Universidade Federal do Rio de Janeiro
processo seletivo GRIS
Autor: Pedro Jullian Medina Torres Graça
Descrição: TAG de WEB

1)O que é o protocolo HTTP e Como ele funciona?

O protocolo HTTP é um protocolo que atua na camada de aplicação no modelo OSI sob base TCP. Ele serve para serviços cliente-servidor sob a ideia de requisições e respostas. O cliente solicita uma requisição a um servidor e este devolve uma resposta de acordo com a requisição, com arquivos html e css por exemplo.

2)O que é um Response Code? Cite um exemplo de um programa que você pode fazer com ele.

É um código de resposta do http em relação a solicitação feita via http. Pode ser um código avisando que tudo foi recebido e entendido (100) ou avisando que o servidor não foi encontrado (404).
Você pode executar uma ação em back-and te redirecionando, mas avisando que está tudo ok.

3)O que é um HEADER? Cite um uso INSEGURO desse cabeçalho.
É o que permite passar informações adicionais via solicitação http. Um uso inseguro é você passar a senha do usuário via cabeçalho para acessar a conta de usuário.

4)O que é um Método HTTP? Explique o funcionamento do método POST, o funcionamento do método GET. Explique qual é considerado mais seguro e por que.

Um método HTTP é a forma de passar informações do cliente para o servidor, basicamente indicando qual função deve ser feita pelo servidor.
O get passa a informação para o servidor via URI, muito usado para indicar o caminho dentro servidor desejado (como uma pagina dentro do site que vai ter outro index). O post recebe a informação pelo corpo da requisição, que pode conter uma camada de criptografia. Dessa forma para passar informações sensíveis, como a senha de um usuário. Se você passar a senha do usuário via GET, ela estará na URI do usuário e isso pode ser facilmente copiado.

5) O que é Cache e como ele funciona? Cite os principais HEADERS de Request e Response responsáveis pelo controle de Cache.

Cache é uma memoria que o browser implementa para guardar informações do HTTP, isso economiza internet, pois impede de você ficar fazendo requisições solicitando a mesma coisa. Cache-control e ETAG.

6) O que é Cookie? Qual é o principal ataque relacionado a ele?

Cookie é um arquivo onde ficam registradas informações do usuário para acesso posterior, isso é feito para validar informações de forma segura e transferir informações de um site para outro.
Captura de cookie, para acessar conta de outras pessoas.

7) O que é O WASP-Top-Ten?

O WASP-Top-ten é um local de agregador de informações para desenvolvedores web que contem os maiores ricos das aplicações web no momento atual e de forma atualizada.

8) O que é Recon e Por que ela é importante?

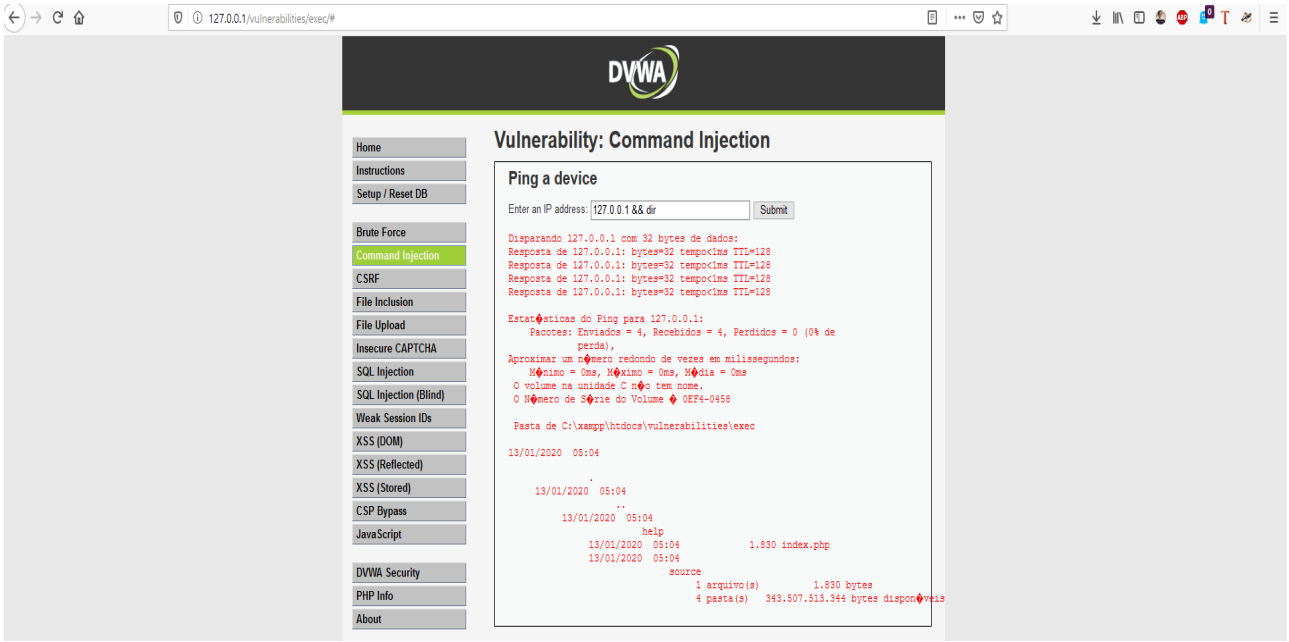
Fase de reconhecimento, é a fase em que você irá listar todos os recursos usados pela aplicação. Ela é importante para orientar aonde você vai buscar as vulnerabilidades.

9)Command Injection (SO-Injection)

a) O que é Command Injection?

É um ataque que busca uma falha na entrada de dados de uma aplicação web, onde você pode passar códigos que serão executados e assim obter acesso ilegítimos.

b)Mostre um exemplo de Command Injection (PoC da exploração)



10) SQL INJECTION

a) O que é SQL injection?

É um ataque que busca uma falha na entrada de dados de uma aplicação web, onde você pode passar códigos SQL que serão executados e assim poder controlar o banco de dados da aplicação.

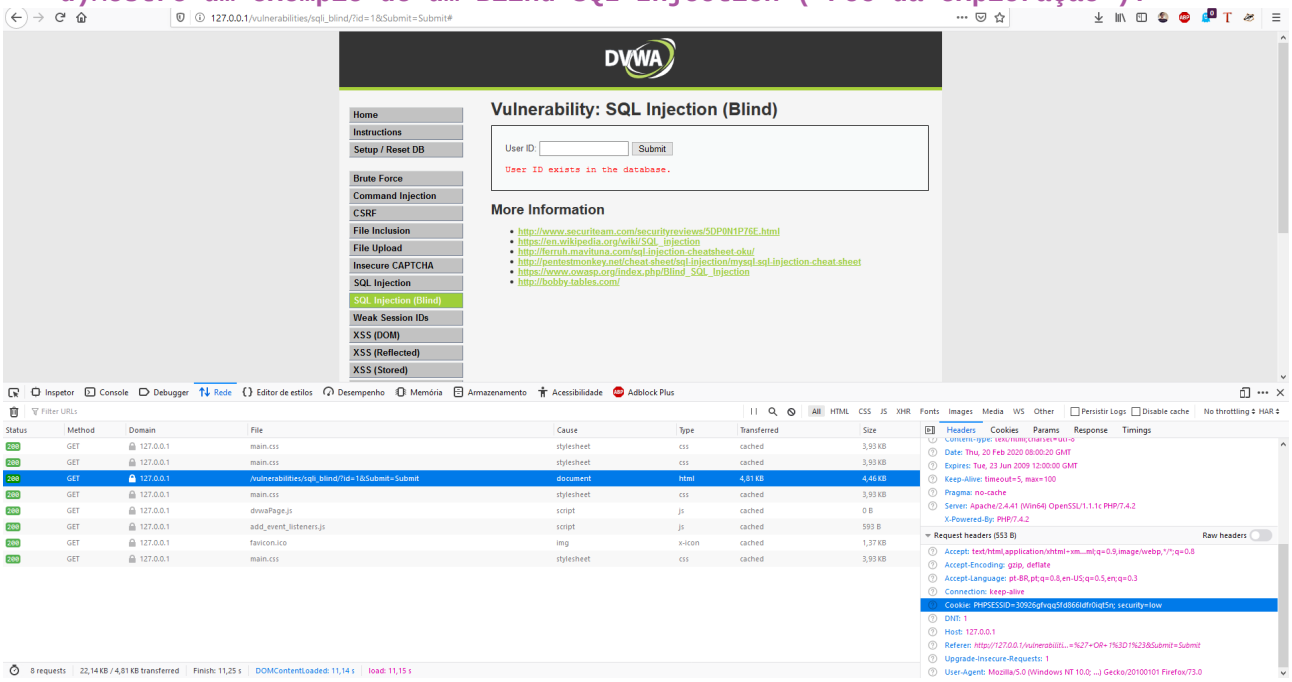
b)O que é Union Based Attack?

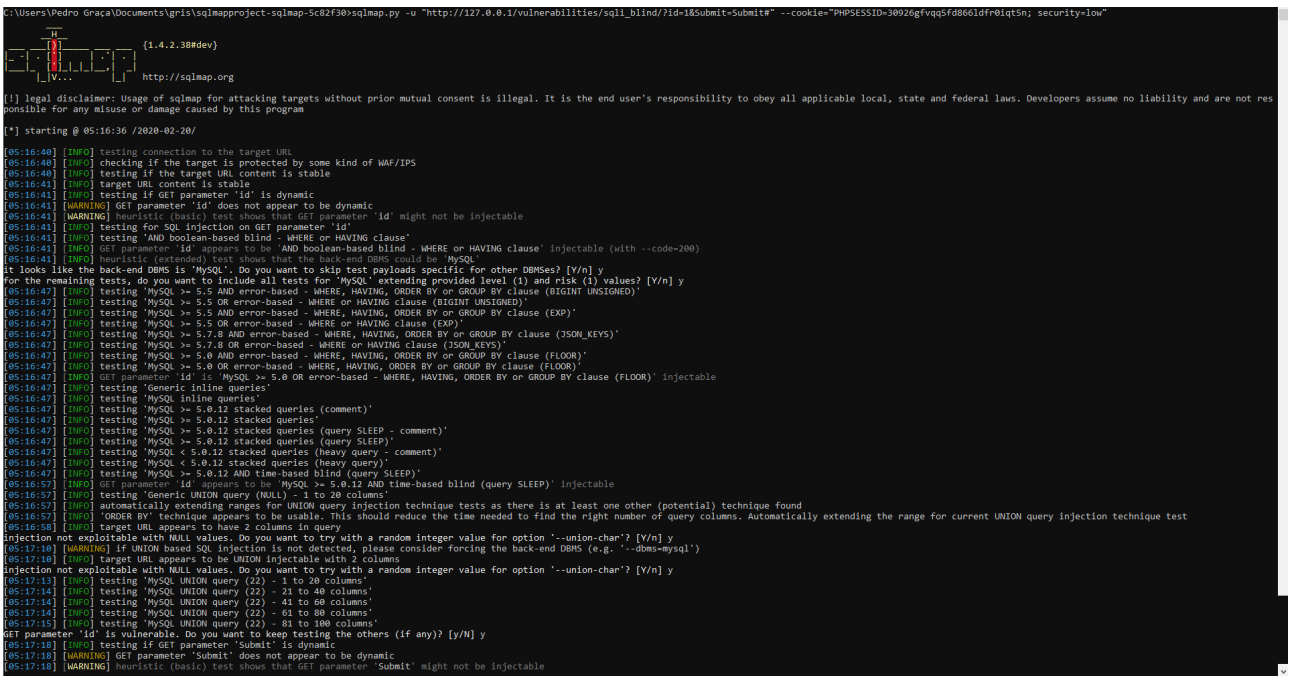
O Union Based Attack permite que o hacker extraia e manipule informações do banco de dados e assim, tendo informações que não deveria.

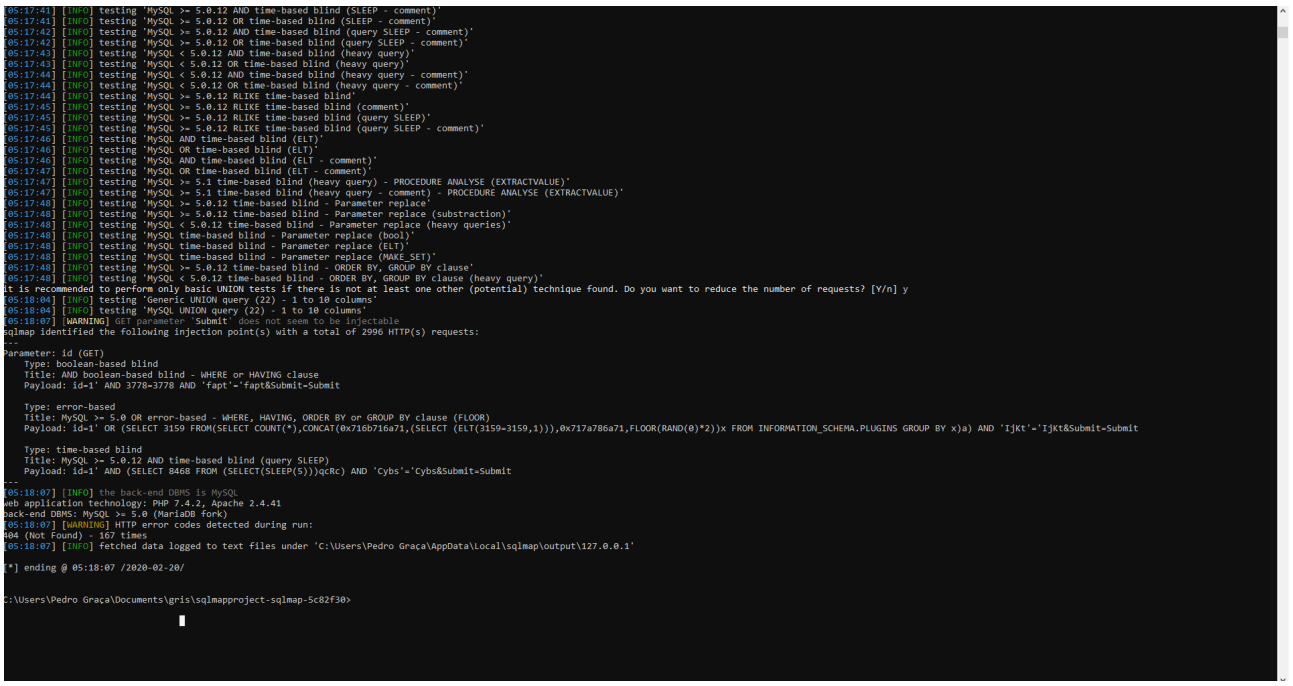
c) O que é Blind-SQL-I?

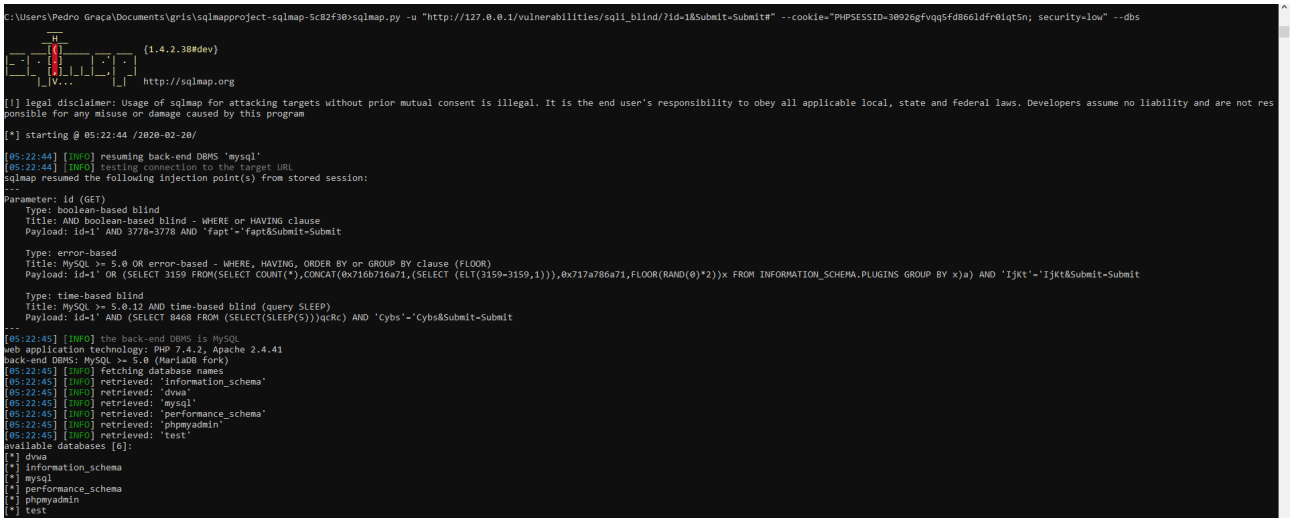
O ataque se baseia em injeção cega de SQL, onde se baseiam em consultas de instruções. A partir dessas instruções se determina o banco de dados, assim podemos obte-lo.

d)Mostre um exemplo de um Blind SQL-Injection (PoC da exploração).









11) XSS

a) O que é XSS?

Um ataque web onde o hacker injeta código no servidor e este irá executar esse código alterado para outros usuários, com isso ele pode roubar informações dos usuários ou fazer com que estes acessem coisas que não foram solicitadas

b)Quais são os tipos de XSS? Explique-os.

Armazenado, refletido e Baseado em DOM.

-> Armazenado

É quando o código é armazenado porque o conteúdo que entra não é filtrado e é armazenado. Com isso você consegue inserir o código.

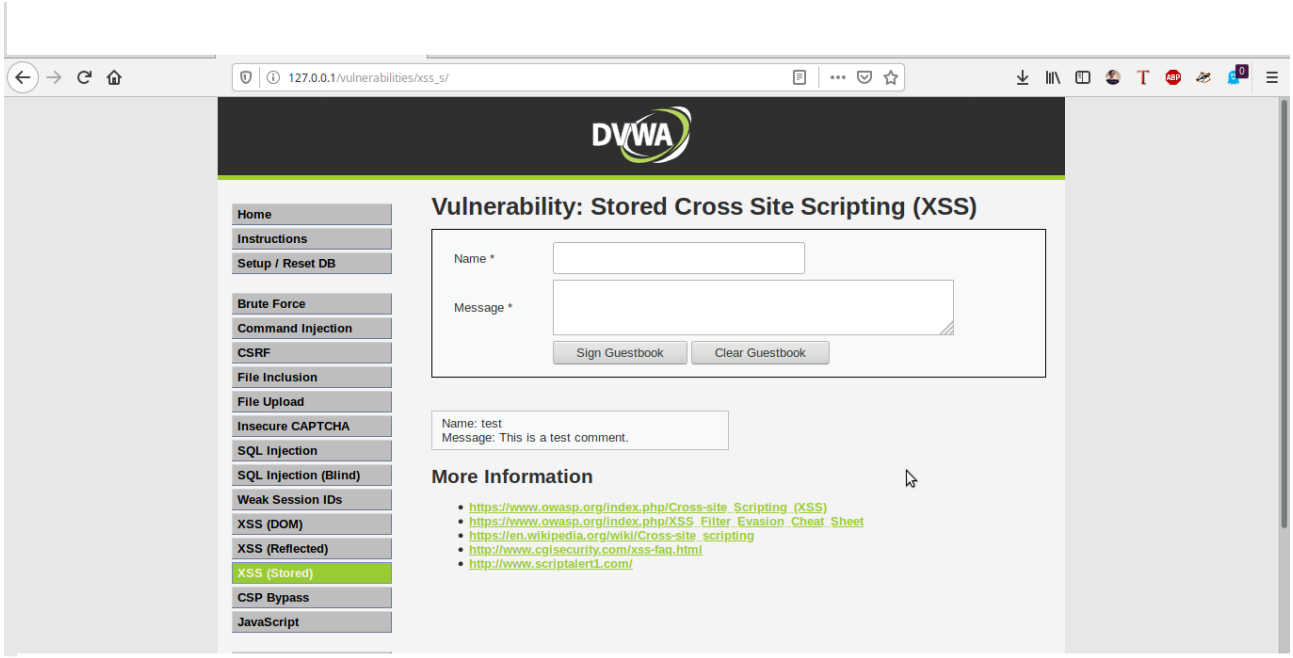
-> Refletido

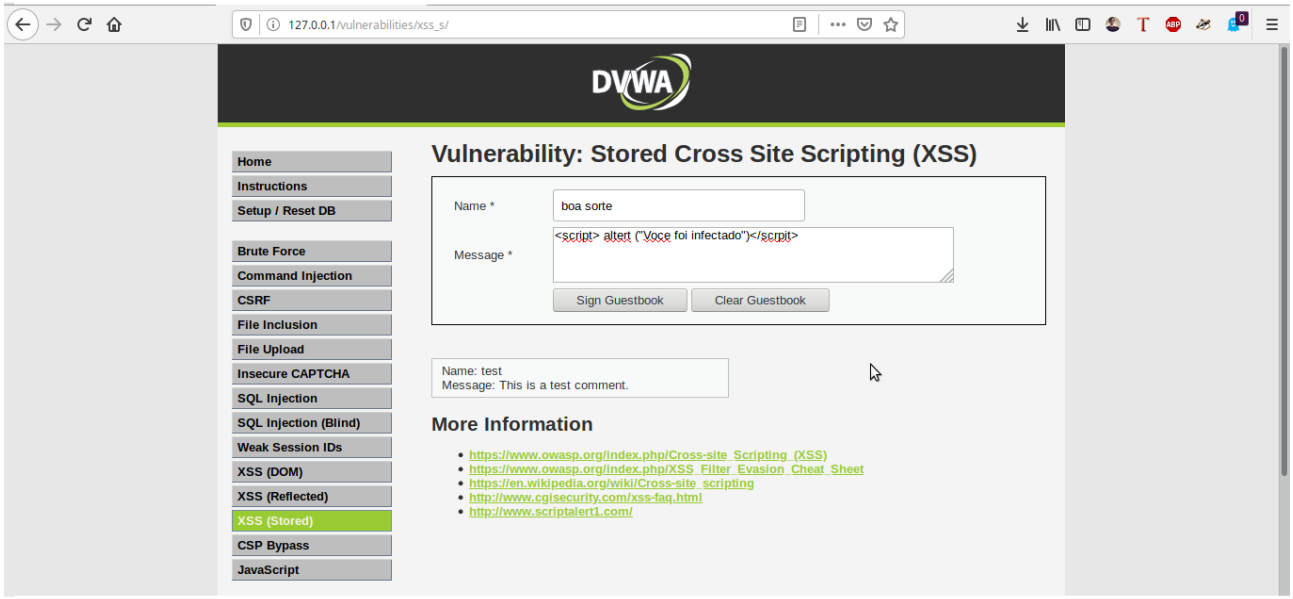
É quando o código é passado pelo hacker de forma direta sem ser filtrado, dessa forma não é armazenado e é executado na hora. Reflete o que foi mandado pelo usuário.

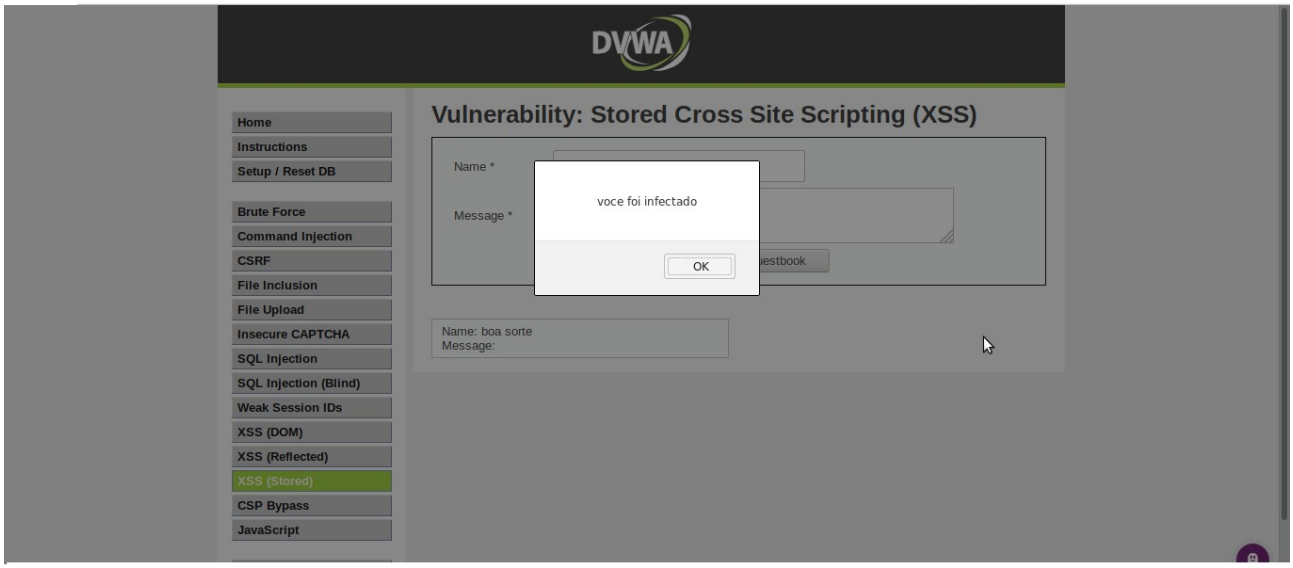
-> Baseado em DOM

É quando o código inserido é disparado no momento de execução do cliente. O Hacker injeta um código (javascript por exemplo) que irá executar pela mudança de uma estrutura da página, mas sem alterar o código fonte.

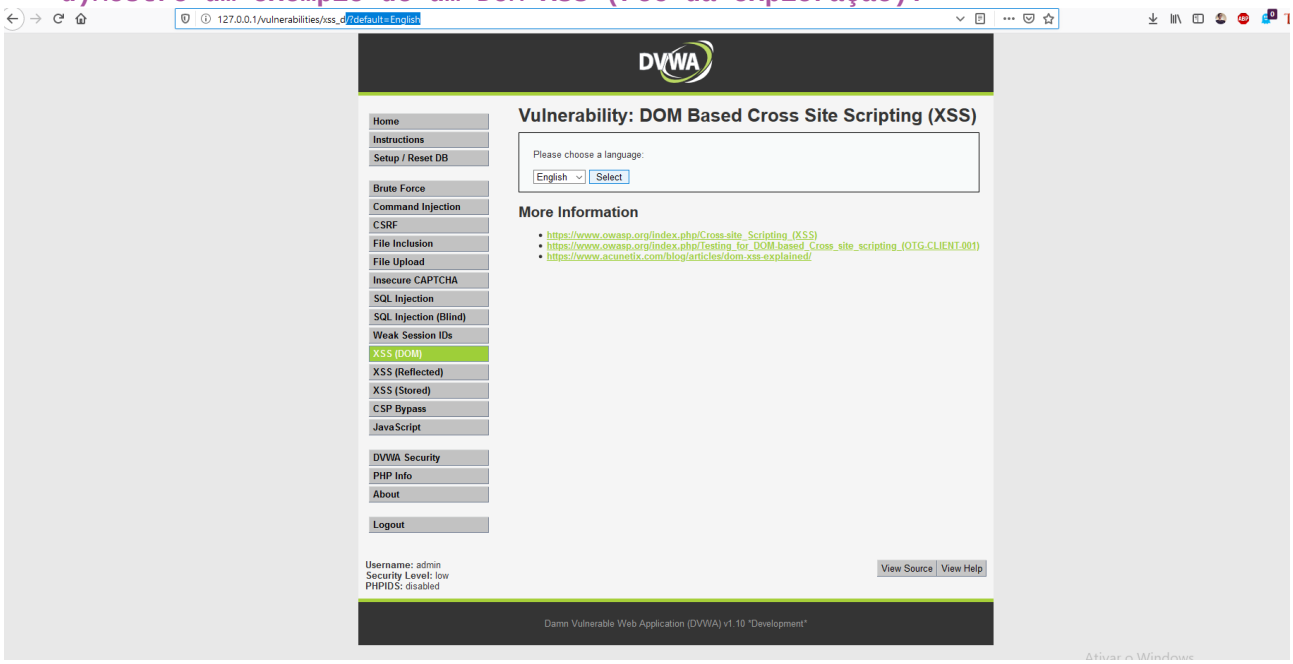
c) Mostre um exemplo de um XSS Stored (PoC da exploração).

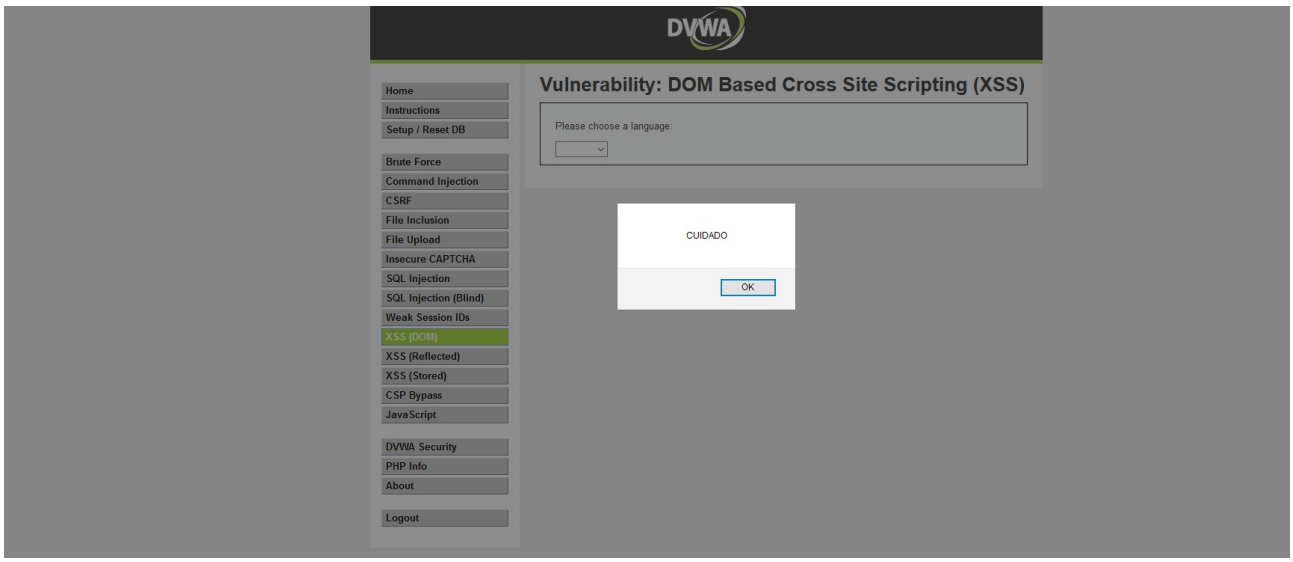






d)Mostre um exemplo de um DOM-XSS (PoC da exploração).





12) LFI , RFI e Path Traversal

a) O que é LFI?

É quando colocamos arquivos que já estão no servidor dentro de outras pastas deste, uma forma é injetar código em arquivos já existentes.

b)O que é RFI?

É muito parecido com o anterior, só que no lugar de usar injeção de código em arquivos existentes no servidor você usa arquivos remotos.

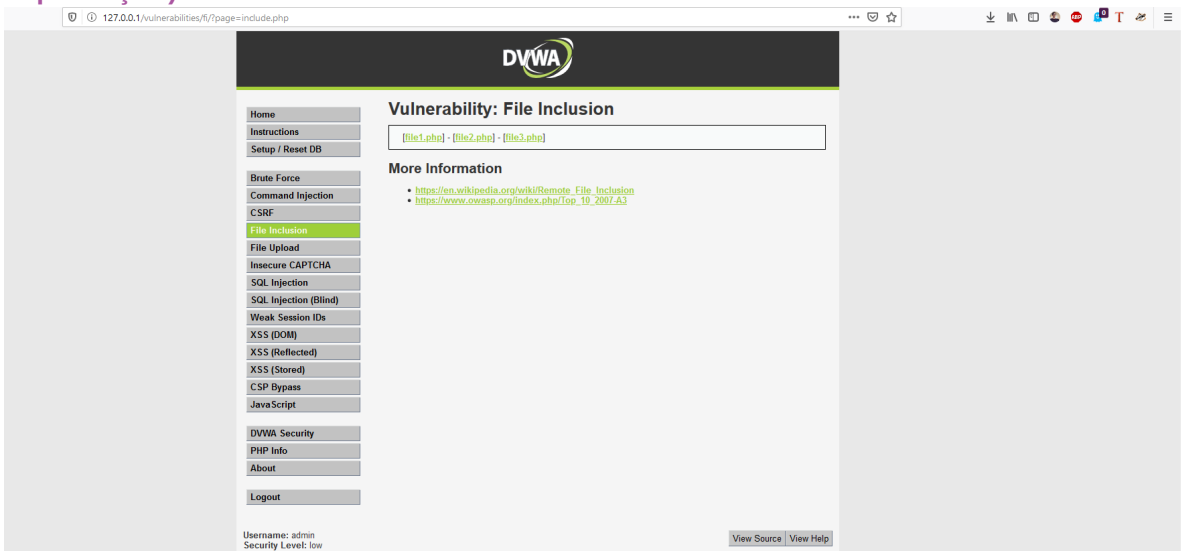
c) O que é Path Traversal?

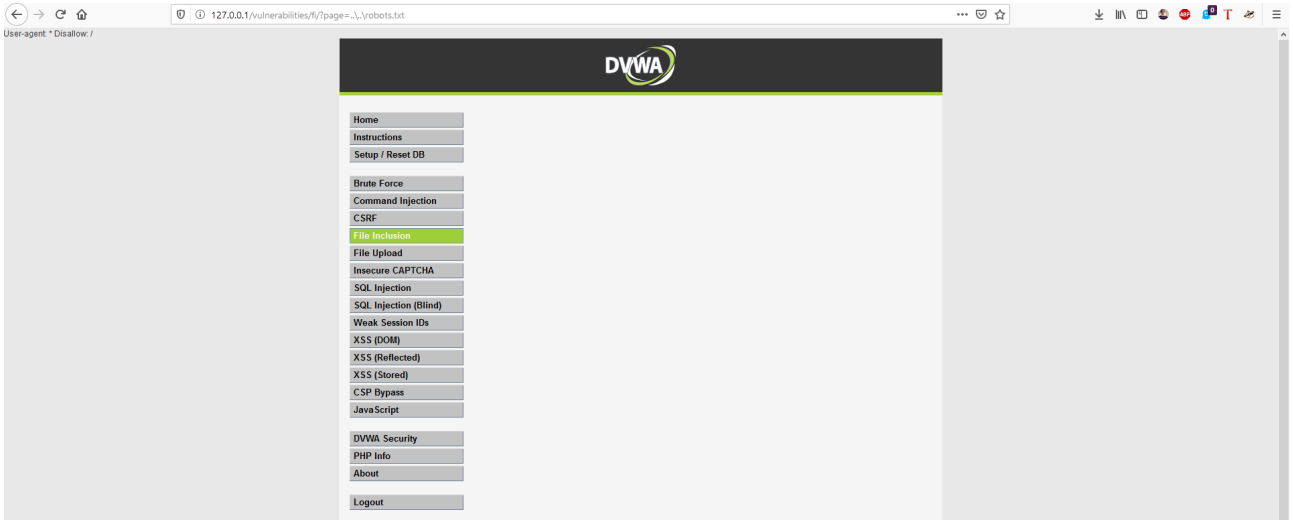
É o processo de usar ../ para andar dentro do servidor (na url) através de arquivos e acessar arquivos que não deviam ser acessadas.

d)Como aliar Path Traversal e LFI

Usando o Path Traversal você pode ter acesso a arquivos para aplicar o LFI.

e) Mostre um exemplo de LFI utilizando a contaminação de LOGS (PoC da exploração).





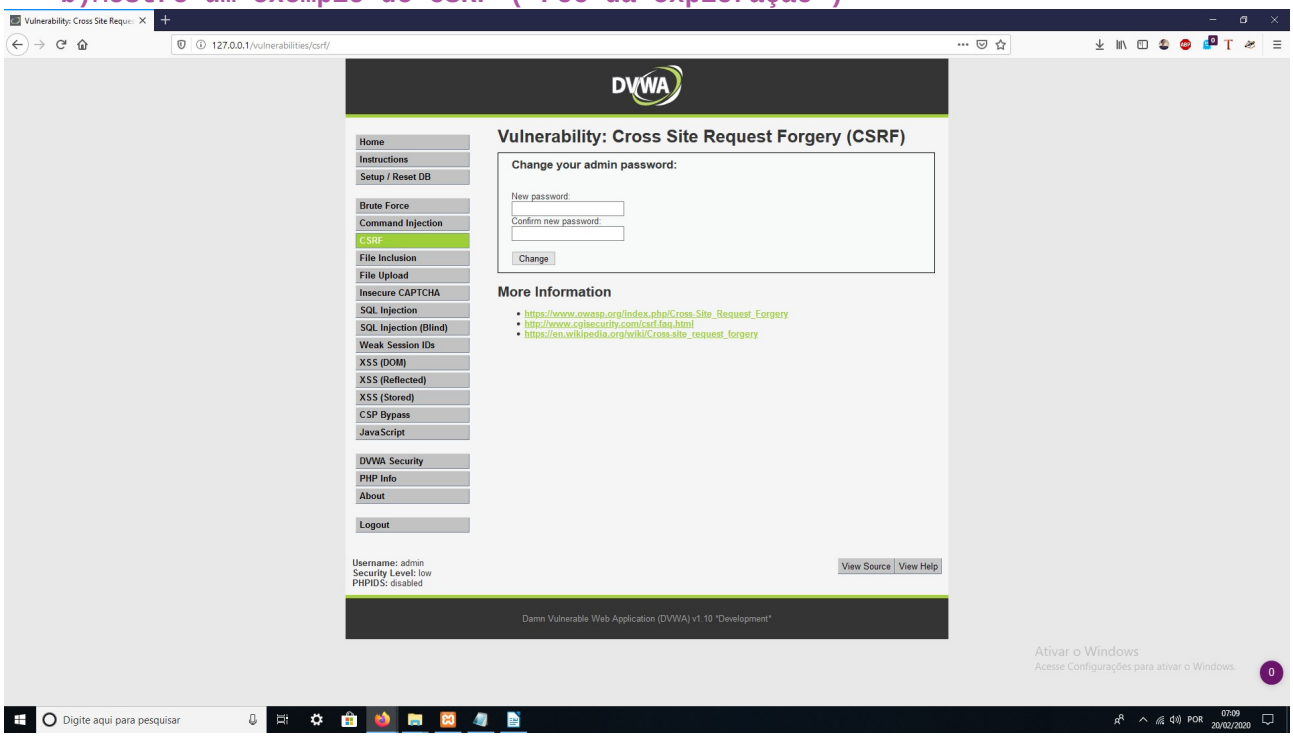
13) CSRF e SSRF

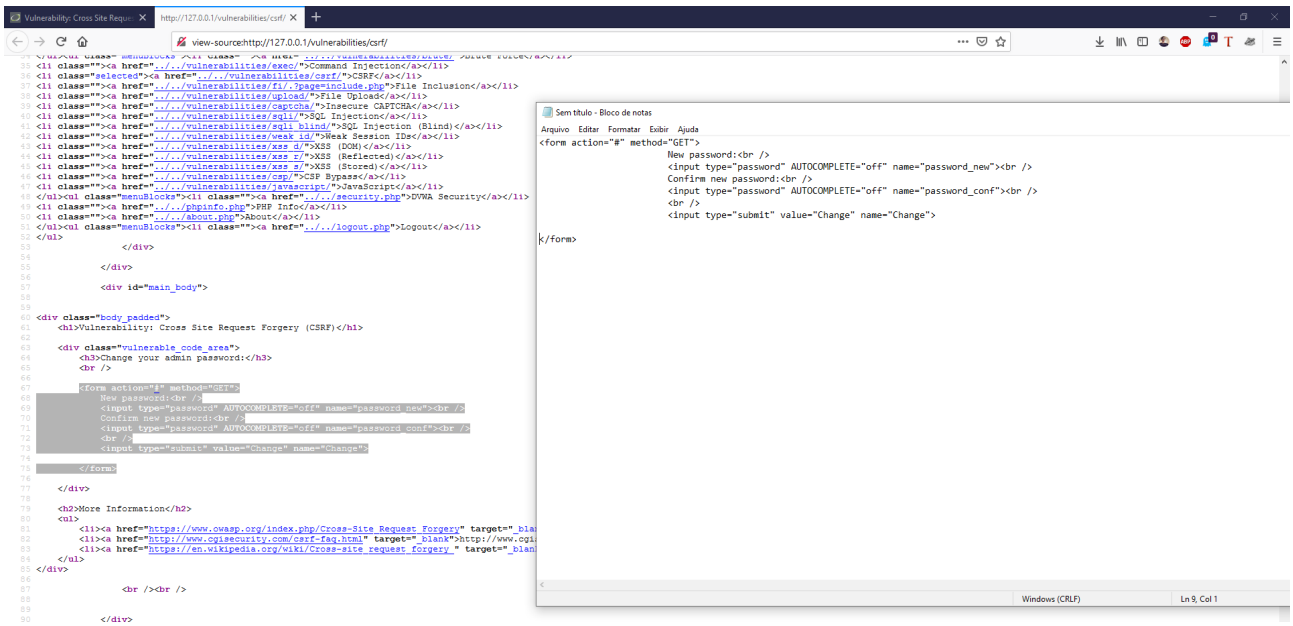
a) O que e CSRF?

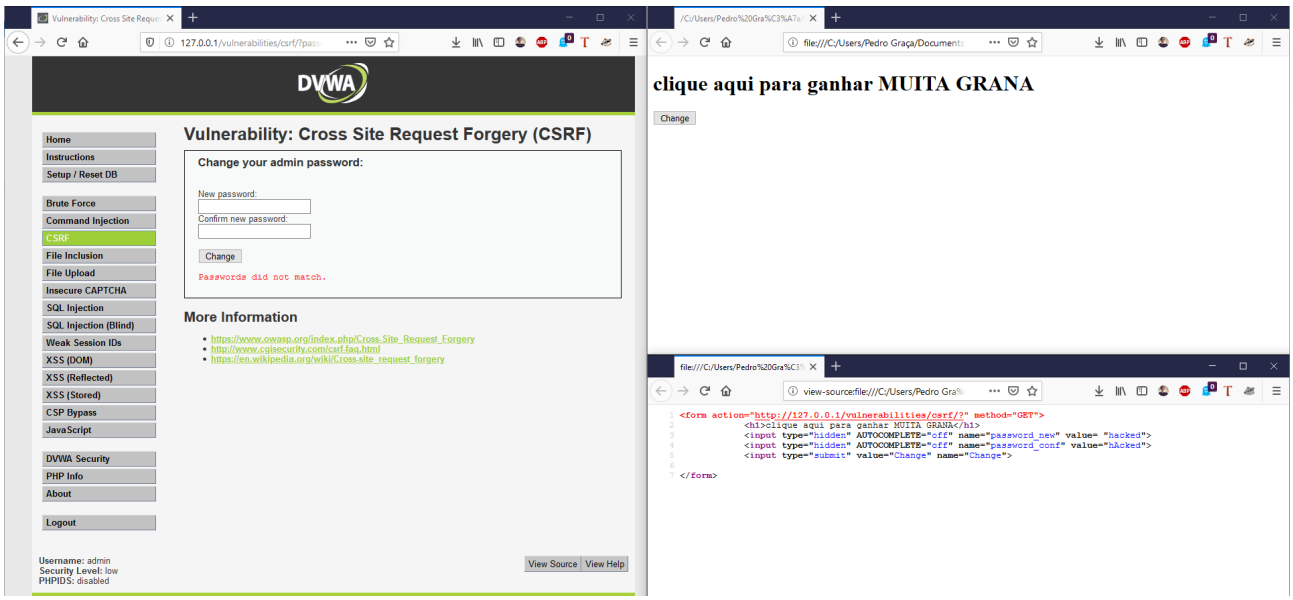
Este, ao contrário do xss, explora a confiança que um site
CSRF explora a confiança que um site tem no navegador de um usuário e não a confiança que um usuário tem no site.]

A ideia principal é iludir o navegador e fazer este enviar as solicitações HTTP para outro site, roubando dados sensíveis.

b)Mostre um exemplo de CSRF (PoC da exploração)



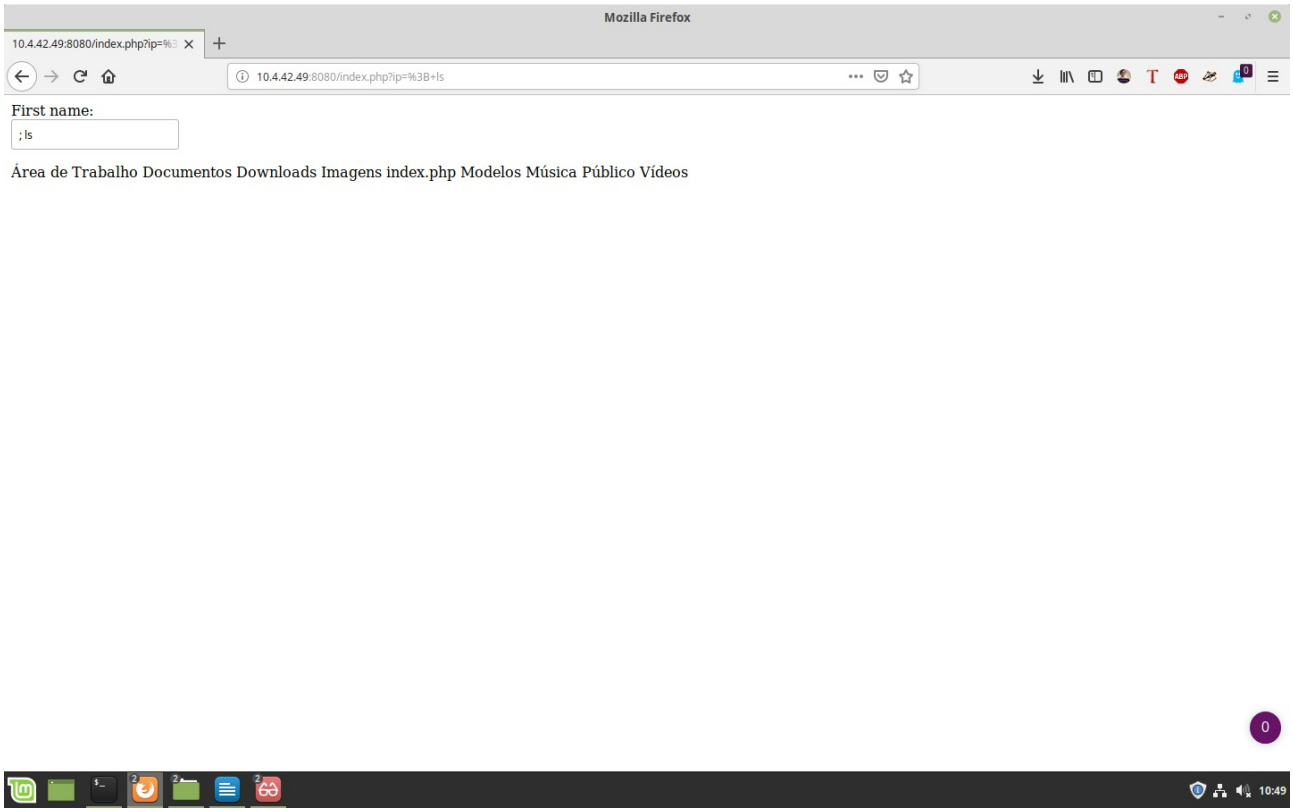


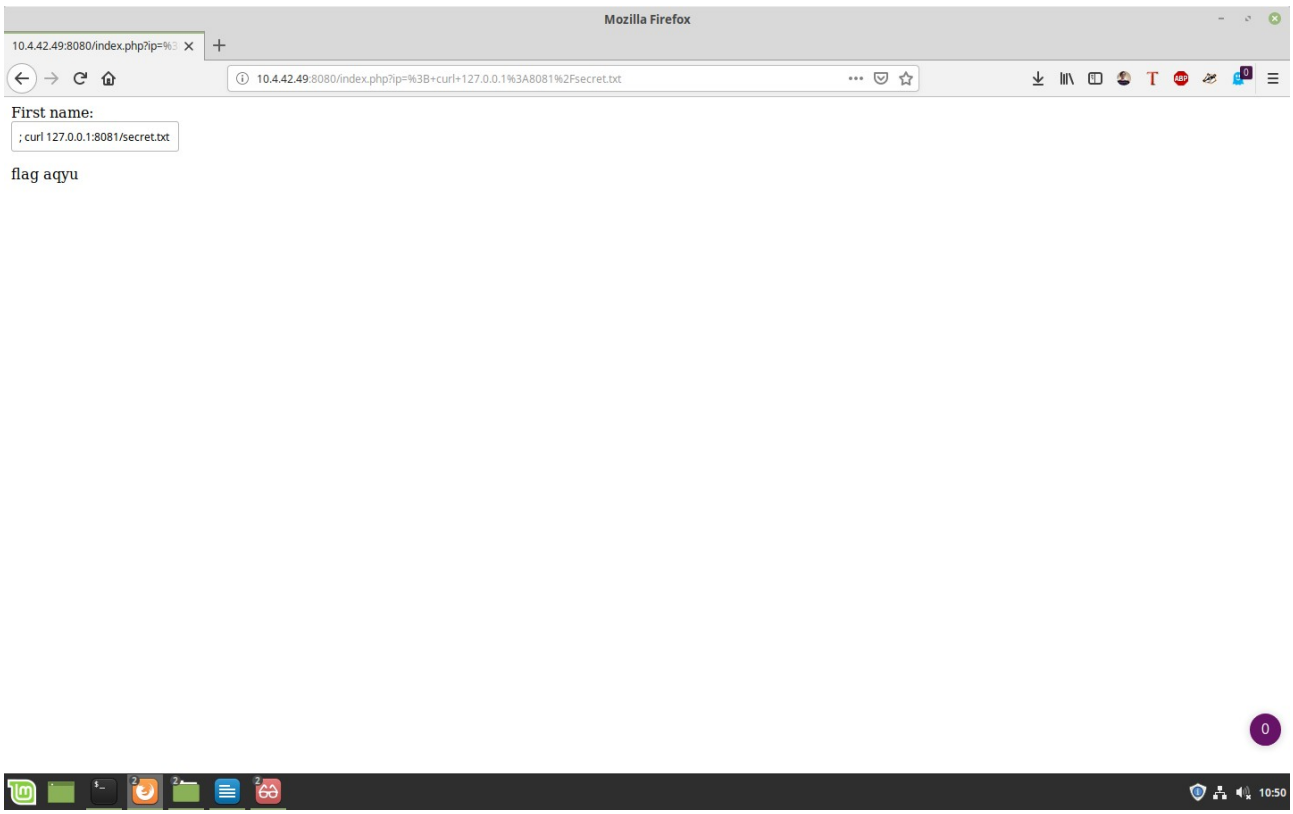


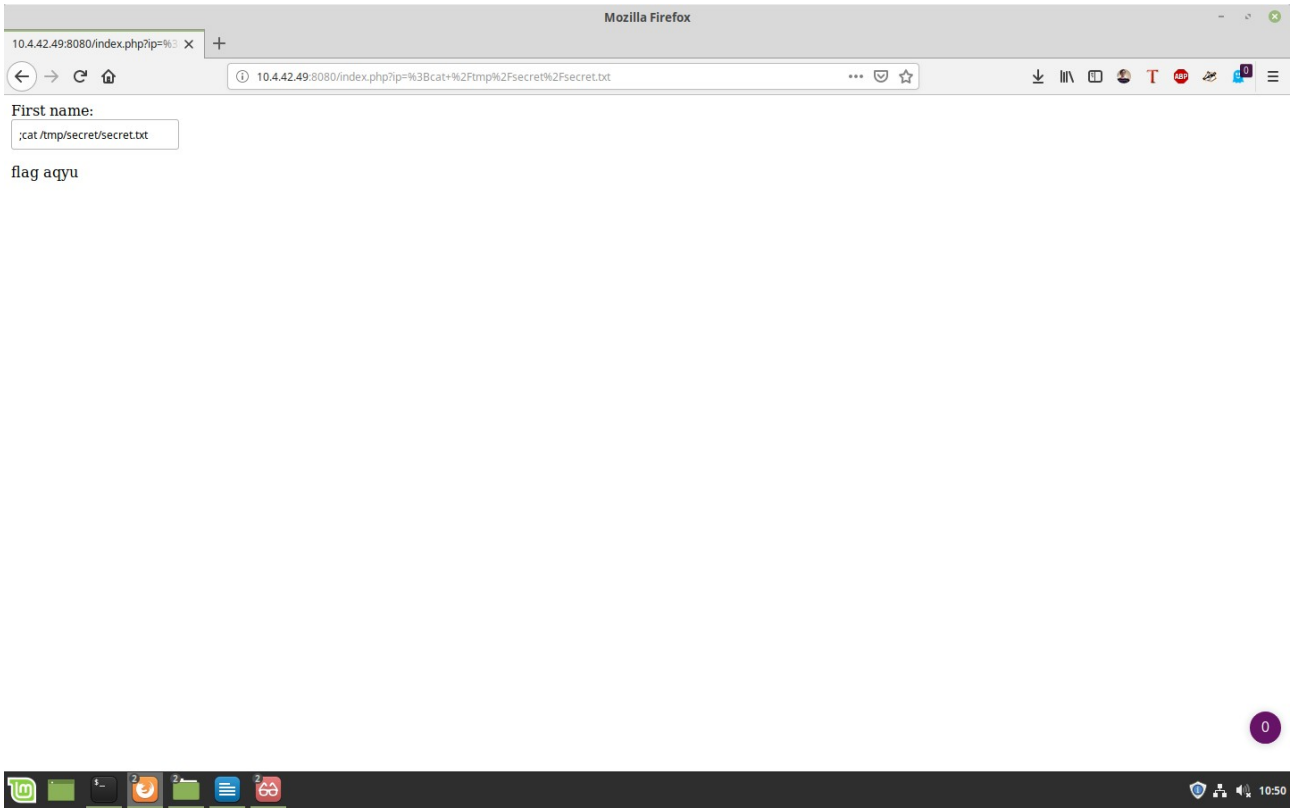
c) O que e SSRF?

E quando abusamos de uma função de um servidor manipulando as informações desse.

d)Mostre um exemplo de SSRF


Mozilla Firefox
10.4.42.49:8080/index.php?ip=%3
10.4.42.49:8080/index.php?ip=%3B+ls
First name:
; ls
Área de Trabalho Documentos Downloads Imagens index.php Modelos Música Público Vídeos
0
10:49


Mozilla Firefox
10.4.42.49:8080/index.php?ip=%3
10.4.42.49:8080/index.php?ip=%3B+curl+127.0.0.1%3A8081%2Fsecret.txt
First name:
; curl 127.0.0.1:8081/secret.txt
flag aqyu
0
10:50



e) Como evitar ataques de CSRF?

Desativar o recurso “lembrar-me”, instalar plugins que nega pedidos de cross-site (o que pode atrapalhar o funcionamento de vários sites), limitar o tempo de vida de cookies. Existem plugins “inteligentes” que tentam bloquear partes de pedidos de cross-site se percever atividade maliciosa, como o CsFire.