MyBB <= 1.8.20: From Stored XSS to RCE

cru**** / 2019-06-20 08:40:00 / 浏览数 5601 安全技术 漏洞分析 顶(0) 踩(0)

---

这篇文章展示了在MyBB 1.8.21 版本之前，攻击者能够通过向管理员发送恶意私信或者创建一个恶意帖子来接管任意托管主机

MyBB是一个开源论坛软件，软件地址：https://mybb.com/

## 影响

我们发现，由于在1.8.20■■■■■■对于所发帖子和私信的解析错误而产生的一个存储性XSS，同时还有一个绕过身份认证的RCE漏洞能够被论坛管理员利用

攻击者仅需一个目标论坛的账号，然后向管理员发送一封包含恶意JS代码（用于利用RCE漏洞）的私信。只要同时一名后端管理员打开恶意的私信，这使得攻击者可以完全接

这使攻击者能够完全访问存储在主机数据库中的所有用户帐户、私有主题和消息。

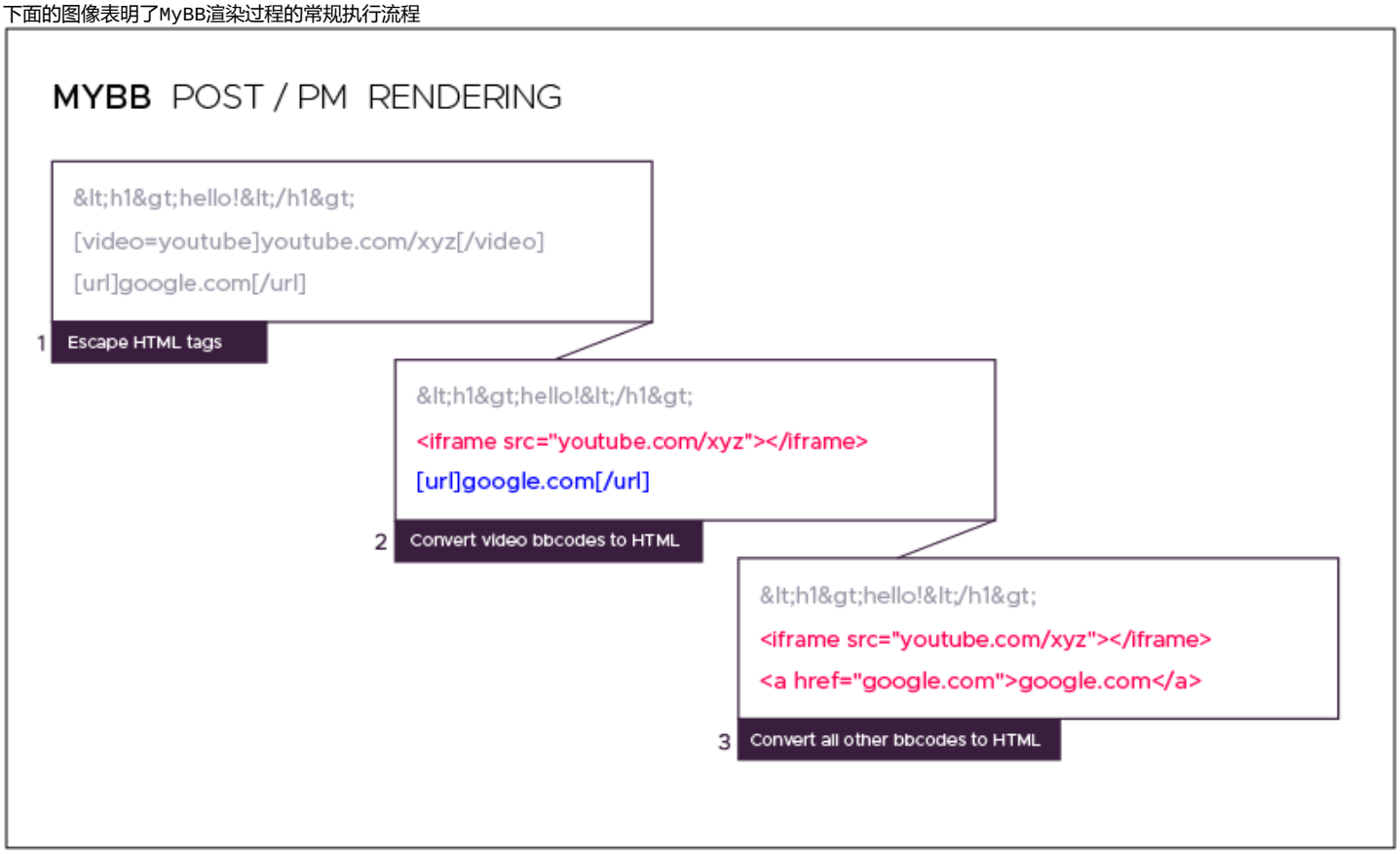
## 技术分析

下面，我们分析了使用RIPS代码分析检测到的安全漏洞。

## bbcode的存储性xss

MyBB利用3个步骤解析和渲染主题，帖子和私信。这一过程的目的是消除用户输入的恶意代码并呈现所谓的mycodes或bbcodes。Bbcodes方便论坛用户在帖子中去嵌入图

下面的图像表明了MyBB渲染过程的常规执行流程




该过程首先简单地转义所有HTML标记和双引号。然后，它会将所有[video] mycodes转换为嵌入视频的<iframe>标签。
例如，YouTube上。视频bbcodes在一个步骤中呈现的原因是管理员可以禁用它们（默认情况下启用它们）。
最后，它会将所有其他mycode（例如[url]，[quote]和[email]）转换为HTML标记。

事实上，与其他bbcodes转换方式不同，[video]bbcodes被转换为html标记的方式引导我们产生了一个想法：即可能可以制作一个[video]bbcode，其结果是html标记

```
<iframe src="youtube.com/xyz[url]http://onload=evilCode()[/url]"></iframe>
```

其想法是MyBB随后将用更多包含双引号（“）的HTML标记替换iframe的src中的[url]bbcode，从而损坏HTML并导致属性注入。

上述例子在第三步处理后将会导致产生以下的html标记：

```
<iframe src="youtube.com/xyz<a href="http://onload=evilCode()">.."></iframe>
```

可以看到，iframe的src属性随后由injected href属性和它的引号关闭。这将导致onload事件处理程序被注入到<iframe>html标记中。

通常，不可能在其他bbcode中注入bbcode，因为regex过滤器已经到位，可以防止此类攻击。但是，负责呈现[video]bbcodes的回调方法调用应嵌入视频（例如youtub

inc/class_parser.php

```
1385  function mycode_parse_video($video, $url)
1386  {
1387      global $templates;
1388
1389      if(empty($video) || empty($url))
1390          return "[video={$video}]{$url}[/video]";
1391
1392      $parsed_url = @parse_url(urldecode($url));
1393
1394      // [...]
```

事实上被urldecode的视频URL允许绕过正则保护并通过URL编码注入[url]bbcode，如上所述。然后，这会导致将onload事件处理程序注入<iframe>标记。一旦ifram

## 通过文件写入利用管理面板中的RCE

MyBB论坛的管理员可以在管理面板中管理其安装的活动主题的样式表。他们还可以在服务器上创建新的样式表文件并选择文件名。

如果管理员帐户角色的攻击者可以简单地创建新的样式表文件并将其称为shell.php，则会出现明显的文件写入漏洞。
但是，对此功能背后的源代码进行快速调查后发现，只允许使用.css文件扩展名：

admin/inc/functions_themes.php

```
263  foreach($theme['stylesheets']['stylesheet'] as $stylesheet) {
264      if(substr($stylesheet['attributes']['name'], -4) != ".css"){
265          continue;
```

引起我们注意的是扩展检查后发生的事情。MyBB不是简单地在文件系统中创建样式表文件，而是首先存储样式表文件的名称，以及为启动MySQL的数据库中的内容。当我

Table definition of mybb_themestylesheets

```
MariaDB [mybb]> DESC mybb_themestylesheets;
+--------------+----------------------+------+-----+---------+----------------+
| Field        | Type                 | Null | Key | Default | Extra          |
+--------------+----------------------+------+-----+---------+----------------+
| sid          | int(10) unsigned     | NO   | PRI | NULL    | auto_increment |
| name         | varchar(30)          | NO   |     |         |                |
  [...]
| stylesheet   | longtext             | NO   |     | NULL    |                |
  [...]
+--------------+----------------------+------+-----+---------+----------------+
```

然后我们注意到，当通过XML文件导入时，样式表文件名的长度不会被检查，从而导致攻击者能够欺骗MyBB插入超过允许30个字符的文件名。MySQL在许多系统上的默认

攻击者可以通过将文件名设置为例如aaaaaaaaaaaaaaaaaaaaa.php.css来滥用此行为。这个文件名有34个字符。因为它以.css扩展名结尾，所以它通过了mybb的安全

然后，攻击者可以使用管理面板生成新导入的样式表文件并将其写入文件系统。这将在缓存目录中创建一个php shell。

## 时间线

| 时间 | 事件 |
| --- | --- |
| 2019/04/29 | 向MyBB团队私下报告了多个漏洞。 |
| 2019/04/29 | MyBB承认这些漏洞。 |
| 2019/06/10 | MyBB发布1.8.21版，其中包含针对漏洞的补丁。 |

## 总结

这篇博客文章详细描述了一个漏洞链，它可以被滥用来接管在1.8.21版本之前运行mybb的任何论坛。攻击者可能滥用了XSS漏洞来接管目标论坛上的任何论坛帐户，或者通

reference：
利用视频：https://blog.ripstech.com/videos/mybb-stored-xss-to-rce.mp4
原文：https://blog.ripstech.com/2019/mybb-stored-xss-to-rce/


上一篇：EMOTET深度分析 下一篇：初探漏洞挖掘基础
1. 1 条回复


suolong 2019-06-21 17:19:08

利用数据库字段的特性绕过过滤真香

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