

PORTSWIGGER

Relatório

Gabriel Oliveira

HTTP Host header attacks

PORTSWIGGER

Relatório

HTTP Host header attacks

Relatório sobre host header attacks.

Aluno: Gabriel Oliveira

Julho
08/2021

Sumário

1 O que é?

1.1 Virtual Hosting

1.2 Routing traffic via an intermediary

2 Laboratórios

2.1 Basic password reset poisoning

1 O que é?

HTTP Host header é um cabeçalho de solicitação referente ao HTTP 1.1. Sempre que o usuário tentar acessar um domínio, o navegador irá enviar uma requisição ao servidor desse determinado domínio com o seguinte conteúdo:

Caso acessarmos o web site abaixo

<https://portswigger.net/web-security>

teremos o seguinte cabeçalho:

```
GET /web-security HTTP/1.1
Host: portswigger.net
```

Em alguns casos, é possível realizar a mudança no campo host antes da requisição chegar ao servidor do web site. A finalidade do mesmo é basicamente direcionar a requisição a sua real finalidade. Se o cabeçalho http estiver mal formado ou simplesmente não possuir o cabeçalho, gerará problemas para rotear as requisições de entrada.

Essa ambiguidade não exestiria, pois um único endereço de IP iria dar acesso a uma aplicação web, porém nos tempos atuais com o avanço da tecnologia e o esgotamento do endereço IPV4, várias aplicações web são acessadas por um único endereço de IP.

1.1 Virtual Hosting

Web-sites que são armazenados em um único servidor, ou seja, possuem o mesmo endereço de IP, dessa forma são denominados de “Virtual Hosting”.

1.2 Routing traffic via an intermediary

Nesse caso, os websites são armazenados em diferentes servidores. Porém, cada acesso a esse determinado website a requisição é resolvida sempre para o mesmo IP de acesso.

2 Laboratórios

2.1 Basic password reset poisoning