封神台MYSQL 注入 - Dns注入

原创

VIP文章 炎凰先生 于 2020-10-05 12:55:36 发布 983 收藏 4

分类专栏： Web安全微专业

本文链接：https://blog.csdn.net/qq_40941912/article/details/108927737

一、原理

DNSLOG的使用场景：

在某些无法直接利用漏洞获得回显的情况下，但是目标可以发起请求，这个时候就可以通过DNS请求把想获得的数据外带出来。

对于sql盲注，常见的方法就是二分法去一个个猜，但是这样的方法麻烦不说，还很容易因为数据请求频繁导致被ban。

所以可以将select到的数据发送给一个url，利用dns解析产生的记录日志来查看数据。

LOAD_FILE()读取文件的函数

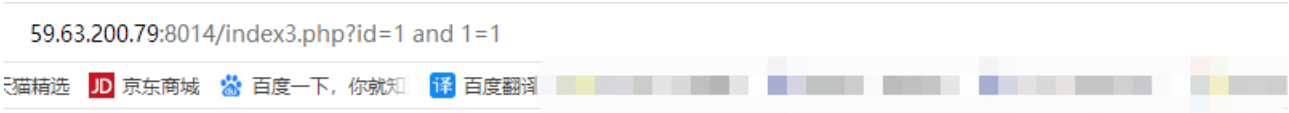
读取文件并返回文件内容为字符串。要使用此函数，文件必须位于服务器主机上，必须指定完整路径的文件，而且必须有FILE权限。 该文件所有字节可读，但文件内容必须小于max_allowed_packet（限制server接受的数据包大小函数，默认1MB）。 如果该文件不存在或无法读取，因为前面的条件之一不满足，函数返回 NULL。

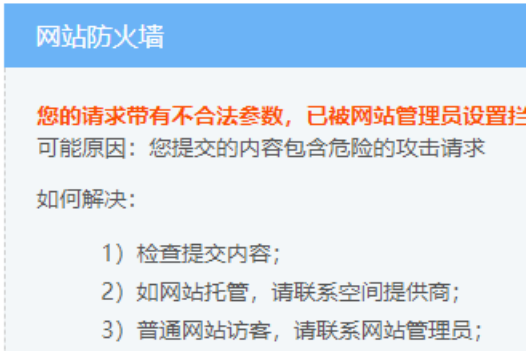
二、作业

MYSQL 注入 - Dns注入 （Rank: 20）

首先我们可以随便尝试下是否存在注入：?id=1 and 1=1

发现被拦截





要想办法绕过防火墙，试下输入：http://59.63.200.79:8014/index3.php/1.txt?id=1 and 1=2

如下