

PicoCTF 2019 – Irish Name Repo 1

Irish-Name-Repo 1 

Medium Web Exploitation picoCTF 2019

AUTHOR: CHRIS HENSLER

Description

Do you think you can log us in? Try to see if you can login!

This challenge requires us to login to the web app without knowing a valid username / password

SQL Injection – Auth Bypass

Hi. I tried adding my favorite Irish person, Conan O'Brien. But I keep getting something called a SQL Error

That's because Conan O'Brien is American.

We see in another page on the website that this app is vulnerable to SQL injection through inclusion of special characters

SQL Injection – Auth Bypass

Hi. I tried adding my favorite Irish person, Conan O'Brien. But I keep getting something called a SQL Error

That's because Conan O'Brien is American.

The comment here references the fact that poorly-coded apps return errors when name with apostrophes (e.g., O'Brien) are put into user input fields

SQL Injection – Auth Bypass

' or 1=1 --

We can send different input, which injects SQL commands into the username field, and allows us to bypass authentication on this app

SQL Injection – Auth Bypass

```
select username, password where  
username = '' or 1=1 -- - and  
password = ''
```

A typical SQL statement which logs a user into the app (with our injected code) may look like the example above

SQL Injection – Auth Bypass

```
select username, password where  
username = '' or 1=1 -- - and  
password = ''
```

Note that our code comments out the part of the statement related to the correct password

SQL Injection – Auth Bypass

```
select username, password where  
username = '' or 1=1 -- - and  
password = ''
```

We should understand that the goal of submitting a valid username and password to the app is to supply a match which creates a True statement

SQL Injection – Auth Bypass

```
select username, password where  
username = '' or 1=1 --- and  
password = ''
```

The `or` portion of our injection creates a True statement by giving `1=1`, which the app will interpret as True and will log us into the app