Report on WebAppSecurity

Using Netsparker

Netsparker is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications and web services, and identify security flaws. Netsparker can scan all types of web applications, regardless of the platform or the language with which they are built.

Vulnerabilities:

The following vulnerabilities are founded by Netsparker in the website http://zero.webappsecurity.com

**Domain : ** webappsecurity

**Sub Domain : ** zero.webappsecurity

1.Password Transmitted over HTTP:

Vulnerability Details:

Netsparker detected that password data is being transmitted over HTTP.

Impact:

If an attacker can intercept network traffic, he/she can steal users' credentials.

Actions to Take:

Move all of your critical forms and pages to HTTPS and don't serve them over HTTP.

Rectify:

All sensitive data should be transferred over HTTPS instead of HTTP. Forms should be served over HTTPS. All aspects of the appliance that accept user input, ranging from the login process, should only be served over HTTPS.

2. Insecure Transportation Security Protocol Supported (SSLv2):

Vulnerability Details:

Netsparker detected that insecure transportation security protocol (SSLv2) is supported by your web server. SSLv2 has several flaws. For instance, your secure traffic may be observed after you have established it over SSLv2.

Impact:

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors. Also an attacker can exploit vulnerabilities like DROWN.

Rectify:

Configure your web server to disallow using weak ciphers. For Apache, you must modify the SSL Protocol directive within the httpd.conf.

For Microsoft IIS, you should make some changes on the system registry.

- Click Start, click Run, type regedt32 or type regedit, and then click OK.
- In Registry Editor, locate the following registry key: HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL2\

- Locate a key named "Server." If it doesn't exist, create it. Under the "Server" key, locate a DWORD value named "Enabled." If it doesn't exist, create it and set it to "0".

3.Out-of-date Version (Apache):

Vulnerability Details:

Netsparker identified you're using an out-of-date version of Apache.

Impact:

Since this is often an old version of the software, it's going to be at risk of attacks.

Rectify:

Please upgrade your installation of Apache to the newest stable version.

4. Expression Language Injection:

Vulnerability Details:

Netsparker identified a possible expression language injection, which occurs when computer file is evaluated by an expression language interpreter.

While Netsparker believes there's an expression language injection in here, it couldn't confirm it. There are often numerous reasons for Netsparker not having the ability to verify it. We strongly recommend investigating the problem manually to make sure it's an expression language injection and desires to be addressed.

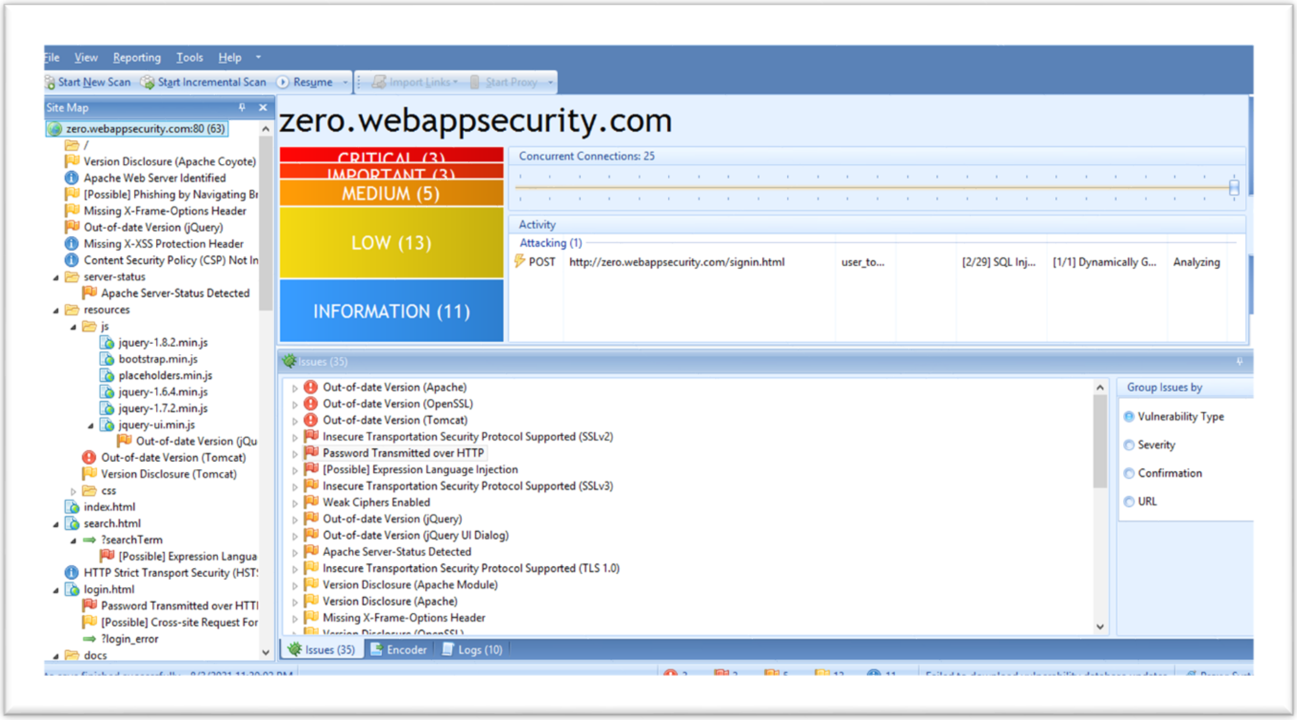
Impact:

An attacker can read server-side data, like the content of server-side variables, and a few other inner configuration details.

This is a quite dangerous vulnerability because developers assume their server-side code wouldn't be read by anyone outside, so that they may place sensitive information like passwords, connection strings, database queries, etc. It may be used for bypassing Http Only protection.

Rectify:

Apply input validation best practices to make sure there are no EL meta characters ("${" and "#{") in the input.


File View Reporting Tools Help
Start New Scan
Start Incremental Scan
Resume
Import Links
Start Proxy
Site Map
zero.webappsecurity.com:80 (63)
/
Version Disclosure (Apache Coyote)
Apache Web Server Identified
[Possible] Phishing by Navigating Br
Missing X-Frame-Options Header
Out-of-date Version (jQuery)
Missing X-XSS Protection Header
Content Security Policy (CSP) Not In
server-status
Apache Server-Status Detected
resources
js
jquery-1.8.2.min.js
bootstrap.min.js
placeholders.min.js
jquery-1.6.4.min.js
jquery-1.7.2.min.js
jquery-ui.min.js
Out-of-date Version (jQu
Out-of-date Version (Tomcat)
Version Disclosure (Tomcat)
css
index.html
search.html
?searchTerm
[Possible] Expression Langua
HTTP Strict Transport Security (HST
login.html
Password Transmitted over HTT
[Possible] Cross-site Request For
?login_error
docs
zero.webappsecurity.com
CRITICAL (3)
IMPORTANT (3)
MEDIUM (5)
LOW (13)
INFORMATION (11)
Concurrent Connections: 25
Activity
Attacking (1)
Issues (35)
Group Issues by
● Vulnerability Type
○ Severity
○ Confirmation
○ URL
Issues (35)
Encoder
Logs (10)

POST http://zero.webappsecurity.com/signin.html user_to... [2/29] SQL Inj... [1/1] Dynamically G... Analyzing

- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Tomcat)
- Insecure Transportation Security Protocol Supported (SSLv2)
- Password Transmitted over HTTP
- [Possible] Expression Language Injection
- Insecure Transportation Security Protocol Supported (SSLv3)
- Weak Ciphers Enabled
- Out-of-date Version (jQuery)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Version Disclosure (Apache Module)
- Version Disclosure (Apache)
- Missing X-Frame-Options Header
- Version Disclosure (OpenSSL)

The above screenshot shows the result analysized by the netsparker over the website http://zero.webappsecurity.com.