Gandalf Interface

Install the application

# First one opens the URL in WebView and Second One loads some contents on local HTML

Graphical user interface, text, application, Teams

Description automatically generated

# When you choose Device Information, it say try harder with other interfaces ,



# Reverse the APK file and observe the source code

There is “callcrypt” Javascript Interface used to request for flag

Graphical user interface, text, application

Description automatically generated

All the interface can be listed using remote debugging on chrome

chrome://inspect

Graphical user interface, text, application, email

Description automatically generated

# Now once you have remote debugging access you can list interface and try to access

MyInterface.callcrypt("test")

A screenshot of a computer

Description automatically generated with medium confidence

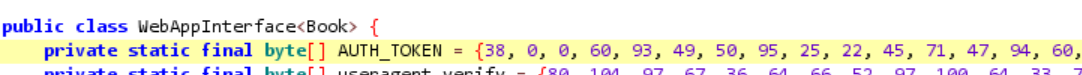
Which output as “Your are on right track Try Harder for flag”

Graphical user interface, application

Description automatically generated

# Further analysis of source code reveals that

# To obtain the parameter we need to XOR of byte array of AuthToken and Salt



Graphical user interface, text, application, email

Description automatically generated

Which can be done with Writing manual Code

import java.nio.charset.StandardCharsets;

import java.util.Arrays;

public class Main

{

public static void main(String[] args) {

byte[] bArr = "RheO5PB6mfL5N3YBH45e5XuCEaWpvWUFESqTYnZk".getBytes(StandardCharsets.UTF\_8);

byte[] AUTH\_TOKEN={38,0,0,60,93,49,50,95,25,22,45,71,47,94,60,54,45,70};

byte[] bArr2 = new byte[AUTH\_TOKEN.length];

for (int i = 0; i < AUTH\_TOKEN.length; i++) {

bArr2[i] = (byte) (AUTH\_TOKEN[i] ^ bArr[i % bArr.length]);

}

String s = new String(bArr2);

System.out.println(s);

}

}

And we will get output the parameter

‘theshapitparameter’

A screenshot of a computer

Description automatically generated

Further upon sending the Parameter using Interface we get the flag as below

Graphical user interface, text, application

Description automatically generated