Web-ctf-StudyNote

原创

ChengKaoAO 于 2017-10-19 10:28:02 发布

分类专栏： CTF 安全 CTF 文章标签： Web ctf

0x01背景说明

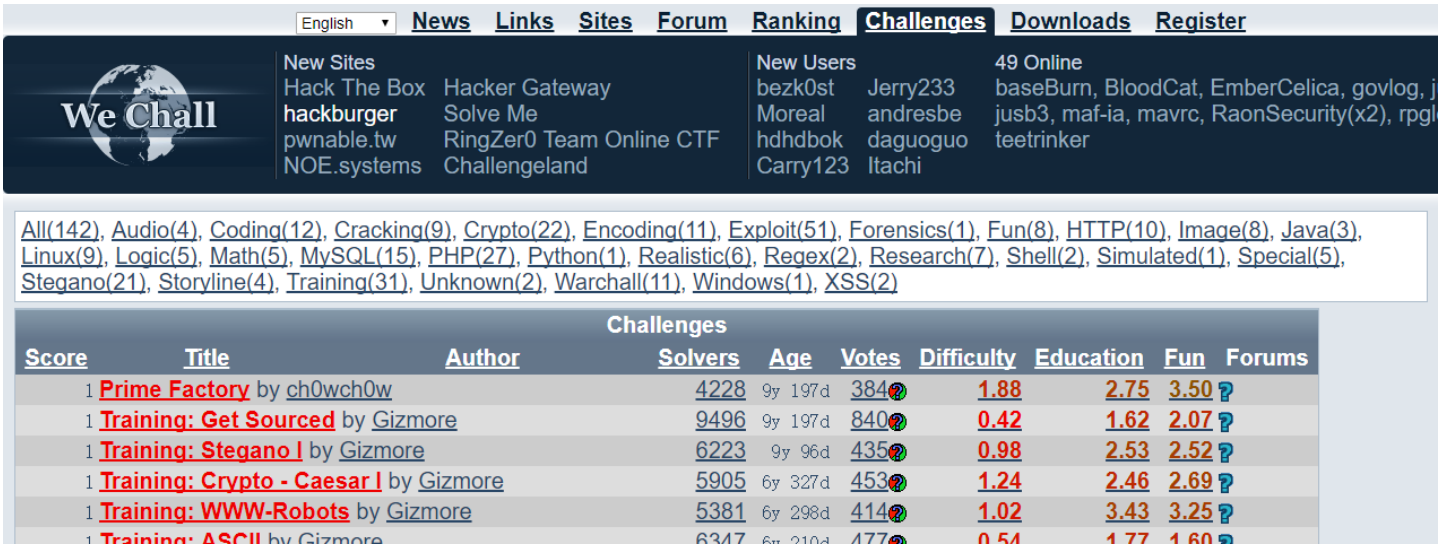
笔记章节：

- 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

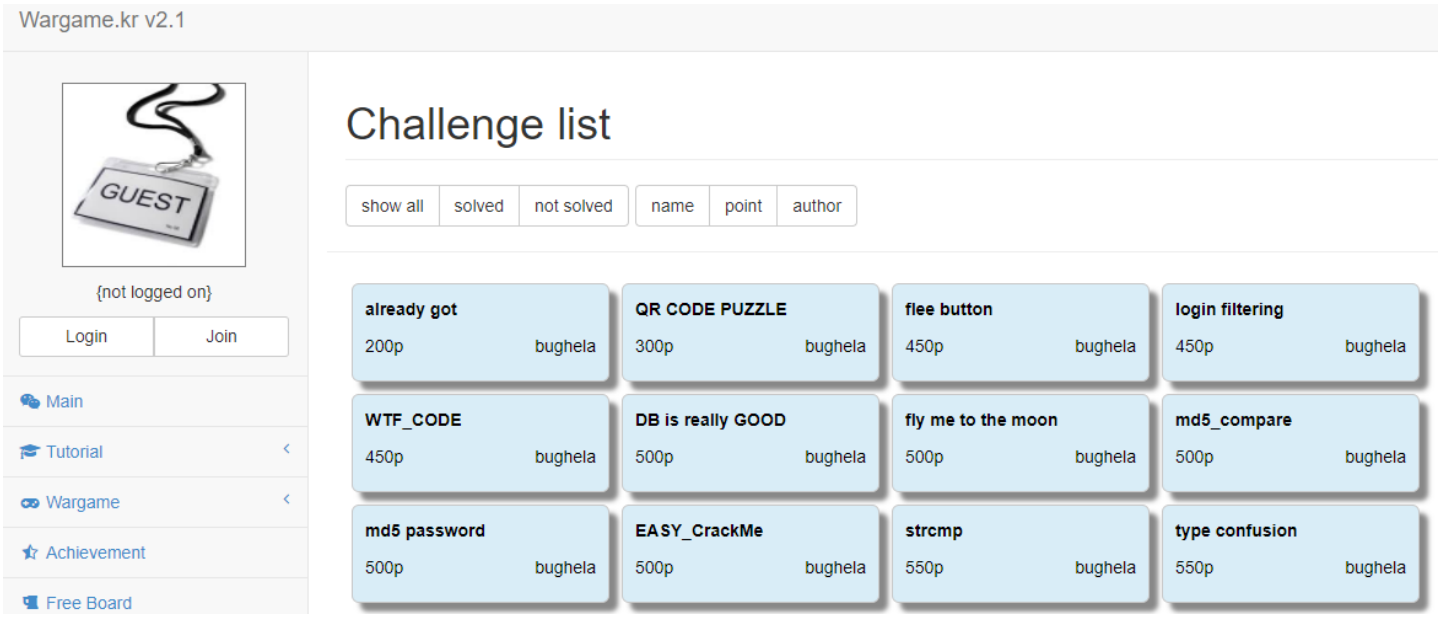
wechall ★★★★★

http://www.wechall.net/challs



Wargame ★★★

http://www.wargame.kr



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,Csrf…}
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)
♫**Exmaple**添加管理员账号

```
    $.ajax(|
    type:*post*
    url: * *
    data:"name=test pass$is admin=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.hacakersb.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

用户网络游侠刚刚答对了题目基情燃烧的岁月

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.strp_tags 去标签
③解码导入webshell
✔php.ini
short_open_tags_on

```
①<?=phpinfo( );?>
②<script language='php'>phpinfo( );</script>
③<?=phpinfo( ):?>
```