Demo App 安全测试报告

1.1 Demo APP

1.1.1 任意文件上传漏洞

漏洞类型：任意文件上传漏洞

危害程度：高

详细信息：在测试中发现，登录后个人主页背景图片更换处，可上传任意文件，因此可在此处上传一个后门文件来获取网站管理权限,并且可以获取网站数据库中的用户详细信息等文件.

URL:

http://api.testdns.com/image/background

http://api.testdns.com/image/voicethumb

http://api.testdns.com/image/avatar

修复建议：严格校验上传的文件名，只允许上传图片类型的文件来修复该漏洞

1.1.2 越权登录任意用户账号

漏洞类型：越权登录任意用户账号

危害程度：高

详细信息：测试中发现，输入手机号、验证码后,点击登录，服务端就会返回用户的 uID，抓包更改 uID 对应的值就可以登录他人的账户，查看、修改其信息，比如提现信息、金额等

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.0
Access-Control-Allow-Origin: *
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 13 Sep 2016 07:37:16 GMT
Content-Length: 249

{"result":{"uID":123456,"regionId":0,"openId":"","unio
nId":"","avatar":"http://testdns/IMAGE/Default/avatar.
png","nickname":"","loginDate":"2016-09-13
15:37:16","lastDate":"2016-09-14
15:37:16"},"code":0,"message":"OK","pager":null}
```

漏洞截图：

因安全问题省略

修复建议：建议采用 session 机制来验证用户的登录信息，避免返回用户的 uID

1.1.3 越权免费兑换商品

漏洞类型：越权免费兑换商品

危害程度：高

详细信息：登录自己的账号选择要兑换的商品，点击 XX，填写 XX 等信息后，确认兑换时抓取请求包修改其中的 uID 对应的值为别人的 id，再提交请求，提示提交成功。可以通过该漏洞用别人的账户为自己免费兑换商品

Request:

```
POST /testdns.com/exchange HTTP/1.1
Host: testdns.com
Content-Length: 83
Accept: application/json, text/javascript, */*; q=0.01
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; SM701
Build/SANFRANCISCO) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/30.0.0.0 Mobile
Safari/537.36; DiabinApp/1.0 /
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN,en-US;q=0.8
```

```
goodsid=1079&uID=277545
```

漏洞截图：

以用 uID=277545 用户的账户兑换商品为例

因安全问题省略截图

修复建议：建议采用身份验证机制来验证用户的身份信息，修复该漏洞

1.1.4 短信炸弹

漏洞类型：短信炸弹

危害程度：高

详细信息：登录时选择手机登录，然后通过输入手机号后来接收验证码，输入手机号后可以不断重复发送验证码，因此可以无限制对任意手机号发送验证码

Request：

```
POST /testdns.com/verifycode/login HTTP/1.1
Host: testdns.com
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://testdns.com
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; SM701 Build/SANFRANCISCO)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.11 Mobile
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```
Referer:
http://testdns.com/login.html?go_url=http%3A%2F%2Ftestdns.com%2F
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8

cellphone=13111111111
```

漏洞截图：

因安全问题省略截图

修复建议：建议在服务端限制发送验证码的时间、次数，修复该漏洞

1.1.5 越权查看手机号

漏洞类型：越权查看手机号

危害程度：高

详细信息：用户登录后可通过修改 uID 的值来查看其他用户的手机号等信息，导致手机号信息泄露

URL：http://api.testdns.com/userprofile/277154?otherId=

漏洞截图：

以 uID=277154 用户为例

因安全问题省略截图

修复建议：建议采用 session 机制来验证用户的身份信息，修复该漏洞

1.1.6 储存型 XSS 漏洞

漏洞类型：储存型 XSS 漏洞

危害程度：高

详细信息：

①在 XX 主页点击攒·XX 按钮，在留言处插入 js 语句，完成后点击确定，再进入 XX 主页，该 js 语句就被执行，通过该漏洞可获取用户的登录信息，攻击者就可以仿冒用户登录，查看其账号信息

Request:

```
POST /testdns.com/peyment HTTP/1.1
Host: testdns.com
Content-Length: 122
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://testdns.com
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; SM701 Build/SANFRANCISCO)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/37.0.0.0
Mobile MQQBrowser/6.2 TBS/036558 Safari/537.36
MicroMessenger/6.3.25.861 NetType/WIFI Language/zh_CN
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://testdns.com/user-home-other.html?otherId=250723
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN,en-US;q=0.8
X-Requested-With: com.tencent.mm

amount=0.01&content=%22%3E%3Cimg%2Fsrc%3D0+onerror%3Dalert(9)%3
```

E &uID=250723&

漏洞截图：

因安全问题省略截图

②在编辑 XXXX 的添加 XXXX 时，在地址处可插入 js 语句，保存后再点击 XXXX，插入的 js 语句被执行；在 XXXX 后，XXXX 就会提交到后台，XXXX 在处理 XXXX 时就可以通过 XXX 该漏洞获取管理员的登录信息，仿冒管理员登录，登录后台。

Request

```
POST /testdns.com/shipping HTTP/1.1
Host: testdns.com
Content-Length: 250
Accept: application/json, text/javascript, */*; q=0.01
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; SM701
Build/SANFRANCISCO) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/30.0.0.0 Mobile
Safari/537.36; DiabinApp/1.0 /
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN,en-US;q=0.8
```

```
uID=277170&regionid=120102&
address=guess%22%2F%3E%3Cimg%2Fsrc%3D0+onerror%3Dalert
(8)%3E
```

因安全问题省略截图

③在编辑 XXXX 的 XXXX 时，在 XXXX 处插入 js 语句，保存后再到 XXXX 时，插入的 js 语句被执行；如果别的用户来访问我的主页时就可以通过该漏洞获取其信息

Request

```
POST
/testdns.com/userprofile/changeoath?uID=277170&oath=t
est%22/%3E%3Cimg/src=0%20onerror=alert(6)%3E HTTP/1.1
Host: testdns.com
Content-Length: 56
Accept: application/json, text/javascript, */*; q=0.01
Origin: file://
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; SM701
Build/SANFRANCISCO) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/30.0.0.0 Mobile
Safari/537.36; DiabinApp/1.0 /
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Accept-Encoding: gzip,deflate
```

```
 Accept-Language: zh-CN,en-US;q=0.8


oath=test%22%2F%3E%3Cimg%2Fsrc%3D0+onerror%3Dalert(6)%
3E
```

因安全问题省略截图

修复建议：建议转义特殊符号:<、>、(、)，修复该漏洞

1.1.7 越权查看支付账单信息

漏洞类型：越权查看支付账单信息

危害程度：高

详细信息：在支付后会返回一个支付编号，通过更改支付编号的值来查看别人的支付信息

URL: http://api.testdns.com/peyment/4725

漏洞截图：

例如支付编号 4725 的信息：

因安全问题省略截图

修复建议：建议采用用户身份验证机制来解决越权问题

1.1.8 越权查银行卡号信息

漏洞类型：越权查看银行卡号信息

危害程度：高

详细信息：登录后在 XXXX 点击我的 XXXX 就可查看绑定的银行卡账号，在请求报文中更改 uID 的值就可以查看他人的银行卡账号、手机号等信息，此问题导致用户信息泄露 URL:

http://api.testdns.com/bankcard/277901

漏洞截图：

例如 uID 为 277091 的账号信息：

因安全问题省略截图

修复建议：建议采用用户身份验证机制来解决越权问题

1.2 Demo APP 基础性分析

本次 Demo APP 客户端基础性安全分析从客户端程序保护、敏感信息安全、安全策略、进程保护、通信安全等方面进行。

1.2.1 Allowbackup 数据备份漏洞

漏洞类型：Allowbackup 数据备份漏洞

危害程度：中

详细信息：在 AndroidMainfest.xml 文件中设置 allowBackup 的属性值为 true,因此可以使用 adb 命令备份整个应用的数据，然后在其他手机上可以恢复该备份数据，就可以登录该账号查看信息

漏洞截图：

因安全问题省略截图

在其他手机上恢复数据后查看信息：

因安全问题省略截图

修复建议：建议在 AndroidMainfest.xml 中将 allowbackup 属性值设置为 false，就可以修复该问题

1.2.2 拒绝服务漏洞

漏洞类型：拒绝服务漏洞

危害程度：中

详细信息：在 AndroidMainfest.xml 文件中 brocdcast receiver 组件的名是 com.diabin.appcross.broadcastreceivers.NetworkReceiver 的属性为设置，默认为 true，就导致其他应用可以向该 receiver 发送指令，在发送空的 action 时导致应用异常退出

dz> run app.broadcast.send --component com.demo.packagename com.diabin.appcross.broadcastreceivers.NetworkReceiver

漏洞截图：

因安全问题省略截图

修复建议：建议将该 receiver 的 exported 设置为 false 来修复该问题

1.3 Demo 微信

1.3.1 任意 URL 跳转

漏洞类型：任意 URL 跳转

危害程度：高

详细信息：登录时修改 url 的值为任意网址（此处以百度为例），登录后就可跳转到百度，可通过伪造网站来获取用户信息

URL：http://testdns.com/login.html?go_url=http%3A%2F%2Fwww.baidu.com%2F

漏洞截图：

因安全问题省略截图

修复建议：建议验证跳转的域名来修复该问题