**ĐỀ THI CUỐI KÌ ĐỢT 1-K16**

Câu 1:  Web Service là:

1. Phần mềm thực hiện giao tiếp với người dùng thông qua một trình duyệt
2. Phần mềm thực hiện tương tác dữ liệu với phần mềm khác qua giao thức một trình duyệt
3. Phần mềm thực hiện giao tiếp với người dùng thông qua các giao thức web
4. Phần mềm thực hiện tương tác dữ liệu với phần mềm khác qua các giao thức web

Câu 3: Thẻ tag trong XML có phân biệt chữ hoa, chữ thường không?

1. Có
2. Không

Câu 4: Khi thiết lập httponly = true thì

1. Trình duyệt chỉ sử dụng phương thức HTTP
2. Trình duyệt không được truy cập cookie bằng javascript
3. Trình duyệt chỉ truyền cookie qua kết nối an toàn
4. Trình duyệt bị tắt javascript

Câu 5: Lệnh jQuery nào để ẩn phần tử có id=test

* 1. $(id= “test”).hide();
  2. $(“test”).hide();
  3. $(“#test”).hide();
  4. $(“.test”).hide();

Câu 6: Bên trong phần tử HTML nào đặt JavaScript?

1. <script>
2. <scripting>
3. <javascript>
4. <js>

Câu 8: HTML chính xác để tạo vùng văn bản là :

1. <input type=”textbox”>
2. <textarea>
3. <input type=”textarea”>

Câu 9: Làm thế nào để thêm màu nền cho tất cả các phần tử <h1>

1. h1.all{background-color:#FFFFFF;}
2. all.h1{background-color:#FFFFFF;}
3. h1{background-color:#FFFFFF;}

Câu 10: Dữ liệu REST API (RESTful API) trả về chỉ có dạng JSON

1. Đúng
2. Sai

Câu 11:  Làm cách nào để viết câu lệnh IF trong JavaScript?

1. if i = 5 then
2. if (i==5)
3. if i = 5
4. if i == 5 then

Câu 12: Mẫu an toàn (Security Pattern) là:.

1. Một thiết kế hoàn thiện cho các cơ chế an toàn để có thể được chuyển đổi trực tiếp thành mã
2. Một mẫu mô tả cách thức ngăn ngừa một hiểm họa bằng việc sử dụng các cơ chế an toàn.
3. Một giải pháp tổng thể cho các vấn đề chung trong thiết kế an toàn phần mềm
4. Một giải thuật mô tả cách thức ngăn ngừa một hiểm họa

Câu 13:  Các biện pháp đảm bảo an toàn phần mềm ở giai đoạn”Phát triển”;

1. Mô hình hóa hiểm họa {Threat Modeling), Mẫu thiết kế an toàn{Security Design Pattern}
2. Mô hình hóa hiểm họa {Threat Modeling), Mẫu thiết kế an toàn{Security Design Pattern}, Lập trình an toàn{Secure Coding}
3. Mô hình hóa hiểm họa {Threat Modeling), Mẫu thiết kế an toàn{Security Design Pattern}, Lập trình an toàn{Secure Coding}, Kiểm thử an toàn{Testing for Security}
4. Mô hình hóa hiểm họa {Threat Modeling), Mẫu thiết kế an toàn{Security Design Pattern}, Lập trình an toàn{Secure Coding}, Kiểm thử an toàn{Testing for Security}, Triển khai

Câu 14:Đâu là cú pháp khai báo đúng của Bộ chọn nhóm trong CSS :

A bổ sung thêm ; rùi nhé

1. \*{

text-align: center;

color: red;

}

1. .center {

text-align: center;

color: red:

}

1. h1, h2.p{

text-align: center;

color: red,

}

1. h1.h2.p{

text-align: center;

color: red,

}

Câu 15: Các thành phần cơ bản của HTML:

1. Các thẻ (Tags), các phần tử (Elements), các sự kiện (Events), các định dạng (Style)
2. Các thẻ (Tags), các phần tử (Elements), các thuộc tỉnh (attributes), các bộ chọn (Selectors)
3. Các thẻ (Tags), các phân tử (Elements), các sự kiện (Events), các bộ chọn (Selectors)
4. Các thẻ (Tags), các phân tử (Elements), các thuộc tính (attributes)

Câu 16: HTML chính xác để tạo danh sách thả xuống là gì?

* 1. <input type="dropdown">
  2. <list>
  3. <select>
  4. <input type="list">

Để tạo một danh sách thả xuống trong HTML, chúng ta có thể sử dụng thẻ <select> và các thẻ con <option> để liệt kê các tùy chọn.

Câu 17: đoạn mã sau kết nối cơ sở sử dụng

<?php

$servername=”localhost”;

$username=”username”;

$password=”password”;

$database=”my\_db”;

$conn = new mysqli($servername,$username,$password,$database);

If ($conn->connect\_error){

Die(“connection\_failed:”.$conn->connect\_error)

}

Echo”connected successfully”;

?>

* 1. MySQLi (hướng đối tượng)
  2. PDO
  3. MySQLi (thủ tục)

Câu 18: Theo OWASP TOP 10 2021, hiểm hoạ nào được xếp hạng thứ 9?

1. Lỗi định danh và xác thực - Identification and Authentication Failures
2. Yêu cầu giả mạo phía máy chủ - Server-Side Request Forgery
3. Lỗi toàn vẹn dữ liệu và phần mềm - Software and Data Integrity Failures
4. Lỗi giám sát và ghi nhật ký an toàn - Security Logging and Monitoring

1. Broken Access Control (Lỗ hổng kiểm soát truy cập)

2. Cryptographic Failures (Lỗi mật mã)

3. Injection (Chèn thêm mã độc)

4. Insecure Design (Thiết kế không an toàn)

5. Security Misconfiguration (Cấu hình bảo mật sai)

6. Vulnerable and Outdated Components (Các thành phần không an toàn và lỗi cũ)

7. Identification and Authentication Failures (Lỗi xác định và xác thực)

8. Software and Data Integrity Failures (Lỗi toàn vẹn phần mềm và dữ liệu)

9. Security Logging and Monitoring Failures (Lỗi giám sát và ghi nhật ký an toàn)

10. Server-Side Request Forgery (Lỗ hổng tấn công từ phía máy chủ)

Câu 19: Trang web sau có thể bị tấn công bằng:

<?php

$name = $\_GET['name'];

echo "Welcome $name<br>";

echo '<a href="http://examples.com/">Click to Download</a>';

?>

1. SQL Injection
2. XSS-Cross-Site Scripting
3. CSRF-Cross-site Request Forgery
4. Brute force

Câu 20: Lệnh HTML chính xác để chèn hình ảnh là gì?

1. <img alt="Myimage">image.gif</img>
2. <img href="image.gif" alt="MyImage">
3. <img src="image.gif" alt="MyImage">
4. <image src="image.gif" alt="MyImage">

Câu 21: php là viết tắt của từ gì?

1. PHP:Hypertext Preprocessor
2. Private Home Page
3. Personal Hypertext Processor

Câu 22: Làm thế nào để khai báo một biến JavaScript?

1. $carName
2. variable carName;
3. var carName;
4. v carName.

Trong JavaScript, khai báo biến bằng các từ khóa "var", "let" hoặc "const"

Câu 23: Cú pháp chính xác của một cặp NAME/ VALUE trong JSON:

1. “teacher":{

“name” : ”Trần Văn Bình”;

“department” : “An toàn thông tin”

}

1. “teacher"{

“name” : ”Trần Văn Bình”,

“department” : “An toàn thông tin”

}

1. “teacher":{

“name” : ”Trần Văn Bình”,

“department” : “An toàn thông tin”

}

1. teacher: {

name : ”Trần Văn Bình”,

department : “An toàn thông tin”

         }

tên thuộc tính (hoặc khóa) luôn phải được đặt trong dấu ngoặc kép “ ” và cách nhau bởi dấu hai chấm. Các giá trị cũng nằm trong dấu ngoặc kép và được ngăn cách bằng dấu phẩy.

Câu 24: Cách chính xác sử dụng jQuery CDN:

1. <body>

<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>

</body>

1. <head>

<script src="jquery-3.6.0.min.js"></script>

</head>

1. <body>

<script src="jquery-3.6.0.min.js"></script>

<body>

1. <head>

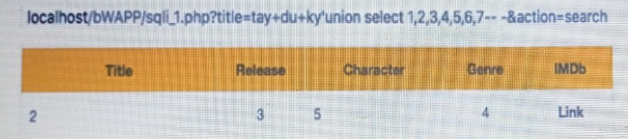
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery min.js"></script>

<head>

Câu 25: Phát biểu nào SAI

1. Thực hiện kiểm tra hợp thức phía client bằng Javascript.
2. Kiểm tra hợp thức phía cient là cách kiểm tra hiệu quả và thân thiện hơn, tăng được tương tác với người dùng
3. Thực hiện kiểm tra hợp thức phía server bằng ngôn ngữ kịch bản.
4. Có thể dùng kiểm tra hợp thức phía client và server thay thế cho nhau.

Câu 26. Trong hình sau các số 2,3,4,5 trong bảng có nghĩa gì?



* 1. Chỉ có những trường tương ứng với những số này trong câu truy vấn mới giống câu truy vấn phía trước
  2. Chỉ có những trường tương ứng với những số này trong câu truy vấn mới nằm trong cơ sở dữ liệu
  3. Chỉ có những trường tương ứng với những số này trong câu truy vấn mới hiển thị trong bảng

Câu 27: Làm thế nào để chọn một phần tử có id="demo" trong CSS

1. demo
2. .demo
3. #demo
4. \*demo

Câu 28: Làm thế nào để chọn các phần tử có tên lớp ‘test’?

1. \*test
2. test
3. #test
4. .test

Câu 29: Cú pháp chính xác để tham chiếu đến tập lệnh bên ngoài có tên "xxx.js" là gì

1. <script name=”xxx.js”>
2. <script href=”xxx.js”>
3. <link href=”xxx.js”>
4. <script src=”xxx.js”>

Câu 30: Doctype nào phù hợp vỚI HTML5?

1. <!DOCTYPE html>
2. <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 5.0//EN" <http://www.w3.org/TR/html5/strict.dtd>>
3. <!DOCTYPE HTML5>

Câu 31: Vị trí nào trong tài liệu html là vị trí chính xác để tham chiếu đến bảng định kiểu bên ngoài (external CSS)

1. Trong phần <body>
2. Ở cuối tài liệu
3. Trong phần <head>
4. Trong phần <head> và <body>

Câu 32: Biện pháp phòng chống tấn công CSRF -Cross-Site Request Forgery là:

1. Sử dụng form token
2. Lọc dữ liệu đầu vào, kiểm thử
3. Lọc dữ liệu đầu vào, kiểm thử, người dùng không mở các đường link từ nguồn không đáng tin cậy

Câu 33: Lệnh HTML chính xác để tham chiếu đến Bảng định kiểu bên ngoài (External Css) là gì?

1. <stylesheet>mystyle.css/stylesheet>
2. <style src="mystyle.css">
3. <link rel="stylesheet".type="text/css" href="mystyle.css">
4. <link rel=”stylesheet" type="text/css" src="mystyle.css">

Câu 34: Trong php, cách duy nhất để xuất văn bản là sử dụng echo

1. Sai
2. Đúng

Câu 35: Việc thay đổi nội dung trang web mà không cần tài lại toàn bộ trang web được thực thi nhờ

1. Hàm SimpleXMLElement()
2. Hàm  geResponseHeader()
3. Đối tượng trong XML HttpRequest
4. Hàm getResponseHeader()

Câu 36: Hình sau mô tả loại tấn công nào?

A diagram of a computer network

Description automatically generated

1. XSS- Cross Site Scripting
2. Injection
3. SSRF - Server Side Request Forgery
4. CSRF - Cross-Site Request Forgery

Câu 37: Làm thế nào để chọn tất cả các phần từ p bên trong phần từ div

1. div.p: chọn tất cả các phần tử div có lớp CSS là "p".
2. div, p: chọn tất cả các phần tử div và p trên trang.
3. div + p: chọn tất cả các phần tử p được theo sau ngay sau một phần tử div
4. div p: chọn tất cả các phần từ p bên trong phần từ div

câu 38: HTML chính xác để chèn hình nền là gì?

1. <body bg="background.gif">
2. <background img="background.gif">
3. <body style="background-image:url(background.gif)”>

Câu 39: Khi sử dụng phương thức POST, các biến được hiển thị trong URL

1. Sai
2. Đúng

Câu 40: Hàm PHP nào chỉ loại bỏ tất cả các biến phiên?

1. Session\_unset();
2. Isset\_session();
3. $\_SESSION=null;
4. Session\_destroy();

Câu 41:  Theo OWASP TOP 10 2021, hiểm hoạ nào được xếp hạng thứ 7?

1. Các thành phần dễ bị tổn thương và lỗi thời -Vulnerable and Outdated Components
2. Lỗi giám sát và ghi nhật ký an toàn - Security Logging and Monitoring Fave
3. Là định danh và xác thực - Identification and Authentication Failures.
4. Lỗi toàn vẹn dữ liệu và phần mềm - Software and Data legity Fatures.

Câu 42: các tệp bao gồm trong php có phải phần mở rộng tệp ".inc"

1. Đúng
2. Sai

Câu 43: Một "iframe" được sử dụng để hiển thị một trang web trong một trang web

1. False
2. Không có thẻ <iframe>
3. True

Câu 44: Đoạn mã sau kết nối cơ sở sử dụng:

<?php

$servername="localhost";

$username="username":

$password = "password";

$database="my\_db";

$conn=mysqli\_connect($servername,$username,$password,$database);

if (!$conn) {

die("Connection failed: ", mysqli\_connect\_error(});

}

echo "Connected successfully";

?>

1. MySQLi (hướng đối tượng)
2. MySQLi (thủ tục)
3. PDO

Câu 45: Thẻ html nào được sử dụng để xác định bảng định kiểu bên trong (internal CSS)

1. <link>
2. <style>
3. <script>
4. <css>

Câu 46: Làm thế nào để viết “ Hello World “ trong một hộp cảnh báo?

1. msg("Hello World");
2. alertBox("Hello World");
3. msgBox("Hello World");
4. alert("Hello World");

Câu 47. Khai báo nào sau đây khai báo chính xác một tài liệu XML?

1. <?xml version='1.0' ?>

<Product>

<name type="Apple"/>

<price>5.99</price>

<description>A delicious apple. </description>

</Product>

1. <?xml version='1.0' ?>

<Product>

<name type="Apple" />

<price>5.99</price>

<description type="A delicious apple." />

</product>

1. <?xml version='1.0' ?>

<product>

<name>Apple</name>

<price>5.99</price>

<description>A delicious apple </description:

</product>

1. <?xml version='1.0' ?>

<product>

<name>Apple</name>

<price>5.99</price>

<description>A delicious apple </description:

</product>

Câu 48: Lệnh HTML chính xác để tạo siêu liên kết là gì?

1. <a url=” https:// actvn.edu.vn"> Học viện Kỹ thuật mật mã </a>.
2. <a>https:// actvn.edu.vn</a>
3. <a name="https // actvn.edu.vn">Học viện Kỹ thuật mật mã</a>
4. <a href="https://actvn.edu.vn">Học Viện Kỹ thuật mật mã</a>

Câu 49: 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 = 20 pixel, đường viền bên phải = 1 pixel?

* 1. border-width:5px 20px 10px 1px;
  2. border-width:10px 1px 5px 20px;
  3. border-width:10px 20px 5px 1px;
  4. border-width:10px 5px 20px 1px;

Câu 50: Đâu KHÔNG PHẢI là cách phòng chống tấn công CSRF trong framework Laravel?

1. <form action="/transfer-money" method="post">

<input type="hidden" name="\_token" value="{{csrf\_token()}}"/>

…

</form>

1. {!!Form::open([url=> ‘/transfer-money’, ‘methods’>’ post’]) !! }…{!! Form:: close() !!}
2. <form action="/transfer-money" method="post">

@csrf

…

</form>

1. <form actions/transter-money.php" method="post">

<input type="hidden" name token" values?php $\_SESSION['csrf\_token’] ?>\*/>

….

</form>

Câu 52: Làm cách nào để tạo một hàm trong JavaScript?

1. function:myFunction()
2. function = myFunction()
3. function myFunction()

Câu 53: Mã khai báo phía dưới để sử dụng bootstrap CDN:

<link href="/bootsstrap.min.css" rel="stylesheet">

<script src="/bootstrap.bundle.min.js"></script>

* 1. Đúng
  2. Sai

Câu 54: Đâu là vị trí chính xác để chèn javascript

1. Cả phần <head> và <body>
2. Phần <body>
3. phần <head>

Câu 55: Kết quả thu được như hình vẽ sau cho thấy:

localhost/bWAPP/sqli\_1.php?title=tay+du+ky order by 8---&action=search

| Title | Reless | Character | Genre | IMDb |
| --- | --- | --- | --- | --- |

Error: Unknown column 8 in 'order cause

1. Câu truy vấn cơ sở dữ liệu tương ứng có kết quả có số cột >8
2. Câu truy vấn cơ sở dữ liệu tương ứng có kết quả có số cột =8
3. Câu truy vấn cơ sở dữ liệu tương ứng có kết quả có số cột <=8

Câu 56 : Hàm nào trong PHP thực hiện việc loại bỏ các ký tự điều khiển có trong đầu vào?

1. filter\_input(), filter\_input\_array()
2. filter\_var(), filter\_var\_array(), filter\_input(), filter\_input\_arrray()
3. filter\_var(), filter\_var\_array(),filter\_input\_array()
4. filter\_var(), filter\_var\_array(), filter\_input(), filter\_input\_arrray(), htmlspecialchars()

Câu 57:  Kết quả của việc mô hình hóa hiểm họa là:

1. Danh mục các hiểm họa và cách thức xử lý các hiểm họa
2. Danh mục các hiểm họa và xếp hạng mức độ ưu tiên của các hiểm họa
3. Danh mục các hiểm họa và các cơ chế an toàn
4. Danh mục các hiểm họa

Câu 58: Để đảm bảo an toàn cho ứng dụng web, cần thực hiện mô hình hóa hiểm họa ở giai đoạn nào trong quá trình phát triển phần mềm theo mô hình thác nước.

1. Thiết kế
2. Kiểm thử
3. Thực hiện
4. Khảo sát, phân tích yêu cầu

Câu 59: HTML là viết tắt của từ gì

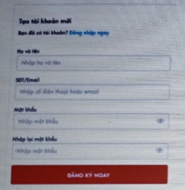
1. Hyperlinks and Text Markup Language
2. Home Tool Markup Language
3. HyperText Markup Language

Câu 60:  Lệnh HTML chính xác để thêm màu nền là gì?

1. <body style="background-color:yellow">
2. <background>yellow</background>
3. <body bg="yellow">

**II. TỰ LUẬN**

**Xây dựng trang đăng kí (register.php)**

****

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

- ID: định danh duy nhất của người dùng

- USERNAME: Họ và tên của người dùng

- EMAIL: Emall của người dùng

- PHONE: Số điện thoại của người dùng

- PASS: giá trị băm của Mật khẩu người dùng cùng với SALT (sử dụng thuật toán SHA1)

- SALT: giá trị ngẫu nhiên cho mỗi người dùng

Nếu một trong số các trường nhập trống (báo lỗi), Mật khẩu và Mật khẩu nhập lại nếu không thoả mãn Chính sách mật khẩu (Mật khẩu phải có >= 8 ký tự, bao gồm > 2 nhóm kí tự ( chữ thường, chữ số và kí tự đặc biệt)) báo lỗi, Mật khẩu mới và Mật khẩu nhập lại không trùng nhau (báo lỗi). Số điện thoại hoặc email không đúng định dạng (báo lỗi)

Mỗi một email hoặc số điện thoại chỉ gắn với 01 tài khoản người dùng.

Khi người dùng đăng ký tài khoản thành công sẽ hiển thị thông báo “Successful account registration!” và điều hướng đến trang login.php.

Áp dụng các cơ chế an toàn cho trang Đăng ký.Áp dụng các cơ chế an toàn cho trang Thay đổi mật khẩu