Antwoorden 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.

Antwoordtoets: B

Feedback:

Cross-site scripting (XSS) is a type of code injection attack. It occurs when an attacker takes advantage of holes, or vulnerabilities, in your web application, which enables him to bypass the security normally imposed by browsers. The attacker injects malicious client-side script into your webpage to gain access to sensitive page content, session cookies, or other user information stored by the site.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

Cross-site scripting is a type of code-injection attack. It is a security vulnerability in which an attacker embeds a 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.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

Cookies can be deleted using JavaScript by reassigning an already past date as an expiration date to the cookie. When a cookie is assigned to an existing cookie name, it replaces the old one. And if the date is set to some point in the past, the cookie expires on creation and is deleted.

(Bron: https://www.ciwcertified.com/.)

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";

Antwoordtoets: C

Feedback:

A user can easily test for the presence of any cookie by using the **document.cookie** statement in your script. For example:

```
<script type="text/javascript">
             <!--
alert(document.cookie);
//-->
             </script>
```

Each time a user accesses this page, he will see a quick listing of all cookies associated with that particular browser session in the following format:

```
name1=value1, name2=value2, etc.
```

If no cookies are present, the user will see an empty alert.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: C

Feedback:

Each browser, and their specific versions, may have unique vulnerabilities and security threats, which can be exploited and targeted by attackers.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: D

Feedback:

A cross-site scripting (XSS) application collects data from the user, usually through a hyperlink that the user is enticed to click, which carries malicious content within it.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: A

Feedback:

Generally, XSS (cross-site scripting) attacks originate at links that carry malicious content. When a user clicks such links, the user's data is collected, and a phony response is generated to a user that looks like original content.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: A

Feedback:

HTML frames contain an inline frame (iframe), which displays a separate file floating within the page. Inline frames appear to be part of the parent page, and generally offer no security indicator or address bar of their own.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

According to the given scenario, the page becomes vulnerable to a non-persistent (reflected) XSS attack. These types of attacks take place when unvalidated user-provided data is included in the HTML page without HTML entities, and received in response from the server. This is the most common type of XSS attack.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: C

Feedback:

Developers should avoid using browser-specific code. Browser-specific code may work fine in one browser, but it may not work in the same manner in other browsers. This may lead to security holes that can be exploited.

(Bron: https://www.ciwcertified.com/.)

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

Antwoordtoets: D

Feedback:

A cookie is saved as a **name=value** pair. The **name** itself is associated with the value of the cookie. A cookie header appears to the browser as follows:

```
Set-Cookie: name=value; expires=date; path=path;
domain=domain; secure
```

(Bron: https://www.ciwcertified.com/.)

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

Antwoordtoets: A

Feedback:

A cookie header is stored in the browser as follows:

```
Set-Cookie: name=value; expires=date; path=path;
domain=domain; secure
```

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

Signed scripts are validated by certificate authorities to prove the authenticity of the author and the integrity of the script. This validation allows the script to override basic security. XSS (cross-site scripting), URL cloaking, and cookies may be used to compromise a user's security.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: D

Feedback:

By understanding the roles of the browser and the operating system, these can be protected by installing anti-virus from malicious software.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

Cookies are small pieces of information sent to a client computer via a browser and stored in memory. Cookies are often sent by a server from a site the user has visited, but can also be set on the client-side using JavaScript.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

As you learned with XSS, creating code that follows proper output encoding and input validation practices (i.e., rigorous syntax standards and checking practices) can protect your site and your users from certain types of attacks. You should not trust user input, and you should always encode output to filter metacharacters; this will help prevent most XSS attacks.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: A

Feedback:

XSS (cross-site scripting) attacks may also appear in emails. When accessing links in an email, even from a trusted site, a user must be careful. The link in the URL may contain malicious code, which may steal sensitive data.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: D

Feedback:

Browser detection helps attackers in targeting the specific vulnerabilities in the user's browser and exploit the security loopholes. Cookies that contain sensitive data can be exploited. There are many solutions to prevent security threats, such as ad blockers, sandbox modes, etc., which helps users to browse the web securely. Cloaking hides the redirected web address from the user and may be used to redirect the user to a malicious site.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: C

Feedback:

Using cookies to authenticate a user presents a security risk. Any other user, with access to a system, may impersonate the authenticated user (authenticated using cookies).

(Bron: https://www.ciwcertified.com/.)

Vraag 20 van 24

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

A. AppName

B. navigator

C. UserAgent

D. BrowserType

Antwoordtoets: B

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.

Antwoordtoets: B

Feedback:

A key consideration for JavaScript developers is that certain JavaScript functionality can be blocked by users. JavaScript can be disabled in the browser by a user.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: D

Feedback:

The user's browser executed the **if** code block because the **else** block was not executed, i.e., the user had no alert message that said "no". Since the expiry date of the cookie was set to a past date, the cookie was not created in the first place by the browser. Therefore, it was not displayed in the last alert message.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: B

Feedback:

Cross-site scripting (XSS) is a security vulnerability in which 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. A signed script is a script validated by a certificate authority that can request extended privileges and abilities in the browser. Frame-to-frame URL changing is a technique in which one frame in a frameset can direct the URL in another frame to display a different page, which introduces security concerns. Client-side browser detection allows the developer to obtain information about the browser used to view his page, such as browser name and version.

(Bron: https://www.ciwcertified.com/.)

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.

Antwoordtoets: D

Feedback:

It is not a good idea to store confidential information, such as login credentials, in cookies. Cookies are vulnerable to attacks. Even if a cookie is tied to a session, hackers can spoof a user's IP and gain access to their session.

(Bron: https://www.ciwcertified.com/.)