你真的了解HTTP协议吗

salt

关于我

- CTF退役选手
- Web狗

关于玄武实验室

- @tombkeeper

- 浏览器安全
- windows 安全
- IOT 安全
- 安卓
- web

关于玄武实验室

- BadBarcode
- BadTunnel
- 应用克隆
- Wombie Attack
- SamsungPay
- pwn2own 2017

...

关于玄武实验室

- @**腾讯玄武实验室**
- 微信公众号 XuanwuLab
- Twitter @XuanwuLab

- https://xlab.tencent.com/
- xlab@tencent.com

目录

- HTTP 请求头
- HTTP 响应头
- URI

HTTP

```
GET / HTTP/1.1
Host: 5alt.me
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS
X 10.12; rv:61.0) Gecko/20100101 Firefox/61.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-
US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
HTTP/1.1 200 OK
server: GitHub.com
content-type: text/html; charset=utf-8
last-modified: Wed, 01 Aug 2018 15:14:23 GMT
access-control-allow-origin: *
expires: Sat, 11 Aug 2018 15:11:34 GMT
cache-control: max-age=600
content-encoding: gzip
content-length: 9918
```


https://zh.wikipedia.org/wiki/HTTP%E5%A4%B4%E5%AD%97%E6%AE%B5

HTTP

- 往端口发送字符串
- \r\n分隔（CRLF）

WebServer

- Apache
- Nginx

- nodejs/python/java

WebServer的运行方式

- Apache
  - 默认prefork mode
  - 同一个连接用同一个进程处理
  - mod_php
- Nginx
  - event-driven
  - 同一个连接请求用不同线程处理
  - php-fpm
- 反向代理

php disabled functions绕过

- /proc/self/mem
- 修改got
- 命令执行！

https://rdot.org/forum/showthread.php?t=3309

HTTP请求头

- Authorization
- Cookie
- Host
- Referer
- User-Agent
- X-Forwarded-For

X-Forwarded-For

- 很多程序员用X-Forwarded-For来获取用户IP
- 在HTTP请求头中可以伪造

- 使用X-Forwarded-For来获取用户IP是否一定有问题？

反向代理

```
location / {
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $remote_addr;

        proxy_pass http://localhost:8000;
        proxy_redirect off;
}
```

HTTP响应头

- Access-Control-Allow-Origin
- Location
- Set-Cookie
- X-XSS-Protection
- Content-Security-Policy
- X-Powered-By

X-XSS-Protection

- X-XSS-Protection: 0
- X-XSS-Protection: 1
  - 浏览器默认
  - 自动去除有问题的部分
- X-XSS-Protection: 1; mode=block
  - 阻止页面渲染

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

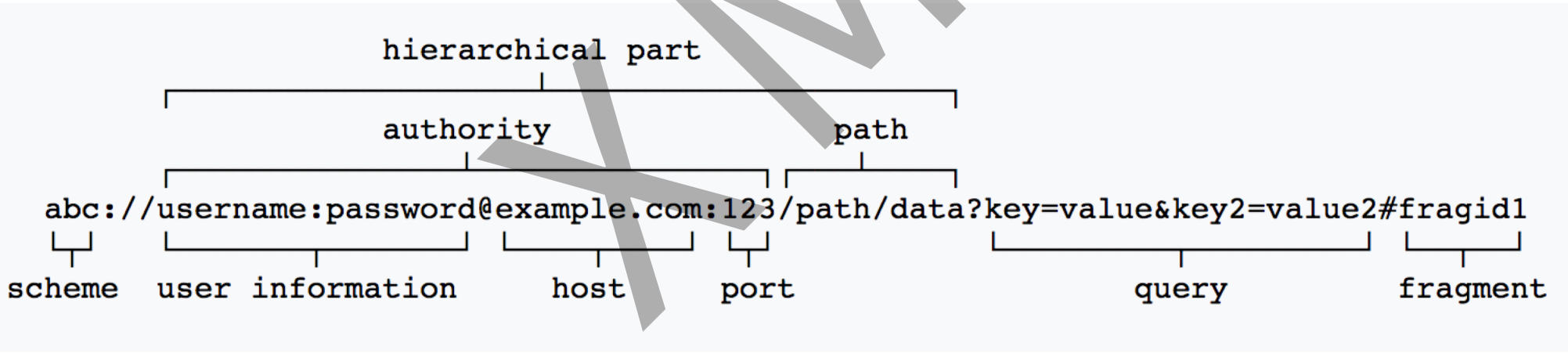
X-XSS-Protection: 1

- <script src=waf.js></script>
- /?xxx=<script src=waf.js></script>

URI

- Uniform Resource Identifier,统一资源标识符

scheme:[//[user[:password]@]host[:port]]
[/path][?query][#fragment]



https://zh.wikipedia.org/wiki/%E7%BB%9F%E4%B8%80%E8%B5%84%E6%BA%90%E6%A0%87%E5%BF%97%E7%AC%A6

scheme

- http, https, ftp
- file, gopher, php, zip （server-side）
- data, javascript （client-side）
  - data:,123 data:;base64,MTIzCg== data:text/plain;base64,MTIzCg==
  - javascript://www.qq.com/%0aalert(1)
- qqbrowser, weixin, chrome, ed2k （app）

Electron 远程命令执行漏洞

- 基于electron构建的app登记了协议，即可以使用该协议直接打开应用程序
- 打开恶意页面就能被入侵

```
someapp://?" "--no-sandbox" "--gpu-launcher=cmd.exe /c start calc
```


https://xz.aliyun.com/t/1990

漏洞原因

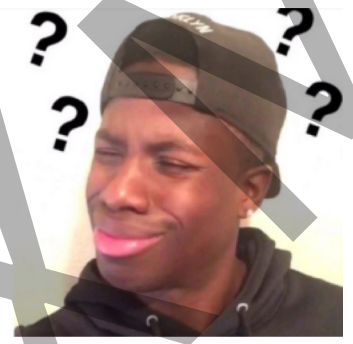
- 在注册表中登记为协议处理程序 "someapp.exe" "%1"
- 使用 Electron 框架创建的程序有其他参数可以执行命令

someapp://?" "--no-sandbox" "--gpu-launcher=cmd.exe /c start calc

someapp.exe "someapp://?" "--no-sandbox" "--gpu-launcher=cmd.exe /c start calc"

://

scheme:[//[user[:password]@]host[:port]]
[/path][?query][#fragment]



://

测试payload	浏览器(location, 基础页面为 http://www.test.com/test/)	浏览器(location, 基础页面为 https://www.test.com/test/)
http:5alt.me	http://www.test.com/test/5alt.me	http://5alt.me
http:/5alt.me	http://www.test.com/5alt.me	http://5alt.me
http:\5alt.me	http://www.test.com/5alt.me	http://5alt.me
/5alt.me	http://www.test.com/5alt.me	https://www.test.com/5alt.me
//5alt.me	http://5alt.me	https://5alt.me
\\5alt.me	http://5alt.me (osx下)	https://5alt.me (osx下)

具体场景需要具体测试和分析

Php? Python? curl?

认证部分

scheme:[//[user[:password]@]host[:port]]
[/path][?query][#fragment]

认证部分

- 用于绕过某些判断
  - url.startswith('http://www.qq.com')
- 用于自动认证
  - HTTP Basic Auth
  - 通常用于路由器自动登录

https://xlab.tencent.com/cn/2018/01/05/a-new-way-to-exploit-cve-2017-17215/

host

- 域名
- ip
- intranet domain

域名

- 自动修正
  - 5alt。me -> 5alt.me
  - CRLF（DNS解析容错）
- 判断绕过
  - url.startswith('http://www.qq.com')
  - 指向内网ip
- DNS Rebind
- homograph attack
  - http://exαmple.com/

ip

- 127.0.0.1
- 八进制：017700000001
- 十进制：2130706433
- 十六进制：0x7F000001

  - Curl 0
  - Curl 127.1

http://ip.chacuo.net/ipcalc

端口

- 用http请求其他端口
  - redis（容错机制）
- 一些限制绕过
  - 火狐下crlf->xss

https://www.leavesongs.com/PENETRATION/bottle-crlf-cve-2016-9964.html

path

- http://127.0.0.1/http/path.php?x=x
- http://127.0.0.1/http/path.php/xxxx?x=x
- http://127.0.0.1/http/path.jpg/a.php

nginx配置问题+php fix_pathinfo

```
1.location ~ \.php($|/) {
2.      fastcgi_pass 127.0.0.1:9000;
3.      fastcgi_index index.php;
4.
5.      set $script $uri;
6.      set $path_info "";
7.      if ($uri ~ "^(.+\.php)(/.*)") {
8.           set $script $1;
9.           set $path_info $2;
10.      }
11.
12.      include fastcgi_params;
13.      fastcgi_param SCRIPT_FILENAME
$document_root$script;
14.      fastcgi_param SCRIPT_NAME $script;
15.      fastcgi_param PATH_INFO $path_info;
16.}
```


http://www.laruence.com/2010/05/20/1495.html

php fix_pathinfo

- http://127.0.0.1/http/path.jpg/a.php
  - nginx: $script -> http/path.jpg/a.php
  - php: SCRIPT_FILENAME -> http/path.jpg
- 上传图片getshell

nginx off-by-slash fail

```
location /static {
    alias /home/app/static/;
}
```

http://target/assets../ ? ? ?

http://target/assets../settings.py

proxy+java

http://example.com/foo;name=orange/bar/

Apache/Nginx: /foo;name=orange/bar/

Tomcat/Jetty: /foo/bar/

http://example.com/portal/..;/manager/html ???

http://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf

query

- a=1&b=2
- a=1&a=2
  - 覆盖
  - 数组
- a[]=1&a[]=2

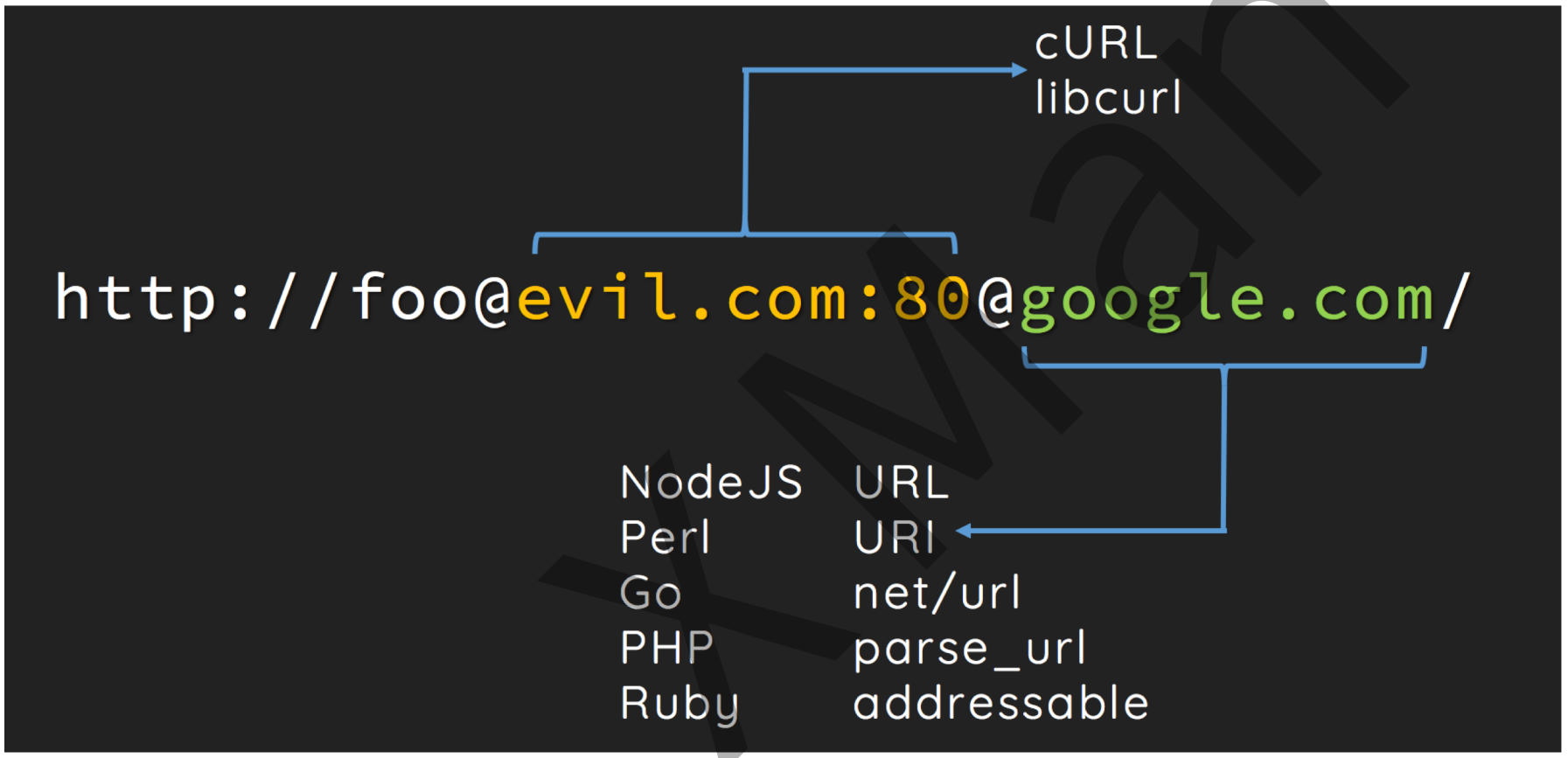
urlencode

- 特殊含义的字符
  - : / ? # [ ] @ & = + ;
  - +会变成空格
    - base64 ???
- 特殊字符
  - php中key中的空格和点号'.'会被替换成下划线'_'
  - CodeIgniter 框架把value中无法打印的字符替换成空
    - waf绕过

Fregment

- 浏览器中的Fregment不会发生到服务器
- XSS

url parser



https://www.blackhat.com/docs/us-17/thursday/us-17-Tsai-A-New-Era-Of-SSRF-Exploiting-URL-Parser-In-Trending-Programming-Languages.pdf

总结

- HTTP是web安全的基础
- 常见的点也会存在安全问题
- 搞安全要懂开发
- 多读文档
- 对问题深入探索原因

Q&A

关于玄武实验室

- @**腾讯玄武实验室**
- 微信公众号 XuanwuLab
- Twitter @XuanwuLab

- https://xlab.tencent.com/
- xlab@tencent.com