# XCTF-CAT

转载

aaecoj8957 于 2019-07-17 10:46:00 发布 212 收藏 1
文章标签： python php 数据库
原文链接：http://www.cnblogs.com/Mikasa-Ackerman/p/11199513.html

果然还是我太菜了呜呜呜，这道题仍然是没有自己做出来。哎。

这一道用的并不是PHP的环境，而是用Python中的Django编写的。

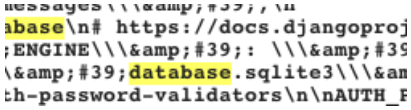
记得做过类似的一道题目。来源于MOCTF中的网站扫描器,当时做完后其实一回想，后台用的应该是file_get_contents类似的函数，还应该开启了远程包含之类的。然后我们才可以直接输入url返回页面的源码等等。

但是这个感觉就是一个命令执行，他返回的是ping的结果。并且这个是不接通外网的，然后尝试了一下dvwa里面的命令执行。还是没有成果,然后看了一下题解才知道这个是Django编写的东西。。

这里面是使用@来进行任意文件的读取(原理是啥我也不太清楚)。显示利用报错获得Django一些敏感信息，至于后面加上 %80以及以后的Url编码会造成报错可能是因为超过了ascii的范围(ascii是0-127)。%80是16进制正好是128

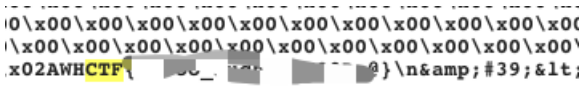
然后读取他的配置文件(/opt/api/api/settings.py),具体为什么是这里，可能是默认的保存路径

url=@/opt/api/api/settings.py可以得到数据库名



然后直接读取数据库文件

url=@/opt/api/database.sqlite3得到flag




总结：幸亏看了一下题解，不然硬肝的话估计也做不出来。

转载于:https://www.cnblogs.com/Mikasa-Ackerman/p/11199513.html