Quiz su PHP, Cookie e Sicurezza Web

Informazioni generali

- Quiz da 40 domande a risposta multipla
- Tempo consigliato: 60 minuti
- La risposta corretta è indicata con un asterisco (*)

---

1. Quale tag è corretto per iniziare e terminare un blocco di codice PHP?

A) `<php> ... </php>` B) `<script language="php"> ... </script>` C) `<?php ... ?>` D) `<p> ... </p>`

2. Quale operatore viene utilizzato in PHP per concatenare stringhe?

A) `+` B) `.` C) `&` D) `:`

3. Quale funzione in PHP restituisce la lunghezza di una stringa?

A) `count()` B) `length()` C) *`strlen()`* D) `sizeof()`

4. Cosa sono i cookie HTTP?

A) Script di programmazione lato server B) *Piccoli file di testo memorizzati dal browser sul computer dell'utente* C) Funzioni speciali di JavaScript D) Protocolli di comunicazione

5. Qual è il modo corretto per iniziare una sessione in PHP?

A) `begin_session()` B) *`session_start()`* C) `$_SESSION = new Session()` D) `session_create()`

6. Come si dichiara una variabile in PHP?

A) `var x = 5;` B) `dim x as integer = 5;` C) `x = 5;` D) *`$x = 5;`*

7. Quale attributo del cookie impedisce l'accesso tramite JavaScript?

A) Secure B) SameSite C) *HttpOnly* D) Path

8. Quale funzione PHP è utilizzata per stabilire un cookie?

A) `make_cookie()` B) *`setcookie()`* C) `create_cookie()` D) `cookie_set()`

9. Quale attacco si verifica quando un malintenzionato ruba un cookie di sessione per impersonare un utente?

A) Cross-Site Scripting B) *Session Hijacking* C) SQL Injection D) Session Poisoning

10. In PHP, quale superglobale contiene i dati dei cookie?

A) `$_COOKIES` B) *`$_COOKIE`* C) `$COOKIES` D) `$GLOBALS['cookies']`

11. Quale funzione PHP è utilizzata per verificare se una variabile è definita e non è NULL?

A) `is_defined()` B) `is_set()` C) *`isset()`* D) `defined()`

12. Quale metodo HTTP è più sicuro per l'invio di dati sensibili?

A) GET B) *POST* C) Entrambi sono ugualmente sicuri D) HEAD

13. Come si imposta correttamente la scadenza di un cookie?

A) `setcookie("test", "value", "expire=tomorrow");` B) *`setcookie("test", "value", time() + 3600);`* C) `setcookie("test", "value", "3600");` D) `setcookie("test", "value", expiry(3600));`

14. Quale attributo del cookie garantisce che il cookie venga trasmesso solo su HTTPS?

A) *Secure* B) HttpOnly C) SameSite D) SSL

15. Quale funzione PHP viene utilizzata per generare un hash sicuro delle password?

A) `md5()` B) `sha1()` C) *`password_hash()`* D) `hash()`

16. In un attacco CSRF (Cross-Site Request Forgery), cosa viene sfruttato dall'attaccante?

A) Password deboli B) *Cookie di autenticazione già presenti nel browser dell'utente* C) Vulnerabilità nel linguaggio PHP D) Mancanza di crittografia

17. Quale funzione PHP è utilizzata per sanitizzare l'output HTML?

A) `clean_html()` B) `sanitize_output()` C) *`htmlspecialchars()`* D) `html_purify()`

18. Come si può verificare se un form è stato inviato usando POST in PHP?

A) `if (form_submitted() == "POST")` B) `if (isset($_POST))` C) *`if ($_SERVER["REQUEST_METHOD"] == "POST")`* D) `if ($_POST == true)`

19. Quale superglobale contiene le variabili della sessione in PHP?

A) `$_GLOBALS` B) *`$_SESSION`* C) `$_SERVER` D) `$_VARS`

20. Il Cookie Poisoning consiste in:

A) L'iniezione di codice SQL tramite cookie B) *La modifica non autorizzata dei valori dei cookie* C) La creazione di cookie falsi sul browser dell'utente D) L'eliminazione di cookie legittimi

21. Quale funzione PHP viene utilizzata per includere il contenuto di un altro file?

A) `import()` B) *`include()`* C) `require_file()` D) `insert()`

22. Come si dichiara un array associativo in PHP?

A) `array("mela", "banana", "arancia")` B) *`array("frutto" => "mela", "colore" => "rosso")`* C) `Array frutta = new Array()` D) `$frutta = ["mela"; "banana"; "arancia"]`

23. Quale tecnica è utilizzata per verificare che un cookie non sia stato manomesso?

A) Base64 encoding B) URL encoding C) *Firma digitale (ad es. HMAC)* D) Compressione dati

24. Quale funzione PHP è utilizzata per rigenerare l'ID di sessione?

A) `session_create_id()` B) *`session_regenerate_id()`* C) `session_new_id()` D) `session_refresh()`

25. Quale attacco sfrutta la mancanza di validazione dell'input per inserire script malevoli in una pagina web?

A) *Cross-Site Scripting (XSS)* B) Man-in-the-Middle C) Cookie Poisoning D) Brute Force

26. Come si può proteggere da attacchi SQL Injection in PHP?

A) Utilizzando solo database MySQL B) *Utilizzando prepared statements o statement parametrizzati* C) Eseguendo il backup regolare del database D) Limitando il numero di query al database

27. Qual è lo scopo principale dell'attributo SameSite dei cookie?

A) Limitare la dimensione del cookie B) Crittografare il contenuto del cookie C) *Impedire l'invio di cookie in richieste cross-site* D) Estendere la durata del cookie

28. Quale istruzione PHP è utilizzata per gestire gli errori in un blocco di codice?

A) `on_error` B) *`try...catch`* C) `handle_error` D) `error_check`

29. In un attacco di Session Fixation, cosa fa l'attaccante?

A) Forza la disconnessione di tutti gli utenti B) *Impone un ID sessione noto all'utente prima dell'autenticazione* C) Modifica i dati di sessione dell'utente D) Ruba il cookie di sessione tramite JavaScript

30. Quale funzione PHP è utilizzata per connettersi a un database MySQL?

A) `mysql_open()` B) *`mysqli_connect()`* C) `db_connect()` D) `pdo_mysql()`

31. Come si può evitare l'esecuzione di script PHP in una directory specifica?

A) Rinominando i file .php in .txt B) *Aggiungendo "php_flag engine off" nel file .htaccess* C) Rimuovendo i permessi di esecuzione dai file PHP D) Aggiungendo un commento all'inizio di ogni file PHP

32. Quale prefisso di cookie offre la maggiore protezione contro il Cookie Tossing?

A) __Secure- B) __*Host*- C) __Protected- D) __Safe-

33. Qual è il modo migliore per memorizzare password in PHP?

A) Utilizzando MD5 B) Memorizzandole in testo chiaro in un database sicuro C) *Utilizzando password_hash() con un algoritmo sicuro come bcrypt o Argon2* D) Utilizzando SHA-1 con un salt

34. Qual è la funzione della direttiva Content-Security-Policy nella protezione contro XSS?

A) Crittografa i cookie B) *Limita le fonti da cui può essere caricato il contenuto* C) Verifica l'integrità dei cookie D) Gestisce la durata delle sessioni

35. Quale modalità PHP è considerata la più sicura per l'inclusione di file?

A) `include()` B) `include_once()` C) `require()` D) *`require_once()`*

36. L'attacco Cookie Tossing sfrutta:

A) Un errore nel protocollo HTTP B) Una vulnerabilità nel linguaggio JavaScript C) *Il comportamento gerarchico dei domini nei cookie* D) Un bug nei browser moderni

37. Come si può limitare l'accesso a un file PHP a utenti specifici?

A) Utilizzando CSS avanzato B) *Implementando un sistema di autenticazione e controllo accessi* C) Rinominando il file con estensione nascosta D) Utilizzando solo query GET

38. Quale meccanismo può prevenire un attacco Replay sui cookie?

A) *Utilizzo di nonce o timestamp nel cookie* B) Memorizzazione di tutti i cookie in un database C) Disabilitazione dei cookie di terze parti D) Rimozione dell'attributo Path

39. Come si può correttamente ottenere un valore da un form POST in PHP?

A) `$name = POST['name'];`

B) `$name = form.elements['name'];`

C) *`$name = $_POST['name'];`*

D) `$name = Request.Form('name');`

40. Quale attributo PHP è necessario impostare per accettare sessioni solo da cookie (non da URL)?

A) session.use_cookies B) *session.use_only_cookies* C) session.cookie_only D) session.no_url_id