
Pentest
em aplicações web
novatec
Daniel Moreno

Resumo de Pentest em Aplicações Web

Aplicações web têm um histórico extenso de vulnerabilidades, que têm sido exploradas pelos hackers. A lista de ataques conhecidos é extensa, envolvendo Cross-site Scripting, SQL Injection, unrestricted file upload, Code Injection, Command Injecion, Remote/Local File Inclusion e Cross-site Request Forgery, somente para citar alguns.

Neste livro, você conhecerá as técnicas mais utilizadas pelos hackers, e poderá implementar mecanismos de proteção em suas aplicações web contra esses ataques. Para facilitar, esta obra é dividida em três seções.

A primeira tem como foco ensinar o básico sobre ambientes web, sendo o PHP a linguagem escolhida. Entendendo bem a primeira seção, a segunda reportará como os ataques são realizados.

Nessa parte, ferramentas e técnicas manuais de ataques serão descritas a fim de se conhecer quais as possíveis vulnerabilidades do website. As técnicas de defesa serão descritas na terceira seção, para que o website seja disponibilizado on-line com o mínimo de segurança.

No decorrer do livro, o leitor aprenderá: Os princípios da programação web (HTML, CSS, PHP e SQL) e quais as funções do PHP com que se deve ter mais cuidado; A realizar um pentest na própria aplicação seguindo as normas da OWASP e saber qual é o modus operandi de um ataque; A analisar um código PHP e determinar se este está ou não vulnerável.