Perform Android Virtual Device (AVD) Test Using Burp Suite

https://github.com/sepdijono/appium

OS: Ubuntu

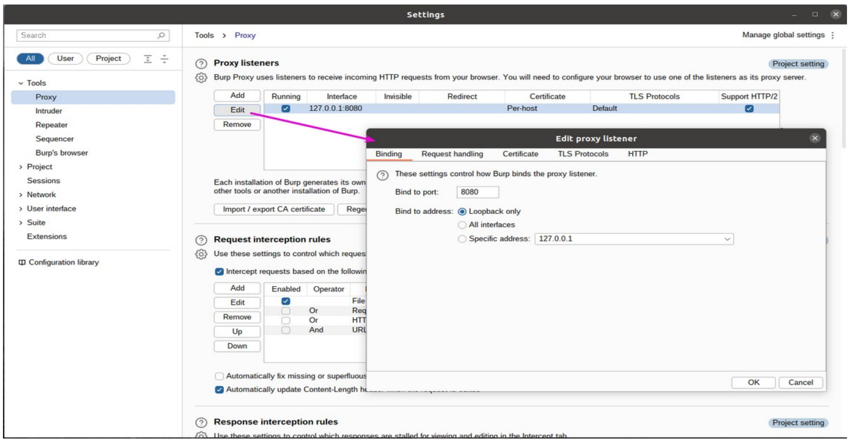
Prerequisite:

- ➢ Burp Suite
  - ✔ Burp Suite DER file
  - ✔ Burp Suite proxy listener
- ➢ Android Studio
  - ✔ Android Studio Virtual Devices (AVD)
  - ✔ Adb command

Instalation

➢ Burp Suite Setup

- ✔ Download Burp Suite desktop application
- ✔ Setup proxy (add proxy listener)



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
☑	127.0.0.1:8080			Per-host	Default	☑

Each installation of Burp generates its own … other tools or another installation of Burp.

Request interception rules

Use these settings to control which reques…

☑ Intercept requests based on the followin…

Enabled	Operator	
☑		File
□	Or	Req
□	Or	HTT
□	And	URL

□ Automatically fix missing or superfluous…

☑ Automatically update Content-Length h…

Response interception rules

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Edit proxy listener

These settings control how Burp binds the proxy listener.

Bind to port: 8080

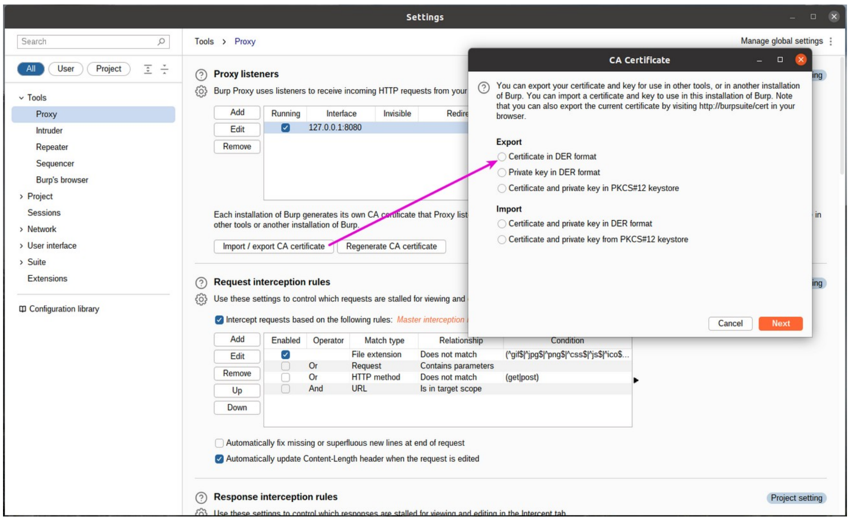
Bind to address: ● Loopback only

○ All interfaces

○ Specific address: 127.0.0.1

➢ Download Burp Suite .der Certificate

Each Burp Suite instalation has it own certificate



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your…

Running	Interface	Invisible	Redire…
☑	127.0.0.1:8080		

Each installation of Burp generates its own CA certificate that Proxy list… other tools or another installation of Burp.

Request interception rules

Use these settings to control which requests are stalled for viewing and…

☑ Intercept requests based on the following rules: *Master interception…*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$…
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

Response interception rules

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

CA Certificate

You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burpsuite/cert in your browser.

Export

○ Certificate in DER format

○ Private key in DER format

○ Certificate and private key in PKCS#12 keystore

Import

○ Certificate and private key in DER format

○ Certificate and private key from PKCS#12 keystore

Please save .der file to easily accessible directory like : ~/Desktop

- ➢ **Convert Burp Suite Certificate to “hash.0” File**
  - ✔ Convert .der to .pem

    ```
    openssl x509 -inform DER -in ~/Desktop/cacert.cer -out burp.pem
    ```

  - ✔ Get hash info from a .pem file

    ```
    openssl x509 -inform PEM -subject_hash_old -in burp.pem | head -1
    ```

  - ✔ Rename .pem to hash

    ```
    mv burp.pem hash.0 (ex: “9a5ba324.0”)
    ```

- ➢ **Run AVD (emulator)**
  - ✔ Change directory to android emulator directory and run the emulator (depends your system)

    ```
    cd ~/Android/sdk/emulator
    ./emulator -avd Nexus_Bla_Bla_API_xx -writable-system
    ```

  - ✔ Push the renamed .pem to */sdcard/*

    ```
    adb push hash.0 /sdcard/
    ```

- ➢ **Install Burp Suite Certificate**
  - ✔ Turn AVD as Writable System and Remount it

    ```
    adb root
    adb shell avbctl disable-verification
    adb disable-verity
    adb reboot (at this point your AVD will be rebooted, please wait until the device is ready)
    adb root
    adb remount (at this point you must receive succeeds notification “remount succeeded”, otherwise
    your next process will be failed)
    ```

  - ✔ To install cacert use command move renamed .pem to /system/etc/security/cacerts/

    ```
    mv hash.0 /system/etc/security/cacerts/
    ```

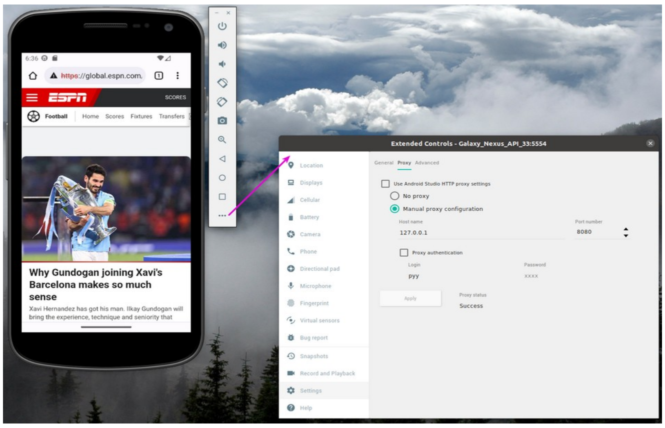
  - ✔ To check the process is succeded use ls command

    ```
    adb root
    adb shell
    ls system/etc/security/cacerts/hash.0 (succeeds if file is exists)
    ```

  - ✔ Pointing AVD to burp

    ```
    adb shell settings put global http_proxy localhost:3333
    adb reverse tcp:3333 tcp:8080 (port 8080 must same with burp)
    ```

- ➢ **Emulator Setup**



Extended Controls - Galaxy_Nexus_API_33:5554

□ Use Android Studio HTTP proxy settings

○ No proxy

● Manual proxy configuration

Host name: 127.0.0.1

Port number: 8080

□ Proxy authentication

Login: pyy

Password: xxxx

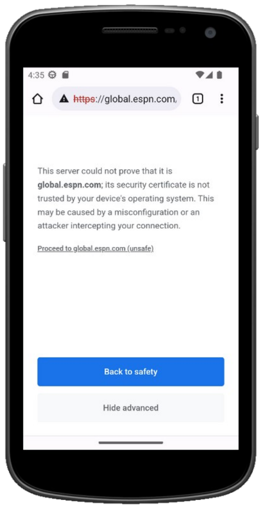
Proxy status: Success

Click the “…” button on your emulator toolbar and set the value as shown on the screenshot, after that click “Apply” and status show “Success”

Perform Small Test

- **Browsing with Chrome**
  - ✔ Open your emulator
  - ✔ Run google chrome – open https://global.espn.com

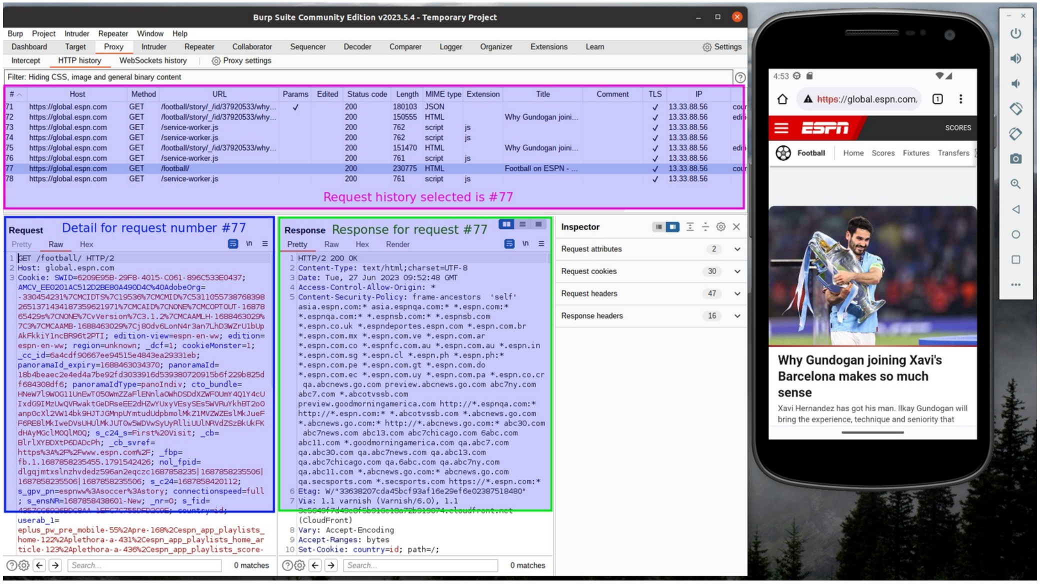
When you found certificate issue on your chrome click "Proceed to global.espn.com (unsafe)" to open the page.
Make sure you use this to test application that you know is safe.



This server could not prove that it is **global.espn.com**; its security certificate is not trusted by your device's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to global.espn.com (unsafe)

- ✔ Click one of request on "HTTP history"
  Screenshot below show user already selected the request history item number #77



Burp Suite Community Edition v2023.5.4 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	
71	https://global.espn.com	GET	/football/story/_/id/37920533/why...	✓		200	180103	JSON				✓	13.33.88.56	cou
72	https://global.espn.com	GET	/football/story/_/id/37920533/why...			200	150555	HTML		Why Gundogan joini...		✓	13.33.88.56	edi
73	https://global.espn.com	GET	/service-worker.js			200	762	script	js			✓	13.33.88.56	
74	https://global.espn.com	GET	/service-worker.js			200	762	script	js			✓	13.33.88.56	
75	https://global.espn.com	GET	/football/story/_/id/37920533/why...			200	151470	HTML		Why Gundogan joini...		✓	13.33.88.56	edi
76	https://global.espn.com	GET	/service-worker.js			200	761	script	js			✓	13.33.88.56	
77	https://global.espn.com	GET	/football/			200	230775	HTML		Football on ESPN - ...		✓	13.33.88.56	cou
78	https://global.espn.com	GET	/service-worker.js			200	761	script	js			✓	13.33.88.56	

Request history selected is #77

Request Detail for request number #77

```
GET /football/ HTTP/2
Host: global.espn.com
Cookie: SWID=6209E95B-29F8-4015-C061-896C533E0437;
AMCV_EE0201AC512D2BE80A490D4C%40AdobeOrg=
-330454231%7CMCIDTS%7C19536%7CMCMID%7C53110557387683982
6513714341873596219 71%7CMCAID%7CNONE%7CMCOPTOUT-16878
65429s%7CNONE%7CvVersion%7C3.1.2%7CMCAAMLH-1688463029%
7C3%7CMCAAMB-1688463029%7Cj80dv6LonN4r3an7LhD3WZrU1bUp
AkFkkiY1ncBR96t2PTI; edition-view=espn-en-ww; edition=
espn-en-ww; region=unknown; _dcf=1; cookieMonster=1;
_cc_id=6a4cdf90667ee94515e4843ea29331eb;
panoramaId_expiry=1688463034370; panoramaId=
18b4beaec2e4ed4a7be92fd3033916d539380720915b6f229b825d
f684308df6; panoramaIdType=panoIndiv; cto_bundle=
HNeW7l9WOG11UnEwT050WmZZaFlENnlaOWhDSDdXZWF0UmY4Q1Y4cU
IxdG9IMzUwQVRwaktGeDRseEE2dHZwYUxyVEsySEs5WVRuYkhBT2oO
anpOcXl2VW14bk9HJTJGMnpUYmtudUdpbmolMkZ1MVZWZEslMkJueF
F6RE8lMkIweDVsUHUlMkJUTOw5WDVwSyUyRlliUUlNRVdZSzBkUkFK
dHAyMGclMOQlMOQ; s_c24_s=First%20Visit; _cb=
BlrlXYBDXtP6DADcPh; _cb_svref=
https%3A%2F%2Fwww.espn.com%2F; _fbp=
fb.1.1687858235455.1791542426; nol_fpid=
dlgqjmtxslnzhvdedz596an2eqczc1687858235|1687858235506|
1687858235506|1687858235506; s_c24=1687858420112;
s_gpv_pn=espnww%3Asoccer%3Astory; connectionspeed=full
; s_ensNR=1687858438601-New; _nr=0; s_fid=
4357CC6926BDC8AA-1EEC7C755DED2C9E; country=id;
userab_1=
eplus_pw_pre_mobile-55%2Apre-168%2Cespn_app_playlists_
home-122%2Aplethora-a-431%2Cespn_app_playlists_home_ar
ticle-123%2Aplethora-a-436%2Cespn_app_playlists_score-
```

Response Response for request #77

```
HTTP/2 200 OK
Content-Type: text/html;charset=UTF-8
Date: Tue, 27 Jun 2023 09:52:48 GMT
Access-Control-Allow-Origin: *
Content-Security-Policy: frame-ancestors  'self'
asia.espn.com:* asia.espnqa.com:* *.espn.com:*
*.espnqa.com:* *.espnsb.com:* *.espnsb.com
*.espn.co.uk *.espndeportes.espn.com *.espn.com.br
*.espn.com.mx *.espn.com.ve *.espn.com.ar
*.espn.com.co *.espnfc.com.au *.espn.com.au *.espn.in
*.espn.com.sg *.espn.cl *.espn.ph *.espn.ph:*
*.espn.com.pe *.espn.com.gt *.espn.com.do
*.espn.com.ec *.espn.com.uy *.espn.com.pa *.espn.co.cr
 qa.abcnews.go.com preview.abcnews.go.com abc7ny.com
abc7.com *.abcotvssb.com
preview.goodmorningamerica.com http://*.espnqa.com:*
http://*.espn.com:* *.abcotvssb.com *.abcnews.go.com
*.abcnews.go.com:* http://*.abcnews.go.com:* abc30.com
 abc7news.com abc13.com abc7chicago.com 6abc.com
abc11.com *.goodmorningamerica.com qa.abc7.com
qa.abc30.com qa.abc7news.com qa.abc13.com
qa.abc7chicago.com qa.6abc.com qa.abc7ny.com
qa.abc11.com *.abcnews.go.com:* abcnews.go.com
qa.secsports.com *.secsports.com https://*.espn.com:*
Etag: W/"33638207cda45bcf93af16e29ef6e02387518480"
Via: 1.1 varnish (Varnish/6.0), 1.1
3c5649f7d49e8f5b916e18a72b919074.cloudfront.net
(CloudFront)
Vary: Accept-Encoding
Accept-Ranges: bytes
Set-Cookie: country=id; path=/;
```

Inspector	
Request attributes	2
Request cookies	30
Request headers	47
Response headers	16

Why Gundogan joining Xavi's Barcelona makes so much sense

Xavi Hernandez has got his man. Ilkay Gundogan will bring the experience, technique and seniority that