

Activities

v.1.0



Ni'am Habibiy Sahid

Detail Dokumen

Judul Dokumen : Lab Manual for Sharing Session

Tujuan Dokumen : Universitas Amikom Purwokerto

Tanggal : 25 Juni 2023

Tipe Dokumen : Lab Manual

Klasifikasi : Publik

A. Vulnerability Assessment

Asumsi scan dilakukan secara **black-box**

1. Nyalakan nessus
2. Klik new scan pilih advanced scan
3. Pastikan sedang ada di tab settings > basic > general
4. Isikan informasi target :

Name : Scan Lab

Description : Vulnerability Assessment praktik

Targets : 192.168.112.132

Scan Lab / Configuration

[Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Scan Lab

Description: Vulnerability Assessment praktik

Folder: My Scans ▾

Targets: 192.168.112.132

Upload Targets [Add File](#)

5. Pindah ke menu Discovery > Host Discovery, matikan "Ping the remote Host"

Scan Lab / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins

BASIC

DISCOVERY

● Host Discovery

Port Scanning

Service Discovery

Identity

ASSESSMENT

REPORT

ADVANCED

Remote Host Ping

Ping the remote host

OFF

Fragile Devices

☐

Scan Network Printers

☐

Scan Novell Netware hosts

☐

Scan Operational Technology devices

Wake-on-LAN

List of MAC addresses

Add File

Boot time wait (in minutes)

5

6. Pada menu Discovery > Port Scanning, ubah "Port Scan Range" dari default menjadi all

Scan Lab / Configuration
[Back to Scan Report](#)

Settings
Credentials
Plugins

BASIC >

DISCOVERY v

Host Discovery

Port Scanning

Service Discovery

Identity

ASSESSMENT >

REPORT >

ADVANCED >

Ports

☐ Consider unscanned ports as closed

Port scan range:

Local Port Enumerators

☒ SSH (netstat)

☒ WMI (netstat)

☒ SNMP

☒ Only run network port scanners if local port enumeration failed

☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

7. Klik tombol Save
8. Launch scan
9. Ambil contoh validasi kerentanan smb signing

```
nmap -p 445 --script smb2-security-mode 192.168.112.132
```

10. Generate report raw di Nessus
11. Contoh report va :

<https://purplesec.us/wp-content/uploads/2019/12/Sample-Vulnerability-Assessment-Report-PurpleSec.pdf>

B. Penetration Testing – Web Application Pentest

1. Buka port 8080, menemukan easychat server
2. Cari exploit easychat server di internet
3. Coba exploit easychat server ke target
4. Mendownload testplan wstg
<https://github.com/OWASP/wstg>
5. Cara menemukan testing guide point, contohnya clickjacking
 - a. Kopikan nama test nya : testing for clickjacking
 - b. Kopikan kode testnya : wstg-clnt-09
 - c. Cari di google : "wstg-clnt-09 testing for clickjacking"
6. Test clickjacking ke target port 80

...

```
<html>
```

```
  <head>
```

```
    <title>Clickjack test page</title>
```

```
  </head>
```

```
  <body>
```

```
    <iframe src="http://192.168.112.132" width="500" height="500"></iframe>
```

```
  </body>
```

```
</html>
```

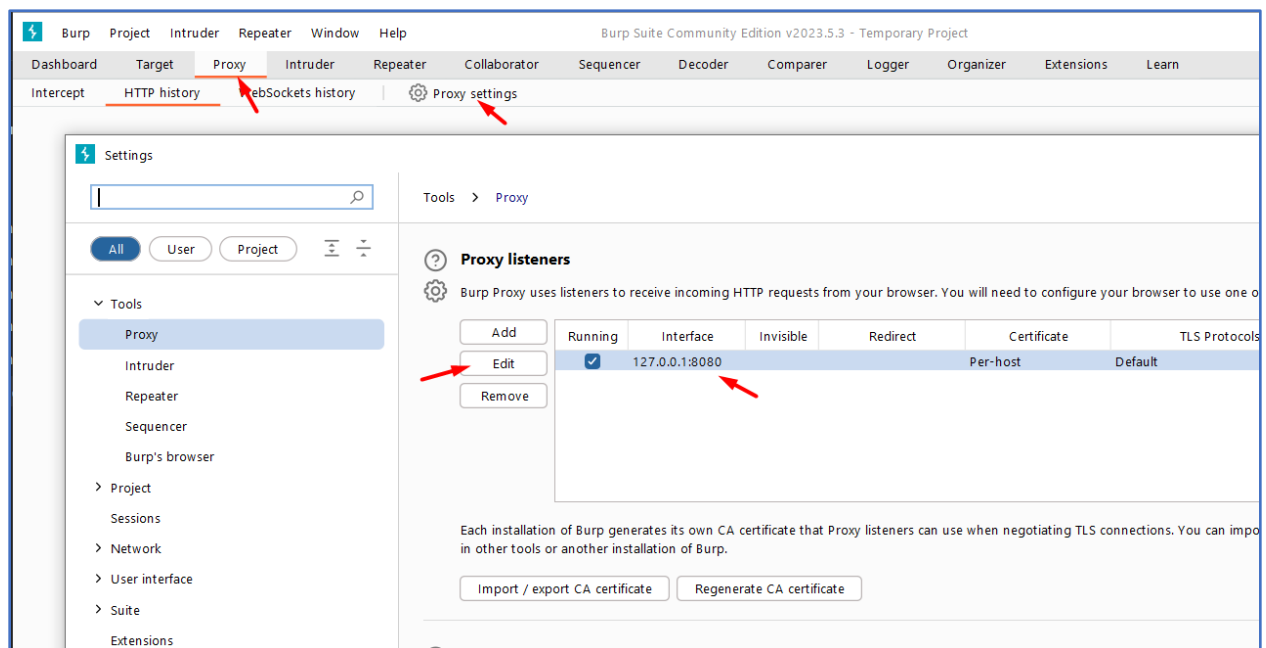
...

7. Buka website cvss 3.1
8. Hitung cvss 3.1 nya

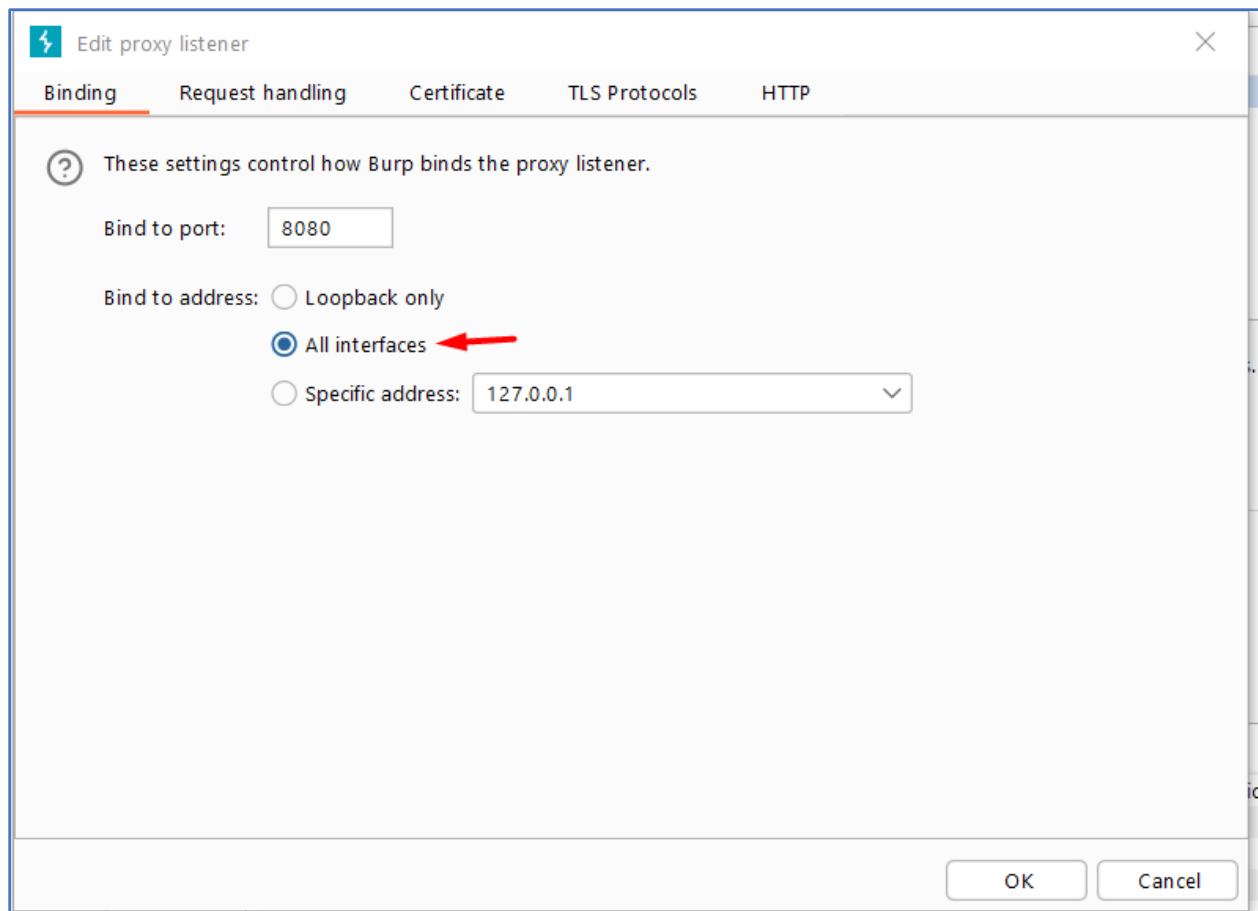
C. Penetration Testing – Mobile Application Pentest

Saya mendetailkan pada bagian dynamic testing (bypass ssl pinning), mengingat kemungkinan besar waktu tidak cukup untuk menjelaskan masing masing detil langkahnya.

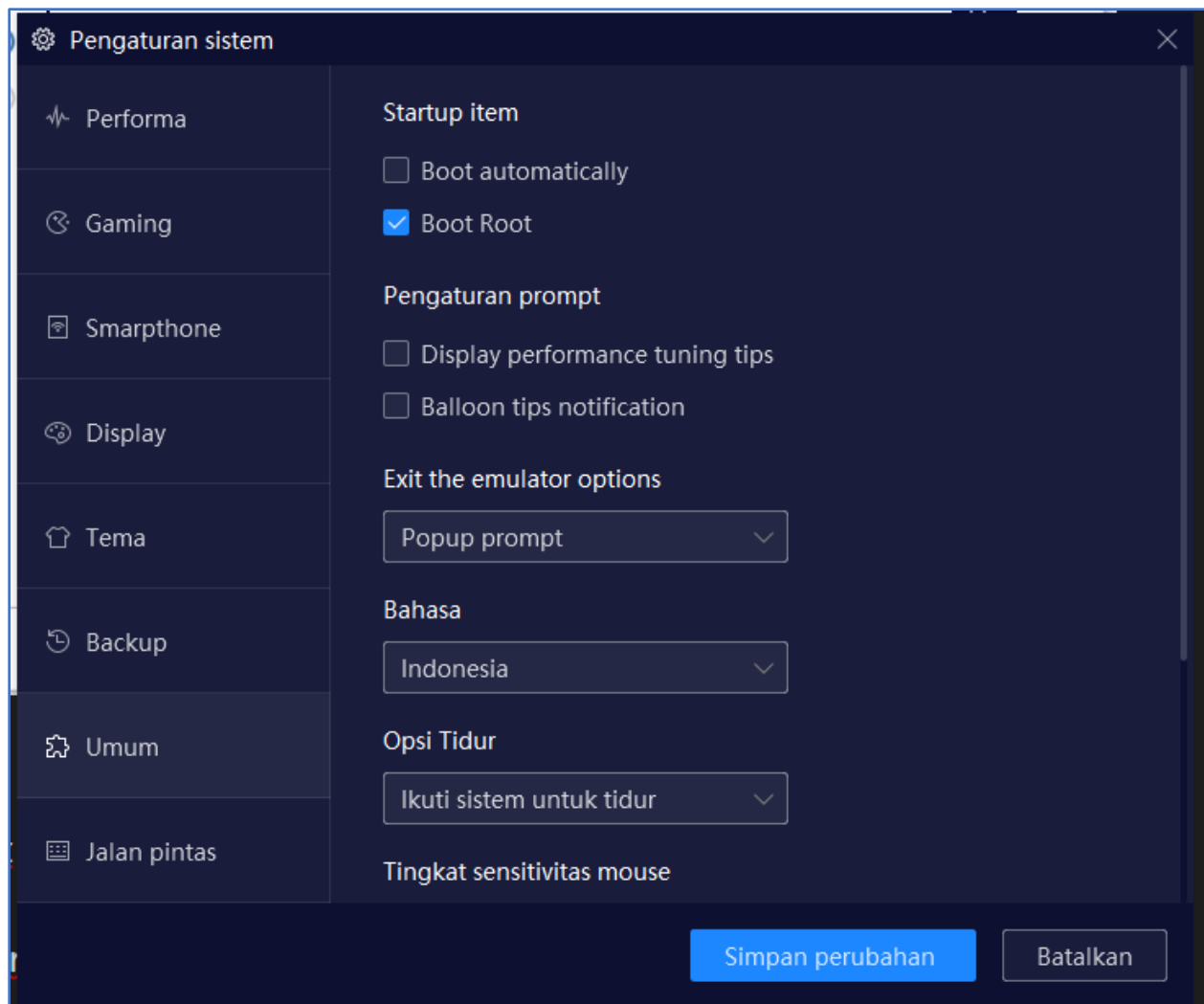
1. Jalankan mobsf
2. Upload file apk ke mobsf
3. Generate report
4. Jalankan aplikasi di emulator
 - Buka nox
 - Install apps pinning-demo.apk
5. Proxy kan nox ke burpsuite
 - Download burpsuite dari sini : <https://portswigger.net/burp/communitydownload>
 - Instalasi burpsuite lihat sini : <https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install>
6. Setel port proxy di burpsuite untuk bisa listen di semua ip address
 - Di burpsuite pergi ke proxy > proxy setting, kemudian klik pilih proxy yang berjalan (127.0.0.1:8080) dan klik edit



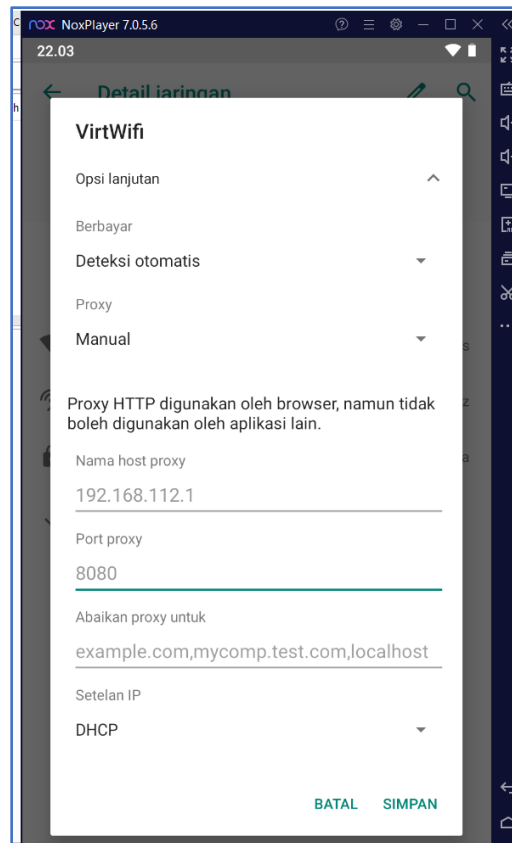
- Ubah ke All Interfaces



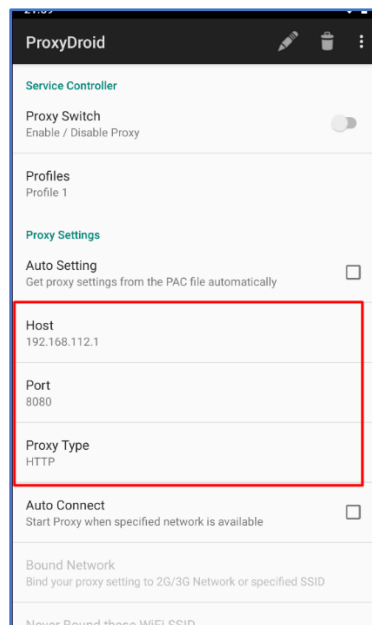
7. Setting proxy di nox (setting nox untuk boot root, install proxy droid dan setel di proxy droid)
 - Pada Nox Player, pergi ke pengaturan System > Umum, dan centang Boot Root. Nox akan merestart vm, setelah itu kita akan booting dg kondisi Rooted di nox.



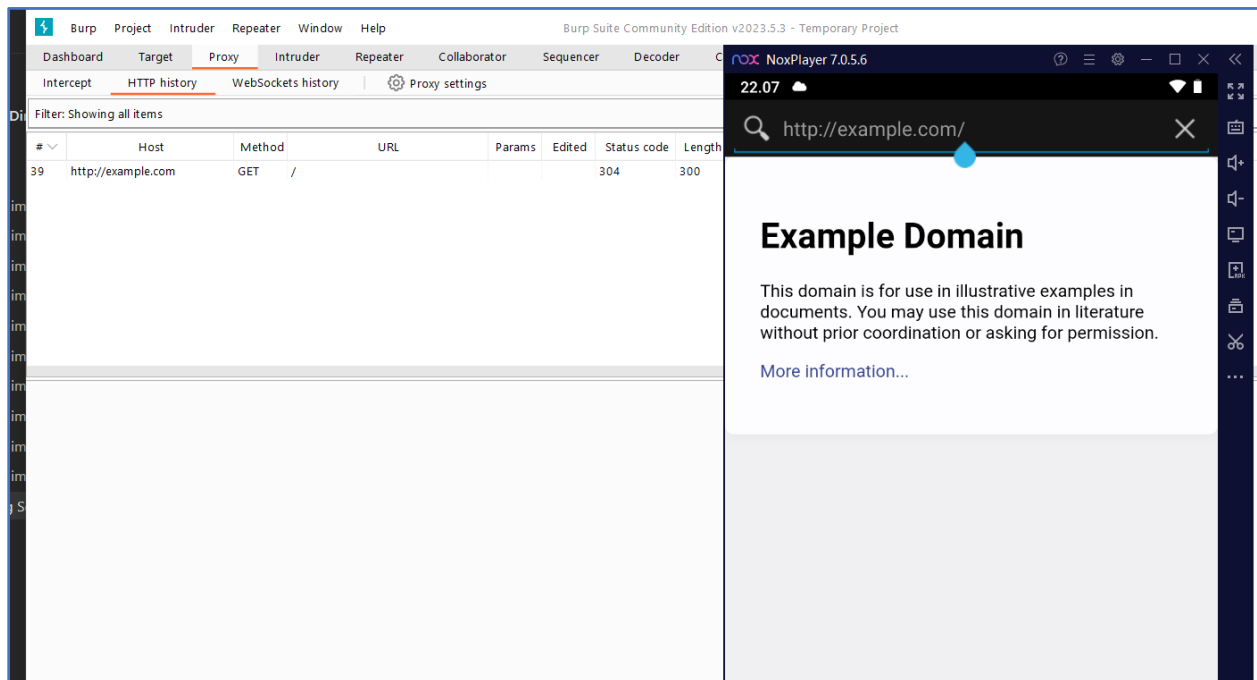
- Ada dua alternatif ketika menggunakan proxy di android, bisa dengan menyetel proxy di pengaturan wifi atau menggunakan proxydroid. Gunakan cara yang paling nyaman saja
- a. Setel Proxy pada settingan koneksi di nox



- b. Menggunakan Proxy Droid. Lakukan Instalasi aplikasi proxyDroid terlebih dahulu



- Atur Host dg IP Address PC kamu yang menjalankan burpsuite
- Port 8080 sesuai dengan settingan Burpsuite
- Proxy Type HTTP
- Kemudian Turn On proxy dg meng-klik Proxy Switch
- c. Kemudian untuk memastikan apakah burpsuite sudah dapat menangkap request HTTP dari nox adalah dengan mengunjungi `http://example.com` atau web dg koneksi http lainnya, ingat bukan https.
- d. Jika burpsuite sudah menangkap request, kita akan lanjutkan dengan instalasi sertifikat postwigger di nox.



- e. ketika mengunjungi website https, akan ada peringatan dari browser bahwa certificate ssl tidak valid. Hal ini dapat diatasi dengan menginstall certificate burpsuite ke device kita.
8. Install certificate burpsuite di nox
- a. Kunjungi `http://burp` di browser yang sudah di set proxy ke burpsuite, kemudian klik tombol CA Certificate.

- Punya saya menjadi :
9a5ba575.0
- g. Ubah cacert.pem jadi 9a5ba575.0
move cacert.pem 9a5ba575.0
- h. Gunakan adb shell untuk mengupload file 9a5ba575.0 ke /system/etc/security/cacerts/
 - *adb root*
 - *adb remount*
 - *adb push 9a5ba575.0 /system/etc/security/cacerts/9a5ba575.0*

```

D:\PPT\Sharing session Amikom>adb push 9a5ba575.0 /system/etc/security/cacerts/9a5ba575.0
adb: error: failed to copy '9a5ba575.0' to '/system/etc/security/cacerts/9a5ba575.0': couldn't create file: Read-only file system

D:\PPT\Sharing session Amikom>adb root

D:\PPT\Sharing session Amikom>adb remount
remount succeeded

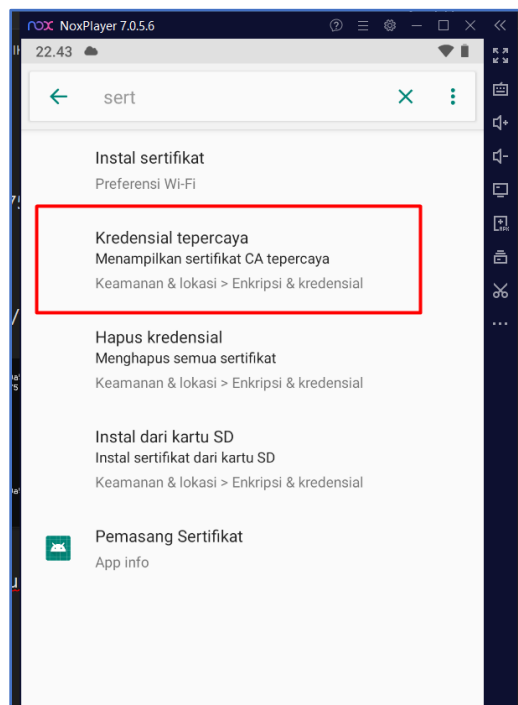
D:\PPT\Sharing session Amikom>adb shell
star2lte:/ # exit

D:\PPT\Sharing session Amikom>adb push 9a5ba575.0 /system/etc/security/cacerts/9a5ba575.0
[100%] /system/etc/security/cacerts/9a5ba575.0

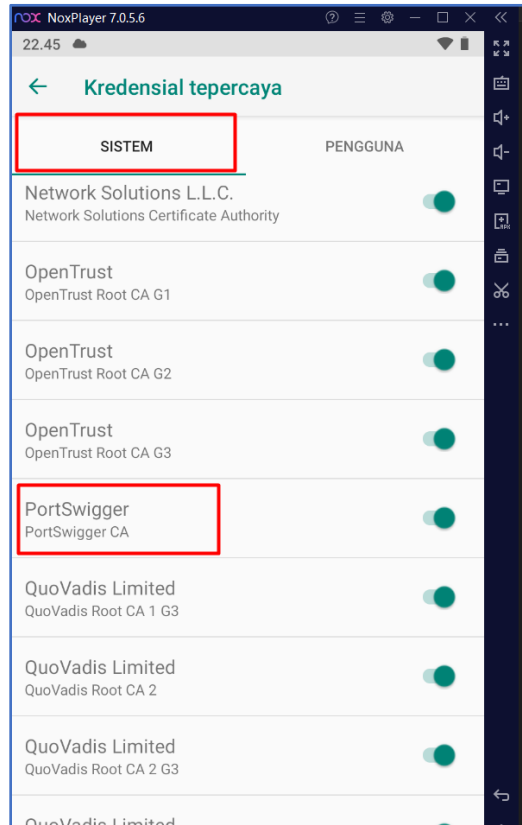
D:\PPT\Sharing session Amikom>

```

9. Masuk ke nox, pergi ke setelan, dan cari dg kata kunci "sert" atau "cert" apa bila dalam bahasa inggris.
10. Pilih Kredensial terpercaya > Kredensial Terpercaya



11. Pada bagian sistem di menu Kredensial Terpercaya, kita bisa menemukan PortSwigger sudah menjadi certificate yang terpercaya



12. Untuk memastikan hasilnya, kita bisa membuka website dengan https. semisal wbesite portal amikom. Dan melihat sudah tidak ada lagi popup ydari browser yang menyatakan bahwa sertifikat tidak valid.

The image shows a Burp Suite interface on the left and a mobile browser on the right. The Burp Suite interface displays a list of intercepted HTTP requests and responses. The selected request is a GET request for the favicon of Universitas Amikom Purwokerto. The response is an HTML page with a title 'Terakreditasi B' (Accredited B) and a message from the Indonesian Ministry of Education and Culture.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
10	https://t.clarity.ms	POST	/collect		✓	204	297			
09	https://t.clarity.ms	POST	/collect		✓	204	297			
08	https://www.facebook.com	GET	/tr/?id=334576448178887&ev=M...		✓	200	331	text		
07	https://www.facebook.com	GET	/tr/?id=614868669095964&ev=M...		✓	200	331	text		
06	https://t.clarity.ms	POST	/collect		✓	204	297			
05	https://www.facebook.com	GET	/tr/?id=334576448178887&ev=P...		✓	200	331	text		
04	https://www.facebook.com	GET	/tr/?id=614868669095964&ev=P...		✓	200	331	text		
03	https://amikompurwokerto.ac.id	GET	/style/icon/favicon.png		✓	200	2907	HTML	png	Universitas Amikom
02	https://www.clarity.ms	GET	/tag/7npdbs5stv?ref=gtm2		✓	200	1248	script	webp	Universitas Amikom
01	https://amikompurwokerto.ac.id	GET	/style/images/index/bg-testimonia...		✓	200	2907	HTML		
00	https://t.clarity.ms	POST	/collect		✓	204	297			

Request

```

1 GET /style/icon/favicon.png HTTP/1.1
2 Host: amikompurwokerto.ac.id
3 Cookie: ci_sessionid=61a7c7e7e302e2b25afcb047066efa6d309e2; ga_J29K44Y112=gs1.1.1687620400.1.1.1687621596.60.0.0; fbp=2.1687621596937.1709106392; _ga=GA1.3.1409638106.1687620401; _gid=GA1.3.2054930258.1687621597; _dc_gtm_UA-193770851-2=1; _clsk=zdch4d12f0q101270; _clsk=jdch4d12f0q101270; _clsk=jdch4d12f0q101270
4 User-Agent: Mozilla/5.0 (Linux; Android 9; SM-G965W Build/QP1A.190711.000; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/92.0.4515.131 Mobile Safari/537.36
5 Accept: image/avif, image/webp, image/apng, image/svg+xml, image/*; q=0.8
6 X-Requested-With: com.android.browser
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: no-cors
9 Sec-Fetch-Dest: image
10 Referer: https://amikompurwokerto.ac.id/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: id-ID, q=0.9, en-US; q=0.8, en; q=0.7
13 Connection: close

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sat, 24 Jun 2023 15:51:24 GMT
3 Server: Apache/2.4.56 (Ubuntu) OpenSSL/1.0.2k-fips
4 X-Powered-By: PHP/5.4.45
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding, User-Agent
9 Content-Length: 2523
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE HTML>
14 <html>
15 <head>
16 <title>
17 Universitas Amikom Purwokerto
18 </title>
19 <link rel="shortcut icon" type="image/x-icon" href="https://amikompurwokerto.ac.id/images/amikompurwokerto/favicon.ico" />
20 <meta name="viewport" content="width=device-width, initial-scale=1" />
21 <meta http-equiv="Content-Type" content="text/html;" />
22 <script type="text/javascript" language="javascript" src="https://amikompurwokerto.ac.id/ckeditor/ckeditor.js"></script>

```

The mobile browser shows the website of Universitas Amikom Purwokerto. The page features a banner for 'SELAMAT DATANG DI KAMPUS Technopreneur BERBASIS TEKNOLOGI DAN BISNIS' and a section titled 'Terakreditasi B' (Accredited B) with a message from the Indonesian Ministry of Education and Culture.

13. Kita sudah bisa melakukan tamper request dan response https pada browser di handphone, tapi proses di aplikasi, apabila ada ssl pinning, masih akan terjadi eror pada saat proses tampering, biasanya di tandai dengan request dan response tidak masuk ke HTTP History dan juga ada pesan eror pada dashboard Burpsuite.

14. Jalankan apps pinning-demo.apk

15. Unpinned Request

The image shows a screenshot of a mobile application interface (NoxPlayer) displaying an "SSL Pinning Demo". The app has a purple header with the title "SSL Pinning Demo" and a status bar at the top showing the time "22:50". Below the header, there is a list of buttons: "UNPINNED REQUEST" (highlighted with a red box), "CONFIG-PINNED REQUEST", "OKHTTP PINNED REQUEST", "VOLLEY PINNED REQUEST", "TRUSTKIT PINNED REQUEST", and "MANUALLY PINNED REQUEST".

In the background, the Burp Suite interface is visible. The "HTTP history" tab is active, showing a list of intercepted requests. The first request is highlighted with a red box. The details of the selected request are shown in the "Request" and "Response" panels.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
333	https://example.com	GET	/			200	1588	HTML		Example Domain
332	https://example.com	GET	/			200	1588	HTML		Example Domain
331	https://biyeshen.com	POST	/sa		✓	200	185	text		
330	http://t4.appmeasurements...	GET	/html/os9/dogs/5e2e2a99842525...			200	701	text	md5	
329	http://bae.appmeasurements...	GET	/bae/ags/agiles9.html			200	2055	HTML	html	
328	https://stup9.appmeasurements...	GET	/stup/postback/1/stup9			200	737	JSON		
327	https://example.com	GET	/			200	1587	HTML		Example Domain
326	https://biyeshen.com	POST	/sa		✓	200	185	text		
325	https://reign.appmeasurements...	POST	/ethic/onward		✓	403	729	text		
324	https://t.clarity.ms	POST	/collect		✓	204	297			
323	https://t.clarity.ms	POST	/collect		✓	204	297			

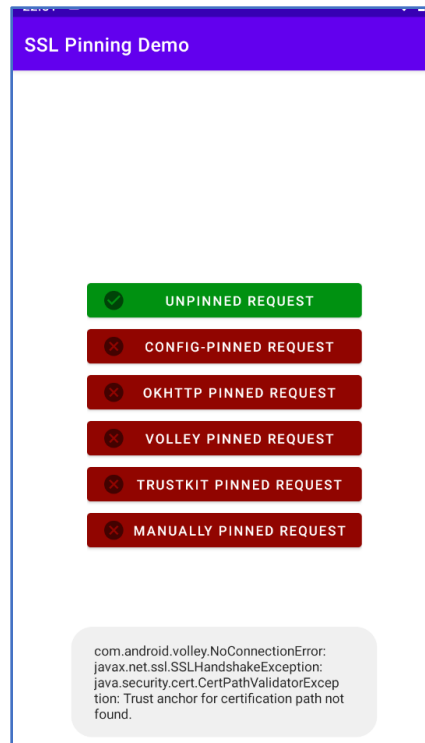
Request

```
1 GET / HTTP/2
2 Host: example.com
3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; SM-G965W
  Build/QP1A.190711.020)
4 Connection: Keep-Alive
5 Accept-Encoding: gzip, deflate
```

Response

```
1 HTTP/2 200 OK
2 Age: 415310
3 Cache-Control: max-age=604800
4 Content-Type: text/html; charset=UTF-8
5 Date: Sat, 24 Jun 2023 15:49:58 GMT
6 Etag: "3147526947+gzip"
7 Expires: Sat, 01 Jul 2023 15:49:58 GMT
8 Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
9 Server: ECS (oxt/8310)
10 Vary: Accept-Encoding
11 X-Cache: HIT
12 Content-Length: 1256
13
14 <!doctype html>
15 <html>
16 <head>
17 <title>
  Example Domain
</title>
18
19 <meta charset="utf-8" />
20 <meta http-equiv="Content-type" content="text/h
  " />
21 <meta name="viewport" content="width=device-wid
  initial-scale=1" />
22 <style type="text/css">
23 body{
```

16. Pinned Request akan menolak karena SSL certificate yang didapatkan berbeda dari yang mereka simpan.



- Pada HTTP History tidak akan ada request dan response yang berhasil di tangkap.
- Pada event log di dashboard, request yang gagal karena SSL ini dapat dilihat

The screenshot shows the Burp Suite Community Edition v2023.5.3 interface. The "Event log" tab is selected, displaying a list of events. The following table represents the data shown in the Event log:

Time	Type	Source	Message
22:52:52 24 Jun 2023	Error	Proxy	[18] The client failed to negotiate a TLS connection to b-graph.facebook.com:443: Received fatal alert: handshake_failure
22:51:02 24 Jun 2023	Error	Proxy	[10] The client failed to negotiate a TLS connection to sha512.badssl.com:443: Received fatal alert: handshake_failure
22:50:56 24 Jun 2023	Error	Proxy	[2] Unknown host: overmind.datatheorem.com
22:44:47 24 Jun 2023	Error	Proxy	[4] The client failed to negotiate a TLS connection to lookaside.facebook.com:443: Received fatal alert: handshake_failure
22:44:42 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to api.facebook.com:443: Received fatal alert: handshake_failure
22:44:42 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to b-api.facebook.com:443: Received fatal alert: handshake_failure
22:44:42 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to graph.facebook.com:443: Received fatal alert: handshake_failure
22:43:08 24 Jun 2023	Error	Proxy	[2] No response received from remote server.
22:33:57 24 Jun 2023	Error	Proxy	[14] The client failed to negotiate a TLS connection to biyeshen.com:443: Received fatal alert: handshake_failure
22:30:04 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to overmind.datatheorem.com:443: Received fatal alert: handshake_failure
22:29:57 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to example.com:443: Remote host terminated the TCP connection
22:29:38 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to edge-mqtt.facebook.com:443: Remote host terminated the TCP connection
22:29:38 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to connectivitycheck.gstatic.com:443: Received fatal alert: handshake_failure
22:29:38 24 Jun 2023	Error	Proxy	[12] Authentication failure from b-graph.facebook.com
22:28:05 24 Jun 2023	Error	Proxy	The client failed to negotiate a TLS connection to alt4-mtalk.google.com:443: Received fatal alert: handshake_failure
22:28:04 24 Jun 2023	Error	Proxy	[8] The client failed to negotiate a TLS connection to mtalk.google.com:443: Received fatal alert: handshake_failure
22:26:42 24 Jun 2023	Error	Proxy	[1] The client failed to negotiate a TLS connection to atm-kfw443-cvnet.scr.sncorp.cn:443: Received fatal alert: handshake_failure

17. Bypass pinning-demo.apk menggunakan frida

- a. Untuk proses upload frida, dan instalasi frida akan kita skip. Bisa cek url berikut :
<https://medium.com/my-infosec-write-ups/frida-installation-40f52845ae98>
- b. Jalankan frida server di nox
 - o adb shell
 - o cd /data/local/tmp
 - o ./frida15 &

```
D:\PPT\Sharing session Amikom>adb shell
star2lte:/ # cd /data/local/tmp
star2lte:/data/local/tmp # ls
frida15 oat re.frida.server
star2lte:/data/local/tmp # ./frida15 &
[1] 9532
star2lte:/data/local/tmp #
```

- c. Cek aplikasi yang berjalan menggunakan frida pada windows
 - o frida-ps -Uai

```
D:\PPT\Sharing session Amikom>frida-ps -Uai
PID   Name                               Identifier
-----
9070   Browser                           com.android.browser
8792   Facebook                         com.facebook.katana
7262   File                             com.android.documentsui
8284   Google Play Store                com.android.vending
4072   ProxyDroid                       org.proxydroid
9292   SSL Pinning Demo                 tech.http toolkit.pinning_demo
-   Amaze                           com.amaze.filemanager
-   App Center                      com.android.Calendar
-   Fita                           com.muna.lively
-   Galeri                         com.android.gallery3d
-   Gods and Demons: Legend         com.tzgames.gadand
-   Google Play Game                com.google.android.play.games
-   GoogleSign                     com.pekall.fmradio
-   KBM App                        com.ketix.application
-   Kamera                        com.android.camera2
-   Qoinpay                        id.qoin.crypto
-   Setelan                       com.android.settings
-   Tutorials                     com.android.calculator2
-   Wpk11 Qt                      com.ytnxuul
-   Wpk11 Qt                      com.ytnxuul

D:\PPT\Sharing session Amikom>
```

- d. Dapat dilihat nama package dari aplikasi SSL pinning demo, yaitu tech.http toolkit.pinning_demo
- e. Gunakan frida multiple unpinning script, untuk bypass SSL pinning
 - o Script : <https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/>
 - o Saya simpan script di local dg nama fmu.js agar lebih mudah mengetik commandnya
 - o Eksekusi command Frida

frida -Uf tech.http toolkit.pinning_demo -l fmu.js --no-pause

```
D:\PPT\Sharing session Amikom>frida -Uf tech.http toolkit.pinning_demo -l fmu.js --no-pause

/---|   Frida 15.2.2 - A world-class dynamic instrumentation toolkit
|_ _|
|_|_|
>_|_|
/_/_|_|

Commands:
  help      -> Displays the help system
  object?   -> Display information about 'object'
  exit/quit -> Exit

More info at https://frida.re/docs/home/

Connected to SM-G965N (id=127.0.0.1:62001)
Spawned `tech.http toolkit.pinning_demo`. Resuming main thread!
[SM-G965N::tech.http toolkit.pinning_demo ]->
=====
[#] Android Bypass for various Certificate Pinning methods [#]
=====
[-] OkHTTPv3 (2) pinner not found
[-] Appcelerator PinningTrustManager pinner not found
[-] Fabric PinningTrustManager pinner not found
[-] OpenSSLSocketImpl Conscrypt (1) pinner not found
[-] OpenSSLSocketImpl Conscrypt (2) pinner not found
[-] OpenSSLEngineSocketImpl Conscrypt pinner not found
[-] OpenSSLSocketImpl Apache Harmony pinner not found
[-] PhoneGap sslCertificateChecker pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey (1) pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey (2) pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning (1) pinner not found
```

- f. Kita sudah bisa melakukan bypass ssl pinning yang dilakukan oleh beberapa library

⚡

Burp

Project

Intruder

Repeater

Window

Help

Burp Suite Community Edition v2023.5.3 - Te

23.03

🔍 ⚙️ 🗖️ 🗖️

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

...

Intercept

HTTP history

WebSockets history

⚙️ Proxy settings

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	E
350	https://sha512.badssl.com	GET	/			200	745	HTML	
349	https://sha512.badssl.com	GET	/			200	745	HTML	
348	https://sha512.badssl.com	GET	/			200	745	HTML	
347	https://sha512.badssl.com	GET	/			200	745	HTML	
346	https://example.com	GET	/			200	1605	HTML	
345	https://content-signature-2....	GET	/chains/onecrl.content-signature...			304	168		ch
344	https://firefox.settings.servic...	GET	/v1/buckets/security-state/collecti...	✓		200	3059	JSON	
343	https://firefox.settings.servic...	GET	/v1/buckets/monitor/collections/c...	✓		200	957	JSON	
342	https://biyeshen.com	POST	/sa	✓		200	185	text	
341	https://biyeshen.com	POST	/sa	✓		200	185	text	
340	https://reign.appmeasure...	POST	/ethic/onward	✓		403	733	text	
339	https://reign.appmeasure...	POST	/ethic/onward	✓		200	185	text	

Request

Raw

Hex

1 GET / HTTP/1.1

2 Host: sha512.badssl.com

3 Accept-Encoding: gzip, deflate

4 User-Agent: okhttp/4.5.0

5 Connection: close

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

135