Protecting the Digital World

OWASP

SOFIA, BULGARIA

Effective Threat Modeling

owasp.org/www-chapter-sofia/

OWASP Sofia

whoami

Danny (me@dnny.sh):

- AppSec engineer
- Former backend eng.
- Offensive & Defensive tools developer
- Interested in:
  - Web Security Research
  - Penetration Testing
  - Bug bounty hunting

OWASP Sofia

Agenda

1. What is threat modeling?
2. Why do we care?
3. How & When we do it?
4. Practical Tip #1
5. Practical Tip #2
6. Practical Tip #3
7. TLDR;
8. Q & A

Threat Modeling

- A proactive process
- Thinking like an attacker
- Collaborative exercise

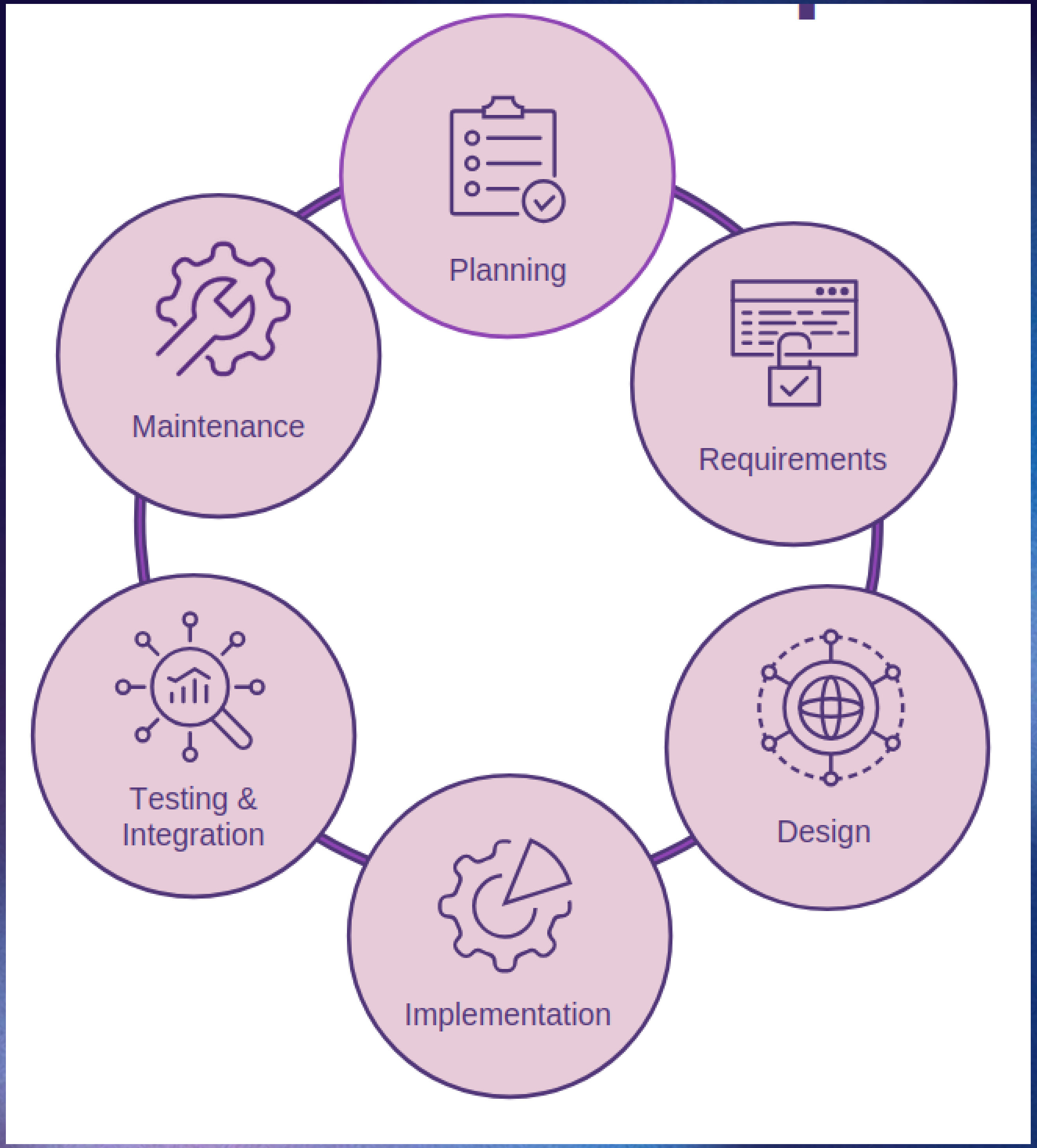
OWASP Sofia

Why do we care?

- Saves time & money
- Advocates security awareness
- CRA
  - Fines of up to €15 million
- It’s cool!

When?

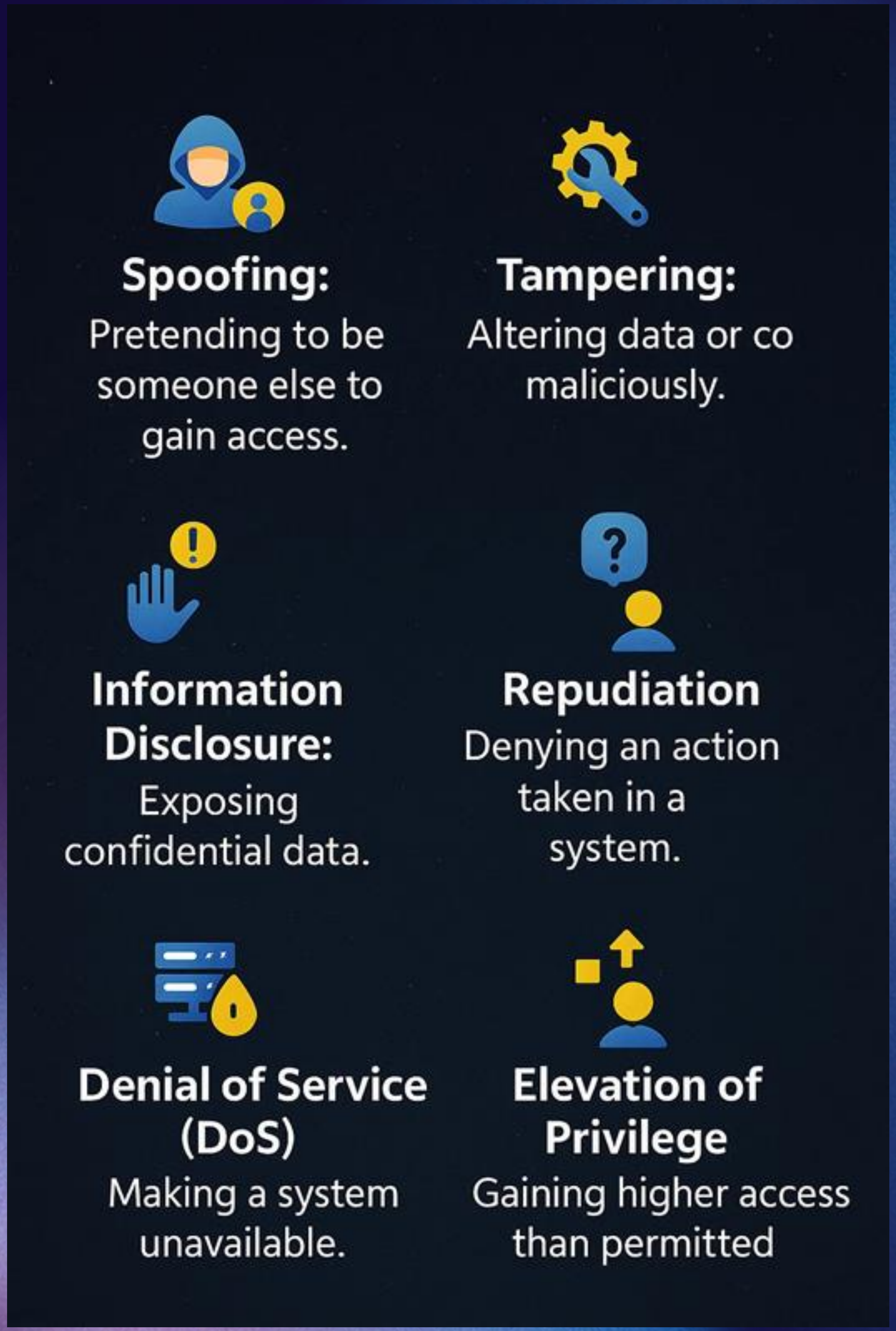
- Planning
  - High-Level threat modelling
- Requirements
  - Technical non-functional security req.
- Design
  - Formal diagram
- Implementation
  - Refine
- Testing & Integration
  - Supportive role
- Maintenance
  - Prevents security decay over time



Frameworks

STRIDE:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- DoS
- Privilege Escalation



Spoofing: Pretending to be someone else to gain access.

Tampering: Altering data or co maliciously.

Information Disclosure: Exposing confidential data.

Repudiation Denying an action taken in a system.

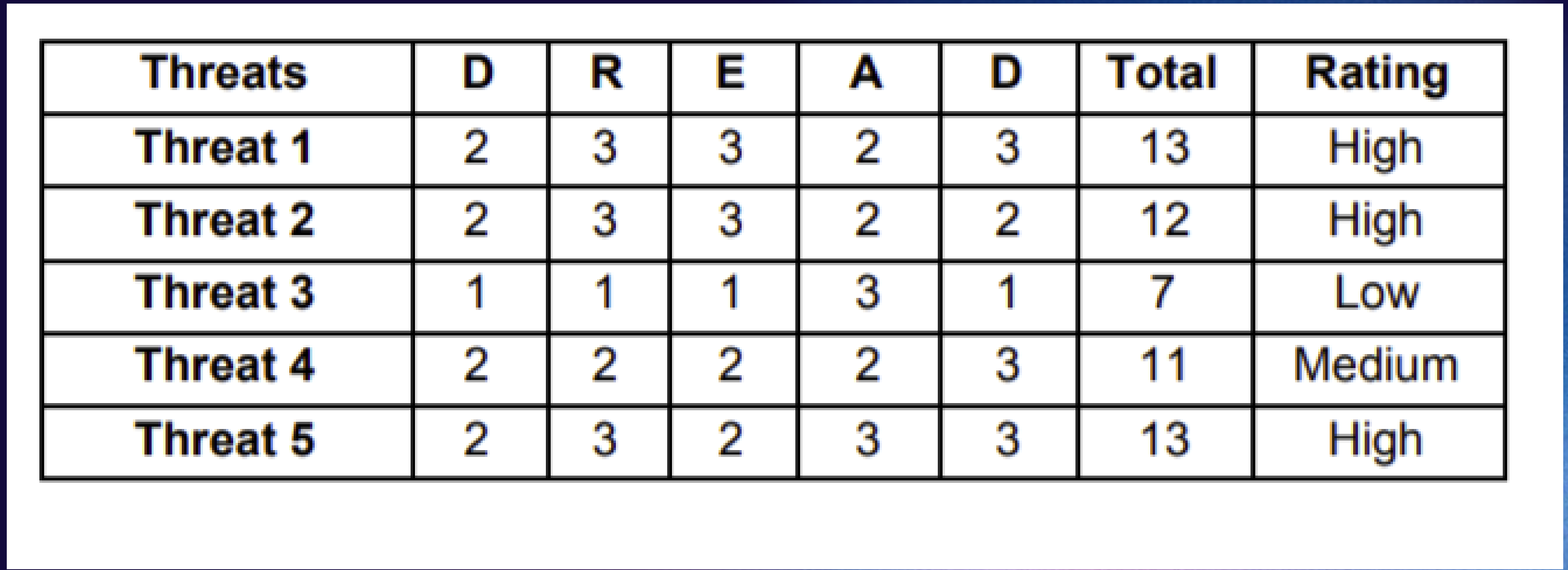
Denial of Service (DoS) Making a system unavailable.

Elevation of Privilege Gaining higher access than permitted

Frameworks

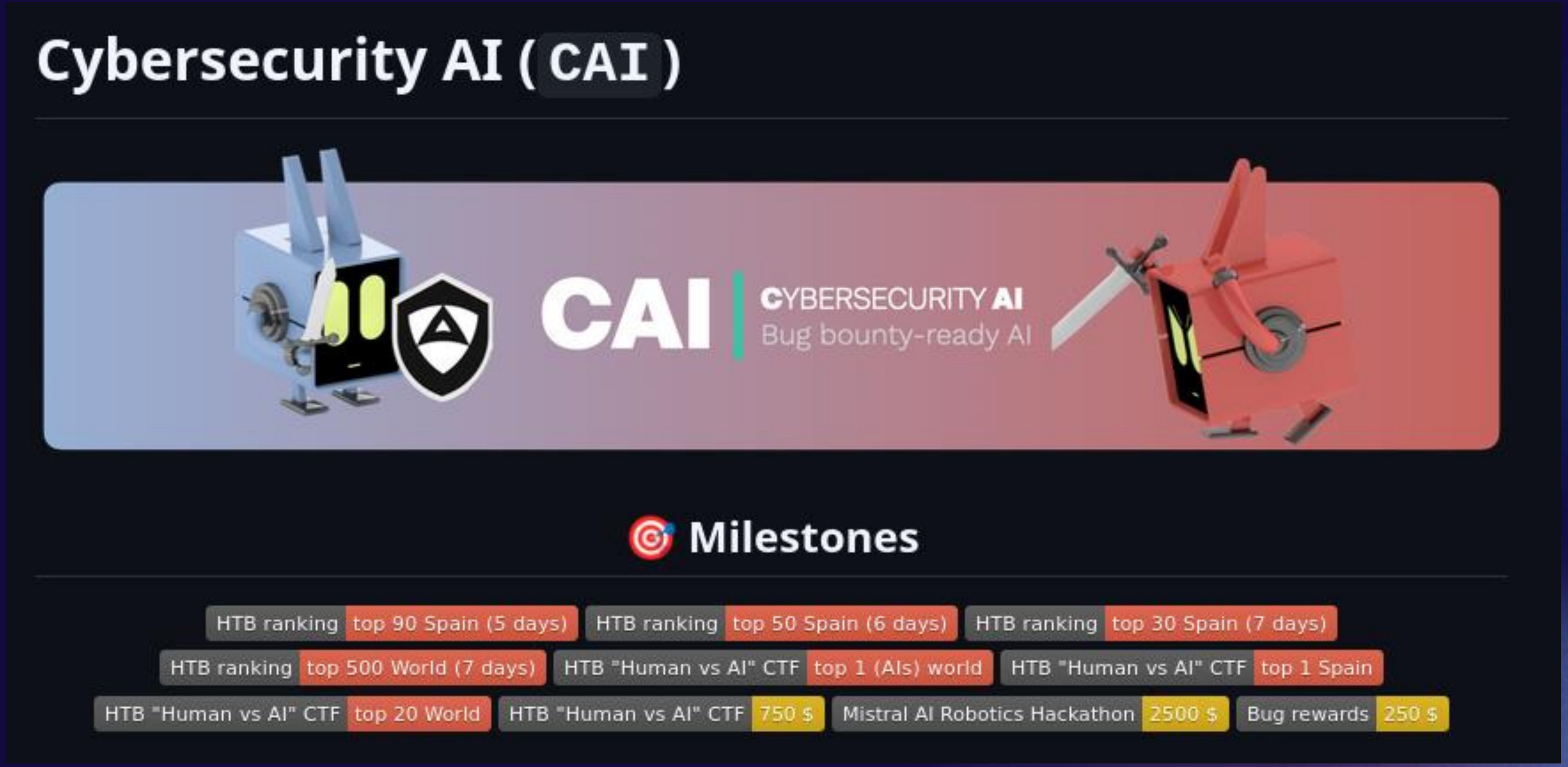
DREAD (for scoring):

- ○ Damage
- ○ Reproducibility
- ○ Exploitability
- ○ Affected users
- ○ Discoverability



Threats	D	R	E	A	D	Total	Rating
Threat 1	2	3	3	2	3	13	High
Threat 2	2	3	3	2	2	12	High
Threat 3	1	1	1	3	1	7	Low
Threat 4	2	2	2	2	3	11	Medium
Threat 5	2	3	2	3	3	13	High

Tip #1



Cybersecurity AI (`CAI`)

CAI | CYBERSECURITY AI
Bug bounty-ready AI

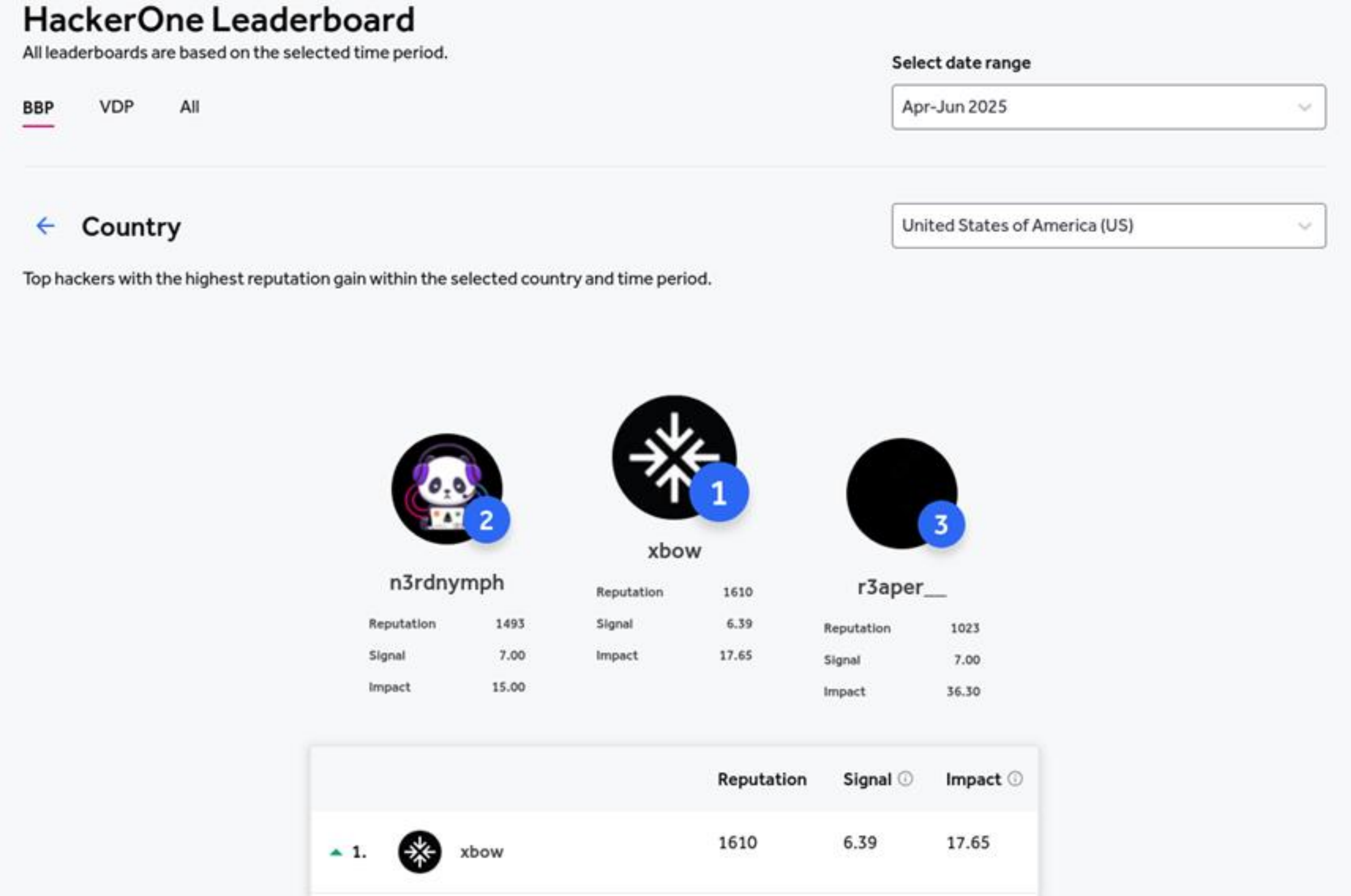
🎯 Milestones

HTB ranking | top 90 Spain (5 days)
HTB ranking | top 50 Spain (6 days)
HTB ranking | top 30 Spain (7 days)
HTB ranking | top 500 World (7 days)
HTB "Human vs AI" CTF | top 1 (AIs) world
HTB "Human vs AI" CTF | top 1 Spain
HTB "Human vs AI" CTF | top 20 World
HTB "Human vs AI" CTF | 750 $
Mistral AI Robotics Hackathon | 2500 $
Bug rewards | 250 $

“We predict that by 2028, AI-powered security testing tools will outnumber human pentesters.”

OWASP Sofia

Tip #1



HackerOne Leaderboard

All leaderboards are based on the selected time period.

BBP VDP All

Select date range: Apr-Jun 2025

Country

United States of America (US)

Top hackers with the highest reputation gain within the selected country and time period.

2 n3rdnymph

Reputation	1493
Signal	7.00
Impact	15.00

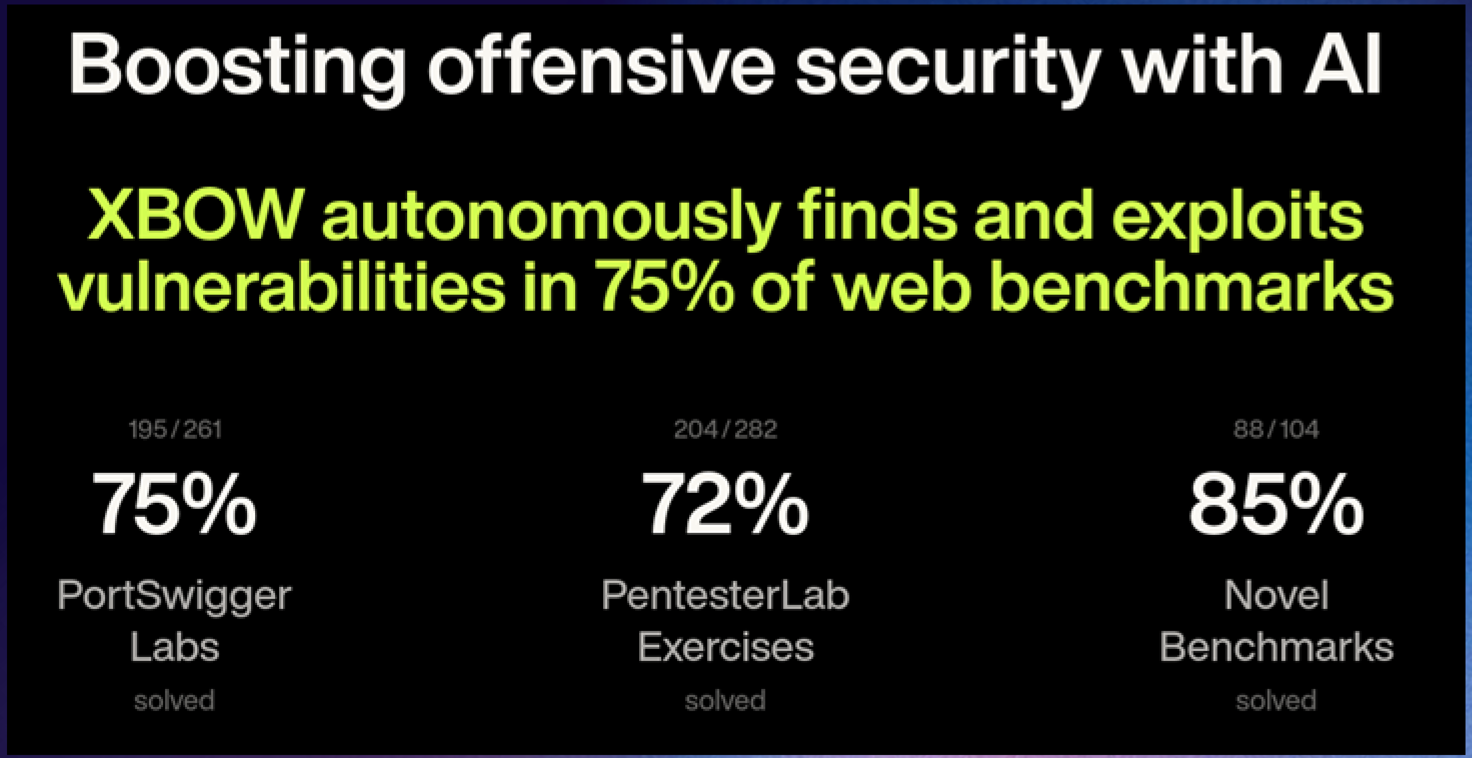
1 xbow

Reputation	1610
Signal	6.39
Impact	17.65

3 r3aper__

Reputation	1023
Signal	7.00
Impact	36.30

		Reputation	Signal ⓘ	Impact ⓘ
▲ 1.	xbow	1610	6.39	17.65

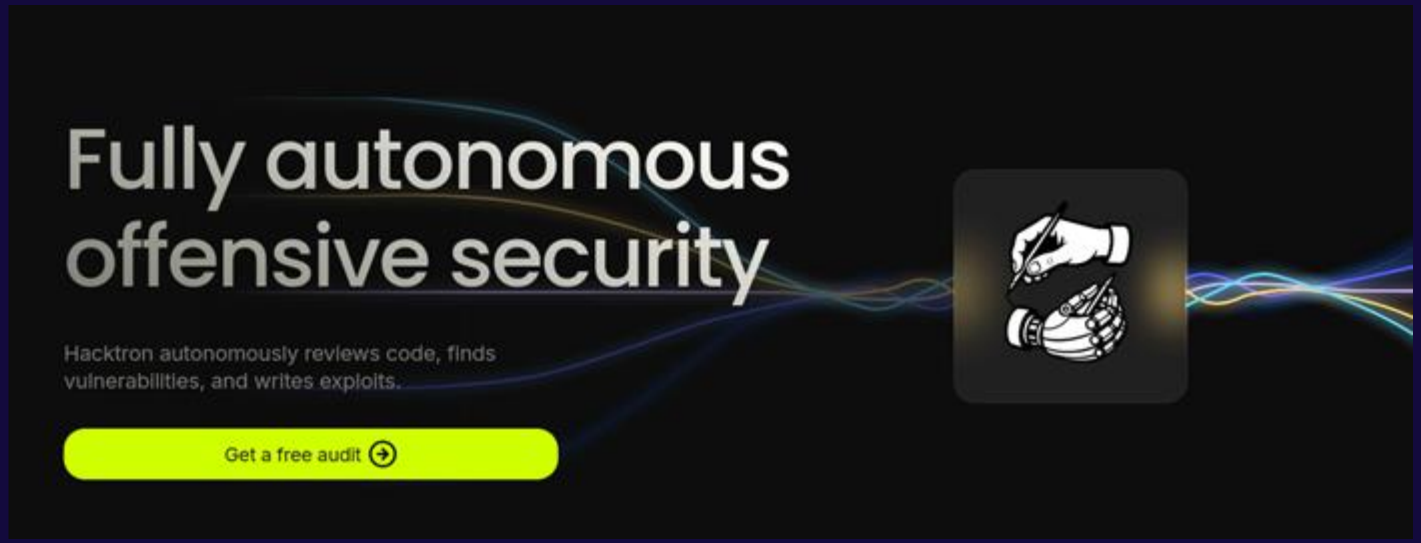


Boosting offensive security with AI

XBOW autonomously finds and exploits vulnerabilities in 75% of web benchmarks

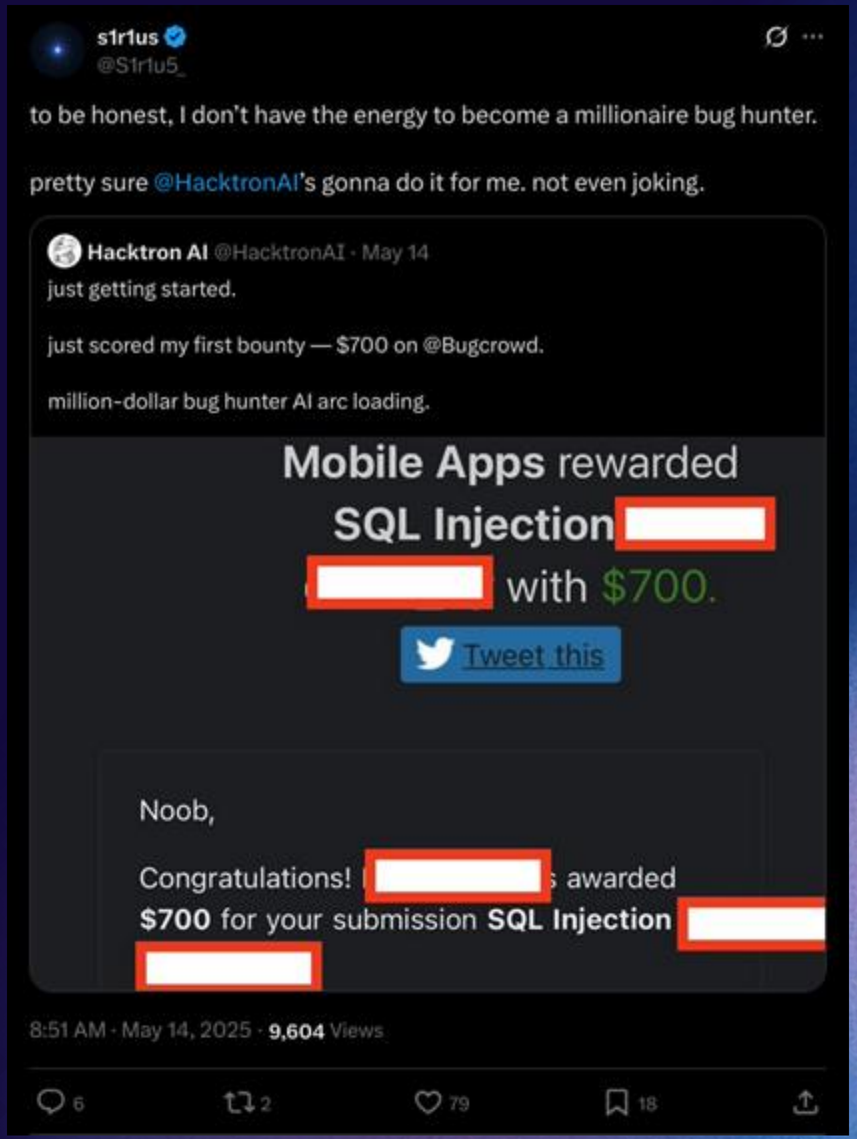
195 / 261	204 / 282	88 / 104
75%	72%	85%
PortSwigger Labs	PentesterLab Exercises	Novel Benchmarks
solved	solved	solved

Tip #1



Fully autonomous offensive security

Hacktron autonomously reviews code, finds vulnerabilities, and writes exploits.



s1r1us
@S1r1u5_

to be honest, I don't have the energy to become a millionaire bug hunter.

pretty sure @HacktronAI's gonna do it for me. not even joking.

Hacktron AI @HacktronAI · May 14
just getting started.

just scored my first bounty — $700 on @Bugcrowd.

million-dollar bug hunter AI arc loading.

Mobile Apps rewarded **SQL Injection** [redacted] [redacted] with $700.

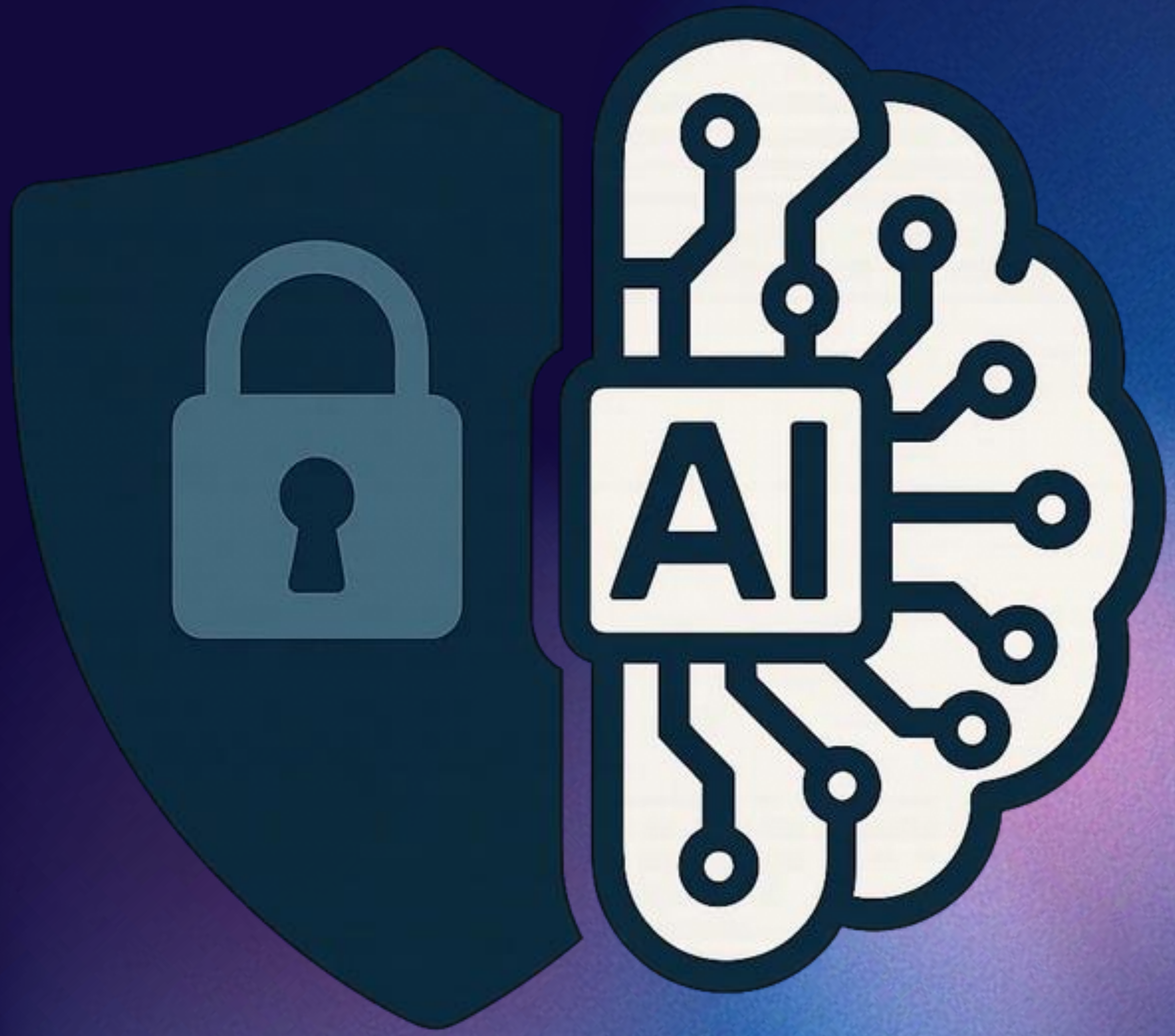
Noob,

Congratulations! [redacted] awarded **$700** for your submission **SQL Injection** [redacted] [redacted]

8:51 AM · May 14, 2025 · **9,604** Views

Tip #1 - Use AI

- DEMO
- Privacy Concerns?
  - Local Model (Qwen) + RAG
  - Masking

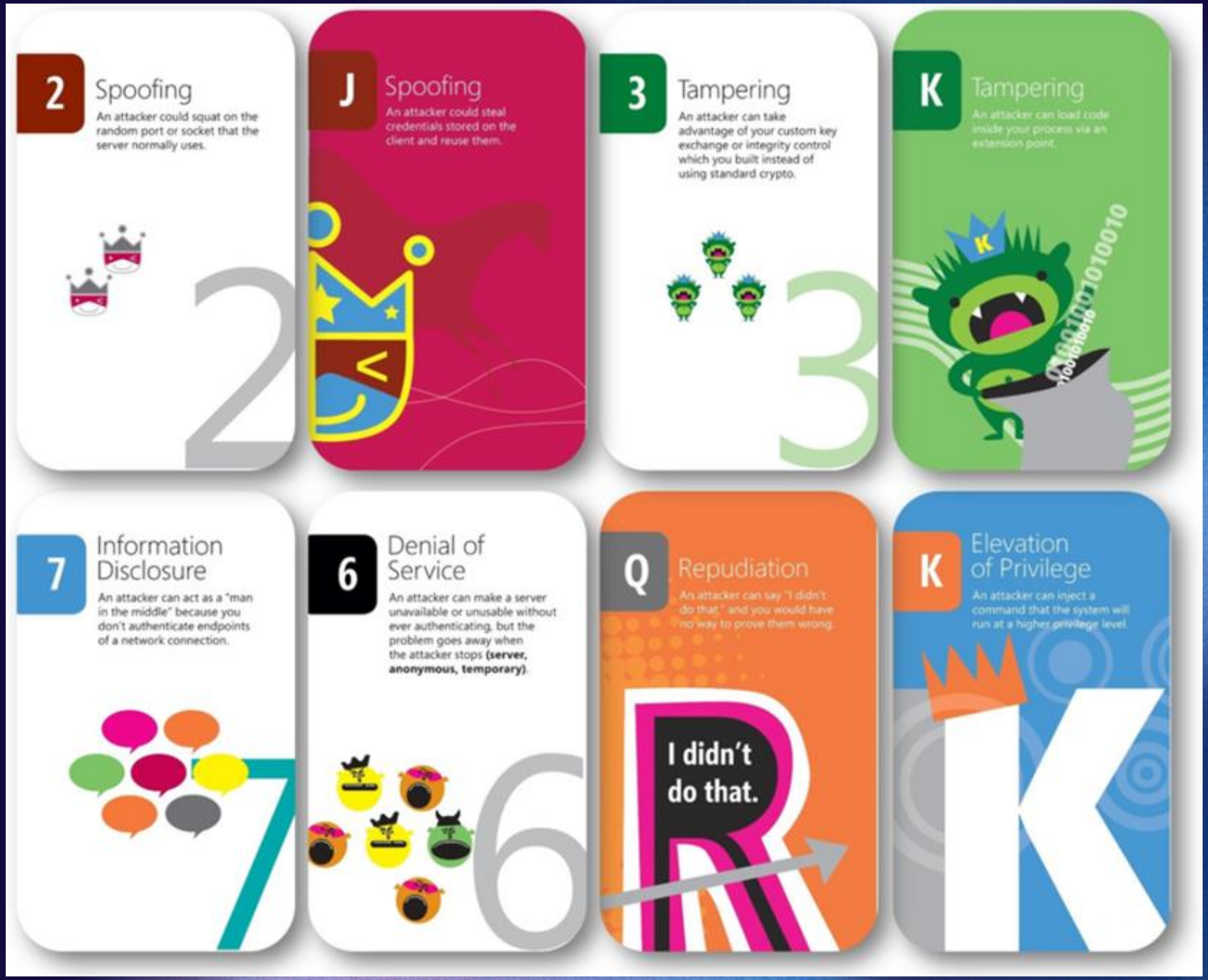


OWASP Sofia

Tip #2 - Gamifying threat modeling

EoP

- Makes it inclusive
- Low entry-level barrier
- Competitive thinking ⇒ creativity



2 Spoofing
An attacker could squat on the random port or socket that the server normally uses.

J Spoofing
An attacker could steal credentials stored on the client and reuse them.

3 Tampering
An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto.

K Tampering
An attacker can load code inside your process via an extension point.

7 Information Disclosure
An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection.

6 Denial of Service
An attacker can make a server unavailable or unusable without ever authenticating, but the problem goes away when the attacker stops **(server, anonymous, temporary)**.

Q Repudiation
An attacker can say "I didn't do that," and you would have no way to prove them wrong.

K Elevation of Privilege
An attacker can inject a command that the system will run at a higher privilege level.

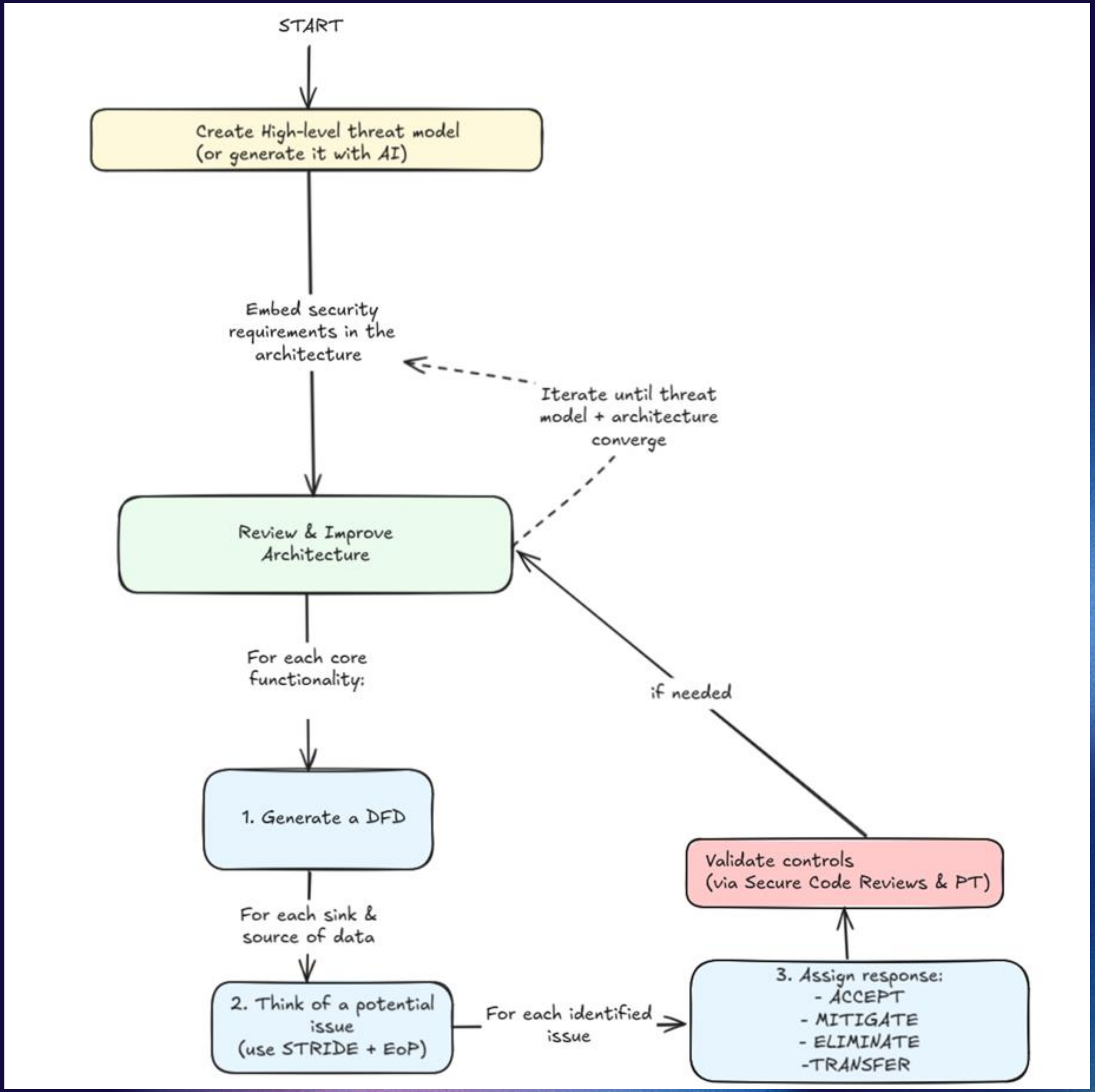
Tip #3 - Start Simple: No Fancy Tools Required

- Whiteboards and Paper
- Digital tools:
  - Draw.io
  - Excalidraw
- Specialized tools:
  - OWASP Threat Dragon

TLDR;

Key times to threat model:

- Requirements & Design phases
- Major feature or architectural change
- Before release
- After incident or periodically


START
Create High-level threat model
(or generate it with AI)
Embed security requirements in the architecture
Iterate until threat model + architecture converge
Review & Improve Architecture
For each core functionality:
if needed
1. Generate a DFD
Validate controls
(via Secure Code Reviews & PT)
For each sink & source of data
2. Think of a potential issue
(use STRIDE + EoP)
For each identified issue
3. Assign response:
- ACCEPT
- MITIGATE
- ELIMINATE
-TRANSFER

Thank you!

Q & A