### **🔹**Challenge Name****

"Hashira's Puzzle"

### **🔹**Vulnerability****

Insecure Storage & Weak Credentials Management

### **🔹**Details****

The application stores **admin credentials** in a **Base64-encoded** format in Firebase. The credentials are used for authentication, and once successfully decoded, access to a **hidden flag** is granted. However:

* The admin credentials are stored in **Base64 encoding**, which is a reversible encoding scheme.
* These credentials are **fetched from Firebase**, and if decoded correctly, allow access to the hidden flag.
* The flag is **XOR-encrypted** with the decoded admin credentials and logged instead of displayed on the UI.

By exploiting Firebase misconfigurations and decoding the credentials, you can retrieve the hidden flag.

### **🔹**Walkthrough****

1. **Extract the Base64-encoded admin credentials from Firebase.**
2. **Decode the Base64 credentials** to get the actual username and password.
3. **Use the decoded credentials** to fetch the hidden flag stored in Firebase.
4. **Check Logcat** for the flag, as it is logged rather than displayed in the UI.

### **🔹**Steps to Decrypt****

**Step 1: Extract Base64-encoded Admin Credentials**

If running on an emulator/rooted device, use **adb** to dump the Firebase database or access the misconfigured Firebase endpoint.

curl <https://your-firebase.firebaseio.com/credentials.json>

This would retrieve the **Base64-encoded admin credentials** from Firebase.

The expected output should look like:

{

"credentials": {

"admin\_access": "QWRtaW46cGFzc3dvcmQ="

},

"admin\_panel": {

"hidden\_flag": "G8KEY{APK\_R3v3r$3\_HunT3r}"

}

}

**Step 2: Decode Base64 Admin Credentials**

The **Base64-encoded credentials** are stored in admin\_access:

QWRtaW46cGFzc3dvcmQ=

Decode the string using:

echo "QWRtaW46cGFzc3dvcmQ=" | base64 -d

**Output:**

Admin:password

**Step 3: Fetch the Hidden Flag**

Use the decoded credentials (**Admin:password**) to access the **AdminFragment**.

The flag is **XOR-encrypted** with the decoded credentials and logged instead of displayed in the UI,

To view the flag, use **adb logcat** or analyze the decompiled APK to see where the flag is logged.

**Command to view Logcat output:**

adb logcat | grep FLAG

**Expected output:**

FLAG: G8KEY{APK\_R3v3r$3\_HunT3r}

### ****Flag Value****

### G8KEY{APK\_R3v3r$3\_HunT3r}

### **🔹 **Riddle****

“Through the valley, step with care,  
Where shadows of demons linger there.  
The blazing sword, in flame it’s forged,  
Unlock the code, the path’s emerged.

Decode the secrets, break the spell,  
And claim the sword where power dwells.”