HTTP Rest API Session

1. HTTP message, methods, urls, headers, body format for request, response.

1.1. **HTTP message**: HTTP messages are the way in which the client and the server communicate; there are two types of HTTP messages, request and response. Requests are what the client sends to the server to which the server responds with a response. These messages are actual text data which is encrypted and span over multiple lines because of which it's impossible to read the actual text data.

1.2. **HTTP methods**: There are a lot of HTTP methods but the ones which are used the most are; Get, Post, Put, Delete. This methods are used to read, post, update or delete data on the server. There are other methods like options, patch etc. but they are not used frequently.

1.3. **HTTP url**: Web clients and browsers like IE, chrome sends request to the server with the help of the url. Url specifies the location of the server.

1.4. **HTTP headers**: HTTP headers are a field of request which contains additional context and metadata about the request and response. Header indicates contexts like; content type, format, media, etc.

1.5. **HTTP body format**:

1.5.1. At first a HTTP method like GET, POST, etc. is used to execute the action according to the request.

1.5.2. Then location of the server is fetched with the help of URL or absolute patch of the protocol.

1.5.3. In the URL, if the URL is complete it is called the absolute form of the URL mostly used with GET method

1.5.4. If the URL consists of the domain name and port, then it is called the authority form. It is used when CONECT when setting up with any HTTP tunnel.

1.5.5. The '*' is used with OPTIONS representing the server as a whole.

1.6. **HTTP response**: The first line of the HTTP response is called a status line which contains the following information-

1.6.1. The protocol version

1.6.2. Status code

1.6.3. A status text describing the current status code.

2. Use following methods to keep your API's secured-

2.1. **Scan for API vulnerabilities**: To maintain high level security of API services it is vital to enable API automatic scanning which will keep the API under watch all the time.

2.2. **Use HTTPS/TLS for Rest API's**: Using HTTPS/TLS will provide security to the API's. It is the method of connecting the web browser with the server in a secured manner. HTTPS also helps to protect the credentials in transit as API's need to maintain confidentiality, integrity and authentication.

2.3. **HTTP methods**: HTTP methods(GET, PUT, POST, DELETE) should be used with a strict allow list to reduce the chances of the data getting hacked while sharing.

2.4. **Validation**: API's should include sufficient validation schemes on the servers as well as the clients side to provide another layer of security making API's more authenticated.

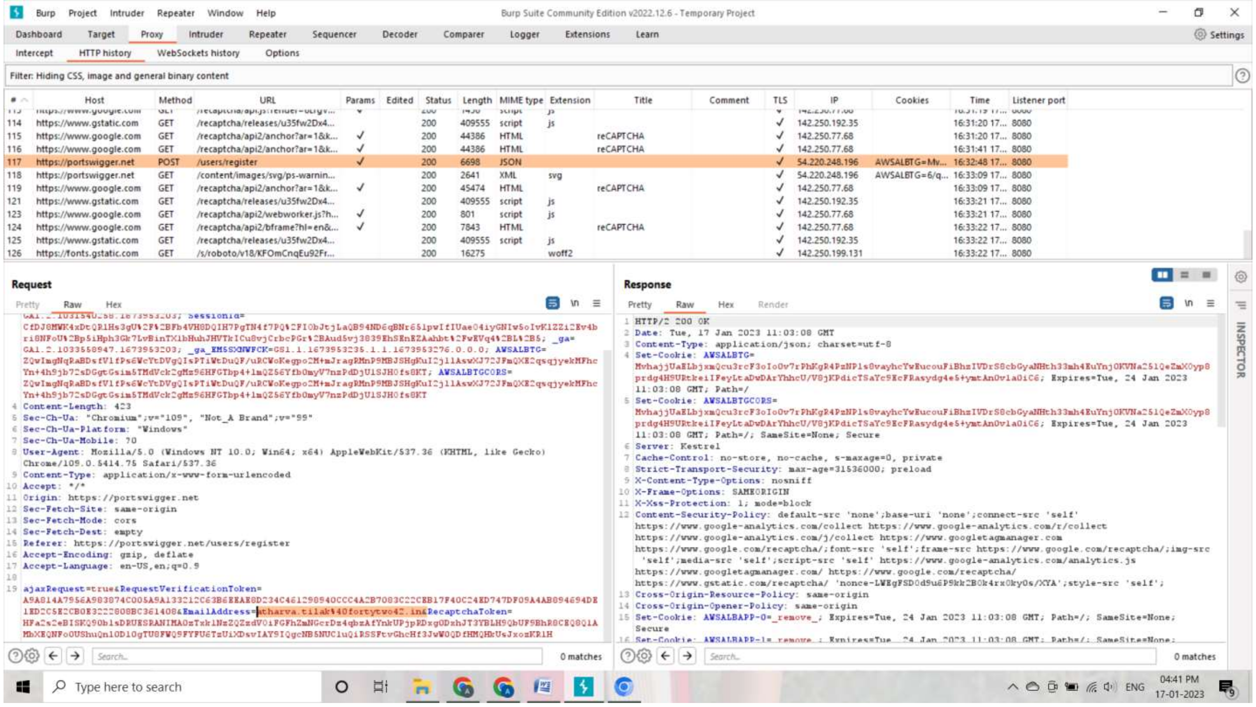
2.5. **API gateway**: If the organization uses a lot of API's it is better to combine them and form a API gateway. This gateway acts as a centralized location for the API requests. This platform also provides different services like telemetry, rate limiting and user authentication. In short it acts like a gatekeeper to the collection of API's present inside

3. Using Nessus for web application penetration

I penetrated a website www.synergy-spark.com using nessus, I have attached the required documents to this mail showing the result of the penetration test.

4. Use burp site to intercept traffic and get the credentials of sample HTTP/HTTPS pages.

4.1. HTTPS site



Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.12.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Options
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Type here to search
04:41 PM
17-01-2023
ENG

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
114	https://www.gstatic.com	GET	/recaptcha/releases/u35fw2Dx4...			200	409555	script	js			✓	142.250.192.35		16:31:20 17...	8080
115	https://www.google.com	GET	/recaptcha/api2/anchor?ar=1&k...	✓		200	44386	HTML		reCAPTCHA		✓	142.250.77.68		16:31:20 17...	8080
116	https://www.google.com	GET	/recaptcha/api2/anchor?ar=1&k...	✓		200	44386	HTML		reCAPTCHA		✓	142.250.77.68		16:31:41 17...	8080
117	https://portswigger.net	POST	/users/register	✓		200	6698	JSON				✓	54.220.248.196	AWSALBTG=Mv...	16:32:48 17...	8080
118	https://portswigger.net	GET	/content/images/svg/ps-warnin...			200	2641	XML	svg			✓	54.220.248.196	AWSALBTG=6/q...	16:33:09 17...	8080
119	https://www.google.com	GET	/recaptcha/api2/anchor?ar=1&k...	✓		200	45474	HTML		reCAPTCHA		✓	142.250.77.68		16:33:09 17...	8080
121	https://www.gstatic.com	GET	/recaptcha/releases/u35fw2Dx4...			200	409555	script	js			✓	142.250.192.35		16:33:21 17...	8080
123	https://www.google.com	GET	/recaptcha/api2/webworker.js?h...	✓		200	801	script	js			✓	142.250.77.68		16:33:21 17...	8080
124	https://www.google.com	GET	/recaptcha/api2/bframe?hl=en&...	✓		200	7843	HTML		reCAPTCHA		✓	142.250.77.68		16:33:22 17...	8080
125	https://www.gstatic.com	GET	/recaptcha/releases/u35fw2Dx4...			200	409555	script	js			✓	142.250.192.35		16:33:22 17...	8080
126	https://fonts.gstatic.com	GET	/s/roboto/v18/KFOmCnqEu92Fr...			200	16275		woff2			✓	142.250.199.131		16:33:22 17...	8080

Request

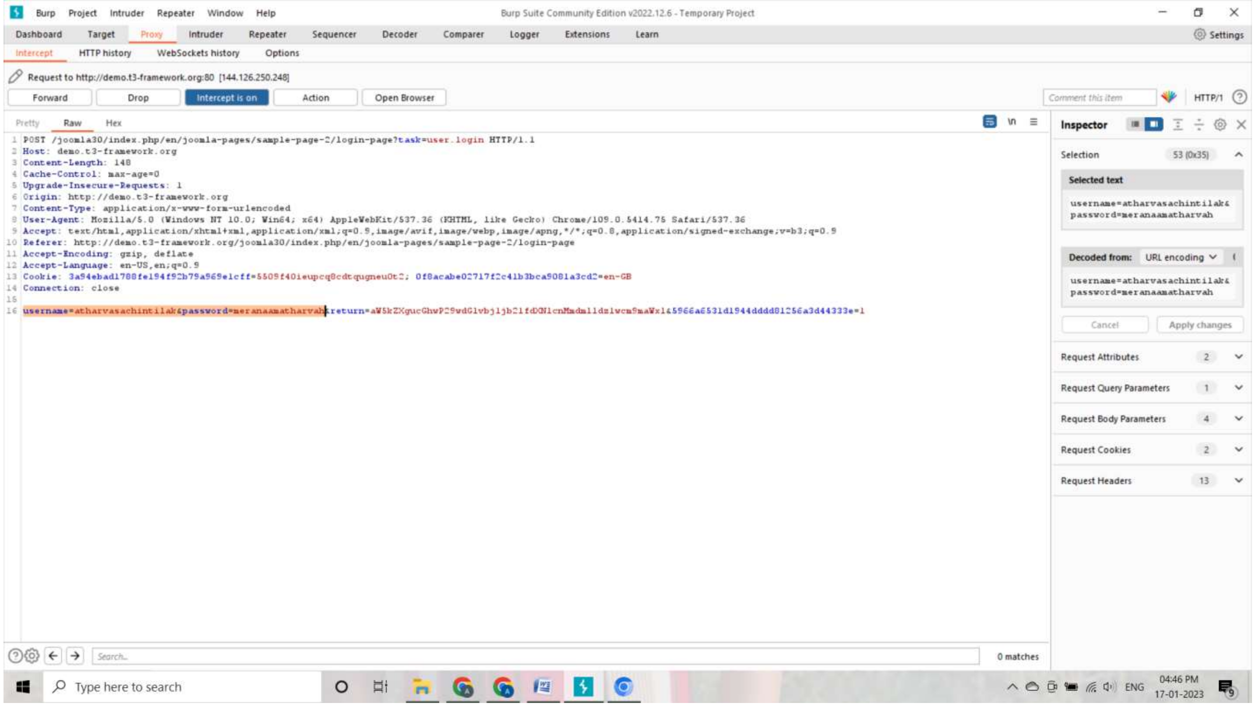
```
GA1.2.1031540258.1673953203; sessionid=
CfDJ8MWK4xDtQRlHs3gU%2F%2BFb4VH8DQIH7PgTN4f7PQ%2FIObJtjLaQB94ND6qBNr65lpwIfIUae04iyGNIw5oIvKlZZi2Ev4b
ri8NFoU%2Bp5iHph3Gk7LvBinTXlbHuhJHVTkICu8vjCrbcPGr%2BAud5vj3839EhSEnEZAahbt%2FwEVq4%2BL%2B5; _ga=
GA1.2.1033558947.1673953203; _ga_EM5SXNWFCK=GS1.1.1673953235.1.1.1673953276.0.0.0; AWSALBTG=
ZQwImgNqRaBDsfVlfPs6WcYtDVgQIsPTiWtDuQF/uRCWoKegpo2M+mJragRMnP9MBJSHgKuI2jllAswXJ72JFmQXE2qsqjyekMFhc
Yn+4h9jb72sDGgtGsim5TMdVck2gMz96HFGTbp4+lmQZ56YfbOmyV7nzPdDjUlSJH0fs8KT; AWSALBTGCORS=
ZQwImgNqRaBDsfVlfPs6WcYtDVgQIsPTiWtDuQF/uRCWoKegpo2M+mJragRMnP9MBJSHgKuI2jllAswXJ72JFmQXE2qsqjyekMFhc
Yn+4h9jb72sDGgtGsim5TMdVck2gMz96HFGTbp4+lmQZ56YfbOmyV7nzPdDjUlSJH0fs8KT
Content-Length: 423
Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.5414.75 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://portswigger.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portswigger.net/users/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

ajaxRequest=true&RequestVerificationToken=
A9A814A7956A983874C005A9A133212C63B6EEAE8D234C461298940CCC4A2B7083C22CEB17F40C24ED747DF09A4AB094694DE
1ED2C5E2CB0E3222808BC361408&EmailAddress=atharva.tilak%40fortytwo42.in&RecaptchaToken=
HFa2s2eBISKQ9Ob1sDRUESRANIMA0zTxklNzZQZzdV0iFGFhZmNGcrDz4qbzAfYnkUPjpRDxgODxhJT3YBLH9QbUF9BhR8CEQ8Q1A
MbXEQNFoOUShuQnl0Dl0gTU8FWQ9FYFU6TzUiXDsvIAY9IQgcNB5NUCluQiRSSFtvGhcHf3JwW0QDfHMQHkUsJxozKR1H
```

Response

```
HTTP/2 200 OK
Date: Tue, 17 Jan 2023 11:03:08 GMT
Content-Type: application/json; charset=utf-8
Set-Cookie: AWSALBTG=
MvhajjUaELbjxmQcu3rcF3oIoOv7rPhKgR4PzNPls8vayhcYwEucouFiBhzIVDrS8cbGyaNHth33mh4EuYnjOKVNa2510eZmX0yp8
prdg4H9URtkeiIFeyLtaDwDArYhhcU/V8jKPdicTSaYc9EcFRasydg4e5+ymtAnOvla0iC6; Expires=Tue, 24 Jan 2023
11:03:08 GMT; Path=/
Set-Cookie: AWSALBTGCORS=
MvhajjUaELbjxmQcu3rcF3oIoOv7rPhKgR4PzNPls8vayhcYwEucouFiBhzIVDrS8cbGyaNHth33mh4EuYnjOKVNa2510eZmX0yp8
prdg4H9URtkeiIFeyLtaDwDArYhhcU/V8jKPdicTSaYc9EcFRasydg4e5+ymtAnOvla0iC6; Expires=Tue, 24 Jan 2023
11:03:08 GMT; Path=/; SameSite=None; Secure
Server: Kestrel
Cache-Control: no-store, no-cache, s-maxage=0, private
Strict-Transport-Security: max-age=31536000; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'none';base-uri 'none';connect-src 'self'
https://www.google-analytics.com/collect https://www.google-analytics.com/r/collect
https://www.google-analytics.com/j/collect https://www.googletagmanager.com
https://www.google.com/recaptcha/;font-src 'self';frame-src https://www.google.com/recaptcha/;img-src
 'self';media-src 'self';script-src 'self' https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/ https://www.google.com/recaptcha/
https://www.gstatic.com/recaptcha/ 'nonce-LWEgFSD0d9u6P9kk2B0k4rx0kyOs/XYA';style-src 'self';
Cross-Origin-Resource-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: AWSALBAPP-0=_remove_; Expires=Tue, 24 Jan 2023 11:03:08 GMT; Path=/; SameSite=None;
Secure
Set-Cookie: AWSALBAPP-1=_remove_; Expires=Tue, 24 Jan 2023 11:03:08 GMT; Path=/; SameSite=None;
```

4.2. HTTP site



Request to http://demo.t3-framework.org:80 [144.126.250.248]

```
POST /joomla30/index.php/en/joomla-pages/sample-page-2/login-page?task=user.login HTTP/1.1
Host: demo.t3-framework.org
Content-Length: 148
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://demo.t3-framework.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://demo.t3-framework.org/joomla30/index.php/en/joomla-pages/sample-page-2/login-page
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: 3a94ebad1788fe194f92b79a969e1cff=5509f40ieupcq8cdtqugneu0t2; 0f8acabe02717f2c41b3bca9081a3cd2=en-GB
Connection: close

username=atharvasachintilak&password=meranaamatharvah&return=aW5kZXgucGhwP29wdGlvbj1jb21fdXNlcnMmdmlldz1wcm9maWxl&5966a6531d1944dddd81256a3d44333e=1
```

Selection 53 (0x35)

Selected text

```
username=atharvasachintilak&
password=meranaamatharvah
```

Decoded from: URL encoding

```
username=atharvasachintilak&
password=meranaamatharvah
```

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 4

Request Cookies 2

Request Headers 13

5. Use postman call HTTPS/HTTP API

I have attached the JSON file in this email as a result of testing postman.