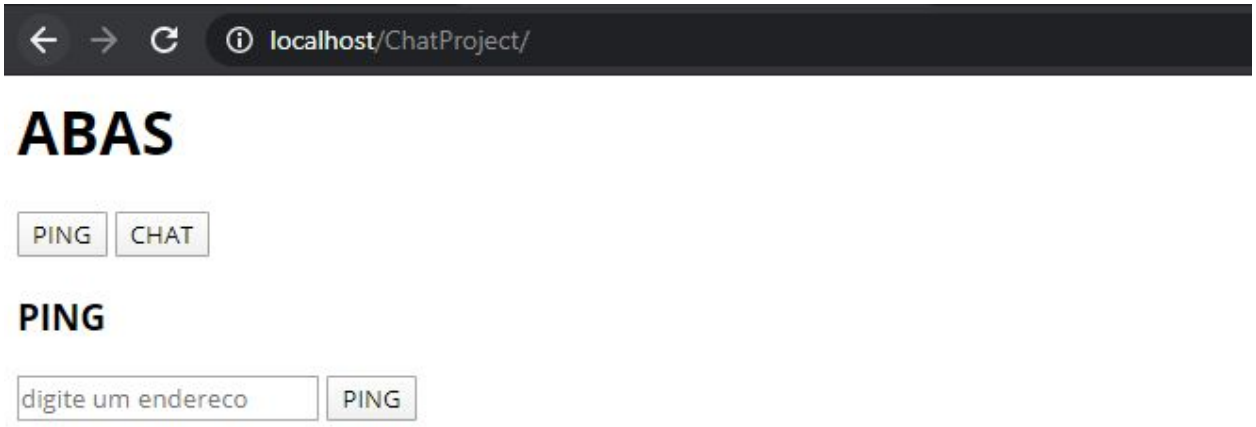
Giovanni Dhery Silva Prieto

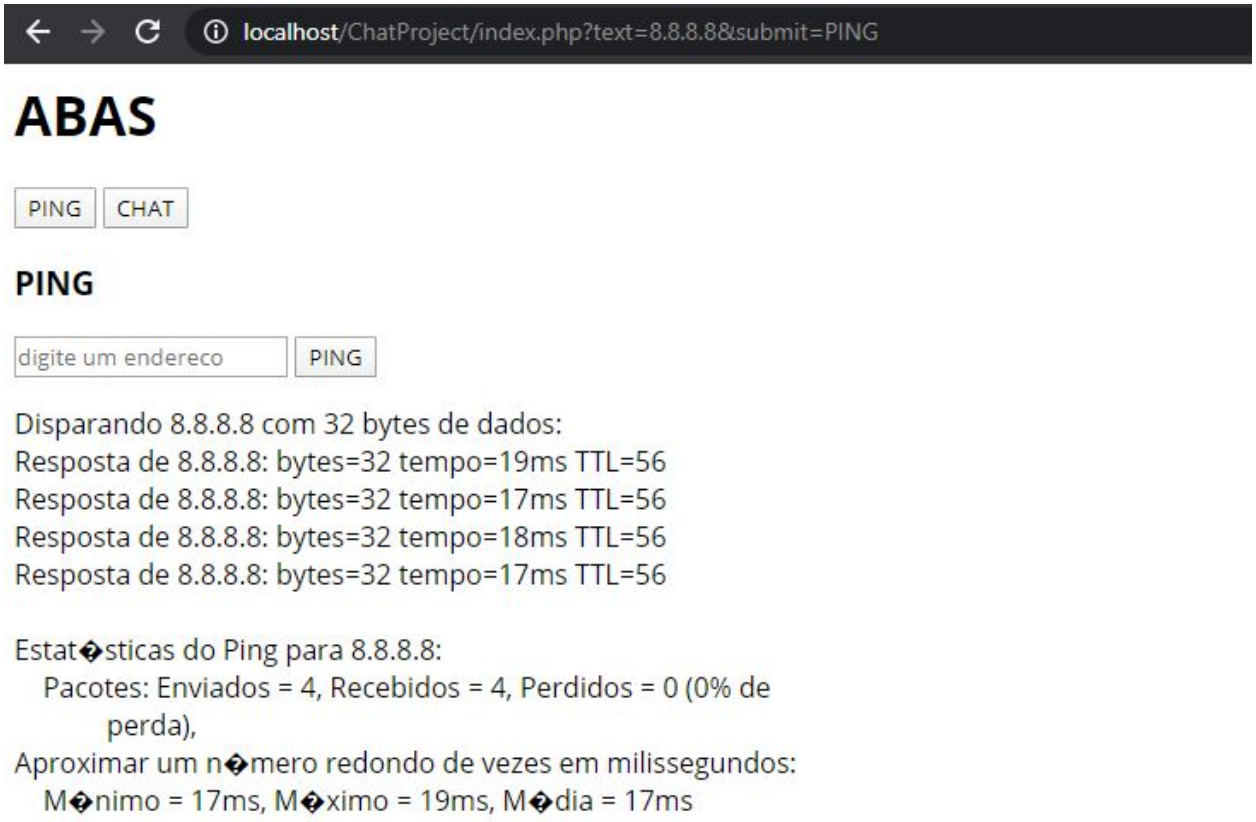
TAG Segurança Ofensiva Ataque: Command Injection

Command injection é uma vulnerabilidade em que se torna possível injetar comandos no shell do host por conta de alguma má sanitização de dados.

O exemplo abaixo foi feito com auxílio do Xampp server e em ambiente controlado.



Como podemos ver acima, há uma janela com uma aba de chat e outra de ping. Quando você insere um endereço, o servidor executa o comando ping e até o endereço que o usuário colocou.



Para saber se esse servidor é vulnerável a injeção de comando, é necessário inserir algum outro comando e ver se há impressão do resultado do mesmo na tela, aplicando uma concatenação de comandos do shell para que seja possível.

É visível que há essa vulnerabilidade, pois ao digitarmos “8.8.8.8 && echo eae, paraziada ”, podemos observar a execução dessa função logo abaixo.

Ao olharmos o código do servidor, vemos que a função responsável por fazer o ping usa a função shell_exec() e sem nenhuma restrição de entrada, fazendo com que qualquer comando concatenado que for inserido seja executado. Isso oferece perigo à máquina, pois algum atacante poderia comprometer as informações dela.

Algumas maneiras de se prevenir contra essa vulnerabilidade são de se ter uma sanitização de entradas, como a não permissão de um grupo de caracteres, não fazer comandos diretamente pelo sistema operacional, se possível, e validar a entrada antes de executar.

```php
<?php

    if(isset($_REQUEST["submit"])){
        $target = $_REQUEST["text"];

        if(strcmp($target,"")==0){
            echo "";
        }
        else{
            $cmd = shell_exec("ping $target" );
            echo "<pre>{$cmd}</pre>";
            }

    }


?>
```