BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, berikut ini merupakan beberapa kesimpulan yang dapat diambil :

1. Hasil analisis dari penelitian ini menjabarkan bahwa website lembaga XYZ terdapat 8 celah keamanan. Dan hasil analisis metode CVSS dapat menentukan peringkat penanganan berdasarkan dampak potensial yang ditimbulkan akibat kerentanan dan celah keamanan website yang ada di lembaga XYZ. Dari temuan diatas dapat disimpulkan Scoring dan status tingkat kerentanan antara lain :

Tabel 5.2 Temuan Kerentanan

No.	Temuan	Status	Scoring
1.	Blind SQL Injection	Medium	6.8
2.	Cross Site Scripting	Medium	4.3
3.	SQL Injection	Medium	6.8
4.	Application Error Message	Medium	5.0
5.	HTML Form Without CSRF Protection	Low	2.6
6.	Multiple Vulnerabilities Fixed In PHP Versions	Low	0.0

	5.5.12 and 5.4.28		
7.	Same Site Scripting	Low	0.0
8.	User Credencial Are Sent In Clear Text	Medium	5.0

2. Menurut hasil yang ditunjukan dari perhitungan *CVSS* menunjukan bahwa website XYZ memiliki tingkatan risiko yang cukup tinggi dampaknya. dianjurkan untuk Lembaga XYZ untuk melakukan perbaikan guna meningkatkan keamanan website.

5.2 Saran

Berdasarkan temuan kerentanan diatas maka dapat disarankan penanganan yang harus dilakukan oleh lembaga XYZ adalah:

1. *Blind SQL Injection*

   Skrip program harus memfilter karakter meta dari input pengguna baik *meta tag* atau *meta description*.

2. *Cross Site Scripting*

   Script pada *website* disarankan untuk memfilter *metacharacter* dari *input user*. Dua tindakan penanggulangan paling penting untuk mencegah *cross-site scripting attacks* adalah *constrain input* (membatasi input karakter, validasi jenis *input*, *length*, *format*, and *range*) dan *encode output* (mengsandi atau mengkodekan output).

3. *SQL Injection*

   Skrip program harus memfilter karakter meta dari input pengguna baik meta tag atau meta description.

4. *Application error message*

Tinjau kembali *source code* untuk *script* yang terkena (ter-*affected*).

5. *HTML form without CSRF protection*

   Meningkatkan *firewall* dan menggunakan *SSL (Secure Socket Layer)* atau implementasikan tindakan pencegahan *CSRF* lain jika diperlukan.

6. *Multiple vulnerabilities fixed in php versions 5.5.12 and 5.4.28*

   Tingkatkan ke versi terbaru PHP

7. *Same site scriping*

   Disarankan bahwa entri localhost non-FQ dihapus dari konfigurasi nama server untuk domain yang meng-host situs web yang bergantung pada manajemen status HTTP.

8. *User Credencial are sent in clear text*

   Karena kredensial pengguna dianggap informasi sensitif, harus selalu ditransfer ke server melalui koneksi terenkripsi (HTTPS).