Antigravity Scanner

EXECUTIVE SUMMARY

Target: http://testasp.vulnweb.com

Scan ID: AG-900E2084

Scan Date: 2026-01-31 01:00:57

Findings: 1 vulnerabilities detected

Overall Status

VULNERABLE

- Detected 1 security issue(s) requiring attention.
- Immediate remediation recommended for critical findings.
- Review each finding below for detailed impact analysis.
- Prioritize fixes based on severity and exploitability.

DETAILED FINDINGS

Finding #1: Insecure Direct Object Reference (IDOR)

HIGH

CWE: CWE-639

CVSS Score: 8.6 (High)

CVSS Score: 8.6 (High)

Description:

- Application exposes internal object references without authorization checks.
- Attackers can access resources belonging to other users.
- Object IDs are predictable and not properly validated.

Impact:

- Unauthorized access to other users' data.
- Privacy breach affecting multiple users.
- Potential for mass data harvesting.
- Regulatory compliance violations (GDPR, etc.).

Evidence:

```
{"admin": true}
```

Remediation:

- Implement proper authorization checks on all resource access.
- Use indirect references or UUIDs instead of sequential IDs.
- Validate user permissions before returning data.
- Log and monitor access patterns for anomalies.

Recommended Code Fix:

```
    # VULNERABLE CODE:
@app.get("/user/{user_id}")
def get_user(user_id: int):
    return db.get_user(user_id)

# SECURE CODE:
@app.get("/user/{user_id}")
def get_user(user_id: int, current_user: User):
    if user_id != current_user.id and not current_user.is_admin:
        raise HTTPException(403, "Access denied")
    return db.get_user(user_id)
```

Antigravity Scanner

RECOMMENDATIONS

Immediate Actions

- Review and patch all identified vulnerabilities.
- Implement input validation on all user-facing endpoints.
- Enable comprehensive logging for security events.
- Conduct code review for similar vulnerability patterns.

Long-term Security Measures

- Establish regular penetration testing schedule.
- Implement automated security scanning in CI/CD pipeline.
- Train development team on secure coding practices.
- Deploy Web Application Firewall (WAF) for additional protection.
- Implement rate limiting on authentication endpoints.

SCAN TIMELINE

- [Orchestrator] TARGET_ACQUIRED - 2026-01-31 00:57:44
- [Sigma] JOB_ASSIGNED - 2026-01-31 00:57:44
- [Beta] LOG - 2026-01-31 00:57:44
- [Gamma] VULN_CONFIRMED - 2026-01-31 00:57:44
- [Kappa] GI5_LOG - 2026-01-31 00:57:44