Web Pentest 101

from abrasax to /dev/null

0x00: Getting Started

The web fundamentals

- A *very* brief comment about networks: clients and servers
- The HTTP protocol and its methods
- Client-Side vs. Server-Side
- What happens in your browser's background
- Challenges

Networks and HTTP stuff

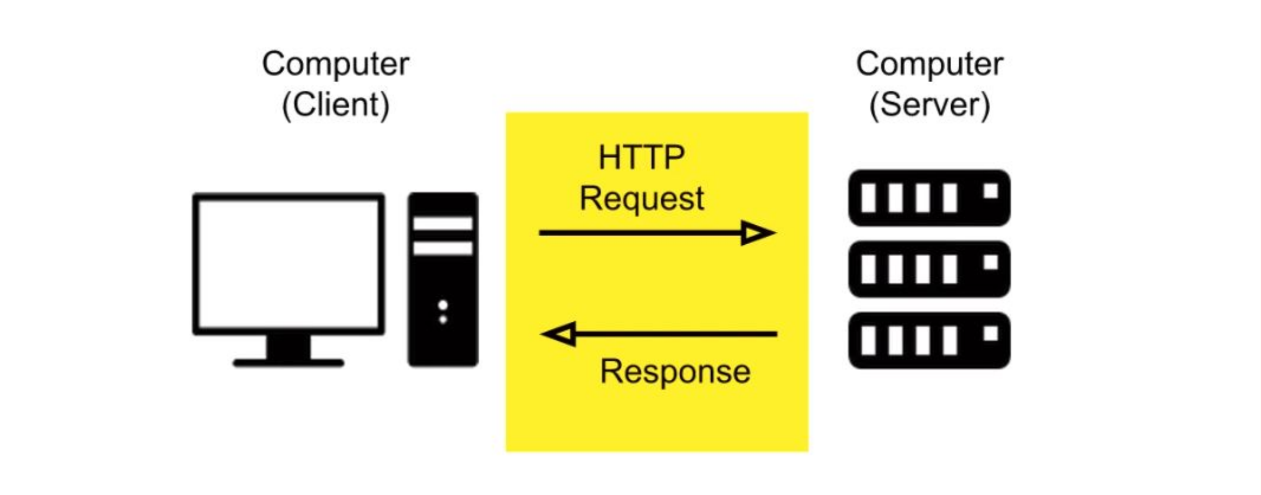
How computers communicate?

- There is some ways of send and receive data across the internet, the commonly used is called client-server model.
- In this model a computer (yours) ask someone (maybe facebook?) for some data (it’s site for example).
- The facebook computer (server) look at your request and get you back their web page.
- Your communication with facebook is about get and send data. You’re the client and the facebook is the server
- The server is prepared to serve a lot of different users, asking for different tasks
- People communicate using languages, what about servers?

HTTP Protocol and stuff

- Web applications talks to each other using a protocol called HTTP (HiperText Transfer Protocol)
- Basically, he ask for content from a server and send stuff across the internet

- There is more than one way of asking for something in the internet
- These different ways are called HTTP methods



HTTP Methods

- An HTTP Method is a way of asking the server for information
- When you want a get my profile in facebook, you cannot only ask for https://facebook.com/ but https://facebook.com/vrechson
- Beside that, sometimes you want to search for something in this site, like posts containing the word politics
- In facebook you can use the url: https://www.facebook.com/search/top/?q=politics&epa=SEARCH_BOX
- These way of asking for some content using the URL itself is called HTTP GET method.
- You can just change these red values marked as red in the url to change your search
- Usually we call the information sent to the server as parameters
- A standard parameter looks like:
  - ?parameter1=value1&parameter2=value2&parameter3=value3...

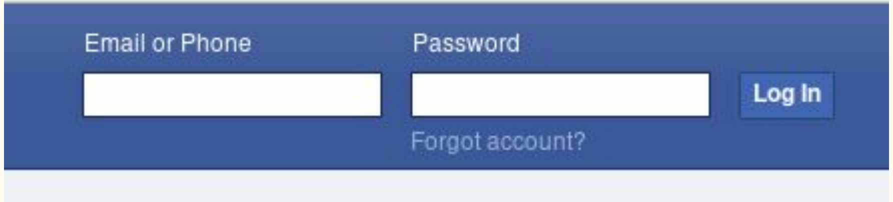
Example:

http://url/page.php?search=politics&news=2

GET Method vs. POST Method

- When you send parameters via GET anyone can access this url and see the same content
- Theses values are clear to everyone see in the URL
- So we need a way to pass passwords to the server without display it in URL or create a link with your password where everyone can just click and enter with you password
- But how?

- The solution is called POST Method
- An POST Method is used by forms in web pages
- It send data inside the HTTP Protocol and is not visible for who is looking to the browser
- You cannot send POST data through URL
- There is more HTTP Methods that I'll cover in the future



Client Side vs. Server Side

- If you enter in that facebook URL with my profile, the result will be different of mine, this happens because I'm the owner of my account and the page will return for me my configuration stuff
- The facebook knows that is me because after my login I store in my "giant random string" called TOKEN or COOKIES (different concepts that I'll introduce better soon)
- So I send these "string" in the HTTP request and the server knows that is me and return a slightly different page for me, with some options more
- These validation of my account happens in the server so we call it server side
- Sometimes when you try to sign up in some website the forms doesn't allow you to put and email without @, have you ever seen that?
- This email validation happens in your browser and there is no need of send data to facebook to return saying that is missing an @
- These validation occurs in your site and is called client-side because happens in your computer

The browser

- The browser is interpreter that tranform HTTP data into graphic pages
- HTTP contains its headers that include the method of request that we saw and languages content, like HTML, javascript and CSS
- These stuff is sent inside HTTP packets and rendered as images and texts by the browser
- These three languages are the main family of languages of web development, HTML struct the page, javascript add dynamism and css an pretty visual

- There is no need to use the browser, you can use cURL to do some HTTP request and get the responses back
- The sintax is *$ curl -X method url*
- GET EXAMPLE WITH CURL:
- $ curl http://localhost/page.php?name=abrasax
- POST EXAMPLE WITH CURL
- $ curl -X POST http://localhost/login.php -H “Host: not.ganesh” --data “login=admin&pass=admin”

The class challenge (easy)

- Para resolver este desafio você deve fazer um request GET em http://localhost/v1/key?email=your@email.com passando o seu email, como resposta você irá receber uma api_key (string) cifrada com cifra de caesar. Lembre-se de usar o header HTTP *Host: pombo.ctf*
- Sua tarefa é descobrir a palavra cifrada e retornar ao servidor fazendo um POST para http://localhost/v1/login com os parametros api_key=PALAVRA_CIFRADA&word=PALAVRA. Se o conteúdo estiver correto você recebe a flag como retorno. Lembre-se de utilizar os headers HTTP *Host: pombo.ctf* neste trecho
- *Dica: use o curl para te ajudar*

The home challenge (medium)

- Talvez esse desafio seja mais difícil para os bixos devido a necessidade de saber programar, mas sintam-se a vontade para tentar e aprender.
- Ele é o desafio que a pagar.me utilizou no processo seletivo da secomp em 2017
- A descrição está em: https://github.com/pombo-ctf/web-101/blob/master/0x00:%20Getting%20Started/challenge/description.md