****

说明：生产实习共性内容已经填写好，无需改动，红色说明部分打印前删除。要求排版规范，目录页码需重新生成。**3.4 实习项目具体内容为重点内容，即知识点描述 及 一次网络渗透测试项目实施过程描述等等**

**生产实习报告**

题 目： 网络渗透测试

院 （系）： 计算机与信息安全学院

专 业： 信息安全

学生姓名： 李玉婷

学 号： 1600300502

企业导师： 蒋春华

校内导师： 姚罡

2019年7月31日

目 录

[1. 实习的目的及任务 3](#_Toc18182234)

[1.1 实习的目的 3](#_Toc18182235)

[1.2 实习任务要求 3](#_Toc18182236)

[2. 实习单位及岗位简介 3](#_Toc18182237)

[2.1 实习单位简介 3](#_Toc18182238)

[2.2 实习岗位简介 3](#_Toc18182239)

[3. 实习内容 3](#_Toc18182240)

[3.1 公司制度及安全 3](#_Toc18182241)

[3.2 企业生产流程 4](#_Toc18182242)

[3.3 自己承担的角色 6](#_Toc18182243)

[3.4 实习项目具体内容 6](#_Toc18182244)

[4. 实习心得体会 9](#_Toc18182245)

[4.1 工程实践对环境与社会可持续发展的影响 9](#_Toc18182246)

[4.2 职业规范 9](#_Toc18182247)

[4.3 个人成长和职业发展的感想 10](#_Toc18182248)

# 实习的目的及任务

## 1.1 实习的目的

生产实习是实现理论知识和实践相结合的重要环节。通过实习，学生将对于课堂学习的基础和专业理论知识有更深入的掌握。特别是对信息安全技术与工程的最新发展和应用有较深入的了解。同时通过生产实习，进一步锻炼学生理论与实践相结合的能力，提高学习的主动性，为毕业后的社会工作打下良好的基础。

## 1.2 实习任务要求

1．严格遵守企业各项规章制度，学生以真实员工的身份融入得到企业的生产环境和管理方式中。

2．了解网络渗透测试、软件开发过程，参与软件项目的管理与开发，了解最新软件技术，熟悉网络渗透测试、软件开发工具，特别是网络安全管理、密码应用、计算机病毒与防护、网络入侵检测等方面的技术与工具在企业信息安全管理中的应用。

3．锻炼学生的人际交往和团队精神、集体荣誉感和责任感，使他们日后能较快融入到社会工作中。

4．学生通过实习，要认清自己能力，发现理论知识的不足，为后续学习增加动力和明确方向。

1. 实习结束后，提交实习心得或实习报告。

# 实习单位及岗位简介

## 2.1 实习单位简介

武汉梦极光科技有限公司成立于2018年5月，是一家提供软件和信息技术服务新型互联网企业。业务范围包括：网络安全产品开发、互联网渗透测试、系统上线测试、应急响应、服务解决方案、安全运维等信息安全服务。目前公司主要的服务对象是公安和政府相关部门。

## 2.2 实习岗位简介

（说明：根据你的实习报告内容进行实习岗位定位，如网络渗透工程师等等，对该岗位进行介绍）

网络渗透工程师：在客户已授权的网站或系统上进行被动信息收集和主动信息收集、漏洞扫描与利用并生成渗透测试报告。

# 实习内容

## 3.1 公司制度及安全

了解公司管理制度以及相应的安全规范，为步入信息安全行业提前打好基础。企业管理制度学习内容包括企业文化学习、企业规章制度学习(如上下班时间、工作内容、如何请假等)、奖惩制度学习等等内容。安全规范学习，由于信息安全行业有其自身特殊性，所以在工作过程中需要特别注意操作规范。安全规范学习目的，一方面是规范的操作可以使甲方系统在测试过程中可以保持稳定运行，再者自己拥有强大的安全意识，才能赢得客户认可。

## 3.2 企业生产流程

一套完整规范的生产流程对于企业工作的开展、软件的开发是起着非常重要的作用的，所以需要掌握信息安全企业在渗透测试或者软件开发时需要用到的规范流程。

1. 渗透测试流程
   1. 甲乙方确定测试对象、范围、时间

确定范围：测试的范围，如：IP、域名、内外网、整站or部分模块

确定规则：能渗透到什么程度（发现漏洞为止or继续利用漏洞）、时间限制、能否修改上传、能否提权...

目标系统介绍、重点保护对象及特性。

是否允许数据破坏？

是否允许阻断业务正常运行？

测试之前是否应当知会相关部门接口人？

接入方式？外网和内网？

测试是发现问题就算成功，还是尽可能的发现多的问题？

渗透过程是否需要考虑社会工程？

**确定需求：**web应用的漏洞(新上线程序)？业务逻辑漏洞（针对业务的）？人员权限管理漏洞（针对人员、权限）？  
根据需求和自己技术能力来确定能不能做、能做多少

分析风险，获得授权

分析渗透测试过程中可能产生的风险，如大量测试数据的处理、影响正常业务开展、服务器发生异常的应急、数据备份和恢复、测试人力物力成本...由测试方书写实施方案初稿并提交给客户（or本公司内部领导）进行审核。在审核完成后，从客户（or本公司内部领导）获取对测试方进行书面委托授权书，授权测试方进行渗透测试。

* 1. 信息收集

采用被动信息收集和主动信息收集方式，尽量多的收集关于目标web应用的各种信息，如：脚本语言的类型、服务器的类型、使用的开源软件、数据库类型、所有链接页面，用到的框架等。

被动收集：利用搜索引擎收集目标系统公开系信息，获得后台、未授权页面、敏感url

基础信息：IP，网段，域名，端口

系统信息：操作系统版本

应用信息：各端口的应用，例如web应用，邮件应用等

版本信息：所有探测到的版本

服务信息：服务器类型、版本

人员信息：域名注册人员信息，web应用中网站发帖人的id，管理员姓名等

防护信息：试着看能否探测到防护设备

* 1. 漏洞探索

利用上一步中列出的信息，使用相应的漏洞检测

方法：

1）漏扫：AWVS、AppScan...

2）结合漏洞去exploit-db等位置找利用

3）在网上寻找验证POC

内容：

系统漏洞：系统没有及时打补丁

Websever漏洞：Websever配置问题

Web应用漏洞：Web应用开发问题

其它端口服务漏洞：各种21/8080(st2)/7001/22/3389

通信安全：明文传输，token在cookie中传送等

* 1. 漏洞验证

将上一步中发现的有可能可以成功利用的全部漏洞都验证一遍，结合实际情况，搭建模拟环境进行试验，成功后再应用于目标中。

1. 自动化验证：结合自动化扫描工具提供的结果。
2. 手工验证：根据公开资源进行验证。
3. 试验验证：自己搭建模拟环境进行验证。
4. 登录猜解：有时可以尝试猜解一下登陆口的账号密码等信息。
5. 业务漏洞验证：如发现业务漏洞，要进行验证。
6. 公开资源的利用：exploit-db、wooyun、渗透代码网站、通用缺省口令、厂商的漏洞警告等
   1. 信息分析

将渗透获得的信息进行分析、为下一步实施渗透做准备。

1. 精准攻击：准备好上一步探测到的漏洞exp（漏洞利用），用来精准攻击
2. 绕过防御机制：是否有防火墙等设备，如何绕过
3. 定制攻击路径：最佳工具路径，根据薄弱入口，高内网权限位置，最终目标
4. 绕过检测机制：是否有检测机制，流量监控，杀毒软件，恶意代码检测等（免杀）
5. 攻击代码：经过试验得来的代码，包括不限于xss代码，sql注入语句等
   1. 修复建议

根据漏洞信息给出相应的修复建议

* 1. 输出报告

1. 信息整理

整理渗透工具：整理渗透过程中用到的代码，poc，exp等。

整理收集信息：整理渗透过程中收集到的一切信息。

整理漏洞信息：整理渗透过程中遇到的各种漏洞，各种脆弱位置信息。

目的：为了最后形成报告，形成测试结果使用。

1. 形成报告

按需整理：按照之前第一步跟客户确定好的范围，需求来整理资料，并将资料形成报告。

补充介绍：要对漏洞成因，验证过程和带来危害进行分析。

修补建议：当然要对所有产生的问题提出合理高效安全的解决办法。

1. 软件开发流程
   1. 产品定义
   2. 需求分析
   3. 市场分析
   4. 产品定位
   5. 产品规划
   6. 产品研发
   7. 产品运营

（说明：以上各小点需扩充）

## 3.3 自己承担的角色

（说明：在整个项目中，个人所起的作用：项目成员或负责人；阐述承担的具体任务）

在整个项目中，我作为项目成员，主要负责渗透测试环节中的信息搜集和渗透工作，信息搜集的主要工作是从网络上搜集到尽量多的目标的信息和公开数据，如通过googlehack、网站子站、网段扫描等进行信息搜集工作，此外还需要对目标系统进行与目标主机进行直接交互，从而拿到目标信息的主动信息收集。

## 3.4 实习项目具体内容

（包括实习项目的需求分析、设计、开发、结论）

**实习报告重点内容**

需求分析

1. nmap 扫描实践

nmap –sV –p 80 –v –script default,http\* 172.16.1.101

nmap -v -sS 172.16.1.101 # 使用SYN扫描目标

nmap -v -sT 172.16.1.101 # 使用TCP Connect()方式扫描

nmap -v -sU 172.16.1.101 # 扫描udp端口

nmap -v -sU -T4 172.16.1.101

nmap -v -O 172.16.1.101 # 扫描并检测目标系统

nmap -v -p1-443 172.16.1.101 #使用默认方式扫描1-443端口

nmap -sS -Pn -A -T4 172.16.1.101 #使用syn扫描，不使用Ping扫描存活主机，全端口扫描，使用模板4进行扫描小实验：扫描所有开放端口，同时检测开放端口的服务以及操作系统，记录好操作的步骤及截图，并且记录扫描时 间。（至少使用十条不同命令）

1. 使用nc连接开放端口

尝试手动连接端口（开放的），记录其返回信息。

nc 172.16.1.101 21

nc 172.16.1.101 22

nc 172.16.1.101 23

nc 172.16.1.101 25

nc 172.16.1.101 80

......

小实验：截图记录NC连接各个端口的结果

1. 编写python扫描器

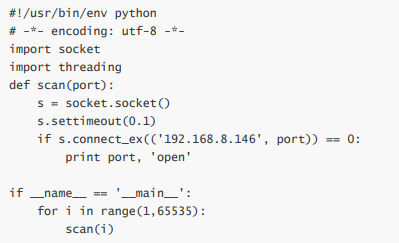
python编写扫描器（TCP Connect）,使用TCP Connect方式扫描端口

安装pycharm

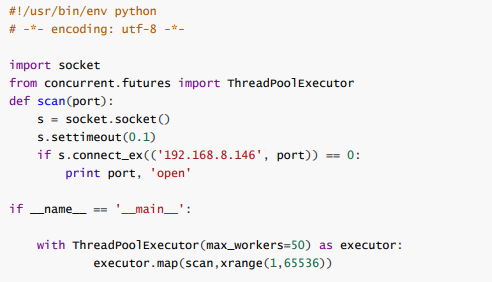
tar -xzvf pycharm-community-2019.1.3.tar.gz #解压

./bin/pycharm.sh #运行

参考代码：



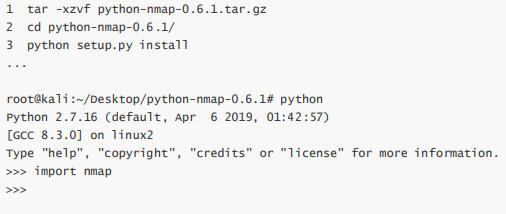
多线程版本：



小实验：自己编写一个多线程的端口扫描器，扫描结果为 （开放端口 - > 对应服务 ）；并对靶机进行扫描，附上代 码以及扫描结果截图

1. python 调用nmap扫描端口

安装python-nmap库



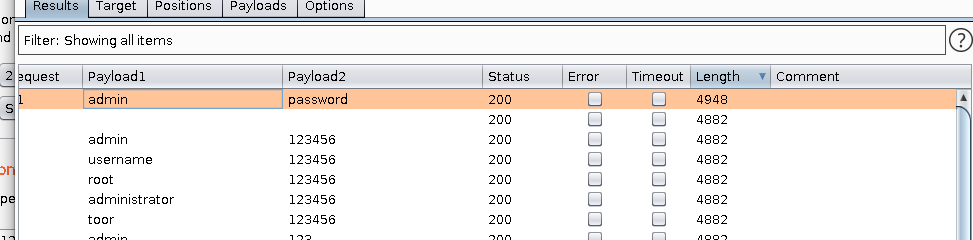
参考代码 略。

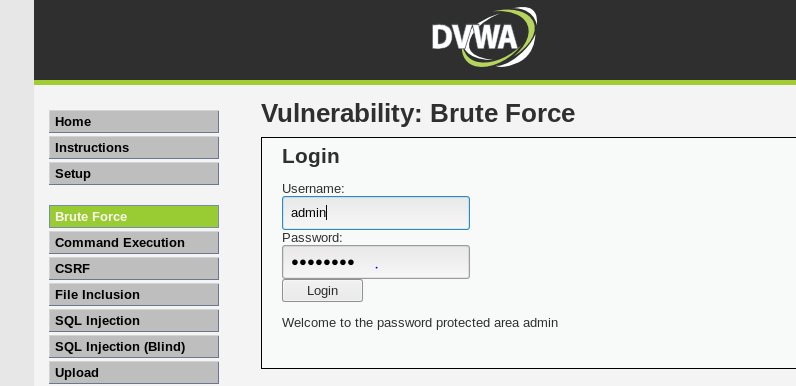
1. metasploitable 靶机渗透

至少复现5个漏洞并且截图记录。

1. 弱密码爆破

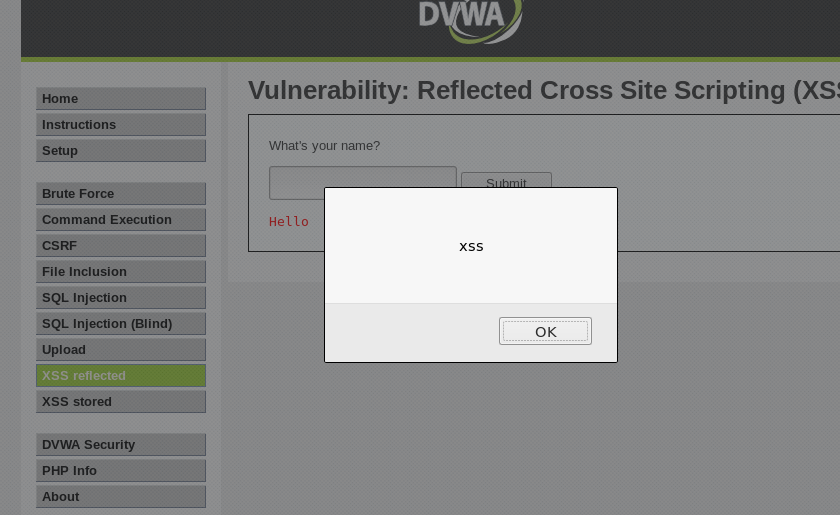
在metasploitable2的DVWA中，在弱密码爆破处可使用burpsuite拦截进行密码爆破，爆破效果如下：





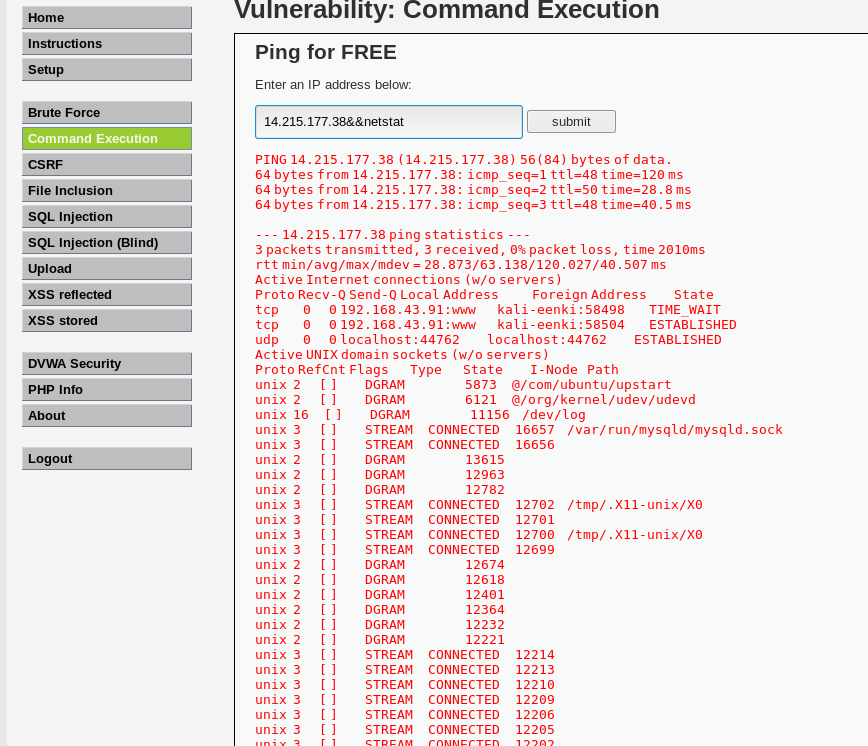
1. XSS漏洞

在DVWA的XSS处存在XSS漏洞，可以输入JavaScript代码并得到执行，输入代码为：



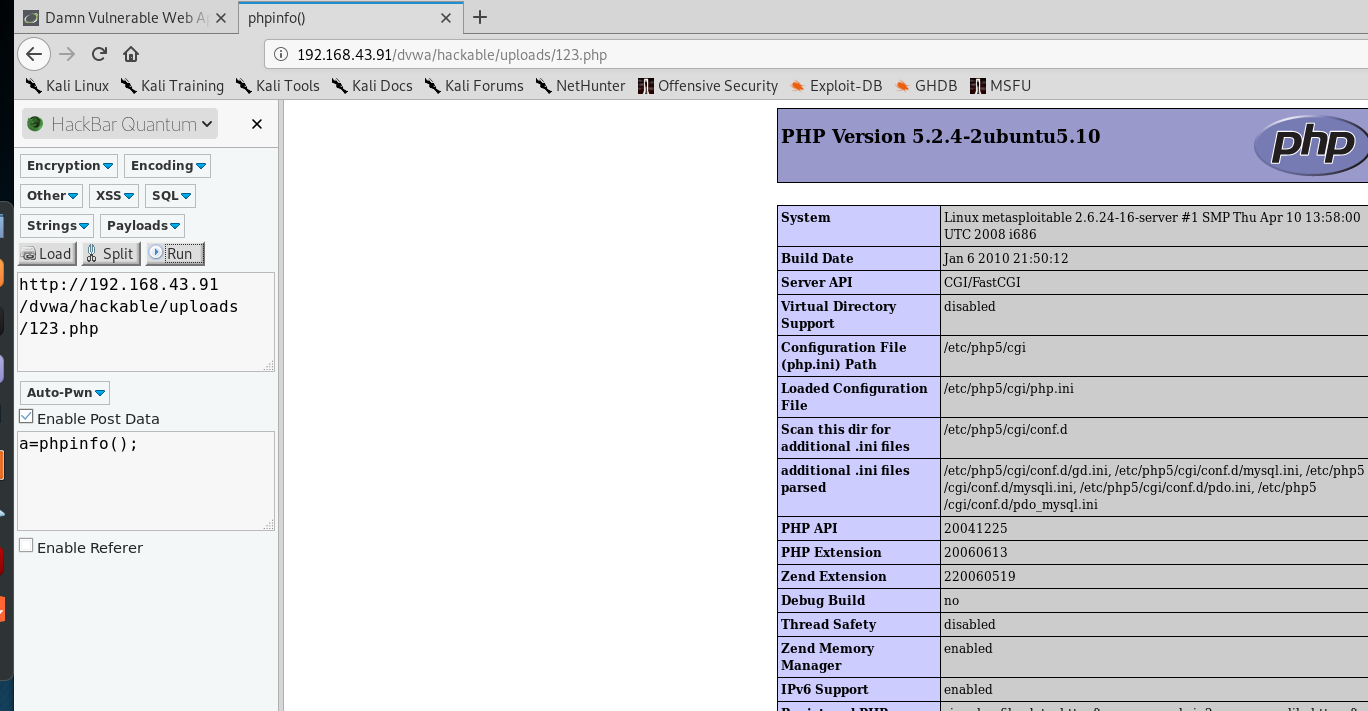
1. 命令执行

命令执行漏洞是由于其在执行命令之后没有校验是否只是执行一个命令而导致的，利用输入参数为：百度IP&&netstat，效果如下：

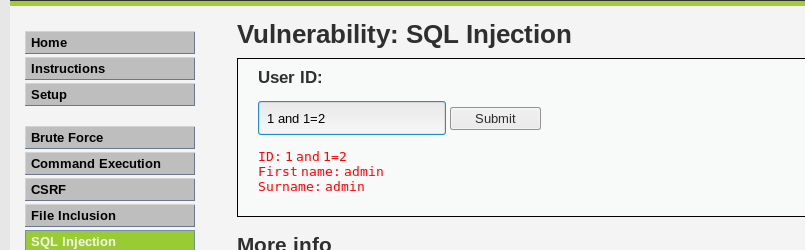


1. 文件上传

文件上传漏洞是服务器未对上文的文件格式，大小进行验证，导致任意文件上传漏洞，效果如下：



1. Sql注入漏洞

Sql注入是由于服务器未对用户输入的参数进行校验而直接将参数进行解析，代入sql语句中进行执行而导致的数据库信息泄露。效果如下

# 实习心得体会

## 4.1 工程实践对环境与社会可持续发展的影响

（说明：具有环境保护和可持续发展意识，正确认识专业工程实践与环境、可持续发展的关系，理解、分析和评价项目周期中可能对环境、社会可持续发展的影响）

通过本次实习学习渗透测试技术，进一步增强了我的渗透测试能力，使得我懂得作为安全专业学员，维护计算机安全的重要性，更加懂得了国家安全对于我们的重要意义，社会与环境的发展是需要建立在安全的基础上，现在是信息时代，计算机的安全显得尤为重要。

## 4.2 职业规范

（说明：阐述工程伦理的核心理念，计算机行业职业性质和责任，论述工程师的职业道德）

任何职业都需遵循职业道德规范，职业道德规范包括基本的道德规则和特殊的职业责任。其中基本的道德规则包括：为社会和人类的美好生活作出贡献；避免伤害其他人；做到诚实可信；恪守公正并在行为上无歧视；敬重包括版权和专利在内的财产权；对智力财产赋予必要的信用；尊重其他人的隐私；保守机密。此外，还有待殊的职业责任包括：努力在职业工作的程序与产品中实现最高的质量、最高的效益和高度的尊严；获得和保持职业技能；了解和尊重现有的与职业工作有关的法律；接受和提出恰当的职业评价；对计算机系统和它们包括可能引起的危机等方面作出综合的理解和彻底的评估；重视合同、协议和指定的责任 。

计算机行业的特点决定了计算机专业人员应遵守严格的职业道德规范：

1. 利用大量的信息。利用现代的电子计算机系统收集、加工、整理、储存信息，为各行业提供各种各样的信息服务，如计算机中心、信息中心和咨询公司等。这使得从业人员应当严格尊重客户的隐私。
2. 软件开发与制造。从事电子计算机的研究和生产（包括相关机器的硬件制造）计算机的软件开发等活动，这要求从业人员能够敬重包括版权和专利在内的财产权。
3. 信息及时、准确、完整地传到目的地点。这要求从业人员能够重视合同、协议和指定的责任。

工程,作为一种职业但又不同于一般的职业,已经进入人们考察和研究的视野之中。工程伦理考察工程实践的社会伦理纬度,其核心是工程师的职业伦理。由于工程具有区别于其他职业的重要特征,即其对社会和人类有着重大的影响。

信息安全工程师职业作为一种特定职业，有较强的专业性和特殊性，从事信息安全职业的工作人员在职业道德方面有许多特殊的要求，但作为一名合格的信息安全工程师应该遵守以下道德规范：

1. 按照有关法律、法规和有关机关团内的内部规定建立计算机信息系统；
2. 以合法的用户身份进入计算机信息系统；
3. 在工作中尊重各类著作权人的合法权利；
4. 在收集、发布信息时尊重相关人员的名誉、隐私等合法权益；
5. 优质高效。瞄准国际前沿，掌握最新技术，勤于发明创造，满足科研需求。
6. 公正服务。坚持一视同仁，公平公正服务，尊重他人劳动，维护知识产权。

## 4.3 个人成长和职业发展的感想

实习，就是把我们在学校所学的理论知识，运用到客观实际中去，是自己所学到的理论知识有用武之地，只学不实践，那么所学的就等于零。理论就应与实践相结合。另一方面，实践更能够为以后找工作打基础。通过这段时间的实习，对平时课内所学知识进行了提炼和升华，有区别于课本有限的学习环境，运用到实际当中，收获不少。因为是学长教于我们他们的经历与知识，偏向实际运用，从中学到的东西自然与课本不一样。我们要学会从实践中学习，从学习中实践。

在一个项目开发当中，学会与项目成员相处有效沟通是第一重要的事，与他人相处，第一要真诚：你能够伪装自己的面孔，但绝不能够忽略真诚的力量。第二是激情与耐心：激情与耐心，就像火与冰，看是两种完全不同的东西，却能碰撞出最美丽的火花。第三是主动出击：当你能够选取的时候，把主动权握在自己手中，在实习期间，我会主动的协同同事工作，主动的做些力所能及的事，并会积极的寻找适宜的时间与他人交流一些生活学习以及接下来的工作的事情，遇到自己解决不了的困难我会虚心向前辈们请教，通过这些我和同事们走的很近，在实习中，他们会教我怎样做事见什么样的人说什么样的话，使我觉得获得了很多收获而且和他们相处的很愉快。第四是感受到学校和社会的距离：在学校，只有学习的氛围，毕竟学校是学习的场所，每一个学生都在为取得更高的成绩而努力。在那里是工作的场所，每个人都会为了获得更多的报酬而努力，无论是学习还是工作，都存在着竞争，在竞争中就要不断学习别人先进的地方，也要不断学习别人怎样做人，提高自己的潜力。

虽然大学生生活不像踏入社会，但总算是社会的一部分，这是不可佛人的事实。作为一个新世纪的大学生，就应懂得与社会上各方面的人交往，处理社会所发生的各方面的事情，这就意味着大学生要注意到社会实践，社会实践必不可少。毕竟，四年大学念完后，我就不再是一名大学生，是社会中的一份子了。要与社会交流。为社会做贡献。只懂得纸上谈兵是远远不及的，以后的人生旅途是漫长的，为了锻炼自己成为一名合格，对社会有用的人才，多接触社会是很有必要的。