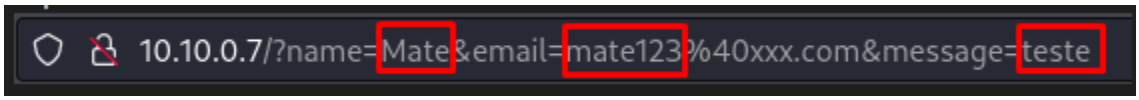
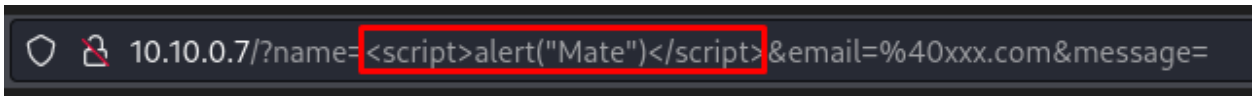
XSS (Reflected)

Notamos que após inserimos dados no campo do formulário as mesma informações são reproduzidas na URL





Notamos que conseguimos inserir um texto dentro de um comando

<script>alert(" Mate ")</script>

Pensando como um atacante vendo que conseguimos inserir texto dentro de um comando script podemos tentar acesso as credenciais armazenadas nos Cookie de Sessão

*<script>alert("Document.Cookie")</script>

A [`Document`](https://developer.mozilla.org/en-US/docs/Web/API/Document)propriedade `cookie`permite que você leia e escreva [cookies](https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies) associados ao documento. Ela serve como um getter e setter para os valores reais dos cookies.

Ao explorar vulnerabilidades de XSS, um invasor pode executar ações maliciosas, como:

- Redirecionar usuários para um site malicioso.
- Capturar as teclas digitadas pelos usuários.
- Acessar o histórico do navegador dos usuários e o conteúdo da área de transferência.
- Executar exploits baseados em navegador da Web (por exemplo, travar o navegador).
- Obter as informações do cookie de um usuário que está logado em um site.

- Roubar o token de sessão de login, permitindo que o invasor interaja com o aplicativo como a vítima sem saber sua senha.
- Forçar o usuário a enviar solicitações controladas pelo invasor a um servidor.
- Mudar o conteúdo de uma página.
- Enganar a vítima para que divulgue sua senha para o aplicativo ou outros aplicativos.
- Infectar a vítima com outro código malicioso usando uma vulnerabilidade no próprio navegador da Web, possivelmente assumindo o computador da vítima.

Tipos de ataques de XSS

Cross-site scripting pode ser classificado em três categorias principais — XSS Armazenado,_ XSS Refletido e XSS baseado em DOM.

Aqui está sendo exibida acima é o REFLETIDO

XSS Refletido (também conhecido como XSS Não persistente). Nesse caso, a carga útil do invasor deve fazer parte da solicitação enviada ao servidor da Web.
Em seguida, é refletido de volta de maneira que a resposta HTTP inclua a carga útil da solicitação HTTP. Os invasores usam links maliciosos, e-mails de [phishing](https://www.kaspersky.com.br/resource-center/threats/spam-phishing) e outras técnicas de [engenharia social](https://www.kaspersky.com.br/resource-center/threats/how-to-avoid-social-engineering-attacks) para induzir a vítima a fazer uma solicitação ao servidor. A carga útil XSS refletida é então executada no navegador do usuário.

O XSS Refletido não é um ataque persistente, portanto, o invasor precisa entregar a carga útil a cada vítima. Esses ataques costumam ser feitos por meio de redes sociais.

🔁Contra medidas
- Garantir que qualquer página em seu site que aceite entrada do usuário filtre as entradas de código, como HTML e JavaScript.
- Faça a varredura em busca de vulnerabilidades de aplicativos da Web e conserte-as de acordo.
- Atualize seu site e software de servidor para evitar a exploração futura de vulnerabilidades que podem ser visadas por um ataque XSS.
- Utilizar cabeçalhos de segurança, como Política de Segurança de Conteúdo (CSP)
- Usando frameworks de desenvolvimento que oferecem proteção contra XSS
- Implementar ferramentas que detectem e mitiguem o esforço de XSS
- Evite clicar em links suspeitos
- Utilização de sites com certificado de segurança SSL
- Manter o navegador da internet atualizado

Embora o **XSS Refletido** seja geralmente considerado menos crítico que o **XSS Armazenado**, ele ainda representa um **risco significativo**, especialmente quando combinado com **phishing, roubo de credenciais e distribuição de malware**.

A organização deve **corrigir essa vulnerabilidade o quanto antes**, aplicando **sanitização e escape de entrada de dados**, implementando **Content Security Policy (CSP)** e utilizando **Web Application Firewalls (WAF)** para mitigar ataques