Assignment 2

Due Jul 5 at 11:59pm	Points 100	Questions 10	Time Limit None	
-----------------------------	------------	--------------	-----------------	--

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	26 minutes	100 out of 100

Score for this quiz: 100 out of 100

Submitted Jun 15 at 4:43pm
This attempt took 26 minutes.

	Question 1	/ 10 pts
	Which of these is an example of a social engineering attack?	
Correct!	•	
	An attacker pretends to be an adminsirator of a website and gets you to message them your password.	
	An attacker gets JavaScript onto a web page that steals the user's passw	vord
	The attacker enumerates a list of usernames and passwords from public	data

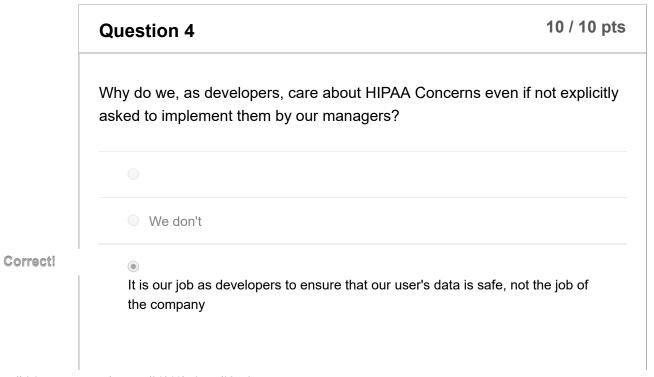
Question 2 10 / 10 pts

What does HTTPS allow for?

Correct!

•	Secure end-to-end encryption
	Digital Ocean
	Redis
	Hypertext Transfer Secure

	Question 3	10 / 10 pts
Correct!	Attackers cannot easily brute-force hashes for bcrypt	
	MD5 is slower to compute than bcrypt, making it infeasible	
	Microsoft does not support MD5 usage	



Because we don't want our data to be data mined

	Question 5 10 / 10 pts
	How do we avoid XSS attacks?
Correct!	By allowing only a whitelisted set of HTML tags and attributes to come from user input
	By manually blacklisting malicious HTML tags
	By stripping SQL strings the user provides

	Question 6 10 / 10 pt	S
	How do we avoid CSRF attacks?	
	By checking the HTTP referer header	
Correct!	By having our server generate 1 time tokens that verify the user is submitting data from the real form	
	By using bcrypt	
	We cannot	

How can we avoid DDOS attacks, 100% of the time? By hosting our website in the cloud By using Cloudflare We cannot; we can mitigate damage, but not avoid it entirely.

Why is username enumeration dangerous? It allows attackers to insert XSS attacks on your website It allows attackers to easily come up with an attack vector to brute force passwords. It allows for easier buffer overflow attacks

	Question 9	10 / 10 pts
	How can some buffer overflow attacks be prevented?	
Correct!	Never manually manipulating memory	

By using strongly typed programming languages
By using a SQL Database
By using loosely typed programming languages

	Question 10	10 / 10 pts
	How do we prevent IDOR issues?	
Correct!	You must implement an access control for all relevant data	
	Never use GUIDs	
	Stalling requests when the user traverses multiple ids	

Quiz Score: 100 out of 100