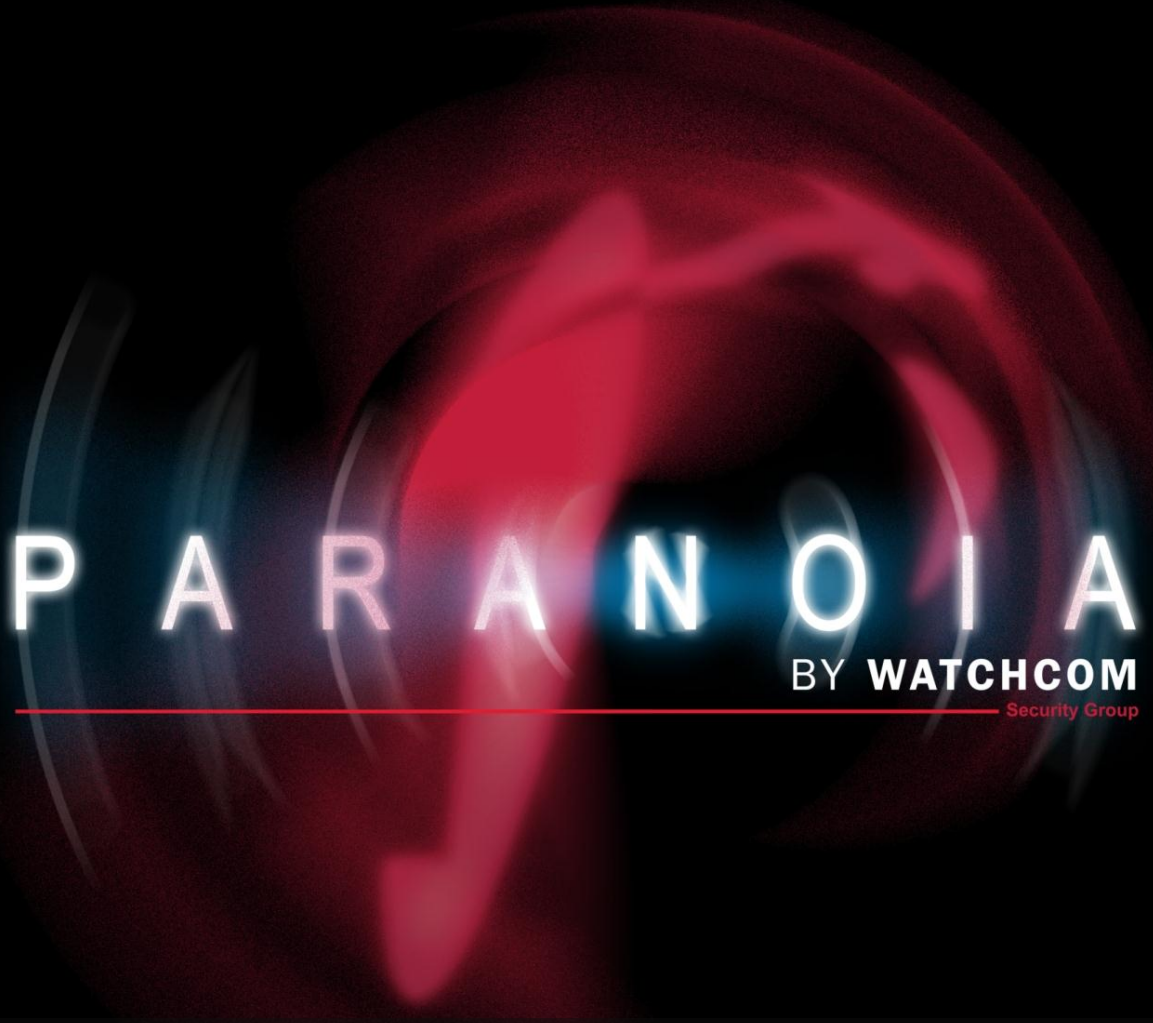


Sikkerhet i mobilapplikasjoner

Espen Graarud

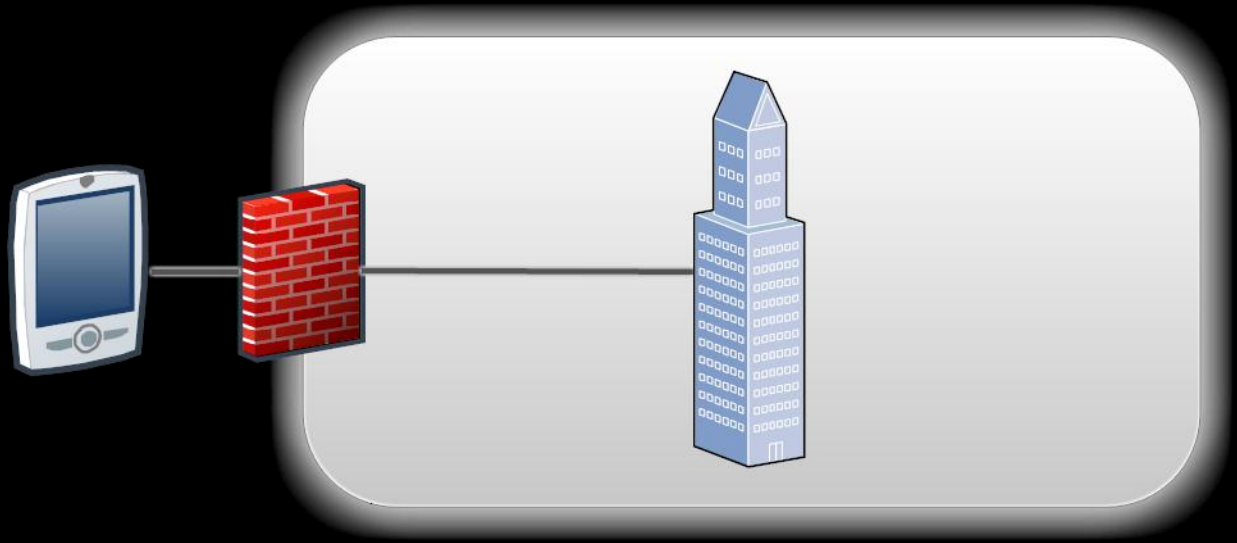
Pentester i Watchcom Security Group

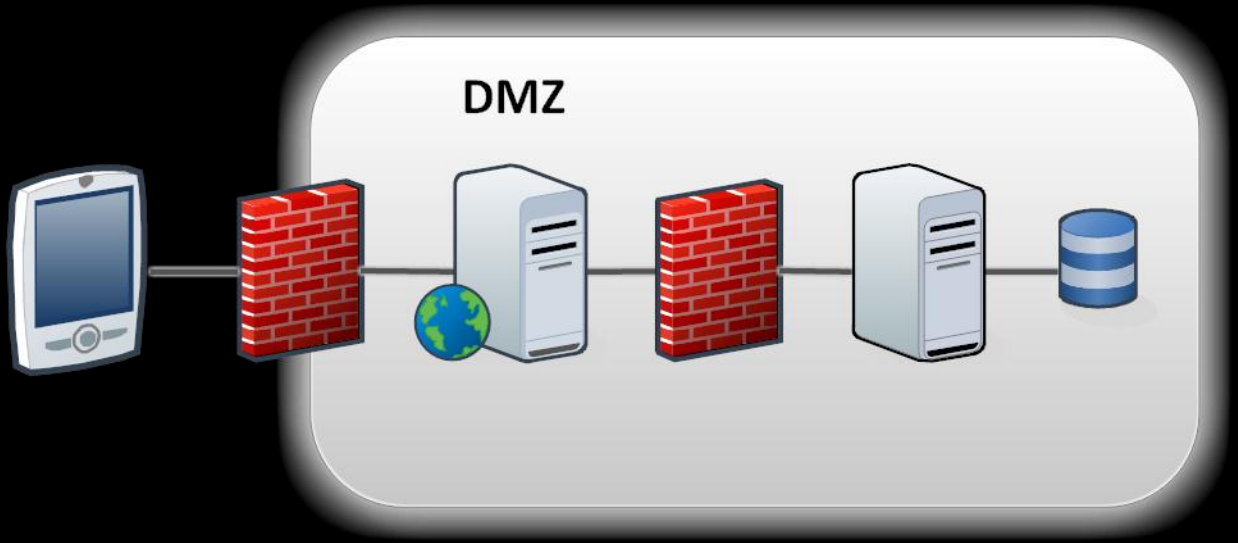
Utført en rekke pentester mot mobilapper

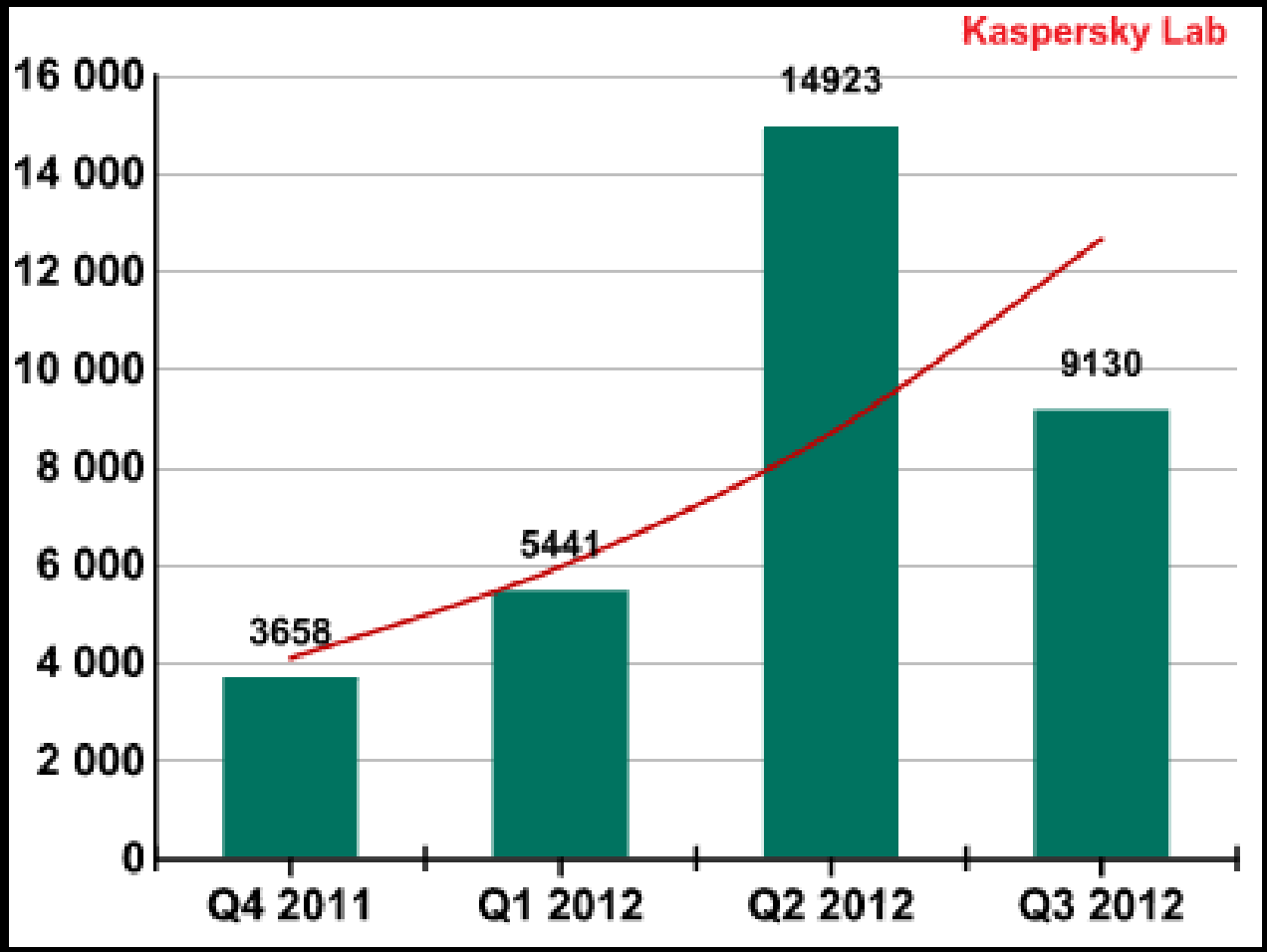
Spesialisert seg på Android plattformen

// mailto:espen.graarud@watchcom.no

Hvordan påvirker mobilapper bedriftens sikkerhet?




DMZ


Kaspersky Lab
16 000
14 000
12 000
10 000
8 000
6 000
4 000
2 000
0
3658
5441
14923
9130
Q4 2011
Q1 2012
Q2 2012
Q3 2012

Hva kan man gjøre for å øke sikkerheten?

Risiko- og sårbarhetsanalyse

Nye informasjonsverdier

Nye angrepsvektorer

Lage sikringstiltak

Pentest / Sikkerhetstest

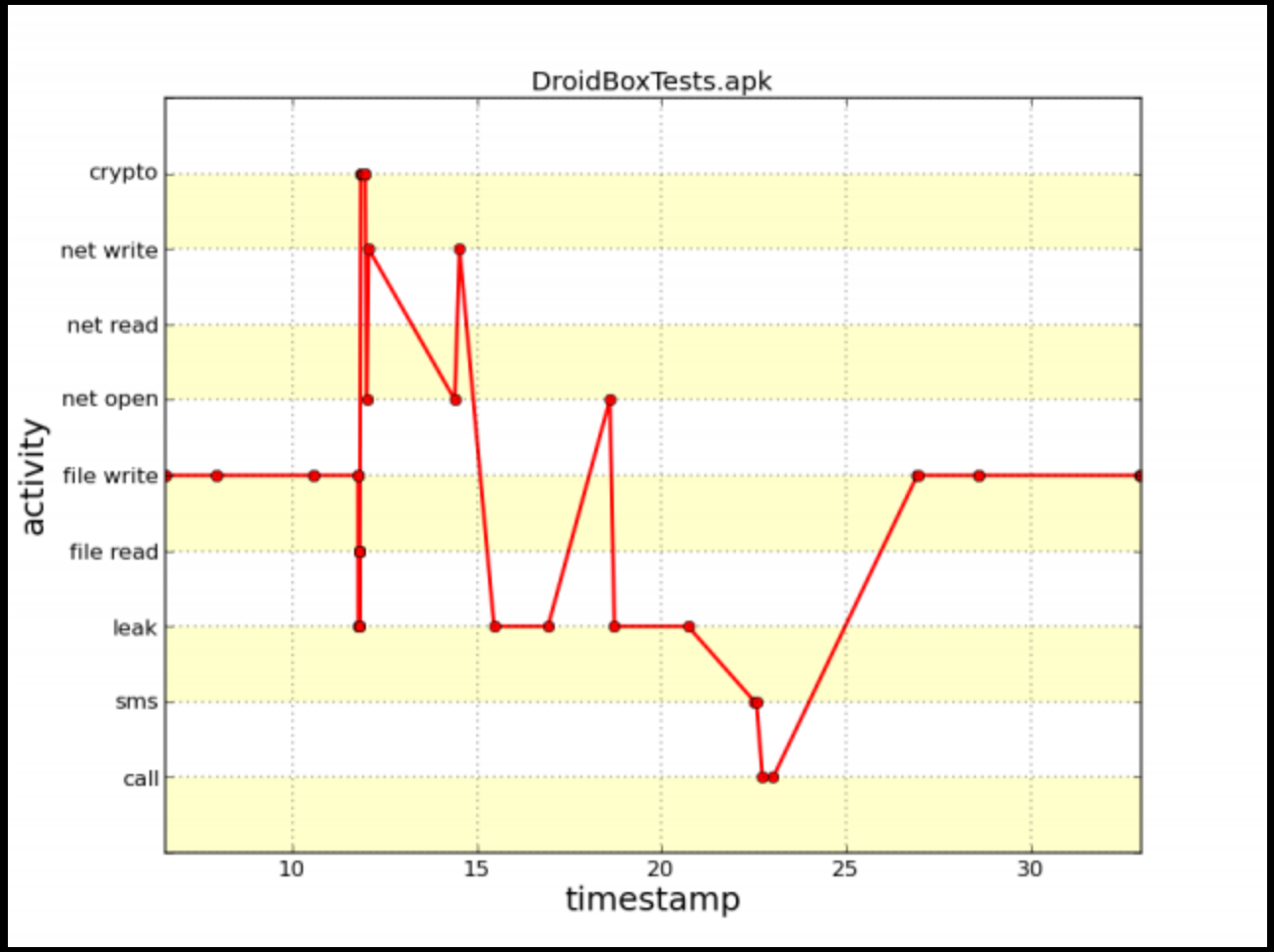
Dynamisk analyse

Kjørende app og prossesser

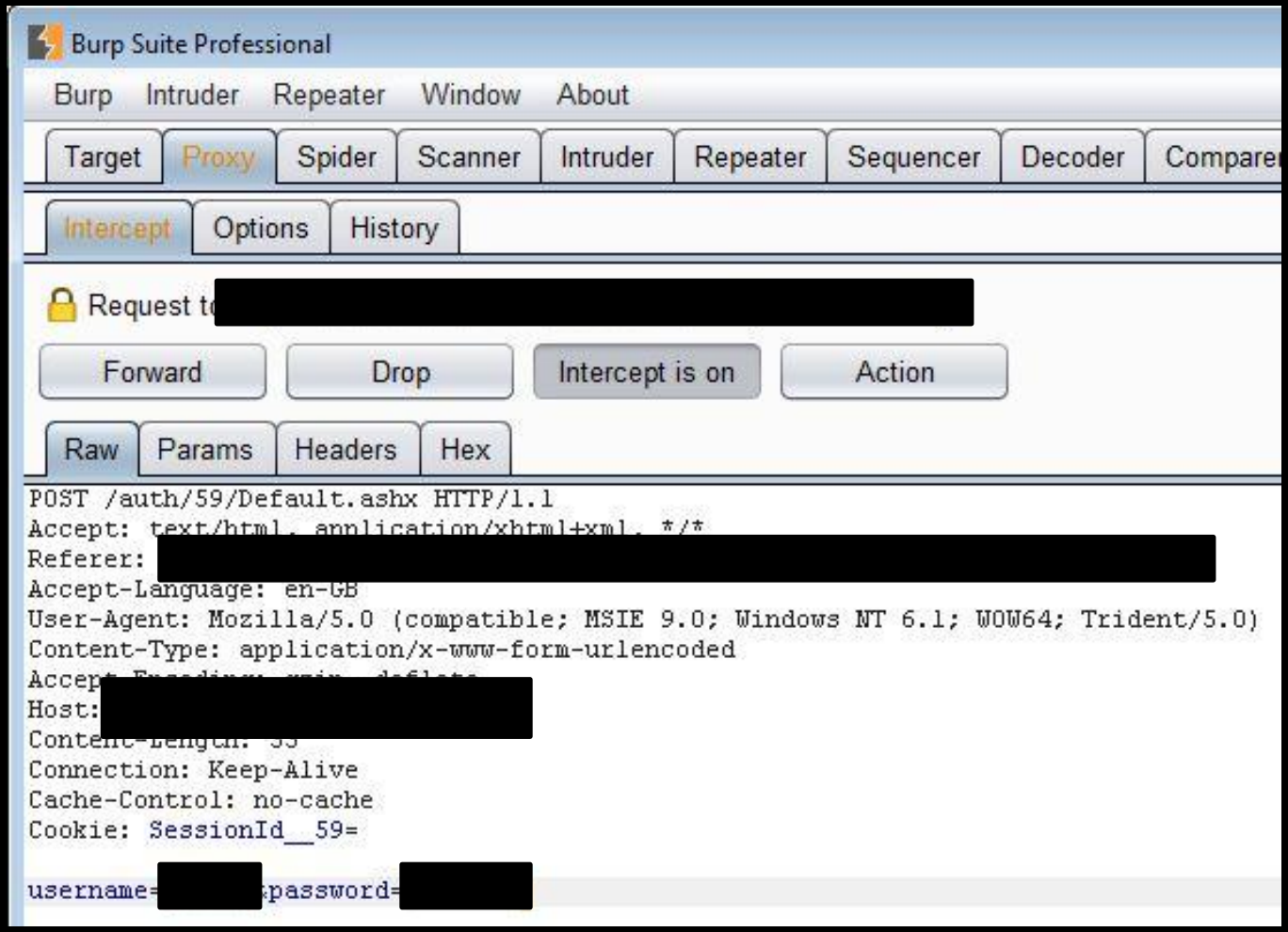
Filer, SQL og logger

Nettverkstrafikk

Ekstern tjeneste (Web Service)


DroidBoxTests.apk
crypto
net write
net read
net open
file write
file read
leak
sms
call
activity
10
15
20
25
30
timestamp


app_database 2012-05-18 12:42 drwxrwxrwx
cache 2012-05-18 12:42 drwxrwxrwx
webviewCacheChromium 2012-05-21 11:18 drwxrwxrwx
data_0 45056 2012-05-21 11:56 -rwxrwxrwx
data_1 270336 2012-05-21 11:56 -rwxrwxrwx
data_2 1056768 2012-05-21 11:19 -rwxrwxrwx
data_3 4202496 2012-05-21 11:18 -rwxrwxrwx
f_000001 27932 2012-05-18 12:44 -rwxrwxrwx
f_000002 103399 2012-05-21 11:18 -rwxrwxrwx
index 262512 2012-05-21 11:56 -rwxrwxrwx
webviewCacheChromiumStaging 2012-05-18 12:42 drwxrwxrwx
databases 2012-05-21 11:55 drwxrwxrwx


Burp Suite Professional
Burp Intruder Repeater Window About
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compare
Intercept Options History
Request t
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /auth/59/Default.ashx HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer:
Accept-Language: en-GB
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Content-Type: application/x-www-form-urlencoded
Host:
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: SessionId__59=
password=

Statisk analyse

Kildekoderevisjon

Reverse engineering

Eksterne bibliotek

apktool

dex2jar + jd-gui

```
<string name="secret_ssl_password"                                                    /string>
<string name="secret_preferences_key">
org.apache.harmony.xnet.provider.jsse.OpenSSLSocketImpl$</string>
```

```
static
{
  char[] arrayOfChar = new char[11];
  arrayOfChar[0] = [redacted]
  arrayOfChar[1] = [redacted]
  arrayOfChar[2] = [redacted]
  arrayOfChar[3] = [redacted]
  arrayOfChar[4] = [redacted]
  arrayOfChar[5] = [redacted]
  arrayOfChar[6] = [redacted]
  arrayOfChar[7] = [redacted]
  arrayOfChar[8] = [redacted]
  arrayOfChar[9] = [redacted]
  arrayOfChar[10] = [redacted]
  SEKRIT = arrayOfChar;
}

/** Called when the activity is
@Override
public void onCreate(Bundle sav
    super.onCreate(savedInstanc
    setContentView(R.layout.ma
    String password = [redacted]
    String username = [redacted]
    System.out.println("BEFORE
    System.out.println("Passwor
    System.out.println("Username: " + decrypt(username));
    System.out.println("AFTER");
}

public String decrypt(String paramString)
{
 try{
     byte[] arrayOfByte = Base64.decode(paramString, 0);

      SecretKey localSecretKey = SecretKeyFactory.getInstance("PBEWithMD5AndDES").generateSecret(new PBEKeySpec(SEKRIT));
      Cipher localCipher = Cipher.getInstance("PBEWithMD5AndDES");
      String salt = Settings.Secure.getString(this.context.getContentResolver(), "android_id");
      localCipher.init(Cipher.DECRYPT_MODE, localSecretKey, new PBEParameterSpec(salt.getBytes("utf-8"), 20));

      return new String(localCipher.doFinal(arrayOfByte), "utf-8");
```

dalvikvm	Debugger has detached; object registry
TabletStat...	lights on
dalvikvm	GC_EXPLICIT freed 10K, 6% free 6197K/6
System.out	BEFORE
System.out	Password: [redacted]
System.out	Username: [redacted]
System.out	AFTER
TLINE	new: android.text.TextLine@408379b0
dalvikvm	GC_EXPLICIT freed <1K, 6% free 6197K/6

Har utviklere tatt lærdom?

OWASP Top 10 2007	OWASP Top 10 2010	OWASP Top 10 Mobile Risks
Cross Site Scripting (XSS)	Injection	Insecure Data Storage
Injection Flaws	Cross-Site Scripting (XSS)	Weak Server Side Controls
Malicious File Execution	Broken Authentication and Session Management	Insufficient Transport Layer Protection
Insecure Direct Object Reference	Insecure Direct Object References	Client Side Injection
Cross Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Poor Authorization and Authentication
Information Leakage and Improper Error Handling	Security Misconfiguration	Improper Session Handling
Broken Authentication and Session Management	Insecure Cryptographic Storage	Security Decisions Via Untrusted Inputs
Insecure Cryptographic Storage	Failure to Restrict URL Access	Side Channel Data Leakage
Insecure Communications	Insufficient Transport Layer Protection	Broken Cryptography
Failure to Restrict URL Access	Unvalidated Redirects and Forwards	Sensitive Information Disclosure

Takk for oppmerksomheten!