

Olá, pessoal.

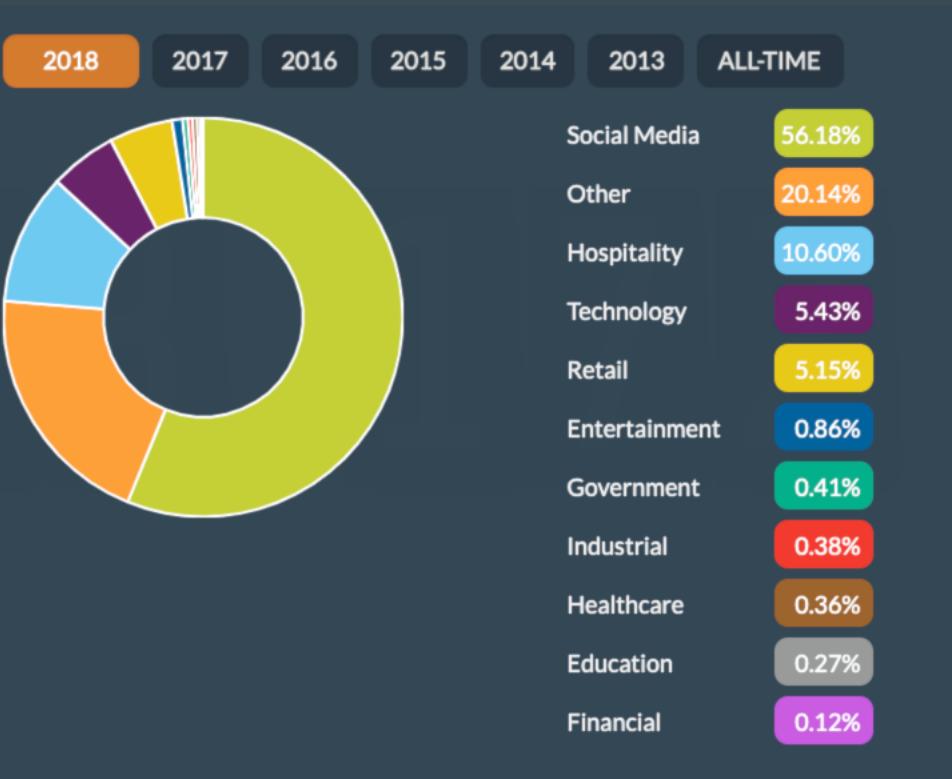
Construindo aplicativos seguros

Nós queremos nossos apps mais seguros.
Mas temos notado uma escalada
de problemas de segurança.

3,353,172,708

Registros vazados no primeiro semestre de 2018

3,35



708

Registros vazados

este de 2018

18,525,816
records lost or stolen
every day



771,909
records
every hour



12,865
records
every minute



214
records
every second



Por que isso acontece?



Por que isso acontece?



#whoami

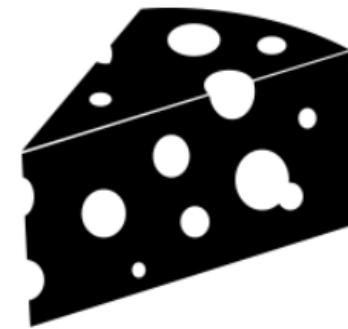
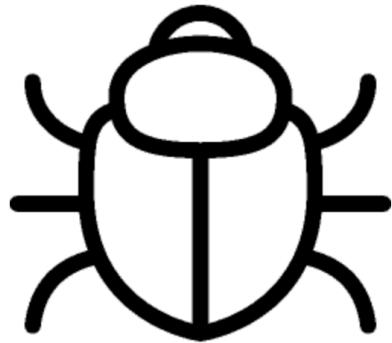
João Pimenta

- Arquiteto de segurança
- Pentester de apps
- Pesquisador de segurança
- Jazz

Além da cereja do bolo e do Forrest

- Crescimento exponencial de dados e acesso à internet
- O mercado da desinformação
- “Segurança inviabiliza o produto”
- “Terminamos o produto, agora vamos investir em segurança!”

Aonde isso nos leva?



Vamos ver...

Chave de API hardcoded

```
private static final java.lang.String CONFIG = "cloudinary://434762629765715:████████@reverb";
```

Informação sensível em log

```
response_headers null (null) 04-12 16:37:27.861 17800 17800/com
request_id 23241935-2b28-4347-98c6-739e0ef215f0 (java.lang.String) 04-12 16:37:27.861 17800 17800/com
response_body {"permission": {"access_token": "885d505e8b4f6677e25f06ffdc2fed34"} } (java.lang.String) 04-12 16:37:27.861 17800 17800/com
response_code 200 (java.lang.Integer) 04-12 16:37:30.221 17800 17800/com
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.221 17800 17800/com
{"permission": {"access_token": "885d505e8b4f6677e25f06ffdc2fed34"} } 04-12 16:37:30.221 17800 17800/com
response_headers null (null) 04-12 16:37:30.281 17800 17800/com
request_id 26d9ee74-3696-4f9d-98dd-dddb8f2e1a35 (java.lang.String) 04-12 16:37:30.281 17800 17800/com
response_code 200 (java.lang.Integer) 04-12 16:37:30.281 17800 17800/com
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.281 17800 17800/com
response_headers null (null) 04-12 16:37:30.281 17800 17800/com
```

Informação sensível em log

```
response_headers null (null) 04-12 16:37:27.861 17800 17800/com
request_id 26d9ee74-3696-4f9d-98dd-dddb8f2e1a35 (java.lang.String)
response_{"access_token":"885d505e8b4f6677e25f06ffdc2fed34"}}
response_headers null (null) 04-12 16:37:30.221 17800 17800/com
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.221 17800 17800/com
{"permission": {"access_token": "885d505e8b4f6677e25f06ffdc2fed34"}}
response_headers null (null) 04-12 16:37:30.281 17800 17800/com
request_id 26d9ee74-3696-4f9d-98dd-dddb8f2e1a35 (java.lang.String)
response_code 200 (java.lang.Integer)
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.281 17800 17800/com
response_headers null (null)
```

Autenticação insegura

```
{
  "video" : {
    "client_device_model" : "iPhone 7",
    "client_device_brand" : "Apple",
    "localization" : "pt-BR",
    "device_ram" : 2099249152,
    "workflow_data" : {
      "face_detection_granularity" : 0.20000000000000001,
      "security_level" : 10,
      "detection_sensitivity" : 100,
      "face_detection_max_size" : 1,
      "perform_construction" : false,
      "frames" : [
        {
          "tags" : [
            ],
          "timestamp" : 1548336428.869246,
          "data" :
        }
      ]
    }
  }
}
```

orHSLCt1c6LWw/XKqgE9FWL55m;J8koOpPctwBzj/FWu0Wj+QdWw11J8wGxT84nyetXLTqzHuw/LqujngDQ7arKz113Bq
2roycu5oKF2SNp4ArF1HVNjAKenpTdU1BY4m07BPsuR1bVl7VvxySkUffydzGvVQtbL/Aig8UosG3cC+mZzxzsp8TPGU7zx
Mzqjlf1Peui8bej3traaRzR8uT9k534K/F7whd48W3Hjxw1F4mtG4XdkQY/Uhehr6fc0HFe6tT43M8bzKyPILwXTTtLLGw
zz9K1tLyWBwlcr7iv0AX4Vfs/+tBwkw8j+Ix4R1iRc/YLwgLn2B/oa+df2gv2wdY+C6c51vLDULCRwqt2swLHP+zXqNfpM
42/1+iSVVSfmeofs3fthwf40CLRt28L6bg0mqAj3EMkrMR/t2Hzv9EDSvgb+OrB7rG4i8MatMOAjCe7vd78pr8vo2lrf5A
VJPtlrsvD+sXMMUf7wgjkEdRw6p0fqJU1LXzn0x8YvhgD8JruKGz8RafrUlt8iqSDz1hQgyiuLhhZY1zxPF6bqFcxXnnTTM7
EDLMF2516Bpqle2xIfIav6tKPLF1qzs95313ieYxqBu55zW3YUuwKOhz3qnbRuGChMgdxxQWaBVxeMh0qpQuzJto6CzhJt0
Ab9ak1QoCh4B4p+mxF4R1pJhpUQo2PE40OvWsrWzwsK3M4jxXoLx2md5VsJhEv0l0m7Tcz78D0Jr17xFcmTTdyuQbzXkdxe
Mb4jdHpu9JdtokesVQYCBg9v9tLRLBiGyORViS1TmcP65pfnxkrt1Hmdawcr0x6XkQhceUS3BHT3qeyn+oyEky1Gc1TAK
J3gcelaG10QryF1wegsFsFypTzyJchG79DVG7VpYpsP91jVqS5Y324BBhsjvdLN5EXGaiborvRJAJDPPCQeYdk46Cp7LV
kzgr9CkQh0N13eOXXyglCnhbg1ALzysP1f9u9iHfdLvvY7Cc8evFZn/CVJHcoFc8npn+1N1+xaeJio+bGLXevPnLhd8x
OfxrWlnCjk7R7P3iSa3PrjntUteje3rQEGVlp473SoVktztlyKOPD/ir7NdauDx3q2St2NRs9d12WSc1Cq20K6CHvBld
DdnGBk/1XnsPiG1lIxox5Yvr30kxzQy71kDqAawu0i3puat3rfjewGSMguOMvg3GpxiauEN2z3NrJZQWgK+yDvn6VWx
3Th435Po6LrsSlYbp1tvgMtVkoAhCleuLk3Yqunp54rJksnS92ycckh3Qr2AcBxkeopPR1L7qzUoKt9Kd64Un3p9hHD
Lbh069hwjfi3N1T+MnJHFZd1bCGFps4A5uxTlRl+pi8eT01nXsyScPbY2QnVs+fxKn23Tng+1QxijsqfhuMrXyV51
c3re5CYVwnB7V7Tnn82UFCeqgqrBTPdsKeFqdmtBbf42VyoDxziuh1CKRG2AGcmq2d57b209q0t8h7o2zQIwySSBwk5q
rA1dQlJuYwCnDa4q5j5+bv64abMgn1IpVgCndhTnHwOsYrmmlupT0F0S+1c5xjyFR7dr/NlSuqOpGPTNng5FpHufw1
kLLGFHeolnyOOBTzIjACTggc0rdQuswFuHxGEwo7muuyjPujsnk5IORipLKzK5PHYGjcd771Vm296u2rmTapXhvVwslywi
fj2q/pjpjbcqPhs7maNo32rzhrs2UvR6zq2tdUg4124YcvK3d+UyIdC9Kt26KVxle7LeteJ1U0Wkj6+Gxiv/h1dLjhTib
jNeGlRCM+kF/2etVUpEEiHctrXvylEmACDxGy0pcsrn6Dgq/NsstJF0TyL1k3mtqVhyjaqBzB1gP4NfLgEvjbtwGvp
Q15qWlzqbaWhusyif1Cfa4qrNoViJy4PesaXXEUD2490ayrjXchb1l4461vClzj2j1ls+1dcrci0uMj3rzvxzd4o2Rsq87R2
q5lyrj00je1B6V554glciCORJdVz5zor2af1kfo7F20Ry/17XGmsGRdbzz6mvom1JWzQc56jtxQ63Jje1mRg81R1A71
imGhrwdx4r20L1Pkg0+dml0m9sds0cux+4XnDctLuluGveg5YTFxdcmYuswX01x1jpaQYHgb+VWYLrlkrB781yuLyU
avndpdSxgtg9wRXxwsiw4jUD68VcyC17zvGcdq6XrRj2utzsdnoa6410izsvdR0u5wcduelej6MB2gJ2xiu0SLRRPMAnVe
c+1dfb/APhlk1B2ruij+R0lu60QcfjwVwpMyhSm7yismKyL7ldTece9uvqataHg33PSfAoN20rapF23mswaPA3S4W1U7
cV7RrH7M6ppq3Whava6uXoaQufQosS+2rC5Qdngq05rsFbxH1XnwA2N/Pa0R/1LP1Fc9S1zlap2IWnr8Nb/cZwfcbsR6
hp88C/w50JB/EcV4vrmhWtnKZWIuk9a+p9Z/a18Q3lq9jlB2F0dW2Yjd2R90lFivx1le+1w+eSlJwnJjES4X8hXp70pid
ztzoc5CXFnHd24kgkY7A02eae3trgrjkaAeLevP4u1kW9NHHCt5RNdrbfEKzrvaNc2c4JYFV3PutoasNxJg72AudevR21
mtwg0evpXy6w4tY1RMDed0rYf0zCNSw+UfpU3RvnLy106Bjx844zw78Bbz2xird3frx3luyvZqgll1uuuhG7injmnyqXq
i2DNKXcwfsrC2MqAktx7Vamnhkttgyq61ldp+gDevk65wDwkuYbu+ooiUct+Vzu02sc2U7APetHv02juw/MceQkZPcwTwRru
JRxs11Dz1TaXbajpSr8HHoecVj62P84r4IGT2HFWhdHkk13qAoh9a7PQo4bMpfVtznHrXnPyXm1ocu/wev13MTt1V28
450KhzG6NefZwP2LxjPrxodp8Qiumg2DjpyelMwUg1l43As05001y60eoex2j+4ulhmjySpb01zLdbnwoNg0na2q5
cMoRAAE961dyPlyQAlYqlNysWrpXMGbU5YzSwbynuo9aNlcw3K52dvlprlp0f8wBbKkdDveTzFIUQFT20avmvotZ2+eCB4
QEIANxstapzbqjYJxycdas20fzoaZG3SjjFZGtWm9KqKsQ01uM2Nklu9/k=,".captured_frame_is_constructed":f
alse,".feedback":[]},{".liveness_result":{},".score":100}}}

Autenticação insegura

orH8LCettic6LUN/XR6g25Pwt55m;BkcoOpcttwBzjFwUoW+j+QdKwii13MaGtTB44nyetXL7qgHovrlqyjnsbA7mrKs1l5Bq
2roycu5oXF2SNp4ArF1HVnjAKenptTd1BY4m07BPSuR1bVltVxjKySKuFFydzGVVQtbL/A1g8UosG3cC+MzzXzp8TPGU7Xzx
QMzjlflPeui8beJ3traaRZ8uT9K534K/F7wh4d8Wy3HjXwlF4ntG4xDkQY/Uhehr6fcOHFe6t4t43M8bzKyPllwXTtLLGw
zz9KtlyWB1wcr7iv0AX4Vfs/+tBwWkAj+Ix4RliRc/YLwgLn2B/oa+dF2gv2WdY+c6C5lvLDULCRwqT2swLHP+zXqXnFqM
42/i+SVSfmeofs3fthWfw40CLrt2816bqOmAj3EMkrMR/tZhZv9EDSvgb+0Rb7rG4i8MatMOAjCE7vdT8pr8vo2lrrf5A
VJPT1rsD+sXMMUF7wjgkEdrW6pqfQJU1LXzn0x8YvhgD8JruKzG8RafrULt8iQSDz1HgyiuLhh2Y1zxXF6bqFxcXnnTTM7
EDLM2f516BpqLe2x1fLAV6tKPLF1qzS95313ieYxqBu55zW3YWuwKohz3qnBrugChMgdXQWaBVXeMH0qpQuzJt06CzhJt0
Ab9ak1oQch484p+tmxF4R1pHpuOgzeP400WsrWzwsK3M4jxXolxZmd5VsjHev010mT7cz78D0Jr17xCMttYduKbzKdxde
Md4jDHpuP9jdtoke5vQYCbv9utRLBiGYORvIs1TmQcp65p8fxnrKt1MdawcrOx6XQkhceUS3BHT3qeyn+oyEkyIGc1TAk
J3gcelaG1qRyFlwegqufsPYpTzyjCgHTg9DVG7vpYpsP91jVgs5Y3Z4BBbhsjVdlN5EXGaibv0RJJaPPCQeYdk46Cp7LV
kgz9KrhQn13i0ExXgkclNhbg11AL2yPS1f9iHFDLwVYYCc8evFZn/CVJHcoFc8npn+1nL+xaeJio+bGclxEvph2Lhd8x
OfxrWlnckjR7fp3isG3PrjntUtje3rQEGVlp473SoVkZt1yK0PD/ir7ndAuDx3qZSTu2NRs9D12wSC1cQ2OK6CHvBFL
DdnGBk/1XnsPiGz1xox5YVr30KxzQy7jKDqAawoui3puat3rfjewGSMguOMVg3GpxaixiuEN2z3NRJZQWgk+YDnv6VVWx
3t435psa6LrsS1Ybjp16tvMtVkrAch1eulK3YquNp54rJksn92yckCh3qR2AckeopPR1L7qZuotK9d64Ucn3p9hHD
LbOh69Wjfi3Nt1+MNjHFZdlbCGFps4Ax5uTx1RlI+p8eTqlinxSyScCpbYzNvVs+fXKN23GTng+lQxijsghfmRxVY51
c3re5CYVwNbW7Tnn82UFCgeqgrbTPdSkEfQdmBbF42Vyzdiuh1CKRG2Agcmqn2d5q7bd209g0tyh8Hz0q1IwySBWxk5q
ra1dGQ1juYWcnDA4gq5V5+bT6ba4B4Mgn1PpVGndhTrnHwOsYmRMnlupPT0fso+1c5xjyfR7dr/NixSuOpGPNTNngP5fHufw1
kLlGFHeolnyOOBTz1JACTggc0rdQuSwUHXGfWo7mUyjPUjpsNk510rIpLk1zK5PHYgjc771VmZ96u2rmTapXHvVWSLyWI
fj2/pjpjhqcS7sMaNo3zRchsZUVR6z2q2tdUgu4124YcvK3d+uyICD9kt26KVxecl7etQleJ1u5Wkj68+Gxiv/hIdljThib
jnNegLRcmF/2etVupPee1HctrXvY1EmaCxDxyGopcsrn6dgq/NSSTJPOFyTg1Kk3mTqVHyjsaqXbIBgpn4NF1gEvjbtvGWP
Q15qWlzqbaWhusy1A4qrNoviJY4PesaXXEUD2409ayrjxhbc1L4461vc1z1j2lus+Idcr10UumJ3rzvx4d02Rsq87R2
q5rlyj00j1E86V554gliCOORJdvLz5z0r2aFc1kFOY7F20RY/17XGmsGrmDbz6mwvM1JWZQc56jxtQ63JJe1mRG81R1A71
imQhRwdx4r20L1pk0+d1m0lm9eds0cx+U4XndCtLUvGeq68YTfxdxCmYUsysw0xk1jpa1QYHGB+vVWYL1KrtB781uYL
avNdpDsxtg9wRXxwiS4wJUD68VycC17zwcGdqj
c+1dfb/APh1K9B2ruij+R0lu60QcfjyWxPmyhs)nVe
cV7RrH7Mr6ppq3Whava6uhXOAQuf0QSK+rZc5D0
hp88C/wB50JB/EcV4vrmhWtnKZWIuk9a+p92/al
ztoczX5CXFnHd24kgkDy7A02ea3tgrjkAelevpm
mtwg0evpXPy6wt4Y1RMED0rf0YzCNSw+UfpU3RV
i2DNKcxwfSrC2MqAkt7xVamnhKtptygg61Dp+gDe
JRXS11D2zLTaxbajsp8rHH0ecVj6z284rq4IGtz
450KzHgr6NefZpWZ1XjPrxodp8QHiimgzDjpyelMvUg1W43sA05001Y6ooEx2jz+4uLhmJySpPb0q1zXdlboNww0gNa2q2s
cmoAQAE916ldpYQYALy1NysWrpXMGDU5YZSWhyu09aNlcw3K52dvlprp0f8hWbKbdDVeTTzFIUQFT2OavmvotZE+oCB4
QEIANStapbjqjYjxycdaS20fzoAZG3SjjFZGWM9vKqKSQ01Un2NklbU/9k=","captured_frame_is_constructed":f
else,"feedback":[]},"liveness_result":{"feedback":[],"score":100}}}}

Insecure Direct Object References

Go Cancel < | > | ▾ Target: <https://business.facebook.com>

Request

Raw Params Headers Hex

```
POST /business_share/asset_to_agency/?dpr=2 HTTP/1.1
Host: business.facebook.com
Connection: close
Content-Length: 436
Origin: https://business.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */
Referer:
https://business.facebook.com/settings/pages/536195393199075?business_id=907970555981524
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8
Cookie: rc=2; datr=AWE3V--DUGNTOAy0wTGmpAXB; locale=en_GB;
sb=BWE3V1vCnIxJF87yY9a8WWjP; pl=n; lu=gh2GPBnmZY1B1j_7J0Zi3nAA;
c_user=100000771680694; xs=25%3A5C6rNSCaCX92MA%3A2%3A1472402327%3A4837;
fr=05UM8RW0tTkDVgbSW.AWUB4pn0DvP1fQoqywWeORlj_LE.BXN2EF.IL.FFD.0.0.BXxBSo
.AWXdKm2I; csm=2; s=Aa50vjfSfyFBHmC1.BXwxOY;
_ga=GA1.2.1773948073.1464668667; p=-2;
presence=EDvF3EtmeF1472469215EuserFA21B00771680694A2EstateFDutF147246921
5051CEchFDp_5f1B00771680694F7CC; act=1472469233458%2F6
parent_business_id=991079870975788&agency_id=907970555981524&asset_id=190
313461381022role=MANAGER&__user=100000771680694&__a=1&__dyn=aKU-XxaAcoau
cCJDzopz8aWKFbGEW8UhrWqw-xG2G4aK2i8zFE8oqCwkoSEvmbgcFV8SmqVUzxeUW4ohAxWdw
SDBzovU-eBCy8b48xicx2aGewzwEx2qEN4yECcKbBy9onwFwBCBxungXKdAw&__req=e&__be
=-1&__pc=PHASED%3Abands_pkg&fb_dtsg=AQBoLGH1HUmf%3AAQGT4fDF1-nQ&ttstamp=
265817211176711044972851091025865817184521026870494511081&__rev=2530733
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
X-Frame-Options: DENY
Strict-Transport-Security: max-age=15552000; preload
Cache-Control: private, no-cache, no-store, must-revalidate
Access-Control-Allow-Credentials: true
Pragma: no-cache
Vary: Origin
Access-Control-Allow-Origin: https://business.facebook.com
Access-Control-Expose-Headers: X-FB-Debug, X-Loader-Length
access-control-allow-method: OPTIONS
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-XSS-Protection: 0
Content-Type: application/x-javascript; charset=utf-8
X-Content-Type-Options: nosniff
content-security-policy: default-src * data: blob:;script-src *.facebook.com *.fbcdn.net *.facebook.net
*.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1: * *.spotilocal.com: * 'unsafe-inline' 'unsafe-eval'
fbstatic-a.akamaihd.net fbcdn-static-b-a.akamaihd.net *.atlassolutions.com blob: data:;style-src data:
'unsafe-inline' *;connect-src *.facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com: * *.akamaihd.net
wss://*.facebook.com: * https://fb.scanandcleanlocal.com: * *.atlassolutions.com attachment.fbsbx.com ws://localhost: *
blob: chrome-extension://boadgeojelhgndagh1jhdcfkmlpafd chrome-extension://dliochdbjfkdacpmhlcpmleaejidimm;
Vary: Accept-Encoding
Content-Encoding: br
X-FB-Debug: j08Vj634V5Rv16IIewJWVC0YJ18Ng9SA/A1SY2td9SRcaZrI2FE7sbUzivLifjjPK24tRhHgEr3R69fan3tI5w==
Date: Mon, 29 Aug 2016 11:18:18 GMT
Connection: close
}
?3@hs@>S@+J T@! @ @ @
@ @=1@@-b#00@ a /@TS|wc@@{ >a@ @y|@*@@ P_A@@Z@:@ K@ Mqt@15@@1@2@
```

Reportada por Arun Sureshkumar

Insecure Direct Object References

Go Cancel < | > | ▾ Target: <https://business.facebook.com>

Request

Raw Params Headers Hex

```
POST /business_share/asset_to_agency/?dpr=2 HTTP/1.1
Host: business.facebook.com
Connection: close
Content-Length: 436
Origin: https://business.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */
Referer:
https://business.facebook.com/settings/pages/536195393199075?business_id=907970555981524
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8
Cookie: rc=2; datr=AWE3V--DUGNTOAy0wTGmpAXb; locale=en_GB;
sb=BWE3V1vCnIxJF87yY9a8WWjP; pl=n; lu=gh2GPBnmZY1B1j_7J0Zi3nAA;
_c_user=100000771680694; xs=25%3A5C6rNSCaCX92MA%3A2%3A1472402327%3A4837;
fr=05UM8RW0tTkDVgbSW.AWUB4pn0DvP1fQoqywWeORl1j_LE.BXN2EF.IL.FFD.0.0.BXxBSo
.AWXdKm2I; csm=2; s=Aa50vjfSfyFBHmCl.BXwxOY;
_ga=GA1.2.1773948073.1464668667; p=-2;
presence=EDvF3EtmeF1472469215EuserFA21B00771680694A2EstateFDutF147246921
5051CEchFDp_5f1B00771680694F7CC; act=1472469233458%2F6
parent_business_id=991079870975788&agency_id=907970555981524&asset_id=190
313461381022&role=MANAGER&__user=100000771680694&__a=1&__dyn=aKU-XxaAcoau
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
X-Frame-Options: DENY
Strict-Transport-Security: max-age=15552000; preload
Cache-Control: private, no-cache, no-store, must-revalidate
Access-Control-Allow-Credentials: true
Pragma: no-cache
Vary: Origin
Access-Control-Allow-Origin: https://business.facebook.com
Access-Control-Expose-Headers: X-FB-Debug, X-Loader-Length
access-control-allow-method: OPTIONS
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-XSS-Protection: 0
Content-Type: application/x-javascript; charset=utf-8
X-Content-Type-Options: nosniff
content-security-policy: default-src * data: blob:;script-src *.facebook.com *.fbcdn.net *.facebook.net
*.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1:* *.spotilocal.com:/* 'unsafe-inline' 'unsafe-eval'
fbstatic-a.akamaihd.net fbcdn-static-b-a.akamaihd.net *.atlassolutions.com blob: data:;style-src data:
'unsafe-inline' *;connect-src *.facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com:/* *.akamaihd.net
wss://*.facebook.com:/* https://fb.scanandcleanlocal.com:/* *.atlassolutions.com attachment.fbsbx.com ws://localhost:*
blob: chrome-extension://boadgeojelhgndaghlijhdcfkmlpafd chrome-extension://dliochdbjfkdacpmhlcpmleaejidimm;
Vary: Accept-Encoding
Content-Encoding: br
X-FB-Debug: j08Vj634V5Rv16IIewJWVC0YJ18Ng9SA/A1SY2td9SRcaZrI2FE7sbUzivLifjjPK24tRhHgEr3R69fan3tI5w==
Date: Mon, 29 Aug 2016 11:18:18 GMT
Connection: close
```

parent_business_id=991079870975788&agency_id=907970555981524&asset_id=190
313461381022&role=MANAGER&__user=100000771680694&__a=1&__dyn=aKU-XxaAcoau

qt@15♦♦1♦2♦

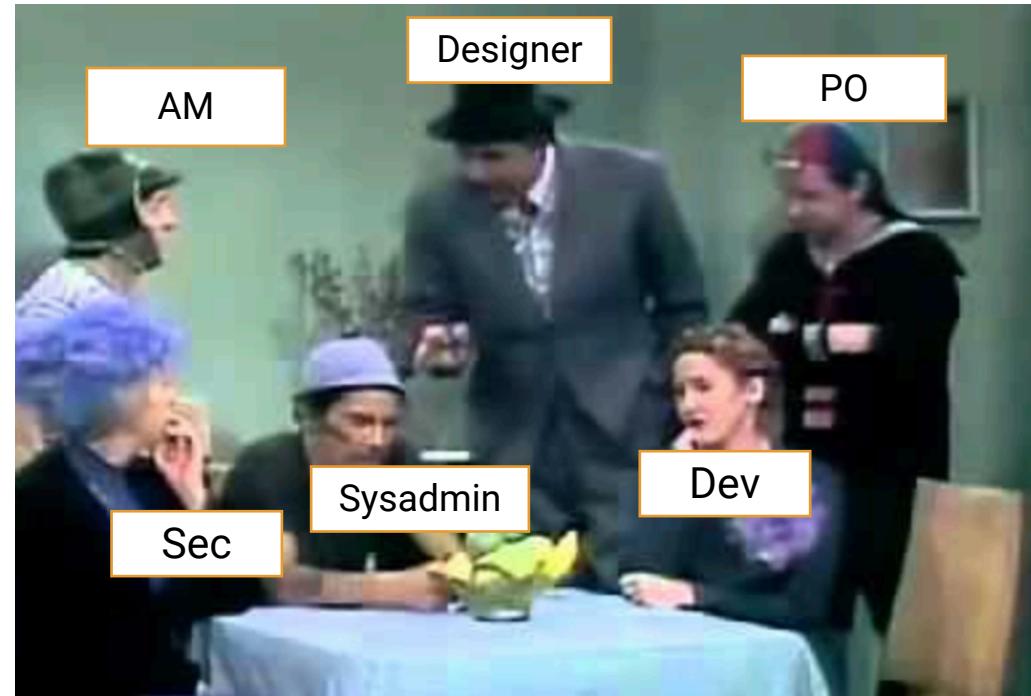
Reportada por Arun Sureshkumar

Qual nosso papel?

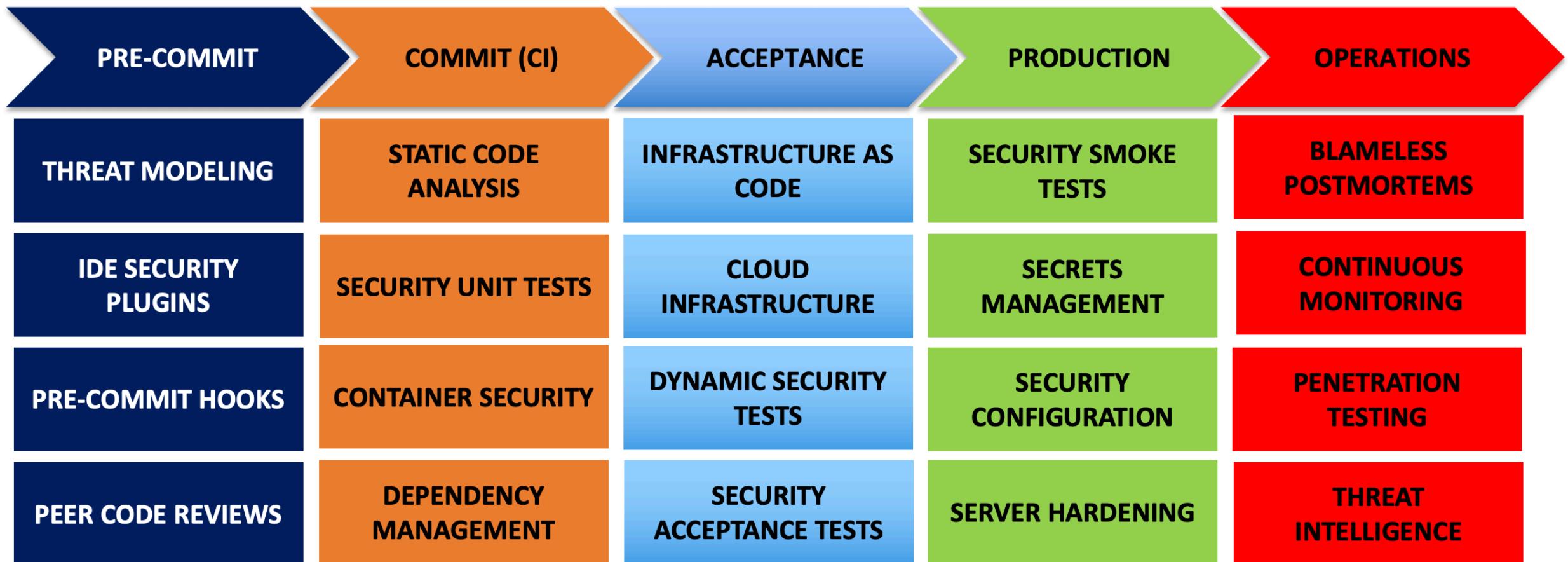
Me pague a segurança!



Se comunicar, integrar a segurança.



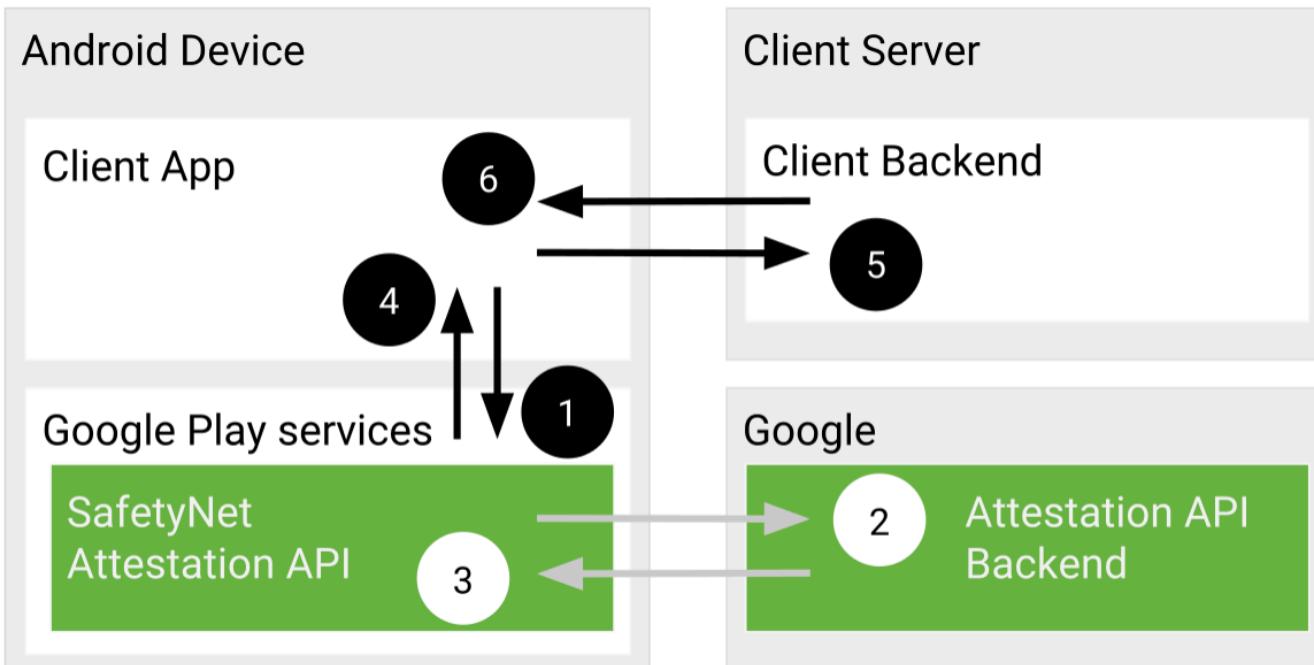
Segurança desde a concepção



Dificultar a vida do atacante

- Ofuscação do código;
- Antitamper;
- Antidebug;
- Antihooking;
- Antiemulador;
- Antiroot/Jailbreak;
- SSL Pinning;
- Criptografar e assinar Payload (RSA + AES).

SafetyNet Attestation API



1. A API SafetyNet Attestation recebe uma chamada do seu aplicativo incluindo um nonce.
2. O serviço SafetyNet Attestation avalia o ambiente de runtime e requisita aos servidores do Google um resultado através de uma mensagem assinada.
3. Servidores do Google retornam uma mensagem assinada ao device para a SafetyNet attestation.
4. SafetyNet attestation retorna esses valores para o seu app.
5. Seu app encaminha para os seus servidores.
6. Seus servidores recebem a informação e utilizam para tomada de decisões de segurança.

SafetyNet Attestation API

Device Status	Value of <code>ctsProfileMatch</code>	Value of <code>basicIntegrity</code>
Certified, genuine device that passes CTS	true	true
Certified device with unlocked bootloader	false	true
Genuine but uncertified device, such as when the manufacturer doesn't apply for certification	false	true
Device with custom ROM (not rooted)	false	true
Emulator	false	false
No device (such as a protocol emulating script)	false	false
Signs of system integrity compromise, one of which may be rooting	false	false
Signs of other active attacks, such as API hooking	false	false

Segurança é colaborativa.
É uma jornada de construção.

Segurança é colaborativa.
É uma jornada de construção.

Obrigado!

Referências

- https://blogs.sans.org/appsecstreetfighter/files/2018/10/DevSecOps_Exploring_Phase1-2.pdf
- <https://arunsureshkumar.me/index.php/2016/09/16/facebook-page-takeover-zero-day-vulnerability/>
- <https://breachlevelindex.com/>
- <https://developer.android.com/training/safetynet/attestation.html>