LAMPIRAN

Hasil *Security Assessment* Web KRS Daring Institusi Pendidikan XYZ.

Lampiran I: Tabel Kerentanan

Dibawah ini akan dijelaskan mengenai temuan kerentanan keamanan pada Web KRS Daring Institusi Pendidikan XYZ menggunakan tool OWASP ZAP.

No.	Nama Kerentanan	*Level*	Deskripsi
1	*Anti CSRF Tokens Scanner*	*High*	Kerentanan ini mengindikasikan tidak ada mekanisme perlindungan token keamanan pada halaman web.
2	*Insecure Component – Microsoft-IIS 7.5*	*High*	Kerentanan ini mengindikasikan IIS masih menggunakan versi 7.5, saat ini IIS sudah versi 10.
3	*Viewstate without MAC Signature (Unsure)*	*High*	Kerentanan ini mengindikasikan situs web ini menggunakan ASP.NET *Viewstate* mungkin tanpa MAC (*Message Authentication Code*).
4	*Proxy Disclosure*	*Medium*	Kerentanan ini mengindikasikan satu *proxy server* terdeteksi informasi ini potensial membantu penyerang untuk menentukan: d. Daftar target untuk serangan terhadap aplikasi. e. Potensi kerentanan pada *server proxy* yang melayani aplikasi. f. Ada atau tidak adanya komponen yang mungkin menyebabkan serangan terhadap aplikasi untuk di deteksi, di cegah, atau dikurangi.

No.	Nama Kerentanan	*Level*	Deskripsi
5	*Reverse Tabnabbing*	*Medium*	Kerentanan ini mengindikasikan halaman Web KRS Daring bisa di kloning untuk serangan berupa *phising*.
6	*X-Frame-Options Header Not Set*	*Medium*	Kerentanan ini berpotensi terkena serangan *ClickJacking*.
7	*Absence of Anti-CSRF*	*Low*	Kerentanan ini mengindikasikan tidak ada token *Anti-CSRF* yang di temukan pada *HTML Submission Form*.
8	*Content Security Policy (CSP) Header Not Set*	*Low*	Kerentanan ini mengindikasikan pada *Content Security Policy (CSP)* tidak diaktifkan.
9	*Incomplete or No Cache-control and Pragma HTTP Header Set*	*Low*	Kerentanan ini memungkinkan data tersimpan di *cache*.
10	*Secure Pages Include Mixed Content*	*Low*	Kerentanan ini mengindikasikan halaman web dapat diakses melalui HTTP bukan HTTPS.
11	*Strict-Transport-Security Header Not Set*	*Low*	Kerentanan ini mengindikasikan pengalihan akses HTTPS ke HTTP dengan memasukkan sertifikat tidak *valid*.
12	*Web Browser XSS Protection Not Enabled*	*Low*	Kerentanan ini mengindikasikan *XSS Protection* tidak diaktifkan.
13	*X-AspNet-Version Response Header Scanner*	*Low*	Kerentanan ini mengindikasikan rentan terkena *sniffing* apabila menggunakan *web browser Internet Explorer* dan *Google Chrome* versi lama.

Lampiran II: Rancangan Serangan

Rancangan penyerangan adalah skenario yang dibuat oleh peneliti untuk melakukan simulasi serangan pada sistem Web KRS Daring. Rancangan ini memanfaatkan satu kerentanan keamanan. Penjelasan singkat mengenai rancangan penyerangan akan dijabarkan pada tabel dibawah ini.

Nama Kerentanan	***Level***	**Alasan**	***Tools***
Secure Pages Include Mixed Content	*Low*	Kerentanan ini bisa dimanfaatkan untuk mendapatkan akun nama pengguna dan kata sandi KRS Daring.	Arpspoof dan SSLStrip

Lampiran III: Hasil Simulasi Penyerangan

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

Kerentanan Keamanan	Dampak	Hasil Pengujian	Success/ Unsuccess
Secure Pages Include Mixed Content	Protocol HTTPS dapat dilemahkan dengan tools SSLStrip dan Arpspoof.	Penguji berhasil mendapatkan akun nama pengguna dan kata sandi Web KRS Daring dengan pendekatan *Social Engineering*.	Success