cat-adworld

非常没思路的一道题

首先国内就不会有网站多少用django，而且看了wp，有重要提示都没给，能一遍过太难了。

在比赛的时候有个提示，练习时候没有给，完全是想不到的，我看了半天又臭又长的html泄露还想了sql注入，完全是在浪费时间

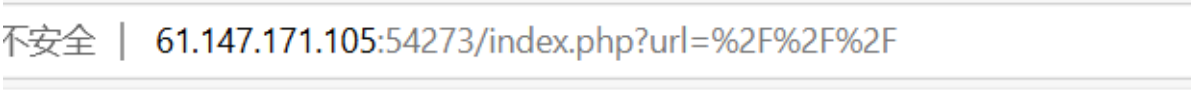
> RTFM of PHP CURL===>>read the fuck manul of PHP CURL???

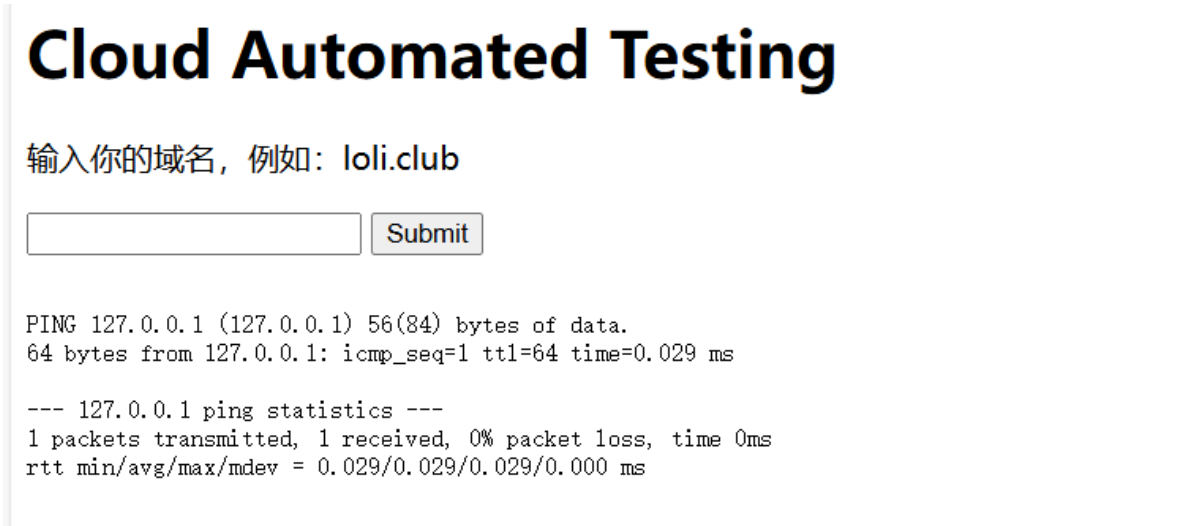
首先打开是一个url的页面，那么思路肯定就是先用ssrf

不过怎么使用file，gopher，http都显示错误，有的还没有显示

进行了WFUZZ的url爆破，也没有什么信息。

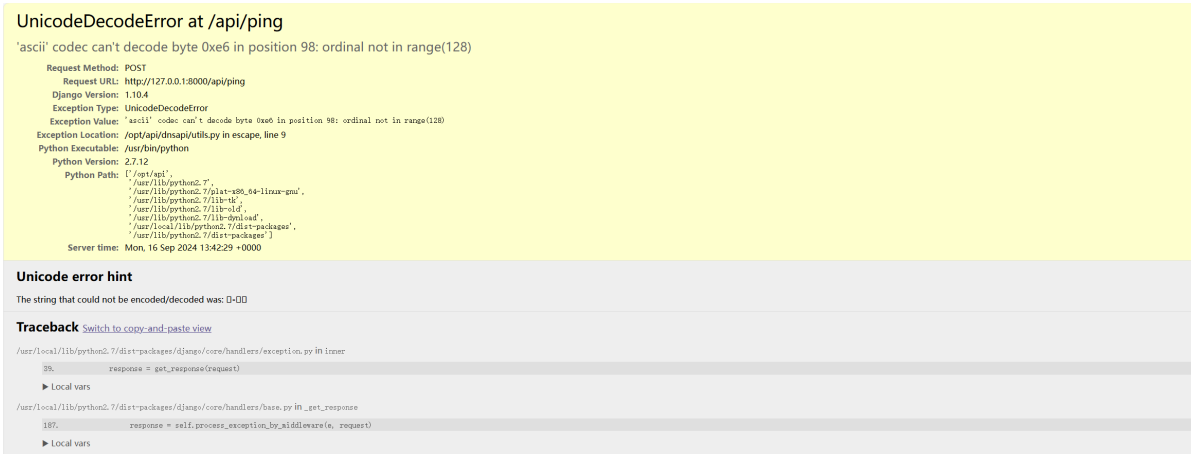
在输入1，或者127.0.0.1时候，有回显，明显是一个ping命令，并且看到页面直接有url编码





本题的漏洞如下，url是16进制的编码，ascii有效到128，那么超过128的url编码在django设置了gbk编码后，会导致解码错误出现文件报错泄露

尝试了%FF报错，显示了django的html页面



并且可以看到jdango的部署在可选文件，/opt/api下，对django还是比较熟悉

django默认配置数据库是sqllite，setting是总体框架配置

这里可以在setting找到数据库路径/opt/api/database.sqlite3

在有了提示的线索下，这里的漏洞是使用php的curl的@会导致对绝对路径的访问，以此访问数据库进行信息获取

如wp中所提示：

- 当 `CURLOPT_SAFE_UPLOAD` 为 true 时，如果在请求前面加上@的话phpcurl组件是会把后面的当作绝对路径请求，来读取文件。当且仅当文件中存在中文字符的时候，Django 才会报错导致获取文件内容。

可以通过路径访问信息泄露直接找到flag库flag表

\x17\x15\x15\x01Utable**flag**flag\x04CREATE TABLE "**flag**" (\n\t"**flag**" TEXT\n)P\x02\x06\x17++\x01Ytablesqlit

\x03\x06\x17\x15\x15\x01Utable**flag**flag\x04CREATE TABLE "**flag**" (\n\t"**flag**" TEXT\n)P\x02\x06\x17++\x01Yta

后面带了flag