

who are worried abt.

Filters for search & who  
to look for

↳ who do we consider & MITM  
• eavesdropper?  
• SSL stripper

3rd party  
looking at servers, who

↳ web attacker.

Another tab in browser

Self attacker → Self XSS

Distinguishing between these.

Targets:

Benevolent or helping a pentester.

es. is the user  
input in a form  
where you can  
see anywhere  
else.

↓  
What headers  
are you using

control between  
each other.

cookies?

↳ What headers should you be  
using?

↳ Good reinforcement of  
being good practices.

by 'Specialists' 2.  
looking

... ..  
... .. why not  
... ..

... ..  
... ..  
... ..

frames

... ..  
... ..

cookies

... ..  
... ..

... ..  
... ..  
... ..  
... ..

same site cookies flag

... ..

headers

... ..  
... ..

JS usage

... ..  
... ..

Remote inclusions,  
dependencies, iframes

... ..  
... ..

CSP & sandboxing policies. → Recommendation.

... ..

extension? Dump the trace somewhere then produce report.