Dynamic Analysis of Medical Android Apps

Nikhil Chopra

Kanika Gupta

Problem Statement

- Analyse SSL implementation of Medical Apps
- Ideal SSL implementation in apps is divided into two parts –

1. Certificate Validation
    - While connecting to the server, App checks if server certificate is signed by a trusted certificate authority

2. Host name Verification
    - App checks if certificate presented by the server is having server’s name in subjectAltName field of type dnsName. **Common Name is deprecated.**

Methodology

- Setup a MiTM proxy server – Telerik Fiddler
- Send data packets from app to the proxy.
- Check Certificate Validation, Host Name Verification and Certificate Pinning individually.

Check Certificate Validation – correct Hostname, wrong Root CA

- **No Fiddler root** is installed as a trusted root CA in the phone as we will be verifying –
    - ✓Is the app checking if server’s certificate is signed by a trusted root CA.

- Fiddler will be sending the **fake server certificate with Correct Hostname** i.e. hostname of the actual server.

- Check if we can log in the app.

Check Host name verification – correct CA, wrong hostname

- **Fiddler root is installed** as a trusted root CA in the phone

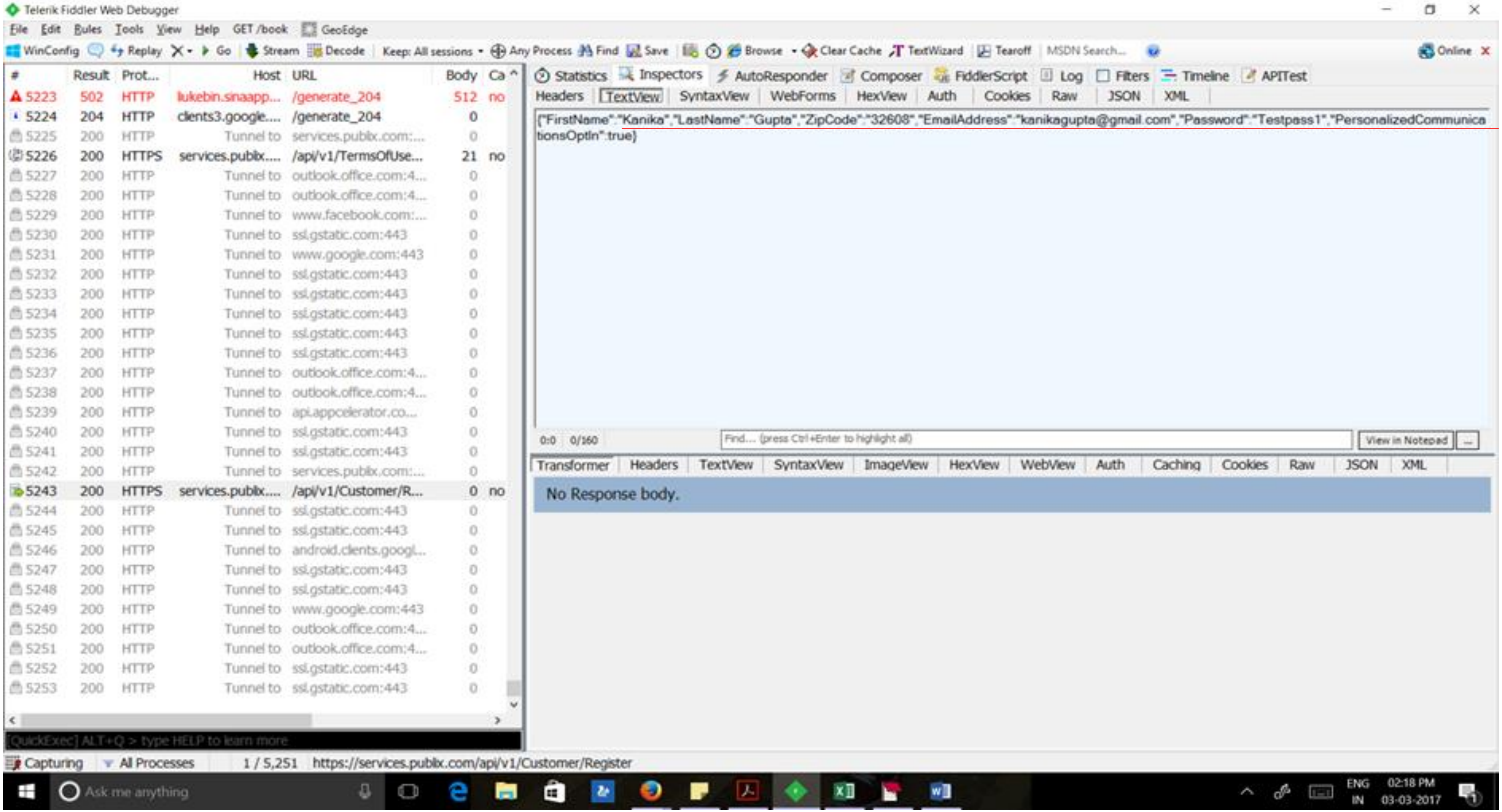
- Fiddler will be sending the **server certificate with Fake Hostname** as we want to check –
  - ✓ Is app explicitly checking the hostname of the certificate or it is letting it pass by just checking that its signed by a trusted CA.

- Check if we can log in the app.

Check Certificate Pinning– correct CA, correct hostname (BOTH FAKE in a way)

- **Fiddler root is installed** as a trusted root CA in the phone
- Fiddler will be sending the **server certificate with correct Hostname**
- We want to check if we can give illegitimate certificate [signed by self-signed proxy] generated by an illegitimate server to the app and whether app accepts it or not.
- Check if we can log in the app.

Publix – No root Installed, Bad Hostname (Sign Up)


Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Statistics Inspectors AutoResponder Composer FiddlerScript Log Filters Timeline APITest
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML
Find... (press Ctrl+Enter to highlight all)
View in Notepad
0:0 0/160
Ask me anything
ENG IN 02:18 PM 03-03-2017

#	Result	Prot...	Host	URL	Body	Ca
5223	502	HTTP	lukebin.sinaapp...	/generate_204	512	no
5224	204	HTTP	clients3.google....	/generate_204	0	
5225	200	HTTP	Tunnel to	services.publix.com:...	0	
5226	200	HTTPS	services.publix....	/api/v1/TermsOfUse...	21	no
5227	200	HTTP	Tunnel to	outlook.office.com:4...	0	
5228	200	HTTP	Tunnel to	outlook.office.com:4...	0	
5229	200	HTTP	Tunnel to	www.facebook.com:...	0	
5230	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5231	200	HTTP	Tunnel to	www.google.com:443	0	
5232	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5233	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5234	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5235	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5236	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5237	200	HTTP	Tunnel to	outlook.office.com:4...	0	
5238	200	HTTP	Tunnel to	outlook.office.com:4...	0	
5239	200	HTTP	Tunnel to	api.appcelerator.co...	0	
5240	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5241	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5242	200	HTTP	Tunnel to	services.publix.com:...	0	
5243	200	HTTPS	services.publix....	/api/v1/Customer/R...	0	no
5244	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5245	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5246	200	HTTP	Tunnel to	android.clients.googl...	0	
5247	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5248	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5249	200	HTTP	Tunnel to	www.google.com:443	0	
5250	200	HTTP	Tunnel to	outlook.office.com:4...	0	
5251	200	HTTP	Tunnel to	outlook.office.com:4...	0	
5252	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	
5253	200	HTTP	Tunnel to	ssl.gstatic.com:443	0	

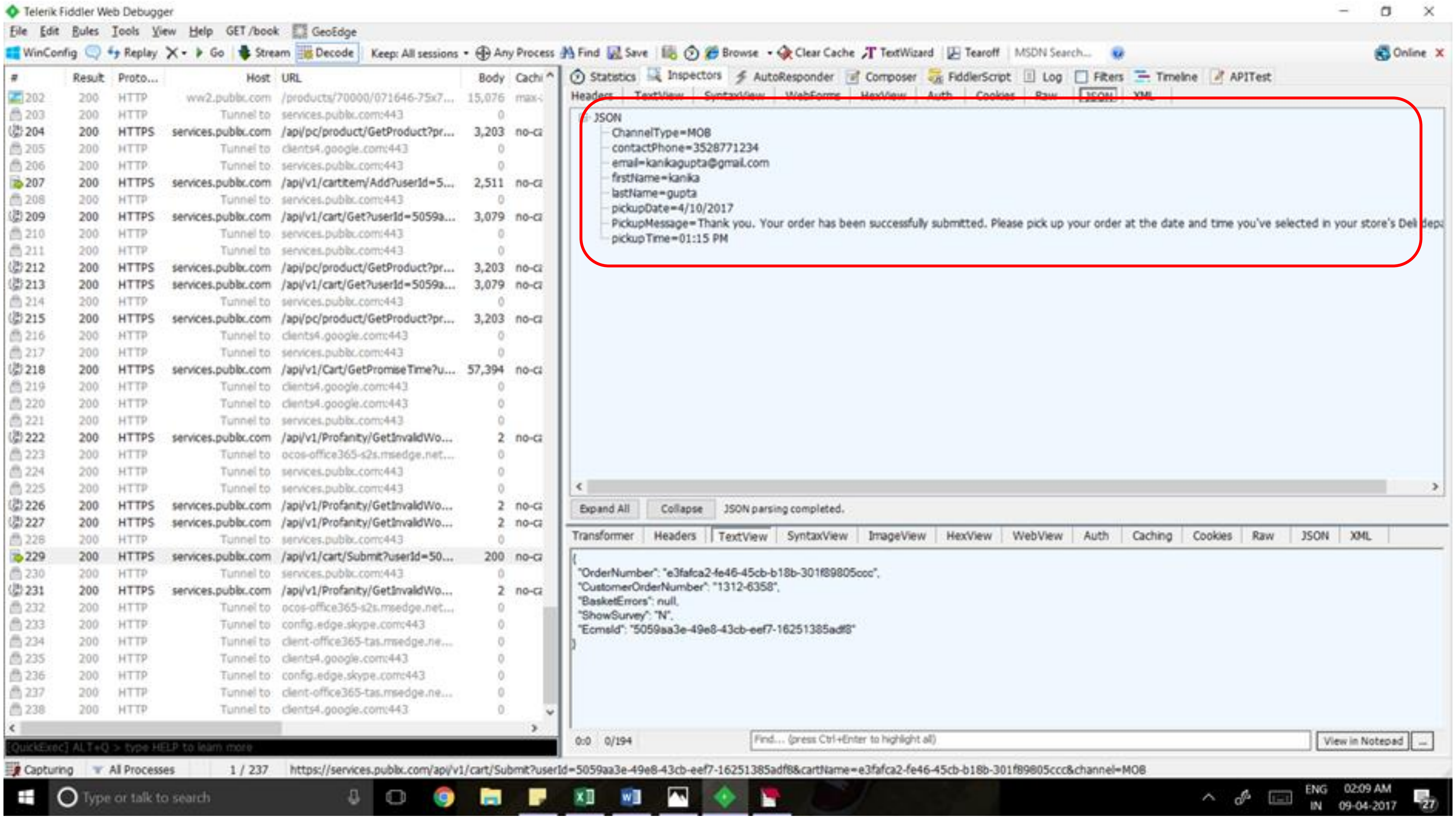
```
{"FirstName":"Kanika","LastName":"Gupta","ZipCode":"32608","EmailAddress":"kanikagupta@gmail.com","Password":"Testpass1","PersonalizedCommunica
tionsOptIn":true}
```

No Response body.

[QuickExec] ALT+Q > type HELP to learn more

Capturing All Processes 1 / 5,251 https://services.publix.com/api/v1/Customer/Register

Publix – Order placed online, No certificate validation, No Hostname Verification


Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
WinConfig Replay X Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Statistics Inspectors AutoResponder Composer FiddlerScript Log Filters Timeline APITest
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Expand All Collapse
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML
View in Notepad
Type or talk to search
ENG IN 02:09 AM 09-04-2017

#	Result	Proto...	Host	URL	Body	Cachi
202	200	HTTP	ww2.publix.com	/products/70000/071646-75x7...	15,076	max-:
203	200	HTTP	Tunnel to	services.publix.com:443	0	
204	200	HTTPS	services.publix.com	/api/pc/product/GetProduct?pr...	3,203	no-ca
205	200	HTTP	Tunnel to	clients4.google.com:443	0	
206	200	HTTP	Tunnel to	services.publix.com:443	0	
207	200	HTTPS	services.publix.com	/api/v1/cartitem/Add?userId=5...	2,511	no-ca
208	200	HTTP	Tunnel to	services.publix.com:443	0	
209	200	HTTPS	services.publix.com	/api/v1/cart/Get?userId=5059a...	3,079	no-ca
210	200	HTTP	Tunnel to	services.publix.com:443	0	
211	200	HTTP	Tunnel to	services.publix.com:443	0	
212	200	HTTPS	services.publix.com	/api/pc/product/GetProduct?pr...	3,203	no-ca
213	200	HTTPS	services.publix.com	/api/v1/cart/Get?userId=5059a...	3,079	no-ca
214	200	HTTP	Tunnel to	services.publix.com:443	0	
215	200	HTTPS	services.publix.com	/api/pc/product/GetProduct?pr...	3,203	no-ca
216	200	HTTP	Tunnel to	clients4.google.com:443	0	
217	200	HTTP	Tunnel to	services.publix.com:443	0	
218	200	HTTPS	services.publix.com	/api/v1/Cart/GetPromiseTime?u...	57,394	no-ca
219	200	HTTP	Tunnel to	clients4.google.com:443	0	
220	200	HTTP	Tunnel to	clients4.google.com:443	0	
221	200	HTTP	Tunnel to	services.publix.com:443	0	
222	200	HTTPS	services.publix.com	/api/v1/Profanity/GetInvalidWo...	2	no-ca
223	200	HTTP	Tunnel to	ocos-office365-s2s.msedge.net...	0	
224	200	HTTP	Tunnel to	services.publix.com:443	0	
225	200	HTTP	Tunnel to	services.publix.com:443	0	
226	200	HTTPS	services.publix.com	/api/v1/Profanity/GetInvalidWo...	2	no-ca
227	200	HTTPS	services.publix.com	/api/v1/Profanity/GetInvalidWo...	2	no-ca
228	200	HTTP	Tunnel to	services.publix.com:443	0	
229	200	HTTPS	services.publix.com	/api/v1/cart/Submit?userId=50...	200	no-ca
230	200	HTTP	Tunnel to	services.publix.com:443	0	
231	200	HTTPS	services.publix.com	/api/v1/Profanity/GetInvalidWo...	2	no-ca
232	200	HTTP	Tunnel to	ocos-office365-s2s.msedge.net...	0	
233	200	HTTP	Tunnel to	config.edge.skype.com:443	0	
234	200	HTTP	Tunnel to	client-office365-tas.msedge.ne...	0	
235	200	HTTP	Tunnel to	clients4.google.com:443	0	
236	200	HTTP	Tunnel to	config.edge.skype.com:443	0	
237	200	HTTP	Tunnel to	client-office365-tas.msedge.ne...	0	
238	200	HTTP	Tunnel to	clients4.google.com:443	0	

```
JSON
  ChannelType=MOB
  contactPhone=3528771234
  email=kanikagupta@gmail.com
  firstName=kanika
  lastName=gupta
  pickupDate=4/10/2017
  PickupMessage=Thank you. Your order has been successfully submitted. Please pick up your order at the date and time you've selected in your store's Deli depa
  pickupTime=01:15 PM
```

JSON parsing completed.

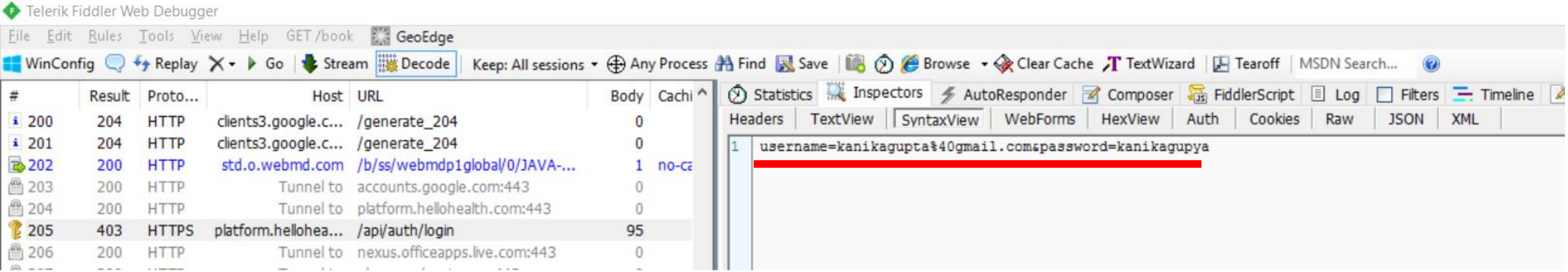
```
{
 "OrderNumber": "e3fafca2-fe46-45cb-b18b-301f89805ccc",
 "CustomerOrderNumber": "1312-6358",
 "BasketErrors": null,
 "ShowSurvey": "N",
 "EcmsId": "5059aa3e-49e8-43cb-eef7-16251385adf8"
}
```

0:0 0/194 Find... (press Ctrl+Enter to highlight all)

[QuickExec] ALT+Q > type HELP to learn more

Capturing All Processes 1 / 237 https://services.publix.com/api/v1/cart/Submit?userId=5059aa3e-49e8-43cb-eef7-16251385adf8&cartName=e3fafca2-fe46-45cb-b18b-301f89805ccc&channel=MOB

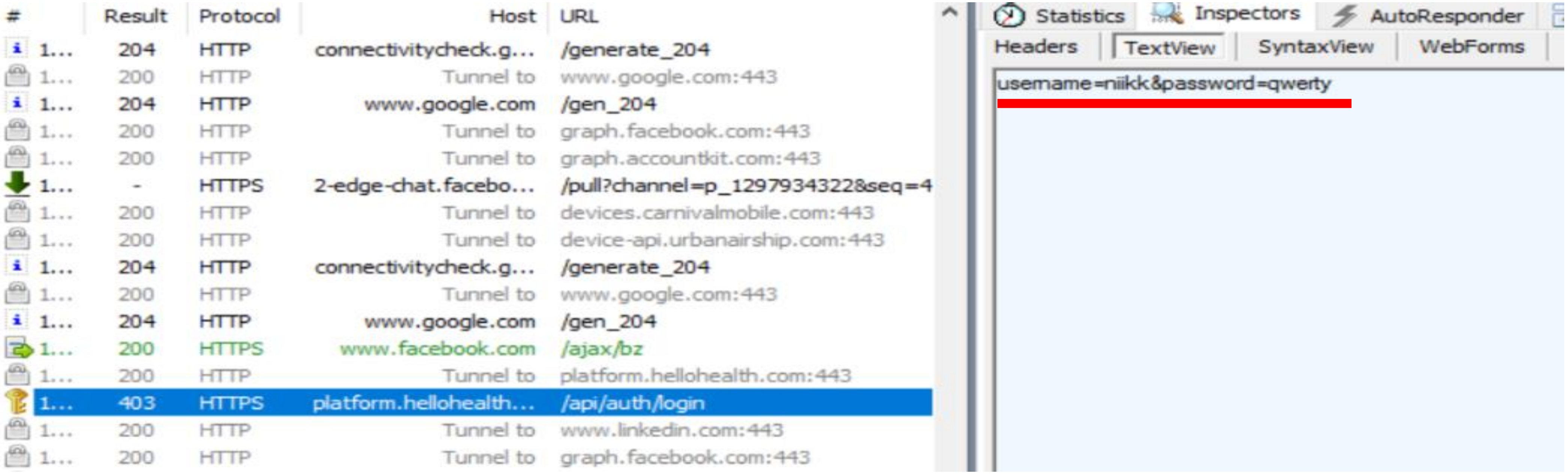
PortalConnect – Bad Hostname Verification


Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...
Statistics Inspectors AutoResponder Composer FiddlerScript Log Filters Timeline
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML

#	Result	Proto...	Host	URL	Body	Cachi
200	204	HTTP	clients3.google.c...	/generate_204	0	
201	204	HTTP	clients3.google.c...	/generate_204	0	
202	200	HTTP	std.o.webmd.com	/b/ss/webmdp1global/0/JAVA-...	1	no-ca
203	200	HTTP	Tunnel to	accounts.google.com:443	0	
204	200	HTTP	Tunnel to	platform.hellohealth.com:443	0	
205	403	HTTPS	platform.hellohea...	/api/auth/login	95	
206	200	HTTP	Tunnel to	nexus.officeapps.live.com:443	0	

```
username=kanikagupta%40gmail.com&password=kanikagupya
```

Bad Certificate Validation

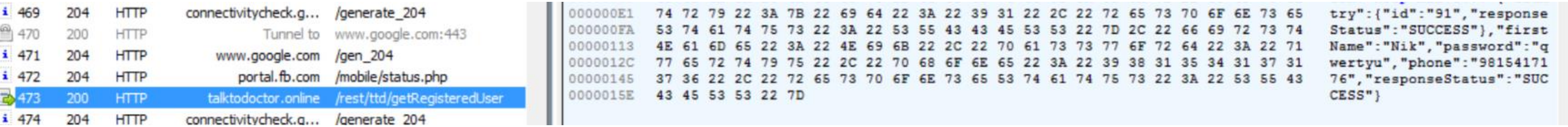

Statistics Inspectors AutoResponder
Headers TextView SyntaxView WebForms

#	Result	Protocol	Host	URL
1...	204	HTTP	connectivitycheck.g...	/generate_204
1...	200	HTTP	Tunnel to	www.google.com:443
1...	204	HTTP	www.google.com	/gen_204
1...	200	HTTP	Tunnel to	graph.facebook.com:443
1...	200	HTTP	Tunnel to	graph.accountkit.com:443
1...	-	HTTPS	2-edge-chat.facebo...	/pull?channel=p_1297934322&seq=4
1...	200	HTTP	Tunnel to	devices.carnivalmobile.com:443
1...	200	HTTP	Tunnel to	device-api.urbanairship.com:443
1...	204	HTTP	connectivitycheck.g...	/generate_204
1...	200	HTTP	Tunnel to	www.google.com:443
1...	204	HTTP	www.google.com	/gen_204
1...	200	HTTPS	www.facebook.com	/ajax/bz
1...	200	HTTP	Tunnel to	platform.hellohealth.com:443
1...	403	HTTPS	platform.hellohealth...	/api/auth/login
1...	200	HTTP	Tunnel to	www.linkedin.com:443
1...	200	HTTP	Tunnel to	graph.facebook.com:443

```
username=niikk&password=qwerty
```

Certificate Validation Broken – some examples

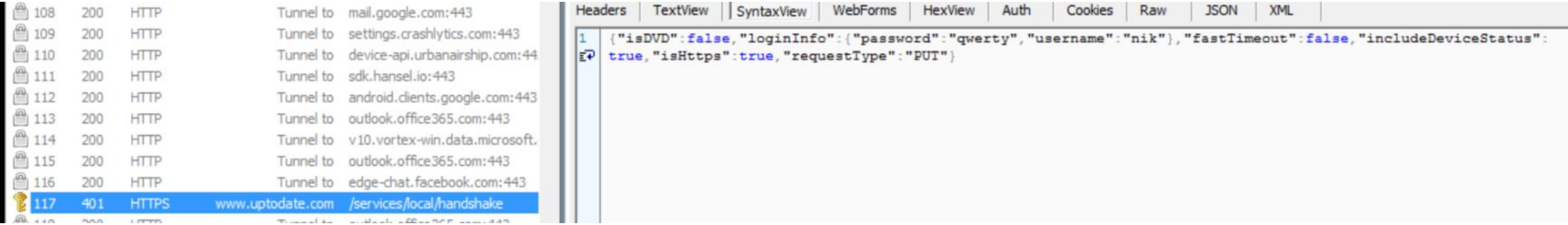
- TalkToDoctor



469	204	HTTP	connectivitycheck.g...	/generate_204
470	200	HTTP	Tunnel to	www.google.com:443
471	204	HTTP	www.google.com	/gen_204
472	204	HTTP	portal.fb.com	/mobile/status.php
473	200	HTTP	talktodoctor.online	/rest/ttd/getRegisteredUser
474	204	HTTP	connectivitycheck.g...	/generate_204

```
000000E1   74 72 79 22 3A 7B 22 69 64 22 3A 22 39 31 22 2C 22 72 65 73 70 6F 6E 73 65   try":{"id":"91","response
000000FA   53 74 61 74 75 73 22 3A 22 53 55 43 43 45 53 53 22 7D 2C 22 66 69 72 73 74   Status":"SUCCESS"},"first
00000113   4E 61 6D 65 22 3A 22 4E 69 6B 22 2C 22 70 61 73 73 77 6F 72 64 22 3A 22 71   Name":"Nik","password":"q
0000012C   77 65 72 74 79 75 22 2C 22 70 68 6F 6E 65 22 3A 22 39 38 31 35 34 31 37 31   wertyu","phone":"98154171
00000145   37 36 22 2C 22 72 65 73 70 6F 6E 73 65 53 74 61 74 75 73 22 3A 22 53 55 43   76","responseStatus":"SUC
0000015E   43 45 53 53 22 7D                                                            CESS"}
```

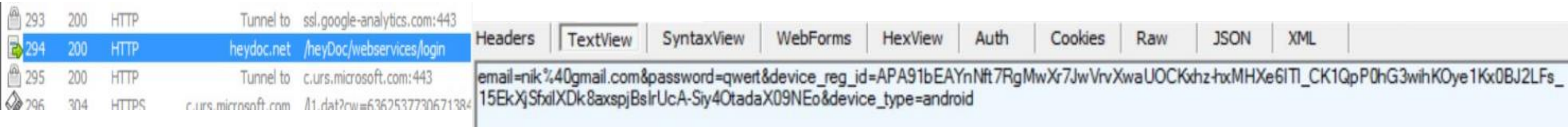
- UpToDate



108	200	HTTP	Tunnel to	mail.google.com:443
109	200	HTTP	Tunnel to	settings.crashlytics.com:443
110	200	HTTP	Tunnel to	device-api.urbanairship.com:44
111	200	HTTP	Tunnel to	sdk.hansel.io:443
112	200	HTTP	Tunnel to	android.clients.google.com:443
113	200	HTTP	Tunnel to	outlook.office365.com:443
114	200	HTTP	Tunnel to	v10.vortex-win.data.microsoft.
115	200	HTTP	Tunnel to	outlook.office365.com:443
116	200	HTTP	Tunnel to	edge-chat.facebook.com:443
117	401	HTTPS	www.uptodate.com	/services/local/handshake

{"isDVD":false,"loginInfo":{"password":"qwerty","username":"nik"},"fastTimeout":false,"includeDeviceStatus":
true,"isHttps":true,"requestType":"PUT"}

- HeyDoc



293	200	HTTP	Tunnel to	ssl.google-analytics.com:443
294	200	HTTP	heydoc.net	/heyDoc/webservices/login
295	200	HTTP	Tunnel to	c.urs.microsoft.com:443
296	304	HTTPS	c.urs.microsoft.com	/l1.dat?cw=6362537730671384

```
email=nik%40gmail.com&password=qwert&device_reg_id=APA91bEAYnNft7RgMwXr7JwVrvXwaUOCKxhz-hxMHXe6ITl_CK1QpP0hG3wihKOye1Kx0BJ2LFs_
15EkXjSfxilXDk8axspjBsIrUcA-Siy4OtadaX09NEo&device_type=android
```

Results

- Total Android Apps Tested – 229
- Certificate Validation Broken – 8
- Host name Verification Broken – 8
- Certificate Pinning – 20(Yes), 100(No)
- No HTTPS – 12
- All Information Remains on the Phone, No internet Usage - 73

Doubt

- There are 68 apps which show No SSL renegotiation in the following scenario –

1. Make SSL connection once, either by just starting the app or by trying to log in the app once using Fiddler's root and Correct Hostname.

2. Again, try to login but just before clicking the Login button, give fake hostname or delete the root or both.

3. Username and password given is visible in this case since SSL connection is already made and app is using the session.

- Can this be considered has Bad SSL Implementation scenario ? There are 36 apps which re-negotiate the SSL for each Login request.