

**教学实习报告**

实习单位: 成都信息工程大学

实习时间： 13周 至 15周

学 院: 网络空间安全学院

专 业: 信息安全

学生姓名: 杨佳伲 学号: 2022132006

2023 年 12 月 15 日

**成都信息工程大学 教务处制**

|  |
| --- |
| 1. 实习目的   通过实际操作，更深入地理解漏洞的形成原理、利用方式和修复方法。掌握漏洞复现技巧。学习并掌握如何有效地复现漏洞，这包括分析漏洞报告、理解漏洞上下文、构造测试用例等。通过实践，积累丰富的漏洞复现经验，为未来的工作和学习打下坚实的基础。通过解决实际问题，提升技能水平，包括对漏洞的认识、分析能力、代码审计能力等。  总的来说，漏洞复现实践实习的目的是为了培养漏洞复现能力、问题解决能力，提升技能水平和对软件安全的深入理解。 |
| 1. 实习单位及岗位介绍   实习单位：成都信息工程大学  岗位介绍：漏洞测试工程师是一种专门负责进行漏洞测试的工程师。他们通过对目标信息、信息系统、信息基础设施和网络进行模拟渗透攻击，以检验和测试其安全性。主要职责：  1）负责对目标信息、信息系统、信息基础设施和网络进行模拟渗透攻击，以检验和测试其安全性。  2）通过工具和技术手段对信息、信息系统、信息基础设施和网络进行分析并完成未知漏洞的发掘工作。  3）对信息、信息系统、信息基础设施和网络的漏洞和安全威胁进行评估，分析差距，评估风险水平，制定或推荐适当的加固措施。 |
| 三、实习内容及过程  1.选题为cve-2021-21389（漏洞复现）  2.需求  复现出该漏洞  3.总体设计  简单来说，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   1. 具体实践   在编程的过程中，感受到了信息安全的重要性，有了网络安全才有国家安全。同时经过查询资料了解到漏洞的一些运用方法，比如越权，0day漏洞等等  5.文档撰写  通过老师的指导，我的文档撰写能力得到很好的提升，能够对文字、图片实现更好的排版，符合格式要求；条理清晰，能够将自己的想法和编程逻辑通过文字传达出来。 |
| 四、实习总结及体会  系统设计期间，学习到很多课堂上没有的知识，还积累了很多实践经验，增强了动手能力和解决实际问题的能力。在此之前，对于漏洞复现技术或是其他的知识都只是略知皮毛，对知识没有深入了解。在短短的两周时间里，作者认真学习了关于漏洞复现等相关的知识，初步认识到漏洞挖掘的技术难度，对信息安全专业有了进一步的体会，学会了一些使用漏洞工具的技能。复现虽然完成，但是距离优秀仍存在一定差距，今后也需要继续学习。希望自己能不断学习和实践，争取以后做得更好。 |