Arxscan Vulnerability Reference AVD-2024-062401

Cross-Site Scripting

Likelihood: High

Target: Web Application CWE CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Impact: High Type: Injection CAPEC CAPEC-63: Cross-Site Scripting (XSS)

CVSS Score: 7.6 Tactic: Execution

MITRE ATTACK T1189: Drive-by Compromise

Published: July 17, 2024 Last Updated: July 17, 2024

Description

Redbot Security uncovered a significant vulnerability in the form of stored cross-site scripting (XSS) across multiple input fields within the web application. Specifically, the 'Region Name', 'First Name', and 'Last Name' fields were identified as susceptible to processing user-supplied JavaScript and HTML. This vulnerability allows attackers to inject malicious scripts into these fields, which are then executed by other users who view the infected content. This XSS vulnerability exposes the application and its users to various security threats, including session hijacking, redirection to malicious websites, and unauthorized access to sensitive information. Since all text fields capable of accepting and reflecting user input were vulnerable, the potential for widespread exploitation is significantly increased, posing a severe security risk to the entire user base.

Affected Resource(s)

Arxview Version 2.1.15086

Remediation

Update the Arxview Solution to Version 2..1.15108 or greater

Mitigations and Workarounds

None

Detections

None