



I. Web (Server-Side Vulns)

Jaime García y Sandra García

1. URL
2. Funcionamiento de una WEB
3. Frameworks
4. HTTP y HTTPS
5. Fuzzing
6. Cookies
7. LFI

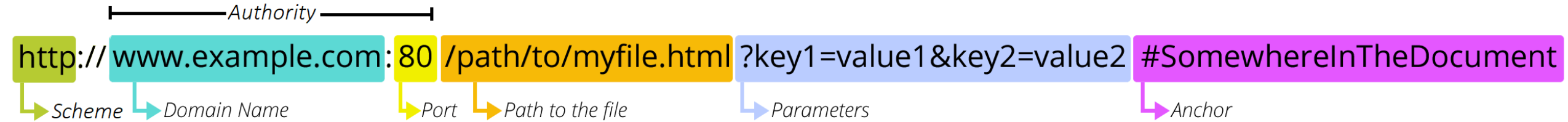


URL



Universidad
Rey Juan Carlos

URL: Uniform Resource Locator



EJEMPLOS

- `https://google.es/search?q=como+ganar+dinero`
- `ftp://ftp.funet.fi/pub/doc/rfc/rfc1738.txt`
- `mailto:raul.martin@urjc.es?subject=Que+aula+es`

Funcionamiento de una página web

Archivos esenciales en una web

Los archivos esenciales son 3, un lenguaje de marcado HTML, uno de estilo CSS y otro funcional JavaScript



HTML: Hyper Text Markup Language

HTML es un lenguaje de marcado, que se forma por etiquetas y texto plano.

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Solo HTML</title>
</head>
<body>
  <h1>Bienvenido a mi página web</h1>
  <p>Este es un ejemplo básico de una página web utilizando solo HTML.</p>
</body>
</html>
```

HTML: Hyper Text Markup Language



CSS: Cascading Style Sheet

Se utiliza para dar estilo al contenido estructurado. También se puede usar con otros lenguajes como XML o SBG

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>HTML con CSS</title>
  <link rel="stylesheet" href="styles.css" <!-- Vincula el CSS -->
</head>
<body>
  <h1>Bienvenido a mi página web</h1>
  <p>Este es un ejemplo básico de una página web utilizando HTML y CSS.</p>
</body>
</html>
```

CSS: Cascading Styles Sheet

Se utiliza para dar estilo al contenido estructurado. También se puede usar con otros lenguajes como XML o SBG

```
/* Estilos generales */
body {
  font-family: 'Helvetica Neue', Arial, sans-serif;
  background-color: #282c34;
  color: #fff;
  margin: 0;
  padding: 0;
  display: flex;
  flex-direction: column;
  justify-content: center;
  align-items: center;
  height: 100vh;
}
```

```
/* Estilo del título */
h1 {
  color: #61dafb;
  font-size: 3em;
  text-transform: uppercase;
  letter-spacing: 5px;
  border-bottom: 2px solid #61dafb;
  padding-bottom: 10px;
  margin-bottom: 20px;
}

/* Estilo del párrafo */
p {
  color: #b0bec5;
  font-size: 1.5em;
  max-width: 600px;
  text-align: center;
  line-height: 1.6;
  margin: 20px;
  border-left: 4px solid #61dafb;
  padding-left: 15px;
  box-shadow: 0 4px 10px rgba(0, 0, 0, 0.3);
}
```

CSS: Cascading Styles Sheet



JavaScript

JavaScript es un lenguaje de programación dinámico que permite agregar interactividad y funcionalidades complejas a las páginas web

Math Class

$1 = 1$
 $1 \neq 2$

Normal Coding Languages

$1 == 1$
 $1 != 2$

Javascript

$1 === 1$
 $1 !== 2$



```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>HTML, CSS y JavaScript</title>
  <link rel="stylesheet" href="styles.css"> <!-- Vincula el CSS -->
</head>
<body>
  <h1>Haz clic en este título</h1>
  <p>Este es un ejemplo básico de una página web utilizando HTML, CSS y JavaScript.</p>
  <script src="script.js"></script> <!-- Vincula el JavaScript -->
</body>
</html>
```

JavaScript

JavaScript es un lenguaje de programación dinámico que permite agregar interactividad y funcionalidades complejas a las páginas web

```
function cambiarColor() {  
    const titulo = document.querySelector('h1');  
    titulo.style.color = titulo.style.color === 'blue' ? '#61dafb' : 'blue';  
}  
  
document.querySelector('h1').addEventListener('click', cambiarColor);
```

JavaScript



Frameworks



Universidad
Rey Juan Carlos

¿Qué frameworks existen?

Existen muchos frameworks para dar dinamismo a nuestras páginas, algunos ejemplos serían PHP y Python con su módulo de Flask

PHP


```
"0000" == 0      => TRUE
"0e12" == 0      => TRUE
"1abc" == 1      => TRUE
"0abc" == 0      => TRUE
"0e12345" == "0e54321" => TRUE
"0e12345" <= "1"  => TRUE
```


FLASK Y JINJA2





Formas de analizar el framework: wappalyzer







 **Wappalyzer** [Website & contact lists →](#)



CMS
 [Wagtail](#)




JavaScript frameworks
 [React](#) 16.14.0


Web frameworks
 [Django](#)

Miscellaneous
 [HTTP/2](#)
 [webpack](#)
 [Gravatar](#)

Programming languages
 [Python](#)

CDN
 [Cloudflare](#)
 [jsDelivr](#)

JavaScript libraries
 [jQuery](#) 3.5.1
 [Modernizr](#) 2.8.3
 [jQuery UI](#) 1.12.1












UI frameworks
 [Bootstrap](#) 4.5.2

[Create an alert for this website](#)  

Formas de analizar el framework: wappalyzer

Wappalyzer

TECNOLOGÍAS MÁS INFORMACIÓN Export

Analítica	Lenguaje de programación
 Google Analytics GA4	 PHP
Framework JavaScript	Tag Manager
 RequireJS 2.3.5	 Google Tag Manager
Reproductor de Video	Librerías JavaScript
 VideoJS	 jQuery 3.6.1
Seguridad	 core-js 3.15.0
 HSTS	 YUI 3.17.2
Tipografía	UI Frameworks
 Google Font API	 Tailwind CSS

U aula
virtual


Acceso usuarios URJC

Otros accesos

Asignaturas en abierto

U online
Oferta de titulaciones online

URJCx
Conocimiento abierto
Cursos gratuitos online


Centro de Innovación Docente
y Educación Digital

Formas de analizar el framework: wappalyzer

Analítica



Framework JavaScript



Reproductor de Vídeo



Seguridad



Tipografía



LMS



Lenguaje de programación



Tag Manager



Librerías JavaScript



UI Frameworks



HTTP y HTTPS



Universidad
Rey Juan Carlos

HTTPS

Estos son los protocolos que hacen que la web funcione, la diferencia entre ellos es que HTTPS es HTTP con TLS, es decir cifrado.

HTTPS va a añadir los siguientes pasos al HTTP

- Cifrar la petición con una clave simétrica
- Enviar el mensaje
- El que reciba la petición lo descifra con la misma clave simétrica



HTTPS

- La información se transmite como **texto**
- Es un protocolo **sin estado**, el servidor no tiene memoria
- Nos centraremos sobre todo en la versión 1.0/1.1. Las versiones 2.0 y 3.0 son muy diferentes



```
GET /index.html HTTP/1.1
Host: google.es
Cabecera2: valor2
Cabecera3: valor3
```

Petición



```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.es/
Content-Type: text/html; charset=UTF-8
Content-Length: 218
[\n\n]
<HTML><HEAD>
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.es/">here</A>.
</BODY></HTML>
```

Respuesta

HTTPS

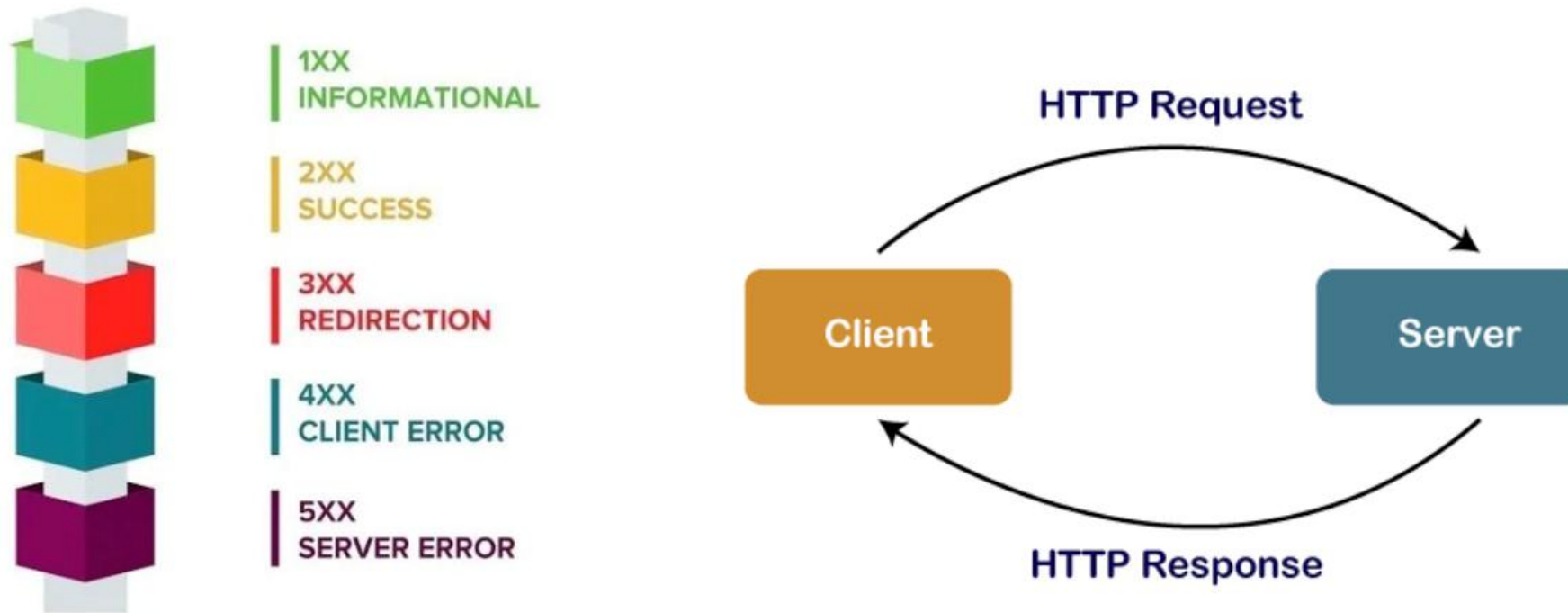
En el ejemplo de antes se ve como realizaba un GET, pero existen más métodos HTTP

- **POST:** Es el más utilizado junto a GET, suele servir para realizar peticiones en las que se envían datos, como podría ser un login.
- **HEAD:** Te devuelve las mismas cabeceras que si hicieras un GET pero no llega a descargar ficheros, por ejemplo si te fuera a descargar una imagen, solo te devolvería el content-length.
- **PUT:** Es similar a POST, pero es idempotente, es decir que si se realiza la misma petición varias veces, solo tendrá efecto la primera.
- **DELETE:** Borra recursos del servidor, normalmente este es un método que quieres quitar de tu web.

Más información aquí: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods>

Códigos de estado

¿ERROR 404? Ya iba tocando saber que significa



Más información sobre los códigos de estado: <https://developer.mozilla.org/es/docs/Web/HTTP/Status>

Herramientas



RETO



Universidad
Rey Juan Carlos

Cookies



Universidad
Rey Juan Carlos

Cookies

me: *goes to a website for the first time*
the website:



¿Qué son las Cookies?

- Pequeños archivos de texto que se almacenan en el navegador del usuario.
- Crean un "registro" que ayuda a personalizar la experiencia del usuario.

Herramientas



Cookie Editor

RETO DE COOKIES

LFI



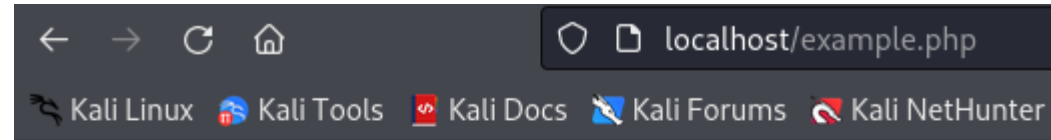
Universidad
Rey Juan Carlos

LFI

```
<?php
echo "<h1>Hola buenas!</h1>";

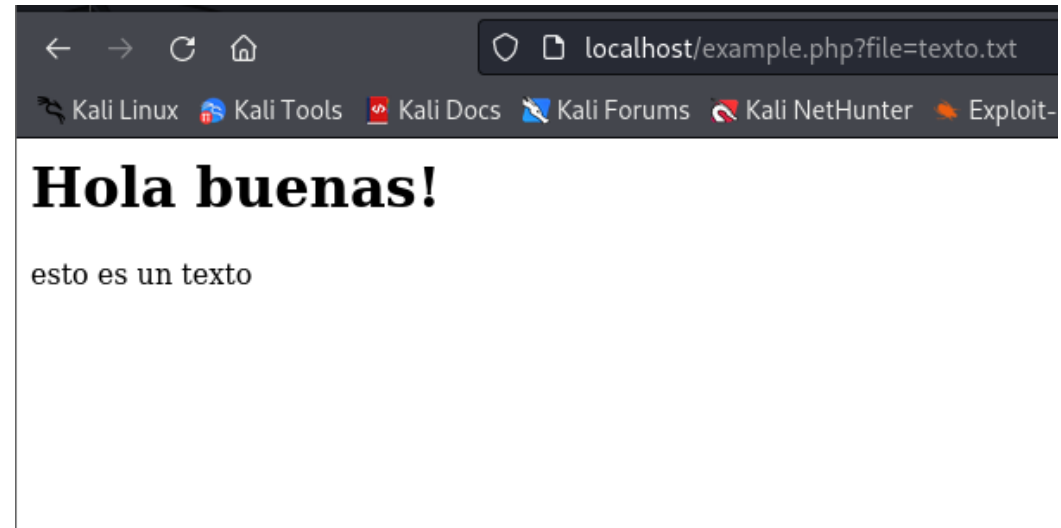
$filename = $_GET['file'];
include($filename);
?>
```

→ **Hola buenas!**



```
texto.txt *
esto es un texto
CyberChef python | GTF0Bin
```

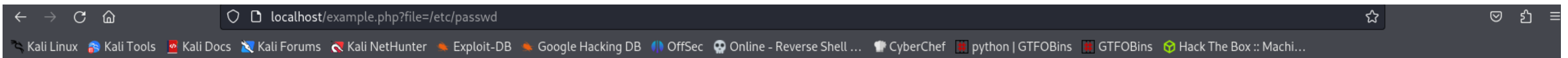
→ **Hola buenas!**
esto es un texto




```
localhost/example.php?file=texto.txt
```

¿Y si en vez de un archivo de texto busco un directorio sensible?

/etc/passwd

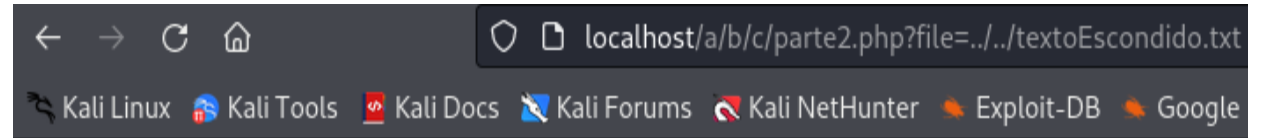


Hola buenas!

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534:./nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin _galera:x:100:65534:./nonexistent:/usr/sbin/nologin mysql:x:101:102:MySQL Server,./nonexistent:/bin/false tss:x:102:103:TPM software stack,./var/lib/tpm:/bin/false strongswan:x:103:65534:/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:992:992:systemd Time Synchronization:/usr/sbin/nologin rhod:x:104:65534:/var/spool/rwho:/usr/sbin/nologin _gophish:x:105:105:/var/lib/gophish:/usr/sbin/nologin iodine:x:106:65534:/run/iodine:/usr/sbin/nologin messagebus:x:107:106:./nonexistent:/usr/sbin/nologin tcpdump:x:108:107:./nonexistent:/usr/sbin/nologin miredo:x:109:65534:/var/run/miredo:/usr/sbin/nologin _rpc:x:110:65534:/run/rpcbind:/usr/sbin/nologin Debian-snmpp:x:111:109:/var/lib/snmpp/bin/false redis:x:112:111:/var/lib/redis:/usr/sbin/nologin usbmux:x:113:46:usbmux daemon,./var/lib/usbmux:/usr/sbin/nologin mosquito:x:114:114:/var/lib/mosquito:/usr/sbin/nologin redsocks:x:115:115:/var/run/redsocks:/usr/sbin/nologin stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin sshd:x:116:65534:/run/sshd:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin statd:x:117:65534:/var/lib/nfs:/usr/sbin/nologin sslh:x:118:118:./nonexistent:/usr/sbin/nologin postgres:x:119:119:PostgreSQL administrator,./var/lib/postgresql/bin/bash avahi:x:120:120:Avahi mDNS daemon,./run/avahi-daemon:/usr/sbin/nologin _gvm:x:121:122:/var/lib/openvas:/usr/sbin/nologin speech-dispatcher:x:122:29:Speech Dispatcher,./run/speech-dispatcher/bin/false inetsim:x:123:124:/var/lib/inetsim:/usr/sbin/nologin pulse:x:124:125:PulseAudio daemon,./run/pulse:/usr/sbin/nologin geoclue:x:125:127:/var/lib/geoclue:/usr/sbin/nologin lightdm:x:126:128:Light Display Manager:/var/lib/lightdm/bin/false saned:x:127:130:/var/lib/saned:/usr/sbin/nologin polkitd:x:989:989:User for polkitd:/usr/sbin/nologin rtkit:x:128:131:RealtimeKit,./proc:/usr/sbin/nologin colord:x:129:132:colord colour management daemon,./var/lib/colord:/usr/sbin/nologin nm-openvpn:x:130:133:NetworkManager OpenVPN,./var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:131:134:NetworkManager OpenConnect plugin,./var/lib/NetworkManager:/usr/sbin/nologin kali:x:1000:1000:kali,./home/kali:/usr/bin/zsh
```

- Para ver mejor usar ctrl+u

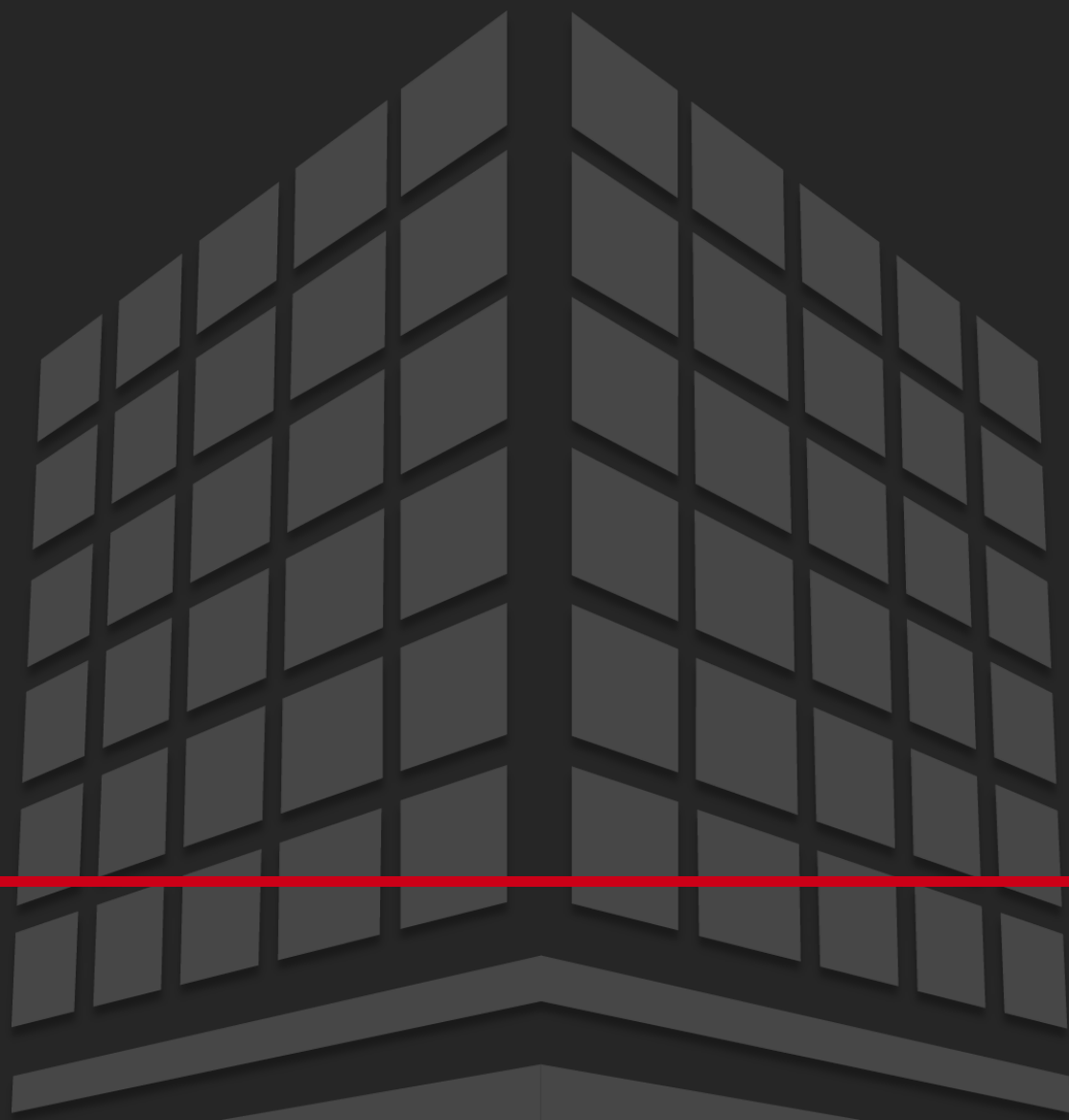
```
(kali㉿kali)-[/var/.../html/a/b/c]  
$ ls  
parte2.php  
  
(kali㉿kali)-[/var/.../html/a/b/c]  
$ ls ../..  
b textoEscondido.txt  
  
(kali㉿kali)-[/var/.../html/a/b/c]  
$ cat ../../textoEscondido.txt  
Un texto muy escondido
```



Ahora con más directorios

Un texto muy escondido

- Los dos puntos .. representan al directorio padre



Universidad
Rey Juan Carlos