****

**实习报告**

姓 名： 方玉昕 学 号： 20125593

学院 (系)：计算机与通信工程学院 专 业：计算机科学与技术

班 级： 2班 指导教师： 王劲松

实习名称：网络安全大数据可视化 实习时间：2015.10.08-2015.12.25

实习单位： 学院重点实验室

前言

专业实习是学生在指导老师的指导下，独立从事专业实践工作的初步尝试。其基本目的是培养学生综合运用所学的基础理论、专业知识、基本技能应对和处理问题的能力，是学生对四年所学知识和技能进行系统化、综合化运用、总结和深化的过程。通过专业实习的过程，检查学生的思维能力、创造能力、实践能力等各方面综合能力。它是学校和社会为毕业生提供的，一个很好的就业实习机会，是从理论学习到实际应用的一条纽带，对我们综合能力的培养，使得我们既能掌握专业的基本理论和基本知识，又能具有对于所学知识的运用能力以及独立工作的能力，为我们在毕业后，能顺利的走上工作岗位打下良好的基础。

通过实习我们可以获得对工作的感性知识，理论联系实际，扩大知识面；同时专业实习又是锻炼和培养学生业务能力及素质的重要渠道，培养当代大学生具有吃苦耐劳的精神，也是学生接触社会、了解产业状况、了解国情的一个重要途径，逐步实现由学生到社会的转变，培养我们初步担任技术工作的能力、初步了解企业管理的基本方法和技能；体验企业工作的内容和方法。这些实际知识，对我们学习后面的课程乃至以后的工作，都是十分必要的。

我们在实习中不仅要综合运用四年所学知识和技能，将理论与实践结合融会贯通，提升自己发现问题、解决问题的能力；也要注重人际交往、与人沟通的能力。为即将到来的校园招聘提高自己的竞争力，也为将来的职场生活提升个人综合素质和能力。

1. 实习目的

训练从事计算机专业技术工作所必须的各种基本知识和实践能力；了解专业在企业内应用现状、存在的问题和应用前景。了解业务范围内的运用生产与应用方法、信息组织形式、软件开发过程及常用技术方法。培养学生理论结合实际，从实际出发，发现问题分析问题和提出解决方法的能力，将理论与实践相结合，在实践中提高能力。通过实习，可以进一步巩固和深化所学的理论知识，弥补理论教学的不足，以提高教学质量。训练学生从事专业技术工作及管理工作所必须的各种基本技能和实践动手能力。综合性地训练学生对项目开发进度的控制能力，对程序的开发、编写能力，以及对问题的处理能力。通过该题目，可以充分了解开发工具的使用，锻炼独立处理问题的能力，将是对学生四年来所学知识的综合测评及训练。培养学生将来从事相关专业的应用、开发所具备的沟通能力，团结协作的素养。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。 网络安全从其本质上来讲就是网络上的信息安全。当今无论是中小企业还是大企业，都广泛使用信息技术，特别是网络技术，以不断提高企业竞争力。企业信息设施在提高企业效益和方便企业管理的同时，也给企业带来了安全隐患。网络的安全问题一直困扰着企业的发展，给企业所造成的损失不可估量。由于计算机网络特有的开放性，网络安全问题日益严重。

基于网络安全问题日益严重的现状，我们观察到目前众多的安全研究者与厂商之间存在着天生的不平等，不尊重。对于漏洞发现者来说，由于缺乏厂商的联系方式，即使发现了漏洞也很难将信息传递给厂商，而厂商也根本无法顾及散落在互联网各地的漏洞信息，最终导致一些漏洞被人遗忘，未得到修复而造成损失。另外一方面，一些厂商对漏洞研究者的报告也很不尊重，甚至是一种轻视的态度，在出现问题之后对问题不是迅速修复以确保互联网用户的安全而是通过其他手段尝试掩盖漏洞甚至是否认漏洞的存在，在这种不尊重的前提下，漏洞研究者就可能直接将漏洞公开，直接损害了厂商的利益。破坏和建设一样，同样作为一种技术的存在，我们尝试唤回大家对技术的尊重，漏洞报告与预警平台将跟踪漏洞的报告情况，所有跟技术有关的细节都会对外公开。

1. 实习时间

2015年10月8日 至 2015年12月25日

1. 实习单位、部门及其简介

学院重点实验室，指导老师为王劲松老师，主要研究方向为网络安全及大数据。

1. 实习内容

实习方向为网络安全方向，具体内容为漏洞报告及预警平台。

在网络飞速发展的当代社会，互联网渗透到人们生活的各个方面。信息的严重不对称，导致安全性很难得到改善。而且大多数公司内部的系统管理员与安全人员没有来自行业与内部的竞争压力，生搬硬套国外的标准做安全管理，工作效率低下、不负责任。漏洞越来越多，最终的结果是用户将会为这些安全问题付出代价。

因此漏洞报告和预警平台就十分必要的，平台可以将白帽子和厂商联系起来，让厂商可以及时发现和修复问题。

平台上积累的真实漏洞，可供技术人员在开发产品时参考，不犯别人犯过的错误。并且提供了大量的案例与安全知识，供大家浏览、了解、学习网络安全相关知识，帮助大家提高安全意识。

而且在平台上不局限于传统意义上的产品漏洞，包括网络配置，服务器管理，钓鱼欺诈甚至是有证据的黑客事件都被算作厂商的漏洞。

漏洞报告及预警平台的开发预计使用Sublime Text3作为开发工具，Grunt作为前端代码构建工具,综合运用HTML、CSS、LESS、JavaScript、jQuery等技术，基于express框架使用Node.js进行服务器端的开发，echarts作为图标展示框架。综合性地训练学生对项目开发进度的控制能力，对程序的开发、编写能力，以及对问题的处理能力。

Sublime Text 是一个代码编辑器，也是HTML和散文先进的文本编辑器。是目前业界主流前端开发编辑器，体积较小，运行速度快而且文本功能强大，并且支持编译功能且可在控制台看到输出，内嵌python解释器支持插件开发以达到可扩展目的，而且支持对大量插件的管理。

Grunt是前端构建工具。对于需要反复重复的任务，例如压缩、编译、单元测试等，自动化工具可以减轻我们的劳动，简化重复的工作。我们只需要在 Gruntfile 文件正确配置好任务，任务运行器就会自动完成这些工作。

LESS是一种动态样式语言，属于CSS预处理语言的一种，它使用类似CSS的语法，为CSS的赋予了动态语言的特性，如变量、继承、运算、函数等，更方便CSS的编写和维护。

jQuery是是轻量级免费、开源的js库，它兼容CSS3，还兼容各种浏览器。jQuery使用户能更方便地处理HTML、events、实现动画效果，并且方便地为网站提供AJAX交互。

Node.js是一个基于Chrome JavaScript运行时建立的平台， 用于方便地搭建响应速度快、易于扩展的网络应用。Node.js 使用事件驱动， 非阻塞I/O 模型而得以轻量和高效，非常适合在分布式设备上运行的数据密集型的实时应用。

Express是基于 Node.js 平台，快速、开放、极简的 web 开发框架，它提供一系列强大的特性，帮助我们创建各种 Web 和移动设备应用。而且Express 不对 Node.js 已有的特性进行二次抽象，我们只是在它之上扩展了 Web 应用所需的基本功能。

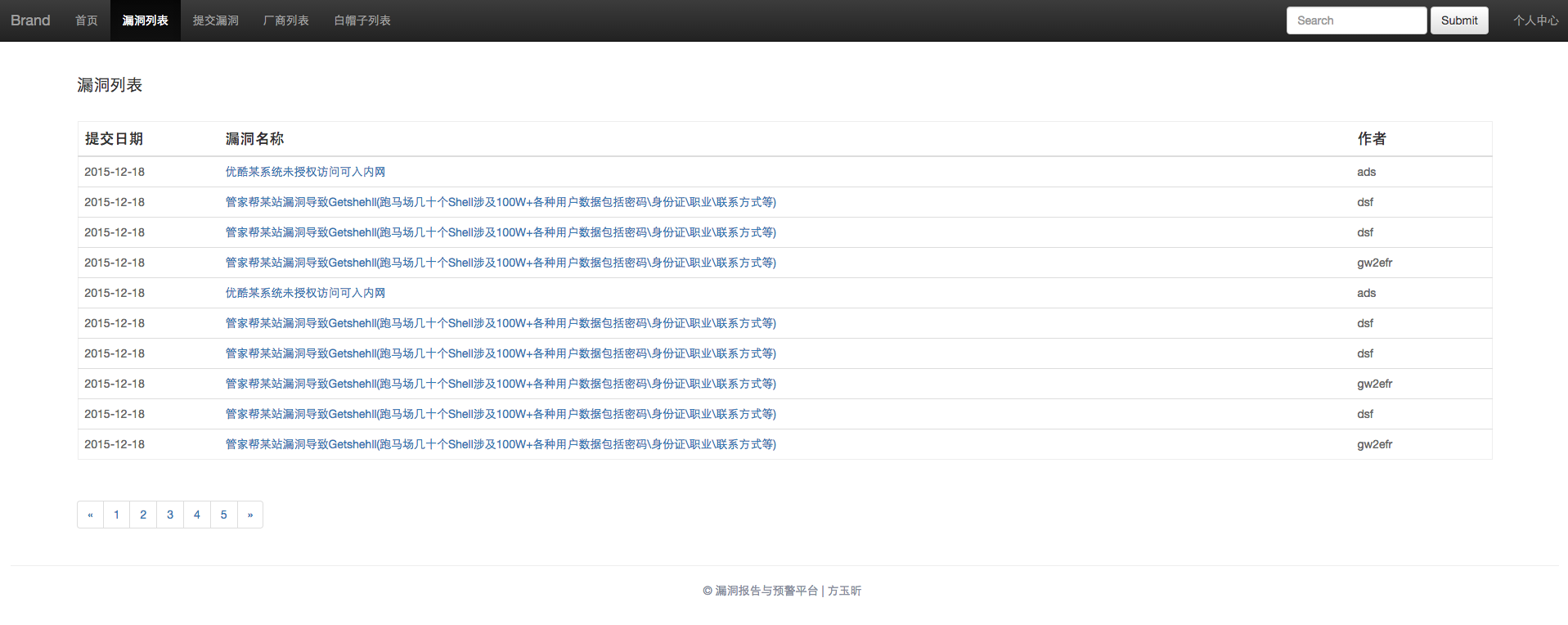
平台包括首页、导航栏、漏洞列表、漏洞信息、提交漏洞、厂商列表、白帽子列表几个模块，下面来分别介绍每个模块的功能。

首页也是平台的欢迎页，采用轮播图的方式展示各个模块的功能，可以通过点选某张图片直接进入到图片对应的功能。

导航栏最左侧展示平台的Logo，然后左侧有首页、漏洞列表、提交漏洞、厂商列表、白帽子列表几个标签，点击可以进入相应模块。右侧有登录或注册，登录后显示为个人中心。



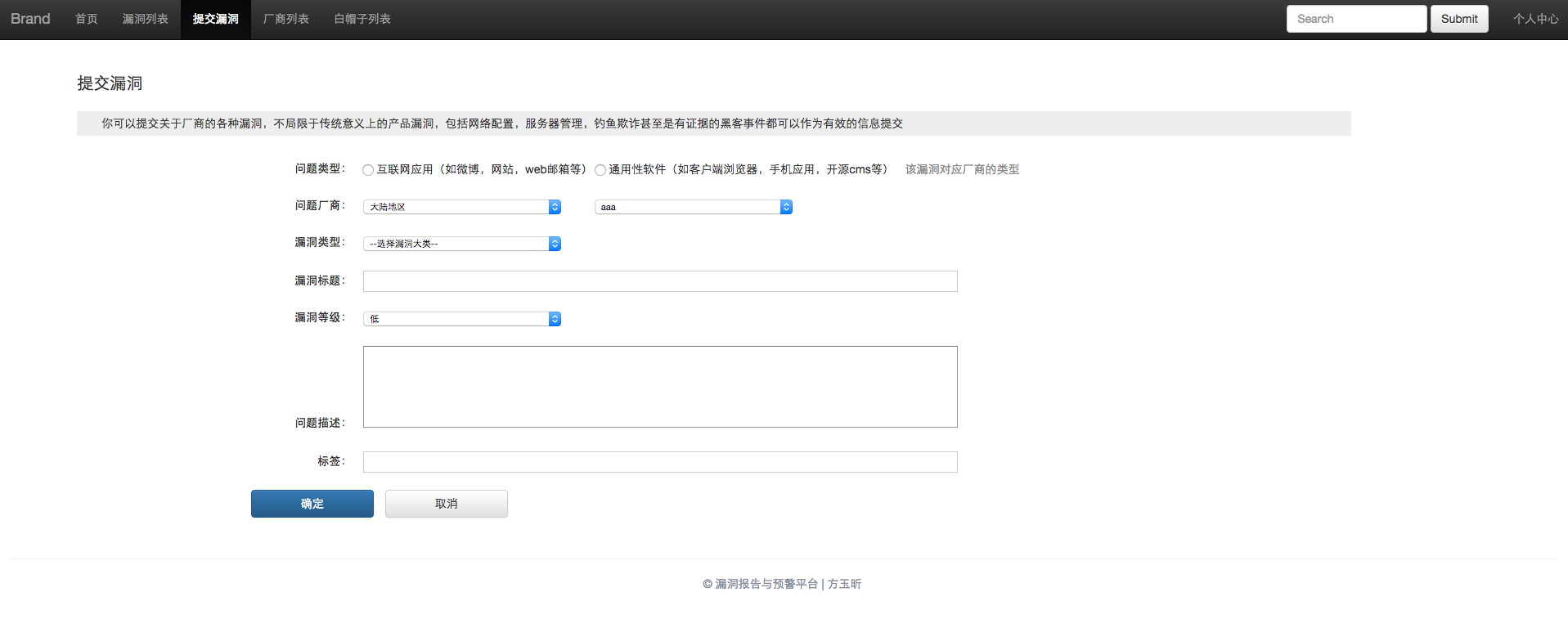
漏洞列表页展示漏洞的提交日期、漏洞名称和作者，下方展示分页功能，每十条漏洞展示为一页。选择列表中其中一条漏洞，点击可进入所选漏洞的漏洞信息页。



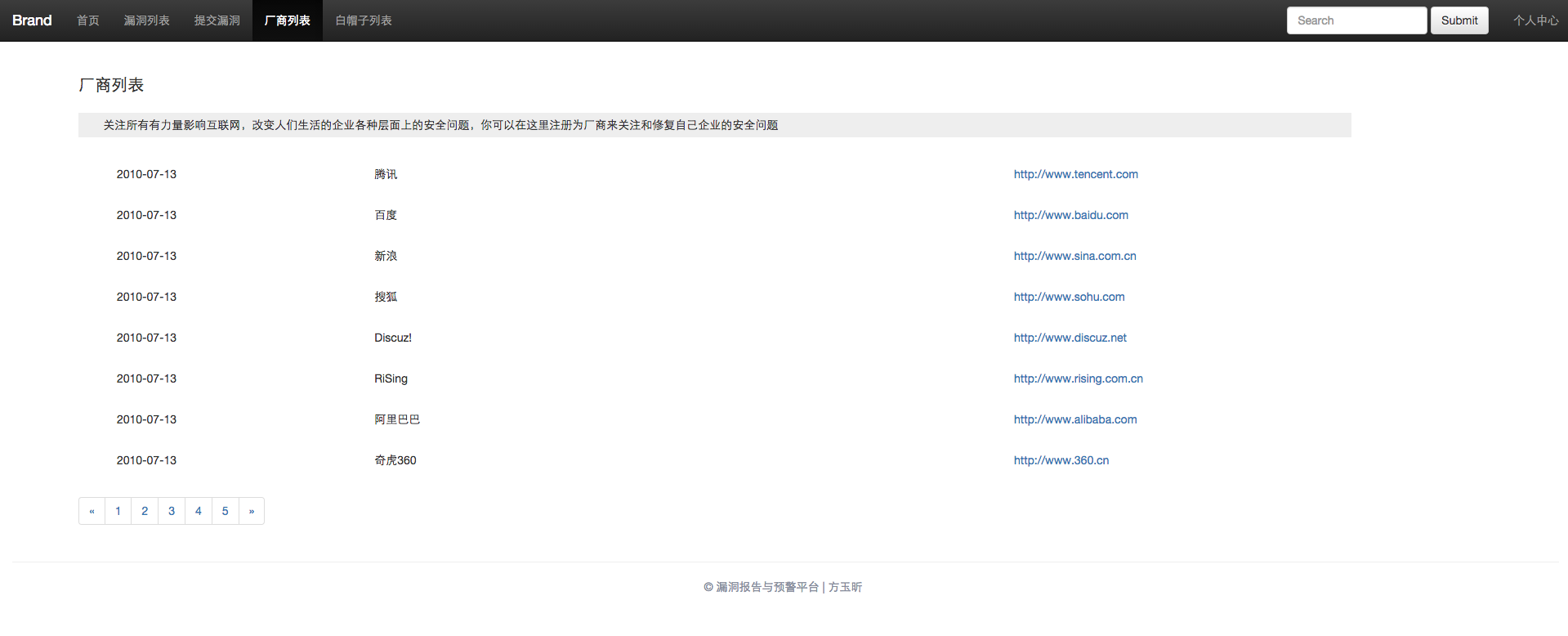
漏洞信息页包括漏洞概要、漏洞详情、漏洞回应及评论，四个部分。漏洞概要展示漏洞的缺陷编号、漏洞标题、相关厂商、漏洞作者、提交时间、公开时间、漏洞类型、危害等级、漏洞状态、漏洞来源、Tags标签几项内容；漏洞详情包括披露状态、简要描述、漏洞hash和版权声明；漏洞回应是漏洞相关厂商对漏洞的回应，对应时间表明漏洞检查状态和对漏洞相应的解释回应；评论为登录用户对漏洞可以发表评论留言，未登录游客在评论去会看到跳转至登录的标签。



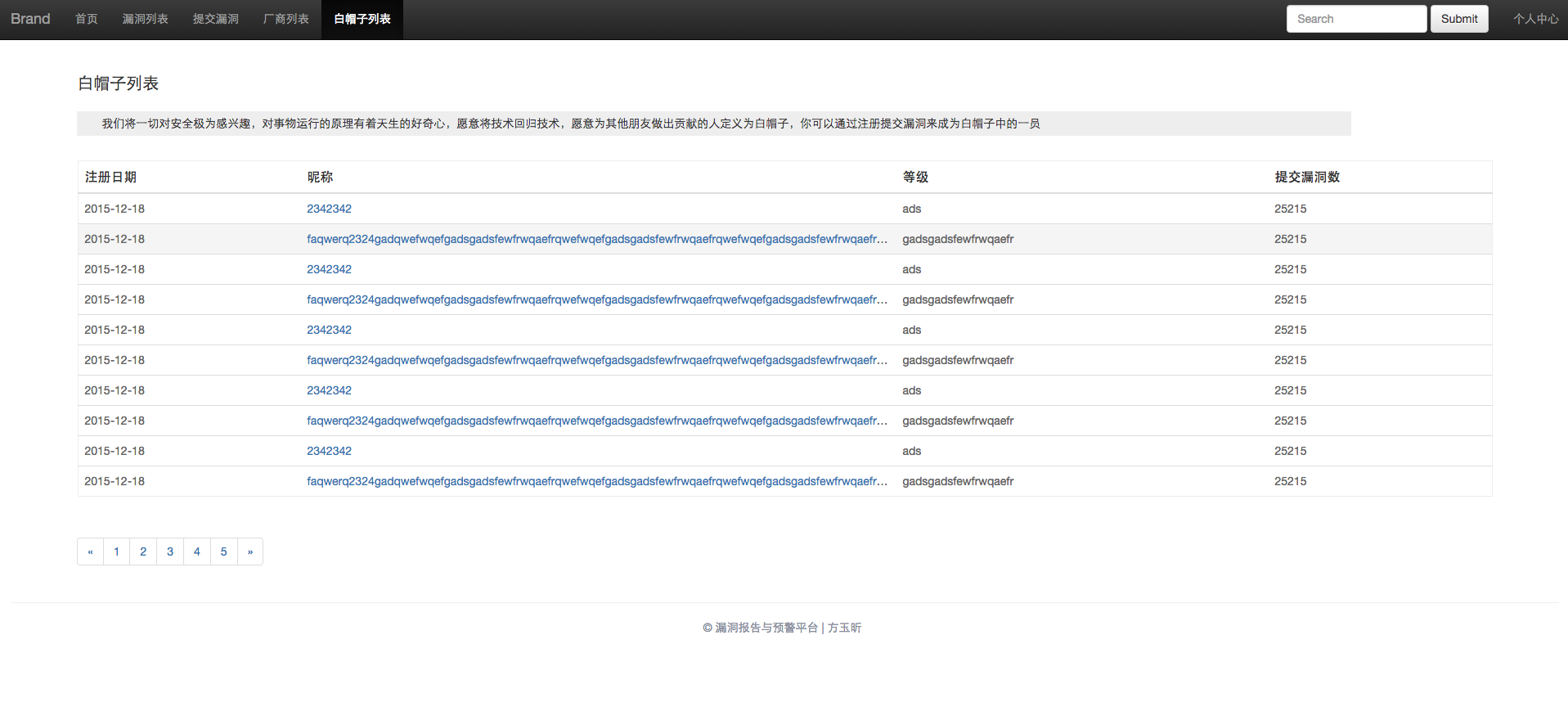
提交漏洞是登录用户发现漏洞后提交到平台的模块，用户可以提交关于厂商的各种漏洞，不局限于传统意义上的产品漏洞，包括网络配置，服务器管理，钓鱼欺诈甚至是有证据的黑客事件都可以作为有效的信息提交。提交信息中问题类型对应厂商的类型，选择问题厂商、漏洞类型，填写漏洞标题，确定漏洞等级，填写问题描述，添加标签。平台涉及到的漏洞类型包括网络边界或基础架构类型、系统运维或服务设置类型、应用程序或应用漏洞、业务安全或运营风险、安全事件或安全情报五个大类型。网络边界或基础架构类型，包含网络设计缺陷或逻辑错误、基础设施弱口令、网络未授权访问和网络敏感信息泄漏四种情况；系统运维或服务设置类型，包含系统或服务补丁不及时、重要敏感信息泄露、未授权访问或权限绕过、服务弱口令、系统或服务运维配置不当五种情况；应用程序或应用漏洞类型，包含xss跨站脚本攻击、SQL注射漏洞、CSRF、任意文件遍历或下载、文件上传导致任意代码执行、文件包含、命令执行、应用配置错误、敏感信息泄露、未授权访问或权限绕过、后台弱口令、设计缺陷或逻辑错误、URL跳转十三种情况；业务安全或运营风险类型，包含钓鱼欺诈信息、账户体系控制不严、内容安全、恶意信息传播四种情况；安全事件或安全情报类型，包含内部绝密信息泄漏、用户资料大量泄漏、成功的入侵事件三种情况。



厂商列表页是提交漏洞中提过的厂商以及在平台注册过的厂商。包含注册时间、厂商名称、官网网址。下方有翻页键，每十条信息占一页。



白帽子列表页是在平台注册的用户列表，按照等级和提交漏洞数排序。我们将一切对安全极为感兴趣，对事物运行的原理有着天生的好奇心，愿意将技术回归技术，愿意为其他朋友做出贡献的人定义为白帽子，游客可以通过注册提交漏洞来成为白帽子中的一员。列表处显示注册日期、昵称、等级及提交漏洞数。



1. 实习总结

在学校中我们只能学到书本上的知识，很少有机会到实地锻炼自己的能力，在十二周的实习中我掌握了许多书本上学不到的内容。

实习时间虽短，但我们在有限的时间里对如何完成完整Web开发的问题，将所学的知识与实际问题相结合，学习到了在实际问题中该怎样应用自己的知识。同时，在实习老师的讲解中，使得学习变的更加的轻松简单，这对以后的专业的学习有很大的帮助。

在开发Web版漏洞报告及预警平台的过程中使用Sublime Text3作为开发工具，调研FIS、Grunt、Gulp、Webpack等前端代码构建工具,综合运用HTML、CSS、LESS、JavaScript、jQuery等技术，熟悉基于express框架使用Node.js进行服务器端的开发，并且尝试图表展示框架Echarts、Highcharts等。各种课内课外的知识交叉综合运用，调研各种前端新技术。同时经过实习我增强了自己的网络安全意识，了解了许多安全类知识，让我受益匪浅。

作为一名即将步入工作岗位的大四学生来说，发现问题解决问题的能力、团队合作能力与他人沟通的能力都是不可或缺的素质，这次实习对我们来说是一次非常难得的积累经验掌握专业技能的机会，这为我们以后毕业工作打下了坚实的基础。