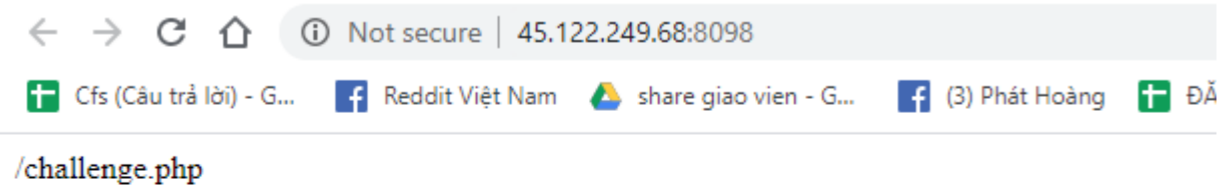


Tunt Robot

Solver: An Võ & reviven&cod201

Đầu challenge, tụi mình vào web thì gặp ntn...



Không biết index còn gì khác không, thôi cứ vào thử

Correct answers continuously: 0

I think you can solve $92+41-77+69+12*97+92-96+72*28-79-48*60+33*9*$

Okie , đây là một chall yêu cầu tính toán đến lúc nào đó sẽ nhả flag(tụi mình nghĩ vậy)

An Võ & revirven đảm nhận phần xử lý chuỗi và tính toán, mình đảm nhận phần send/receive

(Code trong repo writeups của team- folder CNSC3)

```
admin@ThanhPN: /mnt/e/events/cnsc3/web 1
This is data
50-83+89*79*33-54*62*26*47+64-76*44*28*57*39*56*9*46*47
-226803627433730
-----

b'<!DOCTYPE html><h1>Correct answers continuously: 199 <h1><br>Solve this 97+1-87+90+61+37*20-7*42*27+13*77-48 awww<form
action="/challenge.php" method=post><input type=text name=result><input type=submit></form>\n'
This is data
97+1-87+90+61+37*20-7*42*27+13*77-48
-6083
-----

b'<!DOCTYPE html><h1>Correct answers continuously: 200 <h1><br>I think you can solve Your flag: R0b0t!_1s_th4t_u?_1+2_3
get flag~~~~<form action="/challenge.php" method=post><input type=text name=result><input type=submit></form>\n'
This is data
00141+23
164
-----

Traceback (most recent call last):
  File "asas.py", line 108, in <module>
    data = soup.h1.h1.text
AttributeError: 'NoneType' object has no attribute 'h1'
root@ThanhPN:/mnt/e/events/cnsc3/web 1#
```

We won.

Source review :)

Solver: cod201

Chall này cho một file apk .-. Giải nén xem có gì nào

This PC > Downloads > helloworld (1) >

Name	Date modified	Type	Size
assets	8/11/2020 12:21 AM	File folder	
META-INF	8/11/2020 12:21 AM	File folder	
res	8/11/2020 12:21 AM	File folder	
AndroidManifest.xml	8/11/2020 12:21 AM	XML Document	3 KB
classes.dex	8/11/2020 12:21 AM	DEX File	236 KB
resources.arsc	8/11/2020 12:21 AM	ARSC File	4 KB

Type: DEX File
Size: 235 KB
Date modified: 8/11/2020 12:21 AM

Dùng link này <http://www.javadecompilers.com/apk> để decompile file dex, sẽ ra như thế này

Decompilation Results

Decompilation Results

File Name: classes.dex
Decompiler: jadx
Job status: Done.

Save

Twitter Facebook Stumbleupon LinkedIn

<> classes.dex

resources	folder
sources	folder

Mất một lúc để mò thì mình thấy một file khả nghi

Decompilation Results



Decompilation Results

File Name: classes.dex
Decompiler: jadx
Job status: Done.

 Save

[Twitter](#) [Facebook](#) [Stumbleupon](#) [LinkedIn](#)

`</> classes.dex > sources > com > tkyaji > cordova`

 ..	folder
 DecryptResource.java	.java



Mở ra thì.. Eureka

```
import org.apache.cordova.LOG;

public class DecryptResource extends CordovaPlugin {
    private static final String CRYPT_IV = "WIU8k71fDAspR8Ie";
    private static final String CRYPT_KEY = "nFwsAczxEZAs1QPf1lFA5eOWPg2TgvhF";
    private static final String[] EXCLUDE_FILES = new String[0];
    private static final String[] INCLUDE_FILES = {"\\.\\.(htm|html|js|css)$"};
    private static final String TAG = "DecryptResource";

    public Uri remapUri(Uri uri) {
        if (uri.toString().indexOf("/+++/") > -1) {
            return toPluginUri(uri);
        }
        return uri;
    }

    public OpenForReadResult handleOpenForRead(Uri uri) throws IOException {
        String uriStr = fromPluginUri(uri).toString().replace("/+++", "/").split("\\?")[0];
        OpenForReadResult readResult = this.webView.getResourceApi().openForRead(Uri.parse(uriStr), true);
        if (!isCryptFiles(uriStr)) {
            return readResult;
        }
        BufferedReader br = new BufferedReader(new InputStreamReader(readResult.inputStream));
        StringBuilder strb = new StringBuilder();
        while (true) {
            String line = br.readLine();
            if (line == null) {
                break;
            }
            strb.append(line);
        }
        br.close();
        byte[] bytes = Base64.decode(strb.toString(), 0);
        LOG.m0d(TAG, "decrypt: " + uriStr);
        ByteArrayInputStream byteInputStream = null;
        try {
            SecretKeySpec secretKeySpec = new SecretKeySpec(CRYPT_KEY.getBytes("UTF-8"), "AES");
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
            cipher.init(2, secretKeySpec, new IvParameterSpec(CRYPT_IV.getBytes("UTF-8")));
            ByteArrayOutputStream bos = new ByteArrayOutputStream();
            bos.write(cipher.doFinal(bytes));
            byteInputStream = new ByteArrayInputStream(bos.toByteArray());
        } catch (Exception ex) {
            LOG.m3e(TAG, ex.getMessage());
        }
        return new OpenForReadResult(readResult.uri, byteInputStream, readResult.mimeType, readResult.length, readResult.assetFd);
    }

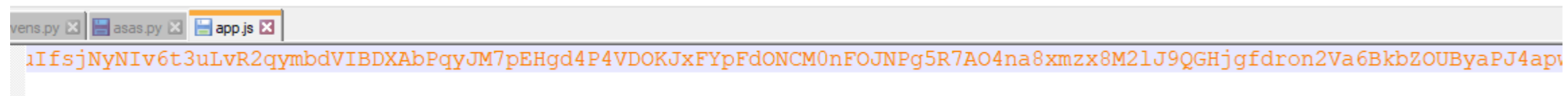
    private boolean isCryptFiles(String uri) {
        String checkPath = uri.replace("file:///android_asset/www/", "");
        if (hasMatch(checkPath, INCLUDE_FILES) && !hasMatch(checkPath, EXCLUDE_FILES)) {
            return true;
        }
    }
}
```

Tất cả nội dung trong www được mã hóa bằng AES-CBC, có cả IV với KEY

Nội dung trong www như thế này

name	date modified	type	size
cordova-js-src	8/11/2020 12:21 AM	File folder	
css	8/11/2020 12:21 AM	File folder	
img	8/11/2020 12:21 AM	File folder	
js	8/11/2020 12:21 AM	File folder	
cordova.js	8/11/2020 4:14 PM	JavaScript File	73 KB
cordova_plugins.js	8/11/2020 12:21 AM	JavaScript File	1 KB
index.html	8/11/2020 4:13 PM	Chrome HTML Do...	2 KB

Nội dung trước khi giải mã:



Dùng tool decrypt AES với từng file, thì ta sẽ tìm ra flag (file app.js)

The screenshot shows an online tool titled 'aes-256-cbc encrypt & decrypt online'. The 'supported encryptions' dropdown menu is set to 'aes-256-cbc'. The tool has two input fields for text. The left field contains the following JavaScript code:

```
1<[<^<d< ]% o){
  document.getElementById("hi").innerText = "Hi
"+document.getElementById("name").value+"!";
}
// comment 2020
// sha1(h3ll0_h0mi3s_nic3_t0_m33t_y0u_!)
```

The right field contains the obfuscated string from the previous image: `syJD1/1W7zOyxKVLClOQVs1Zafp0Bd2FogddDSXKI+tOpCcm317eMbS5PO8A+13ofBule6Lvulf sjNyNlv6t3uLvR2qymbdVIBDXAbPqyJM7pEHgd4P4VDOKJxFYpFdONCM0nFOJNPg5R7AO4na8xmzx8M2lJ9QGHjgfdron2Va6BkbZOUByaPJ4apwXpaKFI+elwFi9c0KbRG63+fy/KUd3CTxIBnl3ce9fOzUi9PnNensWYoxY1WVIX4OcUySs`. Below the input fields is a text box containing the flag: `nFwsAczxEZAs1QPF1lfA5eOWPg2TgvhF`. At the bottom, there are two green buttons: 'Encrypt string →' and '← Decrypt string'.

