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

É uma sigla para HiperText Transfer Protocol, um protocolo para trasferência 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 encerra a conexão. Caso contrário, envia um erro (que também é um tipo de Response Code). Então, o navegador procura por possíveis outros arquivos que são requisitos, e repete o processo para os arquivos requisitos (de uma forma recursiva).

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 apartir disso construir um Crawler.

3) O que é um HEADER? Cite um uso INSEGURO desse cabeçalho.

É o cabeçalho, onde fica informações adicionais sobre a requisição/resposta 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 maneiras de enviar informações e comandos para um servidor. POST envia informações, como submissão de um formulário, pela requisição, enquanto o GET realiza a mesma tarefa, porém pela URL. Dessa forma, além de ser mais seguro (as informações não ficam salvas junto com as urls no histórico no navegador), o POST também permite enviar mais dados.

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 pultimo cache, assim podendo evitar uma transferência de dados desnecessária. 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 "se lembrar" do client em acessos recentes. Cookie Stealing.

7) O que é OWASP-Top-Ten?

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

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

Recon (reconhecimento, em inglês) refere-se a prática de 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)

** FEITO JUNTO COM 13d **
Foi feito em servidor privado dentro do LEP1

Imagens: "ssrf cmd injection.png" e "ssrf cmd injection2.png"
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.

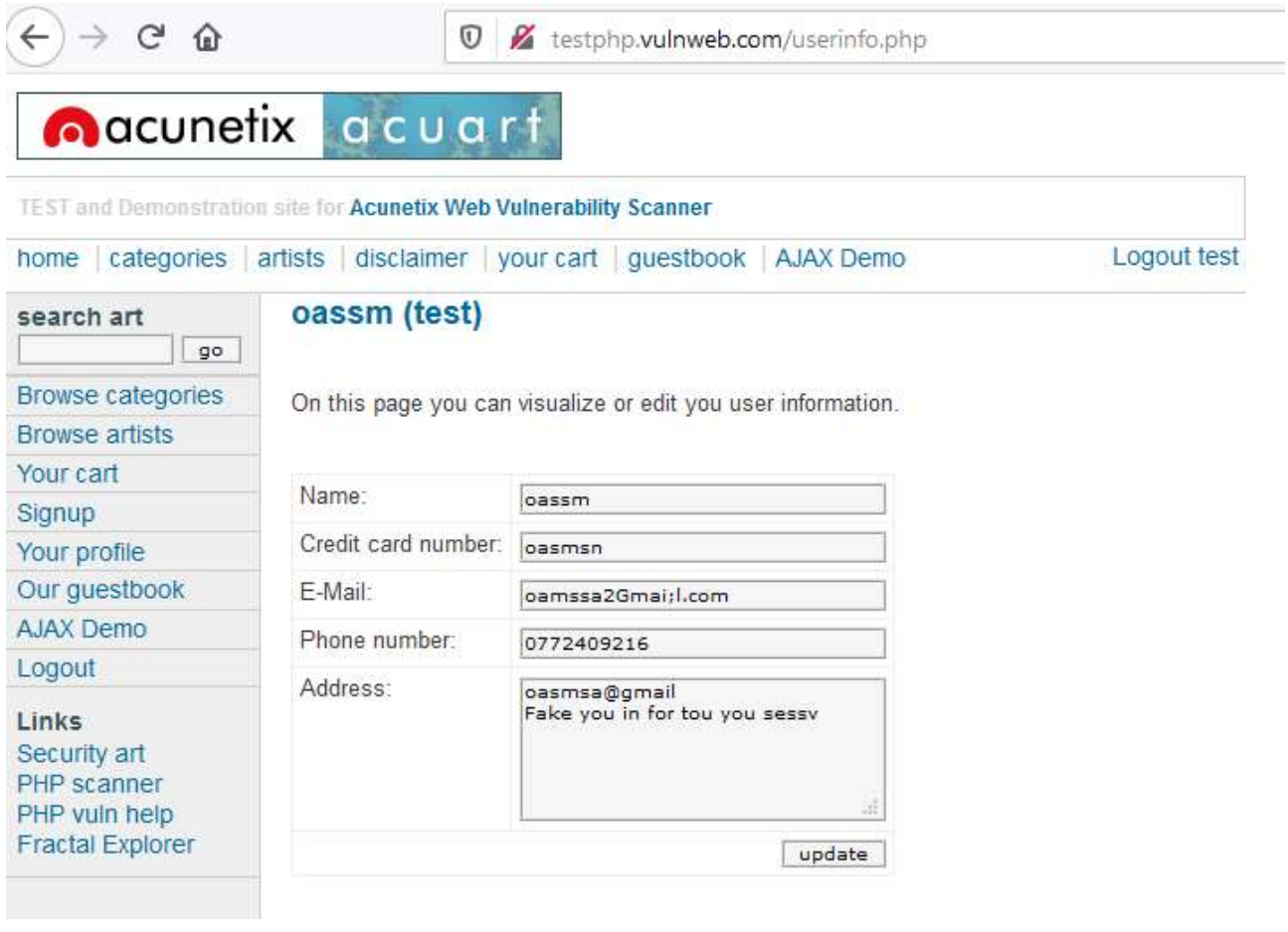
c) O que é Blind-SQL-I?

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

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

Usando site: testphp.vulnweb.com


testphp.vulnweb.com/login.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username : ' /*
Password : ••••••••••••••
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd


testphp.vulnweb.com/userinfo.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
oassm (test)
On this page you can visualize or edit you user information.
Name: oassm
Credit card number: oasmsn
E-Mail: oamssa2Gmai;l.com
Phone number: 0772409216
Address: oasmsa@gmail
Fake you in for tou you sessv
update

Imagens: "sql injection.png" e "sql injection2.png"
Senha usada: "*/ OR 1 = 1 -- "

11) XSS

a) O que é XSS?

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

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

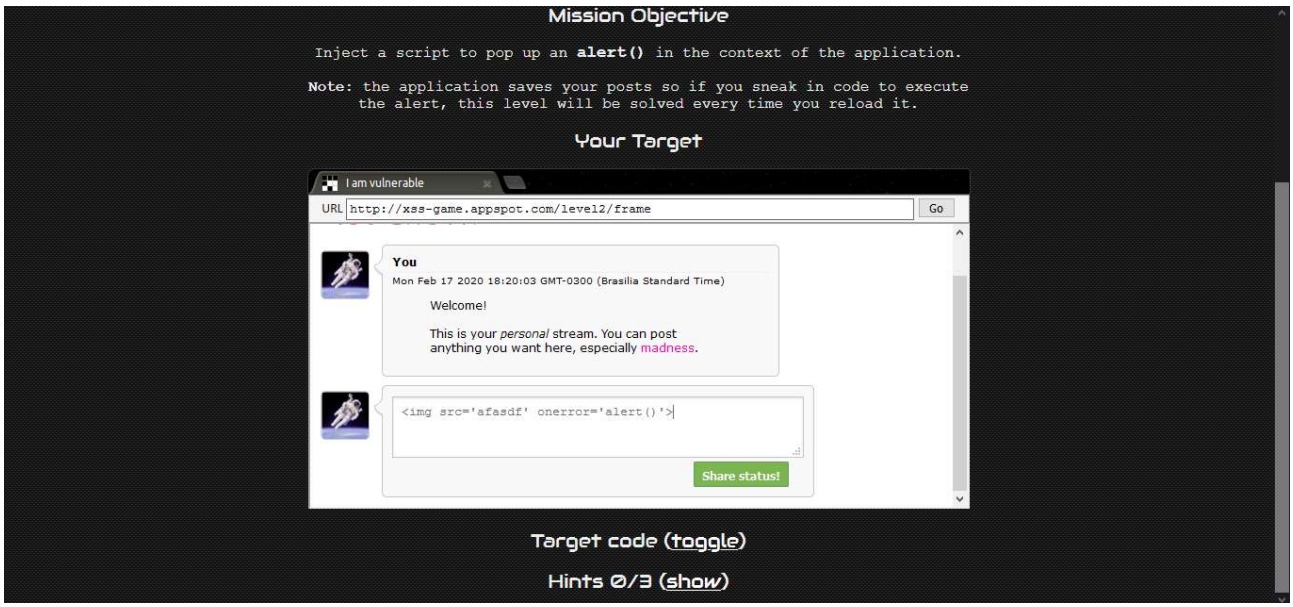
Não persistente: Mais comum, é um script que roda apenas uma vez, ou quando o script é injetado, seja numa barra de busca, ou outra coisa.

Persistente: Ocorre quando é o script injetado vira algo permanente no site, como uma resposta em um forúm ou descrição num site de bate papo.

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

Site: http://xss-game.appspot.com

XSS Stored está exemplificado na imagem: "xss injection stored" feito apartir do lvl 2.



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

Site: http://xss-game.appspot.com

XSS DOM-XSS está exemplificado na imagem: "xss injection dom" feito apartir do lvl 1.

12) LFI , RFI e Path Traversal

a) O que é LFI?

Local File Inclusion: processo onde inclui-se arquivos já existentes no servidor.

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 incluido o arquivo 'etc/passwd' do sistema.

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

13) CSRF e SSRF

a) O que e CSRF?

Cross-Site Request Forgery: o atacante força a vítima a enviar um request para o mesmo ou outro servidor, e assim adquirir algum privilégio.

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

Feito no site: https://portswigger.net/web-security/csrf/lab-no-defenses

Body:

```
<form method="POST"
action="https://ac671f661edfb47080167de200d10015.web-security-
academy.net/email/change-email">
     <input type="hidden" name="email" value="myemail@gmail.com">
</form>
<script>
      document.forms[0].submit();
</script>
```

Store | View exploit | Access log

Imagem: "csrf burp.png"

c) O que e 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 (PoC da exploração)

** FEITO JUNTO COM 9b **

Foi feito em servidor privado dentro do LEP1

Imagens: "ssrf cmd injection.png" e "ssrf cmd injection2.png"
String usada no campo: "; curl 127.0.0.1:8081/secret.txt"

e) Como evitar ataques de CSRF?

Para clientes:

- Realizar logout
- Evitar "Lembre-se de mim"

Para servidor:

- Reduzir o tempo de vida dos Cookies
- Usar CSRF Token
- Confirmação de senha antes de qualquer requisição importante