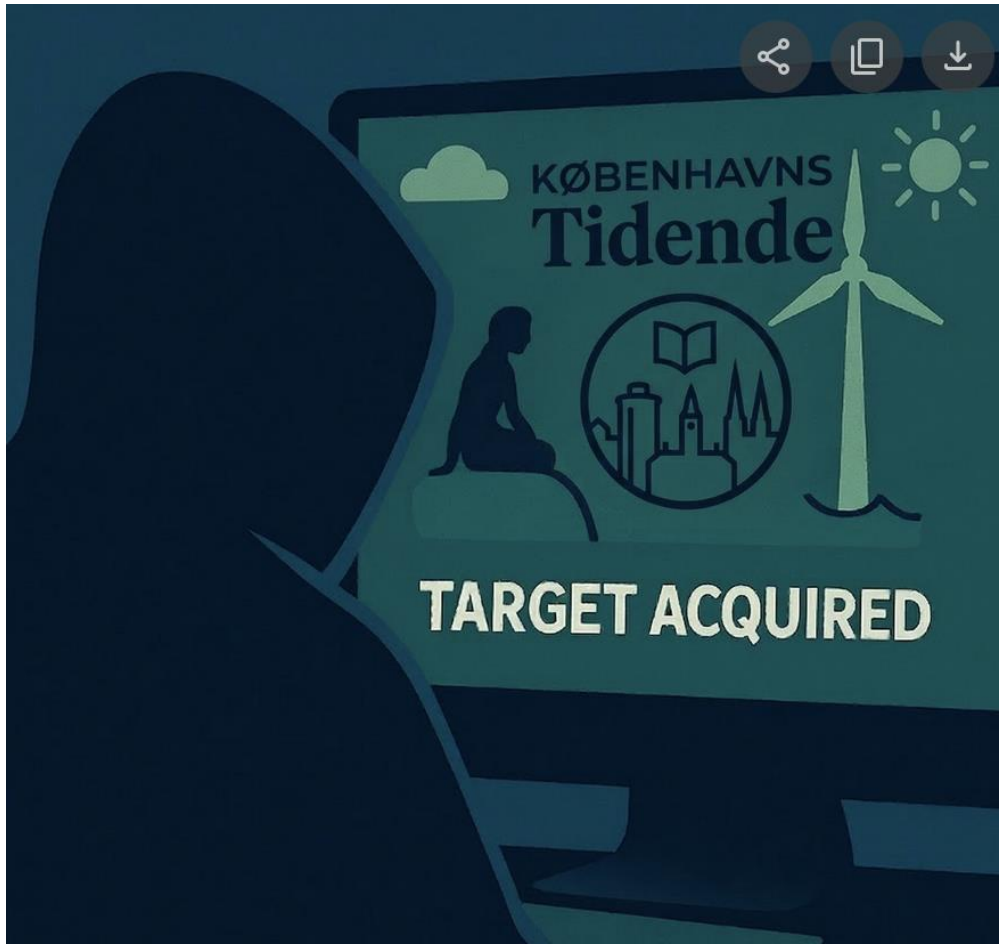
defend Denmark

# LIVE HACKING

## *A modern bounty hunter*




BUG BOUNTY HUNTING AND A HACKERS TOOLKIT

# WHO IS THE HACKER?

- ***Emil Christian Hørning***
- Trained in cybersecurity
- White-hat hacker with 10 years of experience
- Modern bounty hunter – Finds bugs and gets paid to find them
- CEO of Defend Denmark – Startup company that connects Danish companies with Danish ethical hackers

# Danish platform for working with Danish freelance ethical hackers

1. Danish freelance ethical hackers find vulnerabilities in our customers
2. Reporting it to Defend Denmark
3. Defend Denmark verifies and is in contact with the customer
4. The customer receives information about the vulnerability
5. The customer pays a bounty depending on how bad the vulnerability is
6. The system is called the bug bounty

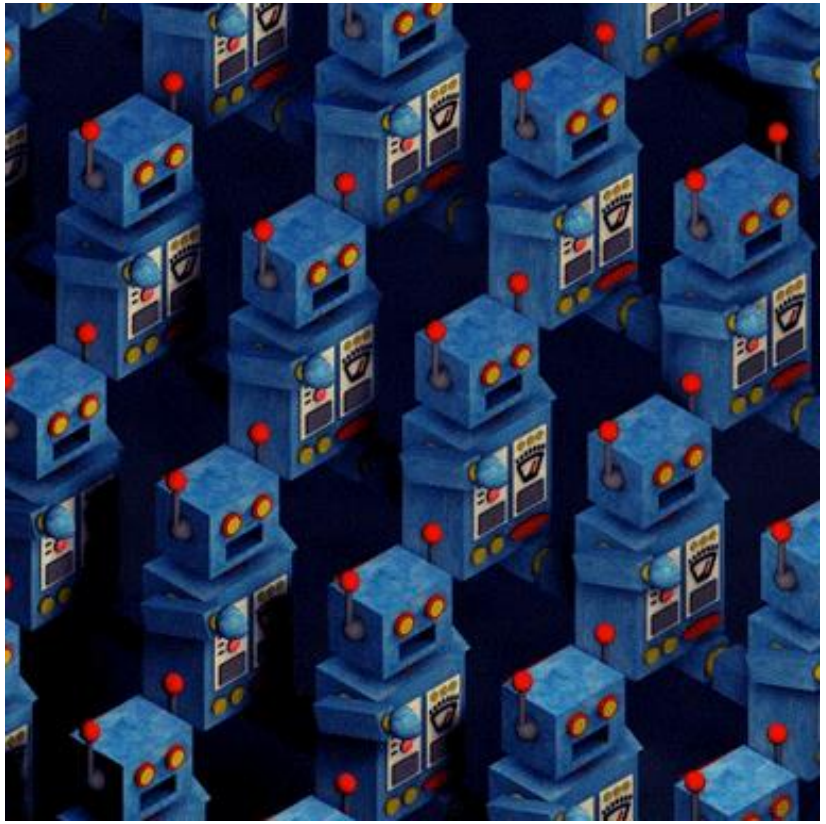
defend Denmark

# Who is the target?

- Københavns Tidende
- Large Media company in Copenhagen
- 500+ medarbejdere
- Takes security seriously, but also has a lot of legacy
- Website:kobenhavns-tidende.dk

# BUT!! Before we get started

- It wouldn’t be a tech talk without including AI
- In Defend Denmark we have developed our own **AI DEFENDER**
- An autonomous hack-bot that acts as a hacker, trained by our fleet of ethical hackers
- Lets give it the same task as we have – Try to hack *kobenhavns-tidende.dk*



# 1. Reconnaisance

- **Objective: Map kobenhavns-tidende.dk's attack surface**


Src: palo alto - https://www.paloaltonetworks.ca/cyberpedia/attack-surface-ass

# 1. Reconnaisance - demo

- Tools: Projectdiscovery's httpx and subfinder



Projectdiscovery.io

# Tip 1 til beskyttelse - Recon

- **Know your attack surface before threat actors do**
- Keep track of what you expose:
  - Subdomains
  - IP ranges that you own
  - Cloud/SaaS solutions that you buy
- Use firewall to remove public access
- Shut down services that are not actively used

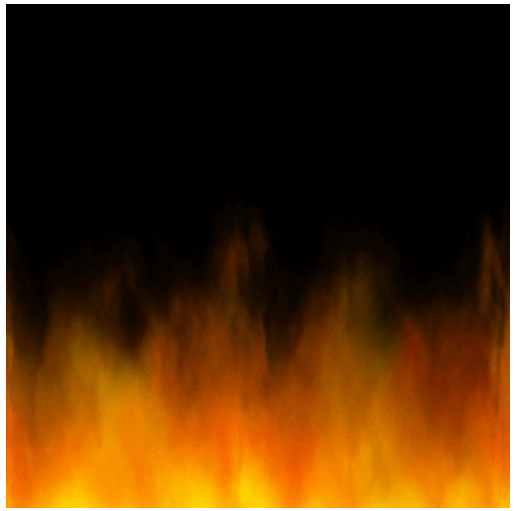
# 2. Attack - Demo

- **Objectives:** Breaking into an admin portal and seeing what we can find
- **Tools:** Hackers swiss knife: web proxy



# Tip 2 for protection – Patching / Default creds

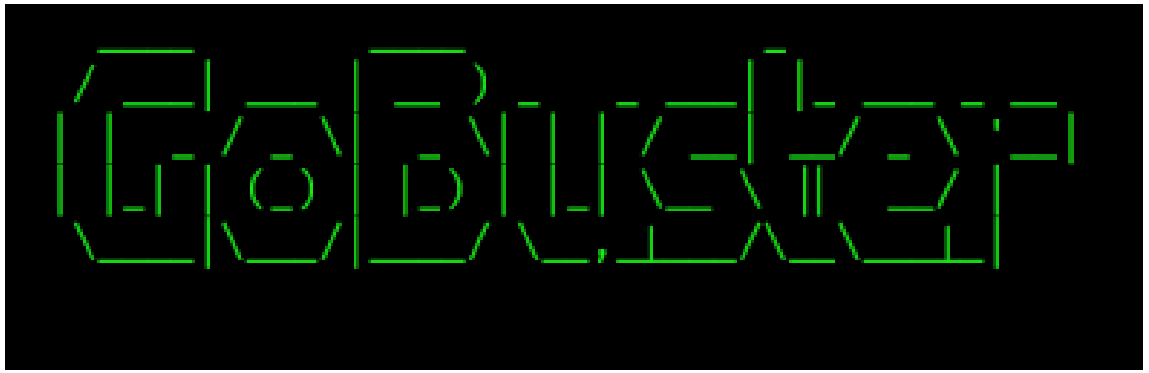
- **Assume Everything is Under Attack**
- Default credentials are seen everywhere – change them
- Make sure everything is up to date – unpatched software GETS hacked
- Establish MFA wherever you can
- Use firewall to remove public access



# 3. Escalation - Demo

defend Denmark

- **Objectives:** Leveraging the admin panel to move forward
- **Tools:** Further scanning with FFUF or gobuster

# Tip 3 for protection – unexpected and abnormal traffic

defend Denmark

- **Spot unanticipated network penalties and shut it down**
  - Suddenly there are many login attempts
  - Suddenly there are many 404 responses
  - Is the traffic isolated to a single user/IP address? – Exclude

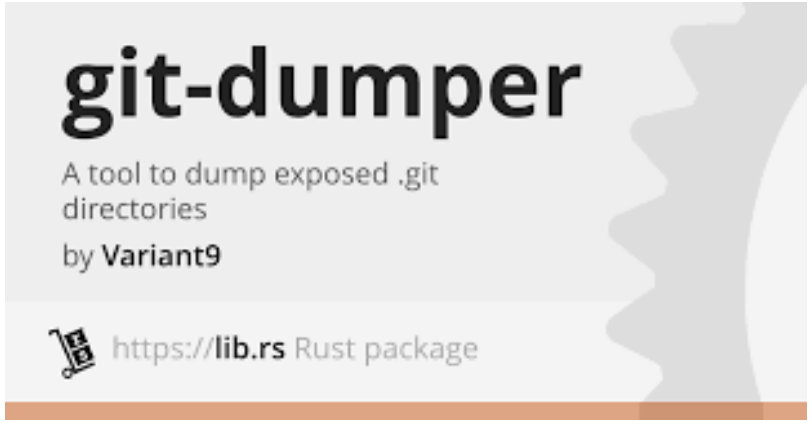
- **Use Web Application Firewalls**
  - Helps block many attempts/malicious attempts
  - Not a bulletproof solution, but helps

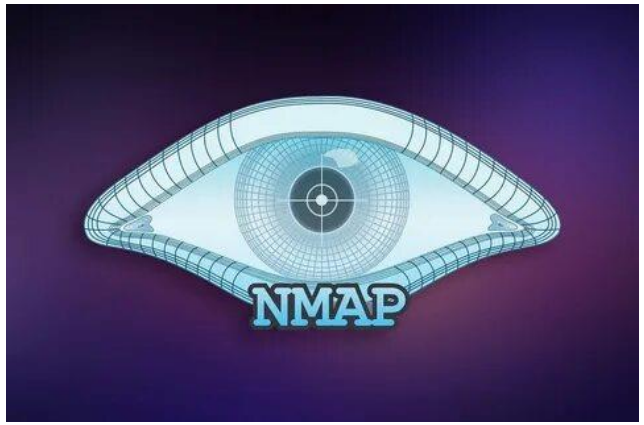
CLOUDFLARE®

# 4. Exfiltration - Demo

defend Denmark

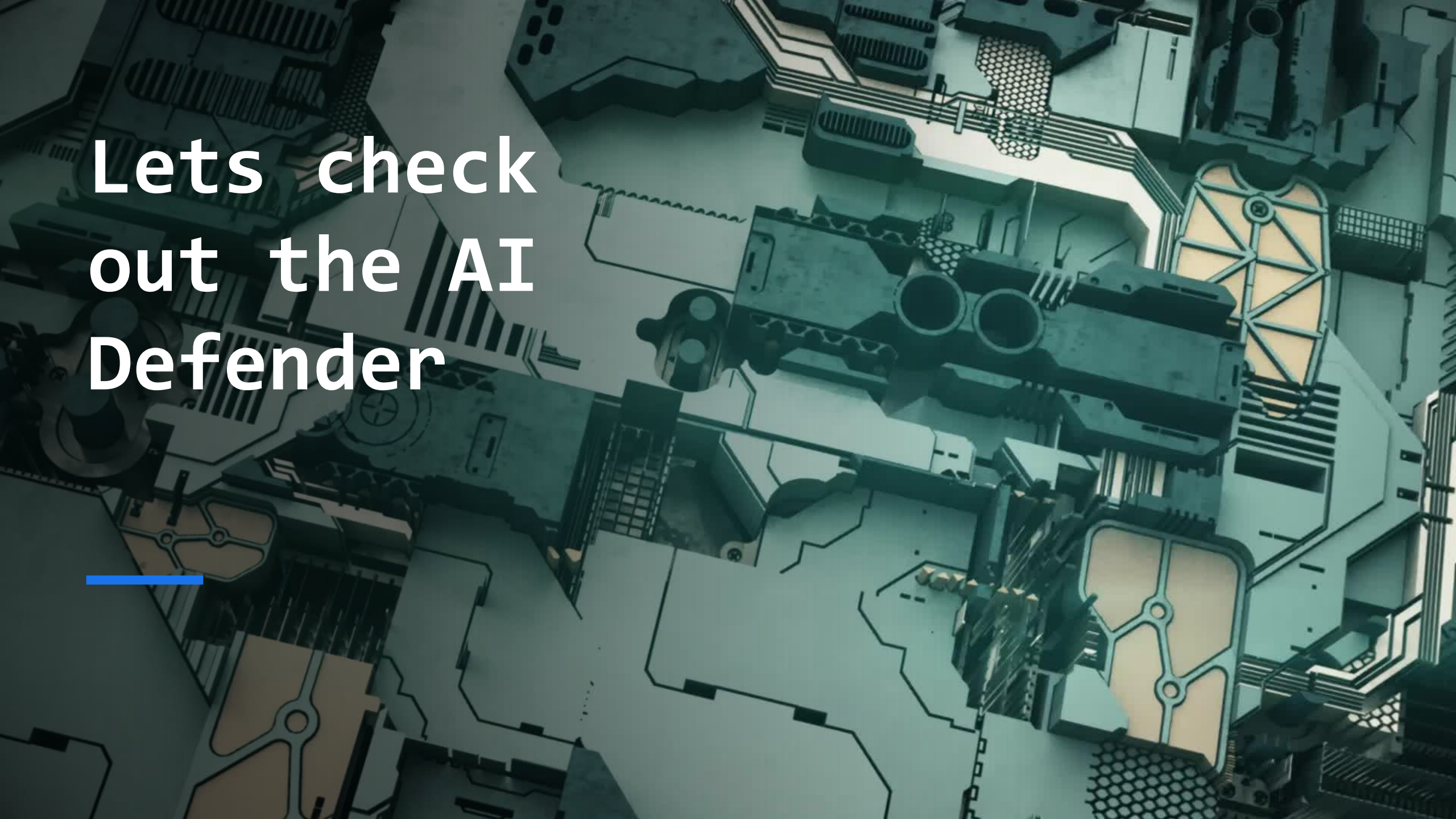
- **Objectives:** Exploiting vulnerabilities to exfiltrate sensitive information and show **impact**
- **Tools:** git-dumper, nmap og mysqldump




# Tip 4 for protection - DevSecOps + separation of environments

- **Have good routines for dealing with secrets**
  - Use DevOps tools with a focus on security to manage passwords / api keys
  - Never keep secrets directly in the code
  - Follow modern best practices
- **Make separation of environments**
  - Compromising one system should not affect another
  - Have separate environments where it makes sense


Lets check out the AI Defender

# Conclusion

- **The threat actors are at work every day**
  - They use the same tools that I have shown today
  - Every small crack is a potential opening to your infrastructure
- **Conduct tests and audits**
  - Helps you identify gaps and crevices
  - Much cooler to pay for consulting hours/bounties rather than a **ransom**
  - Good / Bad hackers all use AI, and its getting better
- **Unauthorized testing is illegal (in Denmark)**
  - Even if done in ”good faith”
  - Got an interesting pitch for a story here 👀

defend Denmark


**Emil Hørning**

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