涉及知识

✧ 常见搭建平台脚本启用

✧ 域名IP目录解析安全问题

✧ 常见文件后缀解析对应安全

✧ 常见安全测试中的安全防护

✧ WEB后门与用户及文件权限

ASP,PHP,ASPX,JSP,PY,JAVAWEB等环境

WEB源码中敏感文件

后台路径，数据库配置文件，备份文件等

（寻找方式：google搜索方法、robots.txt文件、抓包、御剑、铸剑工具等）

IP或域名解析WEB源码目录对应下的存在的安全问题

域名访问，IP访问（结合类似备份文件目录）

脚本后缀对应解析（其他格式可相同-上传安全）

存在下载或为解析问题

常见防护中的IP验证，域名验证等

  用ip访问的权限比域名要高（比如有些目录只有ip才能访问出来：有些网站建设人员会疏忽，可以用ip去访问，有时会发现一些备份文件源码等）,使用御剑或者手动访问的时候就最好用ip，别用域名.

后门是否给予执行权限

后门是否给予操作目录或文件权限

后门是否给予其他用户权限

总结下关于可能会存在的安全或防护问题？

演示案例

(可以自行用iis服务器搭个网站，进行各种测试)

➢ 基于中间件的简要识别

➢ 基于中间件的安全漏洞

➢ 基于中间件的靶场使用

例：漏洞复现之 Apache HTTPD 多后缀解析漏洞

涉及资源

Vulhub靶场：https://www.vulhub.org/

Web中间件常见漏洞总结（pdf文件）