XSS - Dom

XSS - DOM

Opa, seguinte esse será meu último artigo sobre XSS! Meu próximo artigo saíra em breve e entraremos em SQL Injection.

O que é XSS-DOM

Esse é um XSS muito específico que consiste em mudar as propriedades do objeto "Document Object Model (DOM)". Normalmente encontrado em scripts com o `document.write`.

Exemplo

Digamos que existe um site com uma barra de procura e você pode inserir valores lá dentro. Se esse site usar o `document.write` para gravar dados da página, quer dizer que ele puxa isso de um outro comando, que a partir da busca do usuário vai ser chamada pra ser exibida.

Um exemplo disso seria:

Aqui o `document.write` está usando o `+query+` para guardar os valores inseridos pelo usuários, para depois definir ele em uma variável que será usada para fazer uma procura local de resultados com o `location.search` no parâmetro de url `search=`.

Explicado isso, como seremos nós que colocaremos os dados para pesquisa, podemos usar do javascript para burlar parte do processo.

Um exemplo de código que podemos executar:

```
"><svg onload=alert(1)>"
```

E teremos o seguinte resultado:

Explicação

O que acontece aqui é que quando colocamos o **script** mostrado, nós quebramos o **código** `searchTerms="+query">`, isso por que fechamos ele no começo do **script** com o `">` e assim podemos fazer com que o mesmo seja colocado no `search=` da url da página. E com isso ele será executado para todos que estiverem acessando a url modificada.

Tente você mesmo:

Você pode treinar esse tipo de **XSS** nesse laboratório da portswigger:

- https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink

Finalização:

Espero que tenha ficado claro esse XSS em específico, visto que ele é mais complicado que os outros. Mas se você não conseguiu entender, procure auxílio de videos e outros artigos para te ajudar!!

Obs: É sempre importante dizer que o conteúdo colocado nesse artigo é feito meramente para fins educativos e didáticos e não me responsabilizo por qualquer ato ilegal feito a partir do conhecimento desse artigo por mais simples que ele seja!

Soon - (10/08/24)