Week 1 MCQ

Total points 29/30

The respondent's email (**atharvajagdale45@gmail.com**) was recorded on submission of this form.

✓ Which attribute in an HTML tag can be used for injecting malicious JavaScript? *1/1

- ○ href
- ○ src
- ◉ onclick ✓
- ○ alt

✓ Which of the following is an example of sanitizing input to prevent XSS? * 1/1

- ○ Allowing all HTML tags
- ◉ Converting < to < and > to > ✓
- ○ Displaying user input directly in innerHTML
- ○ Using eval() on user input

✓ In which of the following scenarios is Reflected XSS most common? * 1/1

- ○ Login forms
- ◉ URL parameters ✓
- ○ Database storage
- ○ Network packets

✓ Where is the malicious script executed in Reflected XSS? * 1/1

- ○ On the server
- ◉ On the user's browser ✓
- ○ In the database
- ○ On the firewall

✓ What is the main goal of XSS attacks? * 1/1

- ○ To speed up website performance
- ◉ To inject malicious scripts into web pages ✓
- ○ To block users from accessing websites
- ○ To encrypt website data

✓ Which JavaScript function is often targeted in DOM-based XSS? * 1/1

- ○ setTimeout()
- ◉ eval() ✓
- ○ parseInt()
- ○ JSON.stringify()

✓ What is the main difference between Reflected and Stored XSS? * 1/1

- Reflected XSS requires login, Stored XSS doesn't.
- Reflected XSS happens immediately via URL, Stored XSS is saved and executed later. ✓
- Stored XSS only affects local files.
- There is no difference.

✓ Which of the following best describes a DOM-based XSS attack? * 1/1

- The attack modifies the HTML structure stored in the database.
- The attack occurs when the client-side script modifies the DOM with unsanitized data. ✓
- The attack requires a server-side script to process malicious input.
- The attack is performed through phishing emails.

✓ Which input validation technique helps prevent HTML Injection? * 1/1

- Accepting all inputs
- Escaping special characters ✓
- Ignoring user inputs
- Allowing only numeric inputs

✓ Which of the following is a common vector for XSS attacks? * 1/1

- File uploads
- URL parameters ✓
- DNS queries
- FTP connections

✓ What is the main difference between HTML Injection and XSS? * 1/1

- HTML Injection only targets JavaScript, while XSS targets HTML.
- HTML Injection manipulates the webpage layout, XSS executes scripts. ✓
- There is no difference; they are the same.
- XSS only affects local files, while HTML Injection affects databases.

✓ What is the safest way to handle user-generated content on a website? * 1/1

- Trust all user inputs
- Use content sanitization and encoding techniques ✓
- Disable JavaScript on the website
- Encrypt user inputs before displaying

✓ What does XSS stand for? * 1/1

- Cross-Site Scripting ✓
- Extra Secure Scripting
- Extended Site Scripting
- Cross Security Standards

✓ Which header helps protect against XSS by controlling script execution? * 1/1

- (●) Content-Security-Policy ✓
- ( ) User-Agent
- ( ) Content-Type
- ( ) Accept-Encoding

✓ Which type of XSS occurs when malicious scripts are stored on the server? *1/1

- ( ) Reflected XSS
- (●) Stored XSS ✓
- ( ) DOM-based XSS
- ( ) Redirected XSS

✓ What does the Content-Security-Policy: default-src 'self' header do? * 1/1

- ( ) It allows all scripts to run from external domains.
- ( ) It blocks all scripts from running.
- (●) It restricts scripts to run only from the same origin. ✓
- ( ) It encrypts user input.

✓ Which of the following payloads can exploit an XSS vulnerability? * 1/1

- (●) <script>alert('Hacked!')</script> ✓
- ( ) SELECT * FROM users WHERE id=1
- ( ) DROP TABLE users;
- ( ) chmod 777 /root/

✓ Which JavaScript function can be exploited in XSS attacks? * 1/1

- ( ) alert()
- ( ) console.log()
- (●) document.write() ✓
- ( ) Math.random()

✓ Which of the following is a common effect of an XSS attack? * 1/1

- ( ) Deleting files on the server
- (●) Stealing cookies from users ✓
- ( ) Slowing down internet speed
- ( ) Installing antivirus software

✓ What role does the innerHTML property play in XSS vulnerabilities? * 1/1

- ( ) It encrypts user input.
- (●) It directly renders user input as HTML, leading to potential XSS. ✓
- ( ) It blocks script execution.

It filters out malicious code.

✓ Which tool is commonly used to test for XSS vulnerabilities? * 1/1

- ○ Wireshark
- ◉ Burp Suite ✓
- ○ Nmap
- ○ Metasploit

✓ What is the risk of using document.write() with user input? * 1/1

- ◉ It can lead to XSS if the input is not sanitized. ✓
- ○ It deletes the entire document.
- ○ It encrypts user data.
- ○ It improves website performance.

✗ Which tag is commonly exploited in HTML Injection? * 0/1

- ◉ <img> ✗
- ○ <script>
- ○
- ○

Correct answer

- ◉ <script>

✓ Which method is effective in mitigating DOM-based XSS? * 1/1

- ○ Using SSL/TLS
- ◉ Sanitizing user input before updating the DOM ✓
- ○ Using strong passwords
- ○ Disabling browser cookies

✓ Which of the following tags is often misused in XSS attacks? * 1/1

- ○ <p>
- ○ <a>
- ◉ <script> ✓
- ○ <table>

✓ Which of the following is a sign that a website might be vulnerable to HTML Injection? *1/1

- ◉ User input appears exactly as entered without modification ✓
- ○ The website uses HTTPS
- ○ The website requires two-factor authentication
- ○ The site has a fast loading speed

✓ Which of the following is NOT a method to prevent HTML Injection? * 1/1

- Input validation
- Output encoding
- Accepting all HTML tags ✓
- Using security libraries

✓ What does HTML Injection typically target? * 1/1

- Web page structure ✓
- Database queries
- Network traffic
- Password encryption

✓ Which of the following is an example of Reflected XSS? * 1/1

- Injecting a script in a blog comment stored on the server
- Sending a malicious URL that displays an alert when clicked ✓
- Modifying the server-side database through SQL
- Creating a phishing site

✓ Which of the following is a safe practice to prevent XSS attacks? * 1/1

- Displaying raw user input
- Using HTTPS
- Encoding output data ✓
- Disabling cookies