API Security Assessment: Authorization and Access Control Testing

Intern name: Cinchana S
Date: 23-01-2026

Executive Summary

An API security assessment was performed against the DVWA REST API to identify authorization and authentication weaknesses. Manual testing revealed a Broken Object Level Authorization (BOLA) vulnerability, allowing unauthorized access to user data by manipulating object identifiers. The issue persisted even after authentication tokens were removed and security controls were hardened.

Scope

1. **Target Application:** DVWA REST API
2. **API Version:** v1
3. **Endpoints Tested:**

- `/api/v1/user/1`
- `/api/v1/user/2`
- `/api/v1/user/{id}`

Tools Used:

- Postman
- Burp Suite

Methodology (Execution)

Endpoint Enumeration

- Identified accessible REST API endpoints returning JSON responses.
- Verified API behavior through direct requests.

Authorization Testing (BOLA)

- Modified object identifiers within API endpoints.
- Observed responses for unauthorized data access.

Authentication Bypass Testing

- Removed session cookies and authentication tokens.
- Retested API endpoints without authentication.
- Validated server responses.

Security Control Validation

- Increased DVWA security level from *Low* to *High*.
- Repeated authorization and authentication tests

Findings

Test ID	Vulnerability	Severity	Endpoint
001	Broken Object Level Authorization (BOLA)	High	/api/v1/user/{id}
002	Authentication Bypass	High	/api/v1/user/{id}

Attack Execution Log

Step	Action	Result
1	Accessed /api/v1/user/1	User data returned
2	Modified endpoint to /api/v1/user/2	Other user data exposed
3	Removed authentication cookies	Data still returned
4	Changed security level to High	Vulnerability persisted

Impact

An attacker can enumerate and extract sensitive user data without proper authorization. This enables data leakage, privacy violations, and supports further attack chaining.

Remediation

- Enforce object-level authorization checks on all API requests
- Validate authenticated user ownership of requested resources
- Reject unauthenticated requests with proper HTTP status codes
- Apply consistent access control across all security levels

Conclusion

The DVWA REST API is vulnerable to Broken Object Level Authorization due to missing server-side access control. The vulnerability allows unauthorized access to user data and remains exploitable even under hardened security settings.

Summary

During API testing, I identified that user data could be accessed by simply changing object IDs in API endpoints. Even after removing authentication cookies and increasing the security level, the API continued returning valid user data. This confirmed a Broken Object Level Authorization vulnerability caused by missing server-side authorization checks.