

Day23 WEB漏洞-文件上传之解析漏洞编辑器安全

23.1 中间件解析漏洞



- 1 参考共享的中间件漏洞PDF
- 2 IIS6/ 7简要说明-本地搭建
- 3 Apache配置安全--vuthab
- 4 Apache换行解析-vulhub
- 5 Nginx解析漏洞-vulhub
- 6 Nginx文件名逻辑-vulhub

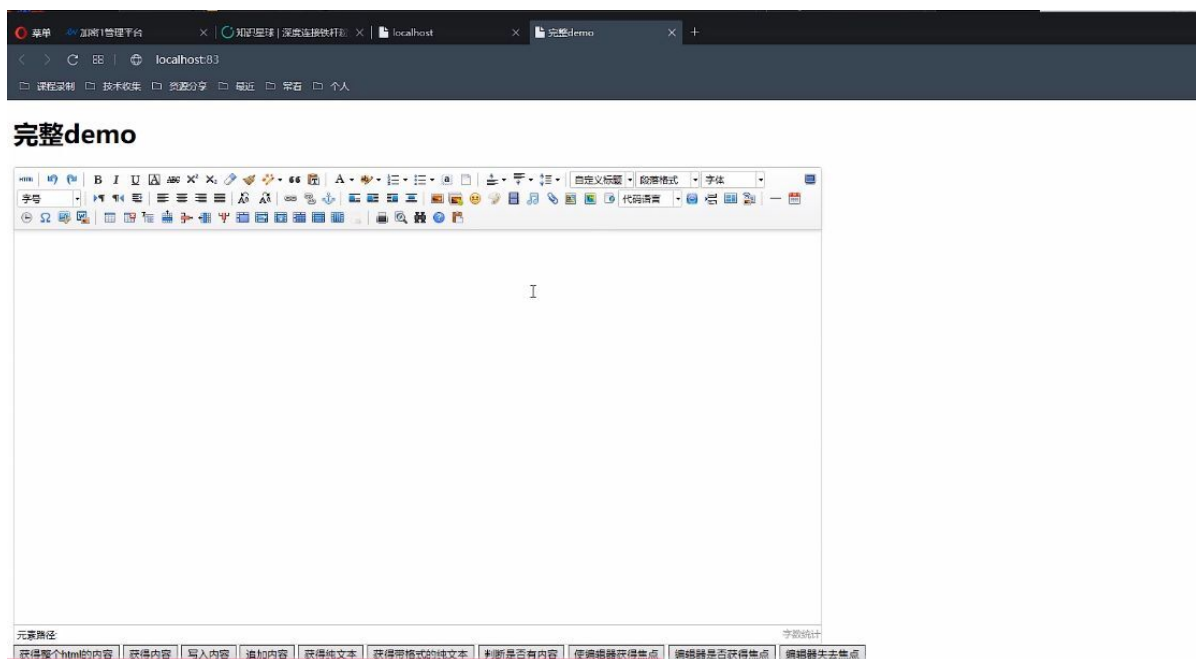


- 1 Apache 低版本解析漏洞
- 2 利用场景：
- 3 我们可以利用文件上传，上传一个不识别的文件后缀(x.php.xxx.yyy)，apache 识别不了最后的yyy，向前解析直到识别，利用解析漏洞规则成功解析文件，随后后门代码被触发。

- cmd命令行制作图片马：copy 1.png/b + 0.txt/a 10.png

23.2 编辑器漏洞

- 编辑器页面，看到这个要想到编辑器漏洞



- 常见的编辑器Fckeditor exp 利用Ueditor



1 扩展

- 2 1.POC(Proof ofConcept), 中文意思是“观点证明”。这个短语会在漏洞报告中使用, 漏洞报告中的POC则是一段说明或者一个攻击的样例, 使得读者能够确认这个漏洞是真实存在的。

3

- 4 2.EXP(Exploit), 中文意思是“漏洞利用”。意思是一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码, 可以使得读者完全了解漏洞的机理以及利用的方法。

5


- 6 3.VUL(vulnerability), 泛指漏洞。

7

- 8 4.CVE漏洞编号,CVE 的英文全称是“Common vulnerabilities & Exposures”公共漏洞和暴露, 例如CVE-2015-0057、CVE-1999-0001等等。CVE就好像是一个字典表, 为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称。如果在一个漏洞报告中指明一个漏洞, 如果有CVE名称, 你就可以快速地在任何其它CVE兼容的数据库中找到相应修补的信息, 解决安全问题。

- 9 可以在<https://cve.mitre.org/>网站根据漏洞的CVE编号搜索该漏洞的介绍。
- 10 也可以在中文社区<http://www.scap.org.cn/>上搜索关于漏洞的介绍
- 11
- 12 5.0DAY漏洞和0DAY攻击
- 13 在计算机领域中，零日漏洞或零时差漏洞（英语：**zero-dayexploit**）通常是指还没有补丁的安全漏洞，而零日攻击或零时差攻击（英语：**zero-dayattack**）则是指利用这种漏洞进行的攻击。提供该漏洞细节或者利用程序的人通常是该漏洞的发现者。零日漏洞的利用程序对网络安全具有巨大威胁，因此零日漏洞不但是黑客的最爱，掌握多少零日漏洞也成为评价黑客技术水平的一个重要参数。
- 14 零日漏洞及其利用代码不仅对犯罪黑客而言，具有极高的利用价值，一些国家间谍和网军部队，例如美国国家安全局和美国网战司令部也非常重视这些信息[1]。据路透社报告称美国政府是零日漏洞黑市的最大买家。

23.3 文件上传实战思路

- 
- 1 1. 上传文件和文件执行是两个东西
- 2 2. 漏洞分类{解析漏洞、cms漏洞、其他漏洞【编辑器漏洞、cve漏洞、安全修复】}
- 3
- 4 思路：
- 5 如果有一个网站，要从文件上传的方向开始
- 6 第一步：先看中间件，看是否存在解析漏洞/CMS/编辑器漏洞/CVE/
- 7 如果有，如何找：
- 8 字典扫描：扫描会员中心，文件上传的位置
- 9 找到后，如何利用：
- 10 验证/绕过

资源:



- 1 <https://navisec.it/>编辑器漏洞手册
- 2 <https://www.jb51.net/softs/75619.html>
- 3 <https://pan.baidu.com/share/init?surl=5gcdBu0FrN1F9xVN7Q7GSA> **enqx**