NFR TESTING REPORT ( SECURITY )

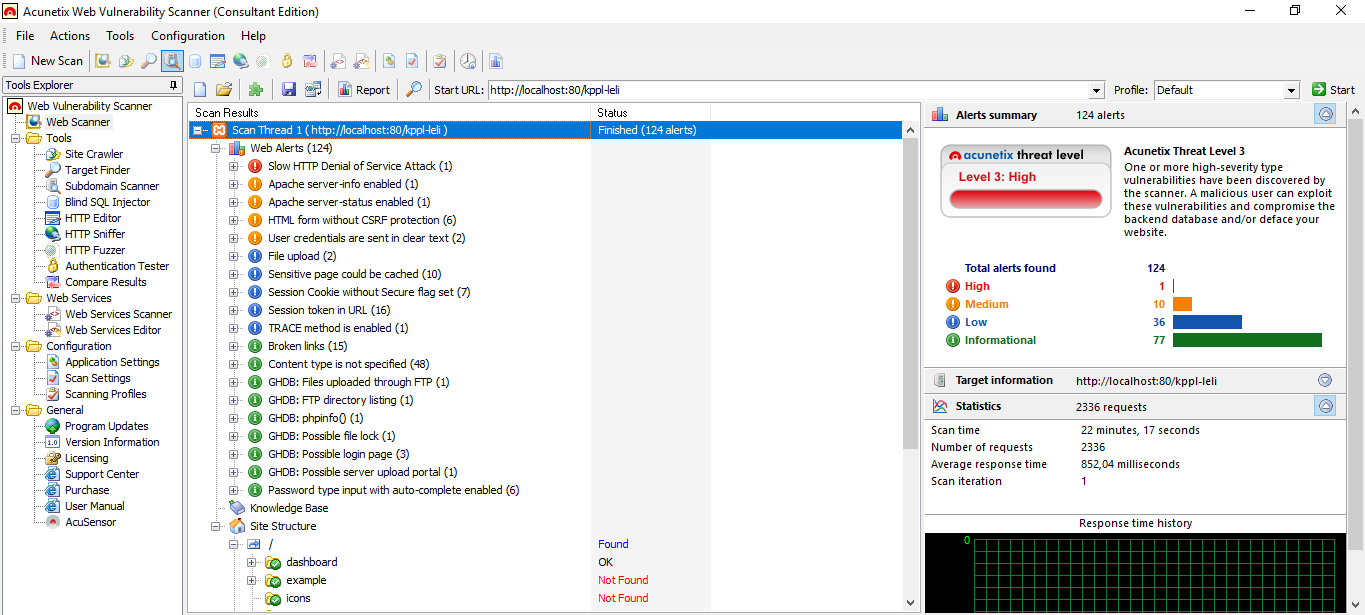
LELI

**METODE**

Non-Functional Requirement(NFR) testing yang telah dilakukan bertujuan untuk mengetes tingkat sekuritas dari website. Testing tersebut dilakukan dengan menggunakan Acunetix sebagai software tool security testing terhadap website LELI. Berikut adalah langkah-langkah yang dilakukan dalam melakukan testing :

1. Mengaktifkan Apache dan MySQL pada XAMPP Control Panel
2. Membuka aplikasi Acunetix
3. Memasukkan url **localhost/kppl-leli** sebagai target scan
4. Jalankan dan menunggu hasil report dari Acunetix

**HASIL**

****

**PEMBAHASAN**

Berdasarkan hasil report, website LELI memiliki tingkat security vulnerability tinggi atau High, yang menunjukkan bahwa banyak sekali cara yang dapat dilakukan penyerang dalam melakukan penyerangan pada website

**HIGH LEVEL VULNERABILITY**

Kerentanan sekuritas tingkat tinggi, sehingga dapat sangat membahayakan website

1. Slow HTTP Denial of Service Attack

Kerentanan ini menandakan bahwa website mengalami kendala performa ketika menerima serangan Denial of Service ( DoS ). Serangan dilakukan dengan interval sebesar 10,000 ms

**MEDIUM LEVEL VULNERABILITIES**

Kerentanan sekuritas tingkat menengah, cukup membahayakan website

1. Apache server-info Enabled

Konfigurasi apache dapat terlihat pada /server-info

1. Apache server-status Enabled

Konfigurasi apache dapat terlihat pada /server-status

1. HTML form without CSRF protection

Halaman HTML tidak memiliki proteksi dari serangan Cross Site Request Forgery ( CSRF )

1. User credentials are sent in clear text

Tidak adanya enkripsi yang memproteksi data-data confidential user sehingga sangat mudah untuk diambil oleh penyerang

**LOW LEVEL VULNERABILITIES**

Kerentanan sekuritas tingkat rendah, sedikit membahayakan website

1. File Upload

User dapat mengupload file yang dapat membahayakan jika tidak dihandle dengan baik, user dapat dengan sengaja mengupload virus atau sql injection

1. Sensitive page could be cached

Halaman-halaman yang mengandung informasi conidential dapat meninggalkan cookie atau Cache sehingga dapat dengan mudah diambil oleh penyerang

1. Session Cookie without secure flag set

Cookie tidak diatur menjadi private. Pada umumnya cookie dipertahankan oleh secure flag sehingga cookie hanya dapat diakses oleh SSL channel yang aman

1. Session token in URL

Session token website dapat terlihat pada url, dimana hal ini seharusnya hidden

1. TRACE method is enabled

HTTP TRACE method pada website ini aktif, yang dapat digunakan oleh penyerang untuk mendapatkan info seperti info autentikasi

**INFROMATIONAL LEVEL VULNERABILITIES**

Kerentanan sekuritas tingkat informational, tidak membahayakan website namun patut dimengerti

1. Broken links
2. Content type is not specified
3. GHBD : Files uploaded through FTP
4. GHBD : FTP Directory listing
5. GHBD : phpinfo()
6. GHBD : Possible file lock
7. GHBD : Possible login page
8. GHBD : Possible server upload portal
9. Password type input with auto-complete enabled