Technical Details of Identified Web Application Vulnerabilities

#	Vulnerability	Risk Level	Status
1	SQL Injection	High	Open
2	Cross-Site Scripting (XSS)	Medium	Open
3	Broken Authentication	High	Resolved

1. SQL Injection

Description: User input is not properly sanitized before being included in database queries, allowing attackers to alter query logic.
Location: /login
Proof of Concept: `' OR 1=1--`

Impact: Database exposure including sensitive user data. Potential for data manipulation or deletion.

Recommendation: Use parameterized queries or prepared statements to handle user input.

2. Cross-Site Scripting (XSS)

Description: Application does not properly encode user-supplied data before rendering in HTML.
Location: /profile
Proof of Concept: `<script>alert('xss')</script>`

Impact: Session hijacking, credential theft, and defacement.

Recommendation: Encode all user-supplied data before rendering it in the browser.

3. Broken Authentication

Description: Insufficient password complexity requirements and insecure session management.
Location: /login, /session
Proof of Concept: Reuse of session tokens allows access without re-authentication.

Impact: Unauthorized access to user accounts.

Recommendation: Enforce strong password policies and implement secure session invalidation on logout.