Assignment 8

Started: Apr 15 at 5:41am

Quiz Instructions

Question 1 — 10 pts

Which of these is an example of a social engineering attack?

- (●) 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 password
- ( ) The attacker enumerates a list of usernames and passwords from public data
- ( )

Question 2 — 10 pts

What does HTTPS allow for?

- (●) Secure end-to-end encryption
- ( ) Digital Ocean
- ( ) Hypertext Transfer Secure
- ( )

Question 3 — 10 pts

Why would you use bcrypt over MD5 for hashing passwords?

- (●) Attackers cannot easily brute-force hashes for bcrypt
- ( ) MD5 is slower to compute than bcrypt, making it infeasible
- ( ) Microsoft does not support MD5 usage
- ( )

Question 4 — 10 pts

Why do we, as developers, care about HIPAA Concerns even if not explicitly asked to implement them by our managers?

- (●) It is our job as developers to ensure that our user's data is safe, not the job of the company
- ( ) We don't
- ( ) Because we don't want our data to be data mined
- ( )

Question 5 — 10 pts

How do we avoid XSS attacks?

- (●) By allowing only a whitelisted set of HTML tags and attributes to come from user input
- ( ) By stripping SQL strings the user provides
- ( ) By manually blacklisting malicious HTML tags

- ( )

Question 6 — 10 pts

How do we avoid CSRF attacks?

- (•) By having our server generate 1 time tokens that verify the user is submitting data from the real form
- ( ) We cannot
- ( ) By checking the HTTP referer header
- ( )

Question 7 — 10 pts

How can we avoid DDOS attacks, 100% of the time?

- (•) We cannot; we can mitigate damage, but not avoid it entirely.
- ( ) By hosting our website in the cloud
- ( ) By using Cloudflare
- ( )

Question 8 — 10 pts

Why is username enumeration dangerous?

- (●) It allows attackers to easily come up with an attack vector to brute force passwords.
- ( ) It allows attackers to insert XSS attacks on your website
- ( ) It allows for easier buffer overflow attacks
- ( )

Question 9 — 10 pts

How can buffer overflow attacks be prevented?

- (●) Never manually manipulating memory
- ( ) By using strongly typed programming languages
- ( ) By using loosely typed programming languages
- ( )

Question 10 — 10 pts

How do we prevent IDOR issues?

- (●) You must implement an access control for all relevant data
- ( ) Never use GUIDs
- ( ) Stalling requests when the user traverses multiple ids
- ( )

No new data to save. Last checked at 12:49am Submit Quiz