Injector

Din titlu ne da un hint ca este o vulnerabilitate de tip command injection.**Command injection** este o vulnerabilitate de securitate care apare atunci când o aplicație permite unui utilizator să introducă date care sunt apoi utilizate direct într-un **comand shell** (de exemplu, într-un script Bash) fără a fi validate sau filtrate corespunzător. Acest lucru le permite atacatorilor să execute comenzi arbitrare pe sistemul gazdă, cu permisiunile aplicației compromise.Pe site putem observa comanda executata anterior si in url adressa ip a comnezi:

http://34.159.151.77:31857/index.php?host=127.0.0.1

```
Command executed: ping -c 2 127.0.0.1
```

De aici putem realiza 2 lucruri ca parametrul host o sa ii fie atribuit adresa ip si dupa atribuire executa comanda ping -c 2 adress . In bash putem executa mai multe comenzi una dupa cealalta prin operatorii: “&&” “||” .

În Bash, putem executa mai multe comenzi succesiv folosind **operatorii de control**:

- `&&` — execută comanda următoare doar dacă prima a avut succes.
- `||` — execută comanda următoare doar dacă prima a eșuat.
- `;` sau `|` — rulează comenzile în ordine sau le leagă printr-un pipe.

De aici Putem realiza Command injection si anume putem trece in url:

http://34.159.151.77:31857/index.php?host=127.0.0.1| ls

```
flag.php
index.phh
```

Care ne va lista tot ce se afla in directorul curent (poti folosi pwd pentru a vedea in ce director te alfi).De aici singurul lucru care mai este de facut este sa fie citit flag.php .In loc de ls sa fie comanda cat flag.php care va rezulta flagul (Atentie aici se va afla in source code click dreapta =>view source code)

CTF{C0mm4nd…..E4sy}

Trolled by masquerade8077