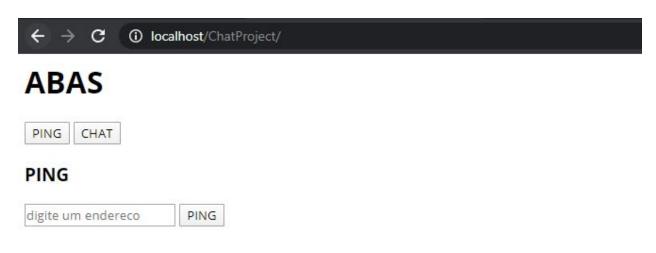
## Giovanni Dhery Silva Prieto

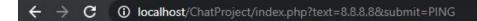
## TAG Segurança Ofensiva Ataque: Command Injection

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.



## ABAS



## PING



Disparando 8.8.8.8 com 32 bytes de dados:

Resposta de 8.8.8.8: bytes=32 tempo=19ms TTL=56

Resposta de 8.8.8.8: bytes=32 tempo=17ms TTL=56

Resposta de 8.8.8.8: bytes=32 tempo=18ms TTL=56

Resposta de 8.8.8.8: bytes=32 tempo=17ms TTL=56

Estat sticas do Ping para 8.8.8.8:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um n�mero redondo de vezes em milissegundos:

M�nimo = 17ms, M�ximo = 19ms, M�dia = 17ms

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.



Estat♦sticas do Ping para 8.8.8.8: Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de

Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=56 Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=56

perda),

Aproximar um n�mero redondo de vezes em milissegundos: M�nimo = 11ms, M�ximo = 16ms, M�dia = 12ms

eae, paraziada

É visível que há essa vulnerabilidade, pois ao digitarmos "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.

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

    if(strcmp($target,"")==0) {
        echo "";
    }

    else{
        $cmd = shell_exec("ping $target");
        echo "{$cmd}";
    }
}
```