







Findings		
	High 1	
	Medium 15	
	Info 0	
	Secure 1	
	Hotspot 8	
<div>high</div> App can be installed on a vulnerable upatched Android version		<a href="#">MANIFEST</a>
<div>medium</div> Application vulnerable to Janus Vulnerability		<a href="#">CERTIFICATE</a>
<div>medium</div> Application Data can be Backed up		<a href="#">MANIFEST</a>
<div>medium</div> Broadcast Receiver (com.duiyun.activity.TakePhotoReceiver) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.services.CancelNoticeService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.services.UpdateDuanpingService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.services.UpdateChangpingService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.services.UpdateRizhiService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.services.UpdateLoggerNotificationService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.account.TestSyncService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> Service (com.duiyun.account.TestAuthService) is not Protected.		<a href="#">MANIFEST</a>
<div>medium</div> High Intent Priority (2147483647)		<a href="#">MANIFEST</a>
<div>medium</div> App can read/write to External Storage. Any App can read data written to External Storage.		<a href="#">CODE</a>
<div>medium</div> Files may contain hardcoded sensitive information like usernames, passwords, keys etc.		<a href="#">CODE</a>

<div>medium</div> Application contains Privacy Trackers	<a href="#">TRACKERS</a>
<div>medium</div> This app may contain hardcoded secrets	<a href="#">SECRETS</a>
<div>secure</div> This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	<a href="#">CODE</a>
<div>hotspot</div> Found 21 critical permission(s)	<a href="#">PERMISSIONS</a>
<div>hotspot</div> App may communicate to a server (developer.umeng.com) in OFAC sanctioned country (China)	<a href="#">DOMAINS</a>
<div>hotspot</div> App may communicate to a server (plbslog.umeng.com) in OFAC sanctioned country (China)	<a href="#">DOMAINS</a>
<div>hotspot</div> App may communicate to a server (ouplog.umeng.com) in OFAC sanctioned country (Hong Kong)	<a href="#">DOMAINS</a>
<div>hotspot</div> App may communicate to a server (lark.alipay.com) in OFAC sanctioned country (China)	<a href="#">DOMAINS</a>
<div>hotspot</div> App may communicate to a server (ulogs.umengcloud.com) in OFAC sanctioned country (China)	<a href="#">DOMAINS</a>
<div>hotspot</div> App may communicate to a server (cmnsguider.yunos.com) in OFAC sanctioned country (China)	<a href="#">DOMAINS</a>
<div>hotspot</div> App may communicate to a server (ulogs.umeng.com) in OFAC sanctioned country (China)	<a href="#">DOMAINS</a>

MobSF Application Security Scorecard generated for  ( System Service 16.3) 