Feedback — week 3 quiz

Help

You submitted this quiz on **Thu 13 Nov 2014 11:21 AM PST**. You got a score of **34.00** out of **42.00**. You can attempt again, if you'd like.

Question 1

What is one difference between an HTTP GET and an HTTP POST request?

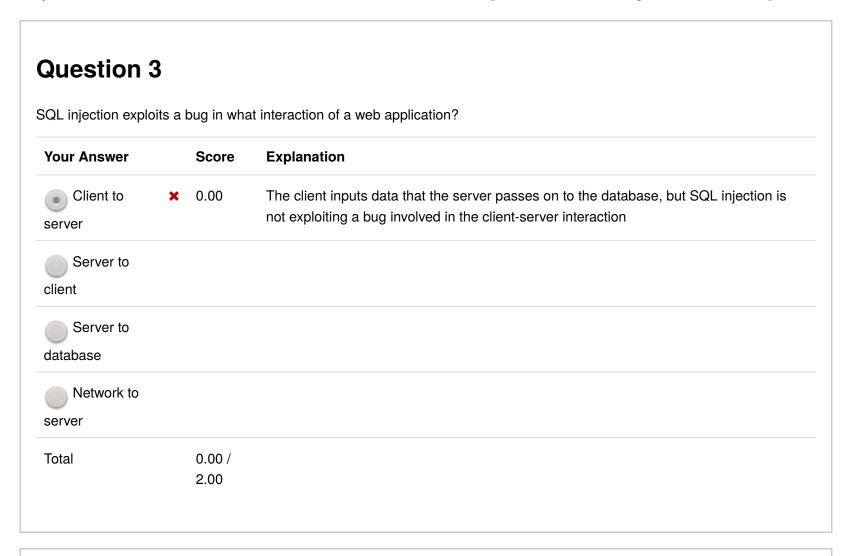
Your Answer		Score	Explanation
Only GET requests are subject to the same-origin policy			
Only POST requests may include parameter data in the request body	~	2.00	POST requests are often issued for web forms whose content is included in the request data
Only GET requests use the REFERER header			
Only POST requests can encode parameters in the URL			

1 of 15

Total	2.00 /	
	2.00	

Which of the following is true about static and dynamic web content?

	Score	Explanation
~	1.00	Dynamic content is regenerated with each request, often including database-resident content
	1.00 / 1.00	
	•	1.00 /

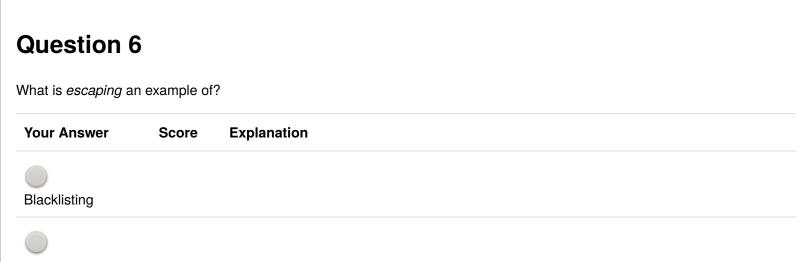


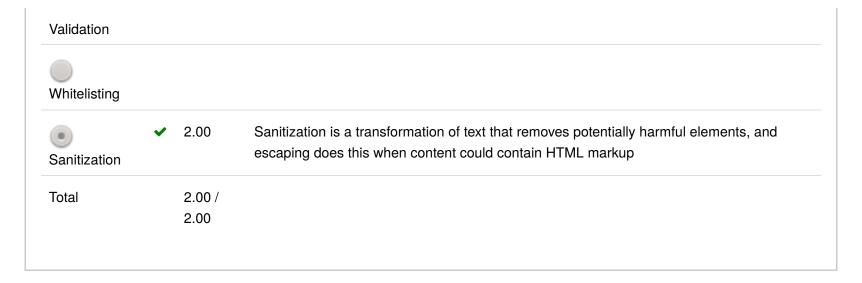
our Answer		Score	Explanation
Access information he			
houldn't			
Overrun a buffer to			
smash the stack			
Cause memory to be			
used after it's freed			
All of the above	×	0.00	Stack smashing and use-after-free bugs are not related to SQL injection,
			which is a bug in how a SQL command is constructed
- Total		0.00 /	
		2.00	

If you had to summarize the key programming failure with SQL injection, it would be:

Your Answer Score Explanation

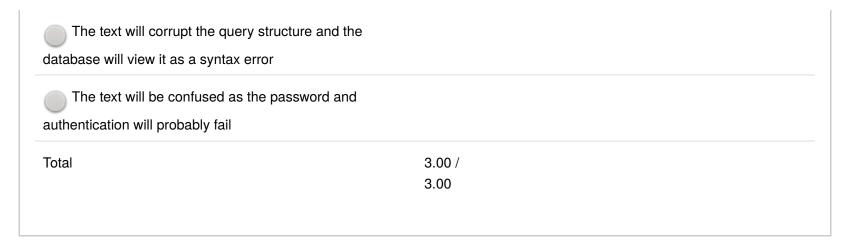






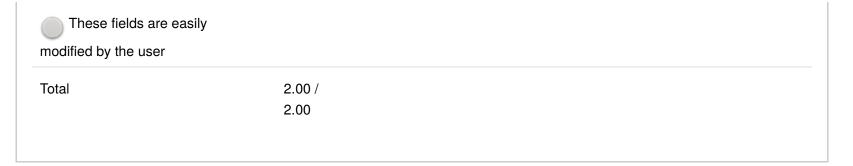
Suppose a web application implements authentication by constructing an SQL query from HTML form data using PHP's prepared statements. What would happen if an attacker entered FRANK' OR 1=1; -- in the web form's user field?

Your Answer	Score	Explanation
The text will modify the structure of the SQL query and possibly bypass authentication		
The application will try to authenticate a user whose name is FRANK' OR 1=1;	✓ 3.00	The text that is entered will be treated as data, and not confused as code



Why is it undesirable to implement session identifiers using (only) hidden form fields?

Your Answer	Score	Explanation
Such fields cannot contain		
binary data		
Such fields cannot include		
timeout information		
The session ID is forgotten	~ 2.00	This adds inconvenience to the user, since closing the window
when the browser window is		necessitates logging in again, and complicates the construction of the site
closed		to always pass around the hidden field



Suppose a browser submits a GET request to URL http://www.mybank.com/accountinfo on 20 February 2015. Which of the following cookies, if already stored at the browser, would be sent with the request?

Your Answer		Score	Explanation
<pre>lang=us-english; expires=Sat, 1-Aug-2015; path=/accountinfo/; domain=.fidelity.com</pre>	~	1.00	This cookie is not sent because the domain name does not match
<pre>prefs=small:blue:refresh; expires=Sat, 1-Aug-2015; path=/specialoffers/; domain=.mybank.com</pre>	•	1.00	This cookie is not sent because the path is not a prefix of the path given in the URL
edition=us; expires=Wed, 18-Feb-2015; path=/; domain=.mybank.com	×	0.00	This cookie is not sent because it has expired

sessid=ABCDEFG; expires=Sat, 21-Feb-2015; path=/; domain=.mybank.com	×	0.00	This cookie has not timed out, has a path that is a prefix of the given path, and references the proper domain suffix
Total		2.00 /	
		4.00	

Which of the following are ways that session cookies could be stolen or forged?

Your Answer		Score	Explanation
Compromising the browser or server	~	1.00	Injected code could exfiltrate cookies used for all users/sites
Predicting the cookie's structure and reconstructing it	~	1.00	Knowing how cookies are constructed, and knowing features of the user, site, etc. permits creation of the cookie
Copying them by keylogging	~	1.00	Session IDs are not entered by the user, but determined by the site
Reading it from an unencrypted web request	~	1.00	An adversary that can see web requests (e.g., in an Internet cafe) can steal cookies from those requests
Total		4.00 /	

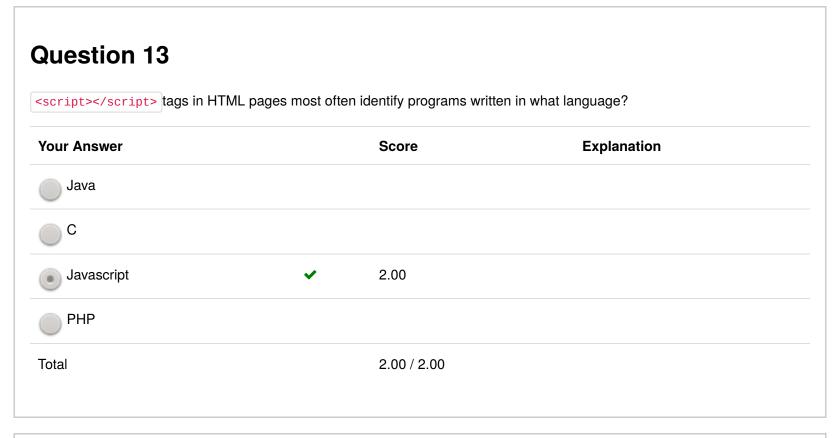
4.00

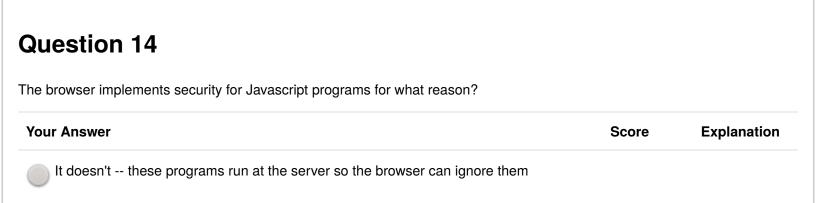
Question 11

Which of the following are ways to reduce the impact of a stolen cookies?

Your Answer		Score	Explanation
Changing a user's cookie from session to session	~	1.00	Per-session cookies, if stolen, cannot affect future sessions
Associate the cookie with the server's IP address	~	1.00	Associating a cookie with the client's IP address can help, despite false positives and false negatives, but associating it with the server's address would not
Prevent cookies from entering the DNS cache	~	1.00	Cookies don't go in the DNS cache, DNS addresses do
Giving each cookie a timeout	~	1.00	Timing out a cookie means it can only be misused for a limited period
Total		4.00 / 4.00	

ow can the referer field be used to defend a	gainst CSRF	attacks?
Your Answer	Score	Explanation
It enforces that sensitive requests		
are (only) initiated by interaction with a site's own pages		
It ensures that requests only come rom authenticated users	× 0.00	HTTP has nothing to do with user-level authentication (HTTPS authenticates a client with a server, but that has no impact on CSRF)
It can't be used reliably because it		
only works for dynamic content		
It can be used to check that a		
lavascript program is from the proper		
prigin		
Fotal	0.00 /	
	2.00	





Such programs may access browser-controlled resources, which include potentially sensitive data in HTML documents and cookies	•	3.00
It doesn't these programs are only used to render dynamic content but are otherwise not security-relevant		
Such programs could deny service by running forever		
Total		3.00 / 3.00

Question 15 XSS subverts what policy? Your Answer Score Explanation Secure defaults Availability Whitelisting Same Origin ✓ 3.00 XSS uploads a script from host A to site B, which serves the script with its privileges, thus violating the same origin policy

Total	3.00 /		
	3.00		

What is the difference between stored (or persistent) XSS and reflected XSS?

Your Answer		Score	Explanation
Stored XSS works by injecting code in a site's served content, while reflected XSS	~	3.00	
injects code in a URL			
Stored XSS is amenable to blacklisting but reflected XSS is not			
Stored XSS embeds Javascript in an a URL, while reflected XSS embeds it in a			
mirrored site			
Stored XSS works on database queries while reflected XSS works on cookies,			
which are received from and reflected back to the server			
Total		3.00 / 3.00	

https://class.coursera.org/softwaresec-001/quiz/feedback?subm...