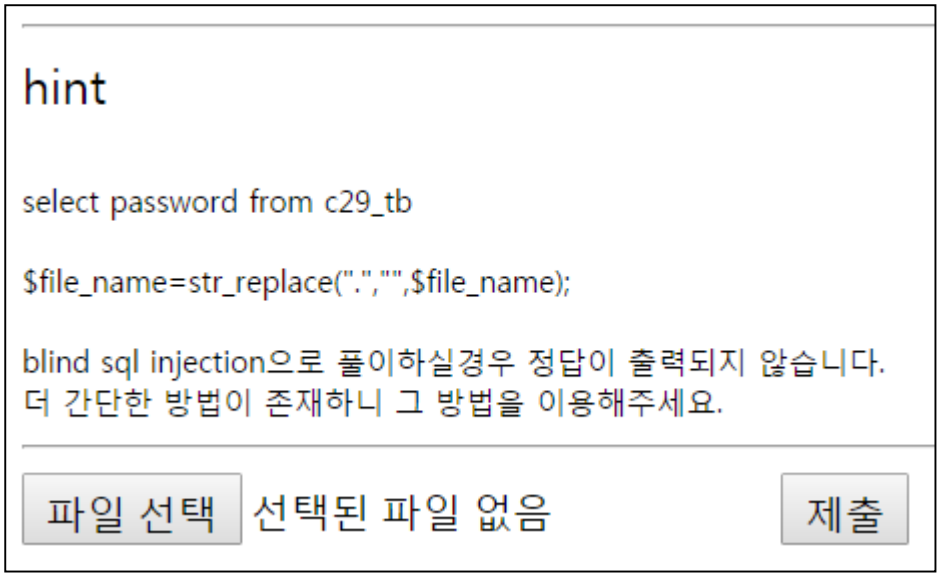
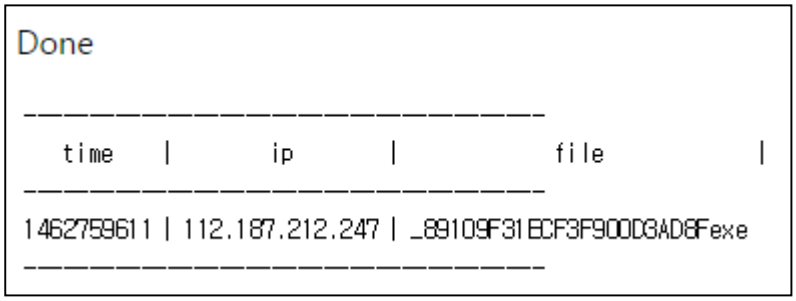
webhacking.kr 29번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-10
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

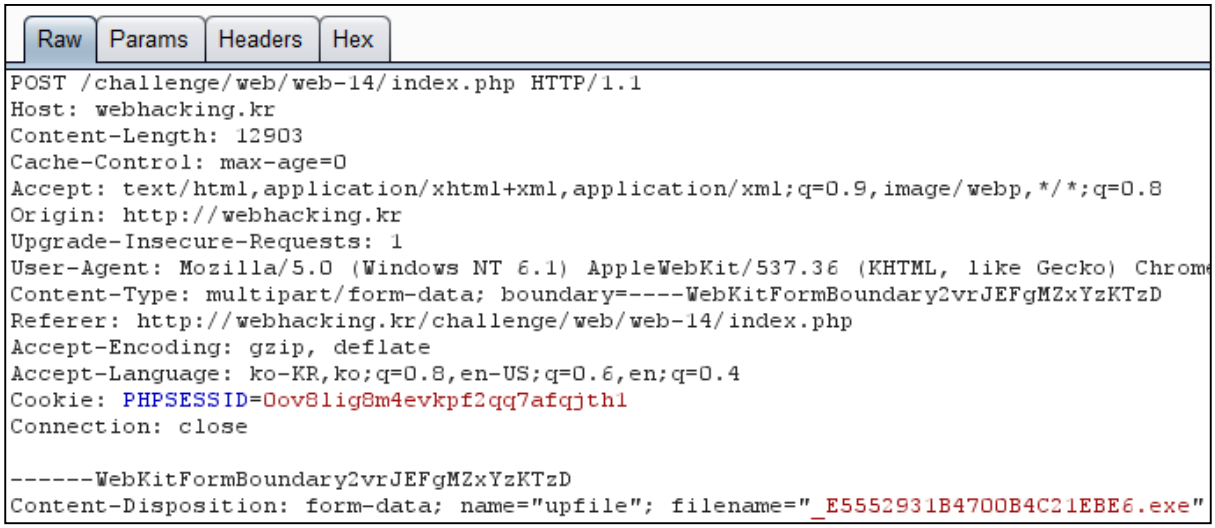
hint와 파일 제출이 가능하다.



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



Burp Suite로 잡아보면 filename 값을 보내는 것을 볼 수 있다.



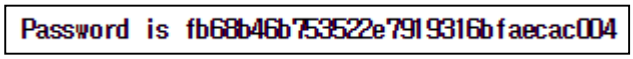
filename에 여러 SQL Injection을 해보다가 insert into되는 순서가 file, time, ip순인 것을 알아냈다.
1', 1, 1)# 로 모두 1 값을 보내보면 Done만 뜨고 업로드가 되지 않는다.
따라서 정상적인 값을 보내보기로 했다.
우선 ipip.kr에서 내 ip를 알아냈다.

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.



Auth에 인증하면 다음과 같이 클리어된다.

KEY : fb68b46b753522e7919316bfaecac004