CTF-1

原创

Algcc 于 2020-10-07 11:56:48 发布 157 收藏
分类专栏： CTF 文章标签： 信息安全

CTF解题模式的题目类型

1. **web安全**：通过浏览器访问题目服务器上的网站，寻找网站漏洞（sql注入、xss、文件上传、包含漏洞、xxe，ssrf，命令执行、代码审计等），利用网站漏洞获得服务器的部分或全部权限，拿到flag，通常包含分值最大的web渗透题。
2. **逆向工程（Reverse）**：题目是一个软件，但通常没有软件的源代码；需要利用工具对软件进行反编译甚至反汇编，从而理解软件内部逻辑和原理，找出与flag计算相关的算法并破解这个算法，获得flag。
3. **漏洞挖掘和漏洞利用（PWN,EXPLOIT):**访问一个本地或远程的二进制服务程序，通过逆向工程找出程序中存在的漏洞，并利用程序中的漏洞获取远程服务器的部分或全部权限，拿到flag，非常难，分多。
4. **密码学（Crypto）**：分析题目中的密码算法与协议，利用算法或协议的弱点来计算密钥或对密文进行解密，从而获得flag。
5. **调查取证（Misc）**：利用隐写术等保护技术将信息隐藏在图像、音频、视频，压缩包中，或者信息就在一段内存镜像或网络流量中，尝试将隐藏的信息恢复出来即可获得flag，杂项，多练练。
6. **移动安全（Mobile）**：对安卓和IOS系统的理解，逆向工程等知识。

难度排行（由易到难）：

1. misc(杂项）
2. crypto（密码学）
3. web（网络）
4. reverse（逆向）难
5. pwn（二进制）大佬可

学习攻略

基础知识：

- Linux基础
- 计算机组成原理（了解）
- 操作系统原理（了解）
- 网络协议分析

A方向（需要具备扎实的编程基础）：

- PWN+Reverse+Crypto
- IDA工具（f5插件）
- 逆向工程
- 密码学
- 缓冲区溢出

B方向（需要熟悉web安全漏洞）：

- web+Misc
- 网络安全
- 内网渗透
- 数据库安全
- 信息收集能力
- HTTP协议、网络技术（HCNA/CCNA)、数据库的操作（SQL）
- 量变到质变