Oefenopgaven Applied JavaScript 3

Vraag 1 van 24

Which of the following is a type of code injection attack?

A. SQL injection.

B. Cross-site scripting.

C. Cross-site request forgery.

D. Session hijacking.

Vraag 2 van 24

Cross-site scripting (XSS) is a type of:

A. phishing scam.

B. code-injection attack.

C. same-origin policy violation.

D. security risk associated with signed scripts.

Vraag 3 van 24

How can a cookie be deleted using JavaScript?

A. By using the cookie.delete() method.

B. By setting a past expiration date.

C. By reassigning it the null value.

D. By closing the browser window.

Vraag 4 van 24

Which example demonstrates the proper JavaScript syntax to test for the presence of a cookie?

A. document.cookie = "name = value";

B. confirm(cookie);

C. alert(document.cookie);

D. window.cookie = "name = value";

Vraag 5 van 24

Which of the following disadvantages of browser detection is **most** likely to pose a security threat?

A. Unable to identify the correct browser version.

B. All browsers may not be identified.

C. Specific browsers may have unique vulnerabilities.

D. Browsers released after writing the script may not be identified.

Vraag 6 van 24

In cross-site scripting, the malicious code is generally embedded in:

A. the victim's email application.

B. the attacker's webpage code.

C. an executable file.

D. a hyperlink.

Vraag 7 van 24

Which of the following constitutes an XSS attack?

A. A hyperlink that carries malicious content.

B. An infinite loop.

C. Storing cookies.

D. Browser identification.

Vraag 8 van 24

What do you understand by an inline frame?

A. A frame that displays a separate file floating within a page.

B. A technique in which one frame in a frameset can direct the URL in another frame to display a different page.

C. A frame that is developed from a plain HTML file without any other application.

D. A technique used by web applications to prevent their webpages from being displayed within a frame.

Vraag 9 van 24

A user enters confidential data on a website while performing a task. This data was redisplayed on the webpage after the task was completed. The data sent between a server and a browser was not encoded as HTML entities. Which of the following vulnerabilities will occur in the given scenario?

A. Persistent XSS.

B. Non-persistent XSS.

C. DOM-based XSS.

D. Cloaking.

Vraag 10 van 24

Which of the following coding practices may augment security issues in a page?

A. Explain the site's functionality to users.

B. Use standards-based code.

C. Use browser-specific code.

D. Avoid using deprecated code.

Vraag 11 van 24

Which of the following is an invalid parameter in reference to a cookie header?

A. expires=expiry_date

B. path=path_of_cookie

C. domain=domain_name

D. name=cookie_name

Vraag 12 van 24

Which of the following information is NOT a part of the cookie header?

A. username=username

B. path=path

C. domain=domain

D. expires=date

Vraag 13 van 24

Which of the following is least likely to pose a security threat for a user?

A. XSS.

B. Signed scripts.

C. Cloaking.

D. Cookies.

Vraag 14 van 24

Which of the following is true in relation to security?

A. The operating system can be secured but the browser cannot.

B. The browser can be secured but the operating system cannot.

C. The operating system provides a doorway to the browser for security threats.

D. Both the operating system and the browser can be secured with anti-virus software.

Vraag 15 van 24

What are cookies?

A. Malicious JavaScript code.

B. Small pieces of information sent to a client computer.

C. Small JavaScript applications.

D. Compiled Java code with which JavaScript can interact.

Vraag 16 van 24

Which of the following practices will you use for preventing cross-site scripting (XSS) attacks?

A. Avoiding the use of deprecated or unknown code.

B. Using output encoding and input validation practices.

C. Testing scripts thoroughly on various browsers.

D. Writing code consistently and with liberal comments.

Vraag 17 van 24

Which statement is false regarding XSS attacks?

A. They cannot be performed through emails or mail clients.

B. They inject malicious code to gain access to sensitive data.

C. They exploit cookies that may contain sensitive data.

D. Even when users visit trusted sites, XSS code injection may allow hackers to steal sensitive data.

Vraag 18 van 24

Which of the following is true of JavaScript security?

A. Cookies carry no security threat.

B. Disabling JavaScript is the only way to prevent security threats.

C. Cloaking improves the security of a webpage.

D. Browser detection helps in targeting attacks on vulnerabilities in a browser.

Vraag 19 van 24

Which of the following uses of a cookie may compromise a user's security?

A. Maintain user state.

B. Store user preference.

C. Authenticate a user.

D. Store a user's browsing history.

Vraag 20 van 24

Which JavaScript object is used for client-side browser detection?

A. AppName

B. navigator

C. UserAgent

D. BrowserType

Vraag 21 van 24

Which browser security consideration should a JavaScript developer remember when developing a script?

A. JavaScript functionality is immune to viruses, trojans, and malware.

B. JavaScript can be disabled by a user and therefore cannot be relied upon to run.

C. JavaScript is a cross-platform scripting language and will generate consistent results regardless of the client or server being used.

D. Certain JavaScript functionality is built into browsers and has been tested by the browser developers so it cannot be disabled by a user because it is deemed safe.

Vraag 22 van 24

Consider the following code block:

```
if (document.cookie) document.cookie =
"testExample=Test;expires=20-May-1910";
else alert("no");
alert(document.cookie);
```

On executing the script, an alert box is displayed on the page that does not contain the testExample cookie. Why was the cookie not displayed?

A. The user's browser may not support cookies.

B. The last alert message is syntactically wrong, it must be alert(document.cookie.testExample);.

C. The condition in the if block did not evaluate to true.

D. The cookie was not created because the properties of the cookie didn't allow creation.

Vraag 23 van 24

In one JavaScript-related security vulnerability, an attacker embeds malicious script into a link that appears to be from a trusted site. Upon clicking the link, the embedded script is submitted in the client's HTTP request and can execute on the user's computer, enabling the attacker to steal information. What is the term for this security issue?

A. Signed script.

B. Cross-site scripting.

C. Client-side browser detection.

D. Frame-to-frame URL changing.

Vraag 24 van 24

Which of the following solutions will NOT help in preventing XSS attacks?

A. Validating user input before submission.

B. Encoding the output URL in HTML entities.

C. Blocking the script on the browser.

D. Storing login credentials in cookies for security.