zzcms 8.3 CVE漏洞分析

venture / 2018-09-21 11:47:18 / 浏览数 3449 技术文章 技术文章 顶(1) 踩(1)

---

zzcms 8.3 CVE漏洞分析

前言:

zzcms之前在8.2版本是就爆出过不少问题，本文对zzcms8.3版本已爆出过的CVE漏洞进行分析复现，这套CMS也很适合刚入坑的代码审计小伙伴们练习。跟着师傅们学习一

- SQL注入

CVE-2018-17136

问题文件： /zzcms8.3/user/check.php

漏洞分析

这是一个在8.2版本就存在的SQL注入漏洞，在check.php的19行，存在问题的原因是因为在SQL语句中使用了getip方法获取用户IP。

跟进getip方法，在inc/function.php 的100行

可以看到这里并没有对IP进行判断或过滤，可以在http头添加client-ip对IP进行伪造，导致了SQL注入

漏洞复现

该漏洞存在于所有包含了check.php的页面，由于没有直接回显，可以通过盲注或利用DNSlog带出。而cve里师傅提供了一个很好的利用点在/user/manage.php，该页面包
`database())`，然后直接在表单中回显出来。

CVE-2018-14961

问题文件： /zzcms8.3/dl/dl_sendmail.php

漏洞分析

在dl_sendmail.php的42到45行，将POST方法接受到的SQL内容拼接另一段SQL语句然后执行。本来进行了全局过滤，但是这里使用了stripfxg方法处理收到的SQL内容。这

strpfxg方法将传来的字符串中添加的反斜杠去除，如果参数`$htmlspecialchars_decode`为true会把html实体符号解码，这就将原本全句过滤的语句还原为正常数据，如

这导致在最后拼接后，SQL语句相当于没有进行任何过滤。

漏洞复现

思路很清晰，直接POSTSQL语句

CVE-2018-1000653

问题文件： /zzcms8.3/zt/top.php

漏洞分析

在top.php的3到6行，使用了`$_SERVER['HTTP_HOST']`获取域名，并直接拼接到SQL语句，而\$_SERVER是不在cms的全局过滤范围里的，所以如果可以控制host就可以

漏洞复现

在/zt/job.php包含了top.php,可以在job.php进行注入。

由于没有回显，采用盲注或DNSlog带出数据。简单说一下DNSlog,对于SQL注入,一些注入都是无回显的，我们可以通过布尔或者时间盲注获取内容，但是整个过程效率低，

两个好用的免费dnslog平台：http://ceye.io/ http://dnsbin.zhack.ca

- 储存XSS

CVE-2018-14962

问题文件： /zzcms8.3/zt/show.php

漏洞分析

这又是一个stripfxg使用不当造成的漏洞，在/zt/show.php中对变量$content
直接进行输出，并使用了stripfxg方法，之前说到过，这个方法能将转义过滤后的数据还原，这样的话又是相当于没有过滤，只需找到变量输入点即可造成xss漏洞。

而在/user/manage.php的58到60行，这里有更新表数据的操作，这里将$content写进数据库中

漏洞复现

在/user/manage.php点击源码写入paylaod

然后访问`http://www.zzcms3.test/zt/show.php?id=1`或`http://www.zzcms3.test/zt/companyshow.php?id=1`就可以触发漏洞

- 任意文件删除

CVE-2018-13056 CVE-2018-16344

关于任意文件删除漏洞，在这套CMS里很经典，爆出过很过多，思路大都相同。文件删除漏洞可以配合之前爆出过的安装漏洞(CVE-2018-8966)直接getshell。

漏洞分析

首先看CVE-2018-13056

问题文件： /zzcms8.3/user/del.php

漏洞位置在del.php的55到69行，思路比较清晰，首先需要传入tablename令其值为zzcms_main进入分支语句，然后执行SQL语句查询zzcms_main的img,flv,editor的值，

而在/user/zssave.php中可以添加

CVE-2018-16344是差不多相同的思路，但是这里上传视频功能需要管理员去开启才可以。

实际上这样的漏洞还存在于这套CMS的很多地方，比如user/manage.php等

漏洞复现

在/user/zssave.php上传图片，点击发布信息抓包，修改img=/install/insall.lock

然后访问/user/del.php

删除成功显示重装了

- CSRF

CVE-2018-14963

问题文件： /zzcms8.3/admin/adminadd.php

漏洞分析

常见的CSRF攻击利用方式，由于管理后台设计敏感操作的表单没有设置token，导致可以使用CSRF去添加管理员

漏洞复现

POC:

```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
   <form action="http://192.168.224.138/admin/adminadd.php?action=add" method="POST">
     <input type="hidden" name="groupid" value="1" />
     <input type="hidden" name="admins" value="123" />
     <input type="hidden" name="passs" value="123" />
     <input type="hidden" name="passs2" value="123" />
     <input type="submit" value="Submit request" />
   </form>
 </body>
</html>
```

只需诱导管理员点击构造好的恶意页面，即可添加管理员

参考资料

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17136
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14961
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000653

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14962
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13056
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16344
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14963

点击收藏 | 1 关注 | 2

上一篇：利用动态二进制加密实现新型一句话木... 下一篇：蓝鲸安全CTF打卡题——第一期密码学

1. 4 条回复

laura_小狮子 2018-09-21 11:57:44

哇，zzcms 8.3 CVE全家福，享用了~

0 回复Ta

155****3579 2018-09-21 15:39:59

师傅这篇和我写的很像哦~ zzcms 8.3 最新CVE漏洞分析
zzcms 8.3 任意文件删除漏洞深入思考

0 回复Ta

venture 2018-09-21 16:47:20

@155****3579 师傅很巧哦~但是内容不一样的哦~欢迎师傅交流

0 回复Ta


lz1y 2018-09-22 00:12:02

删除文件还有好多！全都是鉴权后没有exit，然后直接前台就可以删除，另外还有一个稍微复杂一丢丢得sql注入：https://gist.github.com/Lz1y/31595b060cd6a0318

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板