中间件特性绕过 waf

首先通过-1 /1 /0 运算判断出存在数字型 sql 注入

一般来说 asp 都是用 access，这里使用--%0a 的方式来构造 payload 也能正常执行,判断出这里为 mssql
这里的测试 payload 是 --随机字符%0a AND--随机字符%0a1=1

在 asp+iis 的环境下 unicode 在 iis 解析之后会被转换成 multibyte，但是转换的过程中可能出现： 多个 widechar 会有可能转换为同一个字符。 打个比方就是譬如 select 中的 e 对应的 unicode 为%u0065，但是%u00f0 同样会被转换成为 e。

```
1.  o -->%u004f --> %u006f -->%u00ba
2.  e -->%u0045 --> %u0065-->%u00f0
```

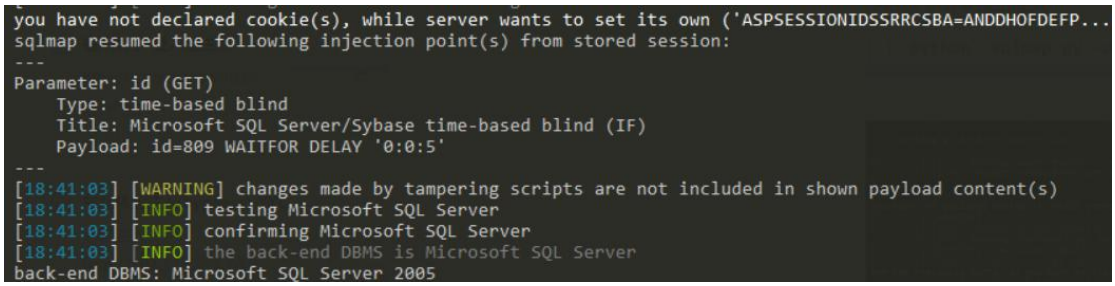
首先测试延时 payload,将里面的 o 替换为%u00ba

```
1.  WAITF%u00baR%20DELAY%20%270:0:0%27
```

返回时间正常

改为 1 页面返回 3 秒,执行了 3 次,不管输入多少都会被乘 3

写个 tamper 即可使用 sqlmap 跑



https://github.com/Junehck/SQL-injection-bypass