1. Vulnerability Findings Summary

Web Application A

Vulnerability Type	Severity	Count	Risk	Recommendation
Access Control Weakness	Critical	1	Unauthorized account access	Implement rate limiting and account lockout mechanisms
Cross-Site Scripting (XSS)	Critical	1	Client-side compromise	Apply strict input sanitization and output encoding
Insecure Direct Object Reference (IDOR)	Medium	1	Unauthorized data access	Enforce authorization checks on every request

---

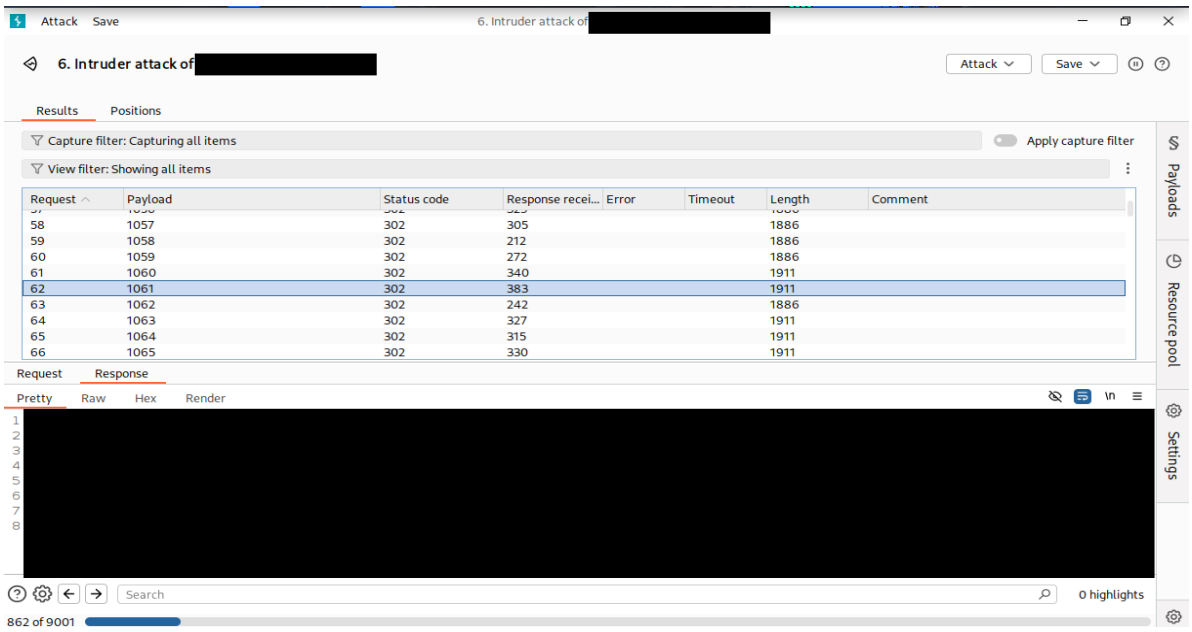
Web Application B

Vulnerability Type	Severity	Count	Risk	Recommendation
HTTP/2 Resource Exhaustion (DoS)	High	1	Service disruption	Apply rate limiting, server hardening, and upstream traffic filtering

---

2. Evidence, Risk, and Remediation (Sanitized)

Access Control Weakness

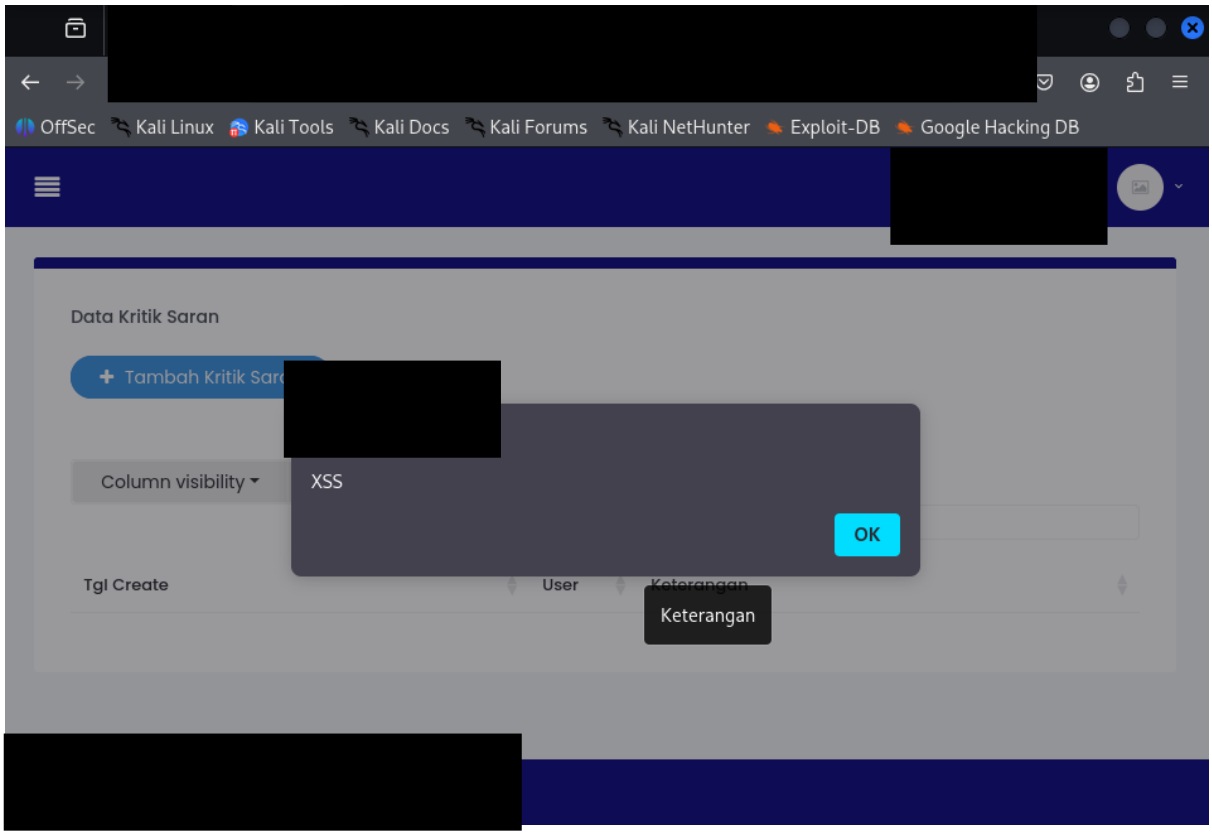


Evidence:
During an authorized blackbox security assessment, an access control weakness was identified on a web application. The issue allowed repeated authentication attempts without sufficient restriction due to weak credential management and absence of rate limiting mechanisms.

Risk:
If left unmitigated, this weakness may lead to unauthorized access, account compromise, financial loss, identity misuse, and increased exposure to targeted attacks.

Recommendation:

- Implement rate limiting on authentication endpoints
- Apply account lockout policies
- Enforce CAPTCHA or similar anti-automation controls



Cross-Site Scripting (XSS)

Evidence:
An input validation flaw was identified where user-supplied input was processed without sufficient sanitization. This allowed injection of malicious client-side scripts under controlled testing conditions.

Risk:
Potential impacts include session hijacking, unauthorized actions on behalf of users, data exposure, reputational damage, and legal consequences.

Recommendation:

- Enforce strict input validation
- Apply output encoding
- Implement Content Security Policy (CSP) where applicable

Resource Exhaustion / Denial of Service

Evidence:
The assessment identified insufficient controls against high-volume request bursts, enabling resource exhaustion scenarios that could impact application availability.

Risk:
Service downtime, operational disruption, financial loss, and reputational damage.

Recommendation:

- Apply request rate limiting
- Harden server configurations
- Utilize CDN or WAF protections

Insecure Direct Object Reference (IDOR)

Evidence:
Authorization checks were not consistently enforced when accessing object references. Under controlled testing, predictable identifiers allowed access beyond intended authorization scopes.

Risk:
Unauthorized data access, data manipulation, privacy violations, and regulatory exposure.

Recommendation:

- Enforce authorization validation per request
- Use non-predictable object identifiers
- Verify requester ownership before data access

---

3. Executive Summary

A security assessment was conducted on two anonymized web applications under authorized testing conditions. Multiple security weaknesses were identified, including access control issues, input validation flaws, and availability-related risks.

The findings demonstrate common security gaps that may lead to unauthorized access, data exposure, and service disruption if not remediated. Practical remediation guidance was provided to reduce risk, improve security posture, and align with industry best practices such as OWASP recommendations.

This assessment focused on responsible disclosure, risk-based analysis, and enterprise security considerations rather than exploitation.