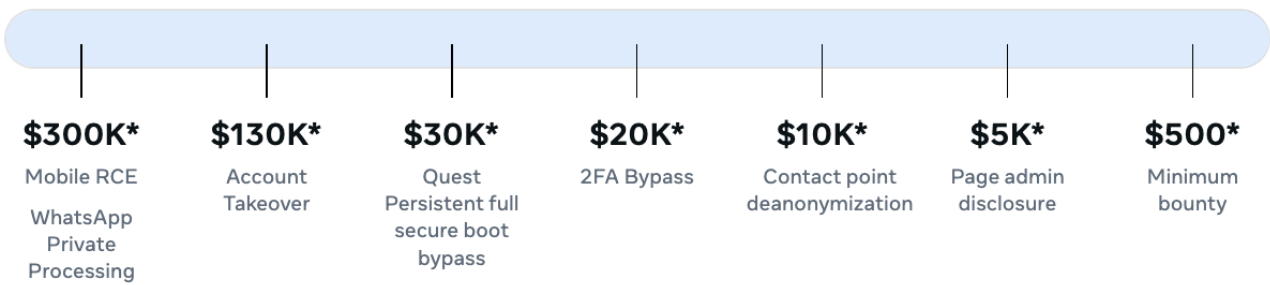
All listed amounts are without bonuses. With Hacker Plus, and any applicable bonuses, you can earn up to 30% of the original bounty amount on top of it!

We pay based on maximum security impact found internally, and our highest payouts reflect that.

Learn more

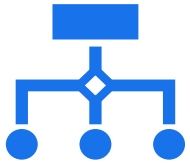
Total rewards for 2026
$2,021,160

Total rewards to date
$28,028,301



Please keep in mind that this graphic is only an overview with maximum payouts per category listed. For more details about rewards, see our payout guidelines. All payout values are in USD.

Bug bounty aktører



Platforme

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

Programmer

VIRKSOMHEDER SOM TILBYDER DUSØRER FOR SIKKERHEDSHULLER I DERES IT SYSTEMER

Hackere

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

Hvordan? Virksomhedens Perspektiv

Hvordan? – Virksomhedens perspektiv

- Virksomheden har 3 årlige pentest
  - 1 Assume Breach og 2 scopede test af applikationer
  - Bruger forskellige konsulenthuse som sender 1-2 folk
  - 3 ugers varighed per test
- Der leveres rapporter med alt fra **informational** til **critical**
- Dette møder compliance krav for sikkerhedstest
- Dette er meget standard for mange virksomheder

Hvordan? – Virksomhedens perspektiv

- Nu er der et ønske om at prøve noget nyt
- Virksomheden indgår et samarbejde med en **platform**
- Kan være som supplement / erstatning til de 2 pentests af applikationer
- Der sættes et scope og et budget op
- Virksomheden modtager løbende rapporter om **vigtige** sårbarheder
- Dette møder stadigvæk compliance kravet


defend
Denmark
Hvordan?
Researcherens
Perspektiv

Hvordan? – Researcher perspektiv

Starter ud med en **sej hacker** som gerne vil tjene en mønt på deres hacking færdigheder

Hvordan? – Researcher perspektiv

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

Hvordan? – Researcher perspektiv

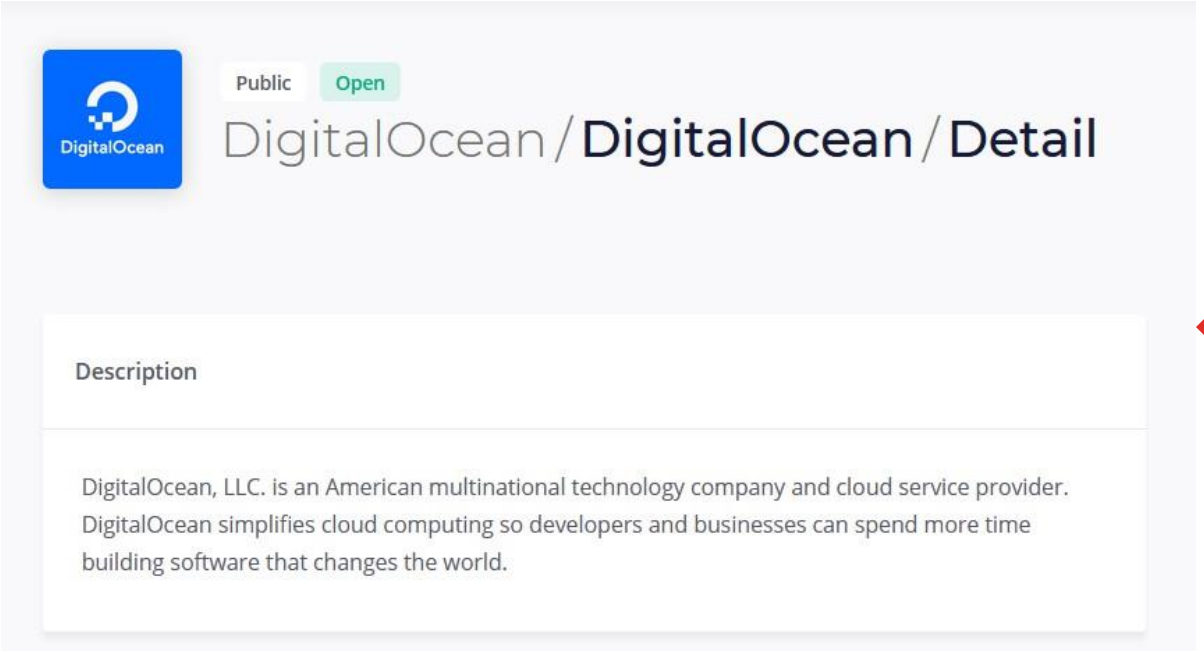
hackerone bugcrowd

YES WE HACK

Synack INTIGRITI

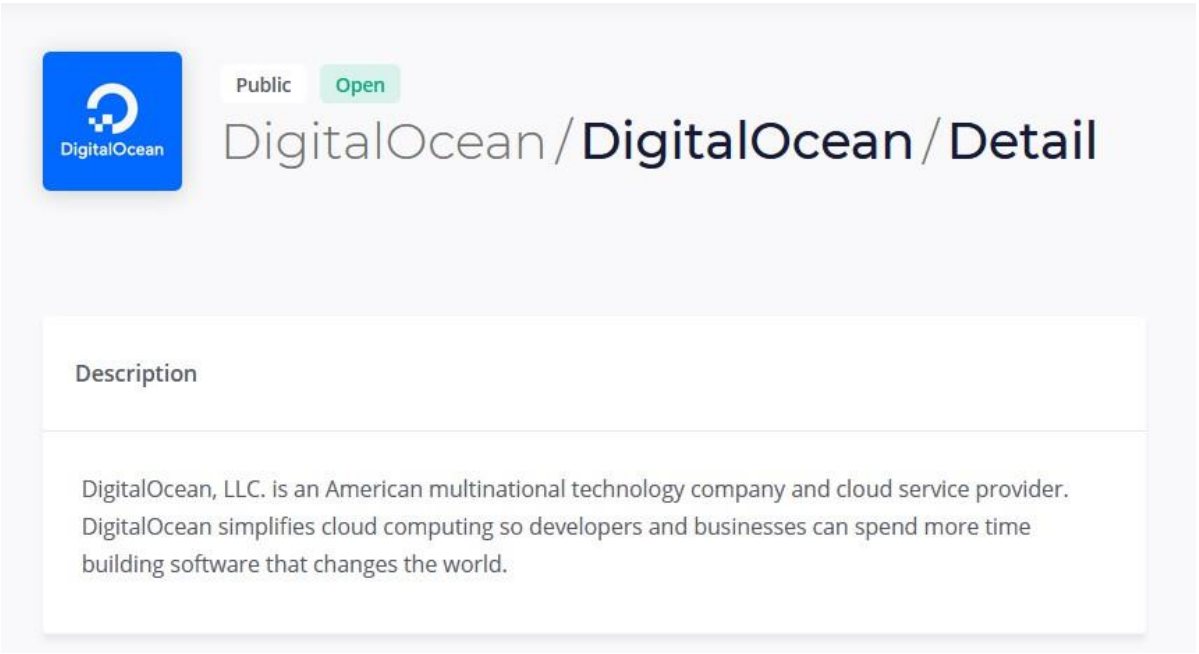
De tilmelder sig en af bug bounty platformene
(KYH skal gennemføres)

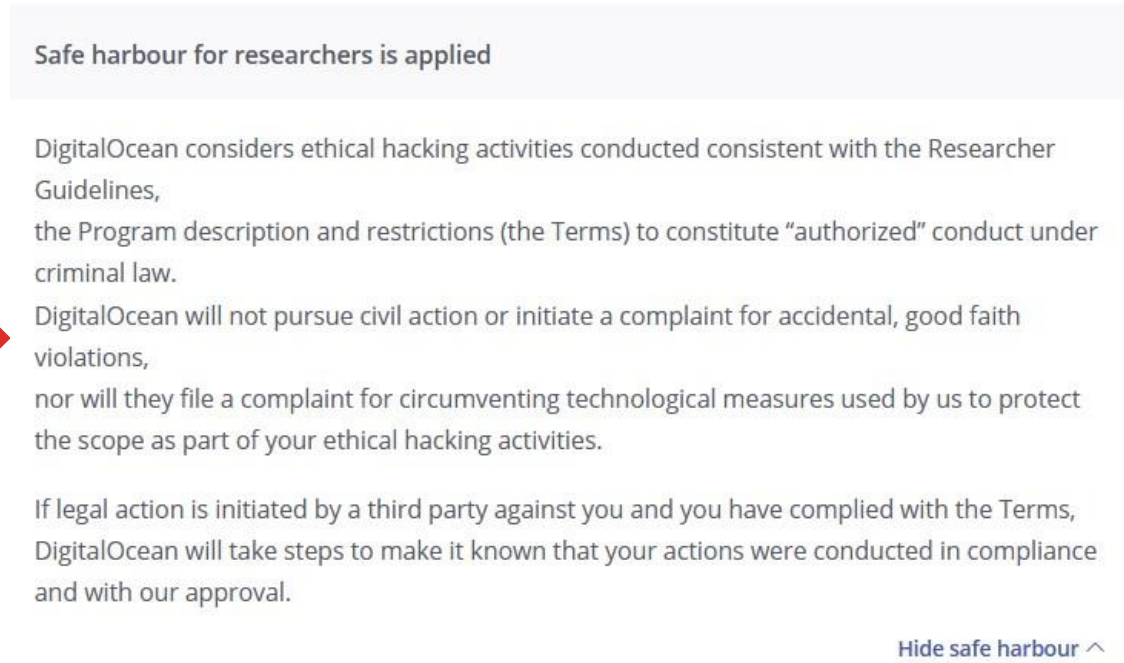
Hvordan? – Researcher perspektiv



De finder en virksomheds program de gerne vil hacke

Hvordan? – Researcher perspektiv





Hackeren godkender og accepterer ”Rules of Engagement” og ”Safe Harbor”

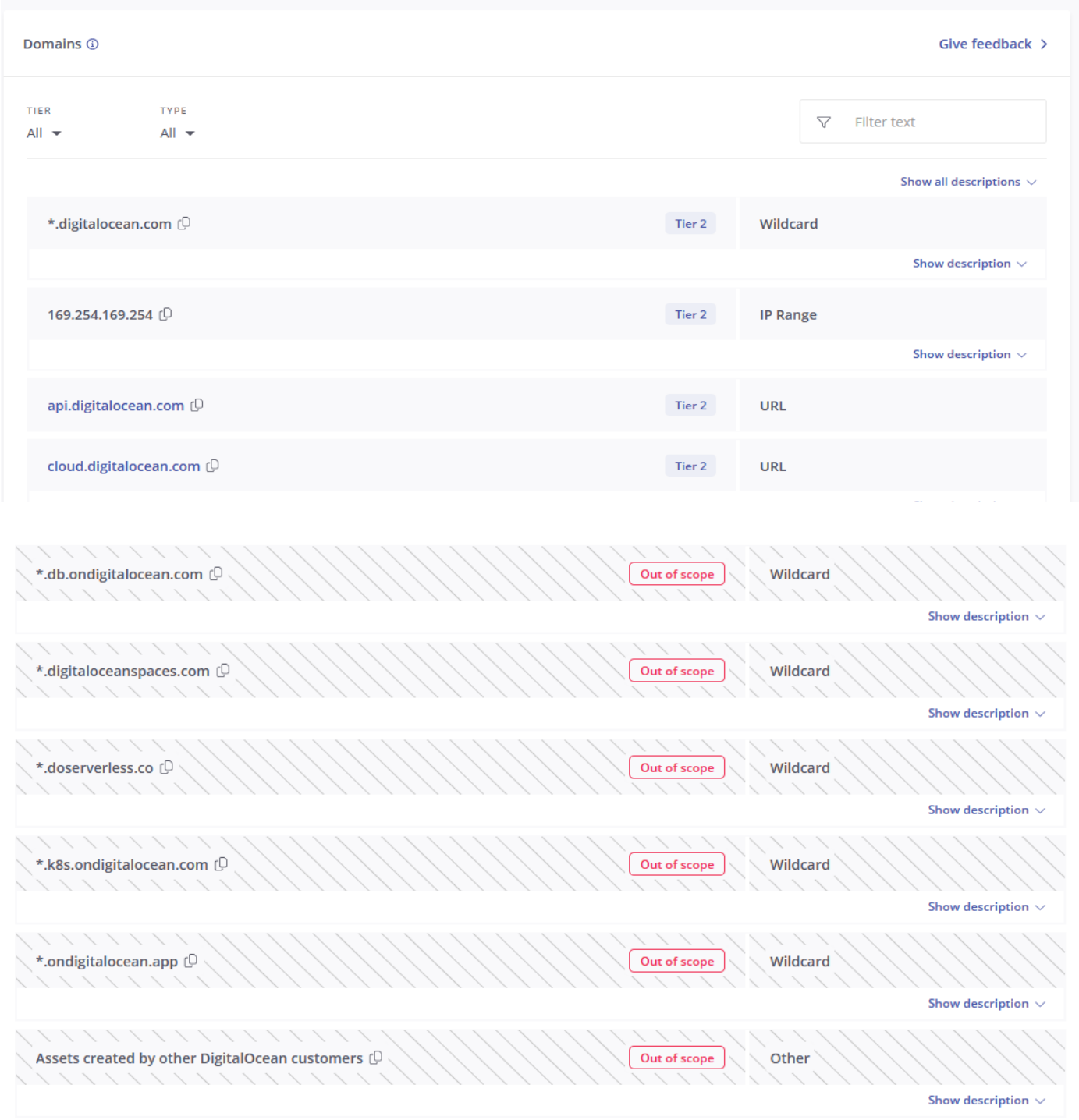
Hvordan? – Researcher perspektiv

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

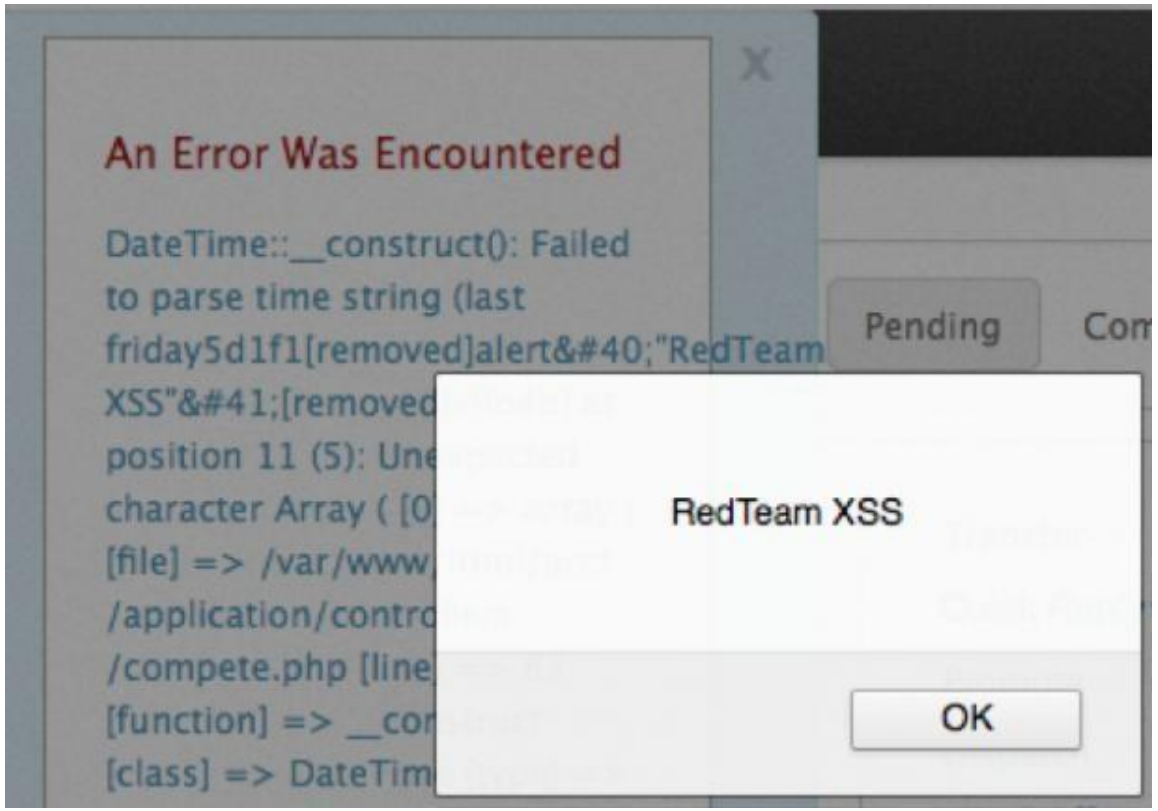
Hvordan? – Researcher perspektiv

- Hackeren ser og accepterer hvad reglerne er.
- *”In scope”*
  - Hvad der gerne må hackes
- *”Out of scope”*
  - Lad være med at hacke det her
- Andre regler
  - Rate limits
  - Forbudte værktøjer
  - Uinteressante sårbarheder



Hvordan? – Researcher perspektiv

- Så finder hackeren en sårbarhed i et asset som er ”in scope”
- Det kunne være en stored xss

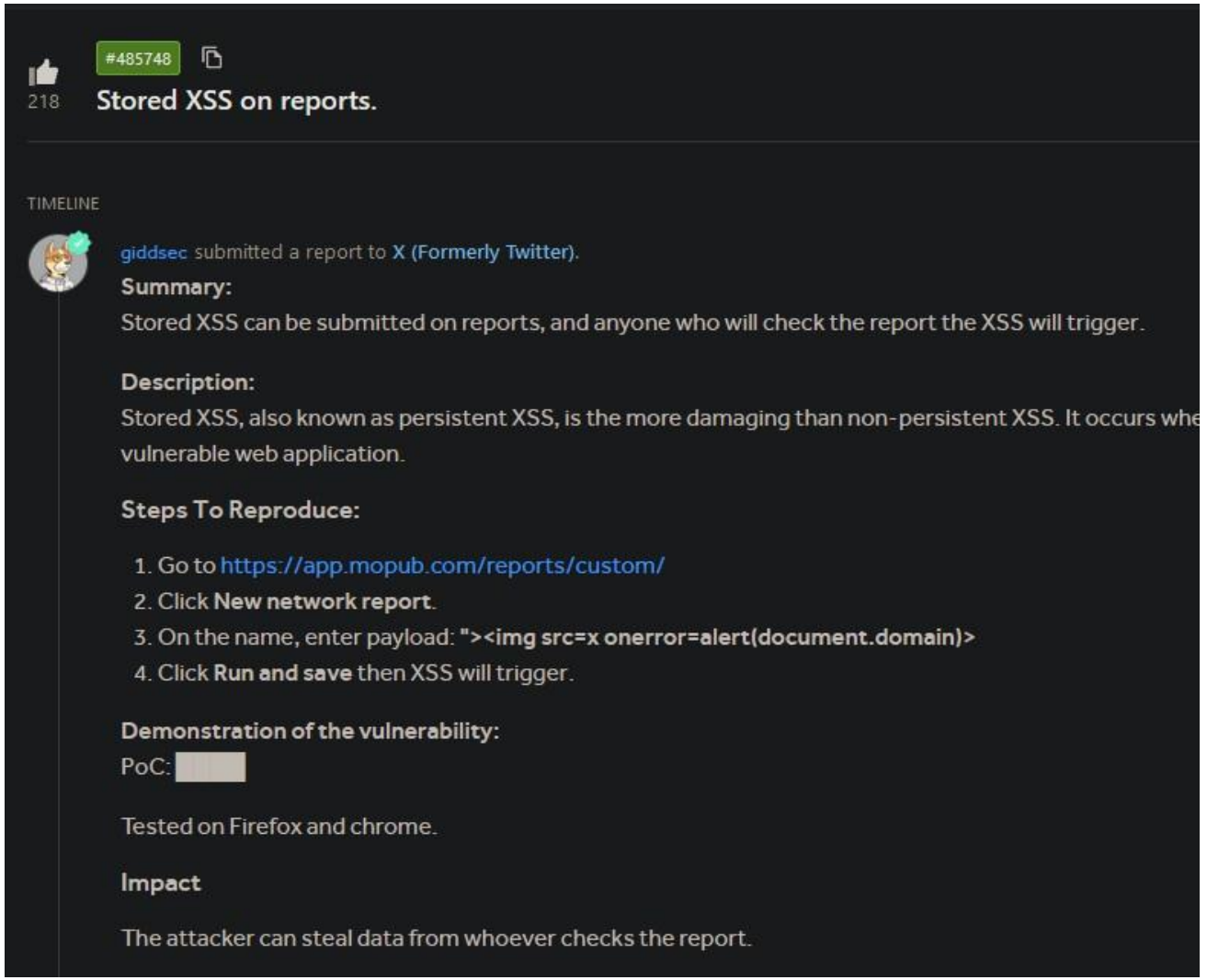


Hvordan? – Researcher perspektiv

- Hackeren skriver derefter en detaljeret rapport om sårbarheden
  - 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)

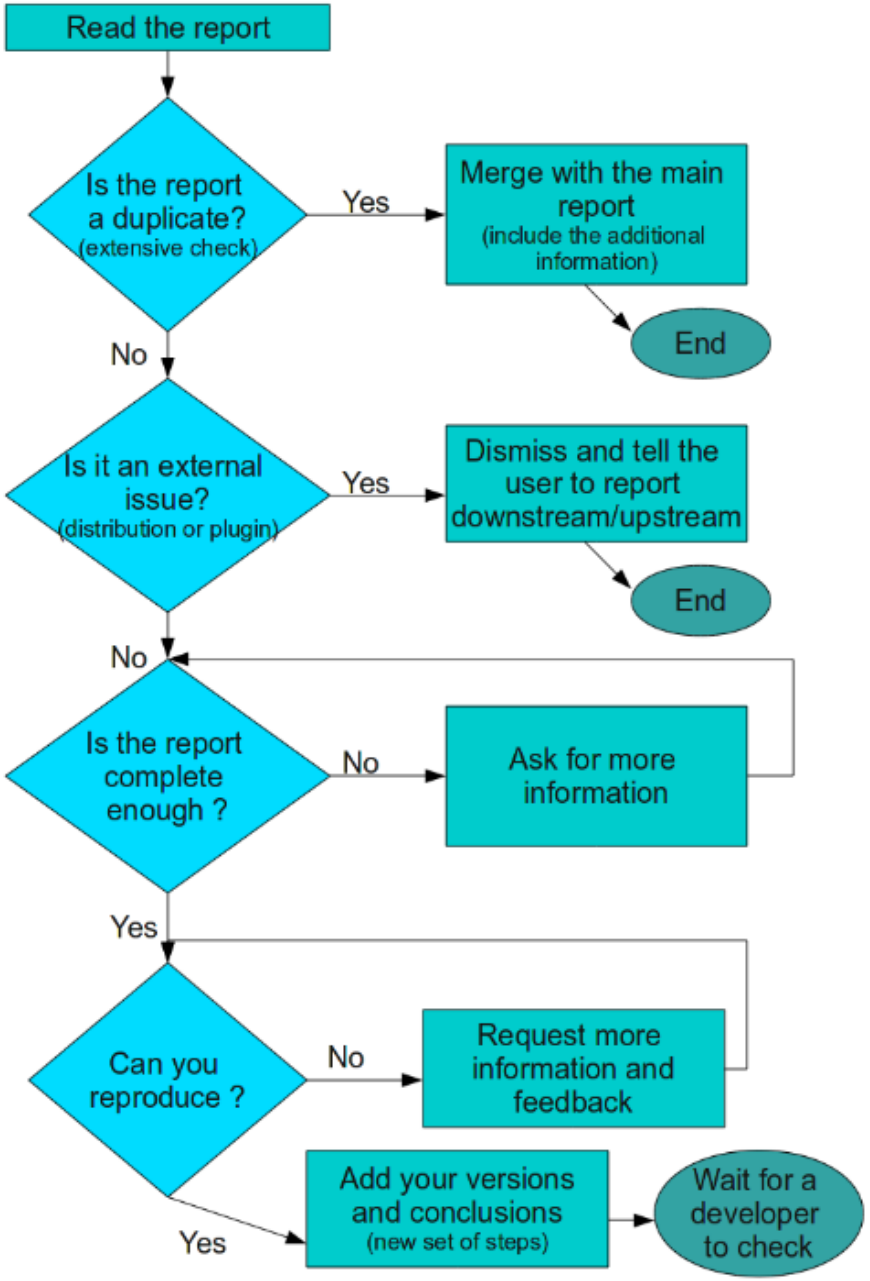
- Forklar impact (hvad kan en ondsindet hacker gøre med denne sårbarhed)



Hvordan? Platformens perspektiv

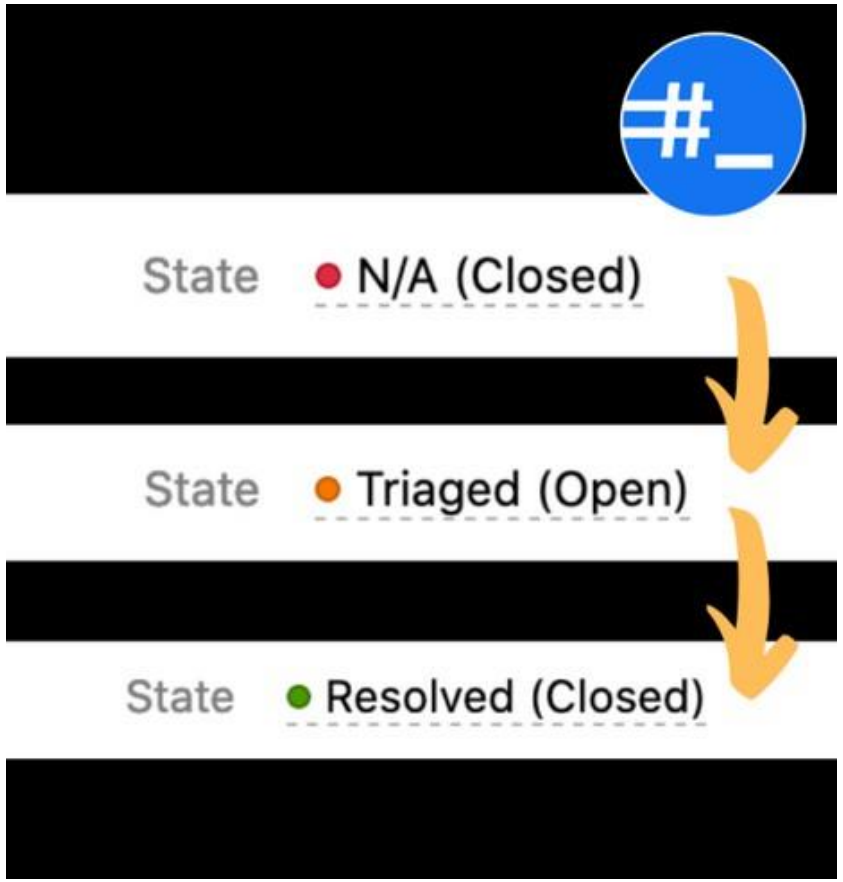
Hvordan? – Platformens perspektiv

- Triage holdet verificerer at der er tale om en **reel** og **vigtig** sårbarhed - filter
- Der tjekkes om sårbarheden er indsendt før
- Der vurderes om sårbarheden falder inden for scope
- Der vurderes om sårbarheden er vel-dokumenteret



Hvordan? – Platformens perspektiv

- Rapporten om sårbarheden sendes videre til virksomheden
- Alt dokumentation bliver sendt med
- Der gives et bud på en potentiel dusør
  - (Denne dusør besluttes dog altid af virksomheden)
- Der gives et bud på hvordan sårbarheden kan fixes
- Virksomheden bliver bedt om at bekræfte at de er enige



Lad os tage et konkret eksempel

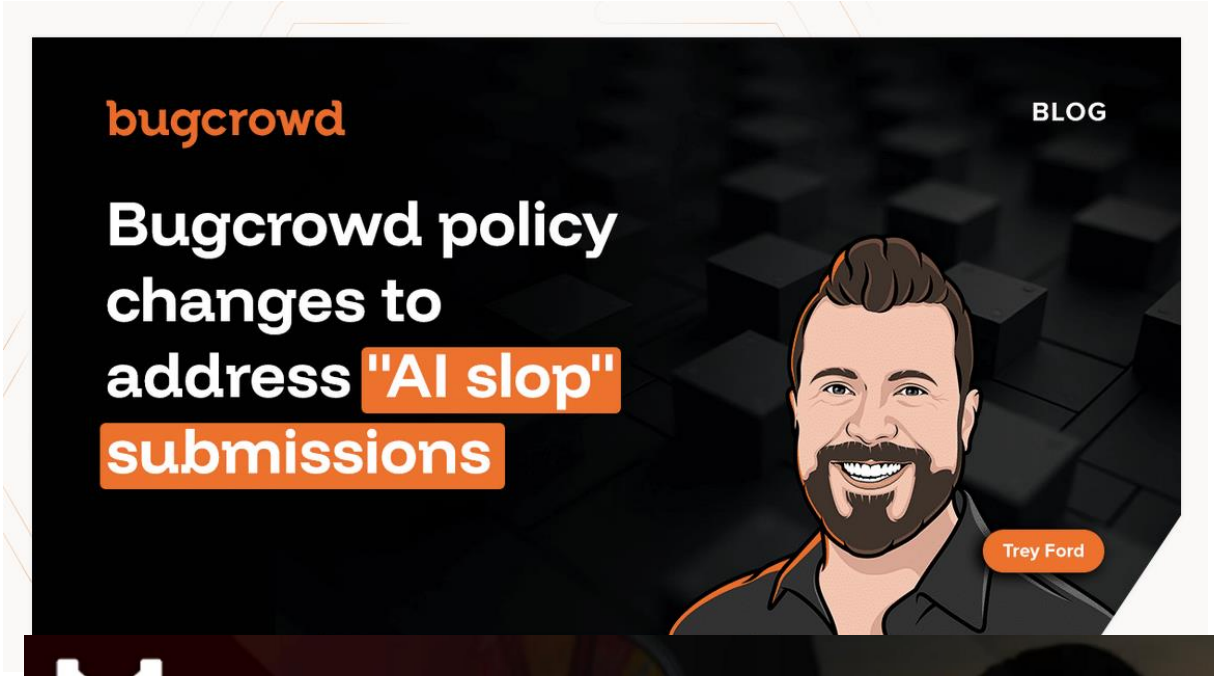
- Københavns Tidende
- Stor mediekoncern i København
- Tager sikkerhed seriøst, men har også en del legacy
- Hjemmeside: kobenhavns-tidende.dk
- **Worst case scenario:** Læk af kunders oplysninger
- Dusører fra 1000 – 20.000 kroner

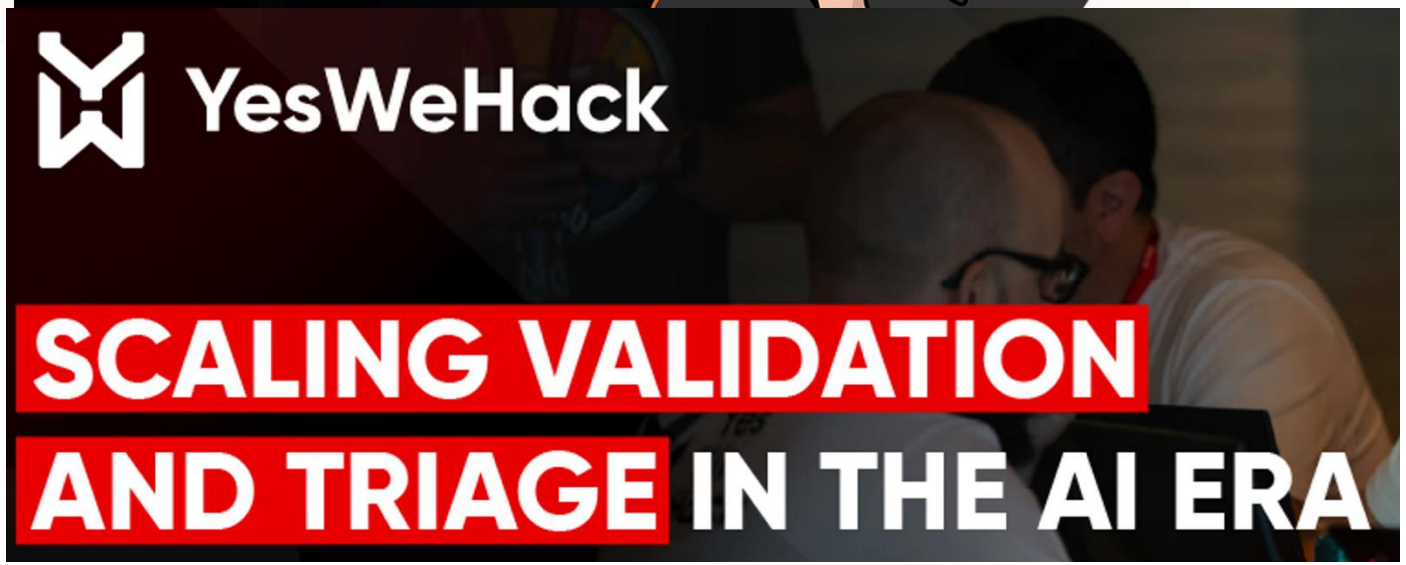
Københavns Tidende – bug bounty

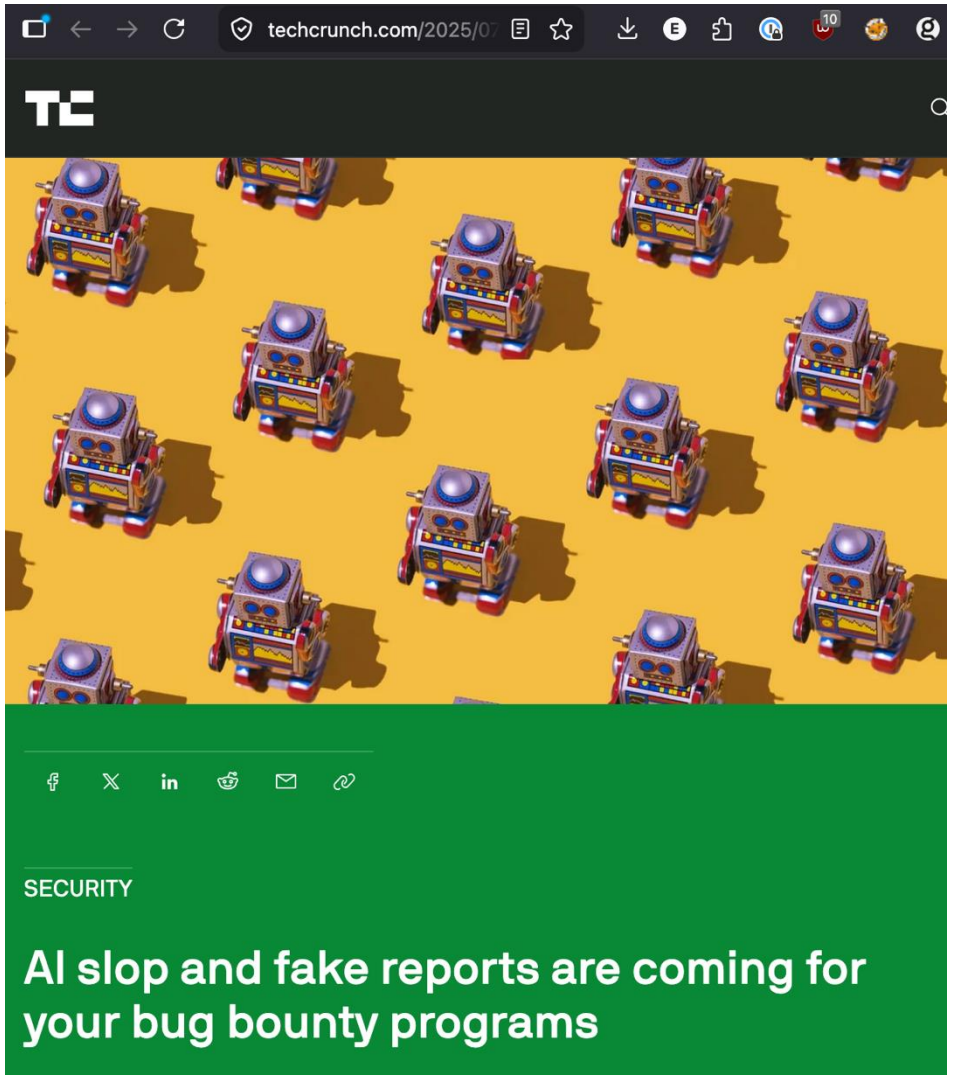
Researcher:	**Rapport:** Exposed .git leaks database secrets, leaking customer PII
Platform:	**Triage:** Kan verificeres, er en vigtig sårbarhed, ikke set før, vurderes som *critical* **->** Sendes videre til kunden
Virksomhed:	Det her er godt nok slemt, vi får dette fixet internt, giver en dusør på 15.000 dkk

Bug bounty anno 2026

defend Denmark

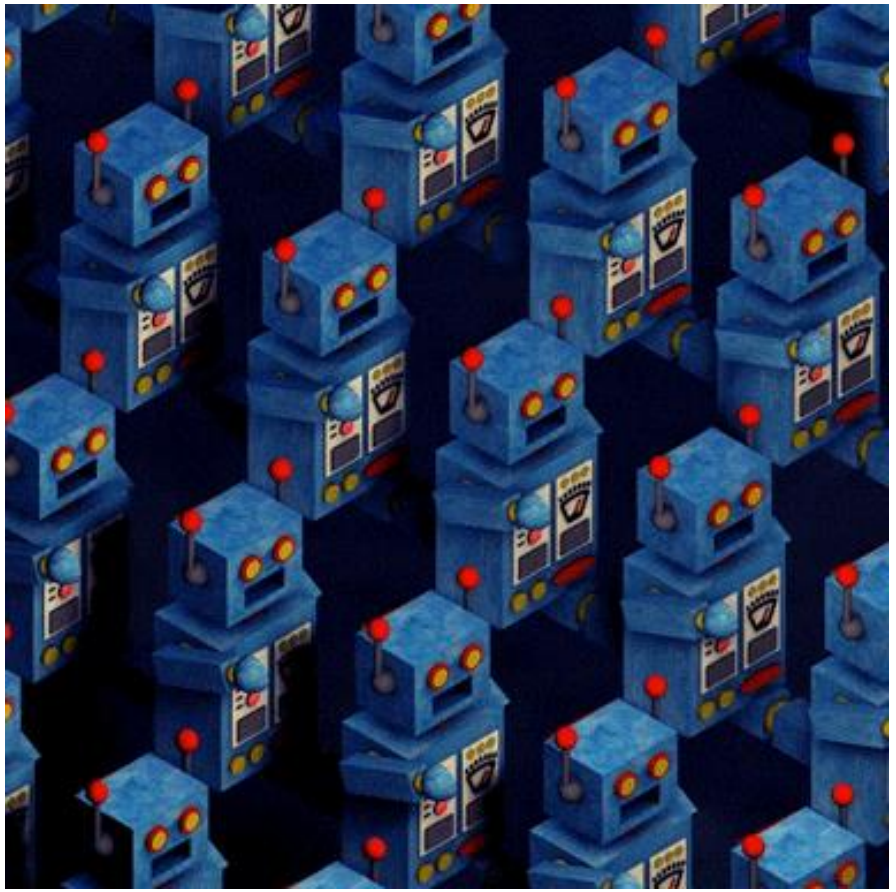






Bug bounty anno 2026

- AI ændrer landskabet lige nu
- De dygtigste hackere – **Supercharged**
- Nye hackere – **Gaslighted af AI**
- Antal indsendte sårbarheder stiger markant nu
  - Vigtige og kritiske sårbarheder
  - AI slop
- Mennesket er nødt til at være in the loop
  - Både hackeren, men også platformen
- Hensigten er stadigvæk at dette skal være en byttehandel
  - Dusører for vigtige sårbarheder



defend Denmark

Emil Hørning

Fremmer Bugbounty i 🇩🇰 med Defend Denmark | OSCP, OSCE3