封神台SQL注入-header注入

原创

VIP文章 炎凰先生 于 2020-08-25 11:47:53 发布 479 收藏 2

分类专栏： Web安全微专业

本文链接：https://blog.csdn.net/qq_40941912/article/details/108218466

一、原理

数据路径出现符号是会爆错的

全局变量：

```
$_REQUEST （获取GET/POST/COOKIE） COOKIE在新版本已经无法获取了
$_POST （获取POST传参）
$_GET （获取GET的传参）
$_COOKIE （获取COOKIE的值）
$_SERVER （包含了诸如头信息(header)、路径(path)、以及脚本位置(script locations)等等信息的数组）
```

$_SERVER（）它包含着诸多的信息，有头信息（heander），路径（path），脚本位置（script locations）等信息的数组
这个变量特别强大：

```
$_SERVER['HTTP_HOST'] 请求头信息中的Host内容，获取当前域名。
$_SERVER["HTTP_USER_AGENT"] 获取用户相关信息，包括用户浏览器、操作系统等信息。
$_SERVER["REMOTE_ADDR"] 浏览网页的用户ip。
```

updatexml（）

这个函数有三个传参如下
update是更新的意思 xml是一种文档的类型
updatexml(目标xml内容，xml文档路径，更新的内容）
updatexml(1,concat(0x7e(select database())0x7e),1)
以上这条语句的意思为
更新xml文档（需要更新的文档,concat(0x是16进制7e转换后