

API Security Assessment Report

Generated on: May 30, 2025 at 01:46

Comprehensive Automated Security Testing

CONFIDENTIAL SECURITY ASSESSMENT

This report contains sensitive security information about potential vulnerabilities in the tested API. This document should be treated as confidential and shared only with authorized personnel responsible for system security.

Executive Summary

| Metric | Value |
|---------------------------------|-----------|
| Total Endpoints Discovered | 21 |
| Total Tests Executed | 31 |
| High Severity Vulnerabilities | 1 |
| Medium Severity Vulnerabilities | 0 |
| Low Severity Vulnerabilities | 0 |
| Overall Risk Level | HIGH RISK |

Risk Assessment:

The API has 1 high-severity vulnerabilities that pose immediate security risks and should be addressed urgently.

Vulnerability Findings

High Severity Vulnerabilities

1. Unknown - Unknown endpoint

Description: The application allows registration with the same email address but different case (e.g., User1@example.com vs user1@example.com). This could lead to account takeover or identity confusion.

Evidence:

```
Successfully registered with 'User1@example.com' when 'user1@example.com' already exists
```

Impact: Impact assessment not available

Endpoint Coverage Analysis

Coverage Summary:

- Total Endpoints Discovered: 21
- Endpoints Successfully Tested: 0
- Coverage Percentage: 0.0%

Discovered Endpoints:

| Method | Endpoint | Status |
|--------|--|--------------|
| POST | /api/users | ✗ Not Tested |
| POST | /api/v2/users/login | ✗ Not Tested |
| GET | /api/user | ✗ Not Tested |
| PUT | /api/user | ✗ Not Tested |
| POST | /api/membership | ✗ Not Tested |
| GET | /api/profiles/{username} | ✗ Not Tested |
| POST | /api/profiles/{username}/follow | ✗ Not Tested |
| DELETE | /api/profiles/{username}/follow | ✗ Not Tested |
| GET | /api/articles/feed | ✗ Not Tested |
| POST | /api/articles/{slug}/favorite | ✗ Not Tested |
| DELETE | /api/articles/{slug}/favorite | ✗ Not Tested |
| GET | /api/articles | ✗ Not Tested |
| POST | /api/articles | ✗ Not Tested |
| GET | /api/articles/{slug} | ✗ Not Tested |
| PUT | /api/articles/{slug} | ✗ Not Tested |
| DELETE | /api/articles/{slug} | ✗ Not Tested |
| POST | /api/debug | ✗ Not Tested |
| GET | /api/articles/{slug}/comments | ✗ Not Tested |
| POST | /api/articles/{slug}/comments | ✗ Not Tested |
| DELETE | /api/articles/{slug}/comments/{comment_id} | ✗ Not Tested |
| GET | /api/tags | ✗ Not Tested |

Technical Details & Evidence

Test Execution Summary:

Test 1:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 2:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 3:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 4:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 5:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 6:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 7:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 8:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 9:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Test 10:

Scenario ID: Status Code: 0 Success: False Response Length: 0 characters Response Preview: ...

Security Recommendations

Immediate Actions Required:

- Immediately patch all high-severity vulnerabilities
- Review and strengthen authentication mechanisms
- Implement proper authorization checks for all endpoints
- Review debug endpoint access controls
- Ensure proper error handling without information disclosure

Long-term Security Improvements:

- Implement automated security testing in CI/CD pipeline
- Regular security code reviews and penetration testing
- Deploy Web Application Firewall (WAF)
- Implement comprehensive logging and monitoring

Best Practices Implementation:

- Follow OWASP API Security Top 10 guidelines
- Implement rate limiting and throttling
- Use secure communication protocols (HTTPS)
- Regular security training for development team
- Maintain updated security documentation