Task 2 (Aakash A aakashspike2001@gmail.com)

Target url : http://zero.webappsecurity.com/

Number of issues found : 33

Critical issues : 5

Medium issues : 7

Low issues : 11

Critical issues

- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Apache)

Password Transmitted over HTTP

Vulnerability Details

Netsparker detected that password data is being transmitted over HTTP.

If the password is *transmitted* from the user to the server as plaintext it could be intercepted as it travels across the network.

In this case a successful attack on the server would not only reveal the user's password, but all the passwords for all the users of the system.

Impact

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

Actions to Take

- Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server.
- Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed.
- These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.
- If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.
- Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Screenshot of the netsparker