**网络空间安全学院课程答辩记录及评分表**

|  |  |  |  |
| --- | --- | --- | --- |
| **课程答辩记录** | | | |
| 教师主要  提问记录 | 1、该漏洞如何复现？  2、所漏洞原理？  3、该漏洞有哪些危害？ | | |
| 学生回答  问题情况 | 答：  1、通过下载相关的漏洞文件到本地，在本地部署好docker之后，再拉取镜像，开启docker容器，搭建好相应的漏洞复现的环境（受影响的软件版本），通过运行写好的poc文件越权到管理员权限，再利用软件自带的添加插件的功能，上传构造的恶意代码php文件  2、越权漏洞是指应用程序未对当前用户操作的身份权限进行严格校验，导致用户可以操作超出自己管理权限范围的功能，从而操作一些非该用户可以操作的行为。从狭义上讲越权访问，是攻击者在获得低权限用户的账户后，可以利用一些方式绕过权限检查，访问或者操作到原本无权访问的高权限功能。这类漏洞往往很难通过工具进行自动化检测，属于逻辑漏洞中的一种  3、越权漏洞的危害主要有1)、数据泄露：攻击者可以利用越权漏洞访问到不应该被其所见的数据，包括敏感信息，如用户名、密码、身份证号等。这些信息一旦被泄露，可能导致用户隐私泄露，给用户带来严重困扰。2)、数据篡改：攻击者可以利用越权漏洞篡改或删除重要的信息，如订单信息、交易记录等。这可能导致数据完整性受损，给企业和用户带来经济损失。3)、系统功能被滥用：攻击者可以利用越权漏洞对系统功能进行滥用，如执行未授权的操作、修改系统配置等。这可能导致系统可用性受到影响，甚至可能导致系统崩溃或数据丢失。 | | |
| **课程答辩成绩评定** | | | |
| 答辩成绩 | | |  |
| 是否同意通过 | | □同意 □不同意 | |
| 答辩教师签名： 年 月 日 | | | |

注：课程设计类课程答辩不通过则课程考核不通过。