



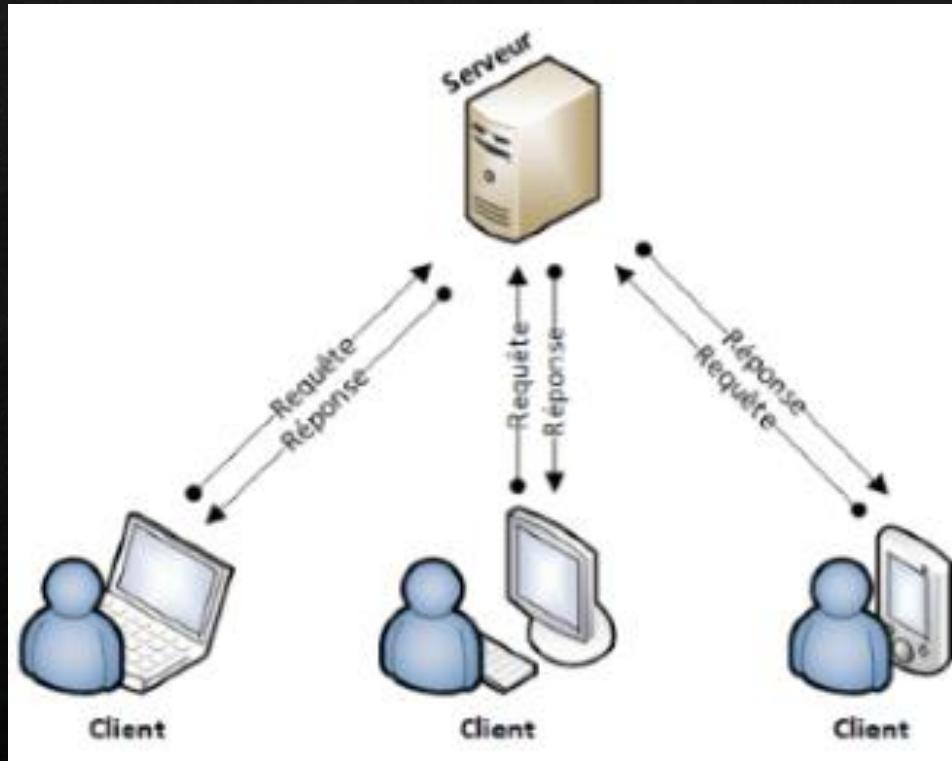
Séance d'introduction hacking web

Hackin'TN

Sommaire

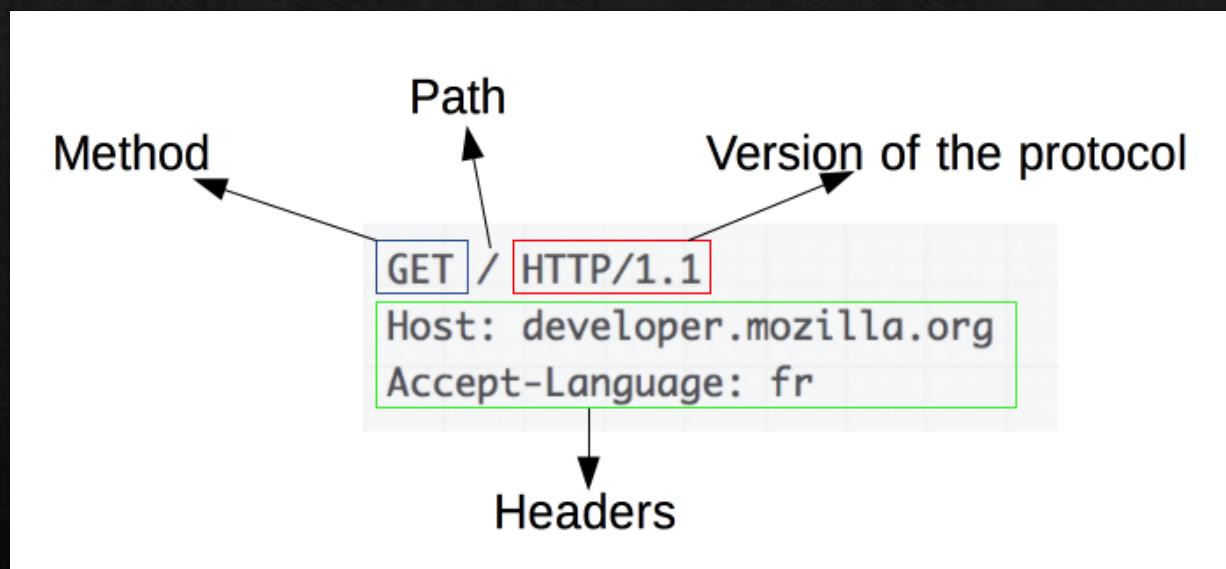
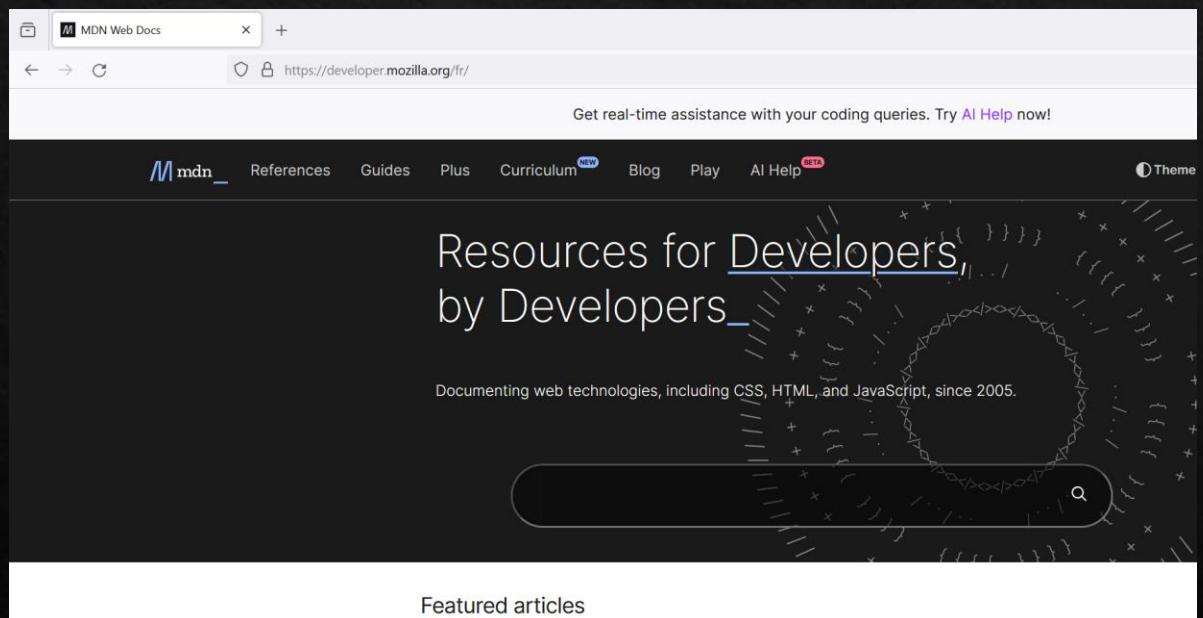
- 1) Architecture Client-Serveur
- 2) Protocole HTTP
- 3) Autres technologies courantes
- 4) Principales menaces
- 5) Outils
- 6) Mise en application

1) Architecture Client-Serveur



- ❖ Les navigateurs des utilisateurs (clients) envoient des requêtes à des serveurs web, qui renvoient ensuite des pages Web et des ressources.

2) Protocole HTTP



2) Protocole HTTP

- **Définition** : protocole de communication utilisé pour **transférer** des données sur le web, reposant sur le modèle **client-serveur**.
- **Méthodes HTTP** :
 - **GET** : **demande de données**. Données envoyées dans l'url en tant que paramètres de requête. Exemple : chargement d'une page par un navigateur.
 - **POST** : **soumission de données** au serveur. Données envoyées dans le corps de la requête. Exemple : données soumises dans un formulaire en ligne.

2) Protocole HTTP

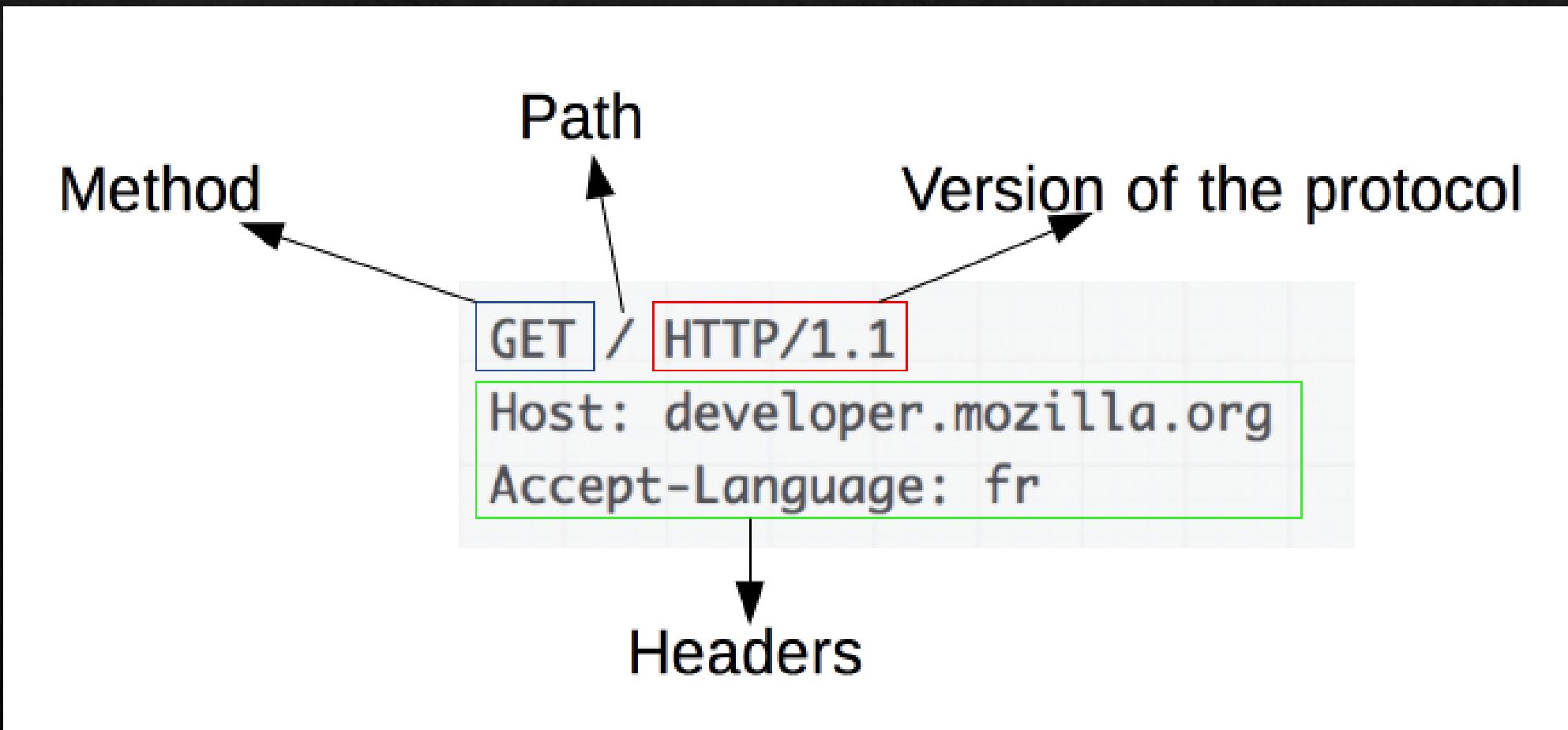
En-têtes de requête HTTP :

Définition : éléments de métadonnées qui fournissent des informations supplémentaires sur la requête envoyée au serveur.

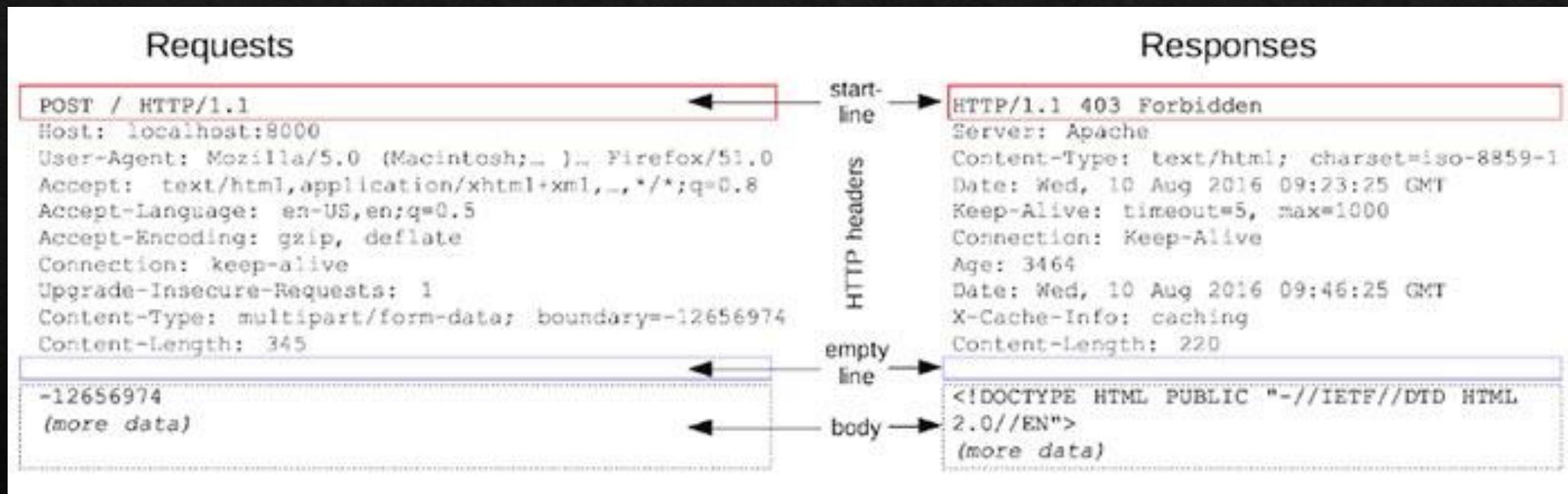
Exemples :

- **User-Agent** : Identifie le logiciel client (navigateur, application, etc.) utilisé pour envoyer la requête.
- **Host** : Spécifie le nom de domaine du serveur auquel la requête est destinée.
- **Content-Type** : Indique le type de contenu envoyé dans le corps de la requête (application/json, multipart/form-data, etc.).
- **Authorization** : Utilisé pour inclure les informations d'authentification, telles que les jetons d'accès ou les identifiants, dans la requête.
- **Accept** : Spécifie les types de contenu acceptables pour la réponse.
- **Cookie** inclus des informations d'identification stockées localement par le client.

2) Protocole HTTP



2) Protocole HTTP



3) Autres technologies courantes

- CSS : mise en forme des pages HTML

3) Autres technologies courantes

- CSS : mise en forme des pages HTML
- JavaScript : utilisé côté client dans les navigateurs Web pour rendre les pages Web interactives en ajoutant des fonctionnalités telles que des animations, des formulaires interactifs et des effets visuels dynamiques.

3) Autres technologies courantes

- CSS : mise en forme des pages HTML
- JavaScript : utilisé côté **client** dans les navigateurs Web pour rendre les pages Web interactives en ajoutant des fonctionnalités telles que des animations, des formulaires interactifs et des effets visuels dynamiques.
- PHP : utilisé côté **serveur** pour créer des sites Web dynamiques en générant du contenu personnalisé en fonction des requêtes des utilisateurs et en interagissant avec les bases de données.

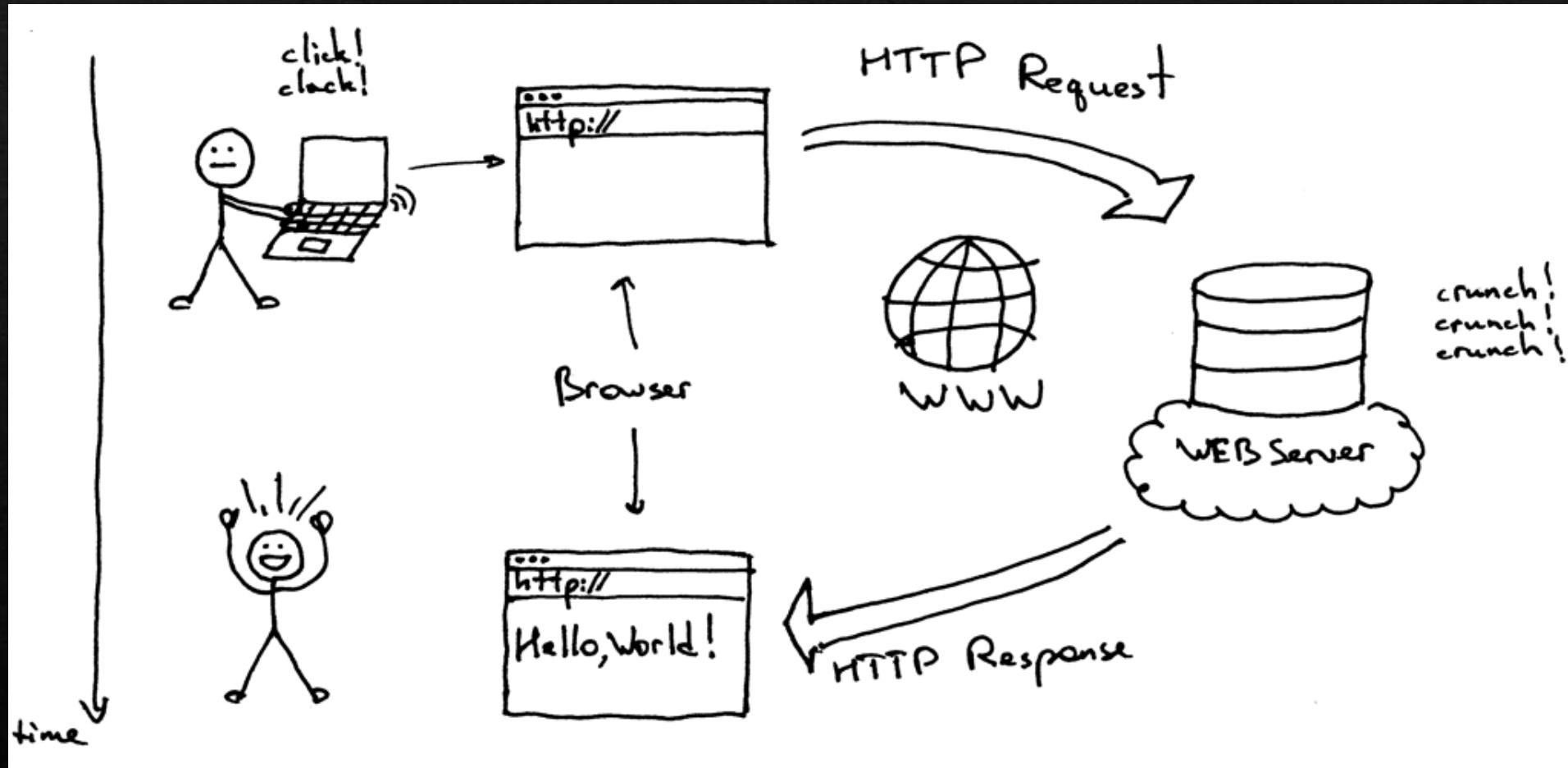
3) Autres technologies courantes

- CSS : mise en forme des pages HTML
- JavaScript : utilisé côté **client** dans les navigateurs Web pour rendre les pages Web interactives en ajoutant des fonctionnalités telles que des animations, des formulaires interactifs et des effets visuels dynamiques.
- PHP : utilisé côté **serveur** pour créer des sites Web dynamiques en générant du contenu personnalisé en fonction des requêtes des utilisateurs et en interagissant avec les bases de données.
- SQL : utilisé pour gérer et manipuler des bases de données.

3) Autres technologies courantes

- CSS : mise en forme des pages HTML
- JavaScript : utilisé côté **client** dans les navigateurs Web pour rendre les pages Web interactives en ajoutant des fonctionnalités telles que des animations, des formulaires interactifs et des effets visuels dynamiques.
- PHP : utilisé côté **serveur** pour créer des sites Web dynamiques en générant du contenu personnalisé en fonction des requêtes des utilisateurs et en interagissant avec les bases de données.
- SQL : utilisé pour gérer et manipuler des bases de données.
- Flask : framework Python utilisé pour créer des applications Web dynamiques et basées sur des microservices en offrant des fonctionnalités telles que le routage URL, la gestion des requêtes HTTP et la création de modèles de pages.

4) Principales menaces



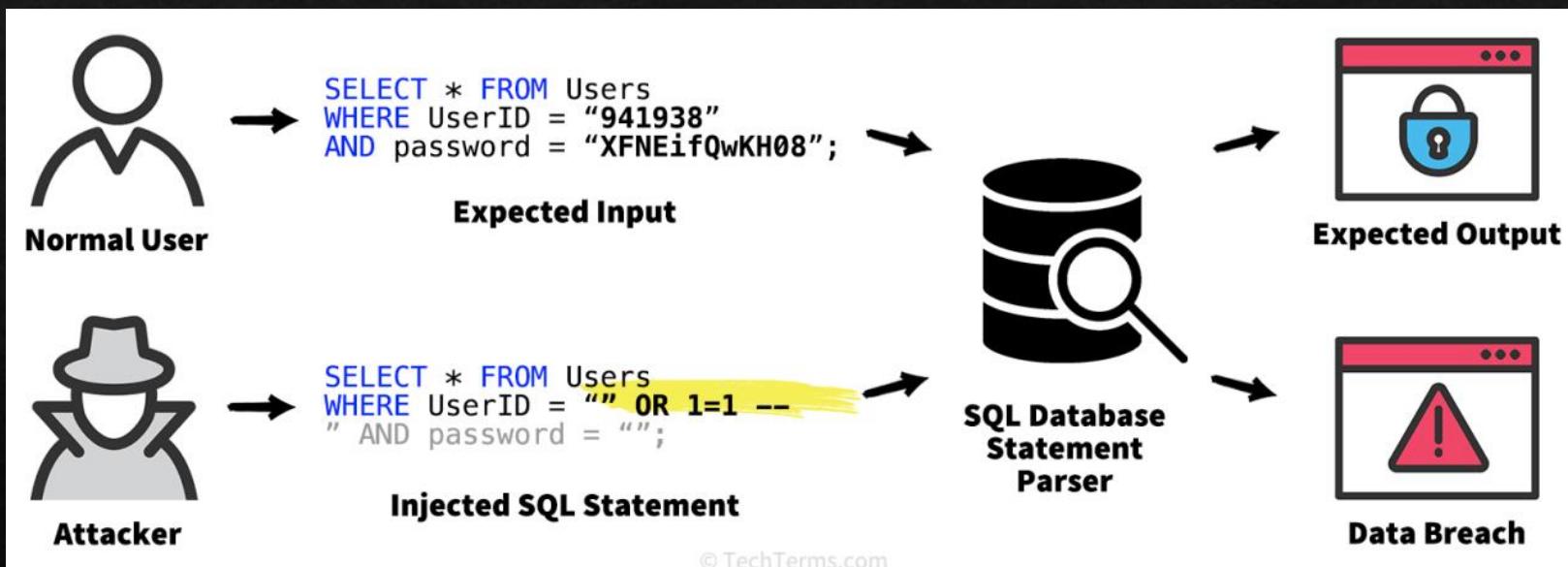
4) Principales menaces

Manipulation des requêtes :

- Modification d'en-têtes (user-agent, en-tête maison tel que is_admin = false, etc)
- Redirection vers une autre url
- Modification des valeurs envoyées dans un formulaire (requête post)
- Etc

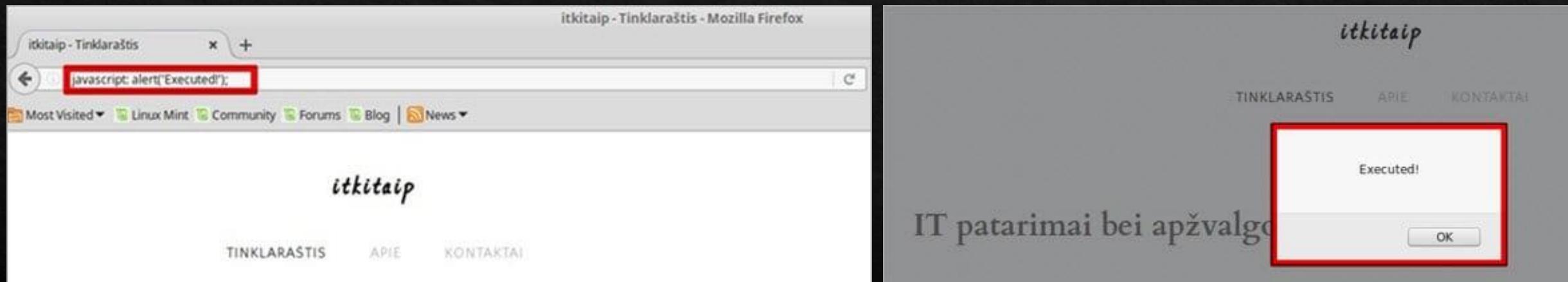
4) Principales menaces

Injections SQL



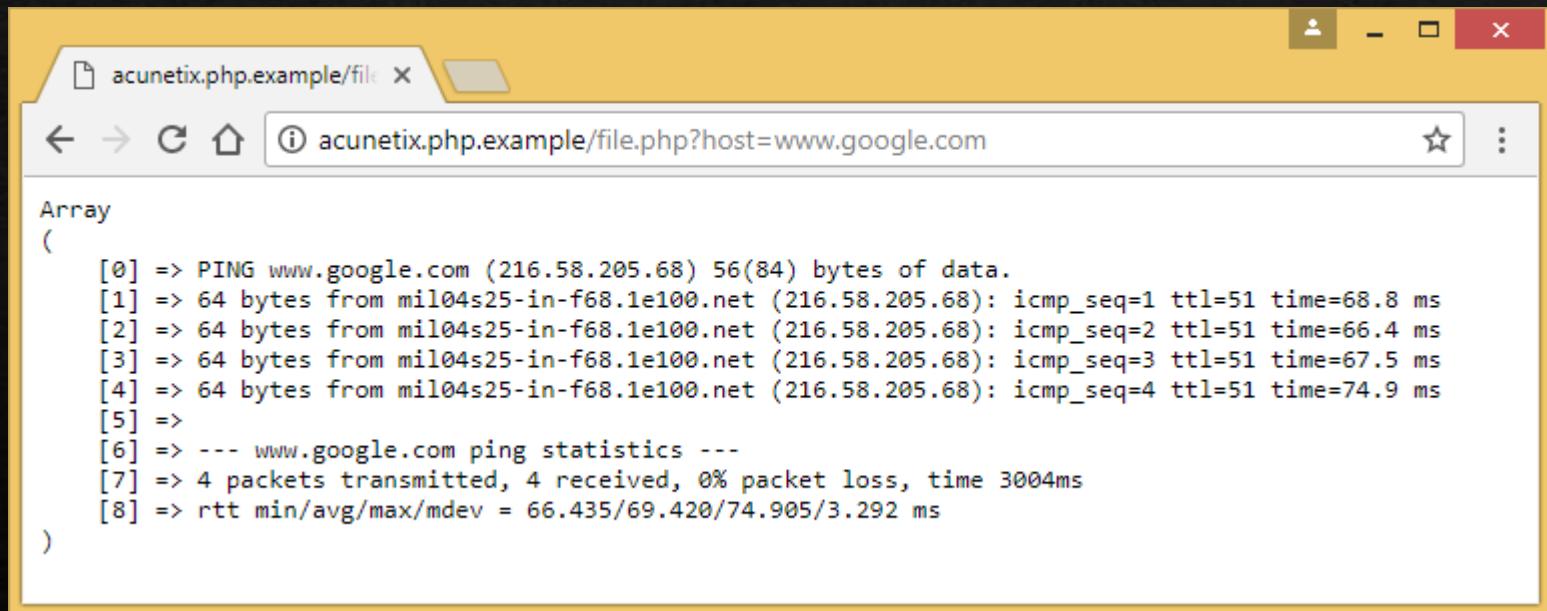
4) Principales menaces

Injections JavaScript

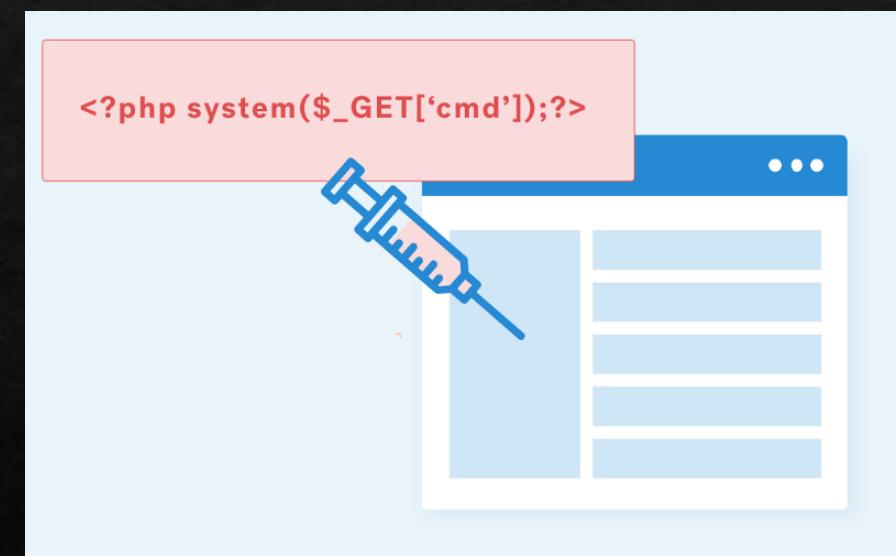


4) Principales menaces

Injections PHP

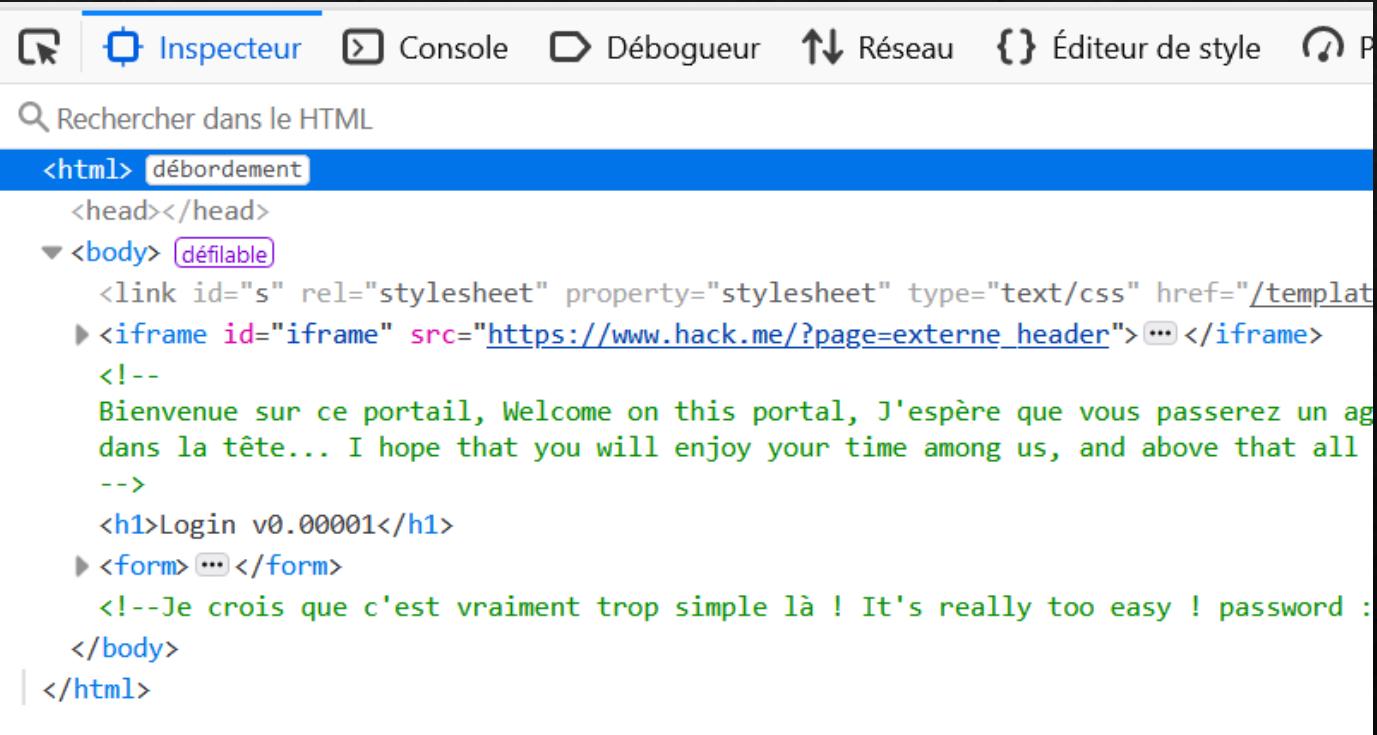


A screenshot of a web browser window titled "acunetix.php.example/file". The address bar shows "acunetix.php.example/file.php?host=www.google.com". The main content area displays the output of a ping command to www.google.com, showing 8 lines of data starting with "[0] => PING www.google.com (216.58.205.68) 56(84) bytes of data." and ending with "[8] => rtt min/avg/max/mdev = 66.435/69.420/74.905/3.292 ms".



5) Outils

Outils développeur du navigateur :



```
<html> [débordement]
  <head></head>
  ▼ <body> [défilable]
    <link id="s" rel="stylesheet" property="stylesheet" type="text/css" href="/template.css"/>
    ▶ <iframe id="iframe" src="https://www.hack.me/?page=externe_header">...</iframe>
    <!--
      Bienvenue sur ce portail, Welcome on this portal, J'espère que vous passerez un agréable moment ici...
      I hope that you will enjoy your time among us, and above all, have fun !
    -->
    <h1>Login v0.00001</h1>
    ▶ <form>...</form>
      <!--Je crois que c'est vraiment trop simple là ! It's really too easy ! password :-->
    </body>
  | </html>
```

5) Outils

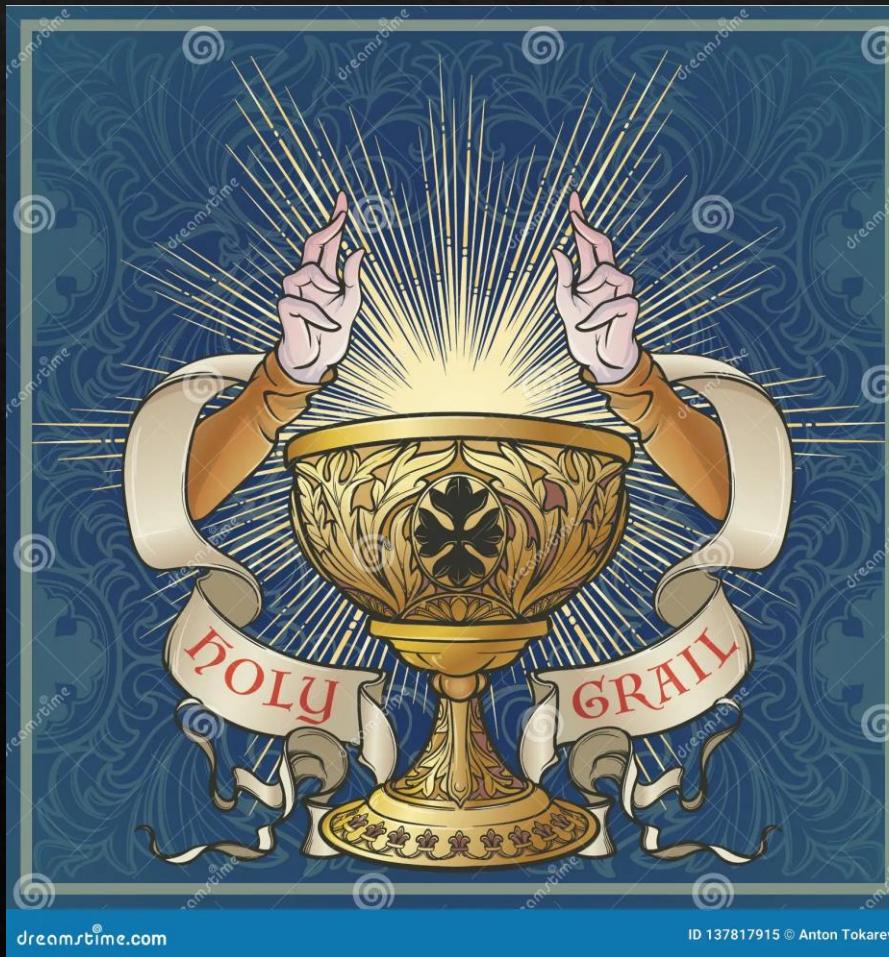
Curl

- GET : curl <http://exemple.com/page>
- POST avec header :

```
curl -H "Authorization: Bearer myAccessToken" http://exemple.com/page
```

5) Outils

BurpSuite



Burp Project Intruder Repeater View Help

Proxy Repeater Repeater

Navigateur intégré Simulation de réponse

Request Response

Requête HTTP Réponse à la requête En-têtes

Target: https://google.com

Inspector Notes

Done

1,565 bytes | 28 millis

1 GET / HTTP/2
2 Host: google.com
3 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Ubuntu; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/120.0.6099.71 Safari/537.36
8 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=0.7
9 X-Client-Data: CISUyWE=
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17 Connection: close
18
19

1 HTTP/2 301 Moved Permanently
2 Location: https://www.google.com/
3 Content-Type: text/html; charset=UTF-8
4 Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src
'nonce-nSrJLWA6bUv-DZggbgTrxA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline'
https://report-uri https://csp.withgoogle.com/csp/gws/other-hp
5 Cross-Origin-Opener-Policy: same-origin-allow-popups; report-to="gws"
6 Report-To:
{"group": "gws", "max_age": 2592000, "endpoints": [{"url": "https://csp.withgoogle.com/csp/report-to/gws/other"}]}
7 Permissions-Policy: unload=()
8 Origin-Trial:
Ap+qNlnLzJDKSmeHjzM5ilaa908GuehlLqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrhnPA8w4IAAAABfeyJ
vcmlnaW4iOijodHRwcovL3d3dy5nb29nbGUuY29t0jQ0MyIsImZlYXRlcwUi0iJQZXtaXNzaW9uc1BvbGljeVVubG9hZC
IsImV4cGlyeSI6MTY4NTY2Mzk5X0=

9 Origin-Trial:
AvudrjMZgL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCCXk80Aqjh01DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJ
vcmlnaW4iOijodHRwcovL3d3dy5nb29nbGUuY29t0jQ0MyIsImZlYXRlcwUi0iJCWNrRm9yd2FyZENhY2h1Tm90UmVzdG
9yZWRsZWFzb25zIwiZkhwaX5IjoxNjkxNTM5MTk5LCJpc1N1YmRvbWFpbI6dHJ1ZX0=

10 Date: Wed, 28 Feb 2024 19:27:28 GMT
11 Expires: Fri, 29 Mar 2024 19:27:28 GMT
12 Cache-Control: public, max-age=2592000
13 Server: gws
14 Content-Length: 220
15 X-Xss-Protection: 0
16 X-Frame-Options: SAMEORIGIN
17 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
18
19 <HTML>
 <HEAD>
 <meta http-equiv="content-type" content="text/html; charset=utf-8">
 <TITLE>
 301 Moved
 </TITLE>
 </HEAD>
 <BODY>
 <H1>
 301 Moved
 </H1>
 The document has moved

 here

 </BODY>
</HTML>

5) Outils

BurpSuite

Démonstration en live

6) Mise en application

- Installation des outils :
 - Curl : sudo apt install curl
 - Burp : <https://portswigger.net/burp/releases/professional-community-2023-12-1-5?requestededition=community&requestedplatform=>
- Challenges :
 - Client (JavaScript) : <https://www.root-me.org/fr/Challenges/Web-Client/>
 - Serveur (HTTP, SQL, PHP) : <https://www.root-me.org/fr/Challenges/Web-Serveur/>

Merci à vous !