S.H.E.L.L.

SECURITY IS AN ILLUSION

What is web penetration ???

- ❑ The Web is the common name for the World Wide Web, a subset of the Internet consisting of the pages that can be accessed by a Web browser. Web consists of large number of server sharing data.

- ❑ A web browser is an application software for accessing the World Wide Web or a local website. When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user's device. Example :- chrome ,mozilla

- ❑ Web Application Penetration Testing is methodology of simulating unauthorized attacks to gain access to sensitive data that is being hosted by web servers and is available to access via web. It helps to find out the possibility for a hacker to access data from the internet and also get to know how secure the web hosting site and server are.

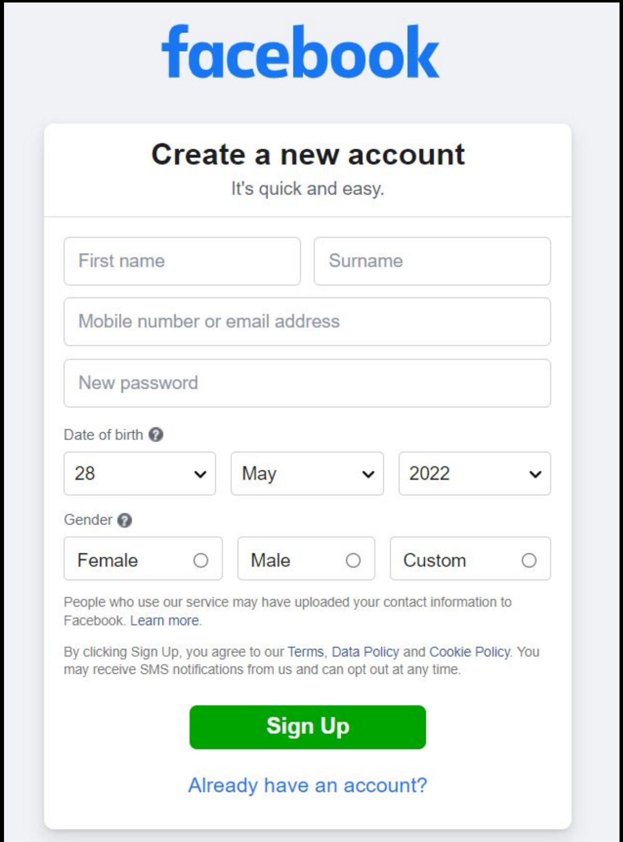
What comes to our mind when we imagine web ???

- A web page
- Html
- Css
- Javascript
- Php
- Front End
- Back End ….

And many more such terms comes to our mind. So web pentesting is checking security of the composition of all this terms/web-components ie a complete web app.

What web look like

https://blog.google/search/?query=hack



Create a new account

It's quick and easy.

First name	Surname

Mobile number or email address

New password

Date of birth ?

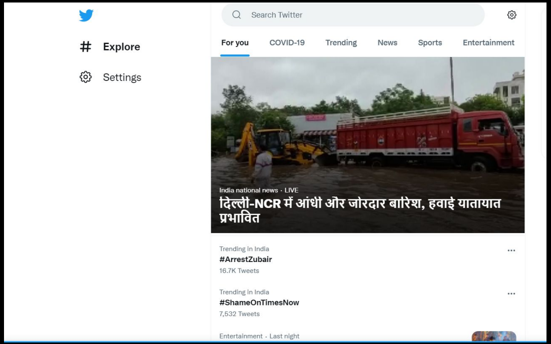
28	May	2022

Gender ?

Female ○	Male ○	Custom ○

People who use our service may have uploaded your contact information to Facebook. Learn more.

By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.



India national news · LIVE

दिल्ली-NCR में आंधी और जोरदार बारिश, हवाई यातायात प्रभावित

Trending in India

#ArrestZubair

16.7K Tweets

Trending in India

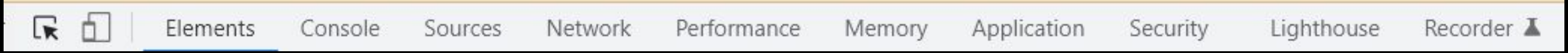
#ShameOnTimesNow

7,532 Tweets

Entertainment · Last night

https://twitter.com/explore

https://www.deccanherald.com/business/business-news/us-regulators-scrutinise-musks-twitter-stock-buys-1113184.html

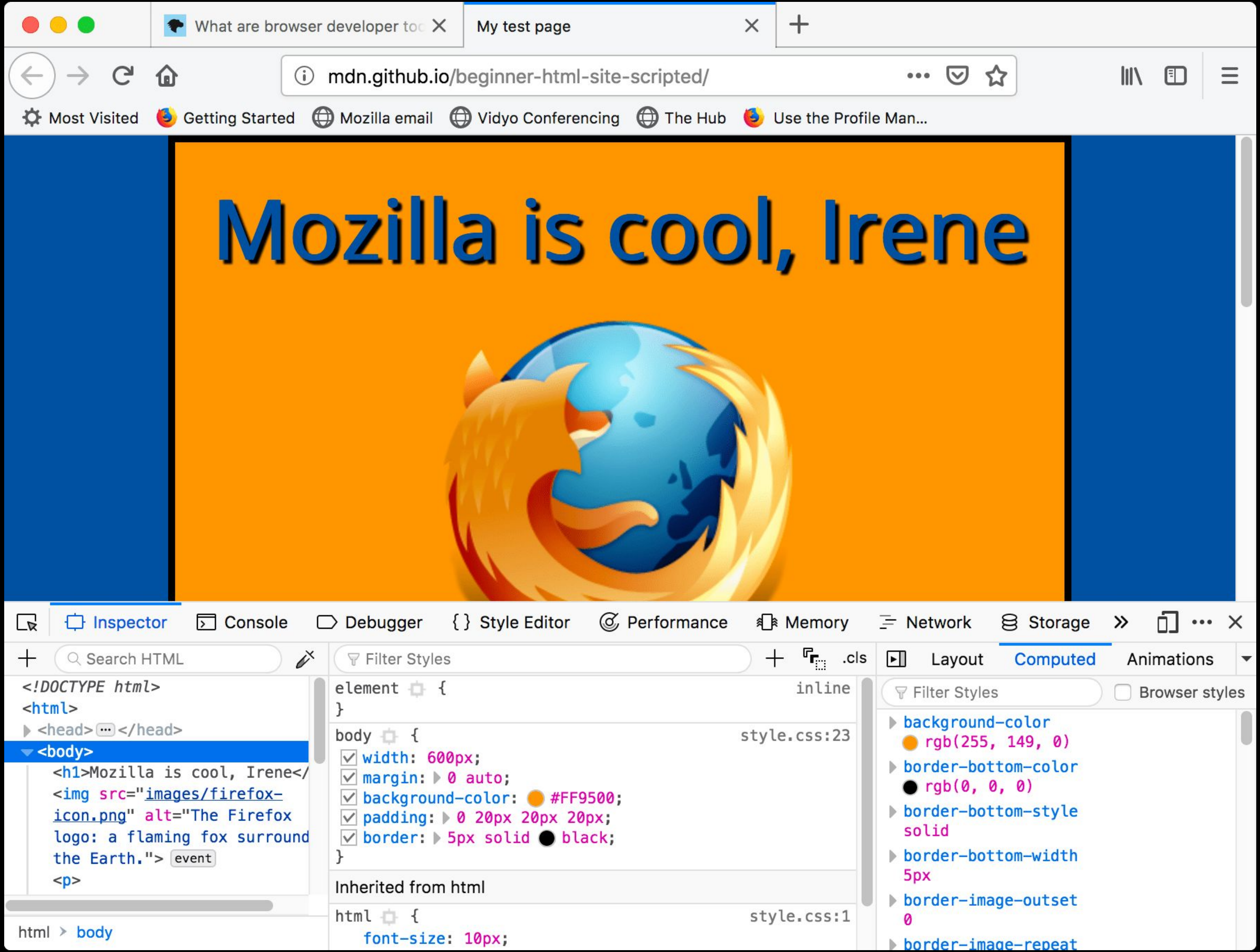


Most basic tool (Inspector)

Inspect element is a feature of modern web browsers that enables anyone to view and edit a website's source code, including its HTML, CSS, JavaScript, and media files. When the source code is modified with the inspect tool, the changes are shown live inside the browser window.

Anything done in inspector affects client, everything remains unaltered in server.

https://jupiter.challenges.picoctf.org/problem/44924/



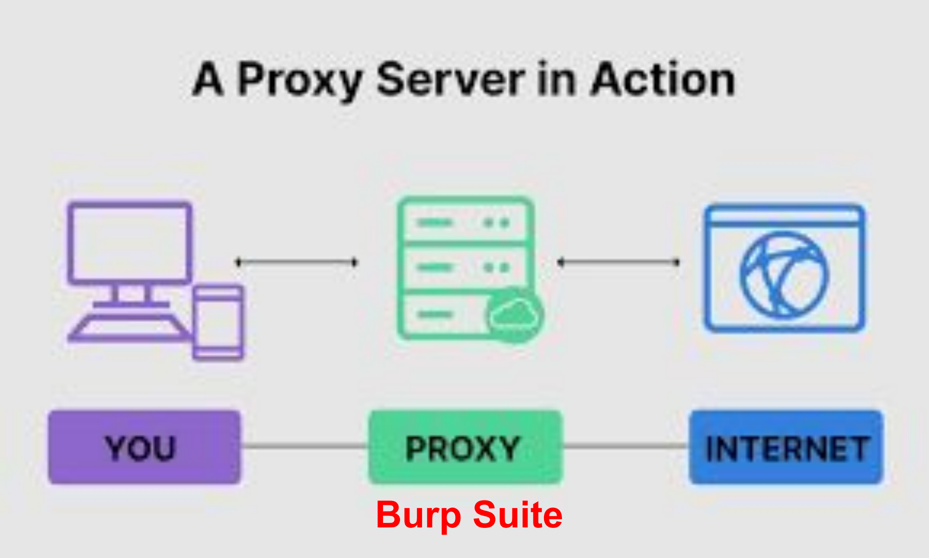
```
<!DOCTYPE html>
<html>
 <head>…</head>
 <body>
   <h1>Mozilla is cool, Irene</
   <img src="images/firefox-icon.png" alt="The Firefox
   logo: a flaming fox surround
   the Earth."> event
   <p>
```

```
element {                              inline
}
body {                                 style.css:23
  ☑ width: 600px;
  ☑ margin: 0 auto;
  ☑ background-color: #FF9500;
  ☑ padding: 0 20px 20px 20px;
  ☑ border: 5px solid black;
}
Inherited from html
html {                                 style.css:1
  font-size: 10px;
```

```
background-color
  rgb(255, 149, 0)
border-bottom-color
  rgb(0, 0, 0)
border-bottom-style
  solid
border-bottom-width
  5px
border-image-outset
  0
border-image-repeat
```

Proxy

A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource. Basically it's man sitting between us and server providing us data. Everything going to server passes through proxy.



There is an inbuilt proxy tool which we can use, but it’s tedious job to use it ,so we use foxyproxy most commonly used by cyber-security people.

Foxyproxy for firefox :- https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/

We use burp suite as proxy tool.

Foxyproxy directs all traffic and burpsuite intercept it and send to server.

Video to setup burp with foxyproxy :- https://www.youtube.com/watch?v=-JLUw3fr-ro

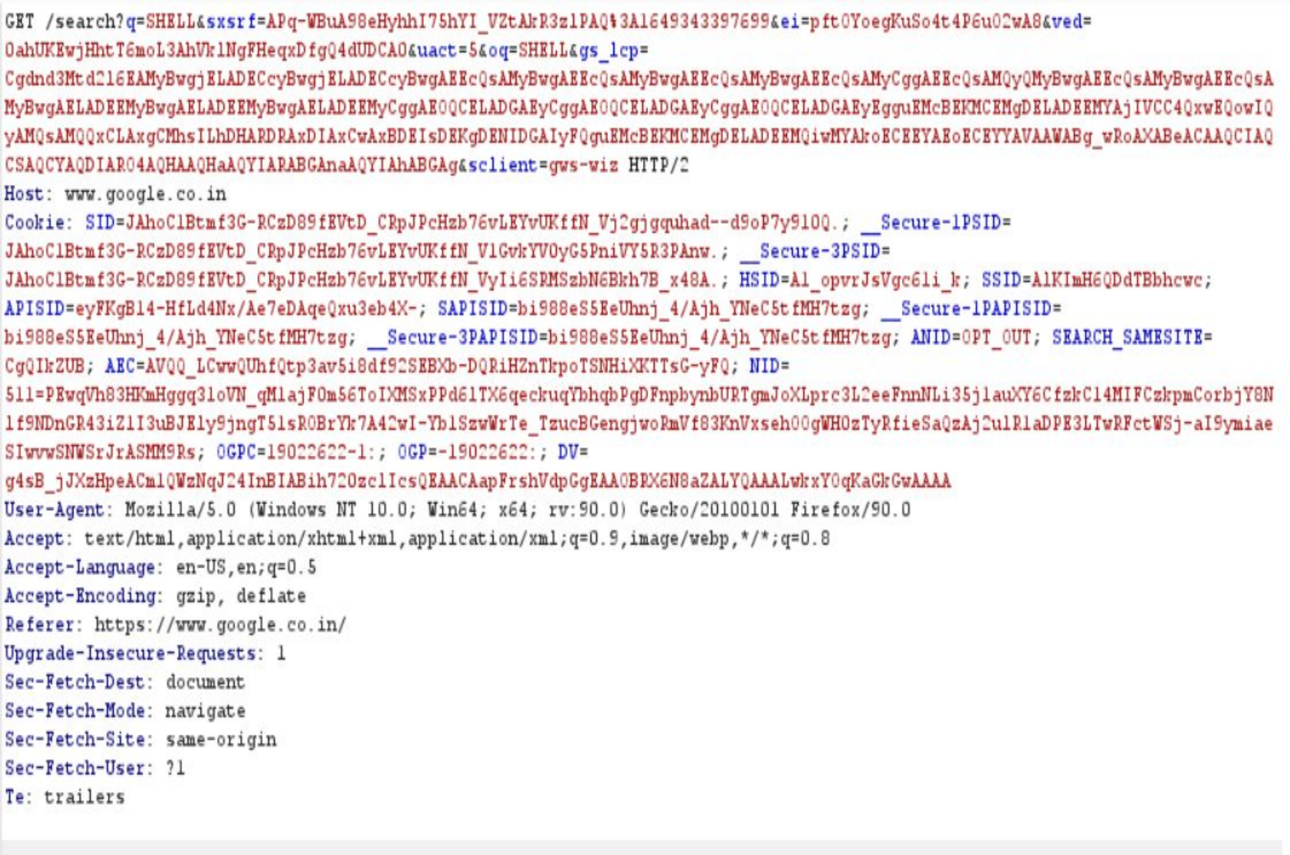
S.H.E.L.L.

SECURITY IS AN ILLUSION

Http Headers

HTTP headers are the name or value pairs that are displayed in the request and response messages of message headers for Hypertext Transfer Protocol (HTTP).

https://jupiter.challenges.picoctf.org/problem/50522/



```
GET /search?q=SHELL&sxsrf=APq-WBuA98eHyhhI75hYI_VZtAkR3z1PAQ%3A1649343397699&ei=pft0YoegKuSo4t4P6u02wA8&ved=
0ahUKEwjHhtT6moL3AhVk1NgFHeqxDfgQ4dUDCA0&uact=5&oq=SHELL&gs_lcp=
Cgdnd3Mtd216EAMyBwgjELADECcyBwgjELADECcyBwgAEEcQsAMyBwgAEEcQsAMyBwgAEEcQsAMyBwgAEEcQsAMyCggAEEcQsAMQyQMyBwgAEEcQsAMyBwgAEEcQsA
MyBwgAELADEEMyBwgAELADEEMyBwgAELADEEMyCggAE0QCELADGAEyCggAE0QCELADGAEyCggAE0QCELADGAEyEgguEMcBEKMCEMgDELADEEMYAjIVCC4QxwEQowIQ
yAMQsAMQQxCLAxgCMhsILhDHARDRAxDIAxCwAxBDEIsDEKgDENIDGAIyFQguEMcBEKMCEMgDELADEEMQiwMYAkoECEEYAEoECEYYAVAAWABg_wRoAXABeACAAQCIAQ
CSAQCYAQDIAR04AQHAAQHaAQYIARABGAnaAQYIAhABGAg&sclient=gws-wiz HTTP/2
Host: www.google.co.in
Cookie: SID=JAhoC1Btmf3G-RCzD89fEVtD_CRpJPcHzb76vLEYvUKffN_Vj2gjgquhad--d9oP7y910Q.; __Secure-1PSID=
JAhoC1Btmf3G-RCzD89fEVtD_CRpJPcHzb76vLEYvUKffN_V1GvkYV0yG5PniVY5R3PAnw.; __Secure-3PSID=
JAhoC1Btmf3G-RCzD89fEVtD_CRpJPcHzb76vLEYvUKffN_VyIi6SRMSzbN6Bkh7B_x48A.; HSID=Al_opvrJsVgc6li_k; SSID=AlKImH6QDdTBbhcwc;
APISID=eyFKgB14-HfLd4Nx/Ae7eDAqeQxu3eb4X-; SAPISID=bi988eS5EeUhnj_4/Ajh_YNeC5tfMH7tzg; __Secure-1PAPISID=
bi988eS5EeUhnj_4/Ajh_YNeC5tfMH7tzg; __Secure-3PAPISID=bi988eS5EeUhnj_4/Ajh_YNeC5tfMH7tzg; ANID=OPT_OUT; SEARCH_SAMESITE=
CgQIkZUB; AEC=AVQQ_LCwwQUhfQtp3av5i8df92SEBXb-DQRiHZnTkpoTSNHiXKTTsG-yFQ; NID=
511=PEwqVh83HKmHggq3loVN_qMlajF0m56ToIXMSxPPd61TX6qeckuqYbhqbPgDFnpbynbURTgmJoXLprc3L2eeFnnNLi35j1auXY6CfzkC14MIFCzkpmCorbjY8N
1f9NDnGR43iZ1I3uBJEly9jngT51sR0BrYk7A42wI-Yb1SzwWrTe_TzucBGengjwoRmVf83KnVxseh00gWH0zTyRfieSaQzAj2ulR1aDPE3LTwRFctWSj-aI9ymiae
SIwvwSNWSrJrASMM9Rs; OGPC=19022622-1:; OGP=-19022622:; DV=
g4sB_jJXzHpeACm1QWzNqJ24InBIABih720zclIcsQEAACAapFrshVdpGgEAA0BRX6N8aZALYQAAALwkxY0qKaGkGwAAAA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.co.in/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

https://www.geeksforgeeks.org/http-headers/

https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

S.H.E.L.L.

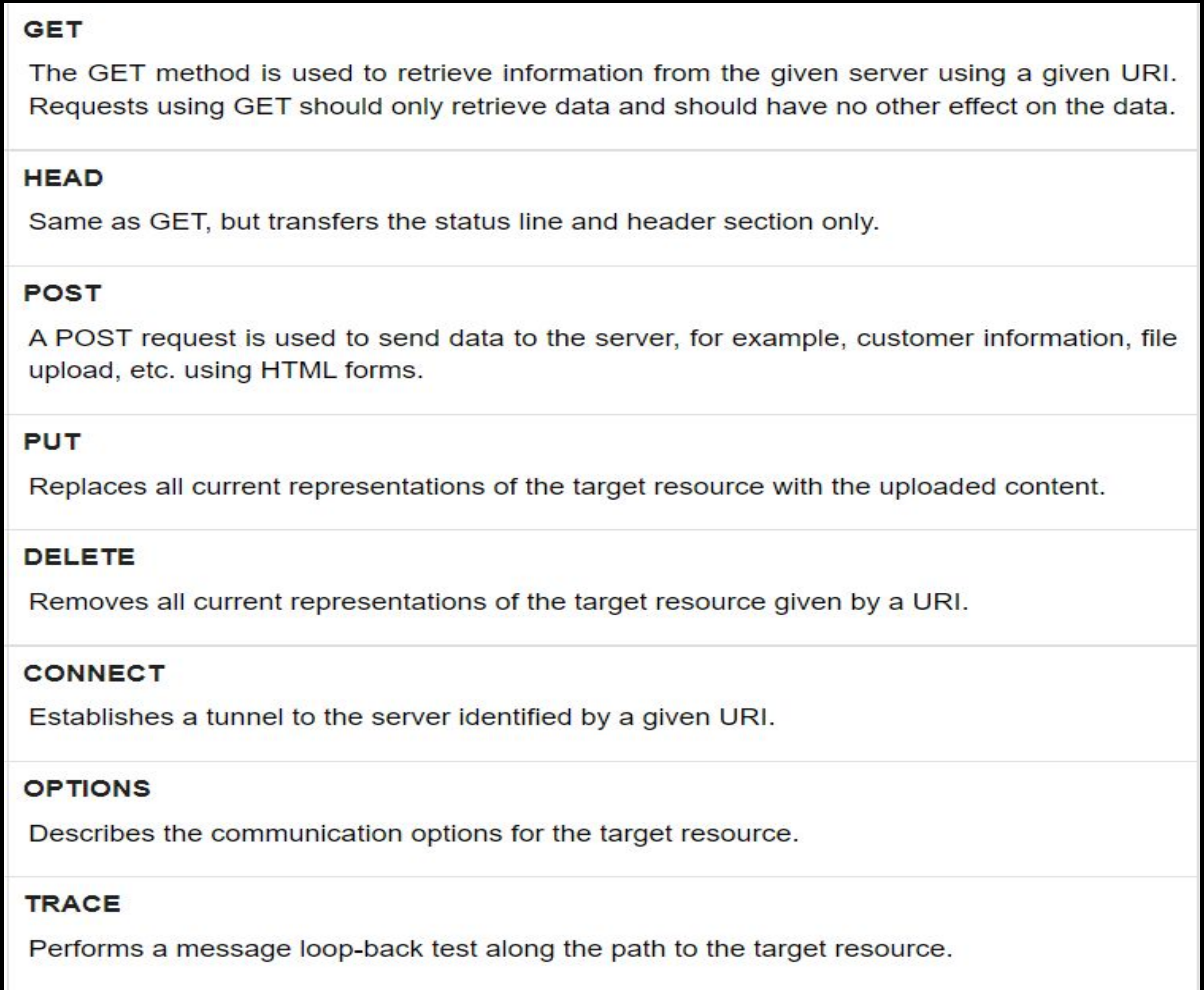
SECURITY IS AN ILLUSION

Various Request methods

Methods used to interchange data between server and client

Resource
https://www.tutorialspoint.com/http/http_methods.htm

CTF Problem
http://mercury.picoctf.net:47967/



GET

The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.

HEAD

Same as GET, but transfers the status line and header section only.

POST

A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.

PUT

Replaces all current representations of the target resource with the uploaded content.

DELETE

Removes all current representations of the target resource given by a URI.

CONNECT

Establishes a tunnel to the server identified by a given URI.

OPTIONS

Describes the communication options for the target resource.

TRACE

Performs a message loop-back test along the path to the target resource.

Cookies

HTTP cookies are small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user's web browser. They enable web servers to store stateful information (such as items added in the shopping cart in an online store) on the user's device or to track the user's browsing activity.They can also be used to save for subsequent use information that the user previously entered into form fields, such as names, addresses, passwords, and payment card numbers.

Cookies are basically storage for web browser to reuse it which fetching data from server.

Cookie can be

- Some ID
- Authentication token
- User ID
- Session ID

Attack that can be formulated is called Cookie Manipulation:-

http://mercury.picoctf.net:27177/

Robots.txt & sitemap.xml

Robots.txt

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index. It’s like telling web-browser not to disclose those files to viewer or touch those to file and simply ignore it.

https://jupiter.challenges.picoctf.org/problem/60915/

http://saturn.picoctf.net:51108/

Sitemap.xml

An XML sitemap is a file that lists a website's important pages, making sure Google can find and crawl them all. It also helps search engines understand your website structure. You want Google to crawl every essential page of your website.

Insecure direct object references (IDOR)

Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly.

Example :-

https://insecure-website.com/customer_account?customer_number=132355 (ID)

https://insecure-website.com/static/12144.txt (Static file)

Owasp juice shop example

Client Side

Validation on client side that is browser based verification can lead to data disclosure or failure to restrict user from malicious action.

It could be client side filtering of user input or authentication mechanism.

https://login.mars.picoctf.net/

https://jupiter.challenges.picoctf.org/problem/29835/

XSS (Cross-Site-Scripting)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into websites and web browser run it without proper validation. The scripts used includes javascripts which can be crafted to steal credentials of users, session tokens, authentication tokens, make user unknowingly run some script making then bankrupt or changing account password and any more.

There are three types of XSS

- Reflected XSS :- Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request.
- Stored XSS :- Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The user retrieves the data or loads a page malicious script from the server get fetched and executed in browser each time user visits that page.
- DOM XSS

https://xss-quiz.int21h.jp/

File Upload

This attack includes upload a malicious file like one which would run on server and give us access to severe. This may include uploading a malicious file in profile photo which get stored in server and when opened runs on server.

Example :-

Uploading php language reverse shell in profile picture of a php based web application

https://abhijithkumar2000.medium.com/dvwa-tutorial-file-upload-vulnerability-affbe3d3dd19

SQL Injection

SQL stands for Structured Query Language. SQL is used to communicate with a database that is for storing, manipulating and retrieving data in databases.

*	=	everything
/*,#,;--	=	comments
1=1	=	True condition

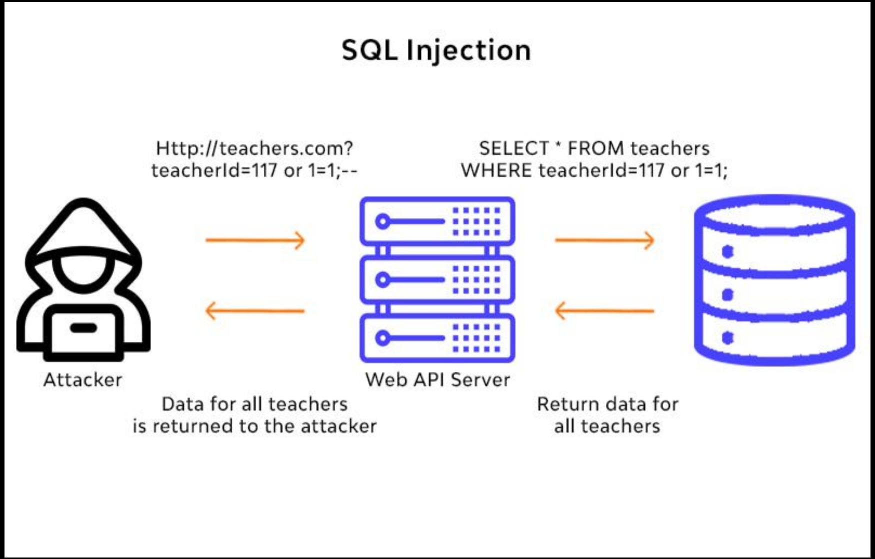
https://www.w3schools.com/sql/

https://sqlzoo.net/wiki/SELECT_basics

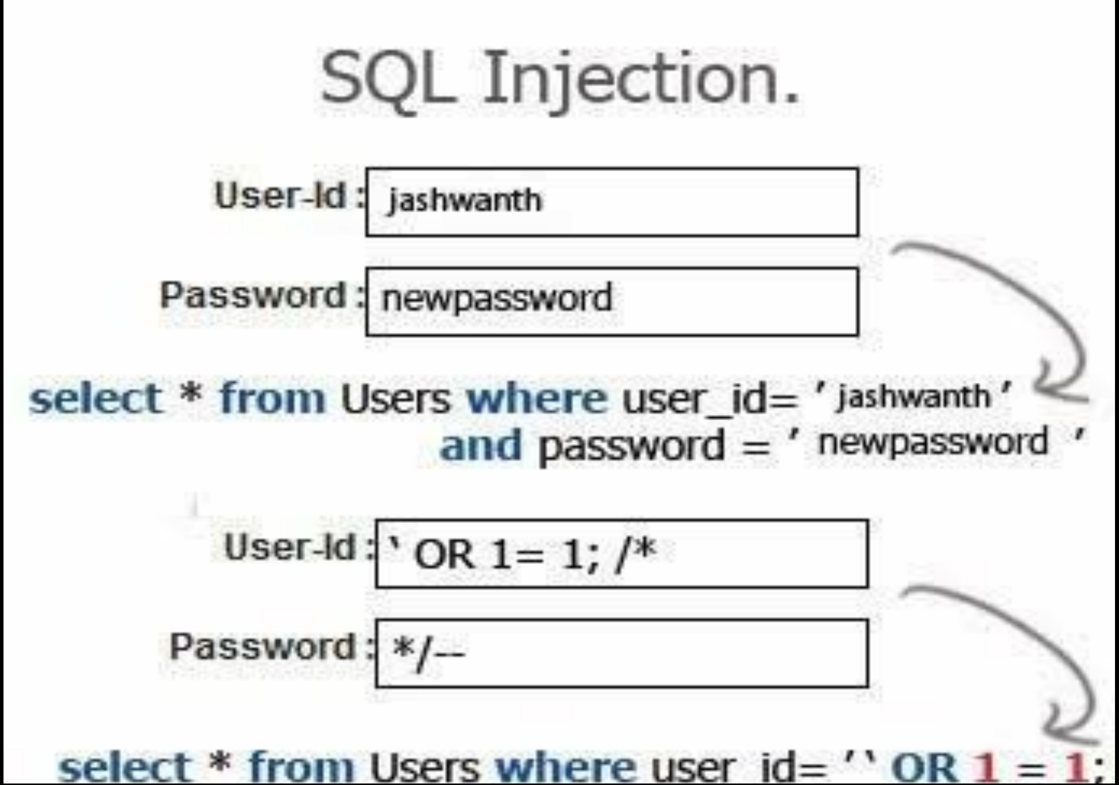
https://www.w3schools.com/sql/sql_injection.as

Normal url = http://teachers.com?teacherId=117 (return data for only teacher id 117)

Crafted url = http://teachers.com?teacherId=117 or 1=1;-- (return data for all teacher ids)



Login bypass sql injection if not handled properly



SQL Injection.

User-Id : jashwanth

Password : newpassword

```
select * from Users where user_id= ' jashwanth '
                          and password = ' newpassword '
```

User-Id : ' OR 1= 1; /*

Password : */--

```
select * from Users where user_id= '' OR 1 = 1;
```