14

Conclusão

Transcrição

Vamos retomar, rapidamente, o que aprendemos nesse curso:

- *Injection*: No primeiro capítulo aprendemos sobre injeção de código SQL, inclusive, fomos capazes de extrair informações do Banco de Dados, mencionamos também problemas de autenticação de força bruta, fizemos downloads de listas e utilizamos o *Burb Suite*;
- *Cross site Scripting*: aprendemos sobre esse tipo de ataque e como exercício introduzimos um código *javascript* e uma imagem do *Anonymus* em um site, ainda, realizamos o sequestro de sessão para nos logar como usuário admin;
- Conseguimos fazer um redirecionamento de objeto, vimos problemas de configuração ou o que acontece quando acreditamos que não indexar um endereço é proteção o suficiente. Falamos também sobre *Upload de arquivos*, cuidados sobre quais arquivos um usuário está enviando e informações sobre exposição de dados sensíveis
- Falamos sobre vulnerabilidades existentes nos sistemas quando fizemos o clone da página do WordPress e exploramos também o `redirect` para enganar a vítima.

Esse curso teve o objetivo de abordar ataques comuns que podem ser realizados em um site e através disso, incentivar o aluno a pensar maneiras possíveis de prevenção a esse tipo de situação.