# Burp Suite Security Assessment Report

## Project Name:

Your Application Name Here

## Tested URL / Application:

https://your-app-url.com or APK version details

## Testing Tools:

- Burp Suite Professional / Community Edition  
- Manual security validation  
- OWASP Top 10 compliance checks

## Testing Date:

## Testing Scope:

- Web application penetration testing  
- API endpoint security testing  
- Authentication and authorization verification  
- SSL/TLS security analysis

## Summary of Findings:

Total Issues Found:   
Critical:   
High:   
Medium:   
Low:

## Detailed Issues and Recommendations:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Issue ID | Issue Description | Severity | Affected URL / Endpoint | Evidence / Screenshot | Recommendation |
| BURP-001 | SQL Injection vulnerability in login POST request. | Critical | /api/login | screenshot-login-sqli.png | Use parameterized queries and sanitize user inputs. |

## Conclusion:

The Burp Suite security assessment identified vulnerabilities that range from critical to medium severity. Immediate remediation is recommended for authentication-related issues, data leakage, and misconfigurations. A retest should be conducted after fixes have been applied.