به نام خداوند متعال

لا نِعْمَةَ اَهْنَاءُ مِنَ الاَْمْنِ .
هیچ نعمتی گواراتر 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

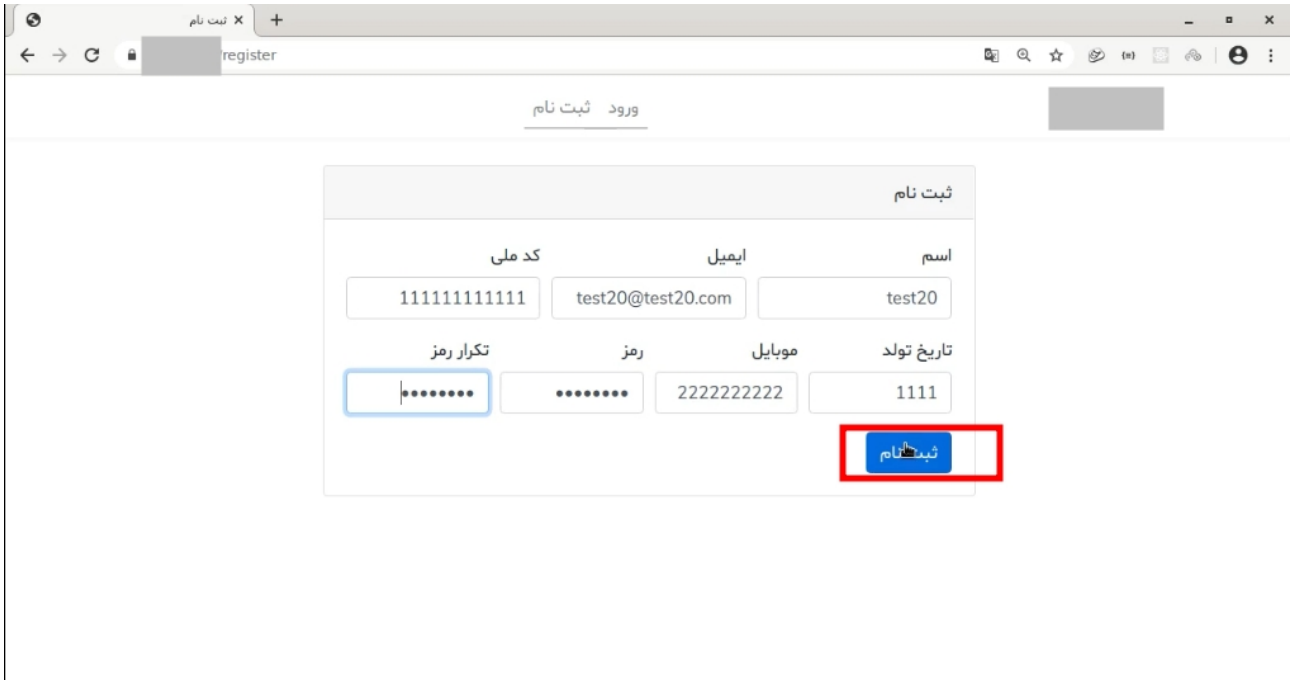
مقدمه :

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 کاملا واقعی در کنار هکر قدم به قدم با طرز فکر و نگاه هکر آشنا میشوید.

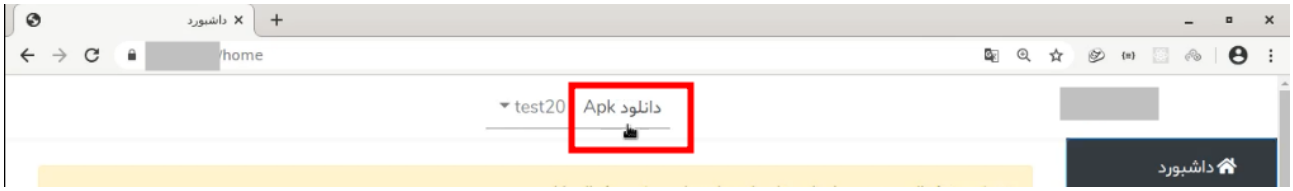
و در این لحظه که شما این مطلب را مطالعه میکنید این مشکلات توسط تیم توسعه برطرف شده است .

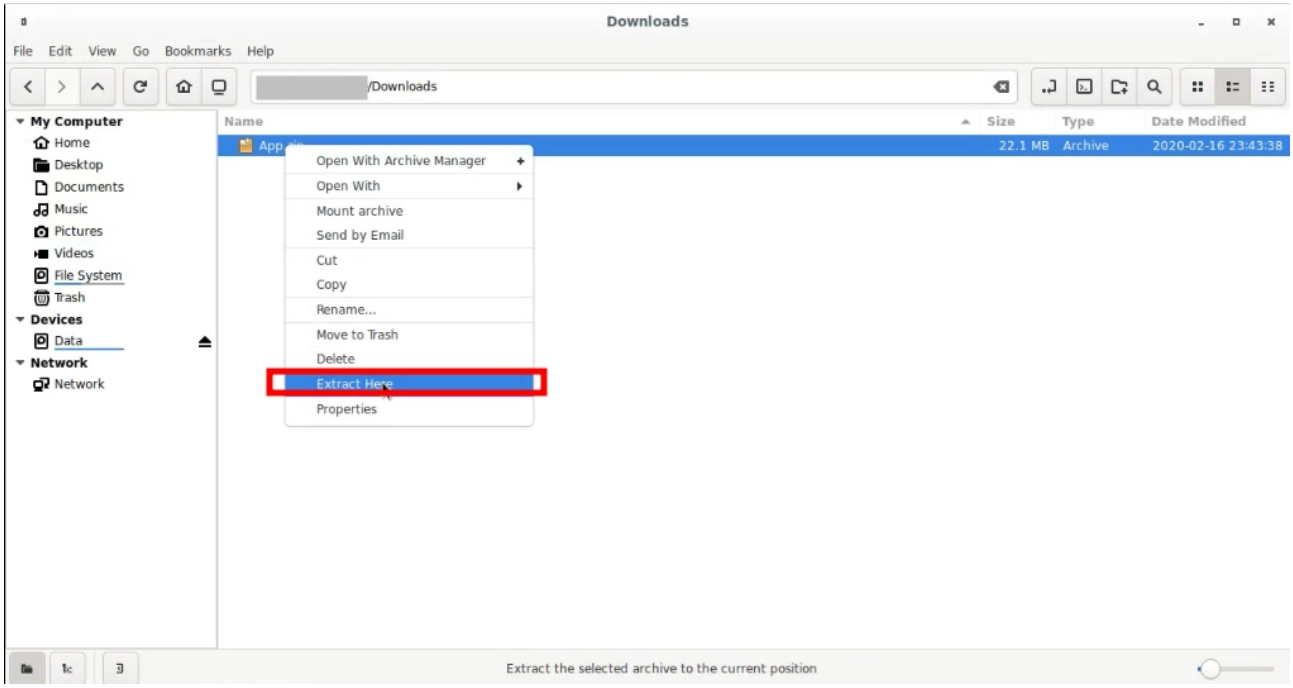
قدم اول : (آغازی برای نفوذ)

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



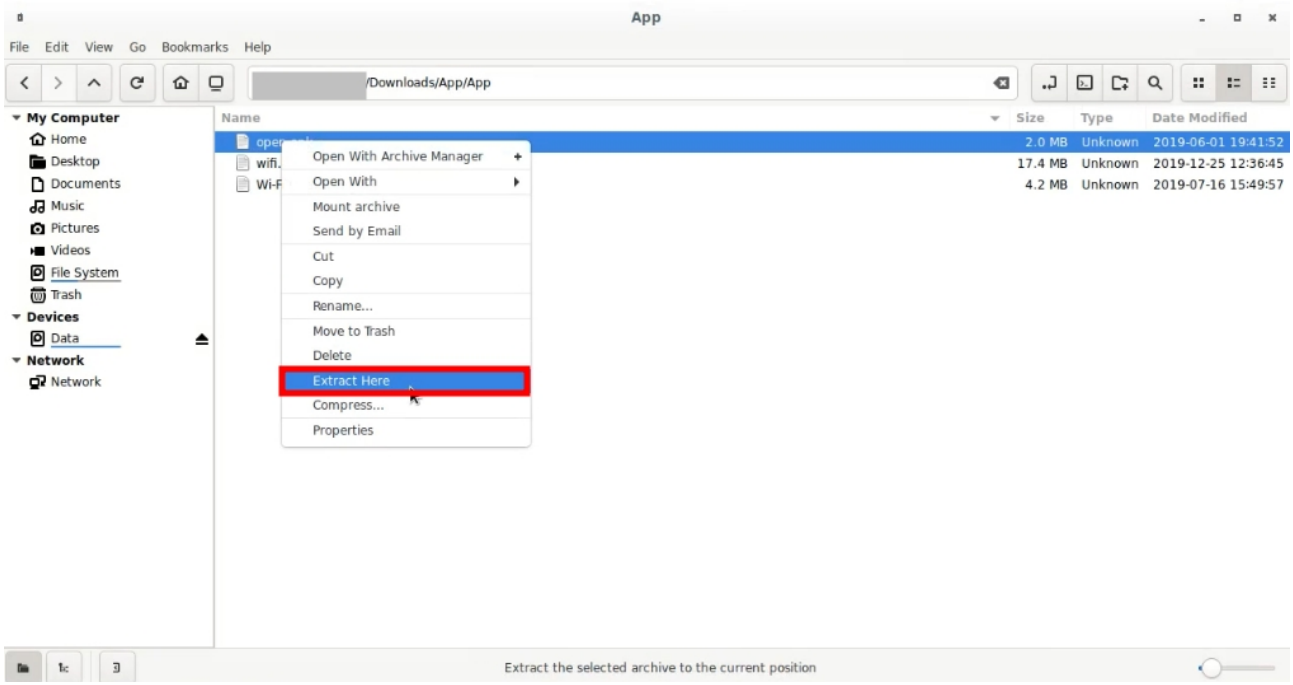
فایل برنامه را دانلود میکنیم .

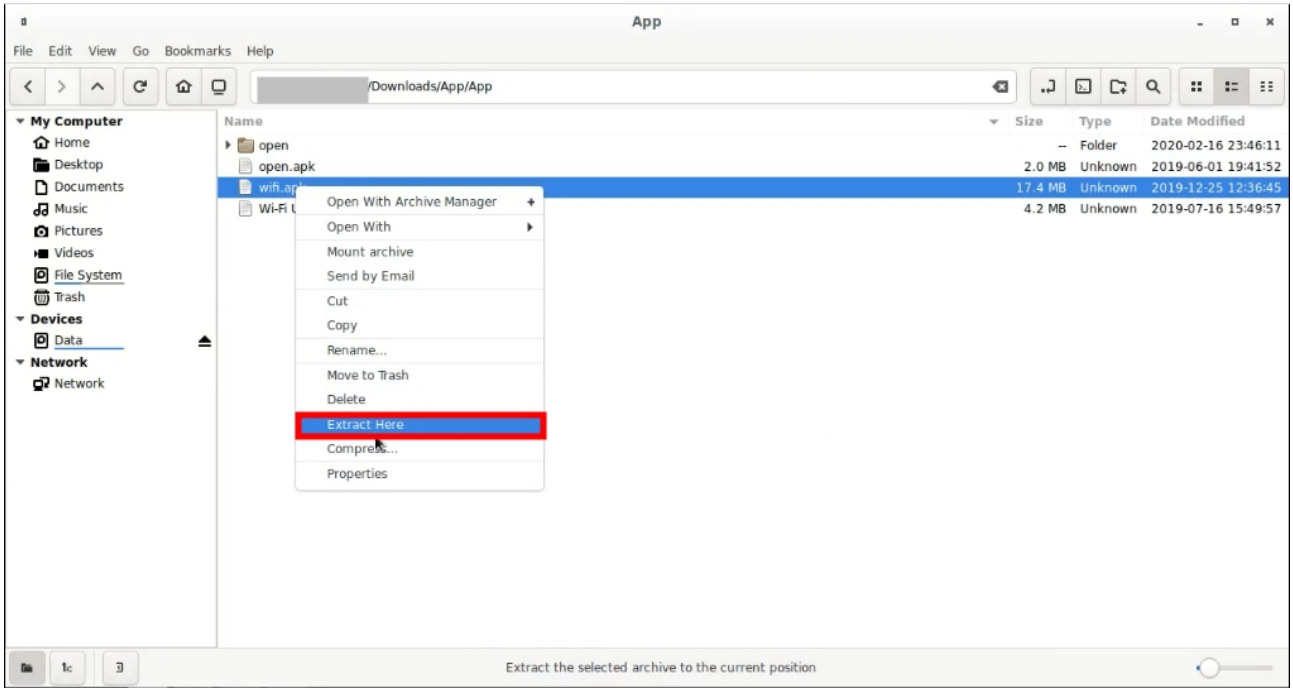


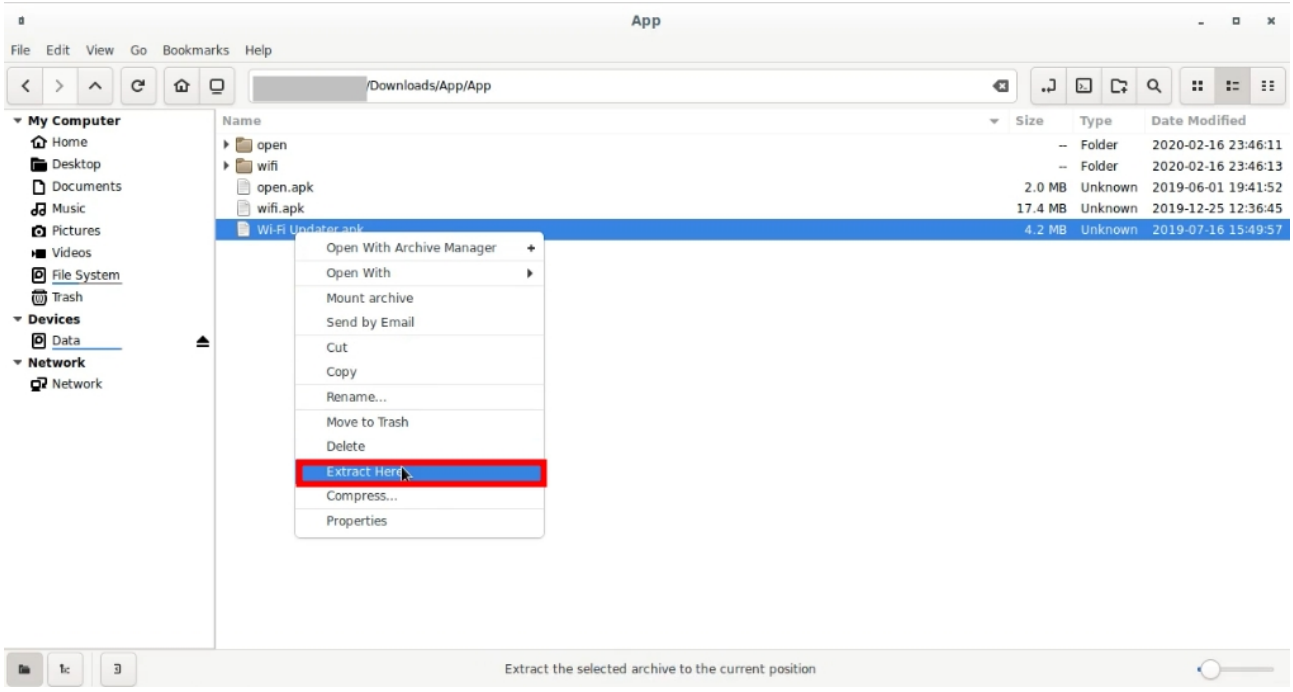


قدم دوم : (مهندسی معکوس Android)

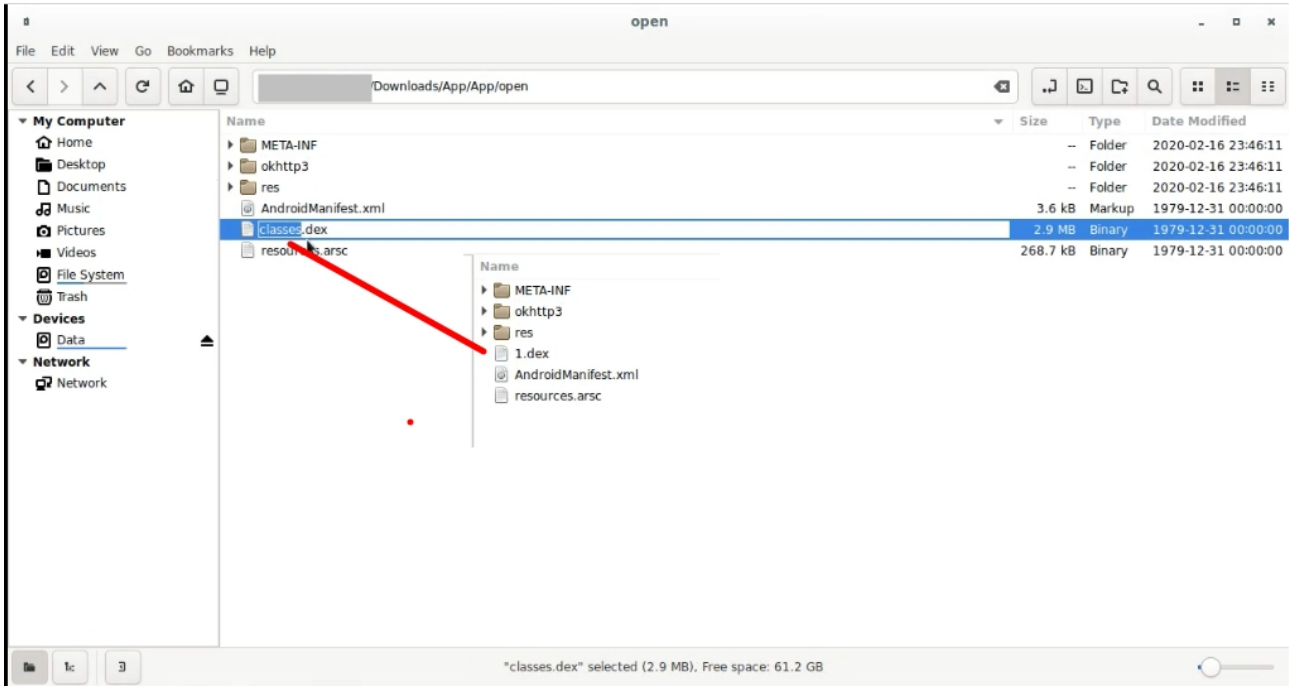
ابتدا فایل های apk را extract میکنیم .

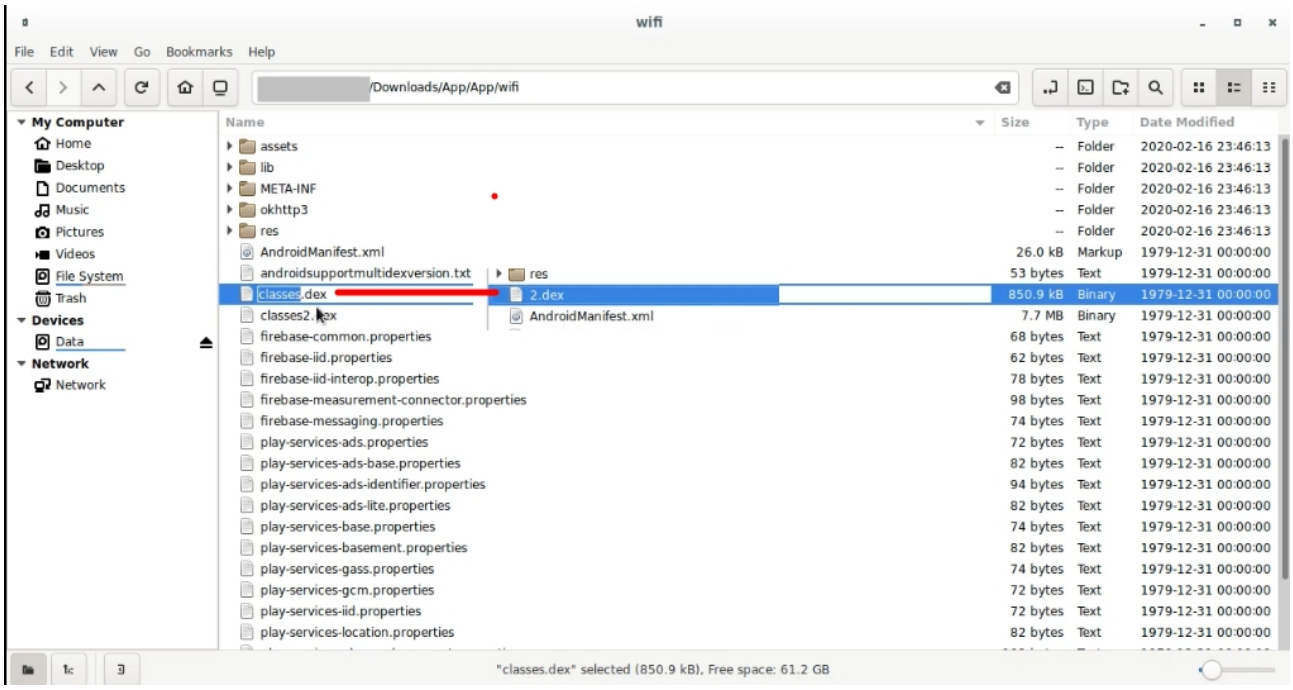


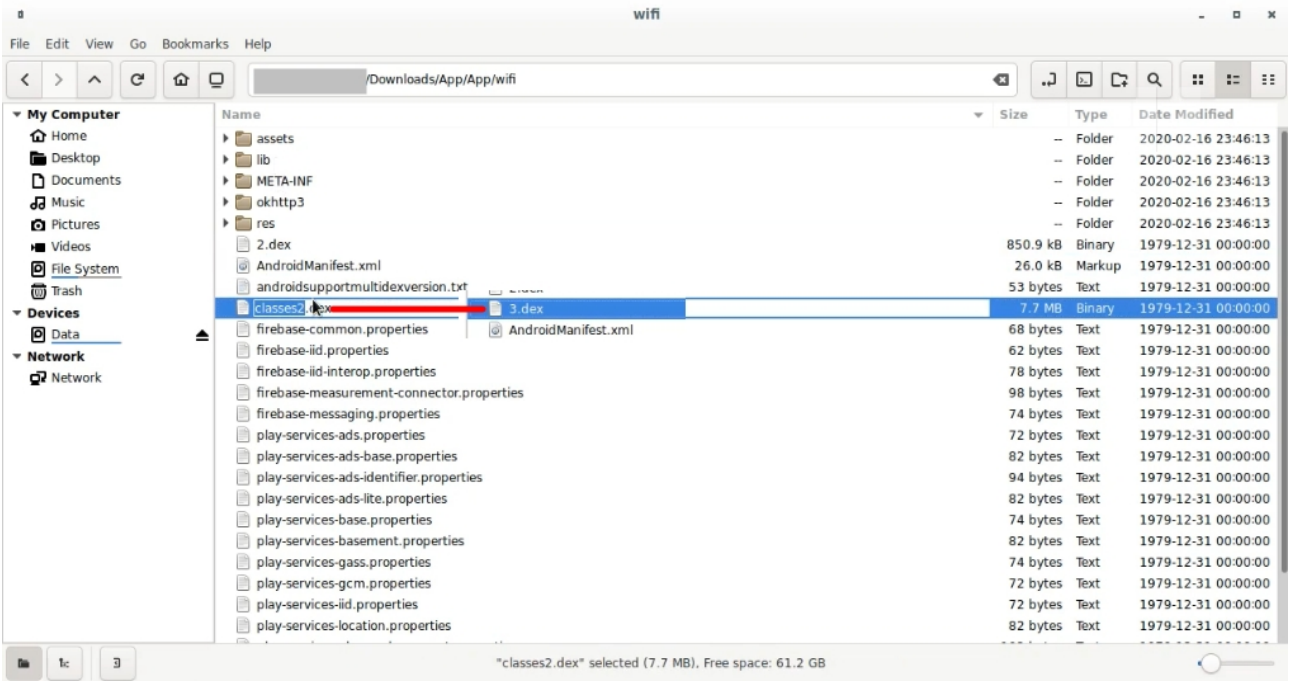


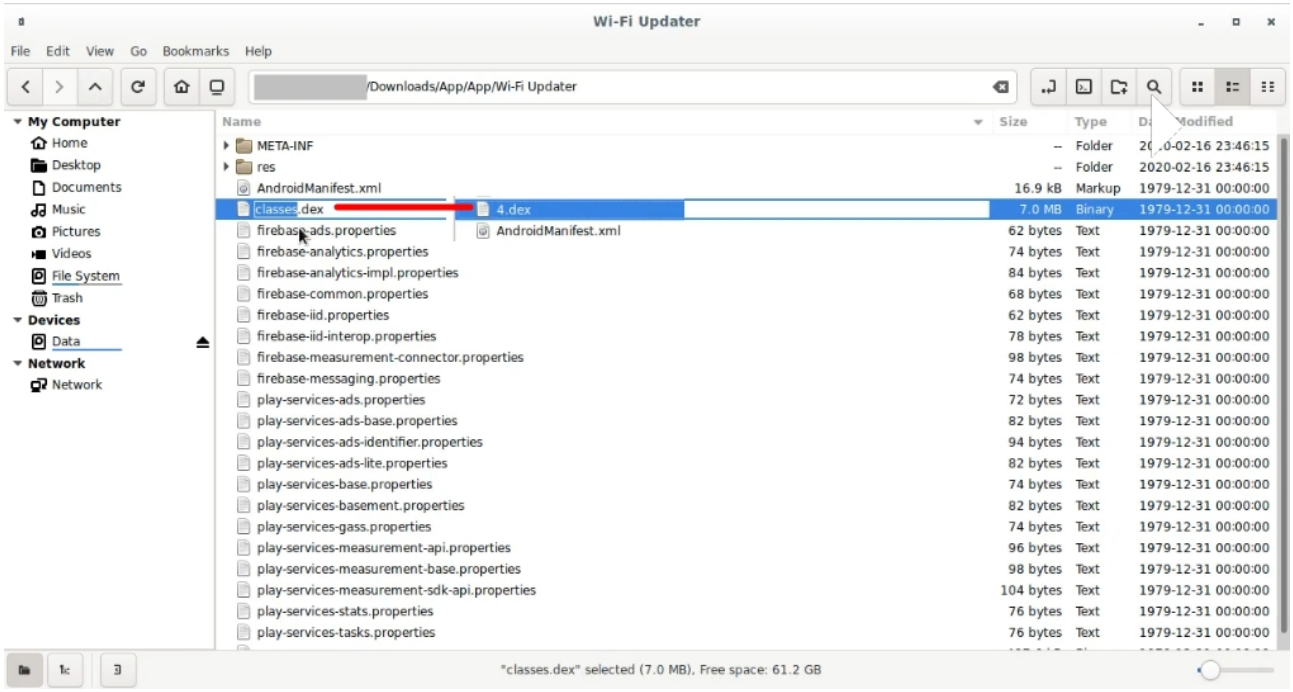


چون تعداد فایل های classes.dex زیاد است ابتدا نام آنها را تغییر میدهیم .

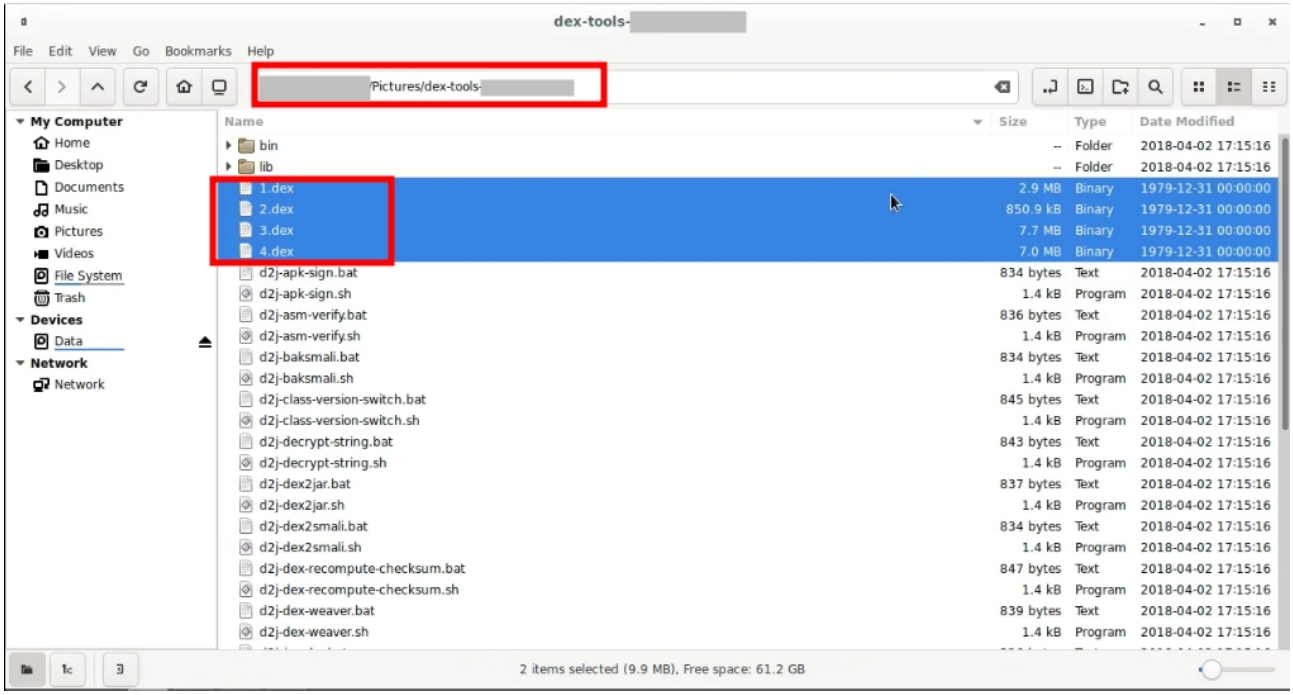

open
File Edit View Go Bookmarks Help
/Downloads/App/App/open
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
File System
Trash
Devices
Data
Network
Network
Name
Size
Type
Date Modified
META-INF -- Folder 2020-02-16 23:46:11
okhttp3 -- Folder 2020-02-16 23:46:11
res -- Folder 2020-02-16 23:46:11
AndroidManifest.xml 3.6 kB Markup 1979-12-31 00:00:00
classes.dex 2.9 MB Binary 1979-12-31 00:00:00
resources.arsc 268.7 kB Binary 1979-12-31 00:00:00
Name
META-INF
okhttp3
res
1.dex
AndroidManifest.xml
resources.arsc
"classes.dex" selected (2.9 MB), Free space: 61.2 GB


wifi
File Edit View Go Bookmarks Help
/Downloads/App/App/wifi
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
File System
Trash
Devices
Data
Network
Network
Name
Size
Type
Date Modified
assets -- Folder 2020-02-16 23:46:13
lib -- Folder 2020-02-16 23:46:13
META-INF -- Folder 2020-02-16 23:46:13
okhttp3 -- Folder 2020-02-16 23:46:13
res -- Folder 2020-02-16 23:46:13
AndroidManifest.xml 26.0 kB Markup 1979-12-31 00:00:00
androidsupportmultidexversion.txt 53 bytes Text 1979-12-31 00:00:00
classes.dex 850.9 kB Binary 1979-12-31 00:00:00
classes2.dex 7.7 MB Binary 1979-12-31 00:00:00
firebase-common.properties 68 bytes Text 1979-12-31 00:00:00
firebase-iid.properties 62 bytes Text 1979-12-31 00:00:00
firebase-iid-interop.properties 78 bytes Text 1979-12-31 00:00:00
firebase-measurement-connector.properties 98 bytes Text 1979-12-31 00:00:00
firebase-messaging.properties 74 bytes Text 1979-12-31 00:00:00
play-services-ads.properties 72 bytes Text 1979-12-31 00:00:00
play-services-ads-base.properties 82 bytes Text 1979-12-31 00:00:00
play-services-ads-identifier.properties 94 bytes Text 1979-12-31 00:00:00
play-services-ads-lite.properties 82 bytes Text 1979-12-31 00:00:00
play-services-base.properties 74 bytes Text 1979-12-31 00:00:00
play-services-basement.properties 82 bytes Text 1979-12-31 00:00:00
play-services-gass.properties 74 bytes Text 1979-12-31 00:00:00
play-services-gcm.properties 72 bytes Text 1979-12-31 00:00:00
play-services-iid.properties 72 bytes Text 1979-12-31 00:00:00
play-services-location.properties 82 bytes Text 1979-12-31 00:00:00
res
2.dex
AndroidManifest.xml
"classes.dex" selected (850.9 kB), Free space: 61.2 GB

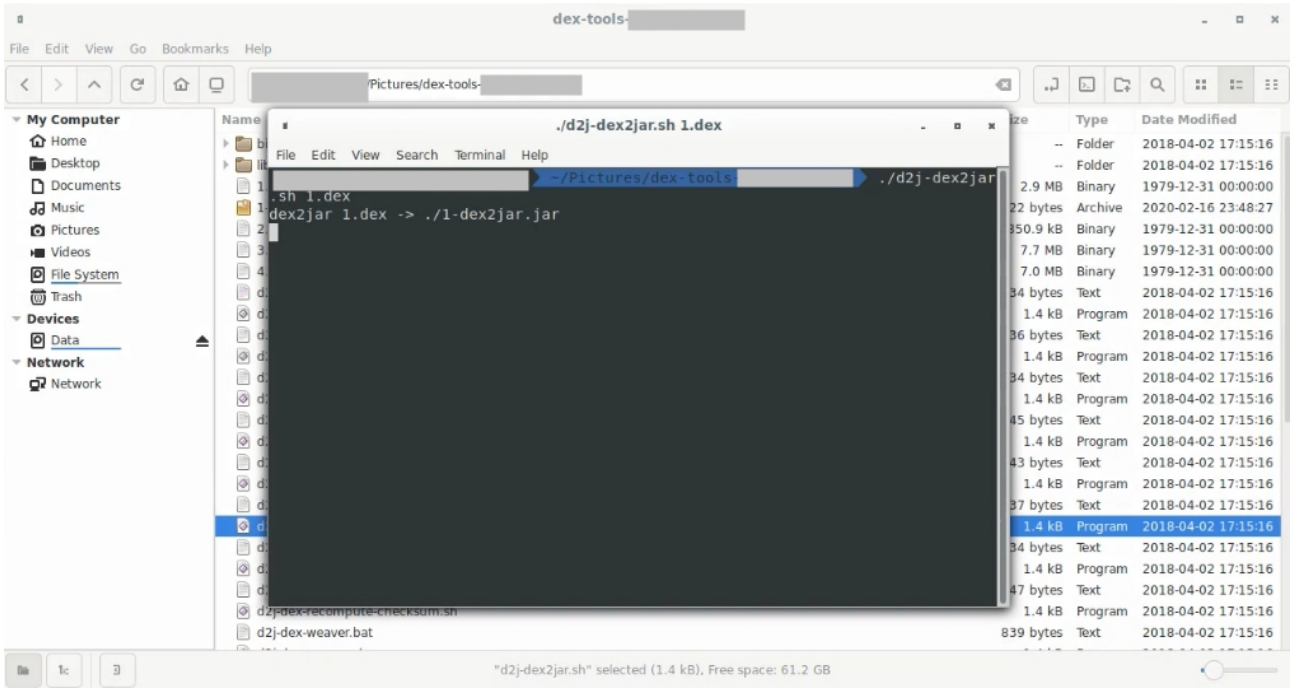

wifi
File Edit View Go Bookmarks Help
/Downloads/App/App/wifi
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
File System
Trash
Devices
Data
Network
Network
Name
Size
Type
Date Modified
assets -- Folder 2020-02-16 23:46:13
lib -- Folder 2020-02-16 23:46:13
META-INF -- Folder 2020-02-16 23:46:13
okhttp3 -- Folder 2020-02-16 23:46:13
res -- Folder 2020-02-16 23:46:13
2.dex 850.9 kB Binary 1979-12-31 00:00:00
AndroidManifest.xml 26.0 kB Markup 1979-12-31 00:00:00
androidsupportmultidexversion.txt 53 bytes Text 1979-12-31 00:00:00
classes2.dex
3.dex 7.7 MB Binary 1979-12-31 00:00:00
firebase-common.properties 68 bytes Text 1979-12-31 00:00:00
AndroidManifest.xml
firebase-iid.properties 62 bytes Text 1979-12-31 00:00:00
firebase-iid-interop.properties 78 bytes Text 1979-12-31 00:00:00
firebase-measurement-connector.properties 98 bytes Text 1979-12-31 00:00:00
firebase-messaging.properties 74 bytes Text 1979-12-31 00:00:00
play-services-ads.properties 72 bytes Text 1979-12-31 00:00:00
play-services-ads-base.properties 82 bytes Text 1979-12-31 00:00:00
play-services-ads-identifier.properties 94 bytes Text 1979-12-31 00:00:00
play-services-ads-lite.properties 82 bytes Text 1979-12-31 00:00:00
play-services-base.properties 74 bytes Text 1979-12-31 00:00:00
play-services-basement.properties 82 bytes Text 1979-12-31 00:00:00
play-services-gass.properties 74 bytes Text 1979-12-31 00:00:00
play-services-gcm.properties 72 bytes Text 1979-12-31 00:00:00
play-services-iid.properties 72 bytes Text 1979-12-31 00:00:00
play-services-location.properties 82 bytes Text 1979-12-31 00:00:00
"classes2.dex" selected (7.7 MB), Free space: 61.2 GB

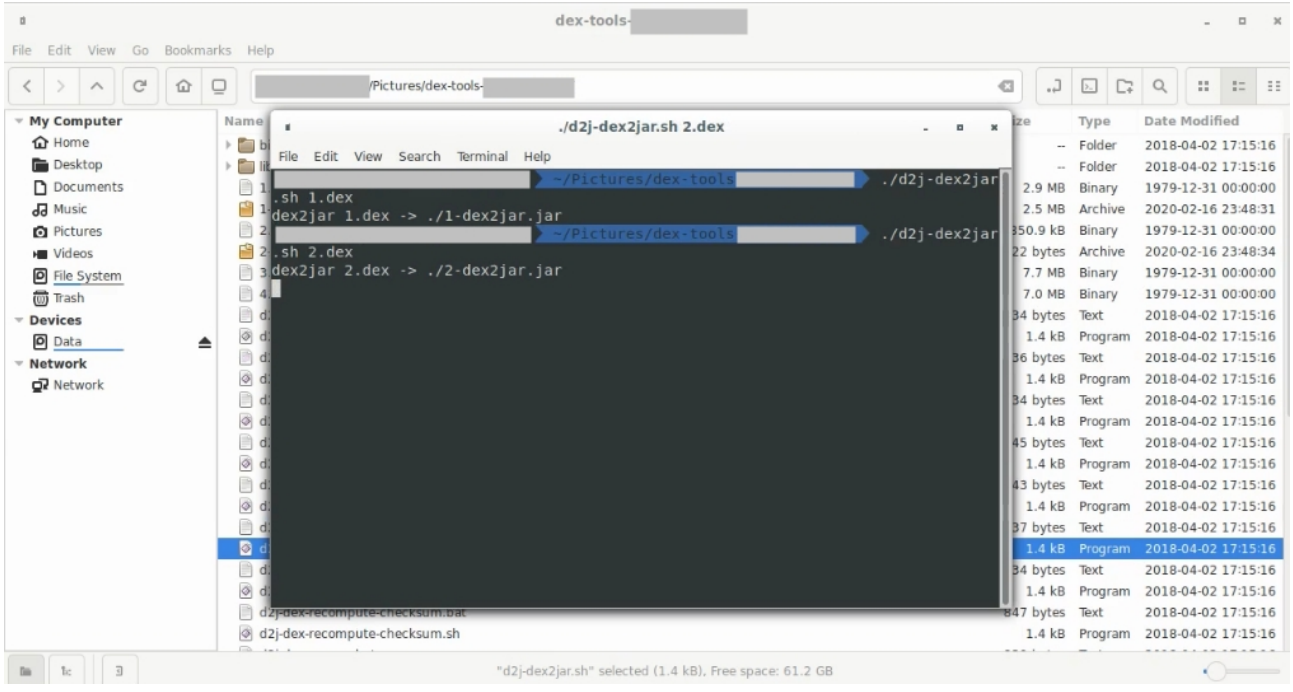


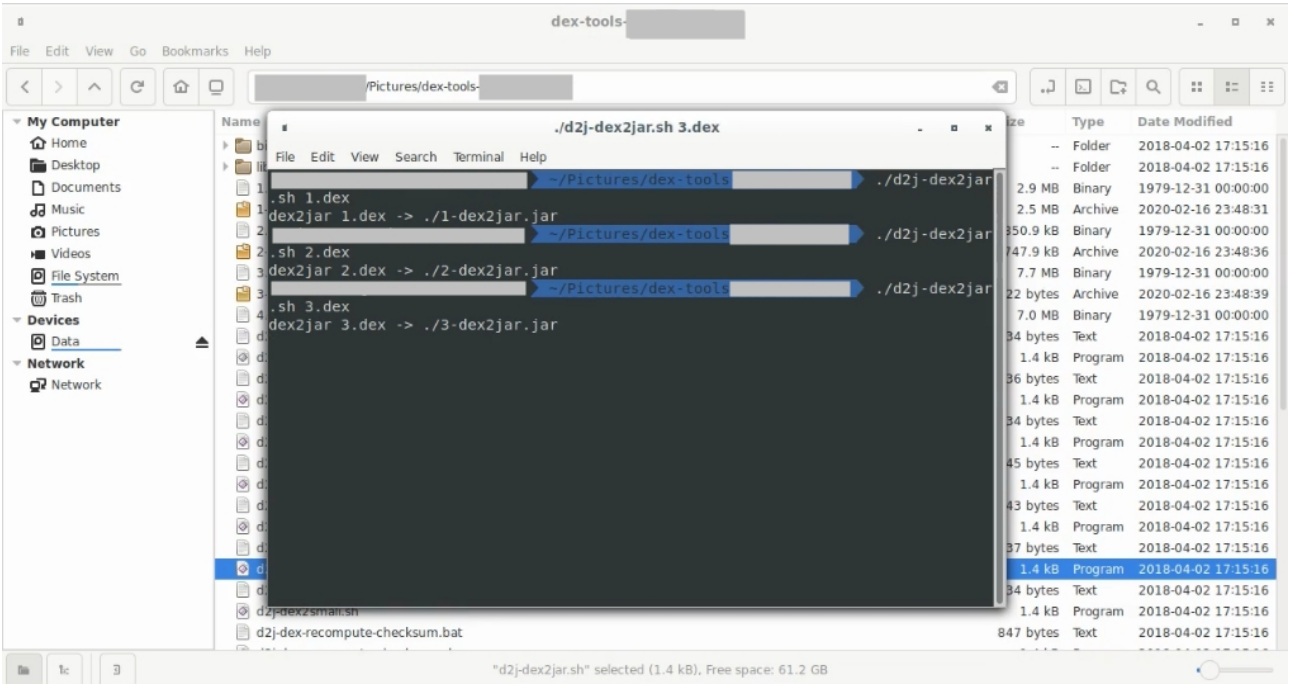
حالا تمامی فایل ها dex رو به پوشه برنامه dex2jar انتقال میدهیم .

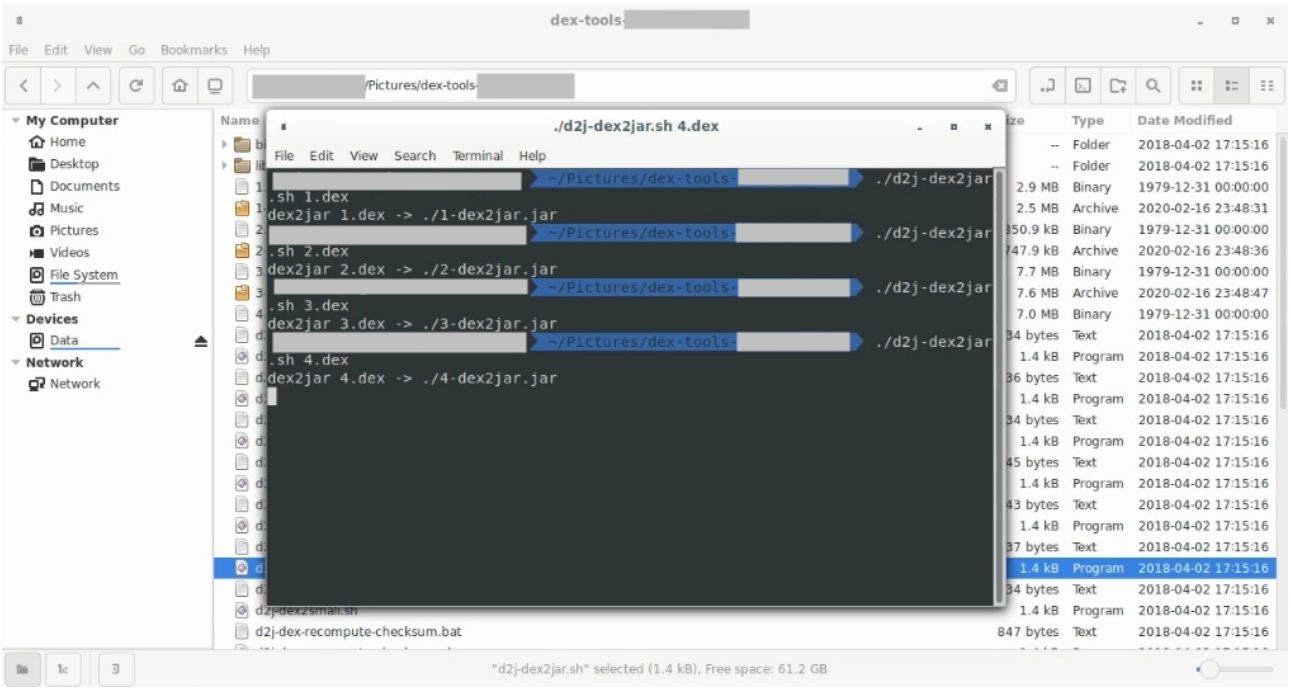


با دستورات زیر فایل های dex رو به jar تبدیل میکنیم تا بتوانیم سورس کد های برنامه را بخوانیم .

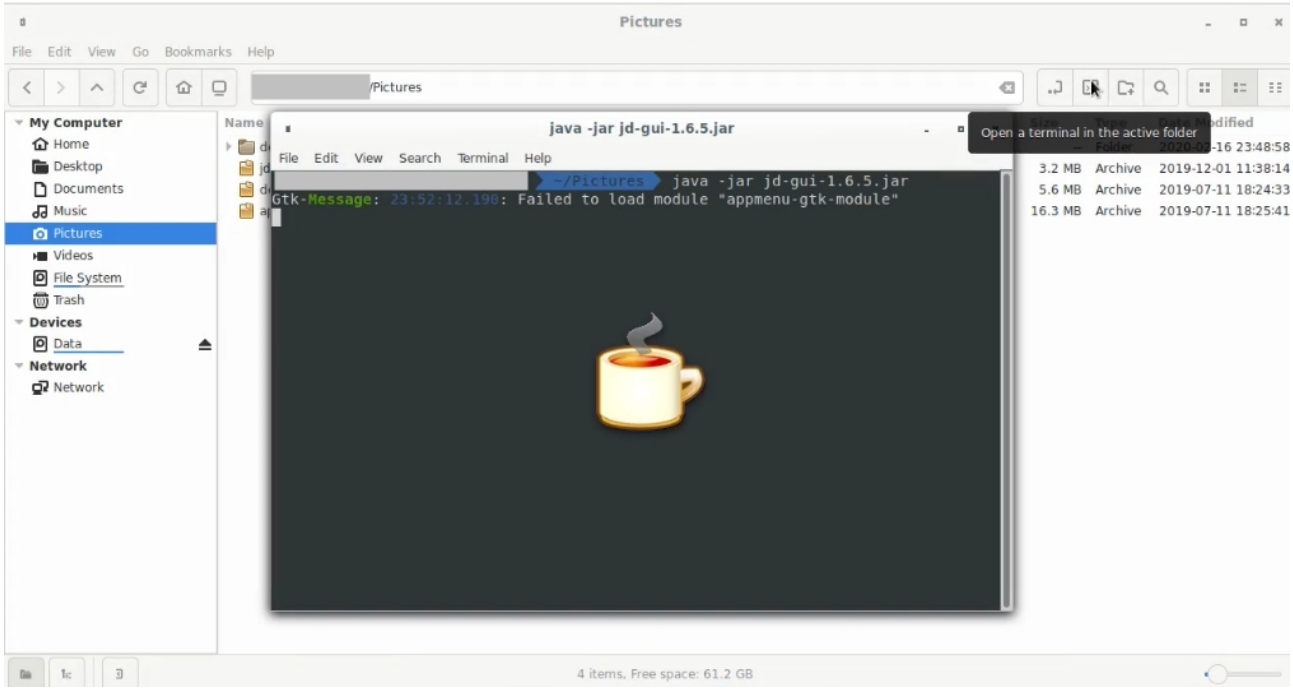

dex-tools-
File Edit View Go Bookmarks Help
/Pictures/dex-tools-
./d2j-dex2jar.sh 1.dex
File Edit View Search Terminal Help
~/Pictures/dex-tools ./d2j-dex2jar.sh 1.dex
dex2jar 1.dex -> ./1-dex2jar.jar
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
File System
Trash
Devices
Data
Network
Network
Name
Type
Date Modified
d2j-dex-recompute-checksum.sh
d2j-dex-weaver.bat
"d2j-dex2jar.sh" selected (1.4 kB), Free space: 61.2 GB

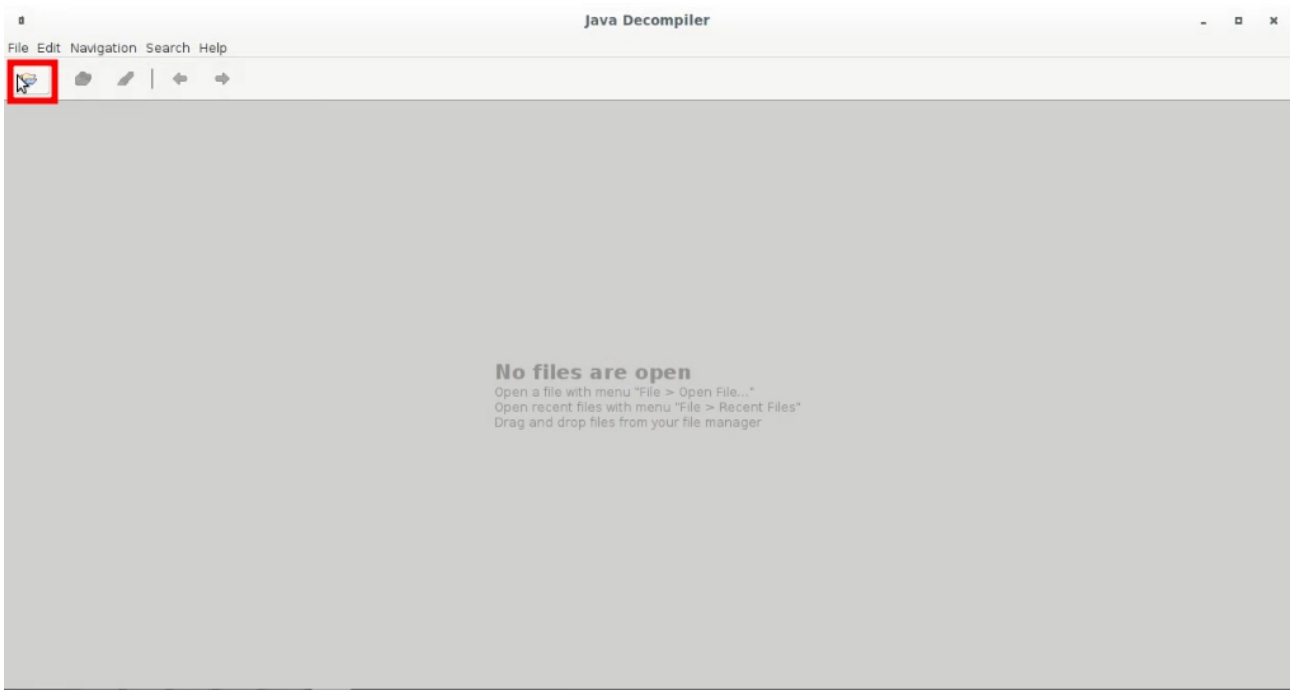

dex-tools-
File Edit View Go Bookmarks Help
/Pictures/dex-tools-
./d2j-dex2jar.sh 2.dex
File Edit View Search Terminal Help
~/Pictures/dex-tools ./d2j-dex2jar.sh 1.dex
dex2jar 1.dex -> ./1-dex2jar.jar
~/Pictures/dex-tools ./d2j-dex2jar.sh 2.dex
dex2jar 2.dex -> ./2-dex2jar.jar
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
File System
Trash
Devices
Data
Network
Network
Name
Type
Date Modified
d2j-dex-recompute-checksum.sh
"d2j-dex2jar.sh" selected (1.4 kB), Free space: 61.2 GB

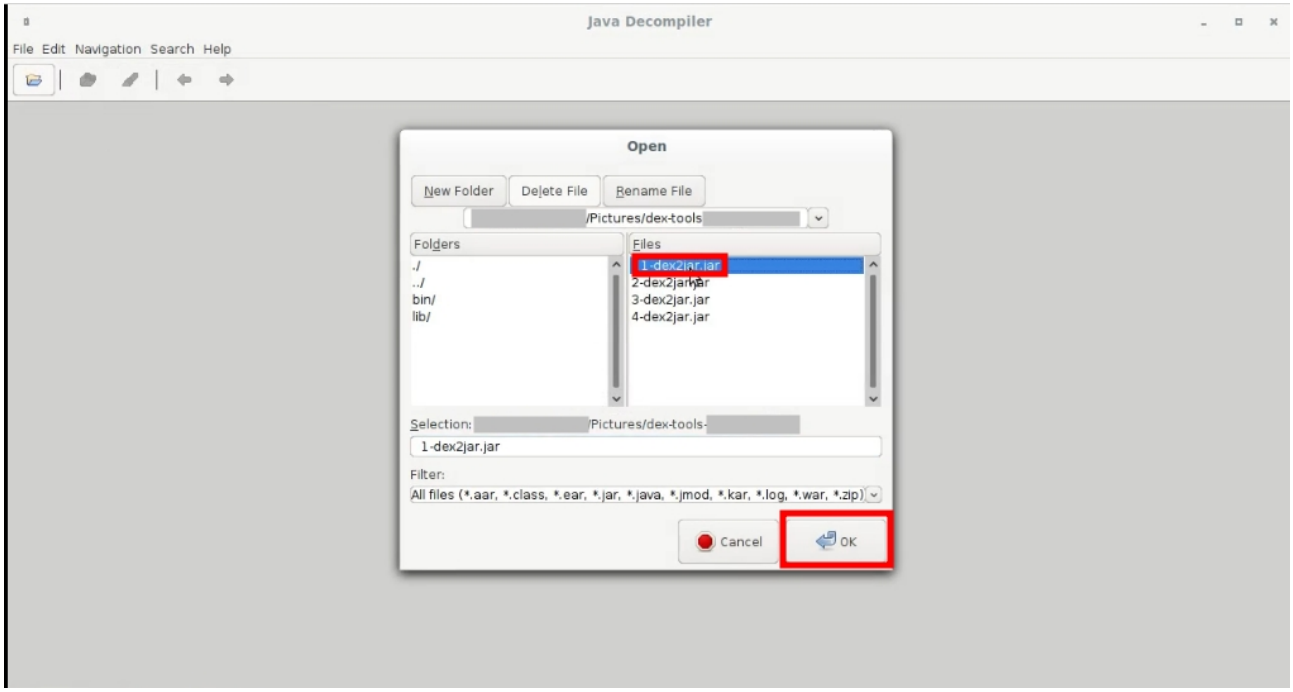


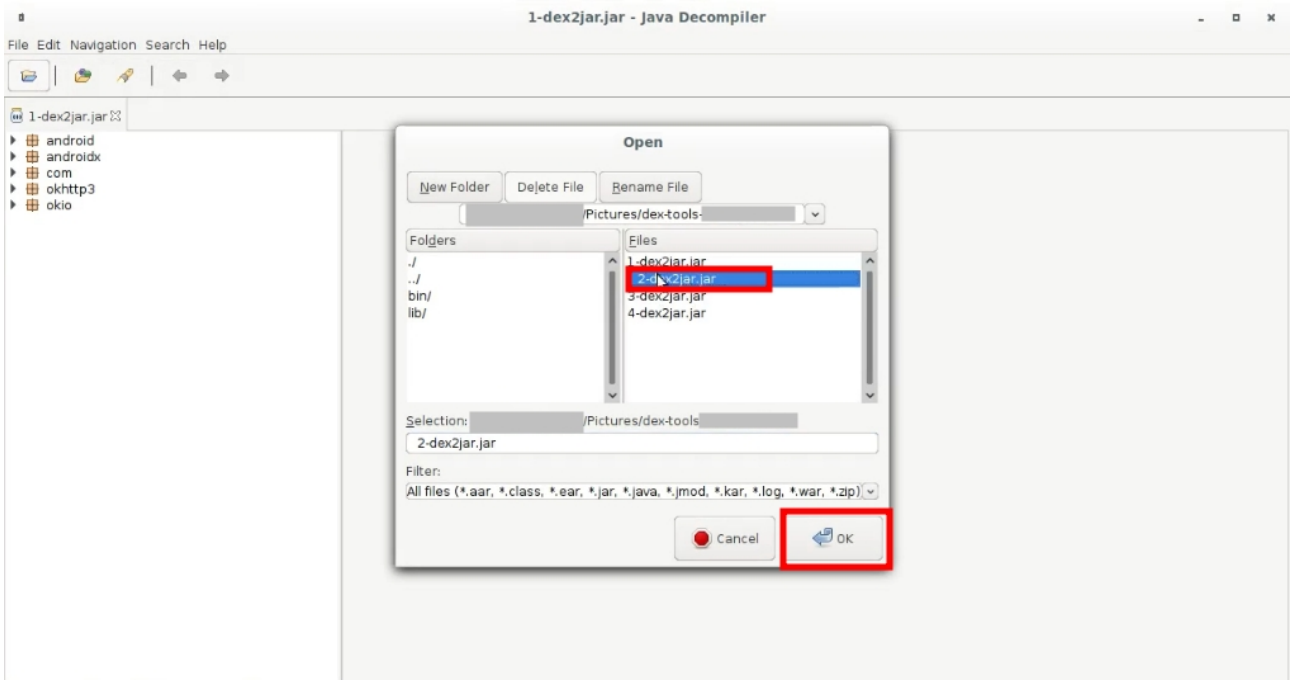


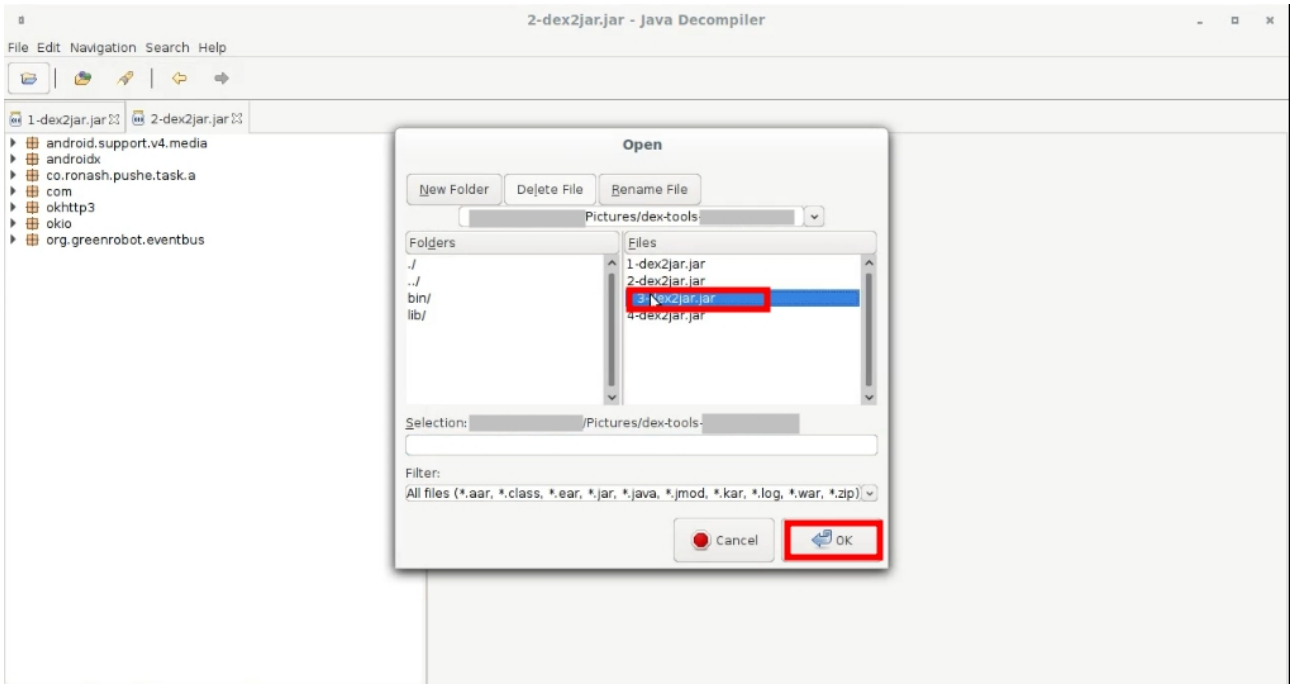
با ابزار jd-gui تمامی فایل های jar را باز میکنیم .

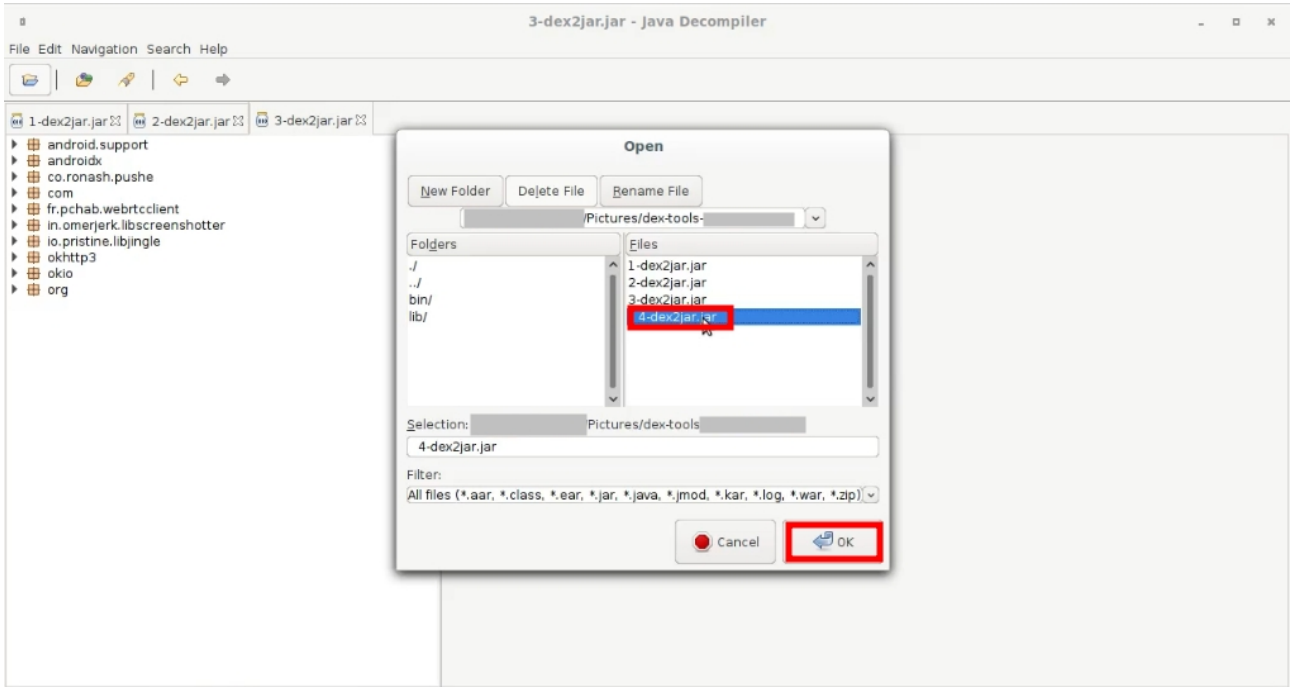

Pictures
File Edit View Go Bookmarks Help
/Pictures
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
File System
Trash
Devices
Data
Network
Network
java -jar jd-gui-1.6.5.jar
File Edit View Search Terminal Help
~/Pictures java -jar jd-gui-1.6.5.jar
Gtk-Message: 23:52:12.190: Failed to load module "appmenu-gtk-module"
Open a terminal in the active folder
3.2 MB Archive 2019-12-01 11:38:14
5.6 MB Archive 2019-07-11 18:24:33
16.3 MB Archive 2019-07-11 18:25:41
4 items, Free space: 61.2 GB


Java Decompiler
File Edit Navigation Search Help
No files are open
Open a file with menu "File > Open File..."
Open recent files with menu "File > Recent Files"
Drag and drop files from your file manager

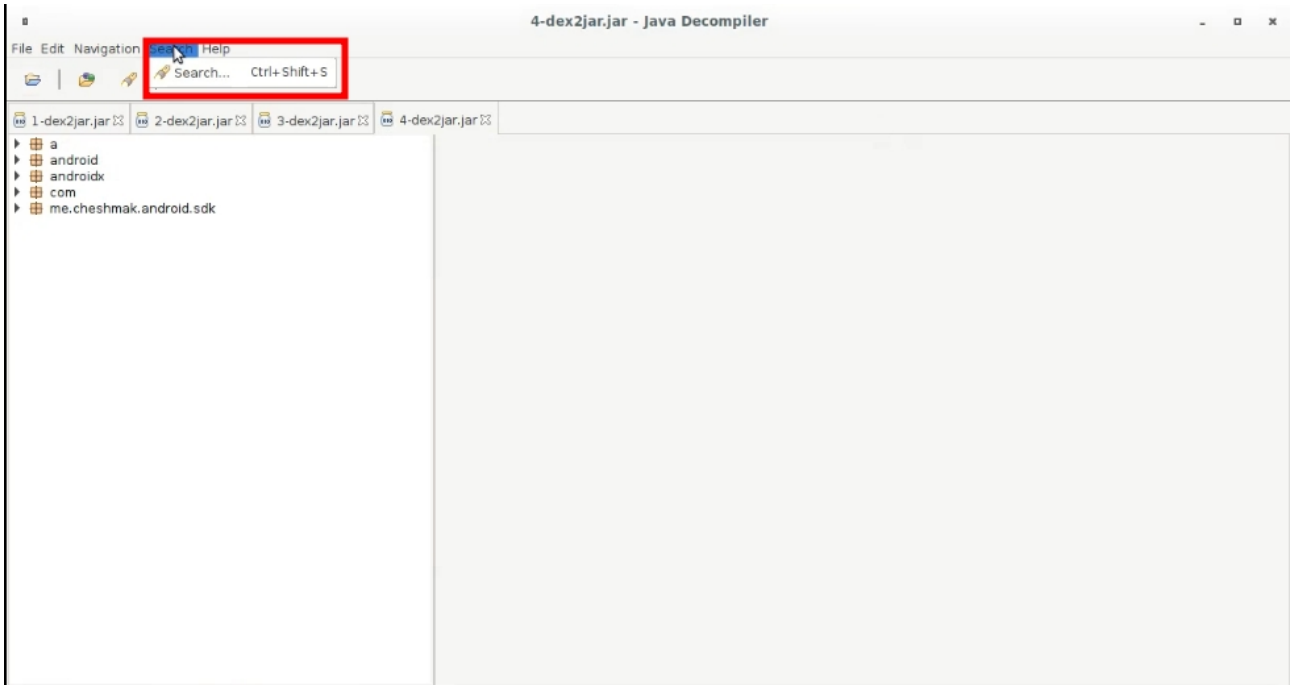

Java Decompiler
File Edit Navigation Search Help
Open
New Folder
Delete File
Rename File
/Pictures/dex-tools
Folders
./
../
bin/
lib/
Files
1-dex2jar.jar
2-dex2jar.jar
3-dex2jar.jar
4-dex2jar.jar
Selection:
/Pictures/dex-tools
1-dex2jar.jar
Filter:
All files (*.aar, *.class, *.ear, *.jar, *.java, *.jmod, *.kar, *.log, *.war, *.zip)
Cancel
OK

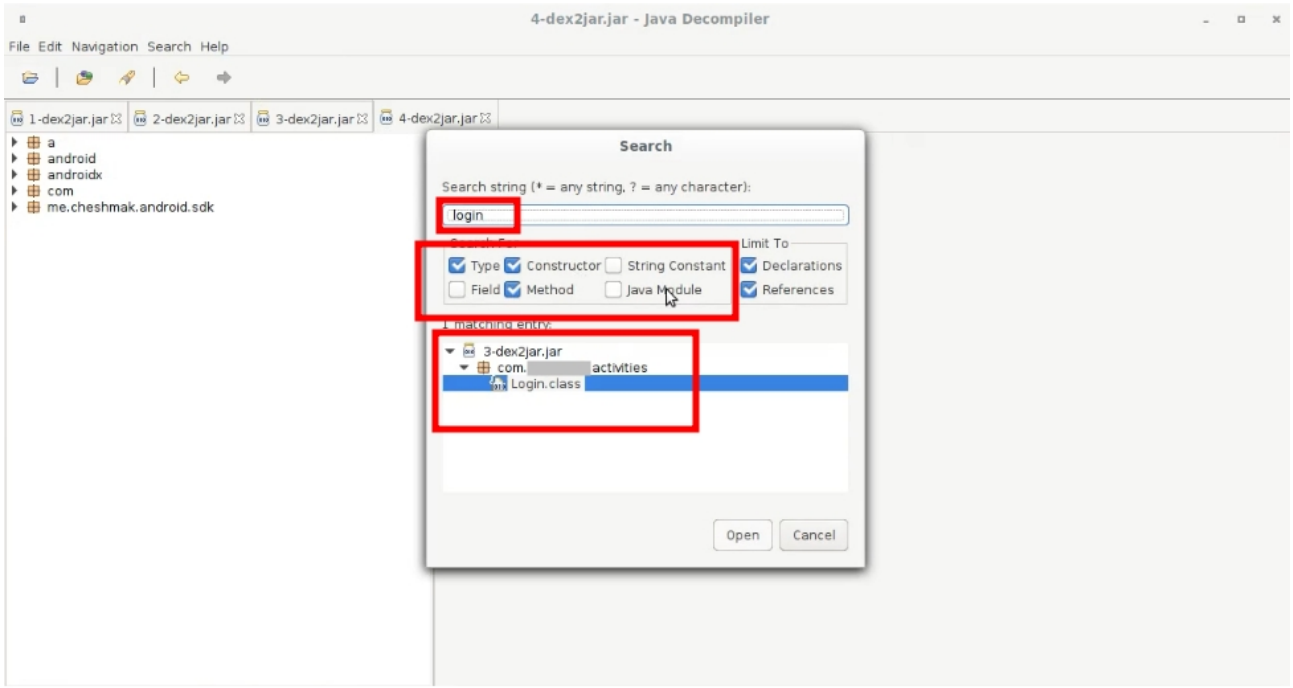

1-dex2jar.jar - Java Decompiler
File Edit Navigation Search Help
1-dex2jar.jar
android
androidx
com
okhttp3
okio
Open
New Folder
Delete File
Rename File
/Pictures/dex-tools
Folders
./
../
bin/
lib/
Files
1-dex2jar.jar
2-dex2jar.jar
3-dex2jar.jar
4-dex2jar.jar
Selection:
/Pictures/dex-tools
2-dex2jar.jar
Filter:
All files (*.aar, *.class, *.ear, *.jar, *.java, *.jmod, *.kar, *.log, *.war, *.zip)
Cancel
OK



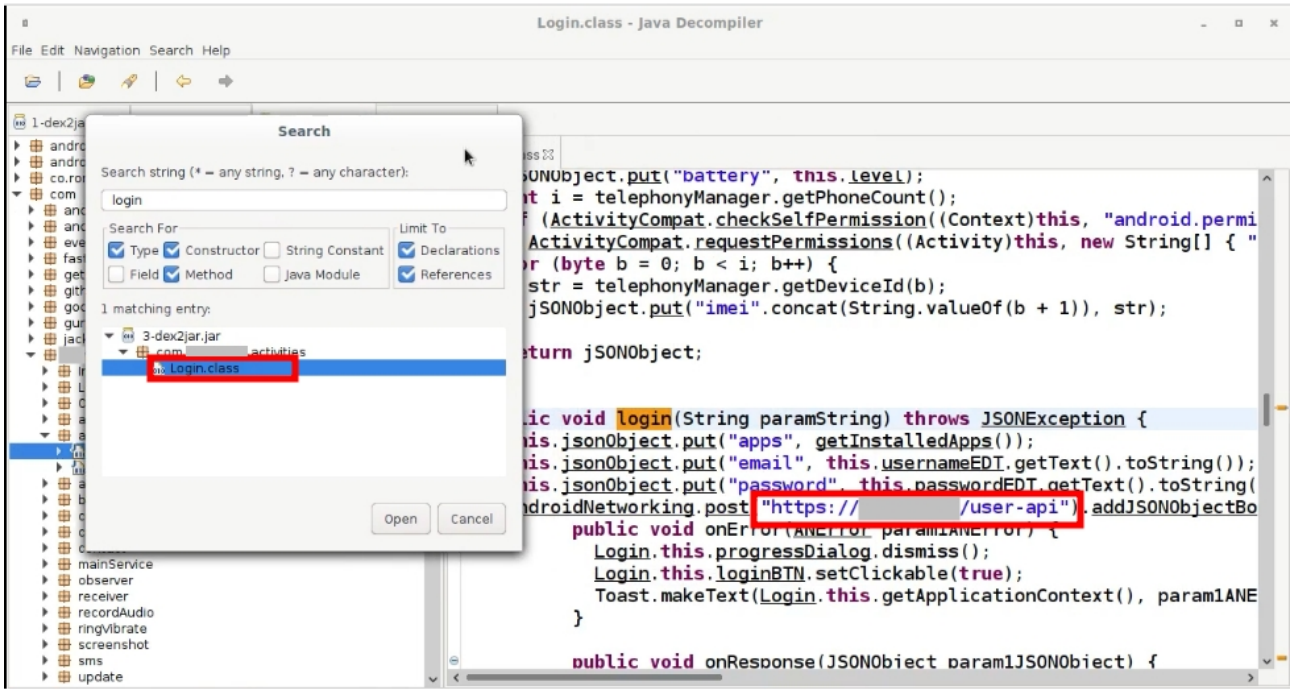


در این مرحله سعی میکنم آدرس اتصال به وب سرویس را پیدا کنیم , من به دنبال کلمه login بودم .





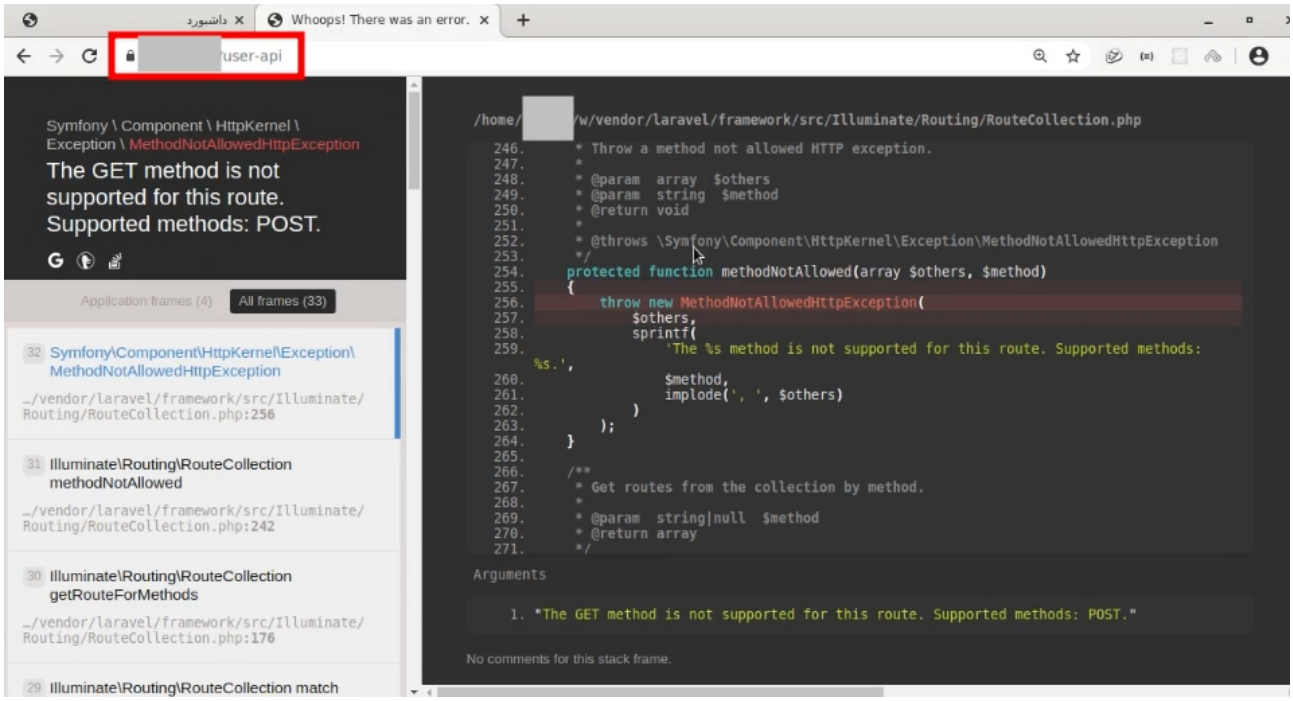
در نتیجه جستجو روی کلمه Login.class کلیک میکنم .



حالا آدرس وب سرویس login پیدا شد میریم ببینیم چی میشه !

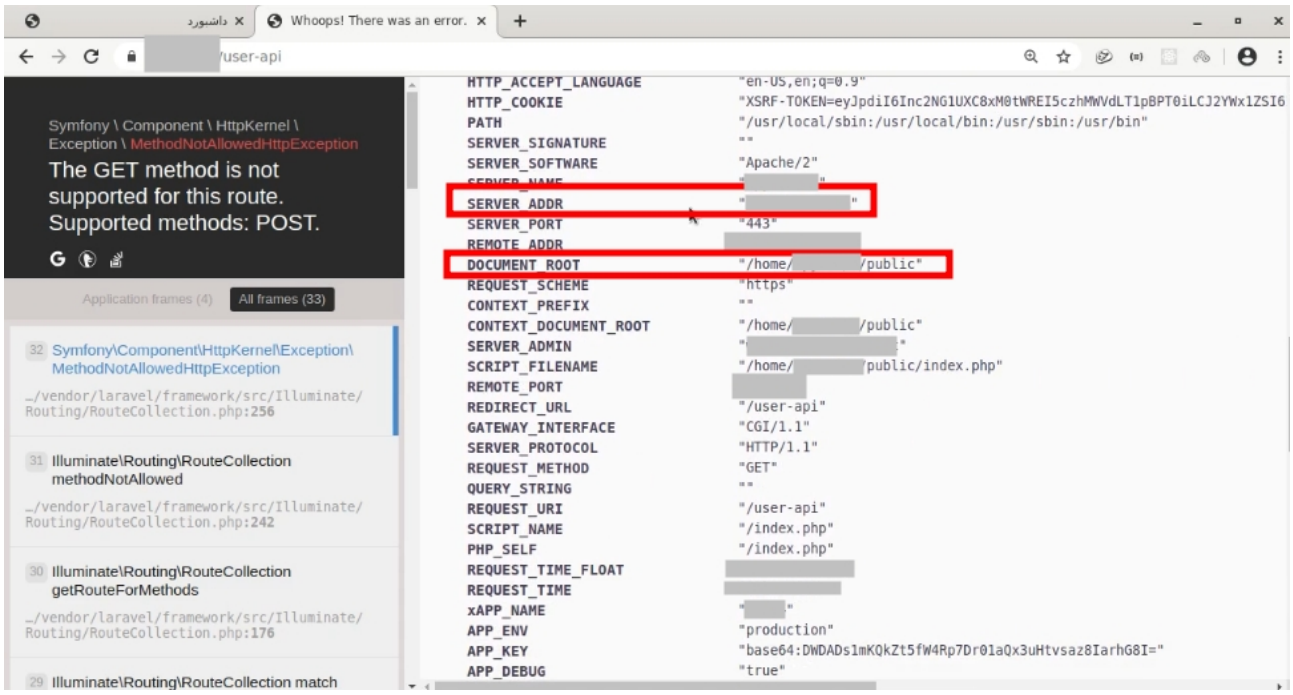
قدم سوم : (نفوذ)

من آدرس رو تو مرورگر زدم ببینیم چی خروجی میده ؟

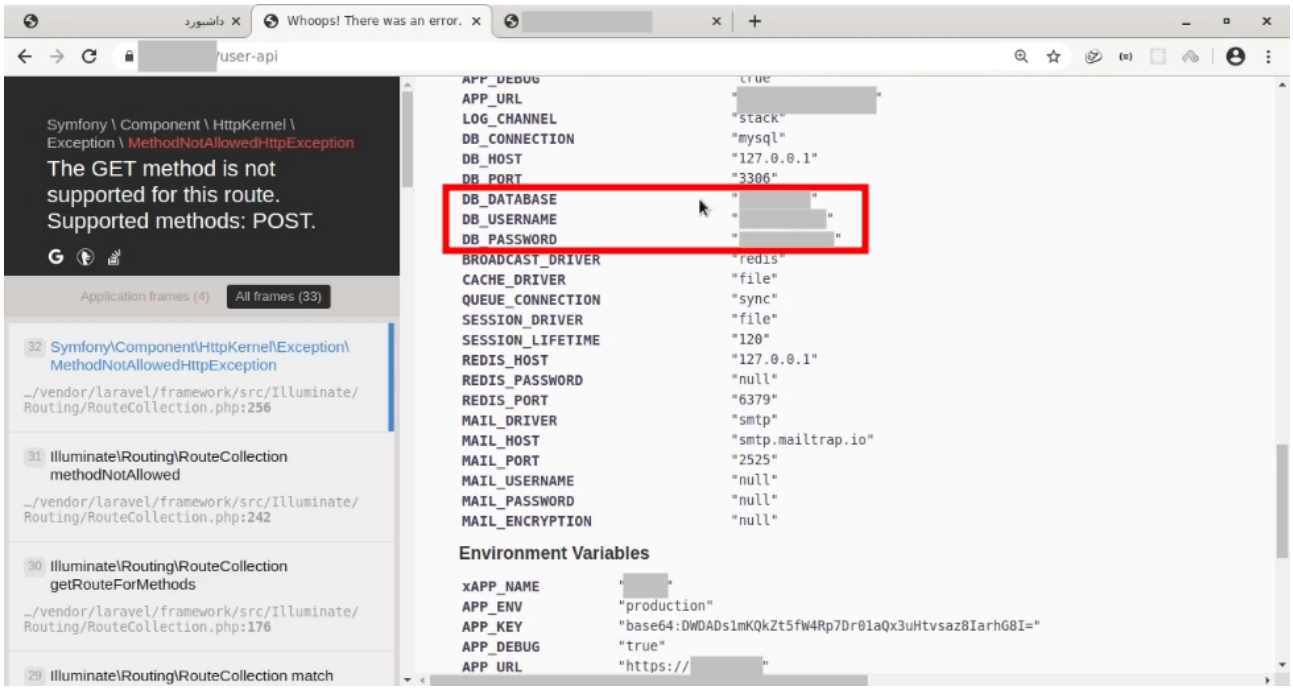


Oh My God خطای PHP و فریمورک محبوب و امن Laravel

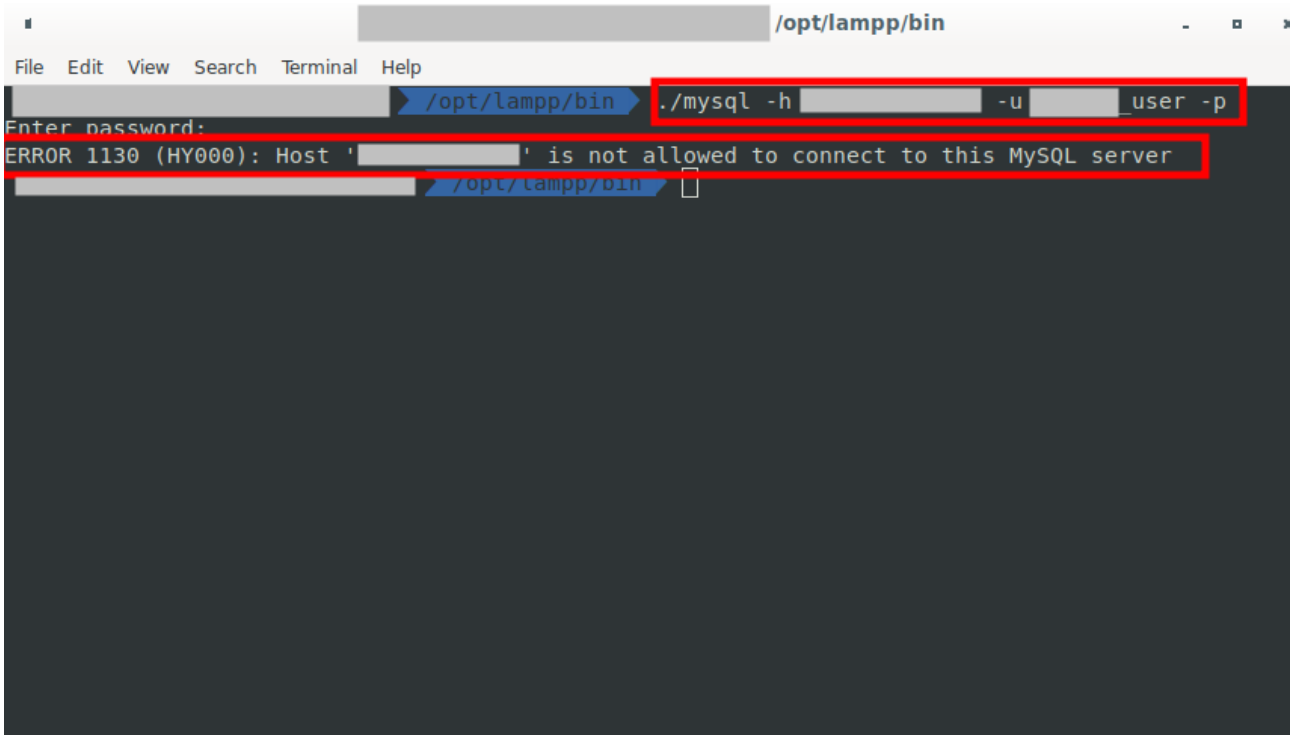
خوب بریم پایین تر ببینم باز چی هست . (منظورم اسکرول بود !)



همنطور که میبینید اطلاعاتی در مورد سرور و مسیر ها و ... بدست آوردیم , باز پایین تر میریم .



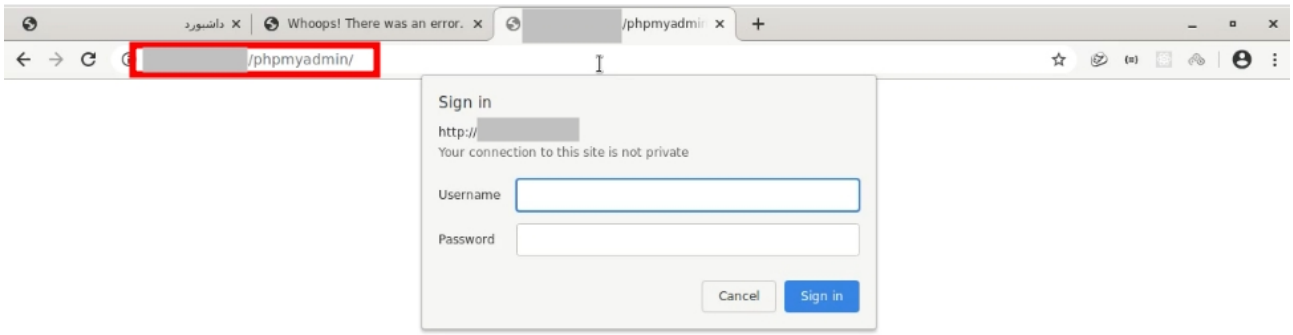
آخ جون ! یوز و پسورد دیتابیس MySQL خوب من سعی میکنم بهش وصل بشم .



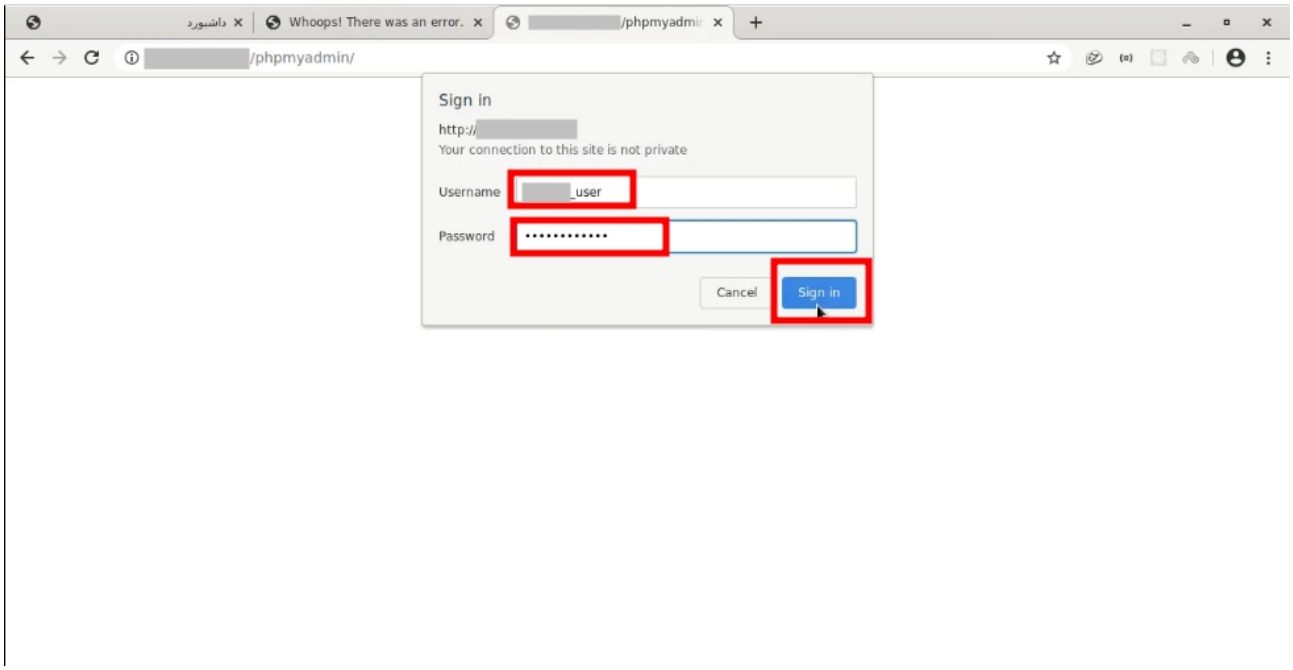
ضایع شدیم رفت ! اجازه اتصال از بیرون رو به ما نداد .

اما یک هکر همه راه ها را امتحان میکنه .

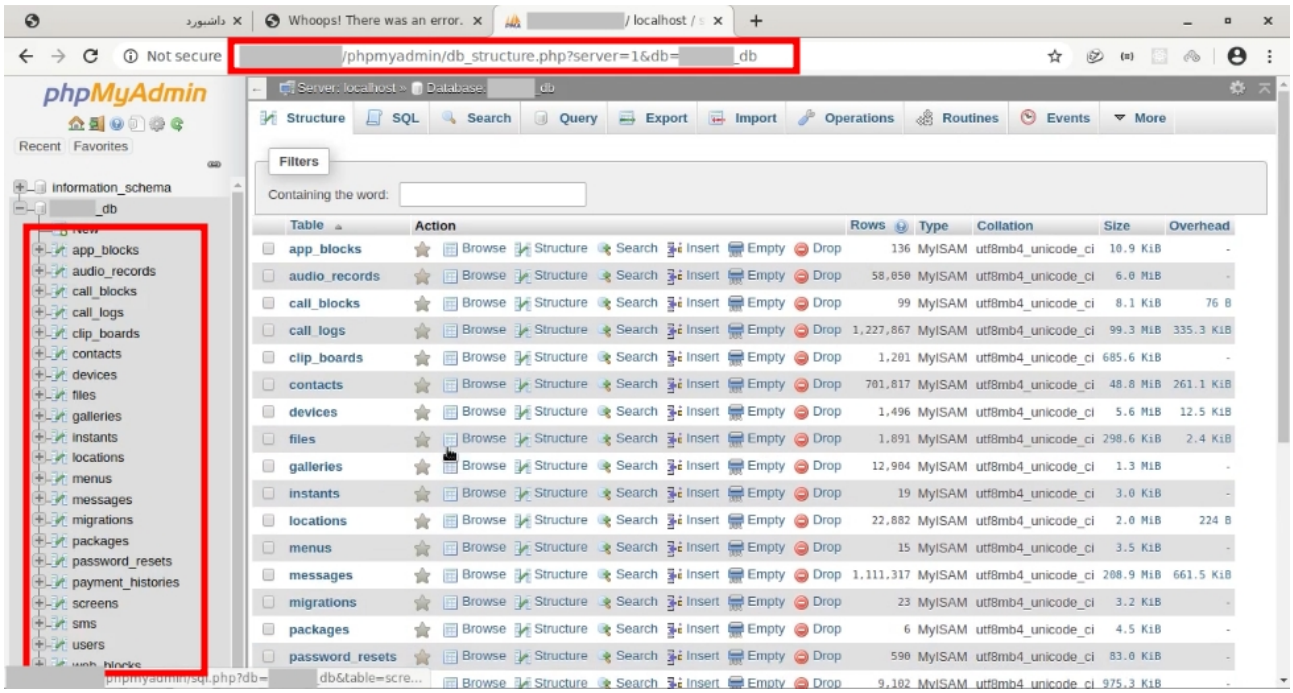
من آدرس IP سرور رو زدم و احتمال میدم که مسیر phpmyadmin باز باشد.
(امیدوارم!)



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



بعد میبینم صفحه ای باز میشود ؟



بله متاسفانه 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 محرمانه 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 افزاها وجود نداشته باشد , به راحتی هکر ها میتوانند به سیستم ها نفوذ کرده و از اطلاعات آن سوءاستفاده کنند.