ESET CYBERSOC

# ETHICAL HACKING

**Serviços de EH confiáveis para manter os sistemas corporativos seguros**


## Web Penetration Testing

# Web Penetration Testing

Um Web Penetration Test é um conjunto de técnicas utilizadas para avaliar a segurança dos recursos e ativos da organização a partir do ponto de vista da matéria de segurança em nível web.

Esta técnica não apenas identifica as vulnerabilidades existentes na infraestrutura web, mas também executa a análise com maior profundidade. Especificamente, busca-se, além da identificação, a exploração das vulnerabilidades e, dessa maneira, observa-se o impacto real sobre a organização.

Este tipo de serviço pode ser executado tanto a partir de um ponto de vista interno como externo da organização. No primeiro caso, busca-se identificar e explorar as vulnerabilidades web que sejam visíveis num cenário com acesso aos recursos e ativos da organização, enquanto no segundo, é realizada a avaliação a partir do ponto de vista de um atacante externo.

## Objetivos principais

- ✓ Obter uma fotografia do estado da segurança web da organização, sistema ou host objetivo em um momento determinado.
- ✓ Visualizar sua empresa a partir do ponto de vista do atacante, localizando fraquezas, vulnerabilidades web e pontos de acesso não autorizados, antes que os atacantes o façam.
- ✓ Comprovar o verdadeiro impacto das vulnerabilidades em seu ambiente particular.
- ✓ Comprovar se o nível de proteção existente condiz com a política de segurança estabelecida pela organização.
- ✓ Comprovar a efetividade de suas medidas de proteção, políticas e processos de detecção de intrusos e resposta a incidentes.

## Por que realizar um Web Penetration Test?

- ✓ Para conhecer o estado da segurança web de uma organização (especialmente se nunca foi realizada uma auditoria dessas características).
- ✓ Para estabelecer um ponto de partida e começar a gerir a segurança web da organização.
- ✓ Está baseado no OWASP TOP TEN 2016 e no OWASP Testing Guide 4.0, garantindo o melhor desempenho.
- ✓ Para constituir um ciclo de revisão e melhoria para a segurança web de forma contínua, desde o ciclo de desenvolvimento ou em suas sucessivas interações.

# As etapas associadas a este serviço são:

- ✓ Reconhecimento web
- ✓ Análise e detecção de vulnerabilidades web
- ✓ Exploração de vulnerabilidades
- ✓ Montagem e apresentação de relatórios

# Relatórios

Neste serviço, são gerados 2 entregáveis ou relatórios que ajudam e orientam o cliente no processo de correção de vulnerabilidades.

O primeiro deles, o **relatório executivo**, descreve o nível de risco da empresa sem entrar em detalhes técnicos, evidenciando os problemas por meio de conceitos claros e gráficos.

O segundo relatório, o **relatório técnico**, direcionado para a área técnica da empresa, visa ajudar a equipe de TI a solucionar os problemas detectados.

Neste relatório, são mostradas todas as evidências dos testes executados de tal forma que todas as tarefas sejam escaláveis e transparentes para o cliente. Baseado no OWASP TOP TEN e no OWASP Testing Guide 4.0.


ESET CYBERSOC