渗透测试工程师技术实战课

编辑器漏洞

常见的编辑器

- 常见的有Ewebeditor,fckeditor,ckeditor,kindeditor等等
  - 基于浏览器的、所见即所得的在线HTML编辑器。她能够在网页上实现许多桌面编辑软件（如：Word）所具有的强大可视编辑功能。WEB开发人员可以用她把传统的多行文本输入框<TEXTAREA>替换为可视化的富文本输入框，使最终用户可以可视化的发布HTML格式的网页内容。eWebEditor!已基本成为网站内容管理发布的必备工具!
- EWEBeditor编辑器漏洞利用
- FCKeditor编辑器漏洞利用
- 如何查看站点的编辑器类型

EWEBeditor编辑器漏洞利用

- 默认后台地址:/ewebeditor/admin_login.asp
- 检测admin_style.asp文件是否可以直接访问
- 默认数据库路径：[path]/db/ewebeditor.mdb
- 使用默认密码:admin/admin888 或admin/admin 进入后台，也可以尝试 admin/123456（有些管理员以及一些cms就是这么设置的）

渗透的一般步骤

- 找后台
- admin_style.asp
- admin/admin.asp
- 进后台
  - 使用默认密码（使用一些弱口令）
  - 下载mdb数据库（找到路径进入后下载）
  - burp 爆破
  - 注入（找注入点用SQLmap跑）
  - cookie欺骗

FCKeditor编辑器漏洞利用

- FCKeditor/_samples/default.html //编辑页
- FCKeditor/_whatsnew.html //查看编辑器版本
- fckeditor/editor/filemanager/connectors/test.html //查看文件上传路径
- 版本<2.4.x版本 通过黑名单验证绕过(.asa\.cer\.asp;jpg\.asp00[空格])
- 高版本可能存在%00截断

渗透的一般步骤

- 找到上传界面
- 上传图片马
- 抓包修改
- 比如在post url请求头最后面加上xxx.php（或asp ）%00 上传成功后会自动将文件名截断，上传后的文件名就改成了xxx.php（或asp）
- 转义

其他类型编辑器漏洞

- ckfinder编辑器漏洞
  - 找到ckfinder目录下的CKFinder.html，上传点就在这里.任意文件上传，然后利用IIS6.0文件解析漏洞，即可拿shell。
- PHPWEB网站管理系统后台kedit编辑器漏洞
  - 第一种是利用IIS6.0文件解析漏洞xxx.php;xx.jpg
  - 第二种方式%00截断xx.php%00jpg

编辑器漏洞防御

- 禁止下载文件类型
- 通过编辑器版本更新
- 修改后台地址
- 添加防爆破

谢谢观赏