

Web Security

Adrianna Holden-Gouveia

Website: aholdengouveia.name

🌀: [aholdengouveia](#)

🐦: [aholdengouveia](#)

Accessibility Notice

This document is also available in HTML format at:

Link: <https://aholdengouveia.name/InfoSec/labs/websecurity.html>

The HTML version provides enhanced accessibility features including keyboard navigation, screen reader support, responsive design, dark mode support, and high contrast options.

Learning Outcomes

By the end of this lab, you will be able to:

- Explain how two common website attacks work, and how website owners can prevent them
- Test how easy your browser is to track, and compare ways to reduce tracking
- Explain what a website's certificate shows, and what browser certificate warnings mean
- Recommend ways people can protect themselves on the web

Lab Instructions

Everything in this lab runs in your web browser, so you don't need to install anything. All the tools are linked under Resources.

You don't need to know how to code. Hacksplaining walks you through each step, and explains what's happening as you go.

Only practice attacks on sites made for practice, like Hacksplaining. Trying an attack on a real website without permission is illegal, even just to see if it works.

Screenshots

This lab asks for 7 screenshots. Each screenshot should have your name, term, and year. One of the easiest ways to do that is make a text document with your name and term/year on your computer and save it to use all term. Any screenshots that don't include this information won't be counted.

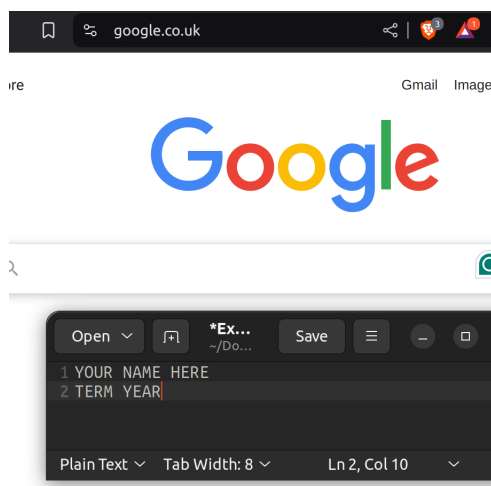


Figure 1: This is an image of what each of your screenshots should look like

Part 1: Attack a Practice Website

Hacksplaining has short lessons where you attack a pretend website it runs, then learn how to fix it. Sign up for a free account. You can use your school email.

Pick **two** of these lessons:

- SQL Injection
- Cross-site Scripting (reflected or stored)
- Password Mismanagement
- SSL Stripping
- Clickjacking

For each lesson:

1. Finish the lesson and its quiz. Take a screenshot of the end of the lesson, showing it's complete.
2. In your own words, explain how the attack works, as if you were telling a friend who doesn't work in IT.
3. What could an attacker get or do with this attack? Who gets hurt: the website, its users, or both?
4. How can the website's owner prevent it?

Part 2: How Trackable Is Your Browser?

EFF's Cover Your Tracks tests how websites and advertisers see your browser, and how unique it looks. No account is needed.

5. Run the test in the browser you use most. Take a screenshot of the results.
6. Run it again with a different setup, such as a private window, a different browser, or your phone. Take a screenshot of the results.
7. For each test, write down the browser and setup you used, whether it blocked tracking ads and invisible trackers, and whether your fingerprint was unique.
8. What changed between the two tests? Which setup protected you better?
9. Pick one thing the results showed about your browser, such as your screen size, time zone, or fonts. Why would a tracker want to know this?

Part 3: Certificates and Browser Warnings

Every HTTPS website has a certificate, which proves the website is who it says it is.

10. Pick 2 websites you use often. Select the padlock (or the icon next to the address), and find the certificate. Take a screenshot of each one.

11. For each website, write down who issued the certificate, when it starts and expires, and how many days it lasts. A calendar or a date calculator website is fine for counting days.
 12. Were the two certificates from the same issuer? Did they last the same length of time? Why do you think certificates are getting shorter?
- badssl.com is a website made for testing. It has pages with broken certificates on purpose, so you can see the warnings safely. Visit each of these pages, and **don't** click through the warnings:
- <https://expired.badssl.com>
 - <https://self-signed.badssl.com>
 - <https://wrong.host.badssl.com>
 - <https://untrusted-root.badssl.com>
13. Take a screenshot of one of the warnings.
 14. For each page, explain in your own words what's wrong with the certificate, and why your browser warned you.
 15. If you saw a warning like this on your bank's website, what would you do? Why?

Part 4: Your Advice

16. Based on this lab, write 3 tips to help a friend or family member stay safer on the web. For each tip, explain which part of the lab it came from.

Deliverables

One file that includes:

- Part 1: your 2 Hacksplaining screenshots, and your answers for each lesson
- Part 2: your 2 Cover Your Tracks screenshots, and your answers
- Part 3: your 2 certificate screenshots, your badssl.com warning screenshot, and your answers
- Part 4: your 3 tips

Resources

References, a video, a PowerPoint and some notes are available at my website
Link: <https://www.aholdengouveia.name/InfoSec/WebSecurity.html>

Hacksplaining lessons, for Part 1 Link: <https://www.hacksplaining.com/lessons>

EFF's Cover Your Tracks, for Part 2 Link: <https://coveryourtracks.eff.org/>

badssl.com, for Part 3 Link: <https://badssl.com/>

What HTTPS and certificates are Link: <https://en.wikipedia.org/wiki/HTTPS>

The OWASP Top 10 web application security risks Link: <https://owasp.org/www-project-top-ten/>