四川农业大学信息与教育技术中心文件

信教发〔 2024 〕 10 号

四川农业大学网络安全渗透管理实施细则

（试行）

为保障学校网络安全，规范网络安全团队在校内开展渗透测试工作，结合学校实际，特制定本管理实施细则。

一、法律法规及管理要求

第一条 团队成员为我校师生，团队管理员由在职教师担任。团队成员在渗透测试中所有活动均应遵守《中华人民共和国网络安全法》及相关法律法规，确保测试行为合法合规。

第二条 团队在进行渗透测试前，应获得目标系统的授权，确保得到合法授权。

第三条 团队应定期向学校网络安全和信息化办公室汇报工作进展和结果，接受学校管理部门的指导和监督。

二、渗透测试范围与流程

第四条 团队只能对学校授权的系统及应用程序进行渗透测试，未经授权不得对未授权目标或校外目标进行测试。

第五条 渗透测试前，团队需向学校网络安全和信息化办公室提交申请，获得书面同意后方可进行相关操作。

第六条 团队在进行渗透测试前，须拟定测试方案，留底备查。推荐测试流程为：信息收集、漏洞扫描、漏洞验证、报告编制与提交。

三、结果上报与保密

第七条 团队应详细记录渗透测试方案、测试结果等，并以书面技术报告形式在完成测试后的 3 个工作日内及时上报网络安全和信息化办公室。

第八条 技术报告中需包括但不限于：漏洞发现过程、风险评估、建议修复措施、白盒测试账号等信息。

第九条 所有涉及渗透测试的信息均属保密内容，团队成员应严格保密，不得泄露给任何非授权人员。

四、注意事项

第十条 在挖掘、提交相关漏洞的过程中，应严格遵守国家相关法律法规，按照对信息系统机密性、可用性、完整性等三方面要素的影响评估，漏洞风险发现与技术验证应遵循无害化原则：

（一）可实现非授权访问或用户权限越权，在完成非授权逻辑、越权逻辑验证时，不应再获取和留存用户信息和信息系统文

件信息;

（二）可执行数据库查询条件，在获得数据库实例、库表名称等信息证明时，不应再查询涉及个人信息、业务信息的详细数据;

（三）可获得系统主机、设备高权限，在获得当前用户系统环境信息证明时，不应再获取其他用户数据和业务数据信息;

（四）禁止利用当前主机或设备作为跳板，对目标网络内部区域进行扫描测试;

（五）应充分估计目标网络、系统的安全冗余，不进行有可能导致目标网络、主机、设备瘫痪的大流量、大规模扫描;

（六）禁止执行可导致本地、远程拒绝服务危害的技术验证用例;

（七）禁止执行有可能导致整体业务逻辑扰动、有可能产生用户经济财产损失的技术验证用例;

（八）可获得信息系统后台功能操作权限，在获得当前用户角色属性证明时，不应再利用系统功能实施编辑、增删、篡改等操作;

（九）可获得系统主机、设备、数据库高权限，在获得当前系统环境信息证明时，不应再执行文件、程序、数据的编辑、增删、篡改等操作;

（十）可在信息系统上传可解析、可执行文件，在获得解析

和执行权限逻辑证明时，不应驻留带有控制性目的程序、代码;

（十一）测试完成之后，应该及时删除测试过程中遗留的相关文件和权限（如 Webshell 等），不得在目标系统中遗留任何后门或可能被其他人猜到的程序、代码;

（十二）不修改、不增加、不删除被测试网站的相关数据。在测试漏洞需要修改一定测试数据的情况下，请联系平台工作人员，获取最终授权后才能进行测试;

（十三）测试过程中仅可证明漏洞存在，进行无害化验证，不允许利用漏洞（如 Sql 注入）获取信息;

（十四）测试过程中利用漏洞获取到相关系统的权限，如若要继续深入，请先联系平台工作人员，请勿利用该权限进行扫描、设置跳板代理;

（十五）涉及金融相关漏洞的测试（如支付相关），请在漏洞报告中说明测试结果与测试账户，禁止借机利用相关漏洞牟利;

（十六）在漏洞挖掘过程中，不允许将漏洞内容泄露给无关人员。

（十七）其他可能存在影响系统安全运行的操作行为。

五、漏洞等级认定

（一）严重

漏洞危害严重，可能导致重大安全事故或数据泄露，需立即采取修复措施;

（二）高危

漏洞危害较大，可能引发中度安全事件，需优先处理;

（三）中危

漏洞存在一定危害，可能导致系统部分功能受损或一般数据泄露，需按计划进行修复;

（四）低危

漏洞危害较小，可能仅影响系统性能或少量数据泄露，可酌情处理;

（五）具体评级以漏洞审核人员根据实际影响判定为准。

六、奖励与处罚

第十一条 对于在渗透测试中表现优秀的团队成员，学校将给予相应的奖励，如证书、奖金或其他荣誉。

第十二条 对于违反本管理细则的团队成员，学校将按《四川农业大学信息化和信息安全管理办法》进行处罚。

七、经费管理

第十三条 网络安全渗透测试所需的相关费用从学校的网络安全专项经费中列支。

第十四条 经费使用应严格按照学校财务管理规定执行，确保专款专用。

八、附则

第十五条 本细则自发布之日起施行，由信息与教育技术中心负责解释和修订。

信息与教育技术中心

2024年12月24日