Análise de vulnerabilidades

Relatório

Gabriel Oliveira Souza

**Cross Site Request Forgery**

Análise de vulnerabilidades

Relatório

**Cross Site Request Forgery**

Relatório sobre um estudo referente

a falha de CRSF. Sob a coordenação do Boot Santos.

Gabriel Oliveira Souza

**Sumário**

1 **Resumo ……………………………………………...1**

2 **O que é?................................................................1**

3 **Como funciona?...................................................1**

4 **Análise de vulnerabilidade..................................2**

5 **Mitigação……………………………………………..3**

1 **Resumo**

O objetivo deste relatorio é realizar um estudo mais aprofundado referente ao tema de vulnerebilidade utilizando a falha CSRF. Contudo, neste relatório utilizaremos imagens e texto para dar mais valorização ao conteúdo descrito.

2 **O que é?**

Uma vulnerabilidade CSRF basicamente força o navegador do usuário, autenticado na aplicação, a enviar uma requisição ao servidor web vulnerável.

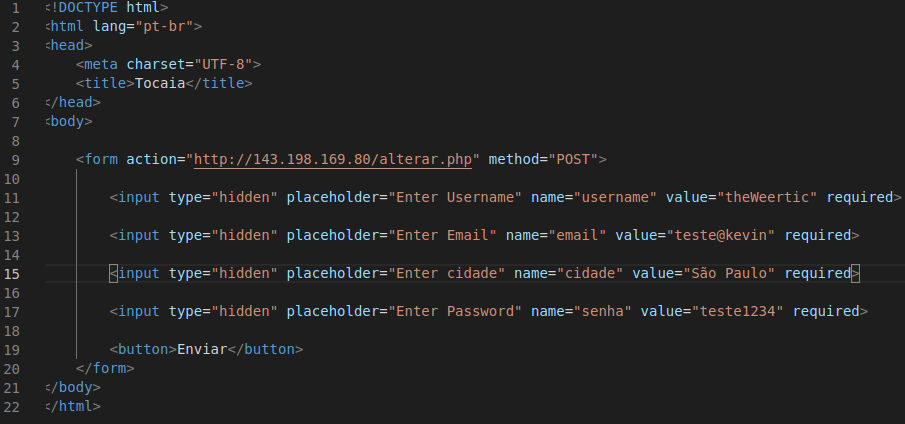
3 **Como funciona?**

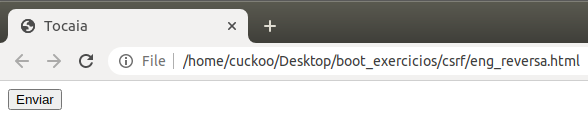
Alvo: Tocaia

Utilizando um código HTML, utilizando os inputs do formulário da aplicação, podemos realizar o ataque CSRF, sendo assim, trocando as credenciais do usuário alvo. Ao colocar todos os inputs no tipo ‘hidden’, os mesmo não vão aparecer para o usuário alvo, irá somentro mostrar na tela o botão de enviar a requisição.

O usuário que já está logado na aplicação web clica no botão e dispara a requisição em seu navegador. Abaixo mostraremos como é feita a falha e a solução para mitigação.

4 **Análise de vulnerabilidade**

Segue abaixo o código utilizado para explorar a vulnerabilidade:



Como explicado acima, utilizando o tipo hidden para deixar os inputs invisíveis e já definindo os valores dos dados juntamente com o método POST, podemors utilizar de engenharia social para o usuário realizar o clique no botão e consequentemente realizar o disparo da requisição.

Com o usuário logado, ao disparar a requisição, ela irá motificar a senha do usuário. Dependendo da aplicação, tem casos que até o e-mail ou o username pode ser alterado. A senha do usuário acima no código foi aterada para **teste1234**.