

Plist

```
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # file cat userInfo.plist
Downloading /var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Documents/userInfo.plist to /var/folders/kv/ctb1fy6572x9fxk1c7kl9ft
00000gn/T/tmpjk7197ob.file
Streaming file from device...
Writing bytes to destination...
Successfully downloaded /var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Documents/userInfo.plist to /var/folders/kv/ctb1fy6572x
9fxk1c7kl9ft00000gn/T/tmpjk7197ob.file
=====
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>password</key>
  <string>lol123</string>
  <key>username</key>
  <string>hey123</string>
</dict>
</plist>
```

Nsuserdefaults

```
DemoValue = lol123userdefaults;
INNextFreshmintRefreshDateKey = "714578246.16363";
INNextHearbeatDate = "714829776.581751";
NSAllowsDefaultLineBreakStrategy = 1;
NSInterfaceStyle = macintosh;
NSLanguages = (
  "en-SG",
  en
);
PKKeychainVersionKey = 4;
WebDatabaseDirectory = "/var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Library/Caches";
WebKitLocalStorageDatabasePathPreferenceKey = "/var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Library/Caches";
WebKitOfflineWebApplicationCacheEnabled = 1;
WebKitShrinksStandaloneImagesToFit = 1;
"com.apple.content-rating.AppRating" = 1000;
"com.apple.content-rating.ExplicitBooksAllowed" = 1;
"com.apple.content-rating.ExplicitMusicPodcastsAllowed" = 0;
"com.apple.content-rating.MovieRating" = 1000;
"com.apple.content-rating.TVShowRating" = 1000;
loggedIn = 1;
}
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # ios nsuserdefaults get
```

Keychain

```
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # ios keychain dump
Note: You may be asked to authenticate using the devices passcode or TouchID
Save the output by adding '--json keychain.json' to this command
Dumping the iOS keychain...
Created Accessible ACL Type Account Service Data
-----
2023-02-14 08:56:53 +0000 WhenUnlocked None Password FlurryAPIKey com.highaltitudehacks.DVIAswiftv2com.flurry.analytics
2023-02-14 08:56:53 +0000 WhenUnlocked None Password FlurrySessionTimestampKey com.highaltitudehacks.DVIAswiftv2com.flurry.analytics
2023-02-14 08:56:53 +0000 AlwaysThisDeviceOnly None Password FlurrySessionInstallIDKey com.highaltitudehacks.DVIAswiftv2com.flurry.analytics
2023-08-26 02:41:08 +0000 WhenUnlocked None Password keychainValue com.highaltitudehacks.DVIAswiftv2
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] #
```

Core data

<https://book.hacktricks.xyz/mobile-pentesting/ios-pentesting>

Core Data

Core Data is a framework for managing the model layer of objects in your application. Core Data can use SQLite as its persistent store, but the framework itself is not a database. CoreData does not encrypt it's data by default. However, an additional encryption layer can be added to CoreData. See the [GitHub Repo](#) for more details.

You can find the SQLite Core Data information of an application in the path /private /var/mobile/Containers/Data/Application/{APPID}/Library/Application Support

If you can open the SQLite and access sensitive information, then you found a miss-configuration.

```
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # ls
NSFileType  Perms  NSFileProtection  Read  Write  Owner      Group      Size      Creation      Name
-----
Directory  493    n/a               True  True  mobile (501)  mobile (501)  448.0 B   2023-02-14 16:56:00 +0000  FlurryFiles
Regular    420    CompleteUntilFirstUserAuthentication  True  True  mobile (501)  mobile (501)  8.1 KiB   2023-08-26 02:42:23 +0000  Model.sqlite-wal
Regular    420    None              True  True  mobile (501)  mobile (501)  32.0 KiB  2023-08-26 02:42:23 +0000  Model.sqlite-shm
Regular    420    CompleteUntilFirstUserAuthentication  True  True  mobile (501)  mobile (501)  24.0 KiB  2023-08-26 02:42:23 +0000  Model.sqlite

Readable: True Writable: True
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # pwd
Current directory: /var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Library/Application Support
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] #
```

```
[SQLite @ Model.sqlite > select * from `ZUSER`;
+-----+-----+-----+-----+-----+-----+-----+
| Z_PK | Z_ENT | Z_OPT | ZEMAIL      | ZNAME      | ZPASSWORD   | ZPHONE      |
+-----+-----+-----+-----+-----+-----+-----+
| 1    | 1     | 1     | test@nail.com | test123     | password     | 123456       |
+-----+-----+-----+-----+-----+-----+-----+

1 row in set
Time: 0.006s
SQLite @ Model.sqlite >
```

Webkit

```
Current directory: /var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Library/Caches/com.highaltitudehacks.DVIAswiftv2
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] # ls
NSFileType  Perms  NSFileProtection  Read  Write  Owner      Group      Size      Creation      Name
-----
Directory  493    CompleteUntilFirstUserAuthentication  True  True  mobile (501)  mobile (501)  192.0 B   2023-03-01 14:01:54 +0000  com.apple.metal
Regular    420    CompleteUntilFirstUserAuthentication  True  True  mobile (501)  mobile (501)  52.0 KiB  2023-02-14 16:56:00 +0000  cache.db
Regular    420    CompleteUntilFirstUserAuthentication  True  True  mobile (501)  mobile (501)  0.0 B     2023-02-14 16:56:00 +0000  cache.db-wal
Regular    420    CompleteUntilFirstUserAuthentication  True  True  mobile (501)  mobile (501)  32.0 KiB  2023-02-14 16:56:00 +0000  cache.db-shm

Readable: True Writable: True
....highaltitudehacks.DVIAswiftv2 on (iPhone: 12.5.6) [usb] #
```

Table: cfurl_cache_response							
entry_ID	version	hash_value	storage_policy	request_key	time_stamp	partition	
Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1	1	0 9167921985616649203	0	http://example.com/	2023-03-01 16:22:30	NULL	
2	2	0 -130858905	0	https://example.com/	2023-03-01 16:23:02	NULL	

Table: cfurl_cache_receiver_data			
entry_ID	isDataOnFS	receiver_data	
Filter	Filter	Filter	
1	1	0 <!doctype html>...	
2	2	0 <!doctype html>...	

Mode: Text

```

32         width: auto;
33     }
34 }
35 </style>
36 </head>
37
38 <body>
39 <div>
40     <h1>Example Domain</h1>
41     <p>This domain is for use in illustrative examples in documents. You may use this
42     domain in literature without prior coordination or asking for permission.</p>
43     <p><a href="https://www.iana.org/domains/example">More information ... </a></p>
44 </div>
45 </body>
46 </html>
47

```

Type of data currently in cell: Text / Numeric

1256 character(s)

Apply

## Realm

## Copy to root folder

```

iPhone-2:/var/mobile/Containers/Data/Application/C2E14680-8620-43DA-9B14-65D6D0B55760/Documents root# ls
Bolts.fid*      default.realm.lock      libswiftCoreFoundation.dylib.fid*  libswiftFoundation.dylib.fid*      libswiftos.dylib.fid*
DVIA-v2.fid*   default.realm.management/ libswiftCoreGraphics.dylib.fid*    libswiftMetal.dylib.fid*          libswiftsimd.dylib.fid*
Flurry_iOS_SDK.fid* default.realm.note|    libswiftCoreImage.dylib.fid*      libswiftObjectiveC.dylib.fid*      secret-data
Parse.fid*     libswiftAVFoundation.dylib.fid*  libswiftCoreLocation.dylib.fid*    libswiftQuartzCore.dylib.fid*      userinfo.plist
Realm.fid*     libswiftCore.dylib.fid*        libswiftCoreMedia.dylib.fid*      libswiftRemoteMirror.dylib.fid*
RealmSwift.fid* libswiftCoreAudio.dylib.fid*    libswiftDarwin.dylib.fid*         libswiftSwiftOnoneSupport.dylib.fid*
default.realm  libswiftCoreData.dylib.fid*    libswiftDispatch.dylib.fid*      libswiftUIKit.dylib.fid*

```

## Download via filezilla

Filename ^	Filesize	Filetype	Last modified	Filename ^	Filesize	Filetype	Last modified	Permissions	Owner/Group
Cache.db	53248	Database Docu...	08/26/23 10:52:...	sshd_config		Directory	02/14/23 15:...	Inwxr-xr-x	root wheel
Cache.db-shm	32768	db-shm-file	08/26/23 10:54:01	aks_migrate	1	File	02/04/23 18:...	-rw-r--r--	root wheel
Cache.db-wal	0	db-wal-file	08/26/23 10:54:01	aks_whitelist	1	File	02/04/23 18:...	-rw-r--r--	root wheel
default.realm	16384	realm-file	08/26/23 11:18:05	bash_history	2388	File	03/10/23 21:...	-rw-----	root wheel
testdata.bin	1169	bin-file	08/26/23 11:00:18	bootstrapped	0	File	02/04/23 18:...	-rw-r--r--	root wheel
				gliteconfig	46	File	02/14/23 16:...	-rw-r--r--	root wheel
				.mkb_seshat_health	117	File	08/26/23 10:...	-rw-r--r--	root wheel
				.obliterated	0	File	02/04/23 18:...	-rw-r--r--	root wheel
				.viminfo	10109	File	02/23/23 20:...	-rw-----	root wheel
				.wget-hsts	215	File	02/15/23 00:...	-rw-r--r--	root wheel
				DVIA-v2-swift.lipa	20307491	ipa-file	02/15/23 00:...	-rw-r--r--	root wheel
				com.apple.MobileAsset.plist	466	plist-file	02/16/23 18:...	-rw-r--r--	root wheel
				com.nabla0d3.sskilswitch2_0_...	7392	deb-file	02/14/23 14:...	-rw-r--r--	root wheel
				CPH19183shim	13254	resin-file	08/26/23 11:...	-rw-r--r--	root wheel
				frida_16.0.4_iphoneos-arm.deb	17540304	deb-file	11/26/22 09:...	-rw-r--r--	root wheel
				frida_16.0.9_iphoneos-arm.deb	17564752	deb-file	02/11/23 20:...	-rw-r--r--	root wheel

No option to view it on legacy format



### The Realm file stores data in an outdated format

This file needs to be upgraded to a newer file format before it can be opened. Would you like a backup of the file, before performing an irreversible upgrade of the file?

Upgrade in-place

Backup and upgrade

Cancel

## Empty strings

CLASSES	+	Enter a query in Realm Query Language (RQL) to filter the list	
RealmUser	3	<b>name</b> string?	<b>password</b> string?
		<i>null</i>	<i>null</i>
		<i>null</i>	<i>null</i>
		<i>null</i>	<i>null</i>