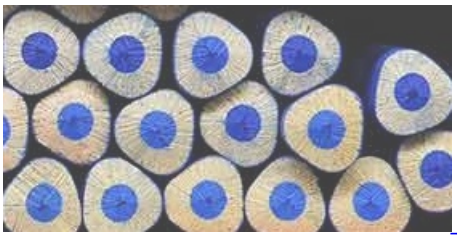
CTF web学习笔记

原创

hiddenCarry 于 2020-06-30 11:29:43 发布 884 收藏 22

分类专栏： CTF

本文链接：https://blog.csdn.net/daqiangdetianxia/article/details/107021825



CTF 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

i春秋视频学习记录

> web狗生存之道 讲师:y4ngshu

日常渗透测试（笔记）

1.信息收集

2.登陆后台----->getshell

3.Getshell失败----->转换思路------>挖掘其它漏洞(sql注入等)------>列库收集用户信息

4.拿到用户密码------>撞邮箱-------->邮箱拿到关键信息---------->拿到vpn

5.通过vpn去访问文件服务器------->写脚本getshell

CTF学习

1.xss打后台----->403---------->ajax抓取页面回转出来--------->sql注入—>getting

2.Bypass Waf来注入 (%00,||,seselectlect 等等)，国内web常见题型

3.代码审计 花式杂耍php的各种特性（反序列化、弱类型）

4.文件上传 花式Bypass上传（.php111 .inc .phpt）

5.各种当前热点漏洞
扫描路径----> phpinfo() ------> php7 -------php7 opcache ---->查看文档 -----> 花式绕坑 ------> Getshell

6.社会工程学（常用密码）

7.各种Web漏洞夹杂

8.具有内网环境真实渗透场景

记大佬的渗透测试记录

```
1.对目标进行信息采集
2.主站拿不下来，决定拿二级域名
3.排查二级域名
4.根据二级域名的名字选择upload edit等等具有操作功能的站点入手
5.存在svn漏洞的话，尝试通过wc、db的形式，利用sqlite将源码还原出来
6.审计源代码，快速定位代码，全文搜索exec、upload，include等等这些危险操作
7.到一个exec命令执行，发现管理员权限
8.回溯代码，定位管理员登录功能，审计出cookie算法可以破解
9.伪造cookie反弹shell，上去后发现很多站点在上面，权限不够
10.查看版本
11.利用之前ctf中的一个一句话提权成功，然后大杀四方。
```

```
1.常规的进行信息搜集踩点工作
2.猜解用户名密码（组合了网站的域名和电话号）
3.登录后台，测试文件上传功能，上传文件中只要含有<?php>就进行上传
4.脑洞一开，<script language =  "php'> 成功getshell
```

web狗如何在CTF-web中的套路中实现反套路

> 讲师：三十、伪赛棍

题目类型

```
1.SQL注入
2.XSS
3.代码审计
4.文件上传
5.php特性
6.后台登陆类
7.加密解密
8.其他脑洞、猜谜、和其它结合
```

SQL注入

1.简单注入
 ‘、and 1=1、or 1=1、xor 1=1
2.宽字节注入
 GBK字符集编码，过滤绕过
3.花式绕mysql
 intervalue(),数字注入
4.绕关键词检测拦截
 重复性(selselectect)
5.MongoDB注入
 nosql注入（nosqlmap）
6.http头部注入
 x-for-ward注入、IP地址注入、refer注入
7.二次注入
 插入注入，另一个页面注入

SQL注入工具

1.burpsuit
2.Hackbar
3.Sqlmap
4.Nosqlmap

SQL解题思路

简单：用sqlmap跑
判断注入点，是否是Http头注入？是否在图片出注入？等
判断注入类型
利用报错信息注入
尝试各种绕过过滤方法
查找是否是通过的某模块存在的注入漏洞
延时注入（对待盲注）

SQL注入技巧

sql-mod="STRICT_TRANS_TABLES"(默认未开启)
 插入数据截断，插入“admin X”绕过或越权访问

注意二次注入
 isg2015 web350 username从session中直接带入查询，利用数据库字段长度
 截断，\被gpc后为\\,但是被截断了只剩下一个\，引发注入。

如果猜解不出数据库的字段，搜索后台，查看源代码，源代码登录时的表单中的字段一班和1数据库的字段名相同

绕过安全狗
 se%lect
 针对asp+access，首先来挖掘一下数据库的特性。
 1.代替空格：%09、%0A、%0C、#0D
 2.可以截断后面语句注释符：%00,%16,%22,%27
 3.当%09、%0A、%0A、%0C、%0D超过一定长度后，安全狗防御失效。
 4.UserAgent:BaiduSpider

magic_quotes_gpc=On的情况下，提交的参数中如果带有引号’，就会被自动转义为\',使很多注入攻击无效

XSS

```
简单：存储型XSS盲打管理员后台
各种浏览器auditor绕过
富文本过滤黑白名单绕过
CSP绕过
Flash xss
AngularJS客户端模板XSS
.....
```

XSS注入工具

```
Burpsuit
HackBar
Xss平台
swf decomplier
flasm
doswf(swf加密)
Crypt Flow (swf加密)
......
```

XSS解题思路

```
简单XSS，直接利用XSS平台盲打管理员cookie
过滤标签，尝试各种绕过方法
存在安全策略csp等，尝试相应的绕过方法
逆向.swf文件，审计源码，构造XSS payload
......
```

文件上传

类型：

- 00截断上传
- multipart/form-data大写绕过
- 花式文件后缀（.php345 .inc .phtml .phps）
- 各种文件内容检测
- 各种解析漏洞
  ngix-fastcgi
- 花式打狗棒法
- 在线编辑器漏洞等
  fckeditor
- fckeditor 2.0<2.2 允许上传asa,cer,php2,php4,inc.pwml,pht后缀的文件上传后它保存的文件直接使用$sFilePath = $sServerDir ,$Filename,而没有使用$sExtension为后缀，直接导致在win下上传文件后面加个 . 来突破
- 文件包含

文件上传工具

- hackbar
- Burpsuit
- Webshell
- 中国菜刀
- AantSword

文件上传解题思路

- 简单文件上传，查看响应
- 是否只是前端过滤后缀名，文件格式，抓包绕过
- 是否存在截断上传漏洞
- 是否对文件头检测（图片马等）
- 是否对内容进行检测，尝试绕过方法
- 是否上传马被查杀，免杀
- 是否存在各种解析漏洞
- http头以两个CRLF（相当于\r\n\r\n）作为结尾，\r\n没有被过滤时，可以利用\r\n作为url参数截断http头，后面跟上注入代码
- …
  练习题：HTCTF-2016 题目14

php特性

- 弱类型
- intval
- strpos和==
- 反序列化+destruct
- \0截断
- iconv截断 （%00截断）
- parse_str函数
- 伪协议(io流操作)

PHP特性-工具

- hackbar
- burpsuit
- 在线调试环境

php特性-解题思路

- 判断是否存在php种截断特性
- 查看源码，判断是否存在php弱类型问题
- 查看源码，注意一些特殊函数
  eval()，system()，intval()
- 构造变量，获取flag
- 是否存在Http （请求参数污染,加两个参数的不同情况。）
- 魔法哈希(magic hash)
  mad5(‘240610708’) = md5(‘QBKCDZO’) = 0e830400451993494058024219903391
- …

php特性-伪协议

php://filter --对本地磁盘文件进行读写
http://localhost/test/index.php?file=php://filter/read=convert.base64-encode/resource=index.php

php://input 伪协议 php://input 需要服务器支持，同时要求 “allow_url_include ”属性设置为 on

```
<?php
 @eval(file_get_contents('php://input'))
?>
post<?php system('ifconfig');?>
```

php://memory 总是吧数据存储在内存中

php://temp会在内存量达到预定义的限制后（默认2M）存入临时文件

…

1.DATA伪协议，分号和逗号有争议

- data:文本数据
- data:text/plain，文本数据
- data:text/html，HTML代码
- data:text/css；base64，css代码
- data:text/javascript;base64,javascript 代码
- 编码的icon图片数据
- 编码的gif图片
- 编码的png图片
- 编码的jpeg图片

glob://查找匹配文件路径模式

后台登录类

- 万能密码绕过
- 变形万能密码绕过
- 社工的方式得到后台密码
- 爆破方式得到后台密码
- 各种cms后台登陆绕过

后台登录类-工具

- burpsuit
- hackbar
- sqlmap
- 社工库
- …

后台登录类解题思路

- 根据提示，判断是否是普通的登录绕过，或是利用社工的方式
- 普通登录绕过尝试各种万能密码绕过，或通过sql注入漏洞得到账号密码，或xss盲打
- 若果是cms系统登陆，查找是否有相应版本的后台绕过漏洞
- 社工方式（谷歌、百度、社工库）
- 爆破获取
- …

加密解密类-考察知识点

- 简单编码（多次basecode编码）
- 密码题（hash长度扩展、异或、移位加密、各种变形）
- js加解密
- 根据加密源码写解密源码
- …

加解密类-工具

- 各种编码转换工具
- Burpsuit
- 浏览器控制台
- …

加解密类-解题思路

- 判断是编码还是加密
- 如果是编码，判断编码类型，尝试解码或者多次编码
- 如果是加密，判断是现有的加密算法，还是字写得加密算法
- 是否是对称加密，是否存在密钥泄露等，获取密钥解密
- 根据加密算法，推断出解密算法
- …

其它类型

社工、花式查社工库、微博、QQ签名、whois、谷歌

例题：ISG CTF 2014 Web4 火眼金睛

google查找googole天涯社会工库，即可查找。
http://www.findmima.com

SSRF，包括花式探测端口，302跳转、花式协议利用、gopher直接取shell等等

例题：XDCTF2015 Web1 300

本题为SSRF，进去是一个框框。利用SSRF漏洞，直接尝试file://index.php,然后就吧index.php的源码读到，之后进行代码审计。

协议，花式IP伪造 X-Forwarded-For/X-Client-IP/X-Real/CDN-Src-IP、花式藏FLAG、花式分析数据包

例题：HCTF2014jianshu (400pt)
解题思路：

- Html编码payload用burp改包提交获得一个ip和审核链接。
  xss获取远程IP地址 ：218.75.123.186
  后台访问页面：
  http://121.41.37.11:2504/get.php?user=V1ew
  X-Forwarded-For 伪造登录上去没有flag。
  看到提示转换思路，后面为sql注入，得到管理员密码
  http://121.41.37.11:25045/get.php?user=A1rB4s1C
  加上 X-Forwarded-For ：218.75.123.186伪造ip登陆上去。

XXE 各种XML存在地方(rss/word/流媒体)、各种XXE利用方法（文件读取）
例题：AliCTF-Quals-2014 Web-300

推荐经**典例题**：http://lab10.wargame.whitehat.vn/web007