Sequel Fun

> Author: howard41436 | 楊皓丞 | B06902097

Problem Description

So I found this login page, but I forgot the credentials :(

source: source.php

Vulnerability

> SQL Injection

Solution

From the source we see that the sql query string is `"SELECT * FROM users WHERE user='" . $user . "' AND pass='" . $pass . "'"`, so it is vulnerable to sql injection. It filters the character `'1'` in username and password, so we could post something like `user=' OR 2=2--&pass`, then the sql query string after commenting will become `SELECT * FROM users WHERE user='' OR 2=2`, then we will log in as admin and get the flag because query results are sorted by uid and admin's uid is 0.