Security Frameworks

High-level web3 security best practices

Security Alliance

Non-profit organization led by **samczsun**

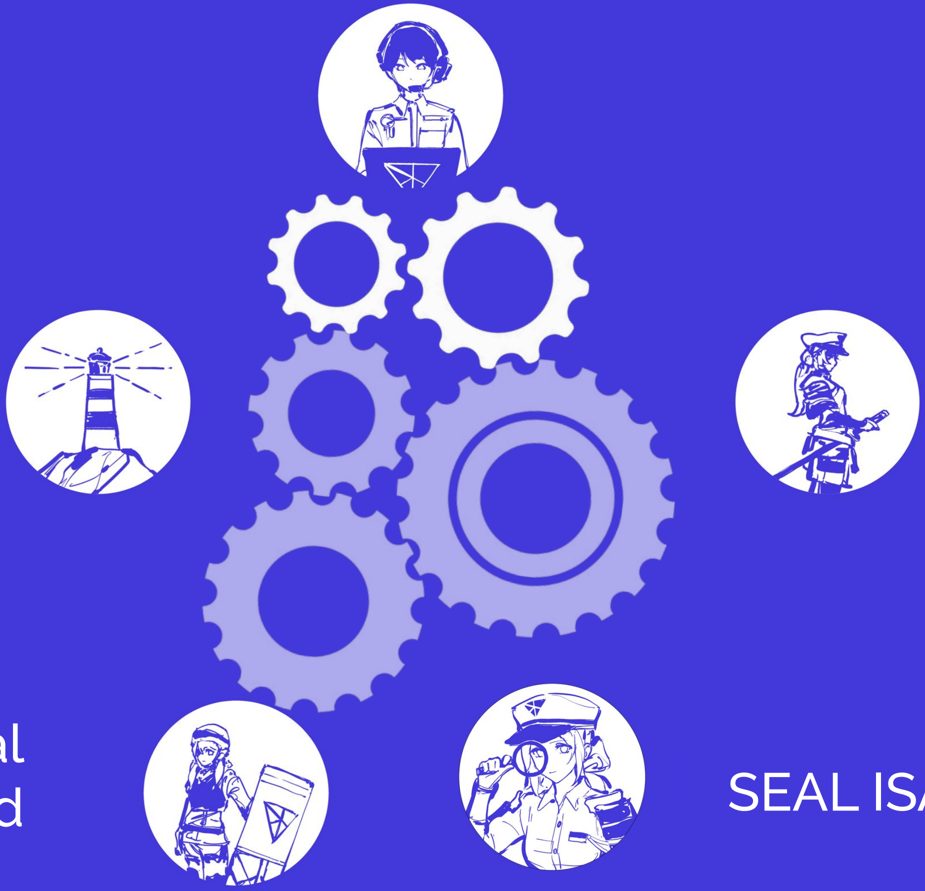
Represents **crypto security** industry

Cross-industry authoritative voice

Security Alliance
THE VILLAGE AT BEACON CENTRE
OFFICE SUITES
8323
Security Alliance
Security Alliance

thx K for this image

SEAL 911



Whitehat safe harbor agreement

SEAL Wargames

Whitehat legal defense fund

SEAL ISAC

Sharing knowledge

Supporting local communities

Original educational content

Social skills development

Contests

Gamified learning platforms

DamnVulnerableDefi

the red guild

Awareness campaigns

Phishing dojo

Hosting conferences

CTFs

Bug hunting

therekgames

Security research

Security Frameworks

Talks
Workshops
Mentoring
Judging

Spotchecks

911

Wargames

Whitehat safe harbor agreement

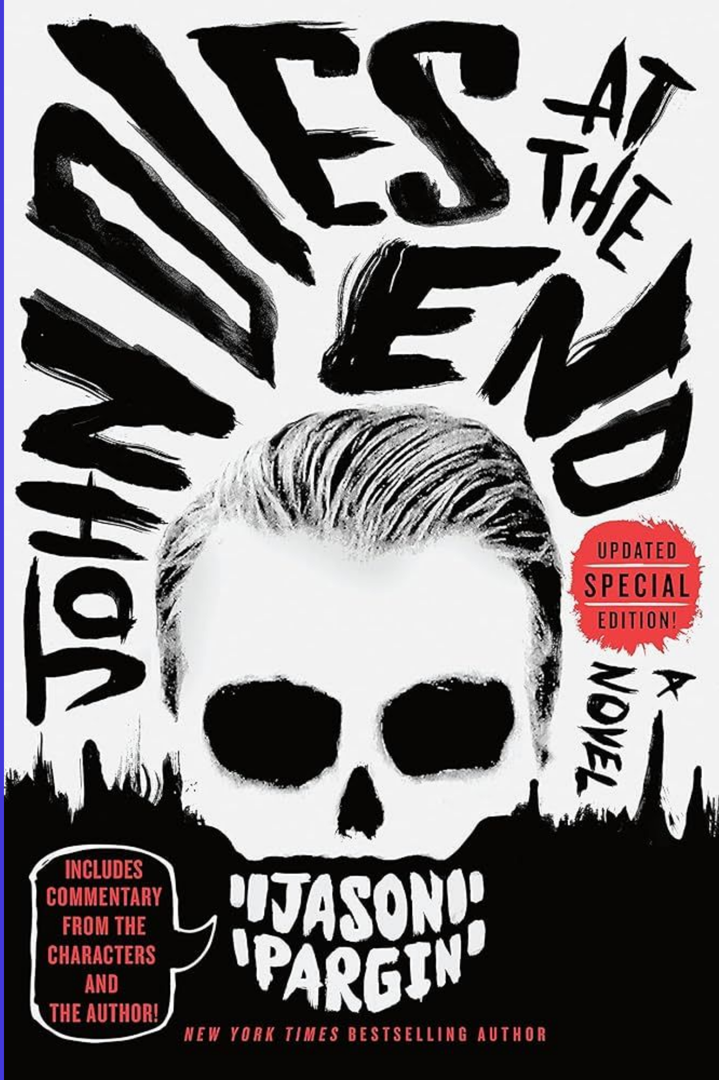
Whitehat legal defense fund

ISAC

Outline

1. Current state
2. Problem
3. Solution
4. Challenges
5. How to collaborate

1. Current state


JOHN DIES AT THE END
UPDATED SPECIAL EDITION!
A NOVEL
INCLUDES COMMENTARY FROM THE CHARACTERS AND THE AUTHOR!
JASON PARGIN
NEW YORK TIMES BESTSELLING AUTHOR

Live deployment (not a release!)

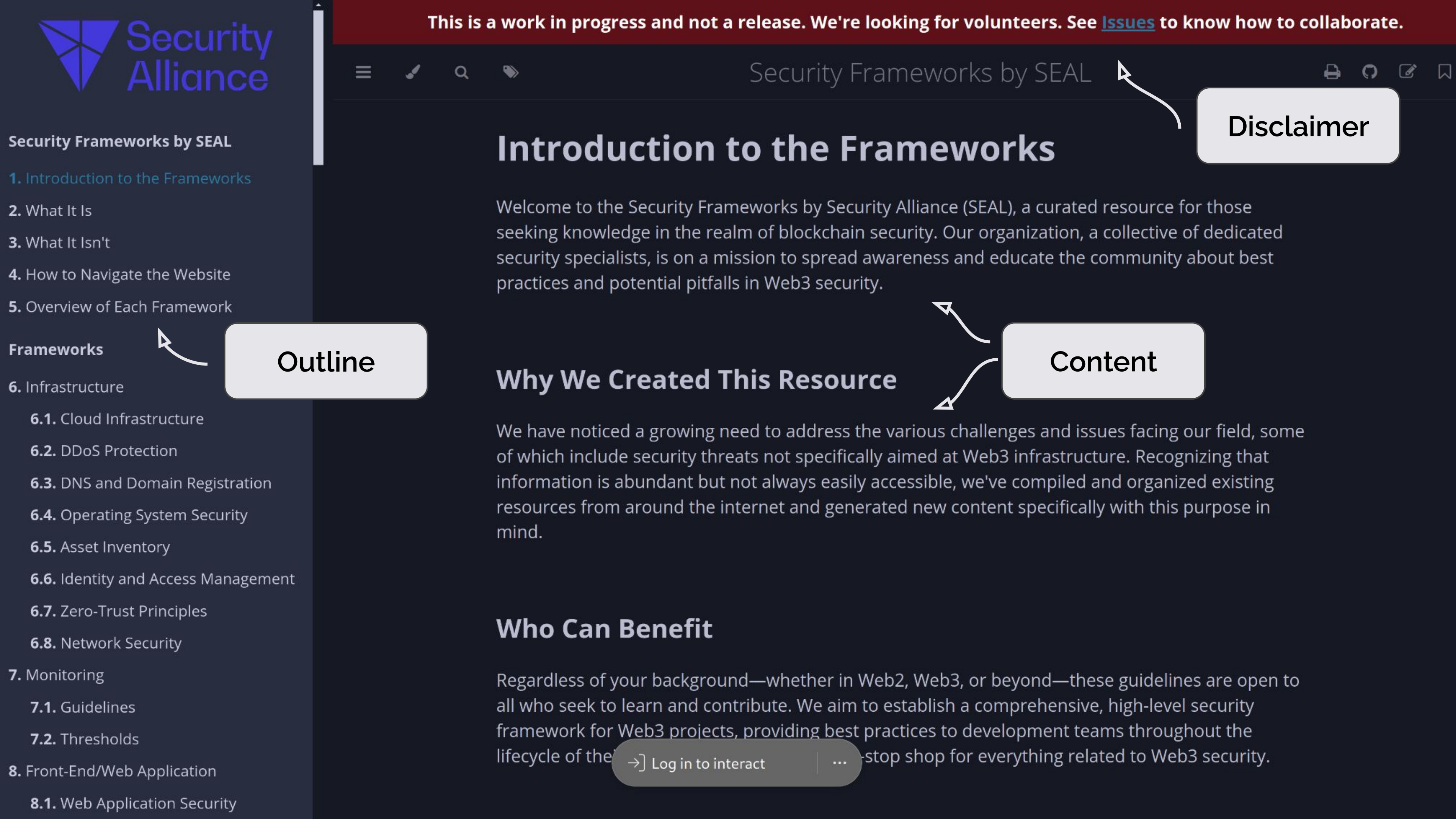
`main`

↳ **frameworks**.securityalliance.**org**

`develop`

↳ **frameworks**.securityalliance.**dev**

Screenshots


Security Alliance
Security Frameworks by SEAL
1. Introduction to the Frameworks
2. What It Is
3. What It Isn't
4. How to Navigate the Website
5. Overview of Each Framework
Frameworks
6. Infrastructure
6.1. Cloud Infrastructure
6.2. DDoS Protection
6.3. DNS and Domain Registration
6.4. Operating System Security
6.5. Asset Inventory
6.6. Identity and Access Management
6.7. Zero-Trust Principles
6.8. Network Security
7. Monitoring
7.1. Guidelines
7.2. Thresholds
8. Front-End/Web Application
8.1. Web Application Security
Security Frameworks by SEAL
Disclaimer
Outline
Content
Log in to interact
···

This is a work in progress and not a release. We're looking for volunteers. See Issues to know how to collaborate.

Introduction to the Frameworks

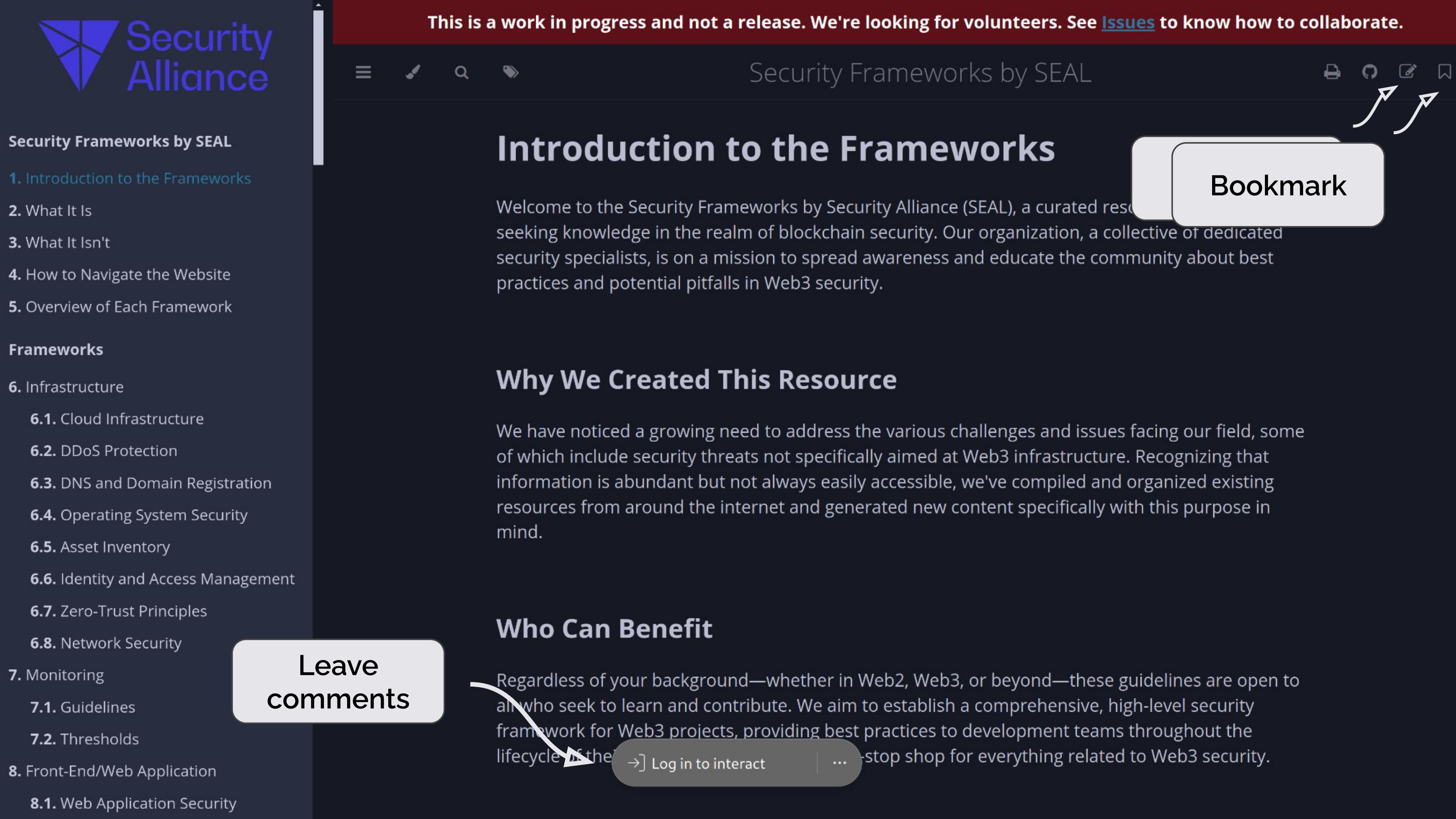
Welcome to the Security Frameworks by Security Alliance (SEAL), a curated resource for those seeking knowledge in the realm of blockchain security. Our organization, a collective of dedicated security specialists, is on a mission to spread awareness and educate the community about best practices and potential pitfalls in Web3 security.

Why We Created This Resource

We have noticed a growing need to address the various challenges and issues facing our field, some of which include security threats not specifically aimed at Web3 infrastructure. Recognizing that information is abundant but not always easily accessible, we've compiled and organized existing resources from around the internet and generated new content specifically with this purpose in mind.

Who Can Benefit

Regardless of your background—whether in Web2, Web3, or beyond—these guidelines are open to all who seek to learn and contribute. We aim to establish a comprehensive, high-level security framework for Web3 projects, providing best practices to development teams throughout the lifecycle of the -stop shop for everything related to Web3 security.



Security Alliance

This is a work in progress and not a release. We're looking for volunteers. See Issues to know how to collaborate.

Security Frameworks by SEAL

Introduction to the Frameworks

Welcome to the Security Frameworks by Security Alliance (SEAL), a curated reso seeking knowledge in the realm of blockchain security. Our organization, a collective of dedicated security specialists, is on a mission to spread awareness and educate the community about best practices and potential pitfalls in Web3 security.

Why We Created This Resource

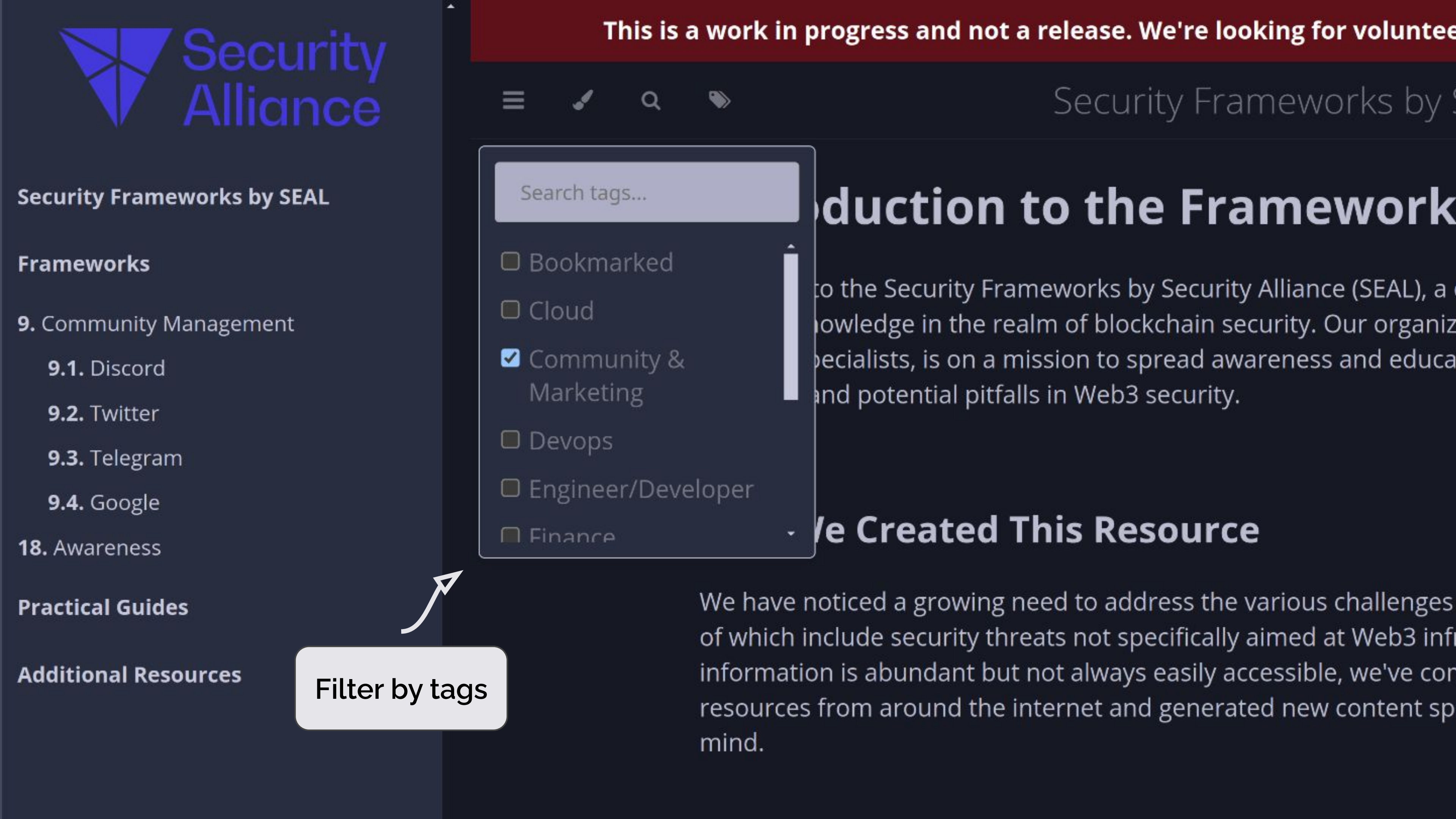
We have noticed a growing need to address the various challenges and issues facing our field, some of which include security threats not specifically aimed at Web3 infrastructure. Recognizing that information is abundant but not always easily accessible, we've compiled and organized existing resources from around the internet and generated new content specifically with this purpose in mind.

Who Can Benefit

Regardless of your background—whether in Web2, Web3, or beyond—these guidelines are open to all who seek to learn and contribute. We aim to establish a comprehensive, high-level security framework for Web3 projects, providing best practices to development teams throughout the lifecycle of the -stop shop for everything related to Web3 security.

Bookmark

Leave comments



This is a work in progress and not a release. We're looking for voluntee

Search tags...

□ Bookmarked
□ Cloud
☑ Community & Marketing
□ Devops
□ Engineer/Developer
□ Finance

duction to the Framework

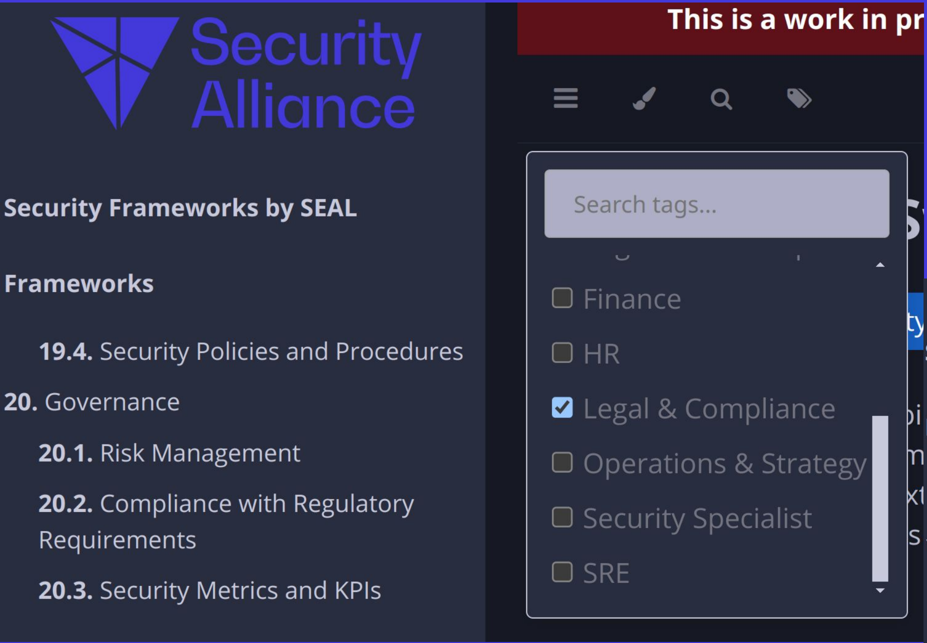
to the Security Frameworks by Security Alliance (SEAL), a
owledge in the realm of blockchain security. Our organiz
ecialists, is on a mission to spread awareness and educa
and potential pitfalls in Web3 security.

/e Created This Resource

We have noticed a growing need to address the various challenges
of which include security threats not specifically aimed at Web3 inf
information is abundant but not always easily accessible, we've co
resources from around the internet and generated new content sp
mind.

Filter by tags

1. Current state



Security Alliance

This is a work in pr

Security Frameworks by SEAL

Frameworks

19.4. Security Policies and Procedures

20. Governance

20.1. Risk Management

20.2. Compliance with Regulatory Requirements

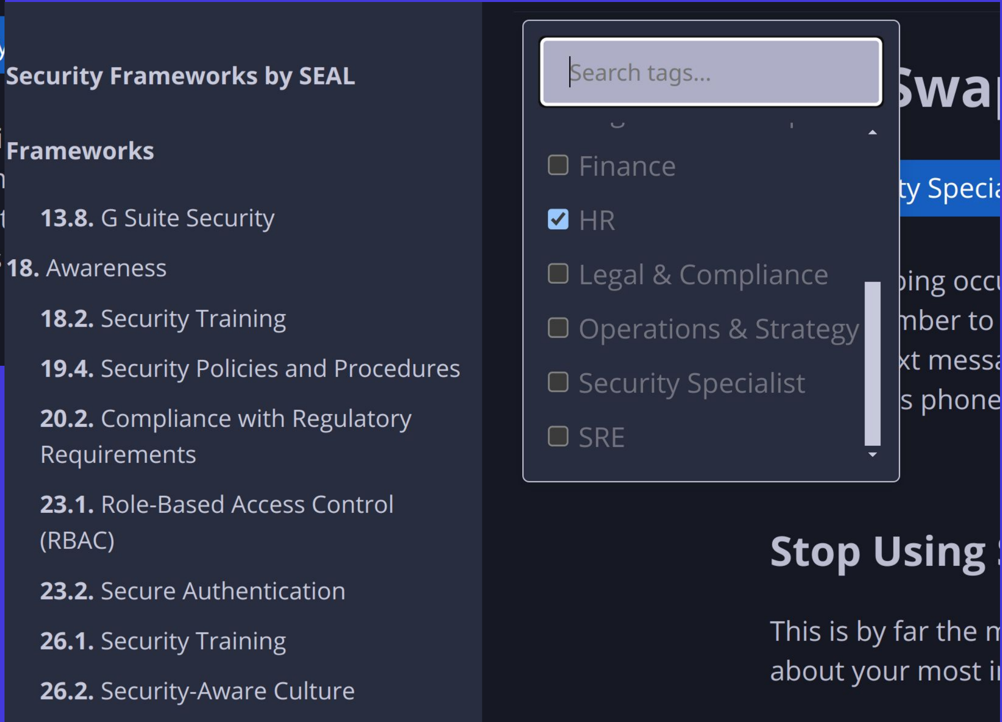
20.3. Security Metrics and KPIs

Search tags...

- □ Finance
- □ HR
- ☑ Legal & Compliance
- □ Operations & Strategy
- □ Security Specialist
- □ SRE

- Cloud
- Community & Marketing
- Devops
- Engineer/Developer
- Finance

- HR
- Legal & Compliance
- Operations & Strategy
- Security Specialist
- SRE



Security Frameworks by SEAL

Frameworks

13.8. G Suite Security

18. Awareness

18.2. Security Training

19.4. Security Policies and Procedures

20.2. Compliance with Regulatory Requirements

23.1. Role-Based Access Control (RBAC)

23.2. Secure Authentication

26.1. Security Training

26.2. Security-Aware Culture

Search tags...

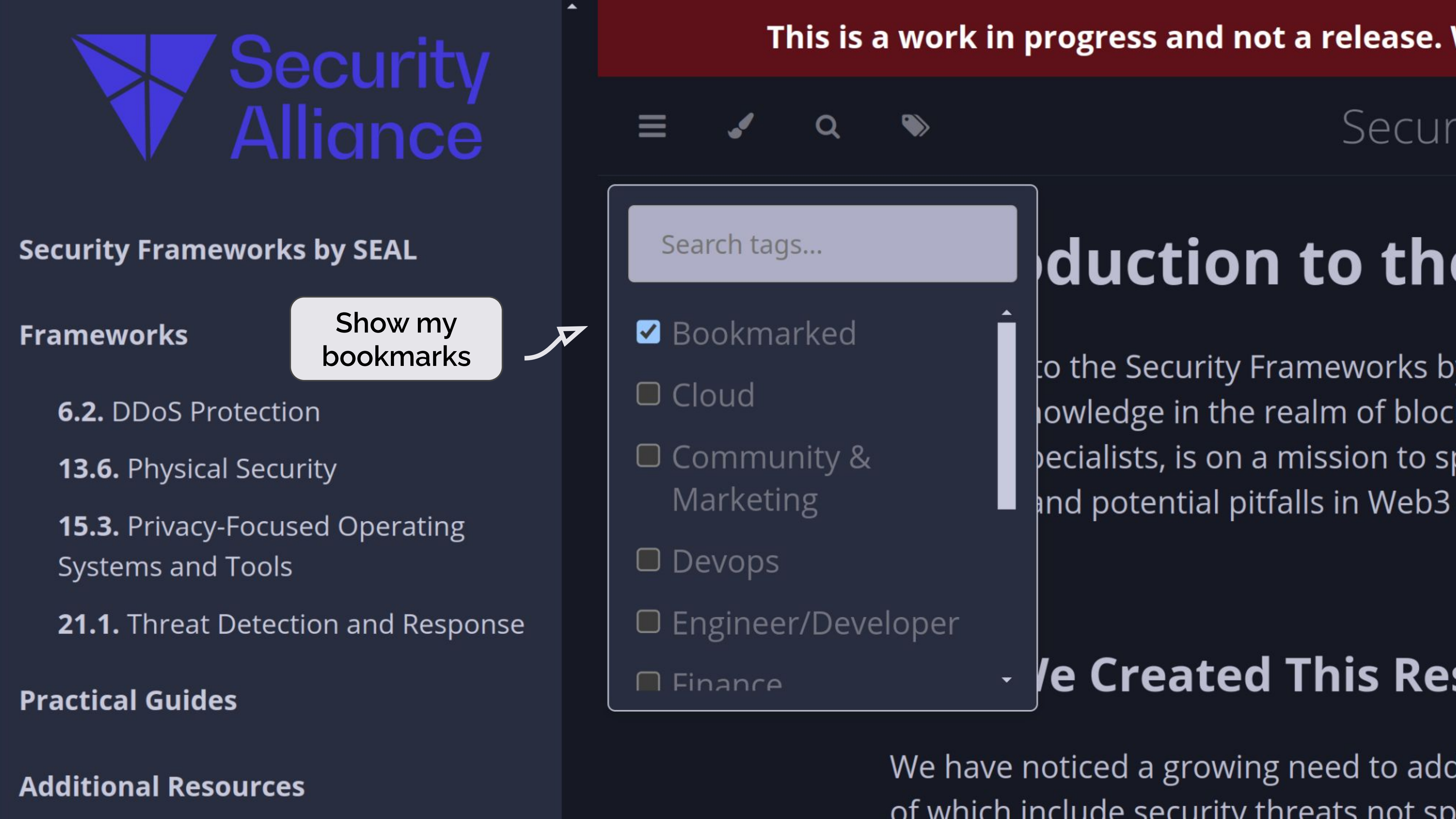
- □ Finance
- ☑ HR
- □ Legal & Compliance
- □ Operations & Strategy
- □ Security Specialist
- □ SRE

Swa

ty Speci

Stop Using

This is by far the m about your most i



Show my bookmarks

This is a work in progress and not a release. V

Secur

Search tags...

☑ Bookmarked

□ Cloud

□ Community & Marketing

□ Devops

□ Engineer/Developer

□ Finance

Security Frameworks by SEAL

Frameworks

6.2. DDoS Protection

13.6. Physical Security

15.3. Privacy-Focused Operating Systems and Tools

21.1. Threat Detection and Response

Practical Guides

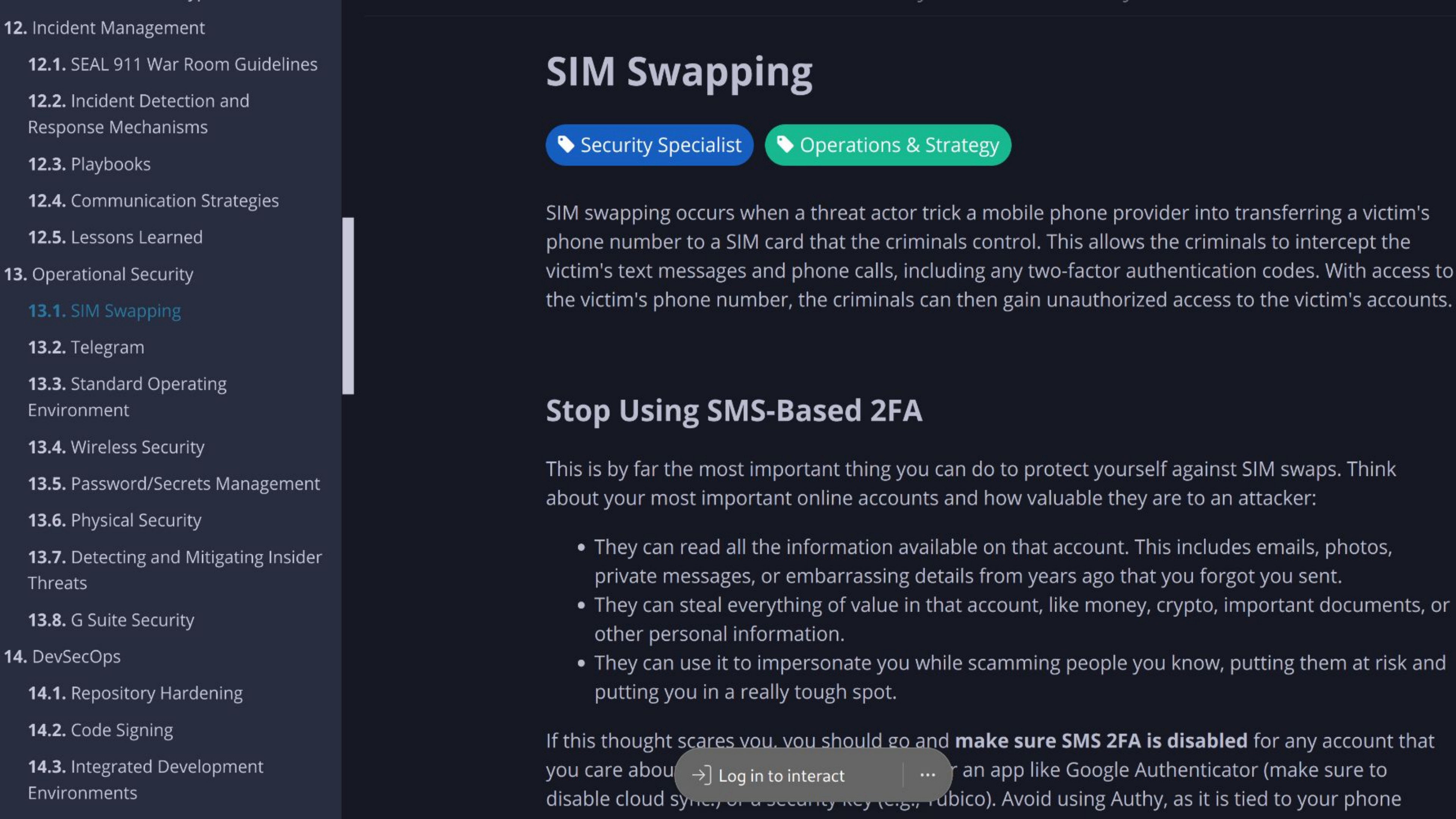
Additional Resources

oduction to th

to the Security Frameworks b
nowledge in the realm of bloc
pecialists, is on a mission to sp
and potential pitfalls in Web3

Ve Created This Re

We have noticed a growing need to ad
of which include security threats not sp



SIM Swapping

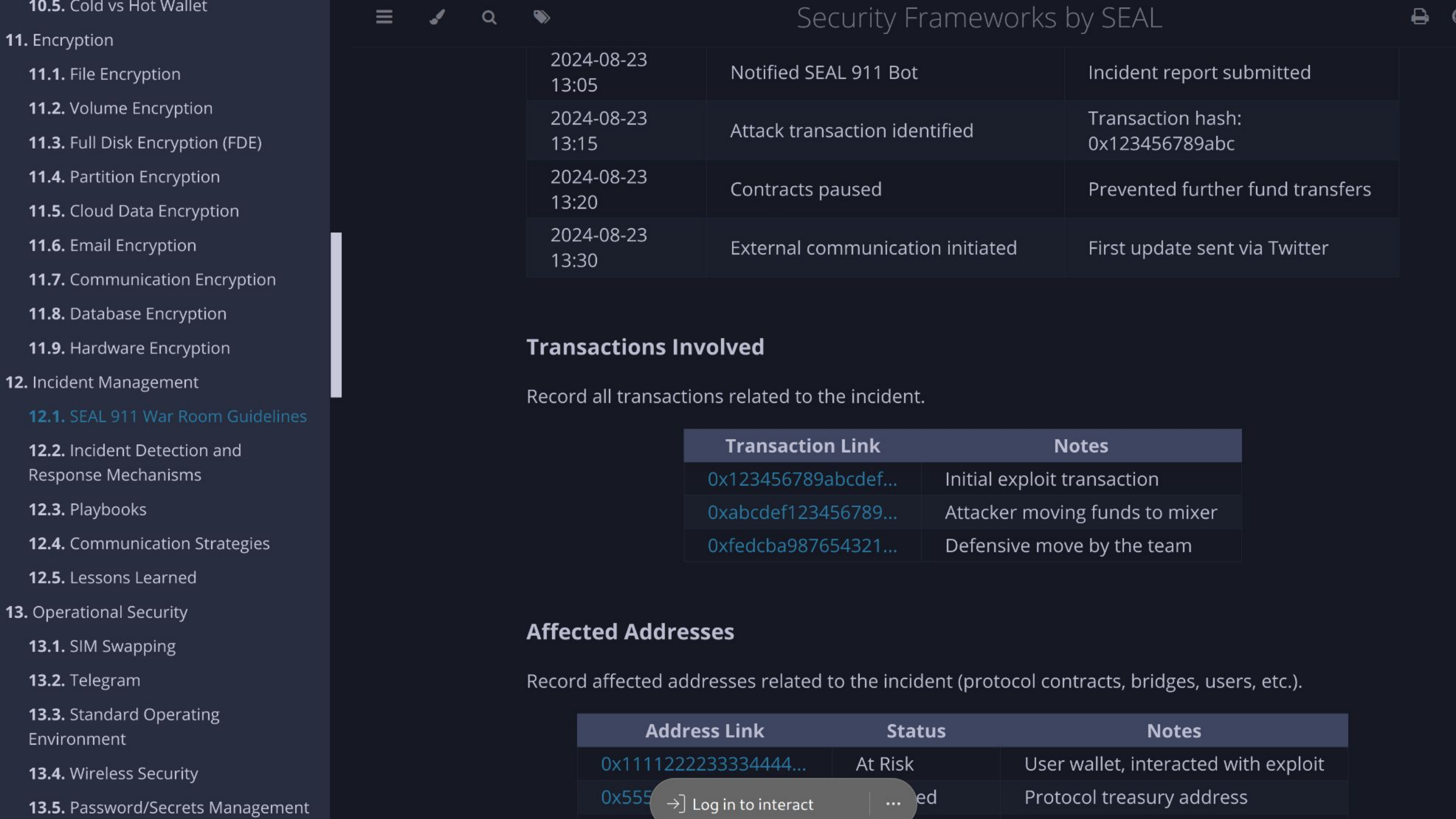
SIM swapping occurs when a threat actor trick a mobile phone provider into transferring a victim's phone number to a SIM card that the criminals control. This allows the criminals to intercept the victim's text messages and phone calls, including any two-factor authentication codes. With access to the victim's phone number, the criminals can then gain unauthorized access to the victim's accounts.

Stop Using SMS-Based 2FA

This is by far the most important thing you can do to protect yourself against SIM swaps. Think about your most important online accounts and how valuable they are to an attacker:

- They can read all the information available on that account. This includes emails, photos, private messages, or embarrassing details from years ago that you forgot you sent.
- They can steal everything of value in that account, like money, crypto, important documents, or other personal information.
- They can use it to impersonate you while scamming people you know, putting them at risk and putting you in a really tough spot.

If this thought scares you, you should go and **make sure SMS 2FA is disabled** for any account that you care abou [illegible] r an app like Google Authenticator (make sure to disable cloud sy [illegible] ubico). Avoid using Authy, as it is tied to your phone



2024-08-23 13:05	Notified SEAL 911 Bot	Incident report submitted
2024-08-23 13:15	Attack transaction identified	Transaction hash: 0x123456789abc
2024-08-23 13:20	Contracts paused	Prevented further fund transfers
2024-08-23 13:30	External communication initiated	First update sent via Twitter

Transactions Involved

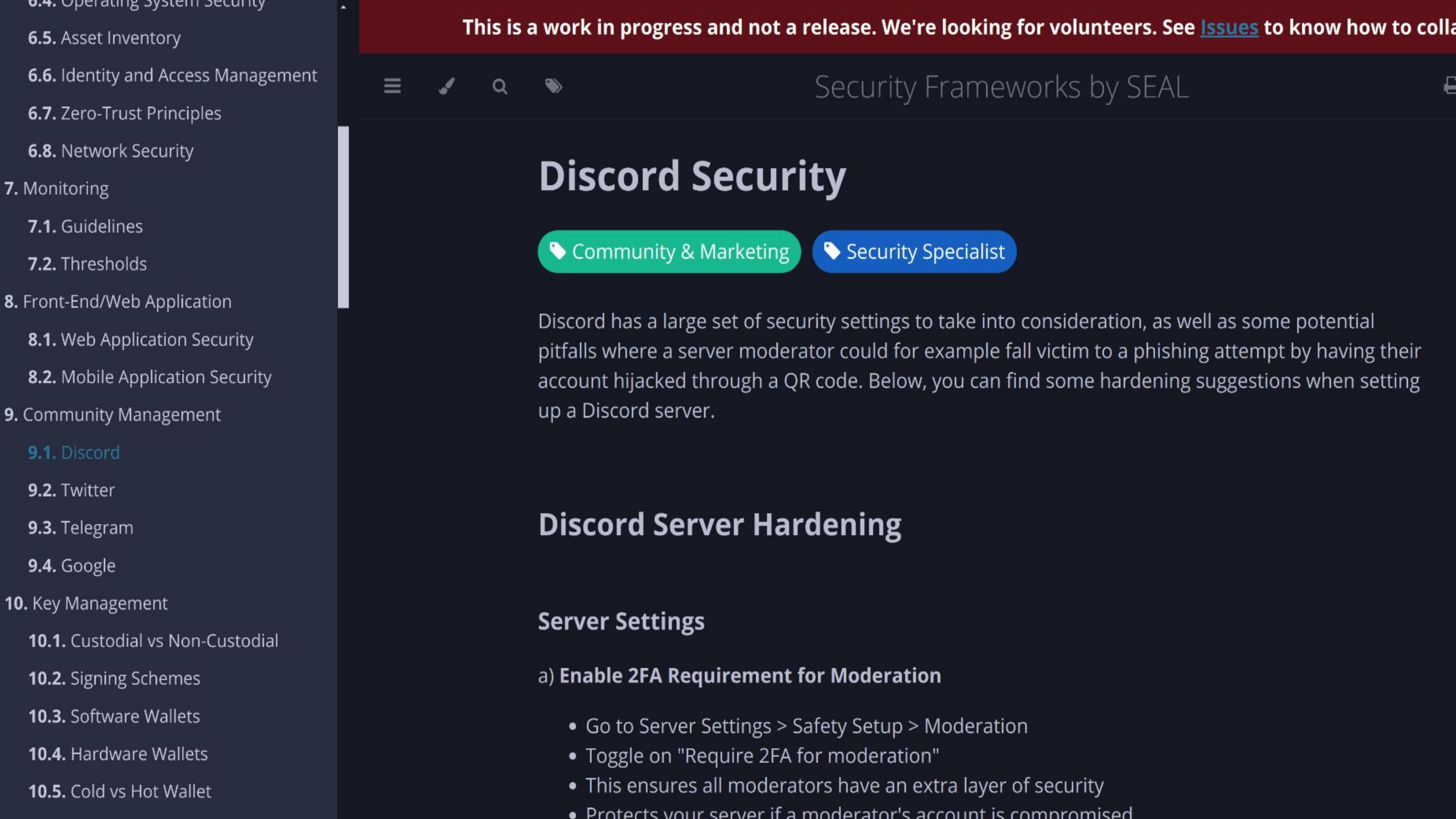
Record all transactions related to the incident.

Transaction Link	Notes
0x123456789abcdef...	Initial exploit transaction
0xabcdef123456789...	Attacker moving funds to mixer
0xfedcba987654321...	Defensive move by the team

Affected Addresses

Record affected addresses related to the incident (protocol contracts, bridges, users, etc.).

Address Link	Status	Notes
0x1111222233334444...	At Risk	User wallet, interacted with exploit
0x555	ed	Protocol treasury address



Discord Security

Community & Marketing Security Specialist

Discord has a large set of security settings to take into consideration, as well as some potential pitfalls where a server moderator could for example fall victim to a phishing attempt by having their account hijacked through a QR code. Below, you can find some hardening suggestions when setting up a Discord server.

Discord Server Hardening

Server Settings

a) **Enable 2FA Requirement for Moderation**

- Go to Server Settings > Safety Setup > Moderation
- Toggle on "Require 2FA for moderation"
- This ensures all moderators have an extra layer of security
- Protects your server if a moderator's account is compromised

Technical details

- gh repo – @security-alliance/frameworks
- **mdbook** plus theme
- **auto-deploy** with vercel
  a. **preview** links upon each **pr**
  b. **frameworks**.securityalliance.**dev|org**
  c. both accept **comments** with **vercel**

General details

- Currently **committed** core **team**
- **Minimum contents** on every page
- A LOT of **work needed** for 1st release
- Moving to the **next phase**: all **public**!
- Seeking community collaboration

2. Problem

Challenges

- ✔ Need to address various challenges in our field
  - ✖ Security threats
  - ✖ ^ not aimed at "web3" infrastructure
  - ✖ Not getting less sophisticated

Information

✔ Abundant but not easy

- ✖ Not always accessible
- ✖ Dispersed
- ✖ Difficult to track
- ✖ Outdated

3. Solution

What can we do?

- ✔ Compile it
- ✔ Organize it
- ✔ Make it accessible
- ✔ Make it digestible
- ✔ Regardless of your background

Our aim

- ✓ curated resource of blockchain security
- ✓ collection of best practices
- ✓ comprehensive guide
- ✓ helps you secure various aspects of your projects
- ✓ build resilience against potential threats
- ✓ applicable regardless of the specific technology

4. Challenges

What might difficult our process?

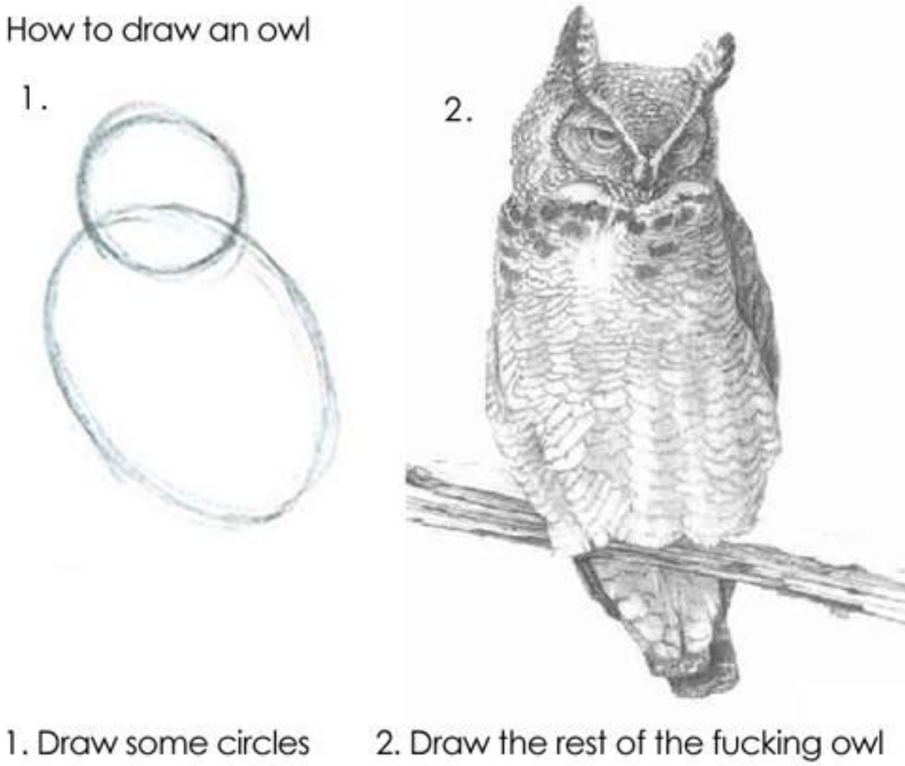
- ✓ We do really need collaboration
- ✓ Seek adoption
- ✓ Make it fairly usable
- ✓ Keep it updated

4. Challenges

High level

vs

Implementation



Matt Gleason originally posted this.
Thanks for the idea other Matt!

5. How to collaborate

Leave comments!
Annotations

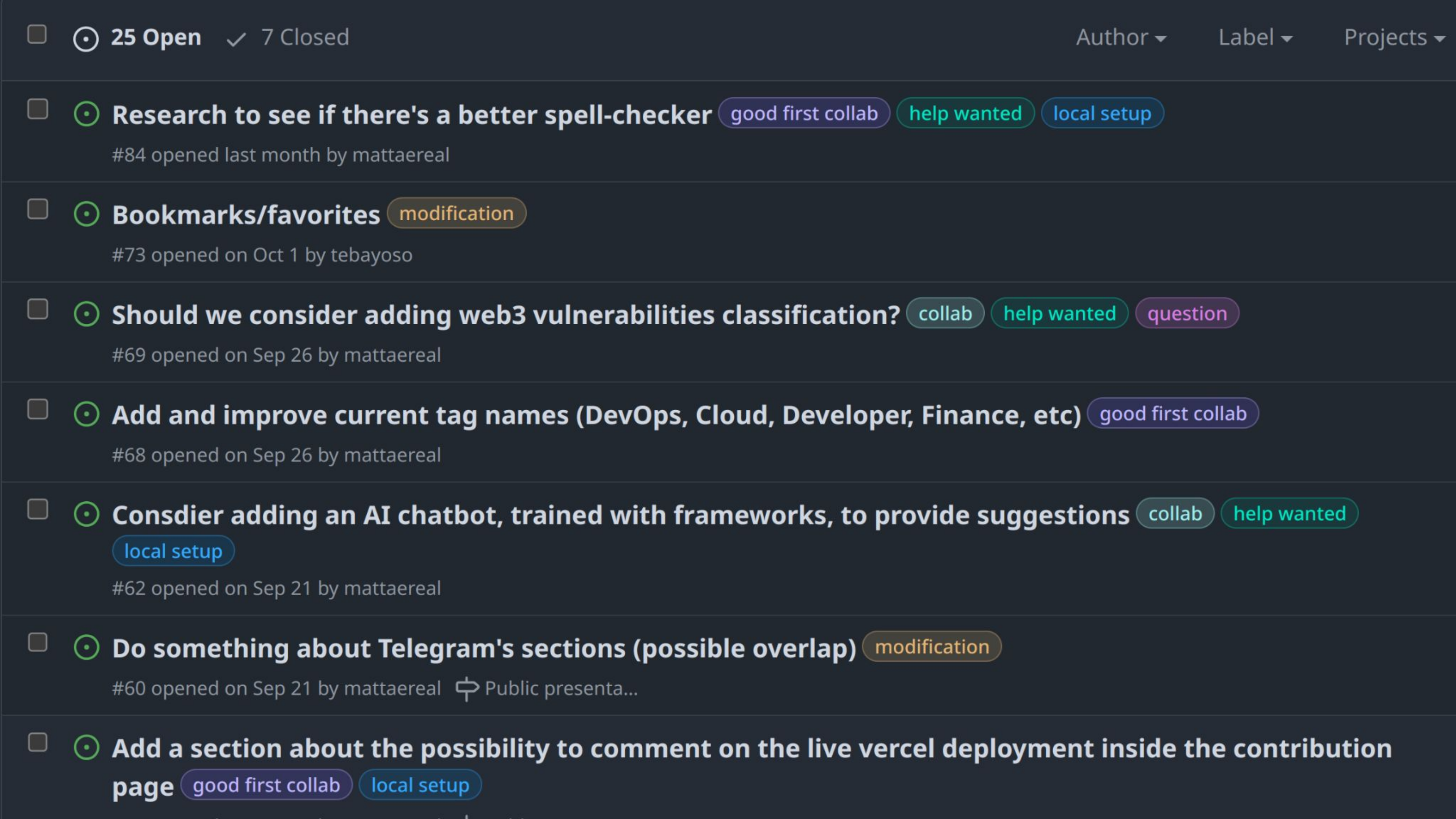
frameworks
.securityalliance
.dev

Send us a PR.
Create a discussion!

no flame warz

ez pz

GitHub
@security-alliance/
frameworks



□ ○ 25 Open ✓ 7 Closed

□ ○ **Research to see if there's a better spell-checker** good first collab help wanted local setup
#84 opened last month by mattaereal

□ ○ **Bookmarks/favorites** modification
#73 opened on Oct 1 by tebayoso

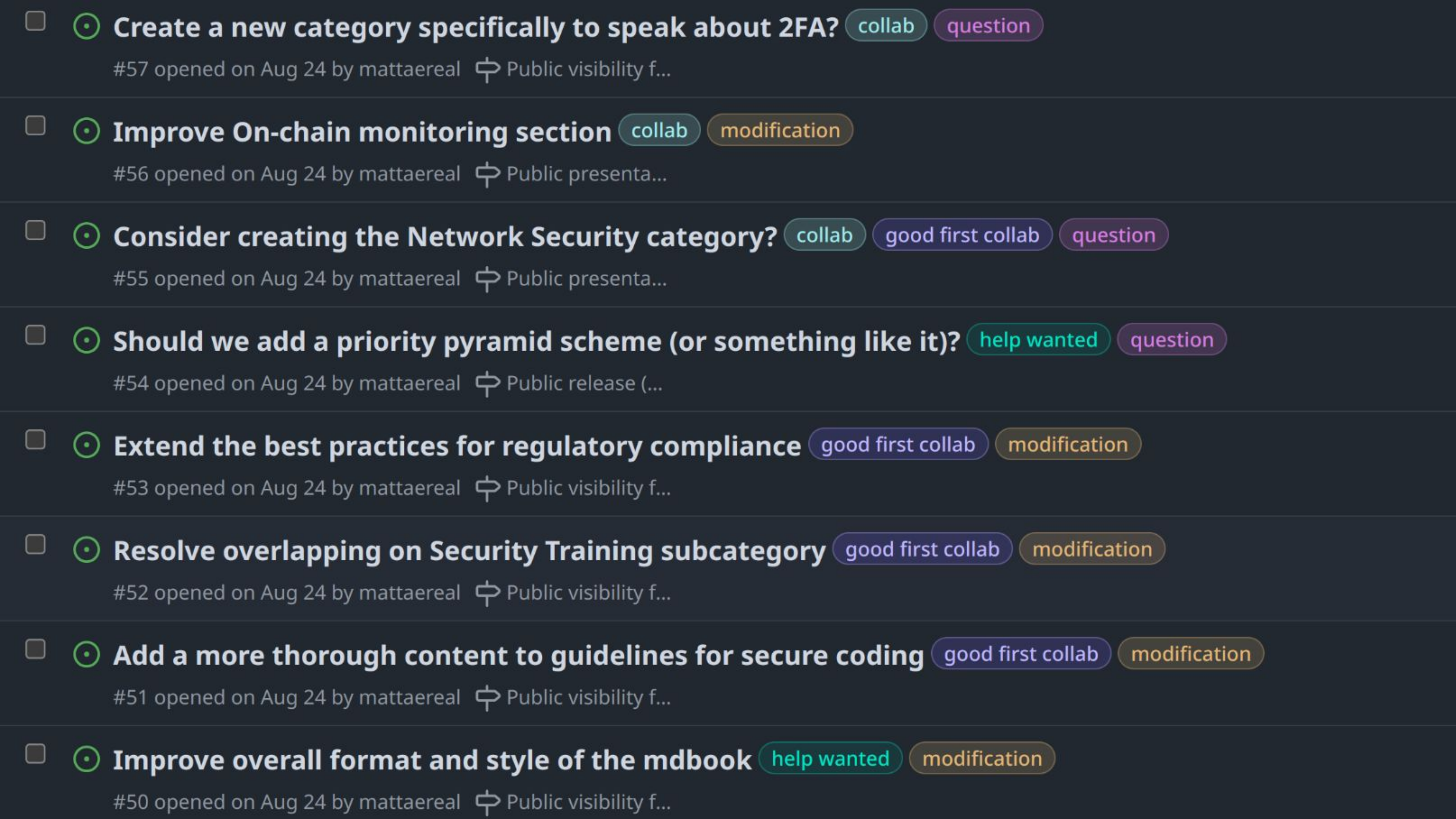
□ ○ **Should we consider adding web3 vulnerabilities classification?** collab help wanted question
#69 opened on Sep 26 by mattaereal

□ ○ **Add and improve current tag names (DevOps, Cloud, Developer, Finance, etc)** good first collab
#68 opened on Sep 26 by mattaereal

□ ○ **Consdier adding an AI chatbot, trained with frameworks, to provide suggestions** collab help wanted local setup
#62 opened on Sep 21 by mattaereal

□ ○ **Do something about Telegram's sections (possible overlap)** modification
#60 opened on Sep 21 by mattaereal Public presenta...

□ ○ **Add a section about the possibility to comment on the live vercel deployment inside the contribution page** good first collab local setup



□ ⊙ **Create a new category specifically to speak about 2FA?** collab question
#57 opened on Aug 24 by mattaereal Public visibility f...

□ ⊙ **Improve On-chain monitoring section** collab modification
#56 opened on Aug 24 by mattaereal Public presenta...

□ ⊙ **Consider creating the Network Security category?** collab good first collab question
#55 opened on Aug 24 by mattaereal Public presenta...

□ ⊙ **Should we add a priority pyramid scheme (or something like it)?** help wanted question
#54 opened on Aug 24 by mattaereal Public release (...

□ ⊙ **Extend the best practices for regulatory compliance** good first collab modification
#53 opened on Aug 24 by mattaereal Public visibility f...

□ ⊙ **Resolve overlapping on Security Training subcategory** good first collab modification
#52 opened on Aug 24 by mattaereal Public visibility f...

□ ⊙ **Add a more thorough content to guidelines for secure coding** good first collab modification
#51 opened on Aug 24 by mattaereal Public visibility f...

□ ⊙ **Improve overall format and style of the mdbook** help wanted modification
#50 opened on Aug 24 by mattaereal Public visibility f...

Why?

- A **shift on our perspective** is imminent
- Don't negate **human nature**
- Build stuff **secure by default**
- **Less** mechanisms of **control**
- **More** mechanisms of **recovery**
- **We can't do this alone**

Security Rangers

Incentivizing Public Goods Security Work for the Ethereum Ecosystem

ethrangers.com

Ethereum Foundation (EF)
Secureum
The Red Guild