BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

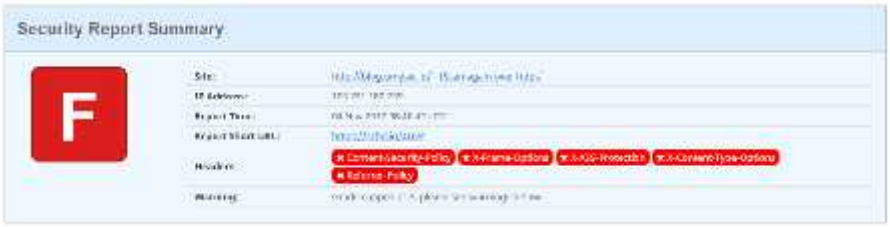
Membahas mengenai kesimpulan, alangkah baiknya terlebih dahulu membahas mengenai *security issue* yang terjadi pada blog UMY. Pada saat pertama kali akan memulai mengerjakan *load balance* pada blog UMY di BSI UMY, langkah pertama yaitu dengan mengidentifikasi masalah yang sering dirasakan para mahasiswa/i di UMY ketika berada dalam masa aktif perkuliahan atau ketika akan menggunakan blog UMY.

Setelah dilakukan analisa, ternyata terdapat beberapa masalah yang menjadi penyebab timbulnya masalah-masalah pada blog UMY, diantaranya:

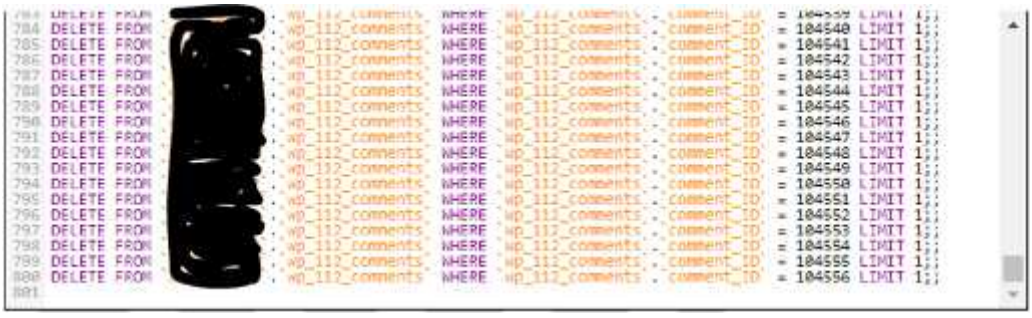
1. Reputasi *ip address* UMY yang buruk di *internet*, hal ini disebabkan oleh banyaknya *malware, botnet*, ataupun *scam link* pada jaringan internal UMY yang mengarah ke *internet*.
2. Banyaknya *spam* baik *back-link spam* maupun *comment spam* yang terdapat pada *database* blog UMY dan juga pada Wordpress yang digunakan pada blog UMY.
3. Terdapat *security issue* lainnya seperti *bug* atau *vulnerability* pada Wordpress, *database*, serta *security issue* yang terkait dengan *DNS hijack, malware, botnet*, dan juga *security header website* blog UMY.

Oleh karena itu, berdasarkan masalah yang berhasil ditemukan selama penelitian, dapat diambil kesimpulan pertama, bahwa blog UMY sering tidak dapat diakses jika pada jam-jam padat perkuliahan adalah, karena disebabkan meningkatnya ukuran *database* yang disebabkan oleh banyaknya *spam* yang masuk melalui Wordpress *comment* pada blog, serta terdapat beberapa *spam* yang disebabkan oleh *malware*.

Oleh karenanya didapat sebuah kesimpulan bahwa alangkah baiknya jika migrasi ke*server* yang baru baik *database* maupun *web server*. Penelitian ini juga dilakukan pada *server* baru, dikarenakan jika memakai server blog yang sekarang, sangat tidak memungkinkan, mengingat aktivitas para akademisi kampus yang menggunakan blog sedang dalam kondisi aktif, serta banyaknya masalah terkait dengan *security* yang telah disebutkan. Gambar 5.1 dan 5.2 berikut merupakan *screenshot* dari *vulnerability* yang terdapat pada blog UMY sekarang.



Gambar 5.1 Unsecure Web Header



Gambar 5.2 Database Spam

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dijadikan sebagai acuan dalam penelitian selanjutnya, yaitu:

1. Lakukanlah *hardening* dan bila perlu sewalah seorang *penetration tester* yang benar-benar telah berkompeten dan telah teruji.
2. Lakukanlah pengamanan baik dari segi program maupun aplikasi.
3. Lakukanlah *maintenance* secara berkala terhadap *software*, dan *system* yang telah dibangun.
4. Edukasi *user* atau pengguna layanan terhadap masalah IT *security* atau apapun yang berkaitan dengan keamanan data atau privasi.
5. Sebagai seorang pengelola pada BSI UMY yang melakukan maintenance terhadap system yang berjalan pada universitas hendaklah memiliki perhatian terkait dengan *issue* IT baik teknologinya, *software*, maupun *security issue* yang terjadi.
6. Untuk menghindari hal-hal yang tidak diinginkan seperti penyebaran *botnet*, *malware* maupun sampai pada kasus peretasan terhadap website maupun server UMY, sangat disarankan agar universitas membentuk kelompok yang benar-benar fokus terhadap layanan teknologi yang digunakan pada saat ini.