API Security Assessment Report Template

Security Assessment Team

November 25, 2025

Abstract

This is a template for API security assessment reports. Replace all placeholders with actual assessment data. Always ensure proper authorization before conducting security assessments.

Contents

1 Executive Summary

1.1 Assessment Overview

This template provides a structure for documenting API security assessments. Replace all bracketed content with actual findings from authorized security testing.

1.2 Risk Summary

Severity	Vulnerability Type	Count
Critical	Authentication Bypass	[COUNT]
High	Data Exposure	[COUNT]
Medium	Security Misconfiguration	[COUNT]
Low	Information Disclosure	[COUNT]

1.3 Key Findings Template

- [**SEVERITY**]: [VULNERABILITY TYPE] - [BRIEF DESCRIPTION]
- [**SEVERITY**]: [VULNERABILITY TYPE] - [BRIEF DESCRIPTION]
- [**SEVERITY**]: [VULNERABILITY TYPE] - [BRIEF DESCRIPTION]

2 Methodology

2.1 Testing Approach

This section documents the security testing methodology used during the assessment.

2.2 Testing Scope

- `[DOMAIN]` - Frontend application
- `[API-DOMAIN]` - Backend API services
- Authentication and authorization mechanisms
- API endpoint security testing

2.3 Security Standards

- OWASP API Security Top 10
- Industry security best practices
- Compliance requirements as applicable

3 Detailed Findings

3.1 [SEVERITY]: [VULNERABILITY NAME]

3.1.1 Risk Rating

- **Severity**: [SEVERITY LEVEL]
- **Impact**: [IMPACT LEVEL]
- **Likelihood**: [LIKELIHOOD LEVEL]

3.1.2 Description

[Detailed vulnerability description goes here. Replace with actual finding details.]

3.1.3 Evidence

```
[Sample request/response or code snippet]
[Replace with actual evidence from assessment]
```

3.1.4 Impact

Impact point 1

Impact point 2

Impact point 3

3.1.5 Remediation

Remediation step 1

Remediation step 2

Remediation step 3

4 Technical Details

4.1 API Architecture

- **Frontend**: [Technology stack]
- **Backend**: [API technology]
- **Authentication**: [Auth mechanism]
- **Data Storage**: [Database type]

4.2 Discovered Endpoints

Endpoint	Method	Function
`[/api/endpoint]`	[METHOD]	[Description]
`[/api/endpoint]`	[METHOD]	[Description]
`[/api/endpoint]`	[METHOD]	[Description]

5 Remediation Recommendations

5.1 Immediate Actions (0-30 days)

1. [**Priority**]: [Action description]
2. [**Priority**]: [Action description]
3. [**Priority**]: [Action description]

5.2 Short-term Actions (1-3 months)

Action description

Action description

Action description

5.3 Long-term Improvements (3-6 months)

Action description

Action description

Action description

6 Conclusion

This assessment identified several security vulnerabilities requiring attention. The findings in this report should be addressed according to their risk priority to improve the overall security posture.

7 Appendices

7.1 Testing Tools

Tool 1 - [Purpose]

Tool 2 - [Purpose]

Tool 3 - [Purpose]

7.2 References

- OWASP API Security Top 10
- Industry security standards
- Compliance requirements