Enumerates threats to a website (or to anyone who visits it)

narrow & deep search in a site.

interaction beyond the front page. any changes during the session.

want to use normal browser. - Full power, human driven.

some way to replicate → ~~Auto~~ Automated analysis.

Behaviour driven new experience.

what threats? — continue

Client & server side.

↳ Send only to client

How it sets up the dom? → XSS?

what scripts.

what is sent & received?

↳ HTTP, Forms being tampered with.

Finding ways what we are doing could

Forms → CSRF
Forms → Anti CSRF tokens.

Step 0 → script injection.

1 → login → HTTPS

↳ CSRF → Protection we can detect.

Filters for search & who to look for.

who are worried about.

↳ who do we consider
- → MITM
- → Eavesdropper?
- → SSL stripper.

Looking at servers, 3rd party, who

↳ • web attacker

Another tab in browser

Self attacker
- • Self XSS
- •

distinguishing between these.

Targets:

Benevolent or helping a protester.

• e.g. is the user input in a form where you can see anywhere else.

↓ limited machine [illegible] permission

control between each other.

[illegible]?

• what damage could you be doing?

• lesser enforcement of privacy practices.

Threats

HTTP?

HTTPS? → can I

HSTS? — why not.

↳ header.

Benchmarks & Testing

Loading a scripts over HTTP → hash of a script to check validity

forms → Protections against CSRF embedded outputs.

cookies → flags? → Not accessing a HTTP cookie?

→ why?

→ what's

Same site cookies flag

↳ Only used in 1st party position.

headers → X-Xss protection. → Flag for usage.

JS usage → Instrument for specific things being seen.

eval being used → Reflected on the site

Remote inclusions, dependencies, iframes → dos, clickjacking.

X-Frame options.

CSP & sandboxing policies. → Recommendation.

↳ You could be using this → inline scripts → scribot.

extension? Dump the trace somewhere that produce report.