

# Vulnerability Assessment Report:

## http://zero.webappsecurity.com

### 1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http	1.1	open
443	https		open
8080	http	1.1	open

### 2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
-----
+ Target IP: 54.82.22.214
+ Target Hostname: zero.webappsecurity.com
+ Target Port: 80
+ Start Time: 2026-01-31 06:11:26 (GMT0)
-----
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ Server banner has changed from 'Apache-Coyote/1.1' to 'Apache/2.2.6 (Win32)
mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40' which may suggest a WAF, load balancer or
proxy is in place
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ 26 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2026-01-31 06:11:59 (GMT0) (33 seconds)
-----
+ 1 host(s) tested
```

### 3. Crawled Website Endpoints

- http://zero.webappsecurity.com/#carousel
- [FORM] http://zero.webappsecurity.com/search.html
- http://zero.webappsecurity.com/index.html

### 4. Vulnerabilities Detected

- Missing Security Headers

## 5. Vulnerability Intelligence (CVE Mapping)

### Vulnerabilities in Apache Tomcat/Coyote JSP engine 1.1

- [MEDIUM 5.0] CVE-2005-1753: ReadMessage.jsp in JavaMail API 1.1.3 through 1.3, as used by Apache Tomcat 5.0.16, allows remote attackers to view other users' e-mail attachments via...
- [MEDIUM 5.0] CVE-2005-1754: JavaMail API 1.1.3 through 1.3, as used by Apache Tomcat 5.0.16, allows remote attackers to read arbitrary files via a full pathname in the argument t...
- [MEDIUM 6.8] CVE-2012-3908: Multiple cross-site request forgery (CSRF) vulnerabilities in the ISE Administrator user interface (aka the Apache Tomcat interface) on Cisco Identity...
- [MEDIUM 5.9] CVE-2017-15698: When parsing the AIA-Extension field of a client certificate, Apache Tomcat Native Connector 1.2.0 to 1.2.14 and 1.1.23 to 1.1.34 did not correctly ha...
- [HIGH 7.4] CVE-2018-8019: When using an OCSP responder Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 did not correctly handle invalid responses. This allowed for re...

## 6. Attack Possibilities & Mitigation

**Attack:** Clickjacking / Cross-Site Scripting (XSS)

**Mitigation:** Implement X-Frame-Options and Content-Security-Policy headers.