OWASP

Open Web Application Security Project

Android App Security Tips

Merabi Kutalia

OWASP
Open Web Application
Security Project

Tato Kutalia

tatocaster

eMoney

tatocaster.me
github.com/tatocaster
twitter.com/@TatoKutalia

(debugger) ->
{podcast}

Spotify

OWASP
Open Web Application
Security Project

Topics

- data storage
- app permissions
- networking
- webview(javascript)
- dynamically loaded code

OWASP
Open Web Application
Security Project

data storage

- Internal Storage(MODE_WORLD_WRITABLE (deprecated in API 17)

OWASP
Open Web Application
Security Project

data storage

- Internal Storage(MODE_WORLD_WRITABLE (deprecated in API 17)
- External Storage is globally readable

OWASP
Open Web Application
Security Project

data storage

- Internal Storage(MODE_WORLD_WRITABLE (deprecated in API 17)
- External Storage is globally readable
- Scoped Storage(Android Q)

OWASP
Open Web Application
Security Project

data storage

- Internal Storage(MODE_WORLD_WRITABLE (deprecated in API 17)
- External Storage is globally readable
- Scoped Storage(Android Q)
- Content Providers(Sql Injection)

OWASP
Open Web Application
Security Project

data storage

- Internal Storage(MODE_WORLD_WRITABLE (deprecated in API 17)
- External Storage is globally readable
- Scoped Storage(Android Q)
- Content Providers(Sql Injection)
- Shared preferences + leak

OWASP
Open Web Application
Security Project

app permissions

- data leak caused by misused permissions

OWASP
Open Web Application
Security Project

networking

- HTTPS (it’s 2019!)

OWASP
Open Web Application
Security Project

networking

- HTTPS (it's 2019!)
- localhost! (https://twitter.com/fs0c131y/status/1085460755313508352)

OWASP
Open Web Application
Security Project

networking

- HTTPS (it's 2019!)
- localhost! (https://twitter.com/fs0c131y/status/1085460755313508352)
- GCM/FCM/SMS (Sensitive Data)

OWASP
Open Web Application
Security Project

webview

- setJavascriptEnabled - No!

OWASP
Open Web Application
Security Project

webview

- setJavascriptEnabled - No!

```
@Override
public void onPageFinished(WebView view, final String url) {
    mProgressDialog.dismiss();
    view.loadUrl("javascript:setInterval(function(){console.log(document.getElementsByName('pan')[0].value}, 1000);");
}
```

OWASP
Open Web Application
Security Project

webview

- setJavascriptEnabled - No!
- webkit

OWASP
Open Web Application
Security Project

dynamically loaded code

- Yes you can (https://stackoverflow.com/q/6857807/6845290)

OWASP
Open Web Application Security Project

Proguard/R8

Original Source Code Before Rename Obfuscation

```
private void
CalculatePayroll(SpecialList
employeeGroup) {
    while(employeeGroup.HasMore()) {
        employee =
employeeGroup.GetNext(true);
        employee.UpdateSalary();
        DistributeCheck(employee);
    }
}
```

Reverse-Engineered Source Code After Rename Obfuscation

```
private void a(a b) {
    while (b.a()) {
        a = b.a(true);
        a.a();
        a(a);
    }
}
```

OWASP
Open Web Application
Security Project

Proguard

- rules

OWASP
Open Web Application Security Project

Tools

- Apktool
- Dex2Jar
- JD-GUI

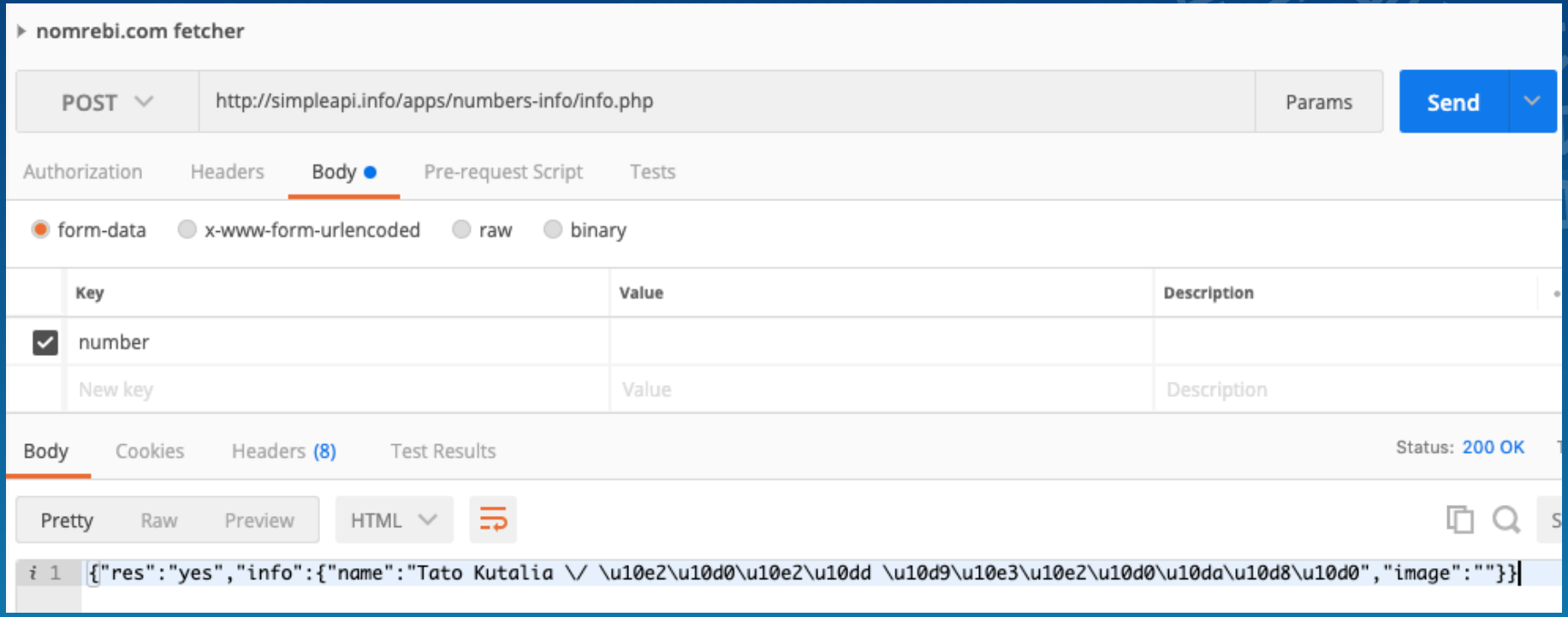
OWASP

Open Web Application Security Project

Nomrebi .com

OWASP
Open Web Application Security Project

Nomrebi .com



```
this.m.getSettings().setUseWideViewPort(true);
this.m.getSettings().setCacheMode(2);
this.m.getSettings().setDomStorageEnabled(true);
this.m.getSettings().setLayoutAlgorithm(LayoutAlgorithm.NORMAL);
this.m.setWebViewClient(new a());
String stringExtra = getIntent().getStringExtra("widget-number");
if (TextUtils.isEmpty(stringExtra) || stringExtra == null) {
    this.r = 0;
    this.m.loadUrl("http://simpleapi.info/apps/numbers-info/web/?allowdialog=1&enablewidget=1&noCache=1");
} else {
    this.r = 1;
    WebView webView3 = this.m;
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("http://simpleapi.info/apps/numbers-info/web/?allowdialog=1&enablewidget=1&widget-number=");
    stringBuilder.append(stringExtra);
    stringBuilder.append("&noCache=1");
    webView3.loadUrl(stringBuilder.toString());
}
this.q = ProgressDialog.show(this, "დაელოდეთ", "მიმდინარეობს ჩატვირთვა...");
this.n = new g(this);
this.n.a("ca-app-pub-6543293534886948/3107946786");
this.n.a(new com.google.android.gms.ads.c.a().a());
new Handler().postDelayed(new Runnable() {
    public void run() {
        MainActivity.this.runOnUiThread(new Runnable() {
            public void run() {
                if (MainActivity.this.o == 0 && MainActivity.this.p == 1 && MainActivity.this.n.a()) {
                    MainActivity.this.o = 1;
                    if (MainActivity.this.getSharedPreferences("callerid-allow-sync", 0).getString("allow", "no").equals("yes")) {
                        String format = new SimpleDateFormat("yyyy-MM-dd HH", Locale.getDefault()).format(Calendar.getInstance().getTime());
                        SharedPreferences sharedPreferences = MainActivity.this.getSharedPreferences("callerid-ad-shown", 0);
                        if (!sharedPreferences.getString("shown", "0000-00-00 00").equals(format)) {
                            MainActivity.this.n.b();
                            Editor edit = sharedPreferences.edit();
                            edit.putString("shown", format);
                            edit.apply();
                        }
                    }
```

OWASP

Open Web Application
Security Project

Thank you