Defenda as suas aplicações web e seja um especialista em Pentest.

Teste de Invasão de Aplicações Web (EaD)

O curso trata de testes de invasão de aplicações web, as quais, atualmente, são um dos principais alvos de ataque, devido à presença massiva nos mais diversos ambientes. Um teste de invasão, também chamado de teste de penetração ou pentest, é um método utilizado para verificar a segurança de um ambiente, plataforma ou sistema, por meio da simulação de ataques reais explorando as vulnerabilidades encontradas. Diferentemente de uma varredura de vulnerabilidades, que muitas vezes recorre ao simples uso de ferramentas automatizadas, pentest é um processo cíclico que depende principalmente do conhecimento técnico do auditor de segurança que o realiza. Este curso, então, espera introduzir as principais técnicas que podem ser empregadas.

Características

- 5 (cinco) semanas de duração, com 2 (dois) encontros online por semana (total de 10 encontros);
- Os encontros serão ao vivo com tutor e terão 2 (duas) horas de duração;
- Para o auto estudo, o material de apoio será disponibilizado no AVA: livro do curso, materiais extras, indicação de leituras, atividades;
- Sugerimos que antes de iniciar o curso, o aluno verifique o seu acesso à internet;
- Para acompanhamento do curso, sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox;
- **Para conclusão do curso é necessário que o aluno responda aos questionários e realize 75% das atividades propostas dentro dos prazos estabelecidos.**

Competências desenvolvidas

Ao final do curso o aluno será capaz de:

- Conscientizar os alunos sobre as vulnerabilidades de maior risco encontradas em sistemas web (OWASP Top Ten) e como elas podem ser exploradas por usuários maliciosos;
- Ensinar técnicas para a realização de Pentest em aplicações web;
- Introduzir ferramentas que podem otimizar o processo de Pentest, por meio da automatização de algumas tarefas.

Conhecimentos prévios

- Conceitos básicos de TCP/IP, HTTP;

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Conceitos básicos de Javascript;
- Conceitos básicos de bancos de dados;
- Conceitos básicos de mecanismos e protocolos criptográficos;
- Ter realizado o curso Análise Forense ou possuir conhecimento equivalente.

Investimento

- R$ 1.440,00

Programa do curso

- Arquitetura e tecnologias de aplicações web;
- Criptografia: cifras simétricas, cifras assimétricas, funções de hash criptográficas, MACs, assinaturas digitais, certificados digitais e SSL/TLS;
- Tipos de pentest e metodologia para teste de invasão;
- Injeção de SQL com acesso à plataforma subjacente, especificidades dos SGBDs e injeção de SQL às cegas;
- Injeção em LDAP, XML, SMTP e injeção de comandos;
- Transporte de credenciais por canais inseguros;
- Enumeração de usuários;
- Política de senhas fortes não implementadas pela aplicação;
- Falhas na programação ou projeto do mecanismo de autenticação;
- Mecanismos de recuperação de senhas vulneráveis;
- Condições de corrida no mecanismo de autenticação;
- Testes sobre o gerenciamento de sessões;
- Cross-Site Scripting (XSS) e CSRF;
- Teste dos mecanismos de autorização;
- Testes dos mecanismos criptográficos;
- Teste completo e relatórios.

Escola Superior de Redes RNP

esr.rnp.br

RNP