LAMPIRAN

Hasil s*ecurity assessment* pada web aplikasi Institusi Pendidikan XYZ.

1. Tabel Kerentanan

Dibawah ini akan dijelaskan mengenai temuan celah keamanan pada web aplikasi repositori institusi pendidikan XYZ menggunakan tool Nessus *Vulnerability Scanner*.

No	Tingkat	Nama	Deskripsi
1	*Medium*	*Apache Tomcat Default File*	Halaman kesalahan, beranda dan halaman contoh dari JSPs yang masih tersimpan di Apache Tomcat Server
2	*Medium*	*Web Application Potentially Vulnerable to Clickjacking*	Halaman web memungkinkan untuk dilakukan Clickjacking
3	*Low*	*Web Server Transmits Cleartext Credentials*	Perjalanan data sensitif seperti username dan password yang bisa dibaca dengan jelas (Cleartext)
4	*Low*	*Web Server Uses Basic Autentication Without HTTPS*	Halaman web menggunakan autentikasi standar dan belum menggunakan HTTPS
5	*Info*	*Nessus SYN scanner*	Beberapa port setengah terbuka; Port 22, 80 dan 5432
6	*Info*	*CGI Generic Injectable Parameter*	Memungkinkan halaman web untuk membaca parameter yang tidak berbahaya pada url

No	Tingkat	Nama	Deskripsi
7	*Info*	*External URLs*	Tool membaca link HREF yang mengarah ke situs luar
8	*Info*	*Web Application Cookies Not Marked Secure*	Cookie yang berjalan pada web ini tidak terautentikasi dan terkonformasi oleh pengguna
9	*Info*	*Web Mirroring*	Tool menggandakan web dan menjalankan CGI
10	*Info*	*Web Server Harvested Email Address*	Terdapat alamat email perorangan pada halaman web
11	*Info*	*Web Server Office File Inventory*	Beberapa file .pdf, .doc yang bisa diakses langsung dari url

2. Rancangan Penyerangan

Rancangan penyerangan adalah skenario yang dibuat oleh peneliti untuk melakukan simulasi serangan pada sistem web aplikasi repositori. Rancangan ini memanfaatkan dua celah keamanan. Penjelasan singkat mengenai rancangan penyerangan, akan dijabarkan pada tabel dibawah ini.

No	Tingkat	Nama	Alasan	*Tool*
1	*Info*	SYN *Scanner*	Untuk mengetahui port yang terbuka	Metasploit
2	*Low*	*Web Server Transmits Cleartext Credentials*	Untuk mengetahui *username* dan *password* dari pengguna	Arpspoof dan SSLStrip

3. Hasil Simulasi Penyerangan

Hasil yang didapatkan peneliti dari proses simulasi penyerangan yang dilakukan adalah sebagai berikut

No	Celah yang Diuji	Dampak	Tool	Success/Un
1	SYN Scanner	Port 5432 yang digunakan untuk postgresql ada kemungkinan untuk disusupi dan penyerang dapat melihat tabel dalam database	Metasploit	Unsuccess
2	Web Server Transmits Cleartext Credentials Paket	Paket yang berjalan dari dan menuju web aplikasi dapat dibaca secara jelas. Hal ini dapat dimanfaatkan untuk mencatat hak akses	Arpspoof dan SSLStrip	Success