URL Parameter Manipulation & HTTP Response Analysis

Authorized Security Testing Case Study

Prepared By: Bablu Kumar
Date: 13 February 2026

---

1. Executive Summary

This report documents the analysis of URL parameters and HTTP response behavior identified during authorized security testing conducted under responsible disclosure guidelines.

The objective of this assessment was to evaluate how user-controlled parameters are processed by the server and to analyze potential risks related to improper validation or access control weaknesses.

2. Scope of Testing

- Testing conducted within authorized scope
- Non-destructive parameter manipulation only
- No data extraction or service disruption
- Responsible disclosure practices followed

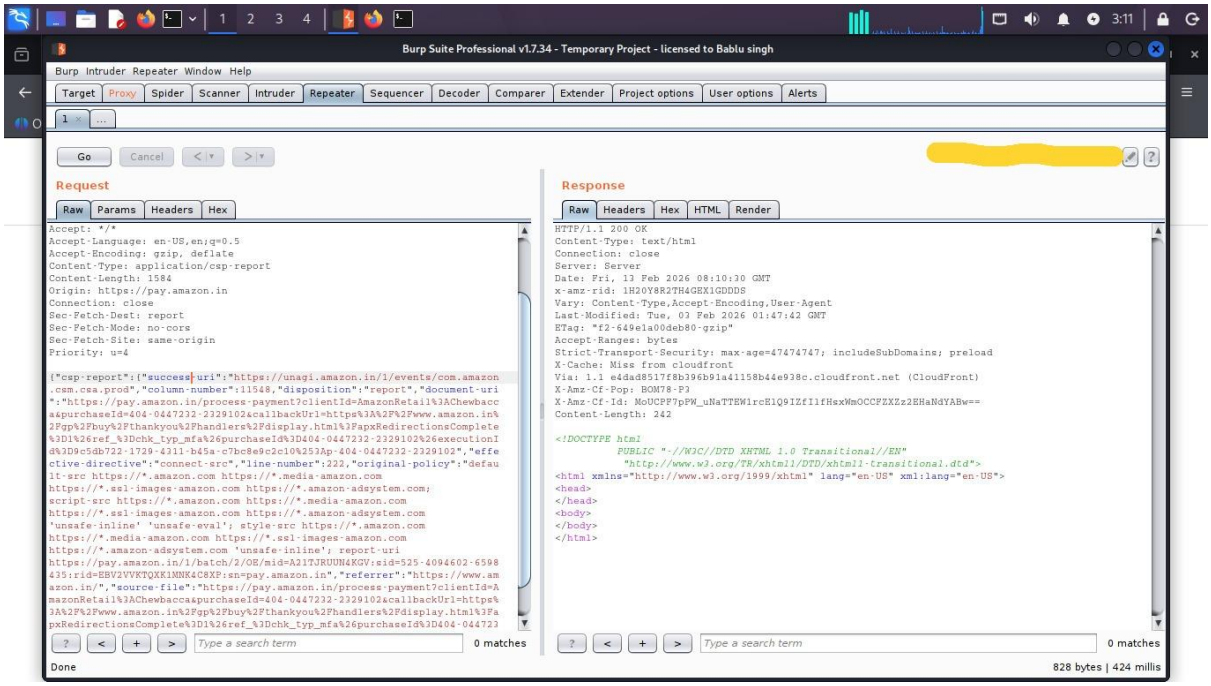
3. Tools Used

- Kali Linux
- Burp Suite Professional v1.7.34
- Mozilla Firefox
- Manual HTTP Request Analysis

4. Methodology

4.1 Traffic Interception

Browser traffic was routed through Burp Suite proxy to capture HTTP requests.



4.2 Parameter Identification

Identified parameters in the request:

Parameter	Category	Risk
user_id	Identifier	Potential IDOR
role	Access Control	Privilege Escalation
page	Pagination	Enumeration Risk

4.3 Parameter Manipulation

Controlled parameter modification was performed to observe server-side validation.

Example (Sanitized):

Original:

user_id=1002

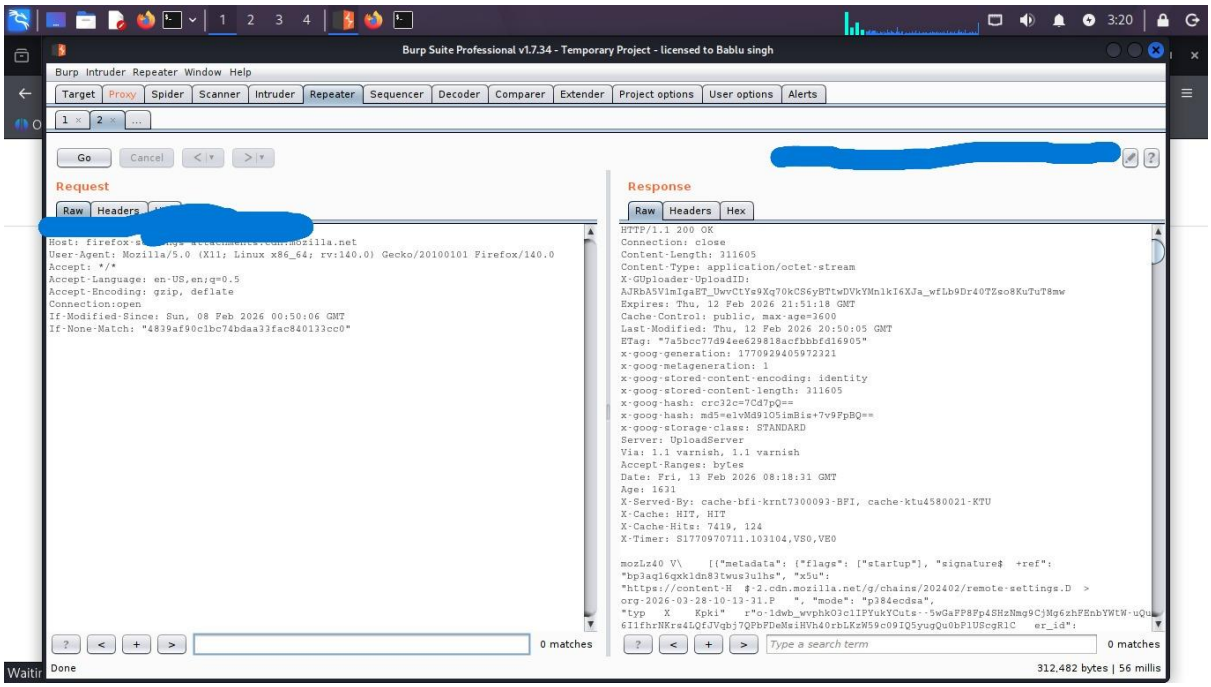
Modified:

user_id=1005

4.4 Response Analysis

The server response was analyzed for:

- HTTP Status Codes
- Content-Length differences
- Redirect behavior
- Security headers (HSTS, CSP, etc.)



5. Risk Evaluation

Improper validation of URL parameters may lead to:

- Broken Access Control
- Insecure Direct Object References (IDOR)
- Privilege Escalation
- Business Logic Manipulation

6. Security Recommendations

- Implement strict server-side validation
- Enforce role-based authorization checks
- Avoid exposing sensitive identifiers in URLs
- Centralize access control logic
- Log abnormal parameter changes

7. Learning Outcomes

- Practical experience with HTTP request manipulation
- Improved understanding of access control validation
- Enhanced professional vulnerability documentation skills

8. Ethical Statement

All activities described in this report were conducted within authorized testing scope under responsible disclosure guidelines. No unauthorized exploitation was performed.