

Web-ctf-StudyNote

原创

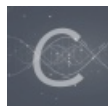
[ChengKaoAO](#) 于 2017-10-19 10:28:02 发布 425 收藏 2

分类专栏: [CTF](#) [安全](#) [CTF](#) 文章标签: [Web ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/ZmeiXuan/article/details/78281353>

版权



[CTF](#) 同时被 3 个专栏收录

5 篇文章 0 订阅

订阅专栏



[安全](#)

55 篇文章 0 订阅

订阅专栏

[CTF](#)

11 篇文章 0 订阅

订阅专栏

0x01背景说明

笔记章节:

- 0x01:可以练习的地方
- 0x02: 常规渗透测试手法
- 0x03:一些有趣的think/思路
- 0x04: 解读一个Writeup

0x02:可以练习的地方

English ▾ **News Links Sites Forum Ranking Challenges Downloads Register**



We Chall

New Sites

Hack The Box
hackburger
pwnable.tw
NOE.systems

Hacker Gateway
Solve Me
RingZer0 Team Online CTF
Challengeland

New Users

bezk0st
Moreal
hdhdbok
Carry123

Jerry233
andresbe
daguoguo
Itachi


49 Online

baseBurn, BloodCat, EmberCelica, govlog, j
jusb3, maf-ia, mavrc, RaonSecurity(x2), rpgl
teetrinker

All(142), Audio(4), Coding(12), Cracking(9), Crypto(22), Encoding(11), Exploit(51), Forensics(1), Fun(8), HTTP(10), Image(8), Java(3), Linux(9), Logic(5), Math(5), MySQL(15), PHP(27), Python(1), Realistic(6), Regex(2), Research(7), Shell(2), Simulated(1), Special(5), Stegano(21), Storyline(4), Training(31), Unknown(2), Warchall(11), Windows(1), XSS(2)

Challenges										
Score	Title	Author	Solvers	Age	Votes	Difficulty	Education	Fun	Forums	
1	Prime Factory by ch0wch0w		4228	9y 197d	384	1.88	2.75	3.50	?	
1	Training: Get Sourced by Gizmore		9496	9y 197d	840	0.42	1.62	2.07	?	
1	Training: Stegano I by Gizmore		6223	9y 96d	435	0.98	2.53	2.52	?	
1	Training: Crypto - Caesar I by Gizmore		5905	6y 327d	453	1.24	2.46	2.69	?	
1	Training: WWW-Robots by Gizmore		5381	6y 298d	414	1.02	3.43	3.25	?	
1	Training: ASCII by Gizmore		6347	6y 210d	477	0.54	1.77	1.60	?	

Wargame.kr v2.1



{not logged on}

Login Join

- Main
- Tutorial
- Wargame
- Achievement
- Free Board

Challenge list

show all solved not solved name point author

already got 200p bughela	QR CODE PUZZLE 300p bughela	file button 450p bughela	login filtering 450p bughela
WTF_CODE 450p bughela	DB is really GOOD 500p bughela	fly me to the moon 500p bughela	md5_compare 500p bughela
md5 password 500p bughela	EASY_CrackMe 500p bughela	strcmp 550p bughela	type confusion 550p bughela

0x03: 常规渗透测试手法

0x01: 渗透准备阶段

✓ 信息收集{子域名、端口、waf、whois...}

端口扫描: nmap, nmap 提权

0x02: 渗透阶段

① Web脚本攻击{Poc/Exp, Sqli, Xss, Csrft...}

② 网络设备攻击{路由器...}

③ 社会工程学

0x03: 后渗透阶段

- ①内网渗透扩大战果
- ②提升权限
- ③后门{rootkit, 木马...}

🔪攻击阶段

✓**SQL inject** (用户可控参数代入SQL文件并执行, 从而造成SQL注入)

几种常见的注入类型:

- 报错注入
- 盲注
- 基于时间的注入

♀[宽字节注入、二次注入]

工具: <https://github.com/sqlmapproject/sqlmap>

允许自己写python脚本, 可用编解码实现Web绕过。

✓**Xss**(在页面中嵌入恶意JavaScript代码, 用户浏览执行)

🎵**Exmample**添加管理员账号

```
$.ajax(|
  type:*post*
  url: * *
  data:"name=test pass$isAdmin=1," |)
```

在ctf中, XSS和CSRF, SQL, 经常一起考查。

🔪Web老司机

♀Ph老师: <https://www.leavesongs.com>

🎵大柠檬: <http://www.cnblogs.com/iamstudy>

♀V师傅: <http://www.vebebof.com>

♀王松: <http://www.hackersb.cn>

♀番茄师傅: <http://www.bl4ck.in>

♀sco4x0: <http://www.sco4x0.com>

🔪ctf-web

- ✓**实战型**: 时下火热漏洞的利用
- ✓**理论性**: 一些常见或不常见的trick考察
- ✓**脑洞性**: 毫无逻辑, 核心就是如何让人找不到flag

0x04:一些有趣的think/思路

flag隐含

0x01:注释里面含有flag

key在哪里？

分值: 100

[过关地址](#)

```
<html>
  <head>
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
  </head>
  <body>
    key就在这里中，你能找到他吗？
    <!--key is jflsjklejflkdsjfklds-->
  </body>
```

0x02: http header: flag

0x03: console

0x04: cookie

php中的小trick

★主要说下封装协议：

0x01: 比较

如果可以获取源码，可以将源码与官方源码进行diff

0x02: is-numeric

0x03: ★封装协议

✓php: //input

✓php://filter 最常用的文件包含命令

可这样绕过获取webshell

①shell进行base64编码

②通过string.stp_tags 去标签

③解码导入webshell

✓php.ini

short_open_tags_on

```
①<?=php echo base64_decode('phpinfo()');?&gt;
②&lt;script language='php'&gt;phpinfo();&lt;/script&gt;
③&lt;?=<?php echo base64_decode('phpinfo()');?&gt;</pre
```