**CÂU HỎI ÔN TẬP**

***Môn: Công nghệ Web an toàn***

**Câu 1:** Biện pháp phòng chống tấn công SQL Injection trong giai đoạn lập trình (Development)

A. Sử dụng câu truy vấn tham số hóa (Parameterized Queries), Validation dữ liệu đầu vào, Lọc dữ liệu đầu vào (Filtering)

B. Lọc làm sạch dữ liệu (Sanitization), Sử dụng câu truy vấn tham số hóa (Parameterized Queries), Validation dữ liệu đầu vào, Lọc dữ liệu đầu vào (Filtering)

C. Lọc làm sạch dữ liệu (Sanitization), Sử dụng câu truy vấn tham số hóa (Parameterized Queries)

D. Lọc làm sạch dữ liệu (Sanitization), Sử dụng câu truy vấn tham số hóa (Parameterized Queries), Validation dữ liệu đầu vào

**Câu 2 - TL:** Xây dựng trang Đăng nhập (login.php):

A screenshot of a phone

Description automatically generated

Giả sử có cơ sở dữ liệu QUANLY\_NV có bảng lưu trữ dữ liệu của tài khoản người dùng: USER (ID,USERNAME, PASS, SALT), trong đó:

- ID: định danh duy nhất của người dùng

- USERNAME: tên đăng nhập của người dùng

- PASS: giá trị băm của mật khẩu người dùng với SALT (Sử dụng thuật toán SHA1)

- SALT: giá trị ngẫu nhiên cho mỗi người dùng

Tên đăng nhập trống (báo lỗi). Mật khẩu < 8 ký tự báo lỗi. Mật khẩu bao gồm < 2 nhóm kí tự (chữ hoa, chữ thường; chữ số và kí tự đặc biệt) báo lỗi.

Khi người dùng xác thực thành công sẽ hiển thị thông báo “Hello <tên\_đăng\_nhập>!” và lưu trạng thái xác thực của người dùng.

Áp dụng các cơ chế an toàn cho trang Đăng nhập.

**Câu 3:** Đâu là vị trí chính xác để chèn JavaScript?

A. Cả phần <head> và phần <body>

B. Phần <head>

C. Phần <body>

Câu 4: Hàm PHP nào chỉ loại bỏ tất cả các biến phiên?

A. session\_destroy();

B. isset\_session();

C. $\_SESSION=null;

D. session\_unset();

**Câu 5:** Theo OWASP TOP 10 năm 2021, hiểm họa nào được xếp hạng thứ 2:

A. Phá vỡ kiểm soát truy cập - Broken Access Control

B. Tiêm lệnh - Injection

C. Lỗi trong việc sử dụng mật mã - Cryptographic Failures

D. Cấu hình an toàn sai – Security Misconfiguration

**Câu 6:** Làm thế nào bạn có thể tạo một danh sách đánh số?

A. <ol>

B. <dl>

C. <ul>

D. <list>.

**Câu 7:** Lệnh HMTL chính xác để thêm màu nền là gì?

A. <background>yellow</background>

B. <body style=”background-color:yellow;”>

C. <body bg=”yellow”>

**Câu 8:** Theo OWASP TOP 10 năm 2021, hiểm họa nào được xếp hạng thứ 9?

A. Yêu cầu giả mạo phía máy chủ - Server-Side Request Forgery

B. Lỗi giám sát và ghi nhật ký an toàn – Security Logging and Monitoring Failures

C. Lỗi toàn vẹn dữ liệu và phần mềm - Software and Data Integrity Failures

D. Lỗi định danh và xác thực - Identification and Authentication Failures

**Câu 9:** Loại kiểm thử nào có độ phủ 100%?

A. Kiểm thử động (DAST = Dynamic AST)

B. Kiểm thử tương tác (IAST = Interactive AST)

C. Kiểm thử tĩnh (SAST = Static AST)

**Câu 10:** Chọn phát biểu SAI:

A. Wab service tương tác với người dùng thông qua các giao thức web

B. Web service tương tác qua các API (SOAP, RESTful)

C. Web service không cung cấp giao diện người dùng

D. Web servicce có thể là một phần (back-end) của một Web Application

**Câu 11:** Khi sử dụng phương thức POST, các biến được hiển thị trong URL

A. Sai

B. Đúng

**Câu 12:** Kết quả của việc mô hình hóa hiểm họa là:

A. Danh mục các hiểm họa và xếp hạng mức độ ưu tiên của các hiểm họa

B. Danh mục các hiểm họa và các cơ chế an toàn

C. Danh mục các hiểm họa và cách thức xử lý các hiểm họa

D. Danh mục các hiểm họa

**Câu 13:** Làm thế nào để tạo một mảng trong PHP?

A. $car = “Volvo”, “BMW”, “Toyota”;

B. $car = array[“Volvo”, “BMW”, “Toyota”];

C. $car = array(“Volvo”, “BMW”, “Toyota”);

**Câu 14:** Hình dưới đây mô tả tấn công nào?



A. CSRF – Cross-site Request Forgery

B. XSS – Cross Site Scripting

C. Injection

D. SSRF – Server-Side Request Forgery

**Câu 15:** Biện pháp phòng chống tấn công CSRF – Cross-site Request Forgery là:

A. Lọc dữ liệu đầu vào, kiểm thử

B. Lọc dữ liệu đầu vào, kiểm thử, người dùng không mở các đường link từ những nguồn không đáng tin cậy

C. Sử dụng form token

**Câu 16:** PHP có thể chạy trên Microsoft Windows IIS (Internet Information Server)

A. Đúng

B. Sai

**Câu 17:** Hàm nào trong PHP thực hiện việc loại bỏ các ký tự điều khiển có trong đầu vào?

A. filter\_var(), filter\_var\_array(), filter\_input(), filter\_input\_array(), htmlspecialchars()

B. filter\_var(), filter\_var\_array(), filter\_input\_array()

C. filter\_input(), filter\_input\_array()

D. filter\_var(), filter\_var\_array(), filter\_input(), filter\_input\_array()

**Câu 18:** Lệnh HTML chính xác để tham chiếu đến Bảng định kiểu bên ngoài (External CSS) là gì?

A. <stylesheet>mystyle.css</stylesheet>

B. <link rel= “stylesheet” type=”text/css” src =”mystyle.css”>

C. <style src=”mystyle.css”>

D. <link rel=”stylesheet” type=”text/css” href=”mystyle.css”>

**Câu 19:** Lệnh jQuery để ẩn phần tử có id=test?

A. $(“test”).hide();

B. $(id=”test”).hide():;

C. $(“#test”).hide();

D. $(“.test”).hide();

**Câu 20:** Lệnh HTML chính xác để tạo siêu liên kết là gì?

A. <a name= “https:// actvn.edu.vn”>Học viện Kỹ thuật mật mã</a>

B. <a href= “https:// actvn.edu.vn”>Học viện Kỹ thuật mật mã</a>

C. <a url= “https:// actvn.edu.vn”>Học viện Kỹ thuật mật mã</a>

D. <a> https:// actvn.edu.vn </a>

**Câu 21:** Khai báo nào sau đây khai báo chính xác một tài liệu XML?

A. <?xml vesion= “1.0”?>

<Product>

<name type= “Apple”/>

<price>5.99</price>

<description>A delicious apple.</description>

</Product>

B. <?xml vesion= “1.0”?>

<Product>

<name>Apple</name>

<price>5.99</price>

<description>A delicious apple.</description>

</product>

C. <?xml vesion= “1.0”?>

<product>

<name>Apple</name>

<price>5.99</price>

<description>A delicious apple.</description>

</product>

D. <?xml vesion= “1.0”?>

<Product>

<name type= “Apple” />

<price>5.99</price>

<description type = “A delicious apple.”/>

</product>

**Câu 22:** Làm thế nào để viết “Hello World” trong một hộp cảnh báo

A. alertBox(“Hello World”);

B. alert(“Hello World”);

C. msgBox(“Hello World”);

D. msg(“Hello World”);

Câu 23: Làm cách nào để viết câu lệnh IF trong JavaScript?

A. if i =5

B. if i ==5 then

C. if (i == 5 )

D. if i = 5 then

**Câu 24:** Hàm trong PHP thực hiện việc chuyển đổi các ký tự điều khiển thành “escape sequence” tương ứng

A. htmlspecialchars(), htmlentities(), mysqli:real\_escape\_string()

B. htmlspecialchars(), htmlentities()

C. htmlspecialchars(), htmlentities(), mysqli:real\_escape\_string(), filter\_var()

D. htmlspecialchars(), htmlentities(), mysqli:real\_escape\_string(), PDO::quote()

**Câu 25:** Thuộc tính HTML nào được sử dụng để xác định kiểu nội tuyến (Inline CSS) ?

A. styles

B. font

C. style

D. class

**Câu 26:** Khi thiết lập httponly=true thì:

A. Trình duyệt chỉ sử dụng phương thức HTTP

B. Trình duyệt không được truy cập cookie bằng javascript

C. Trình duyệt bị tắt javascript

D. Trình duyệt chỉ truyền cookie qua kết nối an toàn

**Câu 27:** Thẻ (Tag) trong XML có phân biệt chữ hoa, chữ thường không?

A. Có

B. Không

**Câu 28:** HTML là viết tắt của từ gì?

A. Hyperlinks and Text Markup Language

B. Home Tool Markup Language

C. Hyper Text Markup Language

**Câu 29:** Chọn chính xác phần tử HTML cho tiêu đề lớn nhất:

A. <h6>

B. <h1>

C. <head>

D. <heading>

**Câu 30:** Kết quả thu được như hình vẽ sau cho thấy



A. Câu truy vấn cơ sở dữ liệu tương ứng có kết quả có số cột <8

B. Câu truy vấn cơ sở dữ liệu tương ứng có kết quả có số cột <=8

C. Câu truy vấn cơ sở dữ liệu tương ứng có kết quả số cột >8

**Câu 31:** CSS là viết tắt của từ gì?

A. Colorful Style Sheets

B. Computer Style Sheets

C. Creative Style Sheets

D. Cascading Style Sheets

**Câu 32:** Các thành phần cơ bản của HTML

A. Các thẻ (Tag), các phần tử (Elements), các thuộc tính (Attributes), các bộ chọn (Selectors)

B. Các thẻ (Tag), các phần tử (Elements), các sự kiện (Events), các định dạng (Style)

C. Các thẻ (Tag), các phần tử (Elements), các sự kiện (Events), các bộ chọn (Selectors)

D. Các thẻ (Tag), các phần tử (Elements), các thuộc tính (Attributes)

**Câu 33:** Lệnh đóng kết nối cơ sở dữ liệu sử dụng MySQLi hướng đối tượng:

A. $conn = null;

B. $conn->close();

C. mysqli\_close($conn);

**Câu 34:** Mã khai báo phía dưới để sử dụng Bootstrap CDN



A. Sai

B. Đúng

**Câu 35:** HTML chính xác để tạo danh sách thả xuống là gì?

A. <input type=”dropdown”>

B. <select>

C. <list>

D. <input type= “list”>

**Câu 36:** Trang web sau có thể bị tấn công bằng?



A. XSS – Cross-Site Scripting

B. Brute force

C. SQL Injection

D. CSRF – Cross-site Request Forgery

**Câu 37:** Đâu là cú pháp khai báo đúng của Bộ chọn nhóm trong CSS

A. h1 h2 p {

text-align: center;

color:red;

}

B. .center{

text-align: center;

color:red;

}

C. \* {

text-align: center;

color:red; }

D. h1, h2, p {

text-align: center;

color:red;

}

**Câu 38:** Cách chính xác sử dụng jQuery CDN

A close up of a logo

Description automatically generated

A close up of a logo

Description automatically generated

A close-up of a computer script

Description automatically generated

A computer code with a white background

Description automatically generated

**Câu 39:** Loại kiểm thửu nào mà mã của trình kiểm thử được nhúng vào trong chương trình được kiểm thử trước khi thực hiện kiểm thử?

A. Kiểm thử động (DAST = Dynamic AST)

B. Kiểm thử tĩnh (SAST = Static AST)

C. Kiểm thử tương tác (IAST = Interactive AST)

**Câu 40:** Để đảm bảo an toàn cho ứng dụng web, cần thực hiện Mô hình hóa hiểm họa (threat modeling) ở giai đoạn nào trong quá trình phát triển phần mềm theo mô hình thác nước (waterfall model)

A. Kiểm thử

B. Khảo sát, phân tích yêu cầu

C. Thực hiện

D. Thiết kế

**Câu 41:** Trong PHP, cách duy nhất để xuất văn bản là sử dụng echo

A. Đúng

B. Sai

**Câu 42:** Một <iframe> được sử dụng để hiển thị một trang web trong một trang web

A. Không có thẻ <iframe>

B. Sai

C. Đúng

**Câu 43:** Trong hình sau, các số 2,3,4,5 trong bảng có ý nghĩa gì ?



A. Chỉ có những giá trị của trường tương ứng với những số này trong câu truy vấn mới hiển thị trong bảng

B. Chỉ có những trường tương ứng với những số này trong câu truy vấn mới giống với câu truy vấn phía trước

C. Chỉ có những trường tương ứng với những số này trong câu truy vấn mới nằm trong cơ sở dữ liệu

**Câu 44:** Bên trong phần tử HTML nào đặt JavaScript?

A. <js>

B. <script>

C. <javascript>

D. <scripting>

**Câu 45:** Làm thế nào để gọi một hàm có tên là “myFunction” ?

A. call myFunction()

B. call function myFunction()

C. myFunction()

**Câu 46:** Cú pháp JavaScript chính xác để thay đổi nội dung của phần tử HTML bên dưới là gì?

<p id = “demo”> Hello World! </p>

A close up of text

Description automatically generated

A. Đáp án A

B. Đáp án B

C. Đáp án C

D. Đáp án D

**Câu 47:** DOCTYPE nào phù hợp với HTML5?

A. <!DOCTYPE HTML PUBLIC “.//W3C//DTD HTML 5.0//EN” “http:// www.w3.org/TR/html5/strict.dtd”>

B. <!DOCTYPE html>

C. <!DOCTYPE HTML5>

**Câu 48:** PHP là viết tắt của từ gì?

A. Personal Hypertext Processor

B. Private Home Page

C. PHP: Hypertext Preprocessor

**Câu 49:** Đâu KHÔNG PHẢI là cách phòng chống tấn công CSRF trong framework Laravel?

A black text on a white background

Description automatically generated



A close up of text

Description automatically generated

A white background with black text

Description automatically generated

**Câu 50:** Dữ liệu REST API (RESTful API) trả về chỉ có dạng JSON

A. Đúng

B. Sai

**Câu 51:** Vị trí nào trong tài liệu HTML là vị trí chính xác để tham chiếu đến Bảng định kiểu bên ngoài (External CSS)

A. Ở cuối tài liệu

B. Trong phần <head> và <body>

C. Trong phần <body>

D. Trong phần <head>

**Câu 52:** Đoạn mã sau kết nối cơ sở sử dụng:

A computer code with black text

Description automatically generated

A. PDO

B. MySQLi (thủ tục)

C. MySQLi (hướng đối tượng)

**Câu 53:** Đâu là cú pháp CSS chính xác?

A. body {color: black;}

B. body:color=black;

C. {body;color:black;}

D. {body:color=black;}

**Câu 54:** Web Service là:

A. Phần mềm thực hiện tương tác dữ liệu với phần mềm khác qua giao thức một trình duyệt

B. Phần mềm thực hiện giao tiếp với người dùng thông qua một trình duyệt

C. Phần mềm thực hiện tương tác dữ liệu với phần mềm khác qua các giao thức web

D. Phần mềm thực hiện giao tiếp với người dùng thông qua các giao thức web

**Câu 55:** Làm thế nào để chọn các phần tử có tên lớp “test”?

A. \*test

B. #test

C. test

D. .test

**Câu 56:** Phần tử nào trong số những phần tử này đều là phần tử <table>?

A. <table> <tr><tt>

B. <table><tr><td>

C. <table><head><tfoot>

D. <thead><body><tr>

**Câu 57:** Mô hình CRUD trong REST API là?

A. Creat (POST), Read (GET), Update (PUT), Delete (DELETE)

B. Creat (PATCH), Read (GET), Update (PUT), Delete (DELETE)

C. Creat (PATCH), Read (POST), Update (PUT), Delete (DELETE)

D. Creat (POST), Read (GET), Update (PATCH), Delete (DELETE)

**Câu 58:** Cú pháp chính xác để tham chiếu đến tập lệnh bên ngoài có tên “xxx.js” là gì?

A. <script src= “xxx.js”>

B. <link href= “xxx.js”>

C. <script href= “xxx.js”>

D. <script name= “xxx.js”>

**Câu 59:** Cú pháp CSS chính xác để in đậm tất cả các phần tử <p> là gì?

A. p {font-weight:bold;}

B. <p style= “text-size:bold;”>

C. <p style = “font-size:bold;”>

D. p {text-size:blod;}

**Câu 60:** Mẫu an toàn (Security Pattern) là:

A. Một mẫu mô tả cách thức ngăn ngừa một hiểm họa bằng việc sử dụng các cơ chế an toàn.

B. Một thiết kế hoàn thiện cho các cơ chế an toàn để có thể được chuyển đổi trực tiếp thành mã

C. Một giải thuật mô tả cách thức ngăn ngừa một hiểm họa

D. Một giải pháp tổng thể cho các vấn đề chung trong thiết kế an toàn phần mềm

**Câu 61:** Làm thế nào để hiển thị một đường viền như thế này

Đường viền trên cùng =10 pixel, đường viền dưới cùng = 5 pixel, đường viền bên trái = 20pixel, đường viền bên phải = 1 pixel?

A. border-width: 10px 1px 5px 20px;

B. border-width: 10px 20px 5px 1px;

C. border-width: 5px 20px 10px 1px;

D. border-width: 10px 5px 20px 1px;

***Hướng dẫn:*** https://webcoban.vn/css/cach-tao-duong-vien-border-cho-mot-phan-tu-html-trong-css.html