Hacksplaing

## Summary

<https://hacksplaining.com> provides interactive labs for the most common web application attacks. The OWASP top ten attacks are highlighted but additional lessons are available.

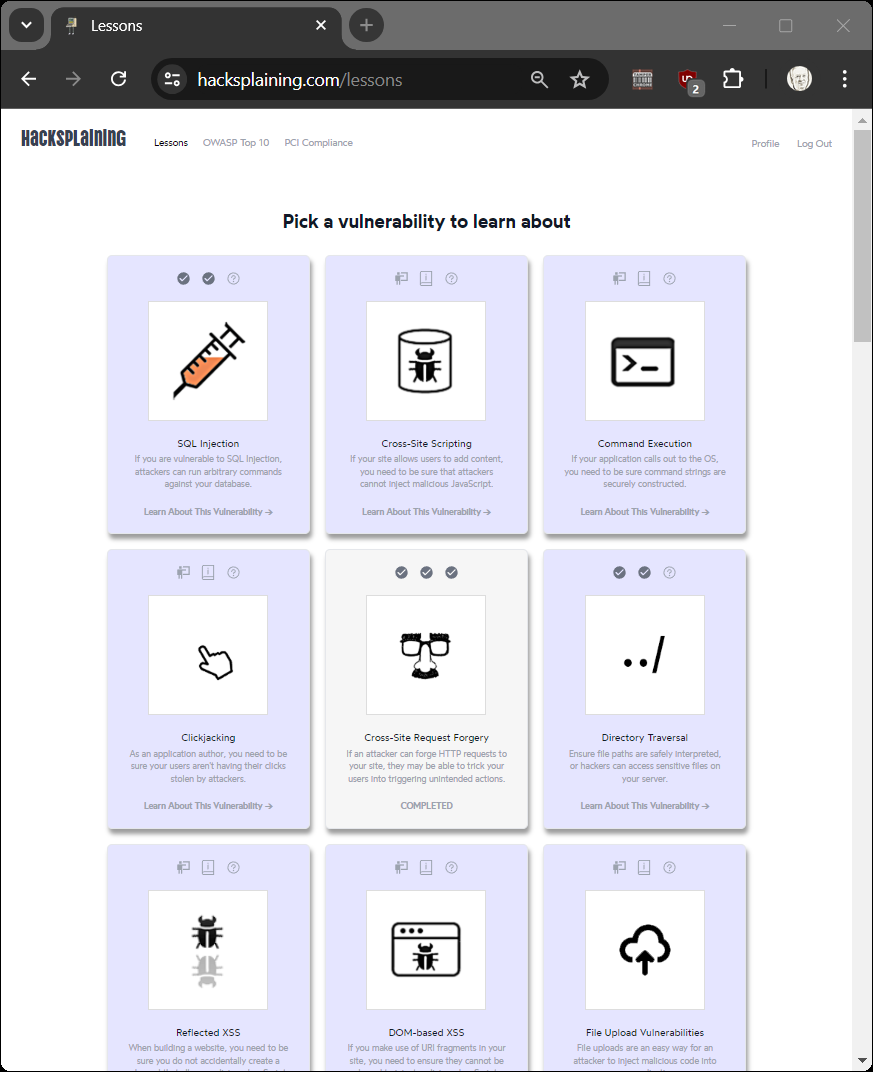
You should create a free account to get the most value out of this site.

## Tools/Resources

Browser

## Walkthrough

1. Show the full set of lessons available

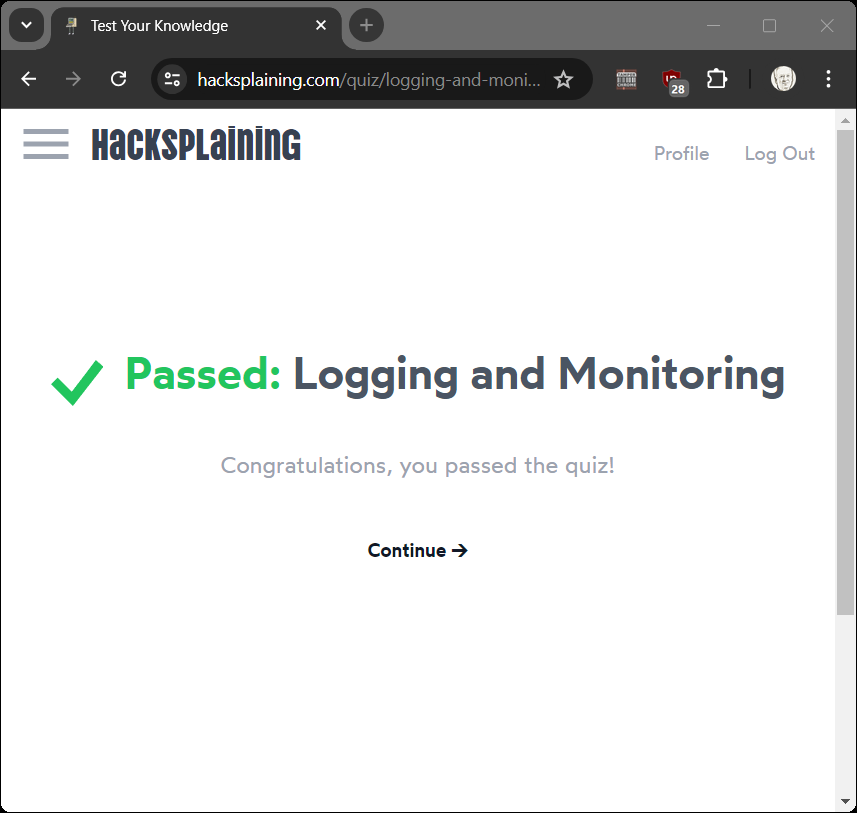


1. Show the OWASP top 10. [link](https://owasp.org/www-project-top-ten/)
2. Hacksplaining provides 18 lessons for 9 of the [OWASP 10](https://hacksplaining.com/owasp). Select 5 lessons to demonstrate to the class.
3. Discuss the levels of Prevalence, Exploitability, and Impact
4. Discuss code examples
5. Show the quiz

## Submission

Upload to Canvas a docx or pdf containing screenshots showing you passed quizzes in 5 lessons.

They will look something like this:



## Additional Thoughts

Do I need to do every lesson? For your personal growth yes. In the past this class required all lessons. The lessons do not take that long, just do it!

Do any exploits rank high for Prevalence (common), Exploitability (easy), and Impact (devastating)?