IOS客户端通用测试

IOS客户端网络通信安全

5.1 通信协议安全

测试项描述

APP使用HTTP协议进行通信过程中可能会遭受中间人攻击，威胁数据安全

测试步骤

方法一：

1.手机设置代理

2.利用burpsuite 对数据包进行抓取，查看是否为https协议

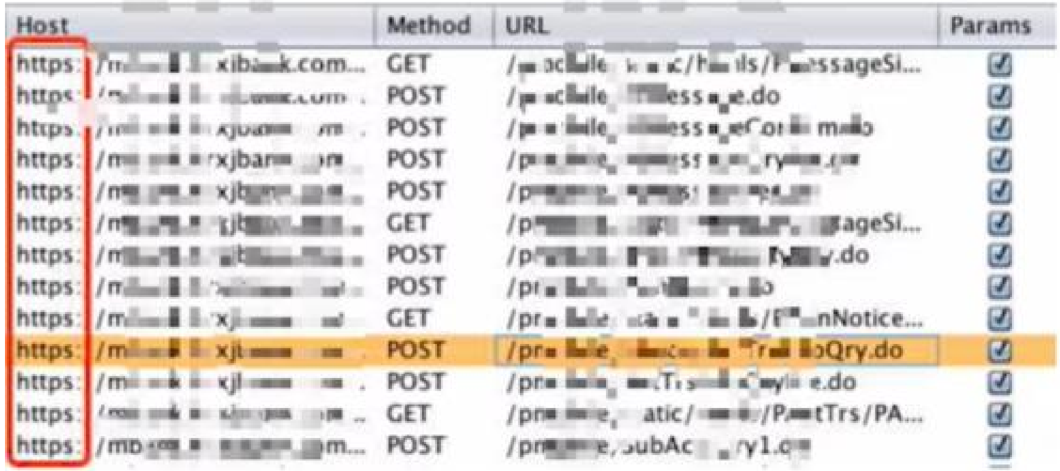
测试步骤

方法二：

反编译程序，搜索字符串中“HTTPS”或者“HTTP”进行回溯检测是否存在相关的

结果判定

如图所示是安全的



Host	Method	URL	Params
https:/[redacted]	GET	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	GET	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	GET	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑
https:/[redacted]	GET	/[redacted]	☑
https:/[redacted]	POST	/[redacted]	☑

风险评级

中风险

安全建议

建议客户端同服务器进行通信时信道使用 SSL 加密信道进行传输，同时保证加密信道的本身安全(SSLV2，SSLV3 已被证明存在漏洞，建议至少使用 TLSV1.1 以上的算法)，或是在通信过程中自实现类似 TLS 协议的算法，同时也要保证自实现算法的安全性。

IOS客户端网络通信安全

5.2 通信数据加密

通信数据加密

测试项描述

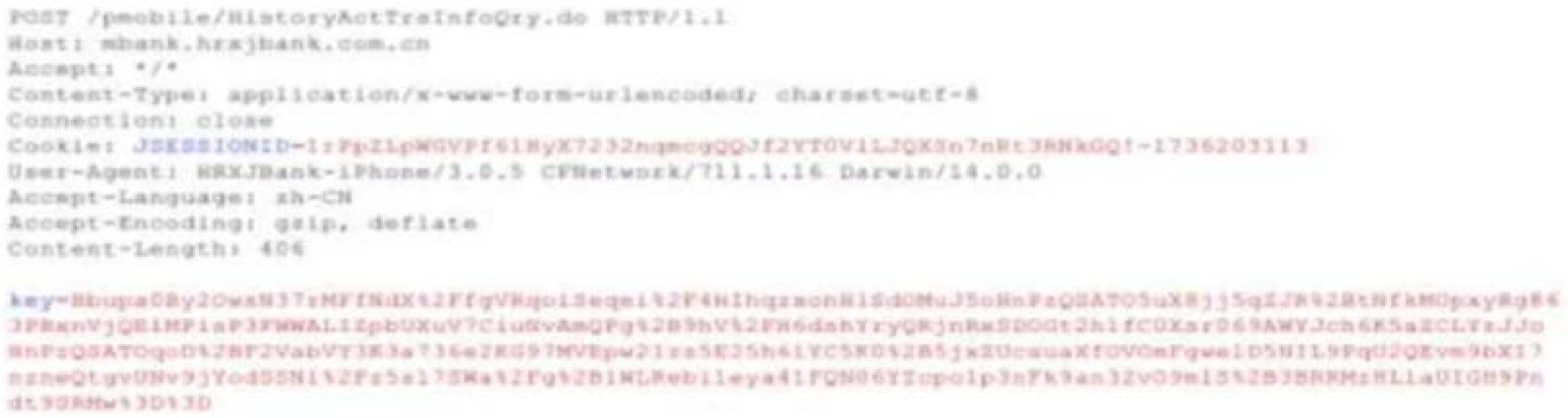
测试客户端程序提交数据给服务端时，密码等关键字段是否进行了加密和校验，防止恶意嗅探和修改用户数据包中的密码等敏感信息。

测试步骤

使用Burpsuite 进行抓包，检查数据包中的数据是否进行加密对于 TCP 协议的，可以利用 wireshark 进行抓包

结果判定

如图所示，目标进行了加密，且无法简单用base64 进行解码，安全



```
POST /pmobile/HistoryActTrsInfoQry.do HTTP/1.1
Host: mbank.hrajbank.com.cn
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Connection: close
Cookie: JSESSIONID=1rFpZLpWGVPf61HyX7232nqmcgQQJf2YTOV1LJQXSn7nRt3RNkGQ!-1736203113
User-Agent: HRXJBank-iPhone/3.0.5 CFNetwork/711.1.16 Darwin/14.0.0
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Content-Length: 406

key=Bbupa0By2OwaN37rMFfNdX%2FfgVRqoiSeqei%2F4HIhqzmonH1SdOMuJ5oHnFzQSATO5uX8jj5qZJR%2BtNfkMOpxyRgB4
3PBanVjQEiMFiaP3FWWALIZpbUXuV7CiuNvAmQPg%2B9hV%2FH6dahYryQRjnRaSDOGt2h1fCUXar069AWYJch6K5aZCLYzJJo
HnFzQSATOqoD%2BF2VabVY3K3a736e2KG97MVEpw21rs5E25h61YC5KD%2B5jx2UcsuaXfOVOmFqwe1D5HIL9PqU2QEvm9bXI7
nzneQtgvUNv9jYodSSN1%2Fz5sl7SWa%2Fg%2B1NLRebileya41FQN06YZopo1p3nFk9an32vO9m1S%2B3BRMMzHLlaUIGH9Pn
dt9ORMw%3D%3D
```

通信数据加密

风险评级

中风险——密码没有加密(在HTTP状况下)

低风险——其他信息没有加密(在HTTP状况下)，密码没有加密(没有证书校验时)

安全建议

建议使用aes进行加解密

IOS客户端网络通信安全

5.3 证书强校验检测

证书强校验检测

测试项描述

客户端可能存在忽略服务端证书校验的安全漏洞对服务器没有校验或者没有在校验错 误时候进行错误提示等。导致攻击者可通过伪造证书等手法进行攻击获取。

证书强校验检测

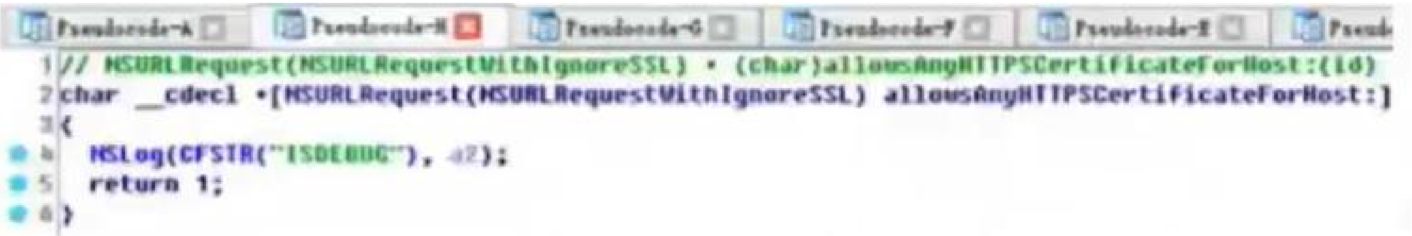
测试步骤

方法一:

安装证书，关闭 SSL Kill Switch，设置代理并进行抓包。如果程序报错或者无法进行正常通信，则存在证书校验

方法二:

反编译，检测是否存在allowsAnyHTTPCertificateForHost 函数(如图)，或者 setAllowsAnyHTTPSCertificate 函数

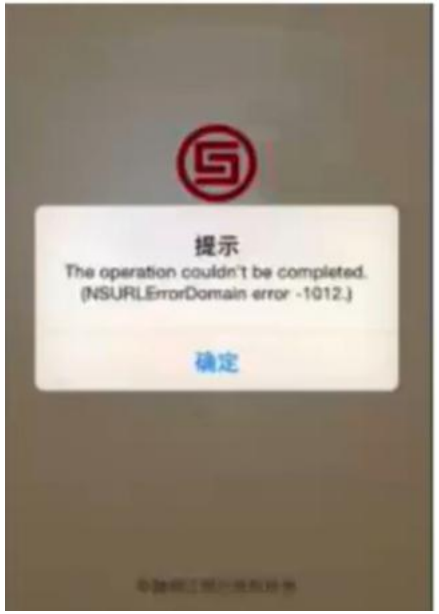


```
// MSURLRequest(NSURLRequestWithIgnoreSSL) • (char)allowsAnyHTTPSCertificateForHost:(id)
char __cdecl •[NSURLRequest(NSURLRequestWithIgnoreSSL) allowsAnyHTTPSCertificateForHost:]
{
  NSLog(CFSTR("ISDEBUG"), 42);
  return 1;
}
```

证书强校验检测

结果判定

如图所示，程序进行了证书校验：



提示

The operation couldn't be completed. (NSURLErrorDomain error -1012.)

证书强校验检测

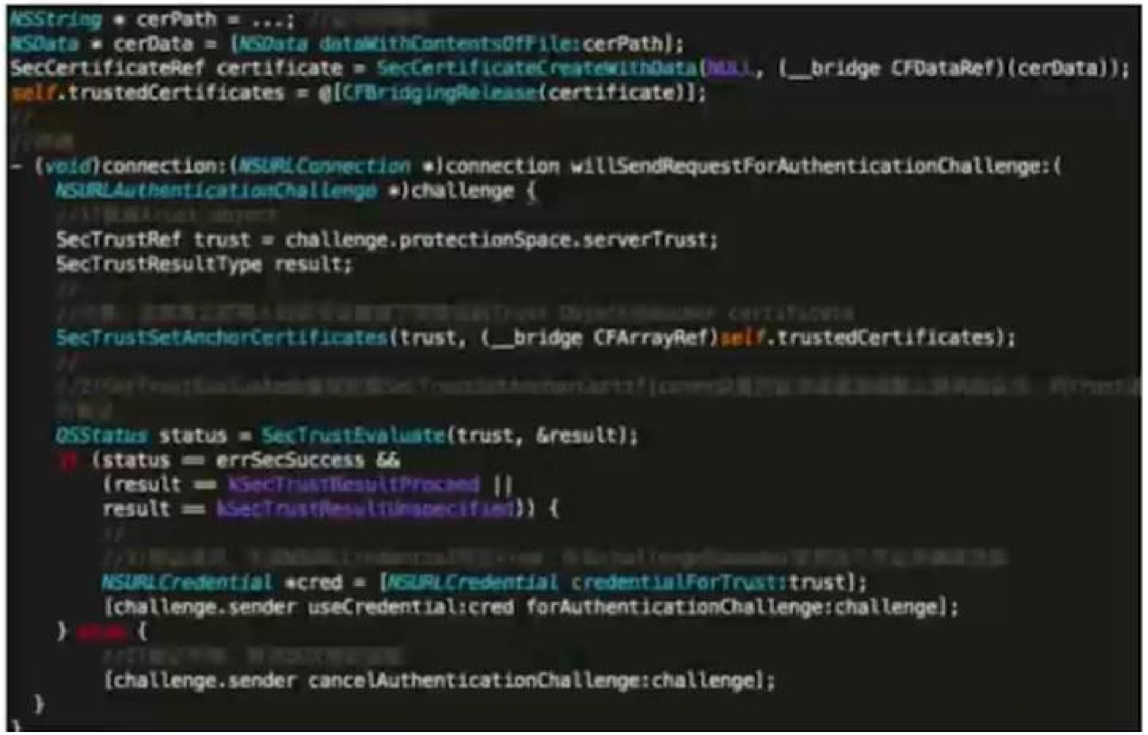
风险评级

中风险

证书强校验检测

安全建议

单向证书校验(NSURLConnection为例)



```
NSString * cerPath = ...; //[illegible]
NSData * cerData = [NSData dataWithContentsOfFile:cerPath];
SecCertificateRef certificate = SecCertificateCreateWithData(NULL, (__bridge CFDataRef)(cerData));
self.trustedCertificates = @[CFBridgingRelease(certificate)];
//
//[illegible]
- (void)connection:(NSURLConnection *)connection willSendRequestForAuthenticationChallenge:(
    NSURLAuthenticationChallenge *)challenge {
    //[illegible]
    SecTrustRef trust = challenge.protectionSpace.serverTrust;
    SecTrustResultType result;
    //
    //[illegible]
    SecTrustSetAnchorCertificates(trust, (__bridge CFArrayRef)self.trustedCertificates);
    //
    //[illegible]
    [illegible]
    OSStatus status = SecTrustEvaluate(trust, &result);
    if (status == errSecSuccess &&
        (result == kSecTrustResultProceed ||
        result == kSecTrustResultUnspecified)) {
        //
        //[illegible]
        NSURLCredential *cred = [NSURLCredential credentialForTrust:trust];
        [challenge.sender useCredential:cred forAuthenticationChallenge:challenge];
    } else {
        //[illegible]
        [challenge.sender cancelAuthenticationChallenge:challenge];
  }
}
```

IOS客户端网络通信安全

5.4 软件升级缺陷

界面切换保护

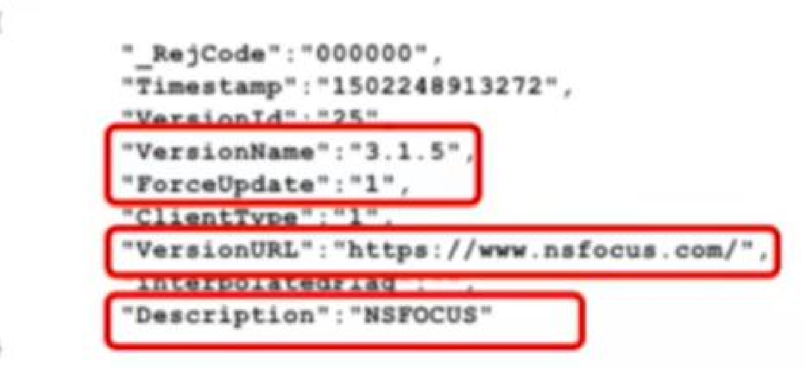
测试项描述

程序在进行版本检查的时候，通常由服务器返回对应的升级地址以方便用户访问升级，可能跳转到APp Store，也可能跳转到某个页面进行下载安装。

界面切换保护

测试步骤

针对程序升级请求，修改返回数据包的升级地址如图

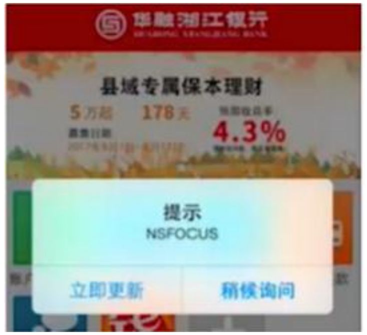


```
"_RejCode":"000000",
"Timestamp":"1502248913272",
"VersionId":"25",
"VersionName":"3.1.5",
"ForceUpdate":"1",
"ClientType":"1",
"VersionURL":"https://www.nsfocus.com/",
"InterpolatedFlag":"",
"Description":"NSFOCUS"
```

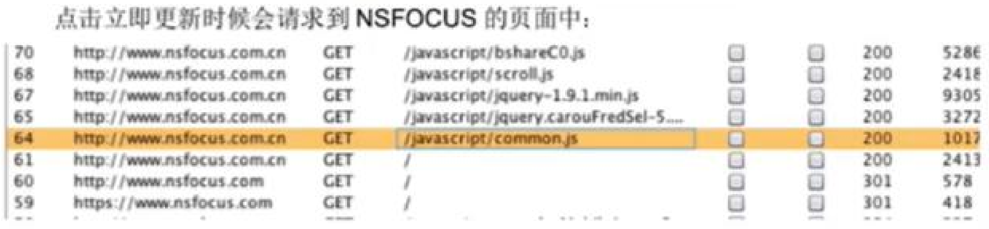
界面切换保护

结果判定

程序显示如下:



提示
NSFOCUS



点击立即更新时候会请求到 NSFOCUS 的页面中：

70	http://www.nsfocus.com.cn	GET	/javascript/bshareC0.js	□	□	200	5286
68	http://www.nsfocus.com.cn	GET	/javascript/scroll.js	□	□	200	2418
67	http://www.nsfocus.com.cn	GET	/javascript/jquery-1.9.1.min.js	□	□	200	9305
65	http://www.nsfocus.com.cn	GET	/javascript/jquery.carouFredSel-5....	□	□	200	3272
64	http://www.nsfocus.com.cn	GET	/javascript/common.js	□	□	200	1017
61	http://www.nsfocus.com.cn	GET	/	□	□	200	2413
60	http://www.nsfocus.com	GET	/	□	□	301	578
59	https://www.nsfocus.com	GET	/	□	□	301	418

界面切换保护

风险评级

中风险——在HTTP情况下

低风险—— HTTPS 证书没有做好校验

界面切换保护

安全建议

方案一：

使用 HTTPS，进行加密通信，并且加密返回数据进行完整性校验防爽打他止篡改。

方案二：

返回地址不包括其域名，域名只在程序内与返回路径进行拼接。

IOS客户端网络通信安全

5.5 数据重放测试

数据重放测试

测试项描述

客户端与服务器之间的数据通信应具有防重放机制，如进行随机数校验，防止数据包重复提交攻击造成业务错误。

数据重放测试

测试步骤

1.设置代理，采用 Burpsuite 进行抓包

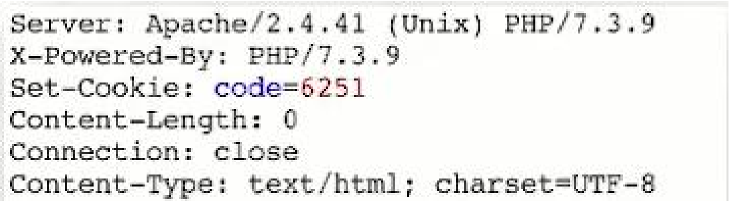
2.进行交易、下订单、获取短信验证码等操作这类操作操作

3.抓取对应数据包，重放数据包并进行拦截

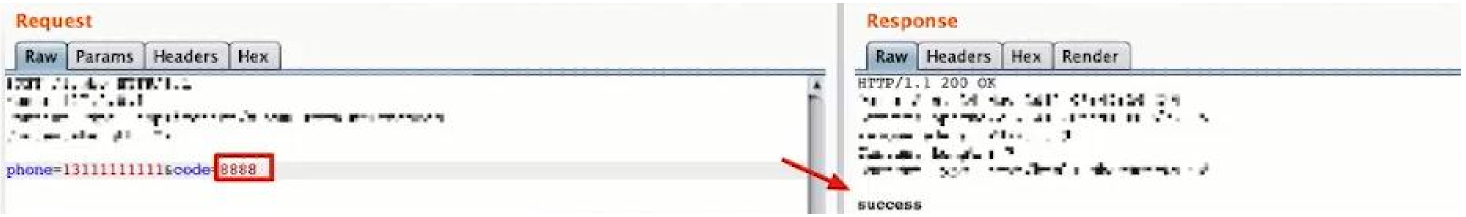
4放开拦截，所有数据同时发送

数据重放测试

漏洞案例

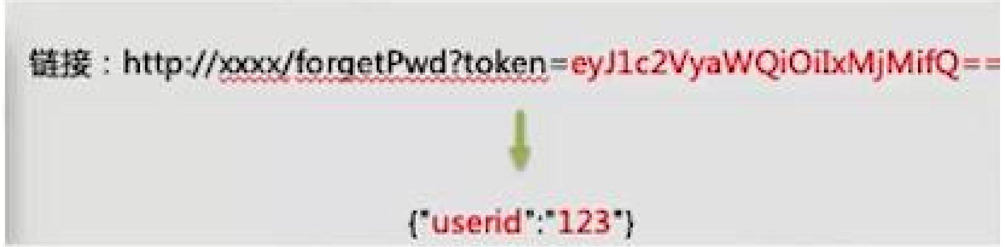


```
Server: Apache/2.4.41 (Unix) PHP/7.3.9
X-Powered-By: PHP/7.3.9
Set-Cookie: code=6251
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```



```
[illegible]
[illegible]
[illegible]
[illegible]

phone=13111111111&code=8888
```

```
HTTP/1.1 200 OK
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

success
```

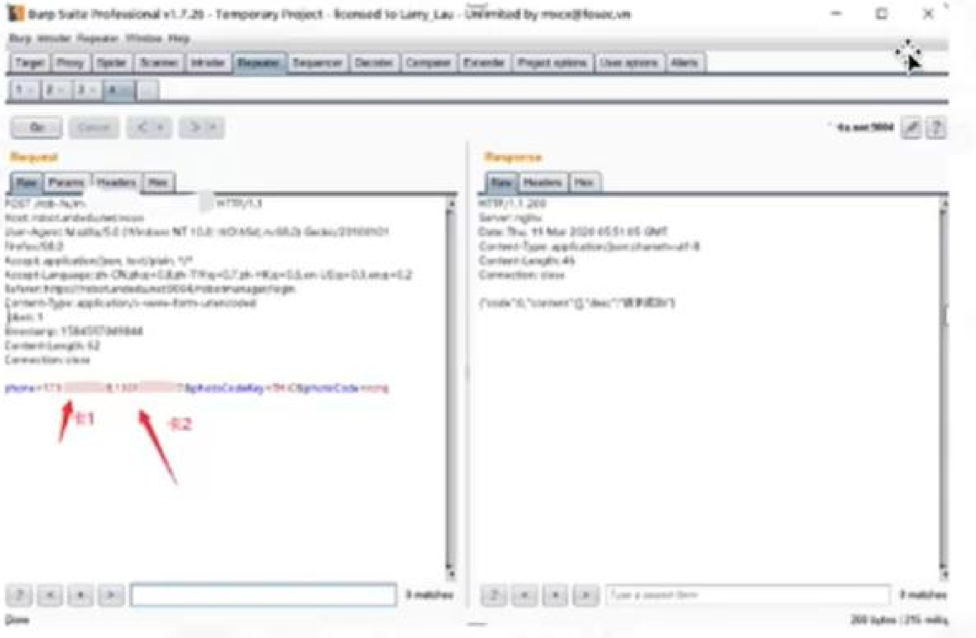


链接：http://xxxx/forgetPwd?token=eyJ1c2VyaWQiOiIxMjMifQ==

{"userid":"123"}

数据重放测试

漏洞案例



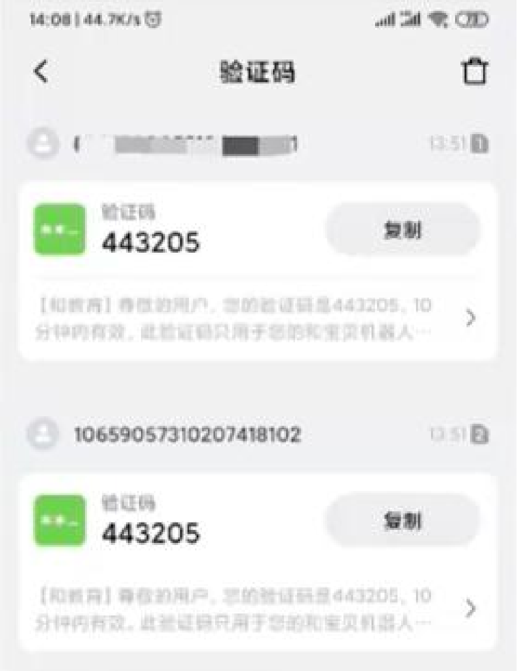
Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 ...
Go Cancel < >
Request
Raw Params Headers Hex
Response
Raw Headers Hex
0 matches
Done
200 bytes | 215 millis

```
POST [illegible] HTTP/1.1
Host: robot.andedu.net:[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:58.0) Gecko/20100101
Firefox/58.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://robot.andedu.net:9004/robotmanager/login
Content-Type: application/x-www-form-urlencoded
token: 1
timestamp: [illegible]
Content-Length: 62
Connection: close

phone=173[redacted],130[redacted]&photoCodeKey=[illegible]&photoCode=[illegible]
```

号1

号2

```
HTTP/1.1 200
Server: nginx
Date: Thu, 19 Mar 2020 05:51:05 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 46
Connection: close

{"code":0,"content":{},"desc":"请求成功"}
```



[redacted] 13:51

验证码
443205

【和教育】尊敬的用户，您的验证码是443205，10分钟内有效，此验证码只用于您的和宝贝机器人…

10659057310207418102 13:51

验证码
443205

【和教育】尊敬的用户，您的验证码是443205，10分钟内有效，此验证码只用于您的和宝贝机器人…

谢谢观赏