EXSS: Um Emulador Educativo de Ataques *Cross-Site Scripting*

Bianca Guarizi[2], Isabela Alves[2], Júlia Souza[2], Guilherme Pimentel[1], João Watanabe[1], Dalbert Mascarenhas[2], Ian Vilar Bastos[3], Marcelo Rubinstein[3], Igor Moraes[1]

1 Universidade Federal Fluminense

2 CEFET/RJ

3 UERJ Universidade do Estado do Rio de Janeiro

Agradecimento

É o resultado parcial de um Grupo de Trabalho selecionado na chamada Chamada Pública de Pesquisa, Desenvolvimento e Inovação da Rede Nacional de Ensino e Pesquisa (RNP) do Programa Hackers do Bem, 2023

HACKERS DO BEM_ Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Projeto apoiado pelo Ministério da Ciência, Tecnologia e Inovações, com recursos da Lei no 8.248, de 23 de outubro de 1991

Qual o tamanho do déficit de profissionais em cibersegurança?

85.000.000 até 2030

World Economic Forum

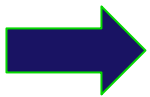
750.000 no Brasil

Fortinet

Objetivo

- Desenvolver um emulador de ataques *Cross-Site Scripting* (XSS): abordagem educacional

- Três pilares
  - Explorar vulnerabilidades
  - Identificar vulnerabilidades
  - Eliminar vulnerabilidades



Ambiente controlado!

70%

das **aplicações Web** são desenvolvidas com **brechas de segurança** severas

CyCognito, 2023

XSS está na OWASP Top 10

CyCognito, 2023

O que é um ataque XSS?

- Um atacante explora vulnerabilidades de sítios Web legítimos
  - Executa de trechos de código maliciosos nos navegadores Web dos usuários legítimos
  - Campos de sítios Web que permitem a entrada de dados e retornam alguma informação sobre os dados de entrada

Visão Geral do Emulador EXSS

- Usuários do emulador realizarão **atividades**
- As atividades são compostas por
  - Uma introdução teórica
  - Procedimentos práticos para realização de testes de exploração e identificação de vulnerabilidade XSS em um servidor Web executados em uma máquina virtual
- O usuário será guiado passo-a-passo pelo emulador durante a execução das atividades
- Atividades para **diferentes níveis de conhecimento**

Oi, eu sou o Hacker Good.
Bem-vindo ao EXSS!

Você sabia que 89% dos funcionários disseram que seriam mais produtivos se o seu trabalho fosse mais gamificado?

2019 Gamification at Work Survey

Iniciante

HACKERS DO BEM

Introdução

XSS Refletido

XSS Armazenado

XSS DOM

11.11%

Pontuação: 10 XP

Logado como usuario

Trocar de Usuário

Olá, usuario!

Meu nome é Hacker Good e estarei te acompanhando nessa jornada!

Iniciante

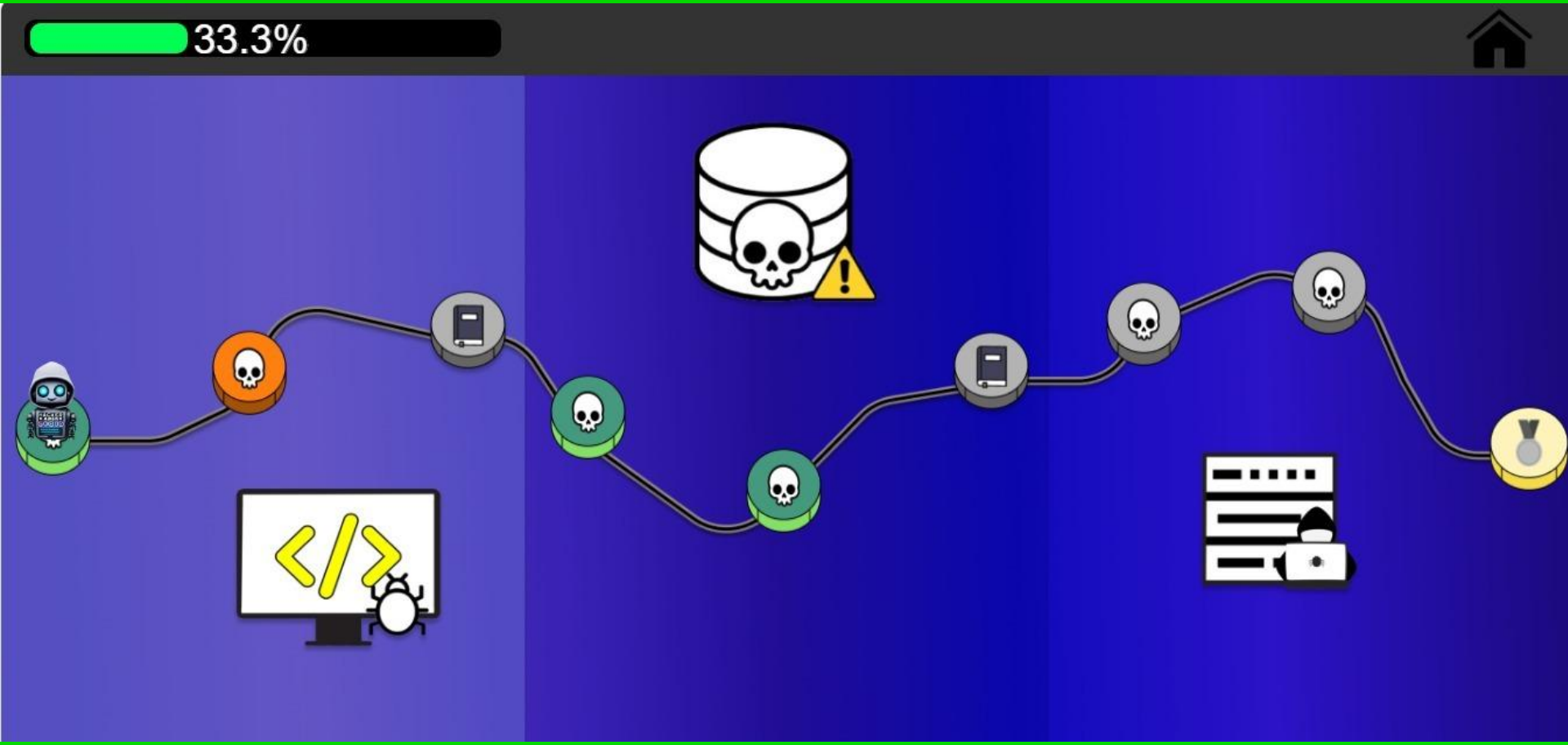
0101
1001

Intermediário

Avançado

Selecione nos botões acima qual nível será acessado.

Os níveis serão desbloqueados a medida que você completar o anterior.


33.3%

Módulos do Emulador

Usuário

Interface do Usuário

Catálogo de Atividades

Análise de Vulnerabilidades

Relatório Técnico

Interface do Usuário

- Página principal
- Trilha sequencial de desenvolvimento do usuário
  - O usuário será recompensado com medalhas de conclusão como parte da experiência gamificada
  - Após a finalização de todas as atividades, o usuário receberá um certificado de conclusão
- Aba lateral expansível
  - Navegação do usuário por todas as atividades propostas
  - Cada atividade é composta por diferentes tarefas, desde a leitura de um texto explicativo até a realização de um ataque

Catálogo de Atividades

- É responsável pela definição das atividades
- Cada atividade é composta por uma introdução teórica sobre o assunto da atividade, seguida de procedimentos práticos para realização de testes de vulnerabilidade XSS
- A cada atividade é associado um nível de conhecimento necessário para o usuário realizá-la
    - Básico, intermediário e avançado

Motivação

As aplicações Web são uma parte essencial do dia-a-dia das pessoas. As corporações usam as aplicações Web para aumentar a qualidade dos seus serviços oferecidos e ao mesmo tempo alcançar uma audiência maior através da Internet. No entanto, as vantagens oferecidas pelas aplicações Web também são acompanhadas de riscos para os seus usuários. Informações sensíveis e confidenciais são, geralmente, armazenadas por grandes corporações através de suas aplicações Web, o que as tornam um grande atrativo para ciberataques. Os ataques XSS são um dos tipos de ataque mais frequentemente realizados sobre aplicações.

Este curso apresentará a motivação por trás dos ataques XSS e os seus impactos na sociedade e como o uso das tecnologias contemporâneas para o desenvolvimento de aplicações Web, sem a conscientização voltada para a segurança, contribui para o aumento dos ataques XSS.

O que é um ataque XSS?

Uma aplicação Web é vulnerável a um ataque XSS quando há a possibilidade de inserir código malicioso em sua página Web legítima por não realizar codificação e validação apropriada dos dados fornecidos como entrada. Uma aplicação Web com vulnerabilidades a um ataque XSS está exposta a instalação de malwares, sequestro de sessões, roubo de dados confidenciais e ataques de engenharia social. Os ataques XSS podem ser classificados em três categorias. Confira os detalhes abaixo:

XSS Refletido

Catálogo de Atividades

- Atividade 1: XSS Refletido
- Atividade 2: XSS Armazenado
- Atividade 3: XSS baseado em *Document Object Model* (DOM)
- Atividade 4: Desenvolvimento Seguro

Catálogo de Atividades

- Nível básico
  - Familiarizar os usuários com o emulador e ataques XSS
  - Identificar e compreender as vulnerabilidades de XSS
- Nível intermediário e avançado
  - Experimentar *scripts* que explorem a vulnerabilidade XSS
  - Aplicar correções nos códigos das páginas

Análise de Vulnerabilidades

- Hospeda sítios Web em uma máquina virtual que executa um servidor Web
  - Ambiente controlado e próximo a um ambiente de produção para aprendizado
  - Sítios Web das atividades estão integrados a um pequeno comércio eletrônico desenvolvido especificamente para o emulador

Iniciante

HACKERS DO BEM

- Página Inicial
- Introdução
- XSS Refletido
- XSS Armazenado
- XSS DOM

Box Anti Hacker

R$ 50.00

Saiba mais

Cofre de Senhas

R$ 30.00

Saiba mais

Firewall

R$ 40.00

Saiba mais

Relatório Técnico

- É responsável por dar o *feedback* ao usuário sobre a atividade realizada
- Experiência gamificada
  - Pontos de experiência, medalhas e certificado

HACKERS DO BEM

22.22%

Pontuação: 20 XP

Para reforçarmos o conteúdo aprendido neste módulo, vamos realizar os exercícios de fixação?

Exercícios de Fixação

1. O que caracteriza um ataque XSS refletido?

- ○ a. A injeção de código malicioso que é armazenado no servidor e executado por qualquer usuário que acessar a página.
- ○ b. A injeção de código malicioso através de um URL que é refletido de volta pelo servidor e executado no navegador do usuário.
- ○ c. A execução de código malicioso diretamente no servidor, comprometendo os dados armazenados.

2. Como o ataque XSS refletido é comumente iniciado?

- ○ a. Enviando um código malicioso diretamente para o servidor através de uma conexão segura.
- ○ b. Inserindo código malicioso em arquivos de configuração do servidor Web.
- ○ c. Induzindo o usuário a clicar em um link contendo um URL malicioso enviado por e-mail, página Web ou outras técnicas de engenharia social.

3. Por que o ataque XSS refletido é considerado não-persistente?

- ○ a. Porque o código malicioso é armazenado permanentemente no servidor.

Ambiente de Execução

- Uso da virtualização é imperativo
  - O emulador tem que ser executado em um ambiente computacional com recursos isolados
    - Atividades práticas que envolvam a exploração de vulnerabilidades não afetem os recursos computacionais de produção

- Máquina virtual
  - Facilidade de instalação e uso

Ferramentas de Desenvolvimento

- Framework Bootstrap (https://getbootstrap.com.br/)
  - Desenvolvimento Web front-end
- Tecnologias envolvidas
  - HTML, CSS, JavaScript, JQuery, PHP e MySQL
- Apache 2
- VirtualBox, sistema operacional Ubuntu

Conclusão e Comparação

Soluções	Interface do usuário	Base de dados	Servidor Web	Atividades	Feedback técnico	Suporte para pt-br?	Facilidade de uso	Offline
GT-EXSS	HTML, CSS, JS, JQuery, Bootstrap, PHP	MySQL	Apache 2	Práticas e teóricas	Relatórios construtivos e recomendações práticas para mitigar as vulnerabilidades encontradas	Sim	Utiliza VirtualBox para facilitar a experiência do usuário	Sim
Portswigger	Não é open-source			Práticas e teóricas	Apenas a solução dos laboratórios de teste	Não	Possui ferramentas de auxílio, mas são pagas	Não

OWASP Juice Shop	Node.js, Angular, Express, Google Material Design	SQLite, MarsDB	Heroku	Mais práticas	Sistema de pontuação com recompensas	Não	Utiliza contêineres através do Docker	Não
Google XSS Game	Não é open-source			Práticas	Dicas para resolução do problema proposto	Não	Abordagem direta, entrar no site e utilizar	Não
OWASP Webgoat	Java, Spring Framework, JSP	Java Database Connectivity	Tomcat	Práticas e teóricas	Visão geral de políticas que poderiam ser aplicadas para mitigar as vulnerabilidades	Sim	Utiliza contêineres através do Docker	Não
TryHackMe	Não é open-source			Práticas e teóricas	Permite a criação de ambientes para acompanhar o progresso dos estudantes	Não	Utiliza VMs para simular o ambiente de estudo	Não

Equipe

Igor Moraes
Professor, UFF
Coordenador

Marcelo Rubinstein
Professor, UERJ
Atualização tecnológica

Ian Bastos
Professor, UERJ
Atualização tecnológica

Dalbert Mascarenhas
Professor, CEFET/RJ
Atualização tecnológica

Isabela Alves
Graduação, CEFET/RJ
Desenvolvedora

Julia Souza
Graduação, CEFET/RJ
Desenvolvedora

Bianca Guarizi
Graduação, CEFET/RJ
Desenvolvedora

Guilherme Pimentel
Graduação, UFF
Desenvolvedor

João Watanabe
Graduação, UFF
Desenvolvedor

Faça o download e avalie nosso emulador!

http://www.midiacom.uff.br/gt-exss

Emulador

Formulário de Avaliação