

Выполнение статического анализа мобильного приложения

--

Для начала работ вам понадобится:

- *docker*
- *k3d*
- *kubectl*

Подробная установка требуемых инструментов подробно рассмотрена на предыдущих уроках

--

Часть 1. Создание кластера k3d и развертывание в нем инструмента mobsf

Создадим кластер k3d:

```
$ k3d cluster create mycluster
```

```
filipp@filipp-notebook:~$ k3d cluster create mycluster
INFO[0000] Prep: Network
INFO[0000] Created network 'k3d-mycluster'
INFO[0000] Created volume 'k3d-mycluster-images'
INFO[0000] Starting new tools node...
INFO[0000] Starting Node 'k3d-mycluster-tools'
INFO[0001] Creating node 'k3d-mycluster-server-0'
INFO[0001] Creating LoadBalancer 'k3d-mycluster-serverlb'
INFO[0001] Using the k3d-tools node to gather environment information
INFO[0001] HostIP: using network gateway 172.22.0.1 address
INFO[0001] Starting cluster 'mycluster'
INFO[0001] Starting servers...
INFO[0001] Starting Node 'k3d-mycluster-server-0'
INFO[0006] All agents already running.
INFO[0006] Starting helpers...
INFO[0006] Starting Node 'k3d-mycluster-serverlb'
INFO[0012] Injecting '172.22.0.1 host.k3d.internal' into /etc/hosts of all nodes...
INFO[0012] Injecting records for host.k3d.internal and for 2 network members into CoreDNS con
INFO[0013] Cluster 'mycluster' created successfully!
INFO[0013] You can now use it like this:
kubectl cluster-info
```

Кластер успешно создан, создадим в нем неймспейс для инструмента mobsf:

```
$ kubectl create ns mobsf
```

```
filipp@filipp-notebook:~$ kubectl create ns mobsf
namespace/mobsf created
```

В созданном неймспейсе создадим deployment на основе образа mobsf:v3.1.1:

```
$ kubectl create deployment mobsf
--image=opensecurity/mobile-security-framework-
mobsf:v3.1.1 -n mobsf
```

```
filipp@filipp-notebook:~$ kubectl create deployment mobsf --image=opensecu
rity/mobile-security-framework-mobsf:v3.1.1 -n mobsf
deployment.apps/mobsf created
```

Создадим службу для деплоймента mobsf:

```
$ kubectl expose deployment mobsf --port=8000 --
type=NodePort -n mobsf
```

```
filipp@filipp-notebook:~$ kubectl expose deployment mobsf --port=8000 --type=NodePort
-n mobsf
service/mobsf exposed
```

Дождемся, когда pods в неймспейсе mobsf будут успешно созданы и запущены:

```
$ kubectl get pods -n mobsf -w
```

```
filipp@filipp-notebook:~$ kubectl get pods -n mobsf -w
NAME                                READY   STATUS             RESTARTS   AGE
mobsf-5db69649fc-4fskn             0/1     ContainerCreating   0           3m52s
mobsf-5db69649fc-4fskn             1/1     Running             0           4m3s
```

Когда под успешно создан, получим external-ip службы traefik и nodeport службы mobsf, чтобы сформировать url веб-интерфейса:

```
$ kubectl get svc traefik -n kube-system
```

```
filipp@filipp-notebook:~$ kubectl get svc traefik -n kube-system
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
traefik	LoadBalancer	10.43.71.45	172.22.0.3	80:31354/TCP,443:32234/TCP	17m

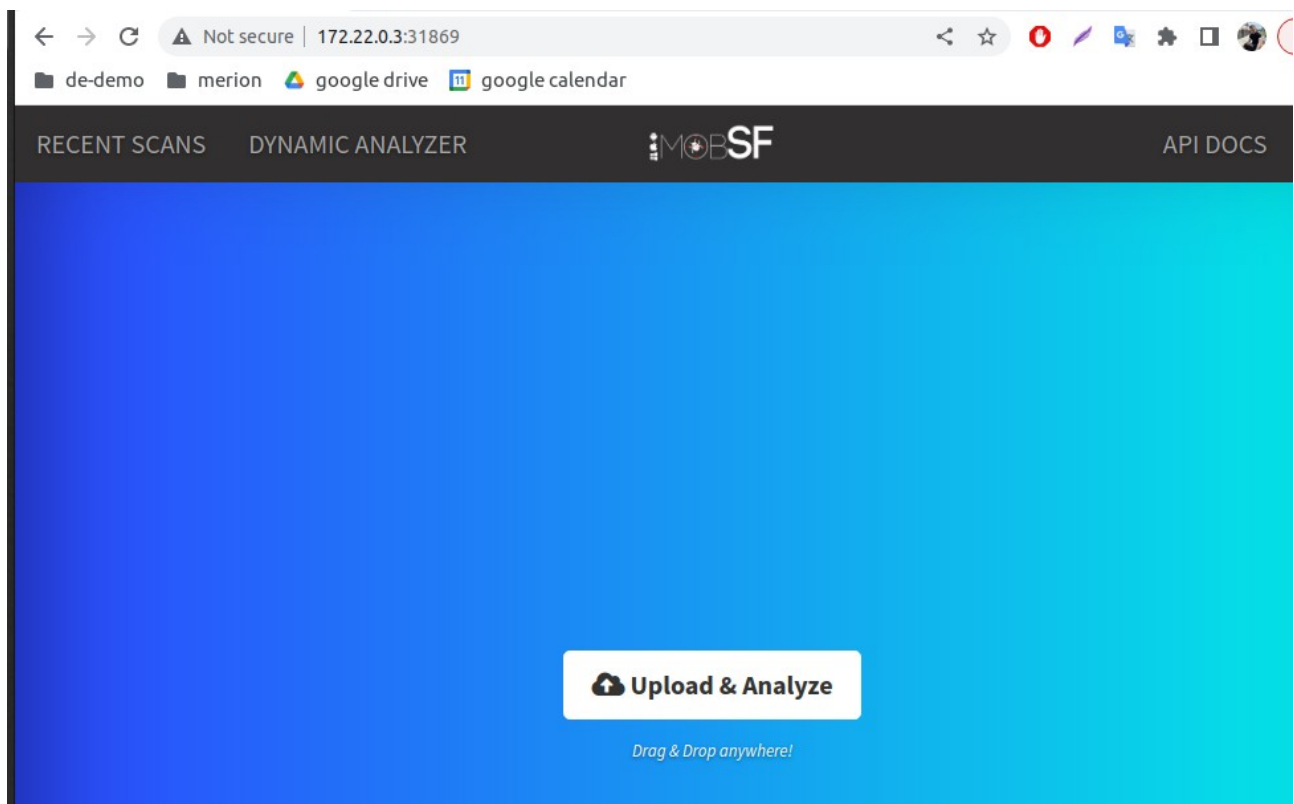
```
$ kubectl get svc mobsf -n mobsf
```

```
filipp@filipp-notebook:~$ kubectl get svc mobsf -n mobsf
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
mobsf	NodePort	10.43.167.64	<none>	8000:31869/TCP	16m

В браузере перейдем в веб-интерфейс инструмента mobsf:

browser: `http://<traefik-external-ip>:<mobsf-nodeport>`



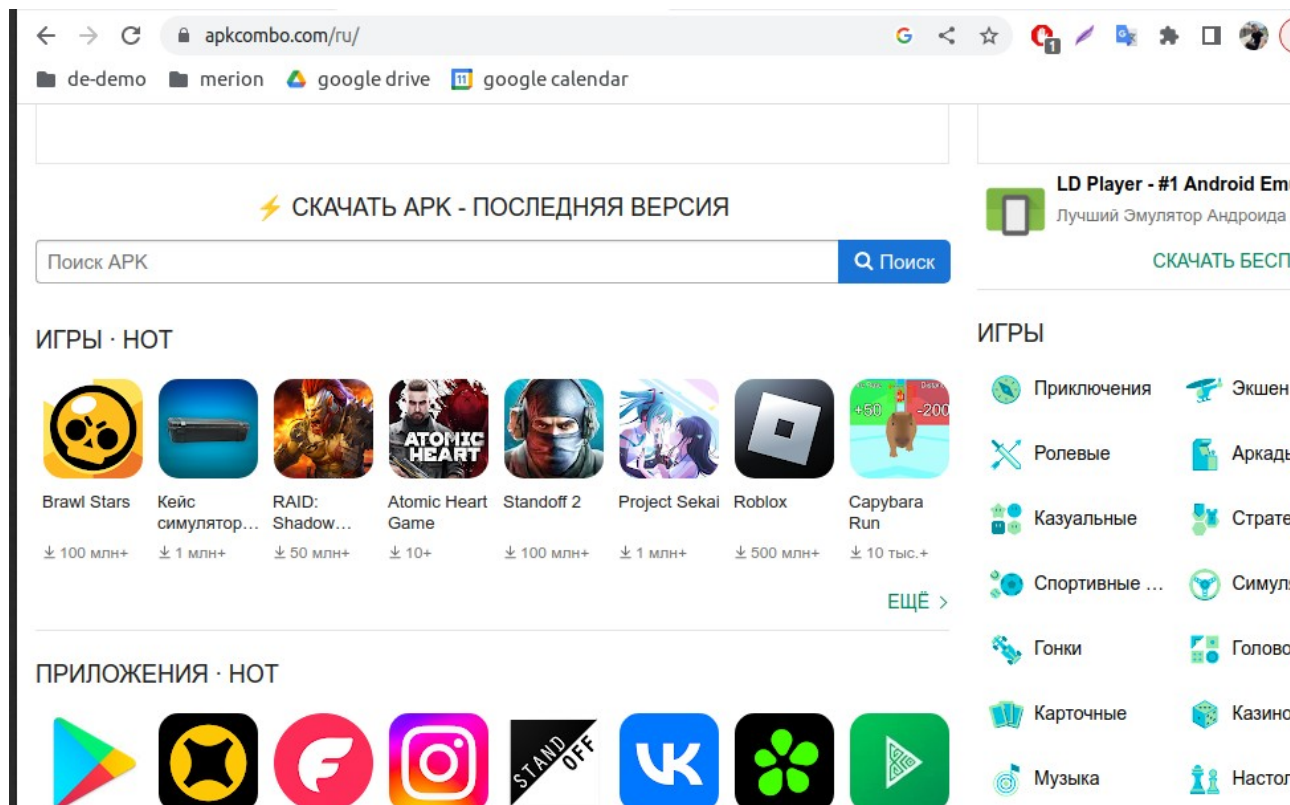
Веб-интерфейс доступен - инструмент готов к работе

--

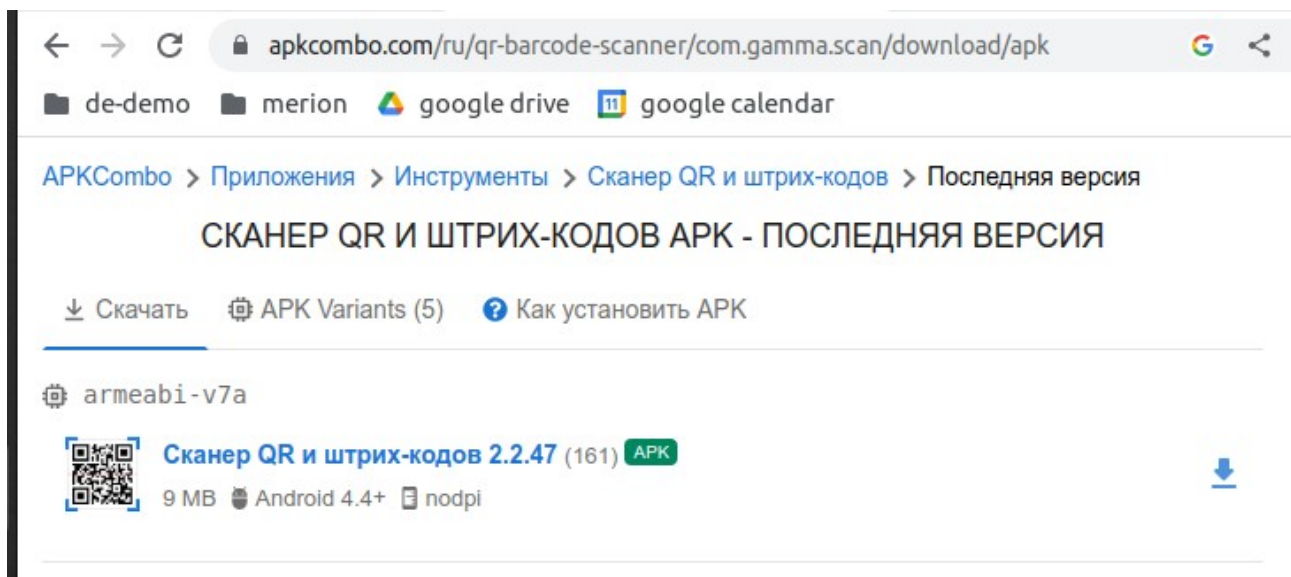
Часть 2. Получение артефакта мобильной сборки и проведение статического анализа

Воспользуемся поиском на портале бесплатных артефактов мобильных сборок (например, ресурс apkcombo.com):

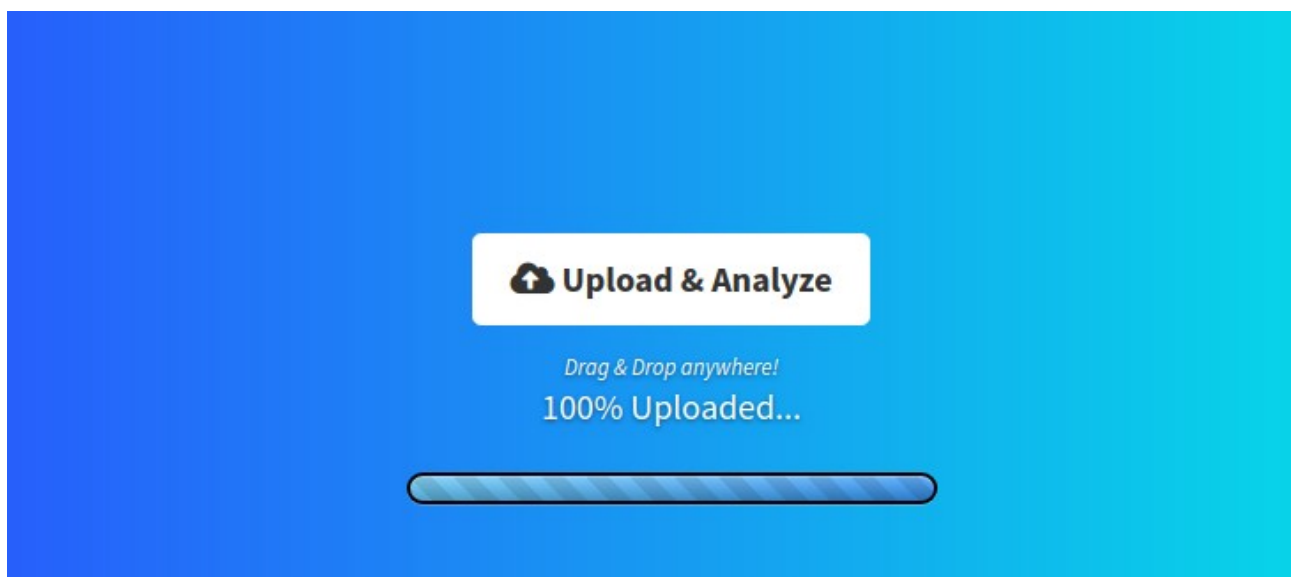
browser: <https://apkcombo.com/ru/>



Для эксперимента лучше выбирать артефакты, имеющие минимальный объем (до 30 мегабайт). Можно воспользоваться категорией "Инструменты" в аркcombo. В нашем случае будем использовать Сканер QR-кодов - скачаем его последнюю версию:



Перейдем в веб-интерфейс инструмента mobsf и запустим сканирование. Можно указать артефакт через кнопку "Upload & Analyze", или воспользоваться drag-and-drop:



Дождемся полной загрузки артефакта, после чего будет выполнено его статический анализ. По завершению сканирования вы сможете ознакомиться с отчетом:

← → ↻ Not secure | 172.22.0.3:31869/StaticAnalyzer/?name=Сканер%20QR%20и%20шт... ☆ 🔍 📄 📱 📅 📁 Update

de-demo merion google drive google calendar


MobSF

Static Analyzer

- Information
- Scan Options
- Signer Certificate
- Permissions
- Binary Analysis
- Android API
- Browsable Activities
- Security Analysis
- Malware Analysis
- Reconnaissance
- Components
- PDF Report
- Print Report

RECENT SCANS STATIC ANALYZER DYNAMIC ANALYZER API DOCS ABOUT Search MD5

APP SCORES FILE INFORMATION APP INFORMATION

 **File Name** Сканер QR и штрих-кодов_2.2.47_apkcombo.com.apk
Size 9.5MB
MD5 1b56133a95176fdd10e2f5b971c7bd37
SHA1 c108a818aa877ec582436bd5595654bfb753dd85
SHA256 16bb34880c188571b38defb263412776eb915d879a3e264090349088c9872f3a

Average CVSS 5.3
Security Score 55/100
Trackers Detection 3/428

App Name QR & Barcode Scanner
Package Name com.gamma.scan
Main Activity com.gamma.barcodeapp.ui.BarcodeCaptureActivity
Target SDK 33 **Min SDK** 19 **Max SDK**
Android Version Name 2.2.47
Android Version Code 161

5 ACTIVITIES View

12 SERVICES View

10 RECEIVERS View

7 PROVIDERS View

Exported Activities 0

Exported Services 1

Exported Receivers 1

Exported Providers 0

--

Часть 3. Сравнительный анализ двух артефактов разных версий одного мобильного сборки

Вернемся к источнику артефактов мобильных сборок и скачаем тот же инструмент (в нашем случае сканер QR-кодов) но предыдущей версии:

ПРЕДЫДУЩИЕ ВЕРСИИ



Сканер QR и штрих-кодов 2.2.47 [APK](#) [XAPK](#)

20 янв. 2023 г. · Android 4.4+



Сканер QR и штрих-кодов 2.2.45 [APK](#) [XAPK](#)

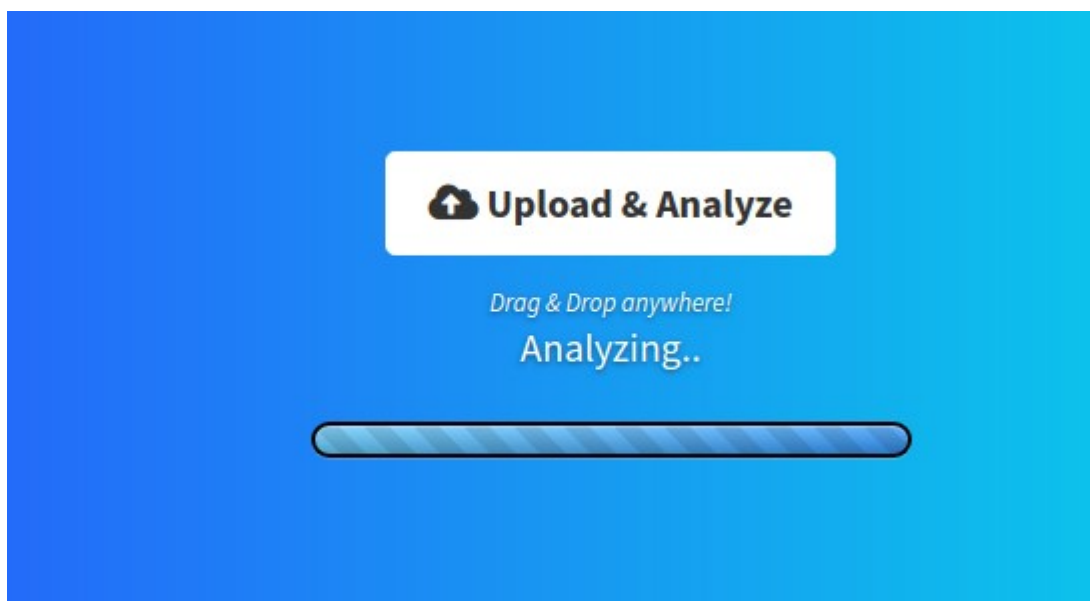
26 окт. 2022 г. · Android 4.4+

















Сканер QR и штрих-кодов 2.2.44 [APK](#) [XAPK](#)

14 окт. 2022 г. · Android 4.4+

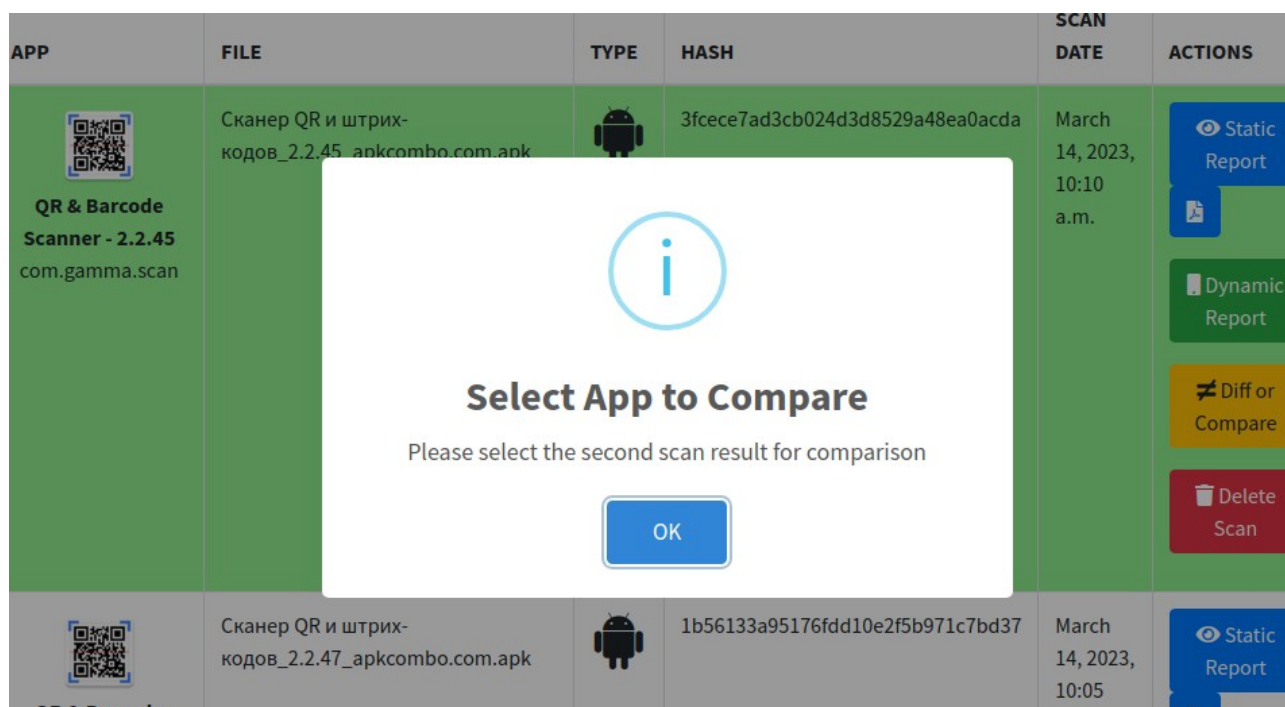
Перейдем в веб-интерфейс инструмента mobsf и запустим сканирование предыдущей версии артефакта:



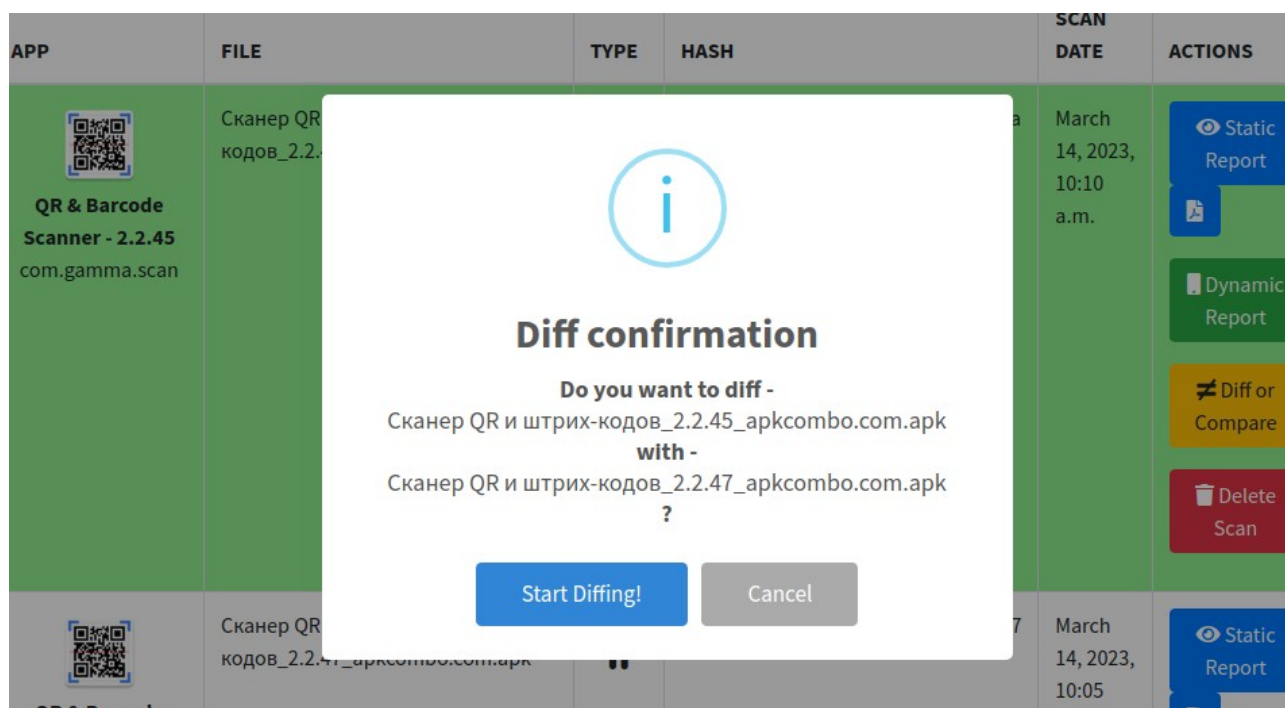
После завершения сканирования перейдем на вкладку "Recent scans":

 Recent Scans					
APP	FILE	TYPE	HASH	SCAN DATE	ACTIONS
 QR & Barcode Scanner - 2.2.45 com.gamma.scan	Сканер QR и штрих-кодов_2.2.45_apkcombo.com.apk		3fcede7ad3cb024d3d8529a48ea0acda	March 14, 2023, 10:10 a.m.	<div>  Static Report  </div> <div>  Dynamic Report </div> <div>  Diff or Compare </div> <div>  Delete Scan </div>
 QR & Barcode Scanner - 2.2.47 com.gamma.scan	Сканер QR и штрих-кодов_2.2.47_apkcombo.com.apk		1b56133a95176fdd10e2f5b971c7bd37	March 14, 2023, 10:05 a.m.	<div>  Static Report  </div> <div>  Dynamic Report </div> <div>  Diff or Compare </div>

Нажмем кнопку "Diff or compare" на одном из артефактов и укажем оставшийся в качестве второго элемента для проведение сравнительного анализа:



Нажмем кнопку "Start Diffing!":



По результатам сравнения проведем анализ общих и частных уязвимостей в обеих версиях:

Comparing com.gamma.scan - 2.2.45 and com.gamma.scan - 2.2.47

APP INFORMATION

	com.gamma.scan - 2.2.45	com.gamma.scan - 2.2.47
File name	Сканер QR и штрих-кодов_2.2.45_apkcombo.com.apk	Сканер QR и штрих-кодов_2.2.47_apkcombo.com.apk
MD5	3fcede7ad3cb024d3d8529a48ea0acda	1b56133a95176fdd10e2f5b971c7bd37
Size	9.36MB	9.5MB
Certificate	Subject: CN=QR & Barcode Scanner	Subject: CN=QR & Barcode Scanner

ICON

com.gamma.scan - 2.2.45	com.gamma.scan - 2.2.47
	

COMPONENTS

	ACTIVITIES	EXPORTED ACTIVITIES	SERVICES	EXPORTED SERVICES	RECEIVERS	EXPORTED RECEIVERS	PROVIDERS	EXPORTED PROVIDERS
com.gamma.scan - 2.2.45	5	0	12	1	10	1	7	0
com.gamma.scan - 2.2.47	5	0	12	1	10	1	7	0

В нашем случае новых замечаний и уязвимостей в новой версии по сравнению с предыдущей не обнаружено

--

Для завершения работ достаточно удалить кластер k3d:

```
$ k3d cluster delete mycluster
```

```
filipp@filipp-notebook:~$ k3d cluster delete mycluster
INFO[0000] Deleting cluster 'mycluster'
INFO[0002] Deleting cluster network 'k3d-mycluster'
INFO[0003] Deleting image volume 'k3d-mycluster-images'
INFO[0003] Removing cluster details from default kubeconfig...
INFO[0003] Removing standalone kubeconfig file (if there is one)...
INFO[0003] Successfully deleted cluster mycluster!
```
