From red team to blue team: the hard life of DeFi protocols

ETH Belgrade 2025

BY: ENGN33R

Today's Agenda

1. Auditor mindset vs. Builder mindset
2. Why audits don't make protocols secure
3. Takeaways from transitioning

Slides: engn33r.com

World's Fastest Intro

I'm engn33r, I do security and code
Currently dev @ Twyne
Formerly auditor @ electisec

twyne

yAudit

yAcademy

Electisec

01

Auditor Mindset vs. Builder Mindset

Virgin Dev

Can't fix
all the bugs

Chad Auditor

Eats bugs
for breakfast

Auditor Mindset

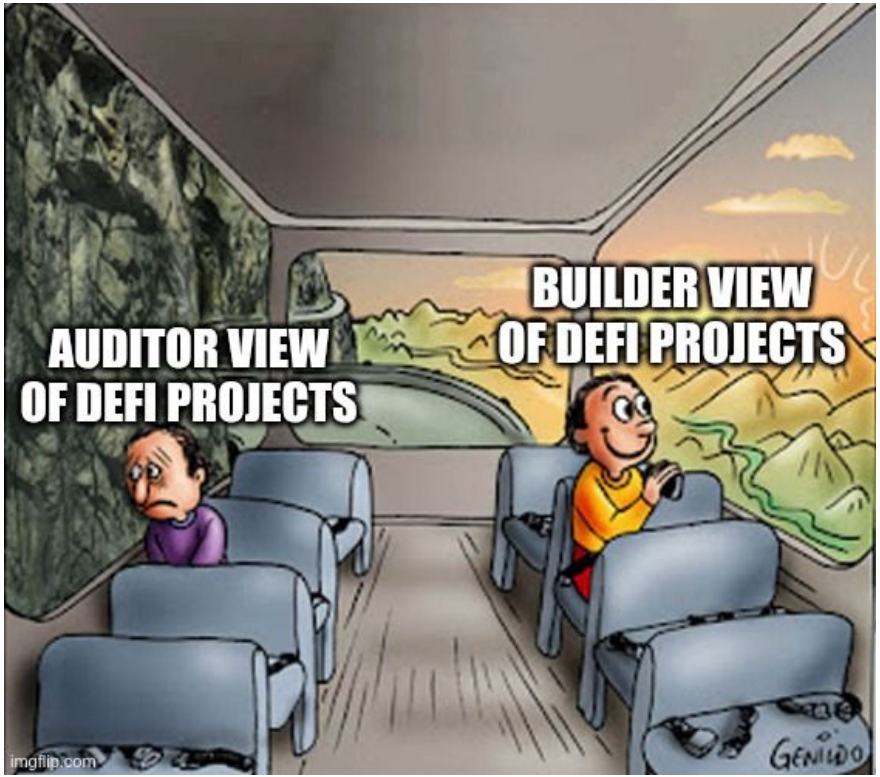
1. Focuses on **finding** problems
2. Finds **joy** in identifying imperfections
3. **Loves** complexity (complexity = bugs!)
4. Usually **flexing** on crypto twitter
5. Always **giving** criticism in audit reports
6. **Finds** one bug in code, becomes a **hero**

Builder Mindset

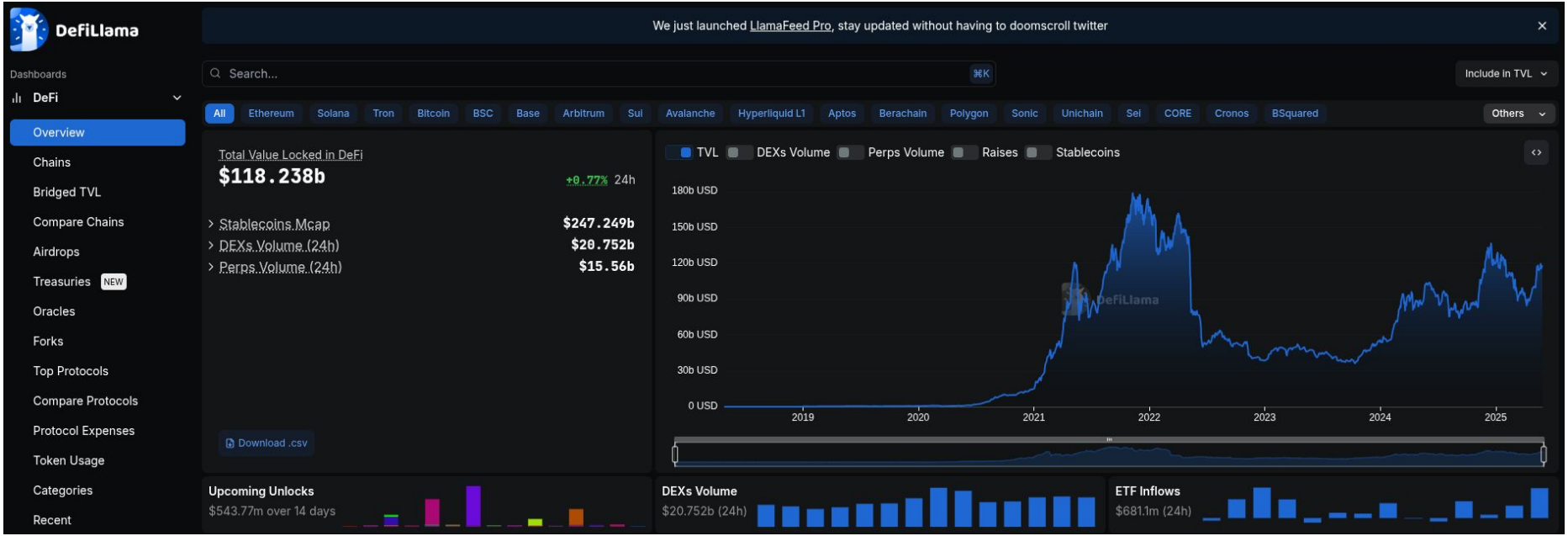
1. Focuses on **solving** problems
2. Finds **stress** in identifying imperfections
3. **Hates** complexity (complexity = bugs!)
4. Usually **silent** on crypto twitter to boost ego
5. Always **receiving** criticism in audit reports
6. **Leaves** one bug in code, becomes a **devil**

Auditor -> Builder = crazy?

Auditor -> Builder != crazy



Different perspectives



Not unique

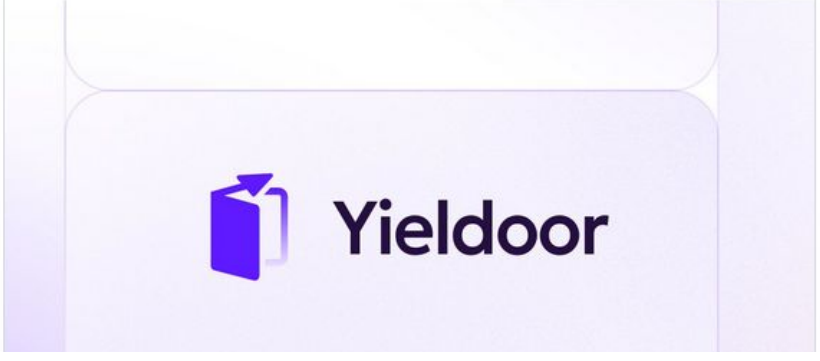
obront | eth/acc
@zachobront

auditooor to frustrated usooor to buildooor pipeline is strong

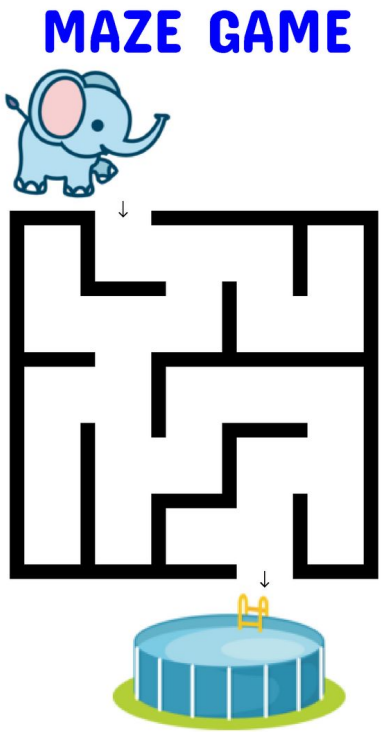
congrats to @deadrosesxyz on the upcoming launch

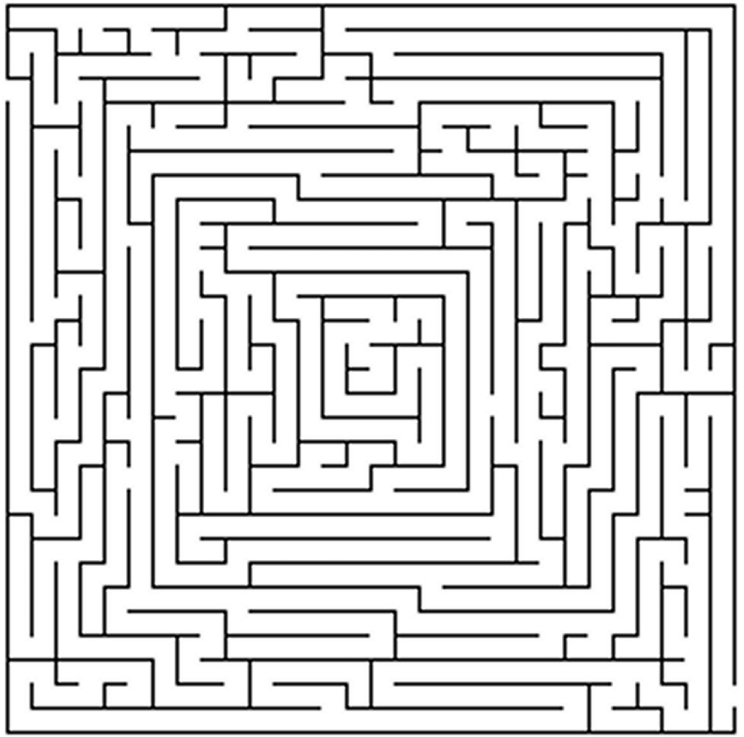
deadrosesxyz @deadrosesxyz · Feb 21
Announcing @YieldoorFi

The past few months I took on the interesting challenge of starting my own protocol and I'm so excited that I can finally share that with you.
...
Show more



Little did I know...





Briefly, about Twyne

https://twyne.xyz/

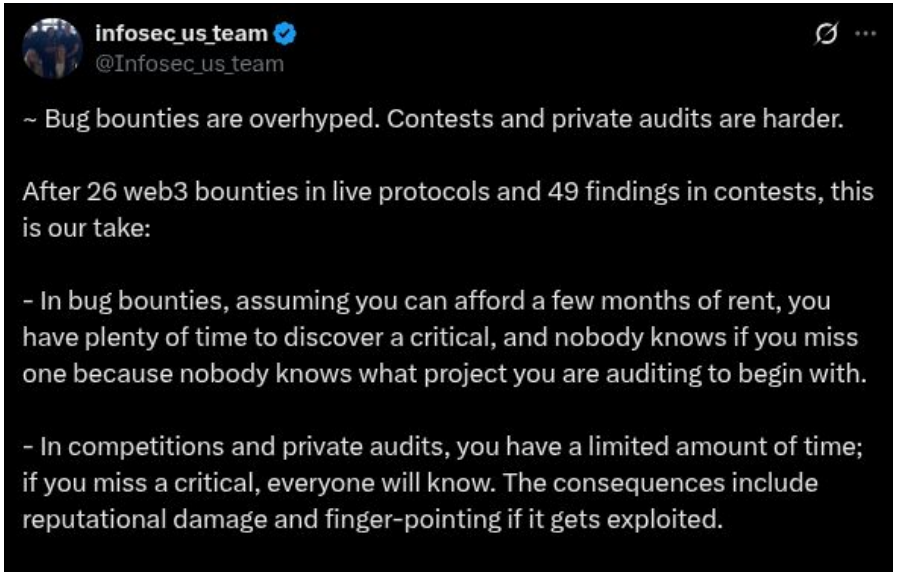
02

Why audits don’t make secure protocols

1. Breaking is easier than building

1. Breaking is easier than building

- A single bug is success or failure
- Like how bug bounty is “easier” than contests/auditing
  https://x.com/Infosec_us_team/status/1926272635509301398



2. Secure contract code is step 1

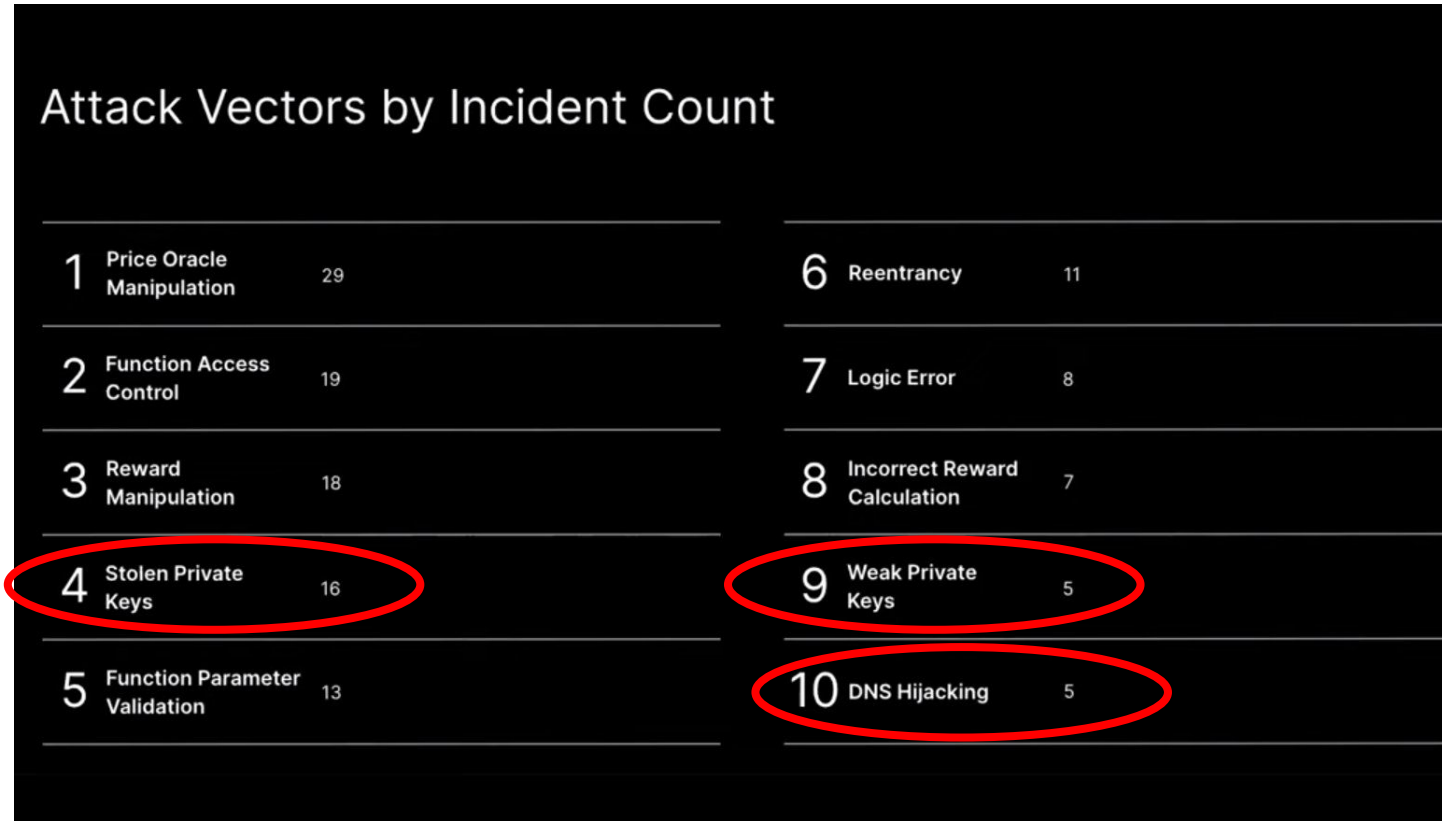
- This is all auditors care about
- It’s the MVP for a successful protocol
- If step 1 fails, everything fails
- If step 1 succeeds, everything can STILL fail

3. No checks of real attack vectors

	Audited	Not Audited
Multisig Security		X
Private key management		X
Team member device security		X
Team member password management		X
Frontend security & integrity		X
Smart contracts	☺	

3. No checks of real attack vectors

3. No checks of real attack vectors



4. Web3 still depends on web2

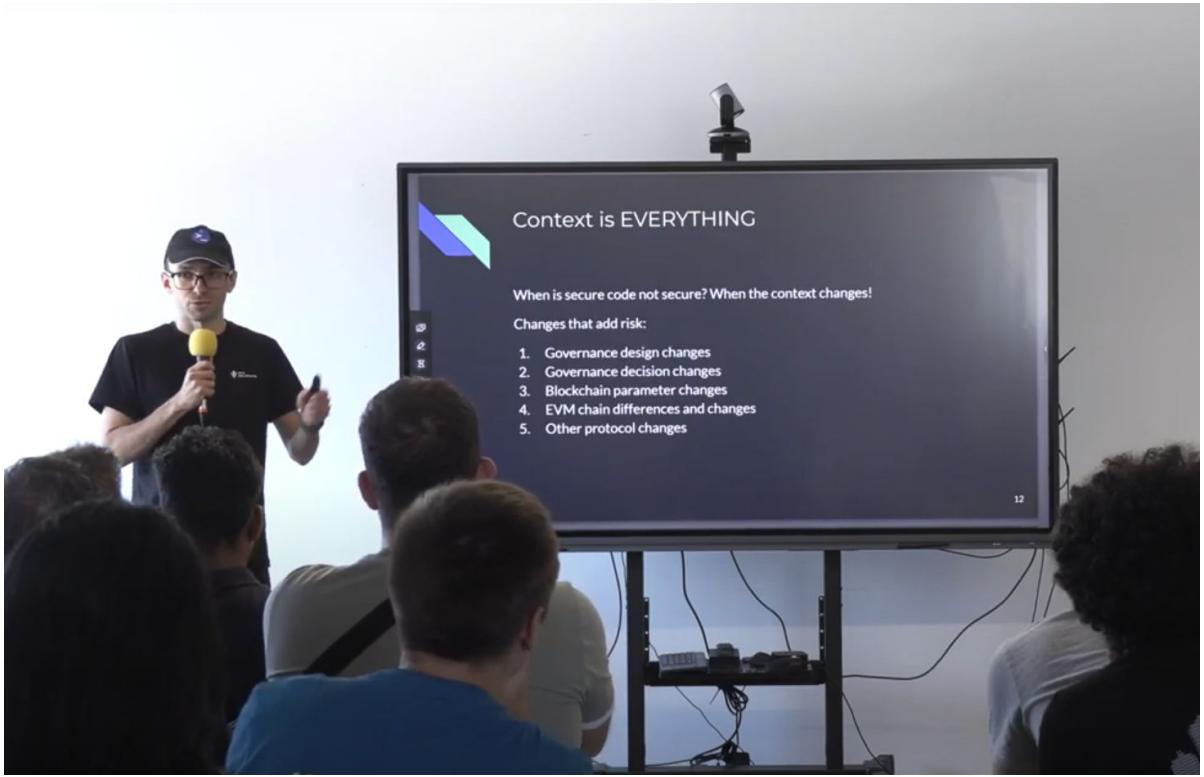
Tops ways traditional companies get hacked:

- Social engineering
- Phishing
- Malicious downloads
- Weak/stolen credentials
- Insider threats

5. Audits omit on-chain context

- Governance configuration
- Multisig signing procedure
- Deployment scripts
- Emergency procedures

5. Audits omit on-chain context



5. Audits omit on-chain context

6. dApp frontends are a huge weakness

6. dApp frontends are a huge weakness

- ByBit hack via Safe frontend could happen to any dApp
- Current web3 frontend security approach is laughable:
  - Confirm you are visiting the proper URL
  - Check crypto twitter to make sure no tweets about “frontend is hacked”
  - Trust the frontend ~99%
  - Protocols have no good way to verify their live frontend

03

Takeaways from Transitioning

Change is good for gaining perspective

- Auditing isn't going to make web3 secure
- UI/UX for new protocols is hard but important
- Protocol integrations are annoying (and web3 docs often bad)

New perspective helps with learning

Learnings to be a better security auditor:

- Primary dev goal is functionality, security comes later
- Best approach for security for devs is reducing complexity
- As contract design changes, refactoring code is mandatory
- Code without test coverage often has bugs!
- ^Especially focus on missing test coverage of branches
- If you see mock contracts in tests, be suspicious - they hide bugs

Writing code is a totally different view

- So much effort is put into test coverage
- Best approach for security for devs is reducing complexity
- As contract design changes, refactoring code is mandatory
- Code without test coverage often has bugs!
- ^Especially focus on missing test coverage of branches
- If you see mock contracts in tests, be suspicious - they hide bugs

Lots of opportunities in this space

- You don’t have to stay in one specialty for years
- If you want to mix things up, mix things up!
- Easier to gain experience in a new technology

You'll see the same people later :)

- In Crypto Twitter
- In Discord
- In Telegram
- And of course, at conferences :)

04

Summary

Summary

- Auditor mindset is different from builder mindset
- Protocol security is multifaceted
  - Secure every team member
  - Secure every piece of tech stack
  - Secure every operational step
- New role = new perspectives
  - Appreciation for builders
  - New learnings of where bugs hide

How it started

How it’s going

Questions?

THANK YOU