✓ Via what technique(s) might a malicious actor "crack" software (that is, bypass registration/payment to use it)? 1/1

Keygen, Reverse Engineering, Patch, Software Protection Bypass

✓ Distinguish the nature of two types of "cross-site" attacks we discussed: cross-site scripting (XSS) and cross-site request forgeries (CSRF). 1/1

cross-site Request forgeries(CSRF) and cross-site scripting(XSS) are two different web security vulnerabilities types. CSRF attacks use the website's trust in the user's browser to trick them into doing unwanted actions on a website where they are authenticated and on the other way we have XSS attacks. in this attack malicious scripts injects into webpage through XSS attacks, which can result in Data manipulation or theft when they run in other users browser. very shortly the XSS attacks the web application's users and CSRF targets the web application itself by tampering with authenticated user actions.

✓ Why do we need to *escape* certain characters in inputs? 1/1

its critical for web security and data integrity to escape characters in user inputs.it protects injection attacks like SQL injection and CSRF by treating special characters as literal text rather than as part of executable code or queries. Escaping characters is a standard practice in programming. It helps make code more secure and understandable. and it can cause issues in processing inputs. Escaping them guarantees that inputs are handled correctly.

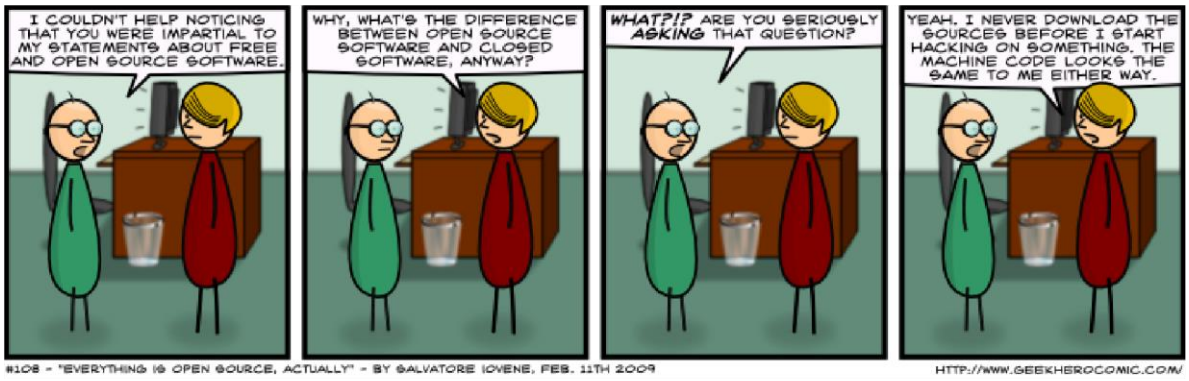
✓ In the context of SQL, what is a *prepared statement*? 1/1

A ready-made statement in SQL and a precompiled SQL query template that decouples SQL logic and data, improving security by preventing SQL injection attacks and repeatedly improving query execution performance ..

✓ Why is client-side validation considered "less secure", perhaps, than server-side validation? 1/1

Because user can change or circumvent it. Since the validation logic is located in the browser, the user with sufficient technical knowledge can change it or even disable it, this allows invalid or malicious data to be sent to the server. On the other hand, server-side validation happens on the server and the user cannot change it, and as a result, data validation becomes stronger and safer.

GeekHero Comic



✓ Pragmatically, the above comic may be correct as it pertains to the behavior of most *users* towards open-source software. Even if that is your attitude towards it, why might it still be a good thing to consider using more open-source software (or, developing it), from a security-minded perspective? 1/1

The use and development of open source software can improve security by allowing people to inspect and improve the code. An improvement that leads to the rapid identification and correction of vulnerabilities. The ability to customize and adapt software gives users more control over their security posture while avoiding security traps through the ambiguities that closed source software may rely on. Therefore, open source often leads to more secure and reliable software.

✓ How are package managers similar to app stores (such as Apple's App Store, Google Play Store, Microsoft Store, etc.), from a cybersecurity perspective? 1/1

They are similar in that they both act as centralized repositories for software distribution. and allows for standardized review processes for the software they distribute. They generally ensure that packaged applications are checked for malicious code before release, which helps prevent the spread of malware. Both have automatic update mechanisms that fix security vulnerabilities when they are discovered.

✓ What threat does use of Content-Security-Policy fields in our source code help to defend against? 1/1

Helps prevent XSS and other types of injection attacks. It also Helps prevent XSS and other attacks.

✓ Provide a specific example of a situation when you might want to use the HTTP POST method instead of the HTTP GET method. 1/1

Password through a login form :)

Heartbleed Logo

✓ More precisely known as CVE-2014-0160 but better known as Heartbleed, the discovery of this exploit caused quite an internet panic in 2014, resulting in one of the first times a bug was actively publicized in mass media outlets, as cybersecurity researchers scrambled to make the public aware of the bug and to encourage rapid download of the fix. 1/1

Read up on Heartbleed either via the Wikipedia article linked in the previous paragraph, or via any other research you like (such as this video).

Why was Heartbleed such a threat to a user's security?

Because the breach in the OpenSSL implementation uses the TLS heartbeat extension and allows an attacker to read memory from affected servers. done in an undetectable manner and leaves no traces behind, this makes it difficult to determine the amount of information that may be at risk. Since OpenSSL is widely used to secure internet connection. A large portion of the web was affected, prompting urgent calls for renewed certificates and user caution.

Feedback

How did you find the difficulty of this assignment? *

	1	2	3	4	5	
Too easy	○	○	○	◉	○	Too hard

About how many MINUTES would you say you spent on this assignment? *

Just to set expectations for future students.

30