STANFORD
SECURITY
CLINIC

Stanford Security Clinic

Miles McCain and Aditya Saligrama

STANFORD
SECURITY
CLINIC

Miles McCain

Stanford ‘24, Apple, CISA, SIO

Aditya Saligrama

Stanford ‘24, Applied Cyber, ESRG

STANFORD
SECURITY
CLINIC

SSC ⇔Applied Cyber

Special thanks to...

Stanford Applied Cyber
Riana Pfefferkorn (Stanford Internet Observatory, Stanford Law)
Alex Keller (Stanford School of Engineering)

Public Interest Cybersecurity

- Stanford student startups don’t have a great security track record
- That’s a problem — embarrassing for them, unsafe for us
- Enter SSC: free 2-hour security reviews & active penetration tests

Alas, we’ve done this before

- We have a history of identifying security flaws in student startups
- One even threatened us with felony charges in order to keep us quiet!
- Better to be proactive — let’s have the startups come to us.

It’s been a busy quarter!

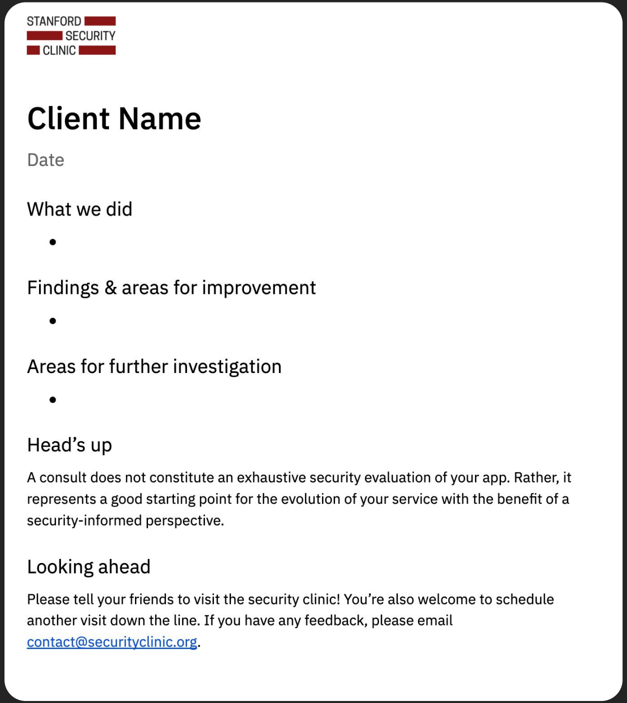
STANFORD SECURITY CLINIC

- The clinic was fully subscribed for the fall quarter.
- We identified critical security flaws in every *student* startup we met with.
- Three main kinds of startups we saw:
  - Ed tech
  - Bio tech
  - AI infrastructure

A typical visit to the clinic

STANFORD SECURITY CLINIC

1. Client fills out ‘intake worksheet’ ahead of time
2. Application walkthrough
3. Threat modeling
4. Infrastructure review
5. Active penetration test
6. Debrief + share a write up



STANFORD SECURITY CLINIC

Client Name

Date

What we did

•

Findings & areas for improvement

•

Areas for further investigation

•

Head’s up

A consult does not constitute an exhaustive security evaluation of your app. Rather, it represents a good starting point for the evolution of your service with the benefit of a security-informed perspective.

Looking ahead

Please tell your friends to visit the security clinic! You’re also welcome to schedule another visit down the line. If you have any feedback, please email contact@securityclinic.org.

Some vulnerabilities we caught

STANFORD SECURITY CLINIC

- Client-side-only access control
  - Get the admin dashboards…
- AWS access keys exposed in frontend
  - This was actively being exploited!
  - We led an incident response
- RCE through command injection

Shaurya, after we identified a critical security vulnerability in his app. Happy client!

Looking ahead

- Berkeley runs the Consortium of Cybersecurity Clinics
  - Provides shared resources and trainings
  - We are exploring joining the Consortium
- Securing the future of the clinic with Applied Cyber & mentorship
  - We are both seniors, give or take
  - How do we ensure the clinic is here to stay? By bringing in others!
- More clients next quarter!

The Consortium of
Cybersecurity Clinics

STANFORD SECURITY CLINIC

Q&A