Valnara Security Scan Report

Scan Details:

Target URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Scan Type: Passive Scan
Scan Depth: 5
Start Time: 2025-04-08 10:35:53
End Time: 2025-04-08 10:36:12

Risk Summary:

Medium Risk Vulnerabilities: 2
Low Risk Vulnerabilities: 31
Informational Risk Vulnerabilities: 7

Detailed Vulnerabilities:

Session Management Response Identified
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Multiple X-Frame-Options Header Entries
Risk Level: Medium
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure only a single X-Frame-Options header is present in the response.

Re-examine Cache-control Directives
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Cookie No HttpOnly Flag

Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie No HttpOnly Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie No HttpOnly Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie No HttpOnly Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie No HttpOnly Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie No HttpOnly Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie No HttpOnly Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the HttpOnly flag is set for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute

Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie Without Secure Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cookie Without Secure Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cookie Without Secure Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cookie Without Secure Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cookie Without Secure Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cookie Without Secure Flag
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cross-Domain JavaScript Source File Inclusion
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Information Disclosure - Suspicious Comments
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Information Disclosure - Suspicious Comments
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Modern Web Application
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: This is an informational alert and so no changes are required.

Timestamp Disclosure - Unix
Risk Level: Low

URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Timestamp Disclosure - Unix
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Timestamp Disclosure - Unix
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Timestamp Disclosure - Unix
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

User Controllable HTML Element Attribute (Potential XSS)
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Validate all input and sanitize output it before writing to any HTML attributes.

X-Content-Type-Options Header Missing
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Session Management Response Identified
Risk Level: Informational
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Timestamp Disclosure - Unix
Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Timestamp Disclosure - Unix

Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Timestamp Disclosure - Unix

Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Timestamp Disclosure - Unix

Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Test Vulnerability

Risk Level: Low
URL:
https://www.iq.zain.com/en?gad_source=1&gbraid;=0AAAAADxYlkUJmVGWboe0w9Xg7hT7iRMJd
Remediation: This is a test vulnerability added to verify the results display is working.