week 3 quiz

Total points 27/30

✓ If a website does not implement CSRF protection, what type of attack can an attacker perform? * 1/1

○ Injection attacks

● Unauthorized actions on behalf of an authenticated user ✓

○ Session hijacking

○ Data interception

✓ How does a CSRF attack typically work? * 1/1

○ By using malicious JavaScript embedded in a page to steal credentials

● By embedding a fake form in a site visited by the target user ✓

○ By exploiting unvalidated input fields to send malicious payloads

○ By intercepting and modifying HTTP requests in transit

✓ Which of the following CORS headers allows servers to specify which domains can access their resources? * 1/1

● Access-Control-Allow-Origin ✓

○ Access-Control-Allow-Methods

○ Access-Control-Allow-Headers

○ Access-Control-Allow-Credentials

✓ Which HTTP method is most commonly exploited in a CSRF attack? * 1/1

● POST ✓

○ GET

○ DELETE

○ PUT

✓ What is a "preflight" request in CORS? * 1/1

○ A request that checks whether the origin is valid

● A request sent by the browser to ask the server whether the cross-origin request is allowed ✓

○ A request to fetch user credentials

○ A request to set custom headers

✓ What does CORS stand for? * 1/1

○ Cross-Origin Request Sharing

● Cross-Origin Resource Sharing ✓

○ Cross-Site Request Sharing

○ Cross-Origin Request Security

✓ Which of the following HTTP headers is used to specify the origin of a request in CORS? * 1/1

○ Accept

● Origin ✓

○ User-Agent

○ Content-Type

✓ Which header is used to allow cookies and credentials to be sent with cross-origin requests? *1/1

○ Access-Control-Allow-Method

○ Access-Control-Allow-Origin

● Access-Control-Allow-Credentials ✓

○ Access-Control-Expose-Headers

✓ Which of the following is a vulnerability in CSRF if the application does not implement proper token validation? *1/1

○ Blind SQL Injection

○ Insecure Direct Object References

○ Unauthenticated API requests

● CSRF attacks where an attacker can force an action on behalf of the user ✓

✓ Which of the following headers helps mitigate CSRF attacks by enforcing same-origin policies? *1/1

○ X-XSS-Protection

○ Content-Type

○ X-Frame-Options

● SameSite cookie attribute ✓

✓ Which HTTP method is commonly used in preflight CORS requests? * 1/1

○ POST

○ GET

○ PUT

● OPTIONS ✓

✓ Which CORS header can be used to expose specific response headers to the browser? *1/1

○ Access-Control-Allow-Origin

● Access-Control-Expose-Headers ✓

○ Access-Control-Allow-Methods

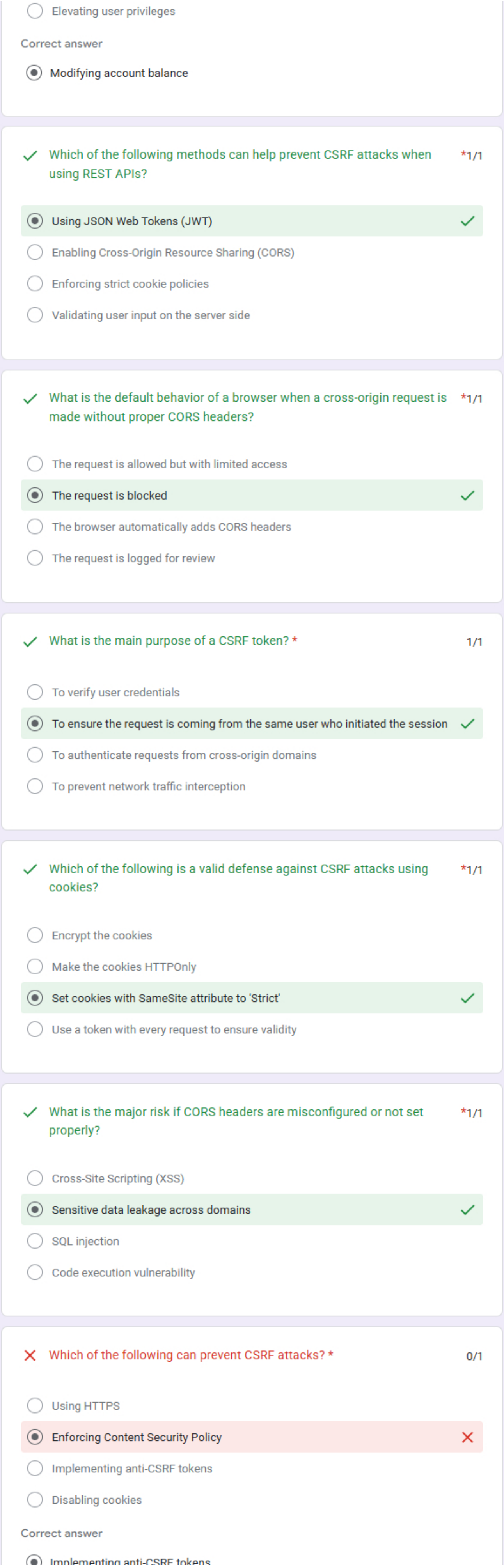
○ Access-Control-Allow-Credentials

✗ Which kind of attack would CSRF be particularly dangerous against in a banking application? *0/1

○ Modifying account balance

○ Exploiting session fixation

● Performing a cross-site scripting attack ✗



○ Elevating user privileges

Correct answer

● Modifying account balance

✓ Which of the following methods can help prevent CSRF attacks when using REST APIs? * 1/1

● Using JSON Web Tokens (JWT) ✓

○ Enabling Cross-Origin Resource Sharing (CORS)

○ Enforcing strict cookie policies

○ Validating user input on the server side

✓ What is the default behavior of a browser when a cross-origin request is made without proper CORS headers? * 1/1

○ The request is allowed but with limited access

● The request is blocked ✓

○ The browser automatically adds CORS headers

○ The request is logged for review

✓ What is the main purpose of a CSRF token? * 1/1

○ To verify user credentials

● To ensure the request is coming from the same user who initiated the session ✓

○ To authenticate requests from cross-origin domains

○ To prevent network traffic interception

✓ Which of the following is a valid defense against CSRF attacks using cookies? * 1/1

○ Encrypt the cookies

○ Make the cookies HTTPOnly

● Set cookies with SameSite attribute to 'Strict' ✓

○ Use a token with every request to ensure validity

✓ What is the major risk if CORS headers are misconfigured or not set properly? * 1/1

○ Cross-Site Scripting (XSS)

● Sensitive data leakage across domains ✓

○ SQL injection

○ Code execution vulnerability

✗ Which of the following can prevent CSRF attacks? * 0/1

○ Using HTTPS

● Enforcing Content Security Policy ✗

○ Implementing anti-CSRF tokens

○ Disabling cookies

Correct answer

● Implementing anti-CSRF tokens

○ Implementing anti-CSRF tokens

✓ How can a CSRF attack target a user who is authenticated on a website? * 1/1

○ By injecting malicious content into the web page visited by the user

○ By using a cross-origin script to read the user's cookies

● By sending unauthorized requests with the user's credentials without their knowledge ✓

○ By forcing the user to log out of the website

✓ Which of the following scenarios would require a preflight CORS request? * 1/1

○ A simple GET request without custom headers

● A POST request with a custom Content-Type ✓

○ A GET request to a same-origin resource

○ A GET request with no headers

✓ Which of the following describes the correct setting for the Access-Control-Allow-Origin header when a server allows requests from multiple origins? * 1/1

● Set to "*" ✓

○ Set to a list of origins separated by commas

○ Set to the domain of the client

○ It is not allowed to allow multiple origins

✓ Which technique is commonly used in a CSRF attack to bypass the Same-Origin Policy? * 1/1

○ DNS poisoning

● Image-based request ✓

○ XMLHttpRequest

○ Cookie hijacking

✓ Which of the following is an example of a CSRF attack? * 1/1

● Changing a user's password without their knowledge ✓

○ Stealing a user's credentials via a keylogger

○ Man-in-the-middle attack to alter requests

○ Phishing an email to steal personal information

✓ Which of the following CORS headers specifies the HTTP methods allowed for cross-origin requests? * 1/1

○ Access-Control-Allow-Headers

● Access-Control-Allow-Methods ✓

○ Access-Control-Expose-Headers

○ Access-Control-Allow-Origin

✓ Which HTTP status code indicates that the server successfully handled the CORS request? * 1/1

● 200 OK ✓

○ 403 Forbidden

○ 401 Unauthorized

○ 405 Method Not Allowed

✓ What does CSRF stand for? * 1/1

○ Cross-Site Resource Forgery

● Cross-Site Request Forgery ✓

○ Cross-Security Request Forgery

○ Cross-Server Request Forgery

✓ Which of the following could result in a CORS error? * 1/1

○ Not including an Authorization header in a GET request

● The server does not include Access-Control-Allow-Origin header ✓

○ The client does not include a User-Agent header

○ The response code is 500

✗ Which of the following techniques would NOT mitigate CSRF attacks effectively? *0/1

● Anti-CSRF tokens ✗

○ User-agent validation

○ SameSite cookie attribute

○ Custom request headers

Correct answer

● User-agent validation

✓ What is the purpose of the Access-Control-Allow-Headers header in CORS? *1/1

○ To specify which HTTP methods are allowed

● To specify the headers allowed in the actual request ✓

○ To expose specific headers to the browser

○ To allow credentials to be included in the request