Challenge 11

http://192.168.2.11/sqli/gbk/ [Level: Advanced]

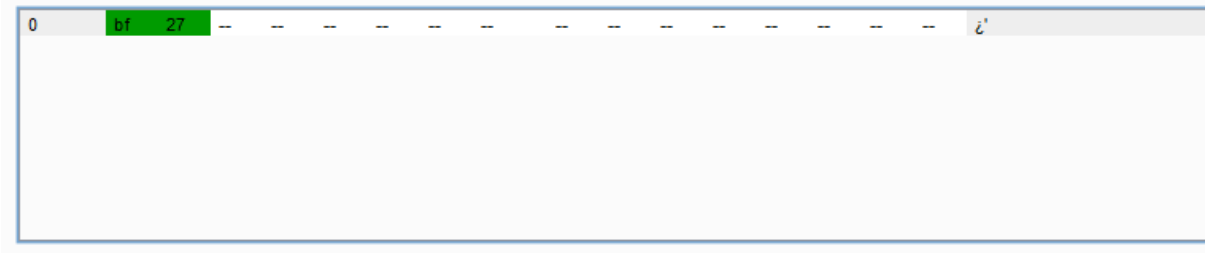
- Bypass Authentication and obtain the flag (5 marks)

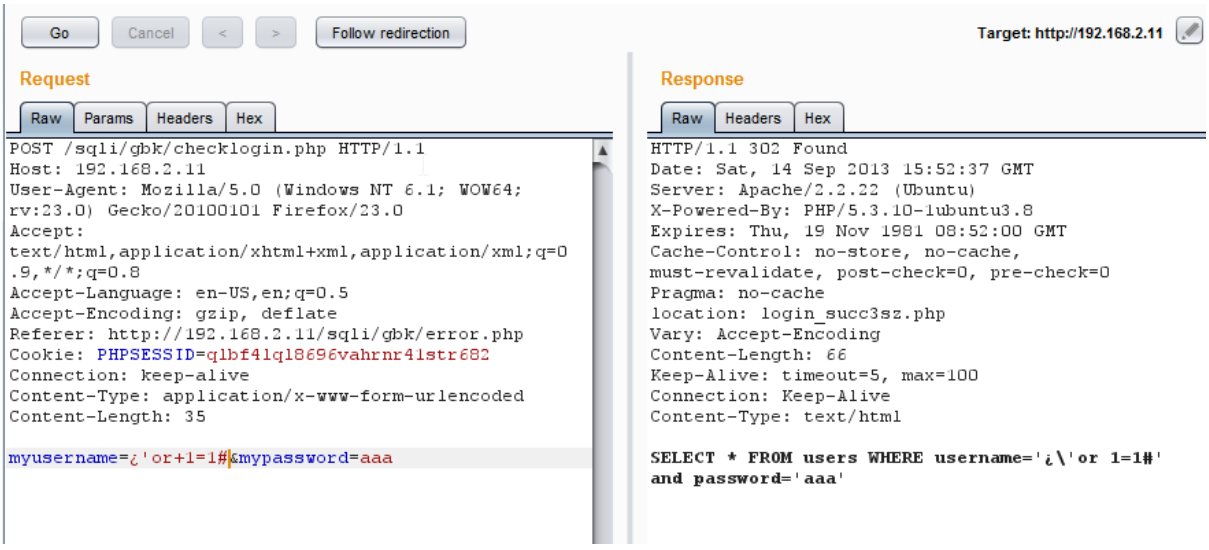
  The username and password fields both have mysql_real_escape_strings() function validating the input. But the database is configured to use GBK encoding.

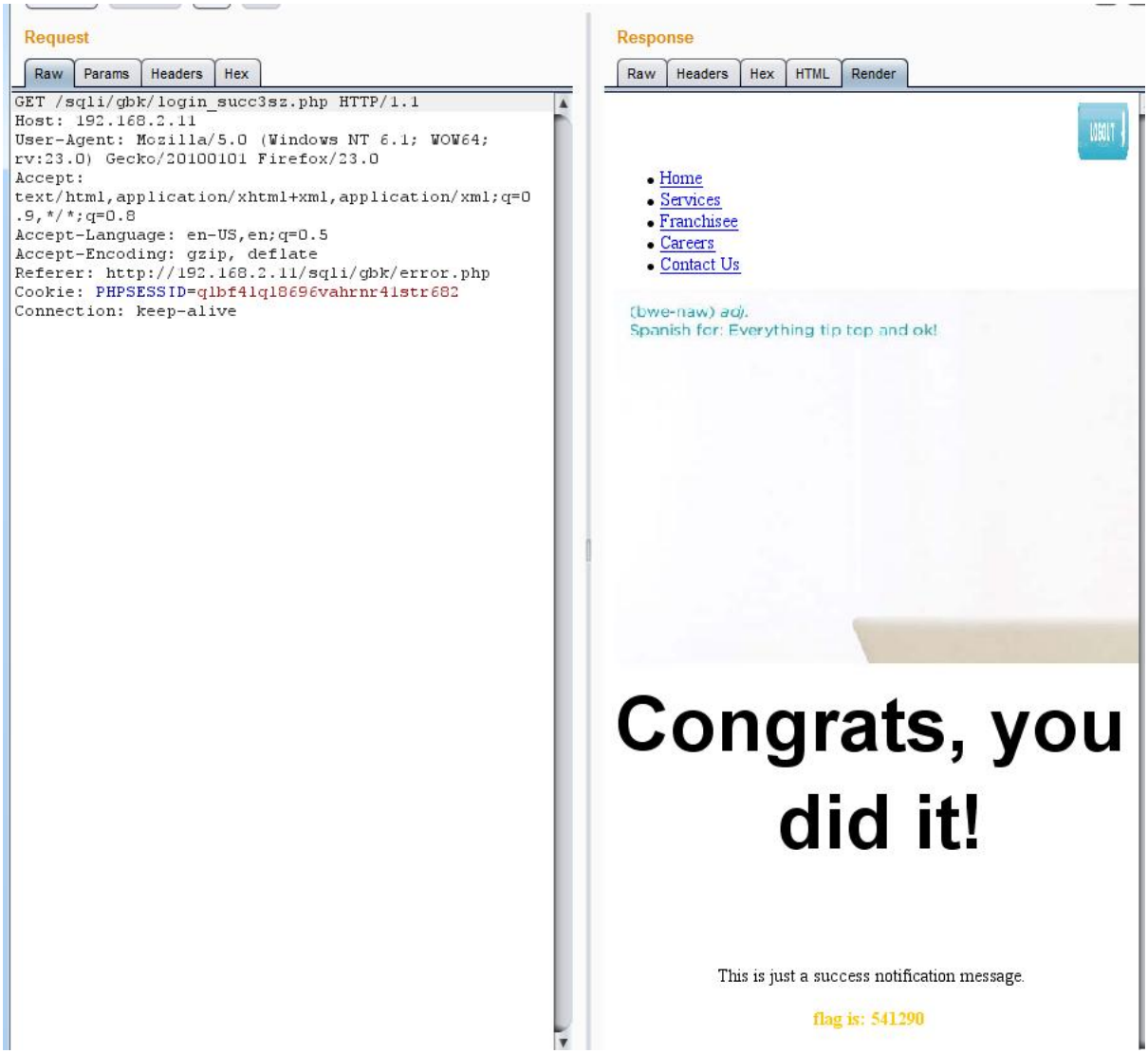
  Read about this issue here: http://shiflett.org/blog/2006/jan/addslashes-versus-mysql-real-escape-string

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

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







Further reading:

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