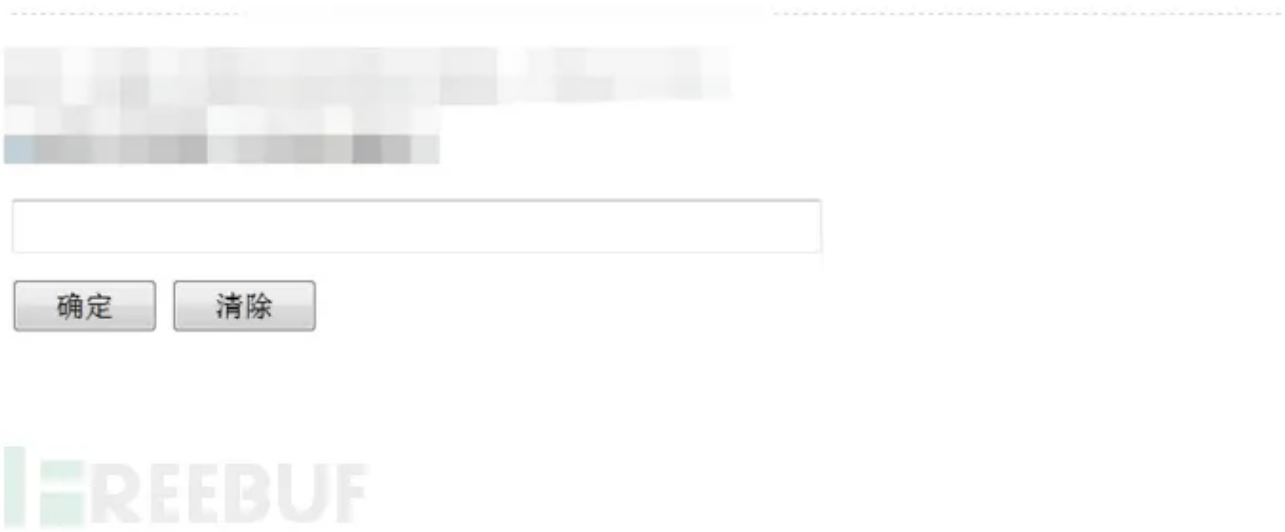
一次SQL注入到代码审计之路

lesssafe FreeBuf 3天前

一、找网站SQL注入点

在测试时后发现有一个信息查询框，就是下面这个图片显示的。一般信息查询框会和数据库存在交互。



我输入数字1，会正常提示木查询到相关信息。

那我们使用1’测试一下，发现不弹未查询到相关信息的提示框，也没有任何数据输出，大致判断这个点存在sql注入，并且不对输出报错信息。

大概猜测出SQL语句为 ：

```
select * from A where id ='$_POST['id']';
```

没有对用户输入的数据做任何过滤。

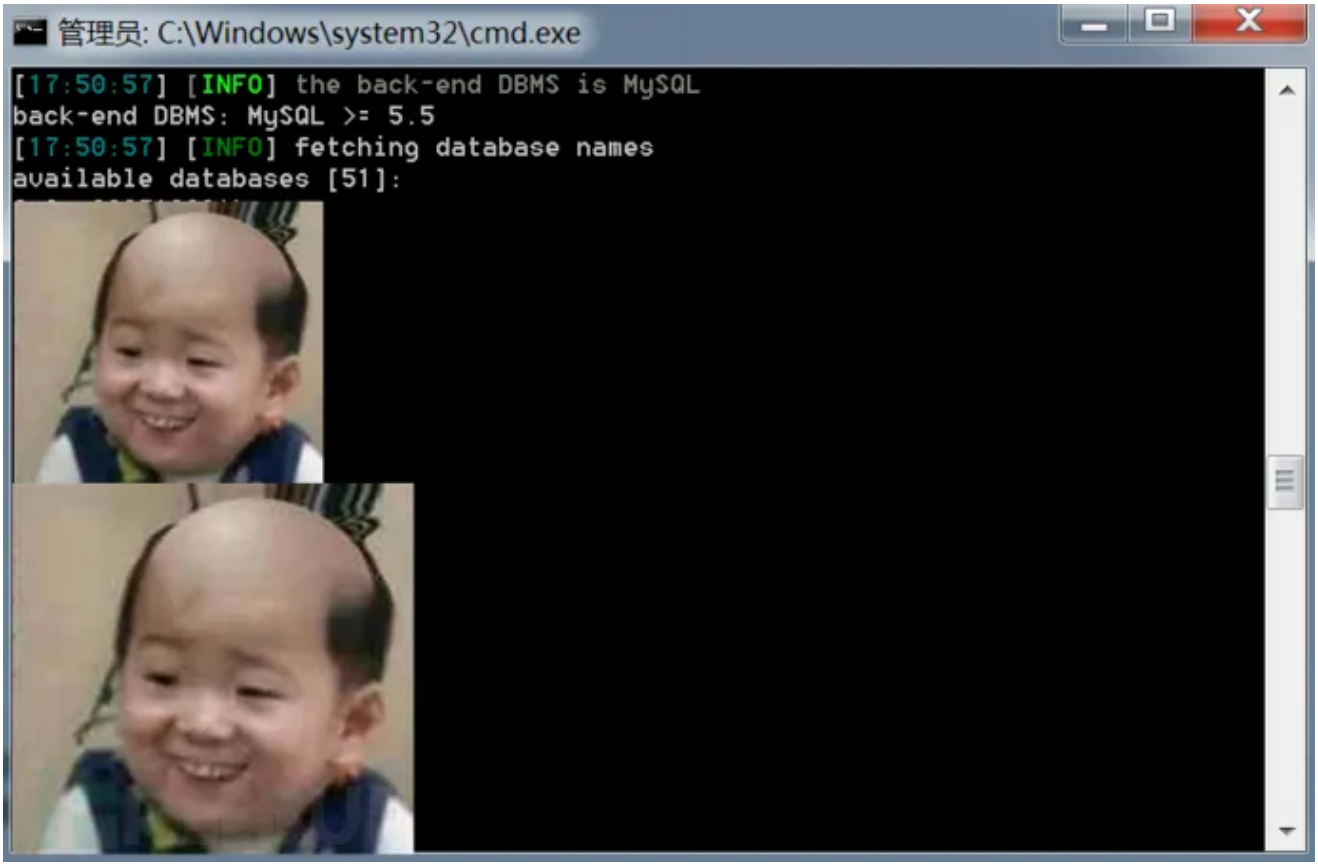
构造一个闭合语句再次确认一些是否确认存在sql注入。

```
payload：1’ #
```

通过上面简单测试，已经确定了，肯定存在sql注入。

二、sqlmap跑一下

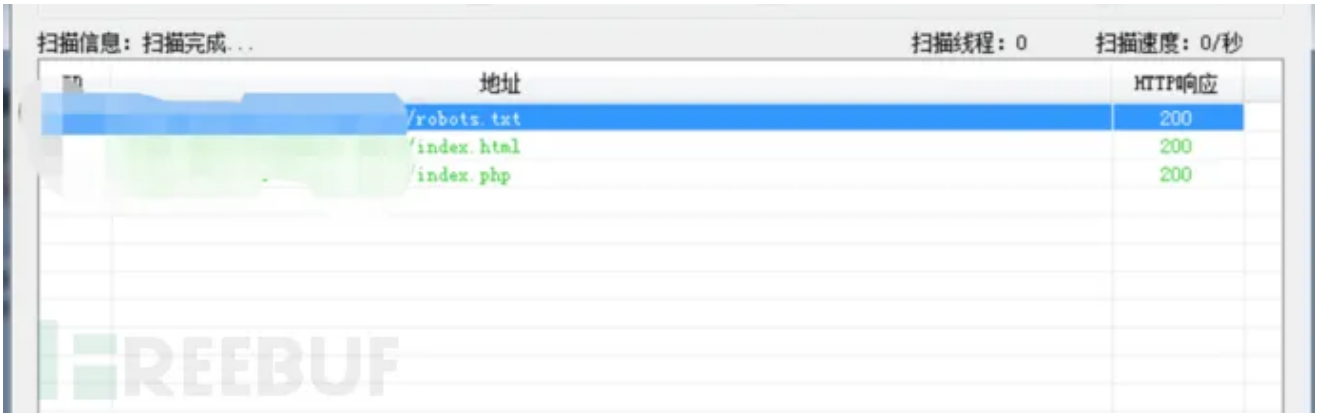
将数据包保存到一个文件，直接用sqlmap跑。非常震惊，居然有51个库。



经过查询，查到后台的账号密码，那我就开始找后台的艰辛路程了。

三、找后台

没有找到后台，但是发现robots文件。



从robots上看到是PHPCMS系统

```
#
# robots.txt for PHPCMS v9
#
User-agent: *
Disallow: /caches
Disallow: /phpcms
Disallow: /install
Disallow: /phpsso_server
Disallow: /api
Disallow: /admin.php
```


使用PHPCMS系统通用后台地址admin.php，m=admin&c=index&a=login，都不行，测了好就发admin模型下的index控制器是存在，当我们访问的时候就会自动跳到首页，这也该是开发者后来做了修改，专门做防黑的。

四、找通用漏洞

这个步骤就不多说了，我测了已暴光的漏洞，都是不行，说明开发者还是有安全意识的，把漏洞都给修复了。

五、返回sqlmap

还有一种思路就是使用sqlmap —os-shell直接获取shell，但是这个基本上不行的，因为网站的文件基本上都是755权限，没有写的权限就会失败。那我还是抱着一丝丝希望去测试了。

使用sqlmap —os-shell需要知道网站的绝对路径，网站绝对路径可以通过中间件配置文件查看。

首先需要知道网站用了什么中间件，我没有用nmap跑，只用404看到是nginx ，nginx的配置文件 /usr/local/nginx/conf/ngixn.conf

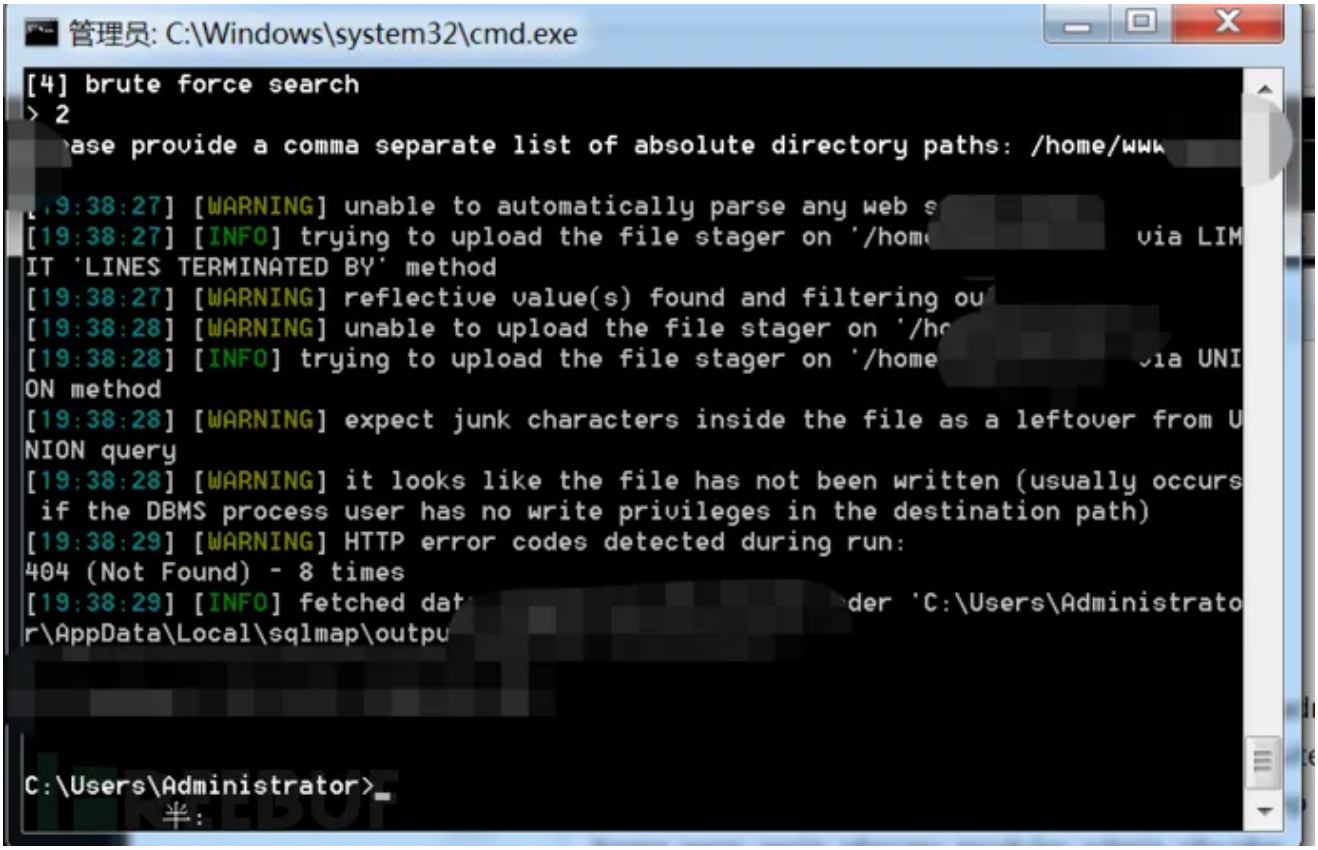
用sqlmap —file-read 去读nginx配置文件。通过配置文件只看到一条默认的配置信息。

```
_usr_local_nginx_conf_nginx.conf
server
    {
        listen 80 default_server;
        #listen [::]:80 default_server ipv6only=on;
        server_name www.lnmp.org;
        index index.html index.htm index.php;
        root  /home/wwwroot/default;

        #error_page   404   /404.html;
        include enable-php.conf;

        location /nginx_status
        {
            stub_status on;
            access_log   off;
        }

        location ~ .*\.(gif|jpg|jpeg|png|bmp|swf)$
        {
            expires      30d;
        }

        location ~ .*\.(js|css)?$
        {
            expires      12h;
        }
```

需要注意的是如果在nginx.conf文件没有看到有价值的信息，有一种可能是存在，/usr/local/nginx/conf/vhost/网站域名.conf 这个位置，果不其然就是它。

```
server
    {
        listen 80;
        #listen [::1:80;
        server_name
        index index.html index.htm index.php default.html default.htm default.php;
        root  /home/www

        #error_page   404   /404.html;
        include enable-php.conf;

        location ~ .*\.(gif|jpg|jpeg|png|bmp|swf)$
        {
            expires      30d;
        }

        location ~ .*\.(js|css)?$
        {
            expires      12h;
        }

        location ~ /\.
        {
            deny all;
        }

        access_log  /home/wwwlog
    }
```

找到了真实的路径，就可以使用 sqlmap —os-shell了，但是正式我当时预料的没有写入权限导致拿shell失败。



六、使用sqlmap读取网站源码

通过上面的思路我们已经知道网站的真实路径，知道了是PHPCMS系统，那我们可以读取网站的文件了。

1、读取路由文件 caches\configs\route.php 查看路由文件没有问题。

2、查看系统文件 caches\configs\system.php （这个文件能看是否开启了域名访问后台）

```
'html_root' => '/html',//生成静态文件路径
'safe_card'=>'1',//是否启用口令卡

'connect_enable' => '1',     //是否开启外部通行证
'sina_akey' => '',  //sina AKEY
'sina_skey' => '',  //sina SKEY

'snda_akey' => '',  //盛大通行证 akey
'snda_skey' => '',  //盛大通行证 skey

'qq_akey' => '',    //qq skey
'qq_skey' => '',    //qq skey

'qq_appkey' => '',  //QQ号码登录 appkey
'qq_appid' => '',   //QQ号码登录 appid
'qq_callback' => '',    //QQ号码登录 callback

'admin_url' => '',  //允许访问后台的域名
);
?>
```

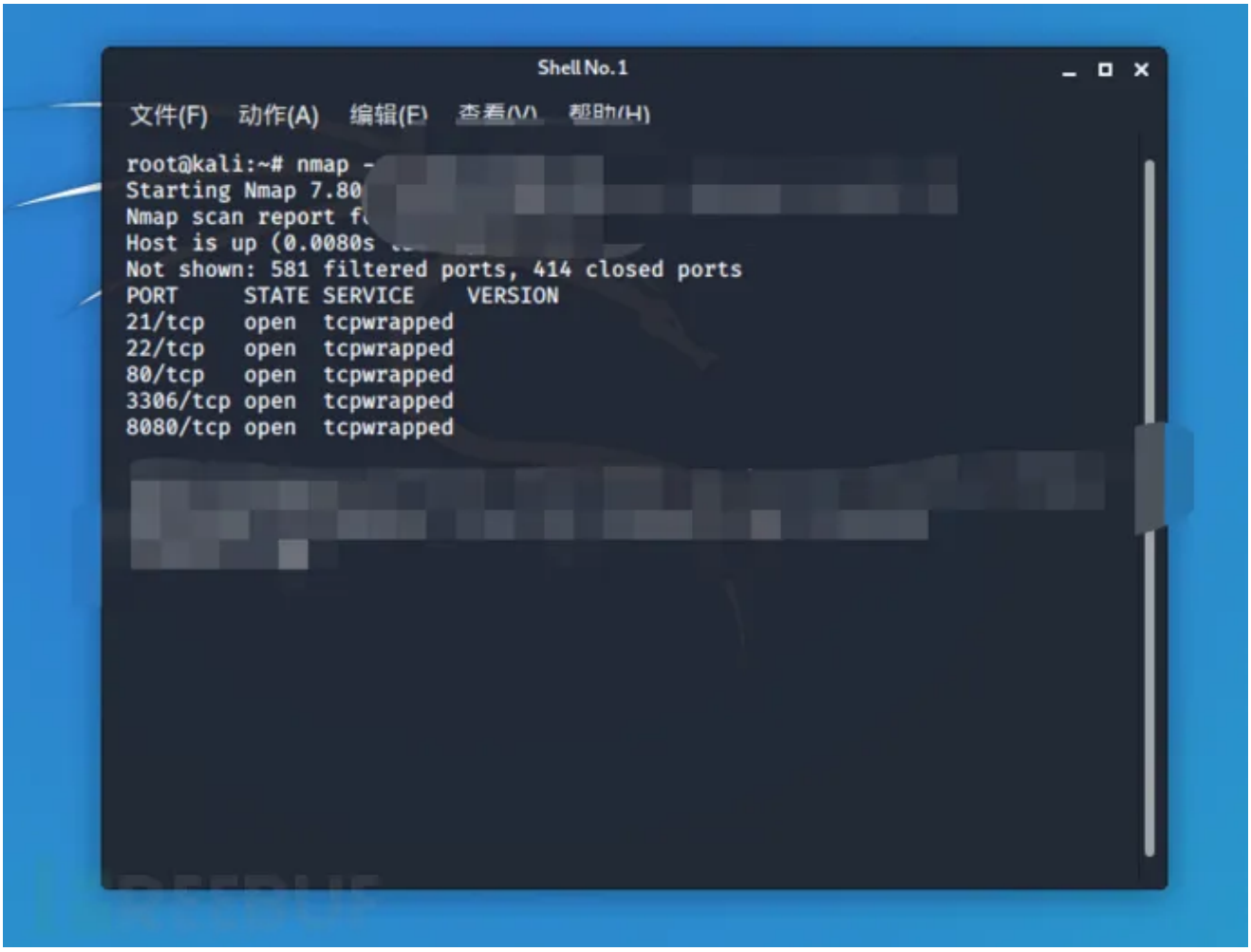
3、在上面我们说到admin模型下index控制器是能访问，知识在访问的时候会跳转到主页，那我们下载index控制器文件看下。phpcms\modules\admin\index.php ，查看index控制器下的login方法是没有做任何修改的。

```
public function init () {
    $userid = $_SESSION['userid'];
    $admin_username = param::get_cookie('admin_username');
    $roles = getcache('role','commons');
    $rolename = $roles[$_SESSION['roleid']];
    $site = pc_base::load_app_class('sites');
    $sitelist = $site->get_list($_SESSION['roleid']);
    $currentsite = $this->get_siteinfo(param::get_cookie('siteid'));
    /*¹ÜÀíÔ±ÊÔ¹ØÀ*/
    $adminpanel = $this->panel_db->select(array('userid'=>$userid), "*",20 , 'datetime');
    $site_model = param::get_cookie('site_model');
    include $this->admin_tpl('index');
}

public function login() {
    if(isset($_GET['dosubmit'])) {

        //²»Ê¹ÓÃ¿ÕÃëÂë
        if (!isset($_GET['card'])) {
            $username = isset($_POST['username']) ? trim($_POST['username']) : showmessage(L('nameerror'),HTTP_REFERER);
            $code = isset($_POST['code']) && trim($_POST['code']) ? trim($_POST['code']) : showmessage(L('input_code'),
                HTTP_REFERER);
            if ($_SESSION['code'] != strtolower($code)) {
                $_SESSION['code'] = '';
                showmessage(L('code_error'), HTTP_REFERER);
            }
            $_SESSION['code'] = '';
        } else { //¿ÚÁî¿ÕÃëÂë
```

七、侧面渗透测试

上面说了一共有51个网站，我随机看了几个，数据库的结构是一样的，说明是同一个建站系统。

那我们用nmap扫一下服务发现有8080服务，这个网站8080端口的网站时dedecms系统搭建的，我正好有后台密码，这样能通过dedecms上传文件。



八、代码审计

通过上面们大概判断是admin模块index控制器有问题。

查看admin模块多了一个MY_index.php控制器，

查看MY_index.php 发现里面有一个构造函数，这个函数大概意思就是会打开这个方法会

判断你的right_enter的session值是否为空，若果为空，那么就回到首页，这这是我们刚开始一直打不开后台的原因。

```php
<?php defined('IN_PHPCMS') or exit('No permission resources.');
class MY_index extends index {
public function __construct() {
if (empty($_SESSION['right_enter'])) {
header('location:./');
exit;
}
parent :: __construct();
}
public function public_logout() {
$_SESSION['right_enter'] = 0;
parent :: public_logout();
}
}
```

经过看phpcms开发手册（我对这看系统二次开发不太熟悉，我只知道是一个MVC结构的php程序），如果需要对控制器进行二次开发需要在同级目录创建一个MY_*.php文件，大概意思就是创建这个文件后程序在运行index模块时会运行MY_index.php里面的代码。

二次开发 —— 控制器扩展技巧

如果要对已存在的控制器进行二次开发，为了方便升级不建议直接对内核文件直接修改该，您可以通过"MY_*.php"的形式进行二次开发。

例如您要对改phpcms/mood/index.php进行二次开发。您可以在与index.php同级的目录下建立"MY_index.php"

MY_index.php代码如下:

```php
class MY_index extends index{
    function __construct() {
        parent::__construct();
        }
        //……your code
}
```

到这了明白了，因为没有$_SESSION[‘right_enter’]值，所以导致登陆不了，所以打开后台首先需要给$_SESSION[‘right_enter’]赋值。经过不懈努力找到了一个正确文件。

```php
<?php define('PHPCMS_PATH', realpath(dirname(__FILE__) . '/..') . '/');
include PHPCMS_PATH . '/phpcms/base.php'; // pc_base::creat_app();
$session_storage = 'session_' . pc_base :: load_config('system', 'session_storage');
pc_base :: load_sys_class($session_storage);
session_start();
$_SESSION['right_enter'] = 1;
unset($session_storage);
header('location:../index.php?m=admin');
```

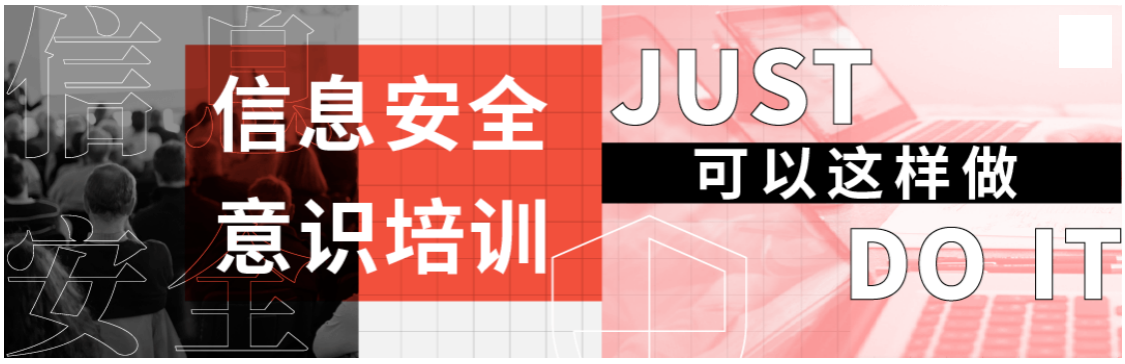
这个文件大概意思就是当我运行改文件时会将$_SESSION[‘right_enter’]=1，然后跳转到登陆界面。

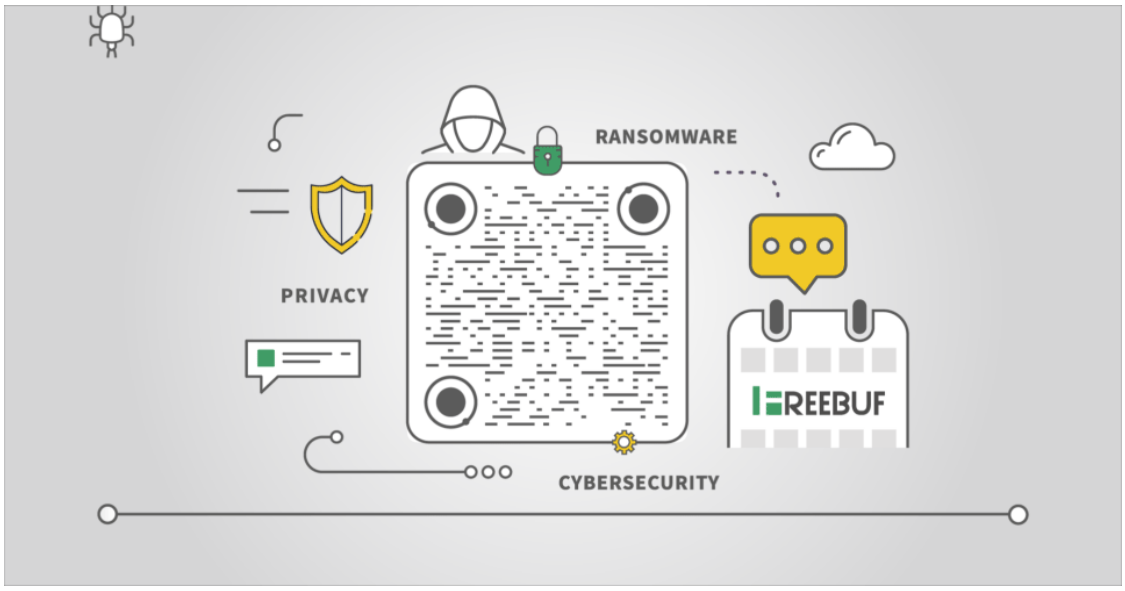
*本文作者：lesssafe，转载请注明来自FreeBuf.COM

精彩推荐


爱奇艺的业务安全风控“秘籍”
卢明樊
安全团队负责人
爱奇艺云服务高级总监


SECURITY OR NOT?
网络安全人员真的
“安全”吗？
娄鹤
北京德和衡律师事务所
高级联席合伙人/律师


信息安全
意识培训
JUST
可以这样做
DO IT


RANSOMWARE
PRIVACY
FREEBUF
CYBERSECURITY

阅读原文