Vulnerability | Browser View | HTTP Request / Response

Controlled Scan | Retest | Send to Request Builder | Generate WAF Rules ▾ | Execute SQL Commands | Get Shell | LFI Exploitation | Generate Exploit

Start a New Website or Web Service Scan ✕

Target Website or Web Service URL

http://zero.webappsecurity.com/ ▾ 🔍 | **Previous Settings** ▾

⌃ **Options**

Scan Settings

🔧 **General**

🕷 **Scope**

🌐 **Additional Websites**

🔗 **Imported Links**

🔗 **URL Rewrite**

Authentication

🔑

✅ **Form**

🔑 **Basic, NTLM/Kerberos**

💬 **Client Certificate**

Scan Policy

Extensive Security Checks 🟨 ⋯ ✏

| **Default Security Checks** |
| Default Security Checks ◆ DOM XSS |
| **Extensive Security Checks** |
| AllOS-AllWebServer-AllAppServer-AllDBServer |
| AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other 1 |
| AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other 2 |
| AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other 3 |

eatures and bug fixes. Here are son

Crawling

☑ **Find & Follow New Links**

☑ **Enable Crawl & Attack at the Same Time**

☐ Pause Scan After Crawling

☐ Incremental Scan

Start Scan ▾ | **Cancel**

Group Issues by

🔵 **Vulnerability Type**

⚪ **Severity**

⚪ **Confirmation**

zero.webappsecurity.com

Scan

Concurrent Connections: 9
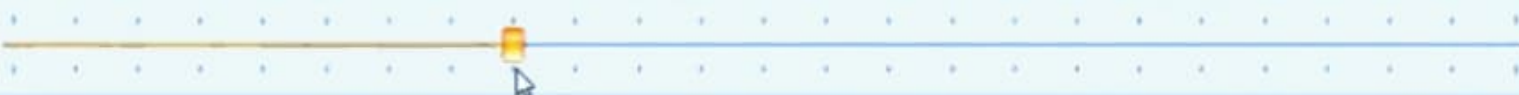
Activity

Passive Analysis (1)

GET   http://zero.webappsecurity.com/   1 s   Signatures   Analyzi...

ut of Ba

(Blind)

rce Sha

(Blind)

(DOM I

Scan

Vulnerability

Scan

Request Builder

Group Issues by

ⓘ Vulnerability Type

zero.webappsecurity.com

| CRITICAL (1) |
| MEDIUM (2) |
| LOW (4) |
| INFORMATION (7) |

Concurrent Connections: 23

Activity

Crawling (11)

GET	http://zero.webappsecurity.com/bank/	1 s	Reques...
GET	http://zero.webappsecurity.com/bank/account-...	1 s	Reques...
GET	http://zero.webappsecurity.com/bank/account-...	1 s	Reques...
GET	http://zero.webappsecurity.com/help.html	1 s	Reques...
GET	http://zero.webappsecurity.com/resources/js/b...	1 s	Reques...
GET	http://zero.webappsecurity.com/resources/js/jq...	1 s	Analyzi...
GET	http://zero.webappsecurity.com/resources/js/jq...	1 s	Parsing...
GET	http://zero.webappsecurity.com/resources/js/jq...	1 s	Reques...
GET	http://zero.webappsecurity.com/resources/js/jq...	1 s	Reques...
GET	http://zero.webappsecurity.com/sendFeedback...	1 s	Reques...
POST	http://zero.webappsecurity.com/sendFeedback...	1 s	Reques...

Static Resource Finder (1)

	http://zero.webappsecurity.com/crossdomain.x...	1 s

Singular (1)

	http://zero.webappsecurity.com/ [SSL]	3 s

Custom Not Found Analysis (1)

Group Issues by

- Vulnerability Type
- Severity

(left panel, partially visible)

d Scan

meters to Scan

urity Tests

aluation
aluation (Out of Ba
nd Injection
nd Injection (Blind)
rigin Resource Shar
e Scripting
e Scripting (Blind)
e Scripting (DOM I

Scan

Import Links... | Start Proxy...

Vulnerability | Browser View | HTTP Request / Response

Controlled Scan | Retest | Send to Request Builder | Generate WAF Rules ▾ | Execute SQL Commands | Get Shell | LFI Exploitation | Generate Exploit

Out-of-date Version (Tomcat)

CRITICAL ⚠

CERTAINTY	████████████
URL	http://zero.webappsecurity.com/resources/js/
IDENTIFIED VERSION	7.0.70 (contains 4 **critical** and 44 other vulnerabilities)
LATEST VERSION	10.0.5
VULNERABILITY DATABASE	Result is based on 22-04-2021 vulnerability database content.

✳ **CLASSIFICATION**

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
CAPEC	310

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of Tomcat.

REMEDY

Please upgrade your **installation of Tomcat to** the latest stable **version.**

---

led - Notepad

Format View Help