Vulnerabilidades – Portal do Instituto Mises

(19/08/2020)

1ª Vulnerabilidade

Esta primeira vulnerabilidade é um Cross-Site Scripting (XSS), ou seja, uma vulnerabilidade que permite executar comandos em Javascript contra os usuários cadastrados ou visitantes não cadastrados no site.

Este caso, em específico, poderia ser explorado através do envio de um link malicioso contendo esse Javascript para um usuário ou visitante do Portal.

Passos:

1. Escrever um Javascript malicioso na barra de pesquisa do site

   Ex:
   <script>alert("Javascript malicioso executado com sucesso!")</script>

   Sendo possível, também, inserir HTML dentro da página.

   Ex:
   <img
   src="https://ilmg.org.br/wp-content/uploads/2018/05/1_JbS7ms9T2csHLfntvj0hog-1.jpeg" />

2. Copiar URL da página de busca com a vulnerabilidade e enviar para a Vítima.

2ª Vulnerabilidade

Também consiste em um Cross-Site Scripting (XSS). A diferença desta vulnerabilidade para a 1ª é que nessa é possível persistir o script malicioso na própria Base de Dados do Portal, podendo ser executada toda vez que um usuário se deparasse com o seu nome no site, ou em outras ocasiões.

Não é possível demonstrar esta vulnerabilidade surtindo efeito na vítima, pois não é possível interagir com outro usuário pelo Portal. Entretanto, quando o Atacante comenta em um artigo, o comentário passa por um moderador, que

pode acabar tendo seus dados (incluindo a chave para acessar sua conta) roubados pelo atacante quando o nome do Atacante aparece na página da moderação. Isso não foi testado, porém o simples fato de poder inserir Javascript e HTML numa informação pública já poderia caracterizar uma vulnerabilidade.

Passos:

1. Injetar Javascript ou HTML no nome de usuário.

   Ex:
<script>alert("Javascript malicioso executado com sucesso!")</script>

2. Verificar que, ao recarregar a página, o código será executado.

3ª Vulnerabilidade

Sendo essa a mais crítica de todas, reforço que não a utilizei contra membros do Portal, mas somente contra uma outra conta que criei com o objetivo de ser a Vítima em meus testes.

A vulnerabilidade consiste em alterar o Cookie armazenado pelo Portal, a fim de fazer o Portal acreditar que sou outro usuário, logando-me automaticamente em sua conta e me dando todos os acessos que o usuário real possui.

Passos:

1. Abrir a “Ferramenta de desenvolvimento”, também conhecida como “Inspecionar Elemento”
2. Clicar em “Application”
3. Clicar em “Cookies”
4. Procurar por “customerId”
5. Alterar o valor de “customerId” de “customerId=[ID_ATACANTE]” pelo “customerId=[ID_VITIMA]”
6. Atualizar a página

Importante ressaltar que os CPFs utilizados no cadastro dos usuários foram obtidos através do seguinte Gerador de CPF :

https://www.4devs.com.br/gerador_de_cpf

Reforço que nunca tive a intenção de prejudicá-los de qualquer forma possível.

Email para contato: darwin.brandao@gmail.com