

Forum:[Hack Forums](#)

Thread: [APK Decompile to rebuild JSON Request](#)

mauricebr - November 13, 2024, 8:26 am

Hello Guys,

I need help,

I have a APK that sends a json Request with base64 encodes Images I figured out how to rebuild the request with jadx . It worked until last week.

I think the Images has some hash property or something that the server don't accept.

Two possible ways:

1. method: Remove the damn SSL Pinning from APK and check with Fiddler which request are made.

I tried it with no luck. No experience in Unpinning.

2. Find with JADX the method why server decline it.

If someone has a plan write me a PN . I will pay for it.

I will send u the APK and further Information.

Uolcan - November 13, 2024, 8:53 am

(Nov 13, 2024 09:26 AM)mauricebr Wrote: [\[CITE\]](#) Hello Guys,

I need help,

I have a APK that sends a json Request with base64 encodes Images I figured out how to rebuild the request with jadx . It worked until last week.

I think the Images has some hash property or something that the server don't accept.

Two possible ways:

1. method: Remove the damn SSL Pinning from APK and check with Fiddler which request are made.

I tried it with no luck. No experience in Unpinning.

2. Find with JADX the method why server decline it.

If someone has a plan write me a PN . I will pay for it.

I will send u the APK and further Information.

i think using fiddler in this cases or wireshark would be more better as you can patch the apk ssl validation logic to validate your certification and there are many other methods to do so

mauricebr - November 13, 2024, 9:40 am

I know but I can't patch can you do?

Will pay for a working solution.

jeannyetal - November 14, 2024, 6:10 am

Hook the ssl.X509ExtendedTrustManager (if they are using x509) and you can patch the checkServerTrusted to pass SSL pinning.

Otherwise approaching this with static analysis will not get you far.

If you can't do it, send me a message.

mauricebr - November 15, 2024, 11:44 am

Done please remove Done please remove Done please remove

Clumsy - November 15, 2024, 2:39 pm

(Nov 15, 2024 12:44 PM)mauricebr Wrote: [\[CITE\]](#) Hello

I figured out how to sniff.

Now I now that the app sending a image from camera. When I analyze the JPEG it looks normal. After opening it in Text Editor I can see clearly that they put some information at the end of file.

That means we have to figure out what it is.

PHP Code

```
<?php
```

Masl, [15 Nov 2024 um 17:33]

```
"CameraInfo_availableRecordingResolutions": "unknown",
```

```
"CameraInfo_availableResolutions":
```

```
"[4096x3072, 4096x2304, 4096x1856, 4000x3000, 3840x2160, 3264x2448, 3072x3072, 2592x1944, 2560x1440, 2400x1080, 1920x1440, 1920x1088, 1920x1080, 1600x720, 1560x720, 1520x720, 1440x1088, 1440x1080, 1440x720, 1280x960, 1280x720, 1152x720, 1080x1080, 1080x720, 960x720, 800x600, 720x720, 720x480, 640x480, 352x288, 320x240, 192x144, 176x144]",
```

```
"CameraInfo_availableStillResolutions": "unknown",
```

```
"CameraInfo_focusMode": "CONTROL_AF_MODE_CONTINUOUS_PICTURE",
```

```
"CameraInfo_hardwareLevel": "3",
```

```
"CameraInfo_previewResolution": "1920x1080",
```

```
"CameraInfo_recordingResolution": "unknown",
```

```
"CameraInfo_resolution": "4096x2304",
```

```
"CameraInfo_stillResolution": "unknown",
```

```
"Device_info_device_manufacturer": "Nothing",
```

```
"Device_info_device_model": "A015",
```

```
"Device_info_os_platform": "Android",
```

```
"Device_info_os_version": "14",
```

```
"Device_info_sdk_version": "4.7.1",
```

```
"Device_info_uuid": "09aea9b6-ecfb-4b34-bc92-f6f8eab8763e",
```

```
"Device_status_info_ae_state": "AE STATE Converged",
```

"Device_status_info_ae_status": "AE Converged",
"Device_status_info_af_mode": "CONTROL_AF_MODE_AUTO",
"Device_status_info_af_state": "AF STATE Converged",
"Device_status_info_af_status": "AF Converged",
"Device_status_info_awb_state": "AWB STATE Converged",
"Device_status_info_awb_status": "AWB Converged",
"Device_status_info_capturing_state": "NO CAPTURING",
"Device_status_info_device_orientation": "Rotation 0",
"Device_status_info_device_orientation_mode": "InterfaceOrientation",
"Device_status_info_interface_orientation": "Rotation 0",
"Device_status_info_roi_mode": "Automatic",
"QA_info_blur_block_blur_area": "0.000000",
"QA_info_blur_block_blur_area_factor": "2.000000",
"QA_info_blur_block_sharp_area": "0.285684",
"QA_info_blur_mode": "2",
"QA_info_blur_score": "0.598015",
"QA_info_blur_threshold": "0.700000",
"QA_info_darkness_mode": "-1",
"QA_info_darkness_score": "0.000000",
"QA_info_darkness_threshold": "0.000000",
"QA_info_hotspot_mode": "1",
"QA_info_hotspot_score": "0.000000",
"QA_info_hotspot_threshold": "900.000000",
"QA_info_mindpi_mode": "-1",
"QA_info_mindpi_score": "0.000000",
"QA_info_mindpi_threshold": "0.000000",
"QA_info_photocopy_detection_mode": "-1",
"QA_info_photocopy_detection_score": "0.000000",
"QA_info_photocopy_detection_threshold": "0.000000",
"QA_info_skew_mode": "-1",
"QA_info_skew_score": "0.000000",
"QA_info_skew_threshold": "0.000000",
"SDK_config_camera_facing": "Rear",
"SDK_config_capture_3A_mode": "BlockWhile3A",
"SDK_config_capture_documents":
"[1.585800, 1.418800, 1.420400, 2.000000, 2.009524, 2.047619, 1.418800]",
"SDK_config_capture_mode": "Frame",
"SDK_config_detection_zone_enabled":
"tl:[0.222868,0.233806],tr:[0.670299,0.240026],br:[0.667685,0.787072],bl:[0.219846,0.787072]",
"SDK_config_edge_detection_mode": "MachineLearning",
"SDK_config_max_crop_resolution": "600",
"SDK_config_shooter_mode": "Auto",
"SDK_process_ae_count": "241",
"SDK_process_af_count": "42",
"SDK_process_aspect_ratio_detected": "1.420400",
"SDK_process_awb_count": "77",
"SDK_process_blur_count": "91",
"SDK_process_capture_mode_used": "ML",
"SDK_process_darkness_count": "0",
"SDK_process_edges_detected_count": "95",
"SDK_process_hotspot_count": "0",
"SDK_process_photocopy_count": "0",
"SDK_process_processed_frames_count": "320",

```
"SDK_process_still_capture_attempts": "0",  
"SDK_process_video_capture_attempts": "0",  
"SDK_process_video_processed_frames_count": "0",  
"SDK_process_video_valid_frames_count": "0",  
"SDK_profiling_capture_time": "43152",  
"SDK_profiling_crop_average_time": "25",  
"SDK_profiling_crop_frames_processed": "95",  
"SDK_profiling_crop_max_time": "44",  
"SDK_profiling_crop_min_time": "8",  
"SDK_profiling_edges_detection_average_time": "41",  
"SDK_profiling_edges_detection_frames_processed": "320",  
"SDK_profiling_edges_detection_max_time": "108",  
"SDK_profiling_edges_detection_min_time": "35",  
"SDK_profiling_engine_initialization_time": "206",  
"SDK_profiling_initialization_time": "361",  
"SDK_profiling_iqa_initialization_time": "356",
```

And this

PHP Code

```
<?php
```

```
"SDK_profiling_qa_checks_average_time": "11",  
"SDK_profiling_qa_checks_frames_processed": "320",  
"SDK_profiling_qa_checks_max_time": "43",  
"SDK_profiling_qa_checks_min_time": "1",  
"SDK_profiling_still_capture_success_time": "0",  
"SDK_profiling_still_capture_taken_time": "0",  
"SDK_profiling_video_capture_duration_time": "0",  
"SDK_profiling_video_capture_success_time": "0",  
"SDK_profiling_video_capture_taken_time": "0"} ? ?? /. ?o,F]z 9Bw  
|StP /%y>2Bu , l cp?}• •6h{/; R\3,. )K ? ?* l ou RAk~\ zC.TO)?w i?GRK<^q/5 ^ hH|Q4, C•^zy3N ]  
00 7l??w2c|*3|Q `!,f;e@='9^?xGn  
GTO
```

objdump -s file.apk

mauricebr - November 15, 2024, 2:56 pm

Sry but it is not solving my problem