**2025年上半年社会实践心得**

**学院**：湖南第一师范学院 **班级**：24级网络2班

**姓名**：罗奋钢 **学号**：24405090232

**实践时间**：2025年6月20日至7月9日09点至17点30

**实践地点**：长沙市岳麓区-枫林三路608号罗马商业广场F1

**实践单位**：湖南省网安基地科技有限公司

**实践内容**：在网安基地学习实践使用Burp等多种软件，完成爆破等多种与网络安全相关的课程内容。

**一、前言**

在 2025 年 6 月 20 日，我怀着既紧张又期待的心情，踏入了位于岳麓区枫林三路 608 号罗马商业广场 F1 的湖南省网安基地科技有限公司，正式开启了为期三周（6 月 20 日至 7 月 9 日，每日 09 点至 17 点 30 分）的 “双百行” 社会实践活动。作为湖南第一师范学院 24 级网络 2 班的一名学生，在此之前，我对网络安全的认知大多停留在课本上的理论知识，对于实际操作中的工具使用、漏洞挖掘等环节，始终存在着一层 “距离感”。而这次实践，就像一把钥匙，为我打开了通往网络安全实战世界的大门。

在这三周的时间里，每一天都充满了新的挑战与收获。从最初面对复杂软件界面时的手足无措，到后来能够熟练运用工具完成指定任务；从对网络攻击流程一知半解，到能够清晰梳理出漏洞利用的逻辑链条，每一点进步都离不开基地导师的耐心指导和同事们的热心帮助。我们不仅系统学习了 Burp Suite、phpstudy 等多种专业软件的使用方法，还通过模拟真实场景，完成了爆破、SQL 注入、XSS 攻击防御等一系列与网络安全紧密相关的实践任务。这段经历让我对网络安全行业有了更直观、更深刻的理解，也让我真切感受到了理论与实践结合的重要性。以下，我将详细分享这次实践的心得体会，希望能为今后的学习和职业发展留下一份珍贵的记录。

**二、实践背景与目的**

随着数字化时代的全面到来，信息技术已深度融入人们的生产生活，从日常的在线购物、社交沟通，到企业的生产运营、政务部门的公共服务，几乎都依赖于网络系统。然而，在享受网络带来便利的同时，网络安全问题也日益凸显，成为威胁个人权益、企业发展乃至国家信息安全的重要隐患。

近年来，全球范围内的网络攻击事件频发，且呈现出手段多样化、影响范围广、危害程度深的特点。例如，2024 年某知名电商平台遭遇大规模数据泄露事件，数百万用户的个人信息和支付数据被窃取，不仅给用户带来了巨大的财产安全风险，也让企业陷入了严重的信任危机，直接经济损失超过亿元。给社会公共服务秩序造成了极大影响。

据中国互联网络信息中心（CNNIC）发布的最新数据显示，2024 年我国网络安全市场规模已达到 1200 亿元，年增长率保持在 25% 以上。这一数据既反映出我国网络安全市场的蓬勃发展态势，也从侧面印证了当前社会对网络安全服务的迫切需求。然而，与快速增长的市场需求相比，我国网络安全人才缺口却持续扩大。据行业报告统计，截至 2024 年底，我国网络安全人才缺口已超过 300 万，尤其是兼具理论知识和实战能力的复合型人才，更是成为企业争抢的 “香饽饽”。在这样的行业背景下，作为一名网络空间安全专业的学生，提升自身实战能力、积累行业经验，不仅是个人成长的需要，更是顺应行业发展趋势、为国家网络安全事业贡献力量的必然选择。

作为一名刚接触网络空间安全专业课程不久的大学生，我深知自己在网络安全领域的知识储备和实践能力还存在诸多不足。课堂上学习的课程，虽然为我搭建了基本的知识框架，但由于缺乏实际操作场景，很多知识点理解得并不透彻，尤其是在工具使用和漏洞分析方面，更是存在明显的短板。因此，我参与这次实践的核心目的，就是希望通过真实的工作场景，弥补理论与实践之间的差距，具体可分为以下三个方面：

****1.深化对核心技术的理解****：希望通过实际操作，深入掌握网络安全领域的核心技术，如渗透测试流程、漏洞挖掘方法、攻击与防御策略等。

****2.熟练掌握主流工具的使用****：网络安全工作离不开专业工具的支撑，Burp Suite、Nmap、Metasploit、phpstudy 等都是行业内常用的工具。我希望通过这次实践，能够熟练掌握这些工具的安装、配置和使用方法，了解不同工具在不同场景下的应用优势，为今后的学习和工作打下坚实的工具基础。

****3.提升解决实际问题的能力****：在实际的网络安全工作中，遇到的问题往往复杂多变，需要综合运用多种知识和技能来解决。我希望通过参与真实的项目任务，学会分析问题、制定解决方案、执行操作并验证结果的完整流程，提升自己的逻辑思维能力和应急处理能力，为未来的职业发展做好准备。

**三、实践内容与过程**

#### **3.1 学习使用Burp Suite进行爆破**

Burp Suite是网络安全领域最常用的渗透测试工具之一，主要用于拦截和修改HTTP请求。在实践的第一周，导师带领我们系统学习了Burp Suite的各项功能。我们从最基础的代理设置开始，逐步掌握了请求拦截、数据包修改等核心功能。

具体操作中，我们首先配置了浏览器代理，将流量导向Burp Suite的监听端口。这个过程看似简单，但却需要注意很多细节，比如证书的安装、端口的设置等。在成功配置代理后，我们开始学习如何拦截HTTP请求。通过修改请求参数，我们可以测试网站的各种功能是否存在漏洞。例如，在测试某电商网站的登录功能时，我们发现该系统没有设置有效的防爆破机制。于是，我们使用Burp Suite的Intruder模块，配合常见的用户名和密码字典，成功实施了爆破攻击，黑入了各种靶场甚至真实网站的后台。

这一过程让我深刻认识到密码安全的重要性。很多系统由于使用了简单的密码组合，或者没有设置登录失败锁定机制，很容易被攻破。作为未来的网络安全从业者，我意识到在设计系统时必须考虑到这些潜在风险，要采用更安全的认证方式，比如多因素认证、验证码等方法来保障安全。

导师在总结时告诉我们，在实际场景中，很多网站由于开发者安全意识不足，没有设置有效的防爆破机制，比如未限制登录失败次数、未使用验证码、允许简单密码等，导致黑客能够轻易通过爆破攻击获取用户账号权限。例如，有些网站即使连续输入 10 次错误密码，也不会锁定账号；有些网站的验证码设计过于简单，甚至可以通过自动化工具识别。这些漏洞都给用户的账号安全带来了极大的威胁。

作为未来的网络安全从业者，我意识到，在今后的工作中，不仅要能够发现这些漏洞，更要学会如何防范这些漏洞。比如，在设计系统时，应采用 “密码复杂度要求+ 登录失败锁定+ 多因素认证” 的组合防护策略，从源头提升账号的安全性。同时，也要向用户普及密码安全知识，引导用户使用复杂密码，并定期更换密码，避免在多个平台使用相同的密码。

#### **3.2使用phpstudy搭建本地环境并实践SQL注入**

如果说第一周的学习让我们掌握了 “攻击工具”，那么第二周的 SQL 注入学习，则让我们深入了解了 Web 应用中最常见的漏洞之一。导师告诉我们，SQL 注入漏洞由于其危害大、利用门槛相对较低的特点，长期以来都是黑客攻击的重点目标，因此，掌握 SQL 注入的原理、利用方法和防御策略，是每个网络安全从业者的必备技能。

我们使用phpstudy搭建了本地Web服务器环境，这个过程让我对Web应用的运行原理有了更深入的理解。phpstudy是一个非常方便的集成环境工具，一键点击即可快速部署Apache、PHP和MySQL等服务。

在环境搭建完成后，我们创建了一个存在SQL注入漏洞的测试网站。这个网站模拟了一个简单的留言板系统，由于开发者没有对用户输入进行过滤，导致存在严重的SQL注入漏洞。我们通过输入' OR '1'='1这样的简单的恶意语句，成功绕过了登录验证，获取了管理员权限。

除了这种简单的 “万能密码” 注入，导师还为我们介绍了多种不同类型的 SQL 注入技术，让我们对 SQL 注入有了更全面的认识：

* ****3.2.1基于错误的注入****：通过输入特殊字符，使服务器执行错误的 SQL 语句，并返回详细的错误信息（如数据库类型、表名、字段名等），攻击者通过分析错误信息来获取数据库结构。例如，在参数中输入' AND 1=2 UNION SELECT 1,version(),database()--，如果服务器返回了数据库版本和当前数据库名，就说明存在基于错误的注入漏洞。
* ****3.2.2联合查询注入****：利用UNION关键字，将两个或多个SQL 查询的结果合并返回。攻击者通过构造UNION SELECT语句，查询数据库中的敏感信息（如用户名、密码哈希值）。例如，在查询留言详情的 URL 中，将id=1修改为id=1 UNION SELECT 1,username,password FROM users--，就可以获取users表中的用户名和密码。
* ****3.2.3布尔盲注****：当服务器不返回错误信息，只返回 “存在” 或 “不存在”（如页面显示正常或显示错误）两种状态时，攻击者通过构造布尔表达式（如' AND EXISTS(SELECT \* FROM users WHERE username='admin')--），逐步判断数据库中的信息。这种注入方式耗时较长，但适用范围广。
* ****3.2.4时间盲注****：当服务器连布尔状态都不返回时，攻击者通过构造包含时间函数（如sleep()）的 SQL 语句，根据服务器的响应时间来判断条件是否成立。例如，输入' AND IF(1=1,sleep(5),0)--，如果页面加载了 5 秒才返回，说明1=1成立；如果立即返回，说明1=1不成立。

在这之后导师还详细讲解了防御SQL注入的各种方法，比如使用预处理语句、输入过滤、最小权限原则等。这些防御措施让我明白，网络安全不仅要会攻击，更要懂得如何防御，攻防兼备才是胜利的关键。

通过第二周的学习，我不仅掌握了 SQL 注入的多种利用方法，更深刻理解了 “攻防结合” 的网络安全理念。在实际工作中，我们既要能通过攻击手段发现漏洞，也要能从防御角度提出有效的解决方案，这样才能真正保障 Web 应用的安全。

3.3学习Web漏洞中的XSS攻击与防御

在掌握了 SQL 注入这一 “数据库层漏洞” 后，第三周我们将学习重点转向了 Web 应用的 “前端层漏洞”—— 跨站脚本攻击（XSS）。导师告诉我们，XSS 漏洞虽然不会直接对服务器或数据库造成破坏，但却能直接危害用户利益，如窃取用户 Cookie、冒充用户身份操作、诱导用户点击恶意链接等，是当前 Web 应用中最常见、危害最广的漏洞之一。

XSS 漏洞的核心原理是：Web 应用未对用户输入的内容进行过滤或转义，导致攻击者可以将恶意 JavaScript 代码注入到页面中，当其他用户访问该页面时，恶意代码会在用户的浏览器中执行，从而实现攻击目的。

为了直观理解 XSS 漏洞，我们首先搭建了一个包含 XSS 漏洞的测试环境 —— 一个简单的用户评论系统。该系统的功能很简单：用户可以在评论框中输入内容，点击提交后，评论会显示在页面的 “最新评论” 区域。由于开发者未对评论内容进行任何过滤，攻击者可以直接在评论框中输入包含 JavaScript 代码的内容，如<script>alert('XSS攻击成功')</script>。

当我们提交这条评论后，刷新页面，浏览器立即弹出了 “XSS 攻击成功” 的弹窗 —— 这表明恶意代码已经成功执行。更有趣的是，当其他用户访问这个评论页面时，只要加载到这条恶意评论，弹窗也会在他们的浏览器中触发。这让我意识到，XSS 漏洞的危害具有 “传染性”，一条恶意评论就可能影响所有访问该页面的用户。

根据恶意代码的存储方式和执行场景，导师将 XSS 分为反射型、存储型和 DOM 型三种类型，并通过实际案例为我们演示了每种类型的攻击过程。：

**3.3.1反射型XSS**：恶意脚本作为请求的一部分发送到服务器，并立即返回到用户的浏览器执行。我们通过构造一个包含恶意脚本的URL，诱使用户点击后触发攻击。

**3.3.2存储型XSS**：恶意脚本被永久存储在服务器（如数据库）中，每当用户访问相关页面时触发。我们在测试环境中模拟了攻击者将恶意脚本存入评论区，其他用户浏览时自动执行。

**3.3.3DOM型XSS**：通过修改页面的DOM结构触发漏洞，不依赖服务器响应。我们分析了前端代码中的不安全操作，并演示了如何利用这些漏洞。

在防御方面，导师强调了输入验证、输出编码和使用Content Security Policy（CSP）的重要性。通过实际操作这些防御策略，我们发现之前搭建的测试环境中的 XSS 漏洞被成功修复 —— 恶意代码要么被过滤，要么被编码为纯文本，无法再触发弹窗或窃取 Cookie。这让我明白，XSS 防御并非单一措施，而是需要结合输入过滤、输出编码、CSP等多种手段，形成 “多层次防御体系”，才能有效抵御各种类型的 XSS 攻击。

3.4 综合实战演练

经过前两周的专项学习，我们已经掌握了 Burp Suite、Nmap、phpstudy 等工具的使用方法，以及爆破、SQL 注入、XSS 等漏洞的利用与防御技巧。为了检验我们的学习成果，实践的最后两天，基地组织了一场综合实战演练，模拟真实的网络渗透测试场景 —— 对一个虚构的 “企业内网” 进行渗透测试，目标是获取域控制器的管理员权限。

#### **3.4.1 实战前准备与目标分析：**演练开始前，导师为我们介绍了目标环境的基本情况：该企业内网包含多台服务器和一台域控制器，所有设备处于同一局域网中；我们的测试机与目标内网处于同一网段，可以通过网络访问目标设备。

接到任务后我制定了渗透测试计划：

第一步，使用 Nmap 对目标网段进行全面扫描。

第二步，针对开放的服务（如 Web 服务、FTP 服务、远程桌面服务），寻找潜在漏洞（如 SQL 注入、弱口令、未授权访问）。

第三步，利用漏洞获取初始访问权限，并尝试提权。

第四步，横向渗透，获取内网其他主机的信息。

第五步，整理测试过程和结果，撰写渗透测试报告。

#### **3.4.2信息收集与漏洞发现：**我决定优先对 192.168.1.100 的 Web 服务进行测试，因为 Web 服务通常是内网渗透的 “突破口”。在浏览器中访问一个网址，发现该主机部署了一个企业内部的 “员工信息管理系统”，包含登录页面、员工列表查询、个人信息修改等功能。

我首先尝试使用 Burp Suite 对登录页面进行弱口令爆破，加载常见的用户名（如 admin、hr、it）和密码字典，选择 “Cluster Bomb” 模式进行爆破。经过大量的测试，成功使用 “admin/admin123” 的账号密码登录到系统后台。在后台中，发现系统存在 “文件上传” 功能 —— 管理员可以上传员工头像图片。我尝试上传包含一句话木马的文件，但系统提示 “仅允许上传 jpg、png 格式的文件”。

为了绕过文件上传限制，我使用 Burp Suite 拦截文件上传请求，将文件后缀名从 “php” 修改为 “jpg”，同时在请求头的 “Content-Type” 字段中添加 “image/jpeg”（模拟图片文件类型）。提交请求后，文件成功上传，系统返回了上传路径，但直接访问该路径无法执行 PHP 代码，因为文件后缀名为 jpg。

此时，我想到之前学习的 “文件包含漏洞”—— 如果系统存在文件包含漏洞，就可以通过包含上传的 jpg 文件，执行其中的 PHP 代码。我在系统后台寻找可能存在文件包含漏洞的功能，最终在 “员工信息导出” 功能中发现了线索。

#### **3.4.3 提权与横向渗透：**获取低权限 Shell 后，发现当前用户无法访问系统的敏感目录，也无法执行高权限命令（如添加管理员账号）。因此，我们需要进行 “提权”—— 将低权限用户提升为管理员权限。

我们首先使用 “Windows Exploit Suggester” 工具（用于检测 Windows 系统的漏洞和可利用的提权 exp）对目标服务器进行检测，发现该服务器运行的 Windows Server 2012 存在 “MS16-032” 漏洞（一种本地提权漏洞）。我们从网上下载了该漏洞的 exp（可执行文件），通过中国菜刀将 exp 上传到目标服务器的临时目录，并在 Shell 中执行 exp。执行成功后，当前用户被提升为 “SYSTEM” 权限（系统最高权限）。

获取管理员权限后，我们开始收集目标服务器的敏感信息：通过查看 “hosts” 文件，了解内网其他主机的域名和 IP 对应关系；通过查看 “远程桌面连接历史记录”，获取其他主机的登录账号和密码线索；通过运行 “net user” 命令，查看当前服务器的用户列表，发现存在一个名为 “itadmin” 的用户，密码可能与其他主机通用。

我们尝试使用 “itadmin” 账号和猜测的密码（根据之前的弱口令规律，猜测为 “itadmin@2025”），通过远程桌面（mstsc）连接端口，成功登录该主机。

#### **3.4.4获取域控制器权限与演练总结：**拿到域控制器的管理员账号和密码后，我们通过远程桌面连接 192.168.1.300，成功登录域控制器。在域控制器中，我们可以查看域内所有用户的账号信息、修改域策略、管理所有加入域的主机，意味着我们已经完成了本次实战演练的目标 —— 获取域控制器的管理员权限。

在演练总结会上，导师对我的表现给予了肯定，同时也指出了我们在过程中存在的不足：例如，在信息收集阶段，我们没有对目标服务器的 FTP 服务进行测试，错过了一个可能存在弱口令的漏洞；在提权阶段，我们花费了较多时间寻找合适的 exp，说明对常见 Windows 漏洞的了解还不够深入。

**四、实践收获与体会**

三周的实践时光虽然短暂，但带给我的收获却远超预期。无论是技术能力的提升，还是对行业认知的深化，都让我对网络安全领域有了全新的理解，也为我今后的学习和职业发展奠定了坚实的基础。

4.1技术能力的提升

在实践开始前，我对网络安全工具的使用仅停留在 “知道名称” 的层面。虽然了解 SQL 注入、XSS 的基本概念，但从未在真实环境中尝试过漏洞利用。而经过这次实践，我的技术能力实现了从“理论” 到“实战” 的跨越。

通过这次实践，我的技术能力得到了显著提升。首先，我熟练掌握了Burp Suite、Nmap、Metasploit、phpstudy等主流安全工具的使用方法。这些工具在实际工作中非常重要，能够大大提高工作效率。其次，我对常见的Web漏洞，如SQL注入、XSS、CSRF等有了更深入的理解。最重要的是，我学会了如何将理论知识应用到实际问题中，这种能力对于网络安全从业者来说至关重要。

4.2 对网络安全行业的认识

在实践之前，我对网络安全行业的认知大多来自影视作品 —— 认为网络安全工程师就是 “坐在电脑前，敲几行代码就能攻破系统” 的 “黑客”。但真正深入行业后，我才发现这种认知存在巨大的偏差。

在这次的实践中，我对网络安全行业有了更清晰的认识。网络安全是一个快速发展的领域，新的攻击技术和防御手段不断涌现。作为从业者，必须保持持续学习的态度，时刻关注最新的技术动态。同时，网络安全工作也肩负着重大的责任，我们的工作直接关系到企业和用户的数据安全。因此，良好的职业道德和法律意识同样重要。

此外，网络安全行业的 “复合型人才需求” 也给我留下了深刻印象。一个优秀的网络安全工程师，不仅要懂技术，还要懂业务（如了解金融、医疗等不同行业的系统架构和安全需求），更要懂沟通（如将复杂的技术问题转化为通俗易懂的语言）。在这次的学习中，我认识到这种 “技术 + 业务 + 沟通” 的综合能力，正是我需要努力提升的方向。

4.3 团队协作与沟通能力

在学校的学习中，我大多是 “独立完成任务”，很少有机会参与团队合作。但在这次实践中，尤其是综合实战演练环节，团队协作的重要性让我有了切身体会。

在综合实战演练中真的是深刻体会到团队协作的重要性。网络安全工作往往需要多人配合，每个人都有自己的专长领域。良好的沟通能够确保信息及时共享，避免重复工作。同时，在遇到困难时，团队成员的互相支持和鼓励也非常重要。这次实践不仅提升了我的技术能力，也锻炼了我的团队协作和沟通能力。

五、不足与改进方向

在实践中，我主要掌握了 SQL 注入、XSS、弱口令爆破等基础漏洞的利用方法。尽管这次实践让我受益匪浅，但我也清醒地认识到自己的不足之处。

首先，对于一些复杂的漏洞，如堆溢出、格式化字符串漏洞、内核漏洞等，却缺乏深入的理解。这些漏洞往往涉及底层原理（如操作系统内核、程序内存结构），利用难度较大，需要较强的编程能力和逆向分析能力。

其次，在当前网络安全行业的发展趋势日益多元化，云安全、物联网安全、工控系统安全等新兴领域逐渐成为热点。但在这次实践中，我接触的主要是传统的 Web 安全领域，对新兴领域的知识几乎没有涉及。例如，我不了解云平台（如阿里云、腾讯云）的安全架构，不知道如何防范云环境中的配置错误、数据泄露等风险，还有多种难题也未涉及。这种知识储备的薄弱，可能会限制我今后的职业发展方向。针对这些不足，我制定了以下改进计划：

1.加强理论学习：系统学习《Web应用安全权威指南》、《黑客攻防技术宝典》等专业书籍，夯实理论基础。

2.参与CTF比赛：通过参加网络安全竞赛，锻炼实战能力，学习最新的攻防技术。

3.建立知识库：定期整理学习笔记，建立自己的安全知识体系。

4.关注行业动态：订阅安全牛、FreeBuf等专业媒体，了解最新的安全事件和技术趋势。

### **六、总结**

回望这三周的实践经历，从最初踏入湖南省网安基地科技有限公司时的紧张与期待，到如今结束实践时的充实与坚定，每一个瞬间都值得珍藏。这次 “双百行” 社会实践，不仅让我在技术层面实现了从 “理论” 到 “实战” 的跨越，更让我在认知层面完成了对网络安全行业的重新理解，它不是影视作品中炫酷的 黑客操作，而是一份需要严谨、责任和持续学习的事业；它不仅需要扎实的技术能力，更需要强烈的法律意识和职业道德。

通过这次实践，我更加坚定了从事网络安全工作的决心。未来，我将以更高的标准要求自己，持续学习和提升。同时，我也希望能有机会参与更多的实际项目，积累经验，为将来成为一名优秀的网络安全工程师打下坚实基础。

最后，我要向湖南省网安基地科技有限公司表示衷心的感谢，感谢公司为我们提供了这么好的实践平台，让我们有机会接触真实的网络安全工作场景；我还要感谢所有指导过我的导师，感谢他们耐心的讲解、细致的指导和无私的分享 —— 是他们的帮助，让我在这次实践中收获满满。

20 天的实践时光虽然短暂，但这段经历已经成为我专业成长道路上的重要里程碑。未来，我将以这次实践为起点，保持学习的热情，不断提升自己的技术能力和综合素养，朝着成为一名优秀网络安全工程师的目标坚定前行！





