Mobile App Security Scanner

by Code Creator

Private mobile application security analysis within your AWS account.

PLATFORM	SECURITY WORKSPACE	DEPLOYMENT	SUPPORTED SCOPE
Ubuntu LTS on Amazon EC2	MobSF (Mobile Security Framework)	Docker Compose + Caddy HTTPS	Static mobile app analysis

> **Authorized testing only.** Scan applications, packages, or source code you own or have permission to assess. Automated results support development and security review; they do not replace a manual penetration test, legal compliance review, or production certification.

01 Launch the EC2 instance

Recommended launch configuration

- Choose **m7i.xlarge** for initial use; select a larger instance for heavy scan workloads.
- Use the AMI root volume unless you need additional scan storage.
- Enable a public IPv4 address for automatic public-IP-based HTTPS setup.
- Select a new EC2 key pair and connect over SSH as **ubuntu**.

Security group inbound rules

PORT	PROTOCOL	SOURCE	PURPOSE
22	TCP	Your administrator IP only	SSH administration
80	TCP	0.0.0.0/0	HTTP redirect and certificate validation
443	TCP	0.0.0.0/0	Secure web workspace

Do not publicly expose ports **8000, 1337, or 5432**. MobSF and PostgreSQL remain behind the HTTPS reverse proxy.

02 Wait for first boot

The appliance generates customer credentials, detects its public IP, prepares its HTTPS hostname, starts PostgreSQL, MobSF, the scan worker and Caddy, and creates the customer login file. Allow several minutes.

```
mobile-security-scanner-status
```

Expected: first boot **complete** and HTTPS health **ok**.

Access your workspace

Use the fresh customer credentials created during first boot.

03 Retrieve your login information

```
cat /home/ubuntu/FIRST_LOGIN.txt
```

The file contains the workspace URL, administrator account, generated password, useful commands, security notes, and open-source notice link. The default administrator username is **ccadmin**.

04 Open the secure workspace

Open the URL shown in the login file, or display it with:

```
mobile-security-scanner-url
```

Typical URL format: https://PUBLIC-IP-WITH-DASHES.nip.io/

Sign in as **ccadmin** using the generated password. Change the administrator password after your first successful sign-in.

05 Run a static mobile app scan

1. Open the secure HTTPS workspace in your browser.
2. Sign in with the generated **ccadmin** credentials.
3. Upload an authorized **APK, AAB, IPA, APPX, JAR, AAR, SO, dylib**, or supported source archive.
4. Allow MobSF to complete its automated static analysis.
5. Review applicable findings, such as permissions, manifests, certificates, code issues, trackers, files, and security warnings.
6. Save or export the report for internal review.

> **Static analysis only.** This appliance does not include a configured Android emulator, iOS device, or separate dynamic-testing environment. Do not treat it as a ready-to-use dynamic-analysis lab.

06 Useful commands

TASK	COMMAND
Display the workspace URL	`mobile-security-scanner-url`
Check service and container health	`mobile-security-scanner-status`
Read customer login details	`cat /home/ubuntu/FIRST_LOGIN.txt`

Inspect Docker Compose services:

```
sudo docker compose --project-directory /opt/mobile-security-scanner \
--env-file /opt/mobile-security-scanner/.env \
-f /opt/mobile-security-scanner/compose.yaml ps
```

Operate securely

Operational guidance, open-source notices, and troubleshooting.

07 Stop and start behavior

After an EC2 stop/start, AWS may assign a different public IPv4 address unless you use an Elastic IP. The included network refresh service updates the public-IP-based hostname and the customer login file.

After the instance starts again, run `mobile-security-scanner-status` and retrieve the current URL if needed.

08 Security and data handling

- Uploaded packages and scan results remain on the EC2 instance and its attached EBS storage unless removed.
- Limit SSH access to trusted administrator IP addresses and use HTTPS for the web workspace.
- Change the generated administrator password after first sign-in.
- Analyze only applications and source code you are authorized to assess.
- Keep internal MobSF and database ports private; do not publish them directly.

09 Open-source notices

This product includes MobSF, distributed under the GNU General Public License. The AMI includes the corresponding license text, third-party notices, and MobSF source bundle.

Documentation and notices: `/usr/share/doc/mobile-security-scanner/`

MobSF source bundle: `/usr/share/mobile-security-scanner/source/`

Notice page: https://PUBLIC-IP-WITH-DASHES.nip.io/open-source-notices.html

10 Troubleshooting

ISSUE	WHAT TO CHECK
Browser cannot connect	Confirm the EC2 public IP and security group rules for HTTP and HTTPS.
Login file is missing	Wait for first boot; run `mobile-security-scanner-status`.
HTTPS certificate not ready	Ensure port 80 is reachable and the hostname matches the current public IP.
Login fails	Use **ccadmin** and the generated password from the customer login file; avoid extra spaces.
Large upload fails	Check instance resources and browser/network stability; choose a larger instance for heavy scans.
API access needed	Open the MobSF API page after signing in, then use the account-specific API key.

11 Support and learning resources

MobSF project

MobSF documentation and API

OWASP Mobile Application Security

AWS VPC security groups

AWS Marketplace AMI policies