

Nome: Thomaz Veloso Rebelo da Silva

Data: 16/02/2020

## **TODAS AS POCS ESTÃO NO FINAL DO ARQUIVO**

### **Perguntas:**

#### **1- O que é o protocolo HTTP e Como ele funciona?**

O HTTP(HiperText Transfer Protocol) é um protocolo para transferência de arquivos, principalmente entre servidor e client,frequentemente usado na internet. Após ser aberta uma comunicação com o servidor, o client faz uma requisição de um arquivo, o servidor, caso encontre, manda o arquivo junto com um Response Code e acaba com a conexão,se isso nao acontecer ele envia um erro (outro Response Code). Então, o navegador procura por possíveis outros arquivos que são requisitos, e repete o processo para os arquivos requisitos (fazendo uma recursão) até receber o Response Code para encerrar a sessão.

#### **2- O que é um Response Code? Cite um exemplo de um programa que você pode fazer com ele?**

É o código de Status da Requisição, se deu certo, ocorreu algum erro, entre outros. Pode-se criar um programa que avalia o Código de Resposta e reporta se deu certo ou não, e a partir disso pode ser feito um Crawler(rastreador de redes).

#### **3- O que é um HEADER? Cite um uso INSEGURO desse cabeçalho.**

Header(cabeçalho), onde ficam informações adicionais sobre a requisição/respost que pode ser ou não necessárias para a comunicação. O header pode ter informações sobre o servidor.

#### **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.**

São duas formas de enviar comandos ou informações para algum servidor o GET envia formulários e informações pela url e o POST faz a mesma coisa mas pela requisição.O POST além de ser mais seguro pois como e por requisição não existe url para ficar salva e também se pode enviar mais dados com ele

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

O Cache é um armazenamento que guarda sites recentemente visitados. Quando o servidor retorna um arquivo, geralmente ele manda a data de expiração do último assim evitando transferência de dados que não existem necessidades de serem feitos. Cache-control, Pragma, Expires, Validators.

## **6- O que é Cookie? Qual é o principal ataque relacionado a ele?**

Cookie é um registro de sessão, serve para o servidor lembrar dos acessos recentes. Cookie Stealing.

## **7- O que é OWASP-Top-Ten?**

O OWASP-Top-Ten é um documento que fala sobre os maiores riscos de segurança para aplicações web.

## **8- O que é Recon e Por que ela é importante?**

Recon refere-se a prática de fazer o reconhecimento do Sistema a ser atacado, seja quais softwares estão sendo usados, suas versões, outros diretórios e arquivos, entre outros.

## **9-Command Injection (SO-Injection)**

### **a) O que é Command Injection?**

Quando por meio de manipulação de entrada um comando é injetado (rm -fr/).

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

Foi feito em servidor privado dentro do LEP1

String usada no campo: "; curl 127.0.0.1:8081/secret.txt"

## **10- SQL INJECTION**

### **a) O que é SQL injection?**

Quando por meio de manipulação de entrada um comando de SQL é injetado (Login: ' ; /\* Passowrd: \*/ OR 1 = 1 -- )

### **b) O que é Union Based Attack?**

São ataques a sistemas SQL baseados no comando UNION, e com certa facilidade consegue extrair informações sobre o banco de dados.

### **c) O que é Blind-SQL-I?**

São ataques onde não se vê o resultado da Query SQL.

## **11- XSS**

### **a) O que é XSS?**

Cross-Site Scripting, quando coloca um código e o client roda esse código.

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

Não persistente: Mais comum, é um script que roda apenas uma vez, ou quando o script é injetado, seja numa barra de busca, ou outra coisa. Persistente: Ocorre quando é o script injetado vira algo permanente no site, como uma resposta em um fórum ou descrição num site de bate papo.

**c/d) Mostre um exemplo de um XSS Stored / Mostre um exemplo de um DOM-XSS**

Para ambos foram usados o site: <http://xss-game.appspot.com> XSS Stored está exemplificado na POC feito apartir do lvi 2.XSS DOM-XSS está exemplificado na POC:feito apartir do lvi 1.

**12- LFI , RFI e Path Traversal**

**a) O que é LFI?**

Local File Inclusion: processo onde inclui-se arquivos já existentes no servidor, geralmente acontece com servidores PHP.

**b) O que é RFI?**

Remote File Inclusion: processo onde inclui-se arquivos que não existiam no servidor.

**c) O que é Path Traversal?**

Usar '../' para acessar pastas anteriores.

**d) Como aliar Path Traversal e LFI**

Pode-se usar o '../' para que seja incluído o arquivo 'etc/passwd' no sistema.

**e) Mostre um exemplo de LFI utilizando a contaminação de LOGS**

Explicado em sala tentei o site da shelterlabs mas eles caíram.

**13- CSRF e SSRF**

**a) O que é CSRF?**

Cross-Site Request Forgery: o atacante se aproveita da confiança do servidor para enviar ou realizar algo malicioso.

**b) Mostre um exemplo de CSRF**

**c) O que é SSRF?**

Server-Site Request Forgery: o atacante faz o servidor abrir uma conexão para outro endereço, muitas vezes ganhando acesso privilegiado.

**d) Mostre um exemplo de SSRF**

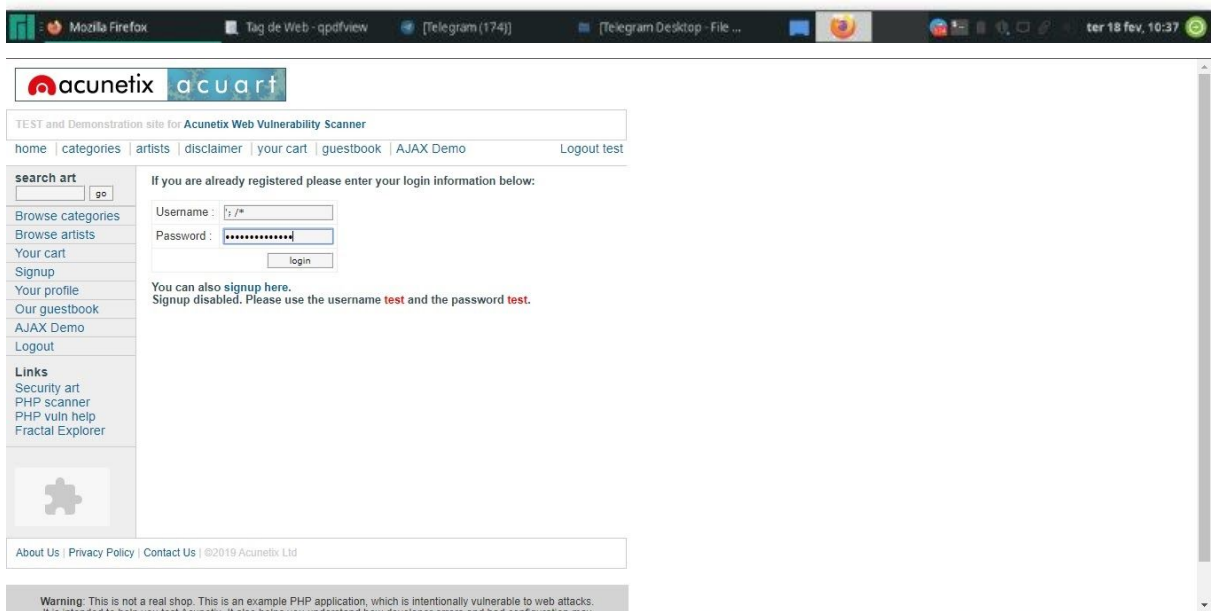
Foi feito em servidor privado dentro do LEP1

String usada no campo: "; curl 127.0.0.1:8081/secret.txt"

**e) Como evitar ataques de CSRF?**

Para usuários:Realizar logout,nao usar o "Lembre-se de mim"

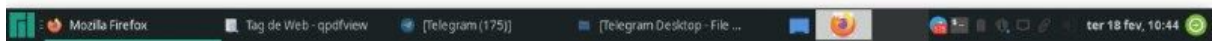
Para servidor:Reduzir a vida útil dos Cookies





First name:

flag aqyu



execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

### Mission Objective

Inject a script to pop up a JavaScript `alert()` in the frame below.

Once you show the alert you will be able to advance to the next level.

### Your Target

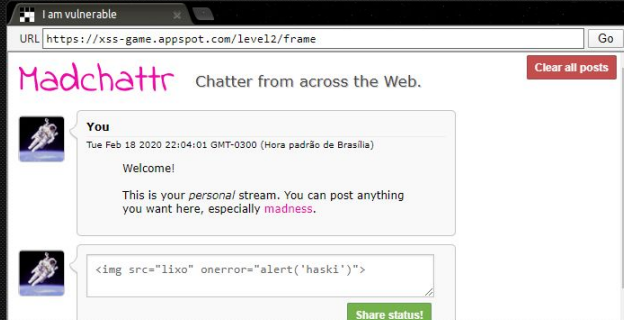


Target code (toggle)

Inject a script to pop up an `alert()` in the context of the application.

**Note:** the application saves your posts so if you sneak in code to execute the alert, this level will be solved every time you reload it.

### Your Target



Target code (toggle)

Hints 0/3 (show)