UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Seguridad en la Web

Práctica opcional

Proxy HTTP

La Universidad en Internet

Javier Parra

Presentación

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

- Vamos a realizar una práctica utilizando varias herramientas para monitorizar la red y realizar secuestro de sesión.

- Para ello vamos a utilizar las herramientas:
  - Firefox Tamper Data
  - Jhijack

- Se va a poner en funcionamiento la práctica Blind String SQL Injection de WebGoat.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Firefox Tamper Data

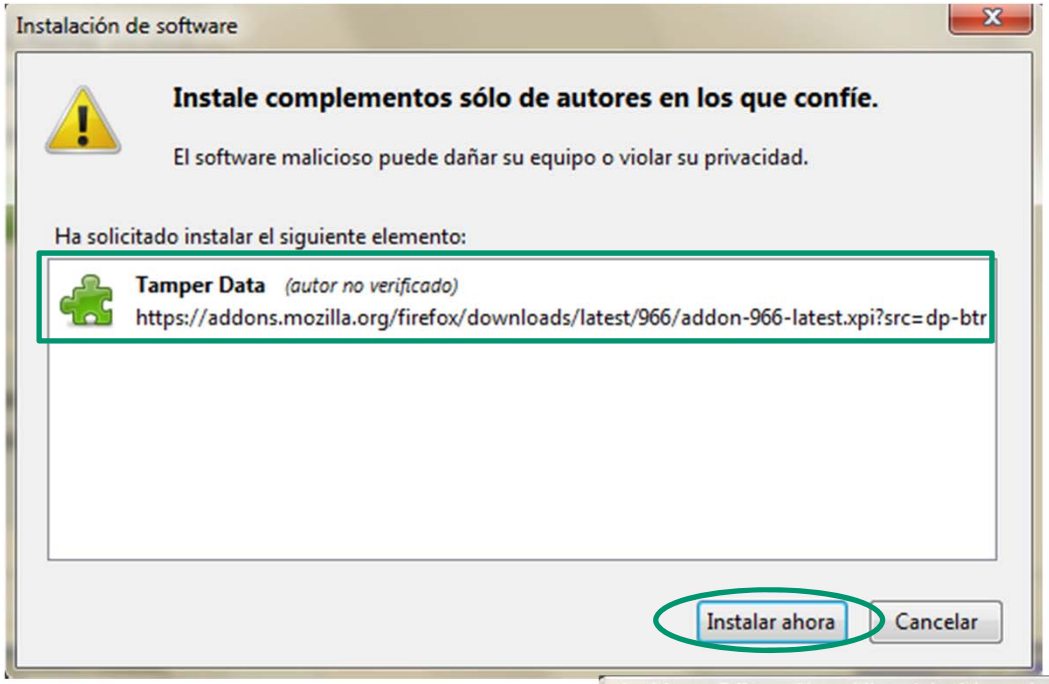
Firefox Tamper Data - Descarga

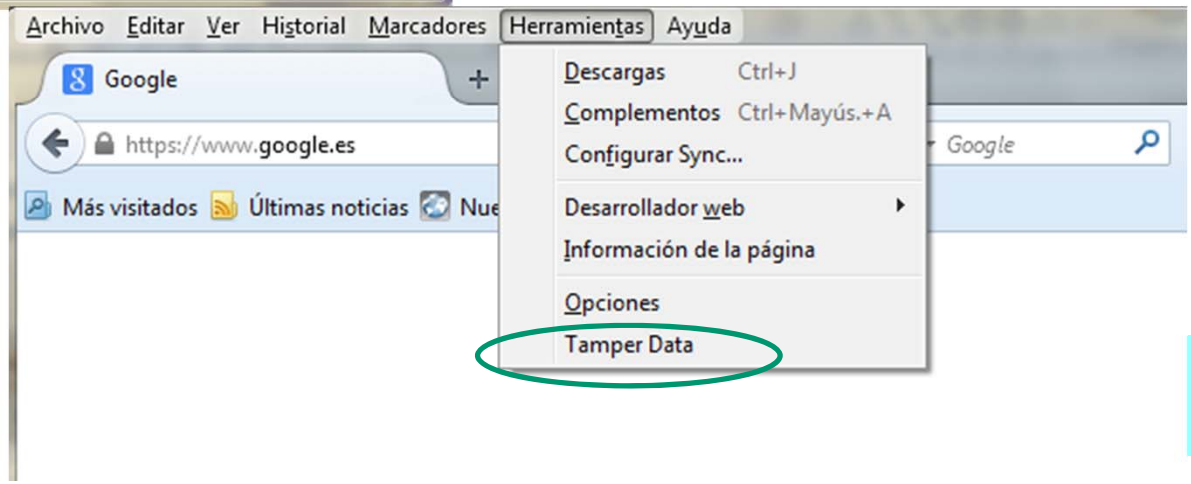
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

- Extensión de Firefox que permite visualizar y modificar las cabeceras y los parámetros POST de las peticiones HTTP/HTTPS
- https://addons.mozilla.org/es/firefox/addon/tamper-data/

Firefox Tamper Data - Instalación

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

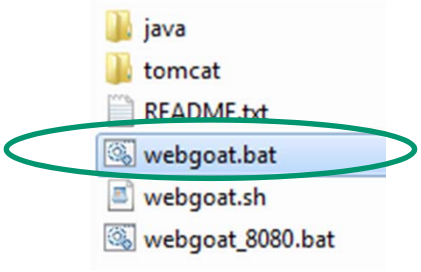


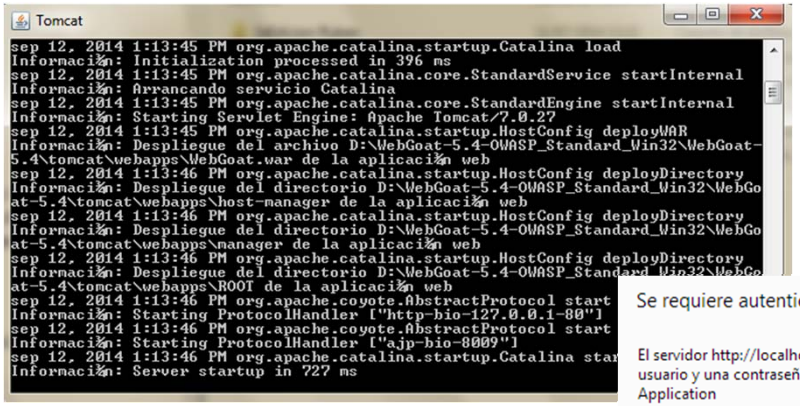


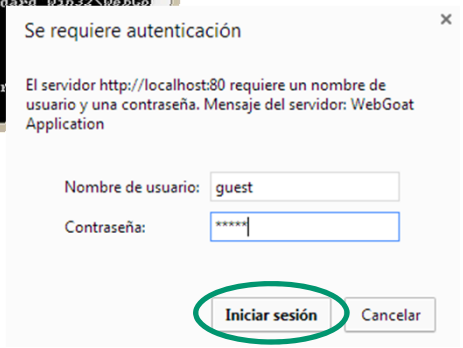
Firefox Tamper Data - Prueba

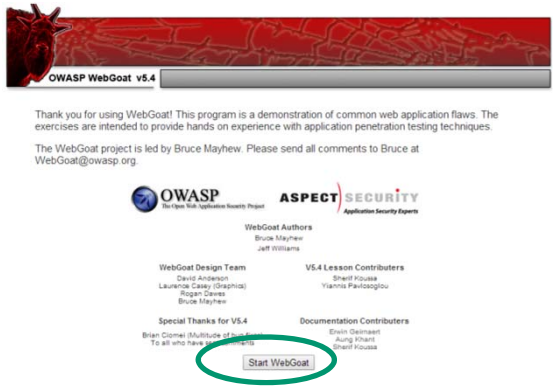
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

- Ejecutar aplicación (p.e. WebGoat)





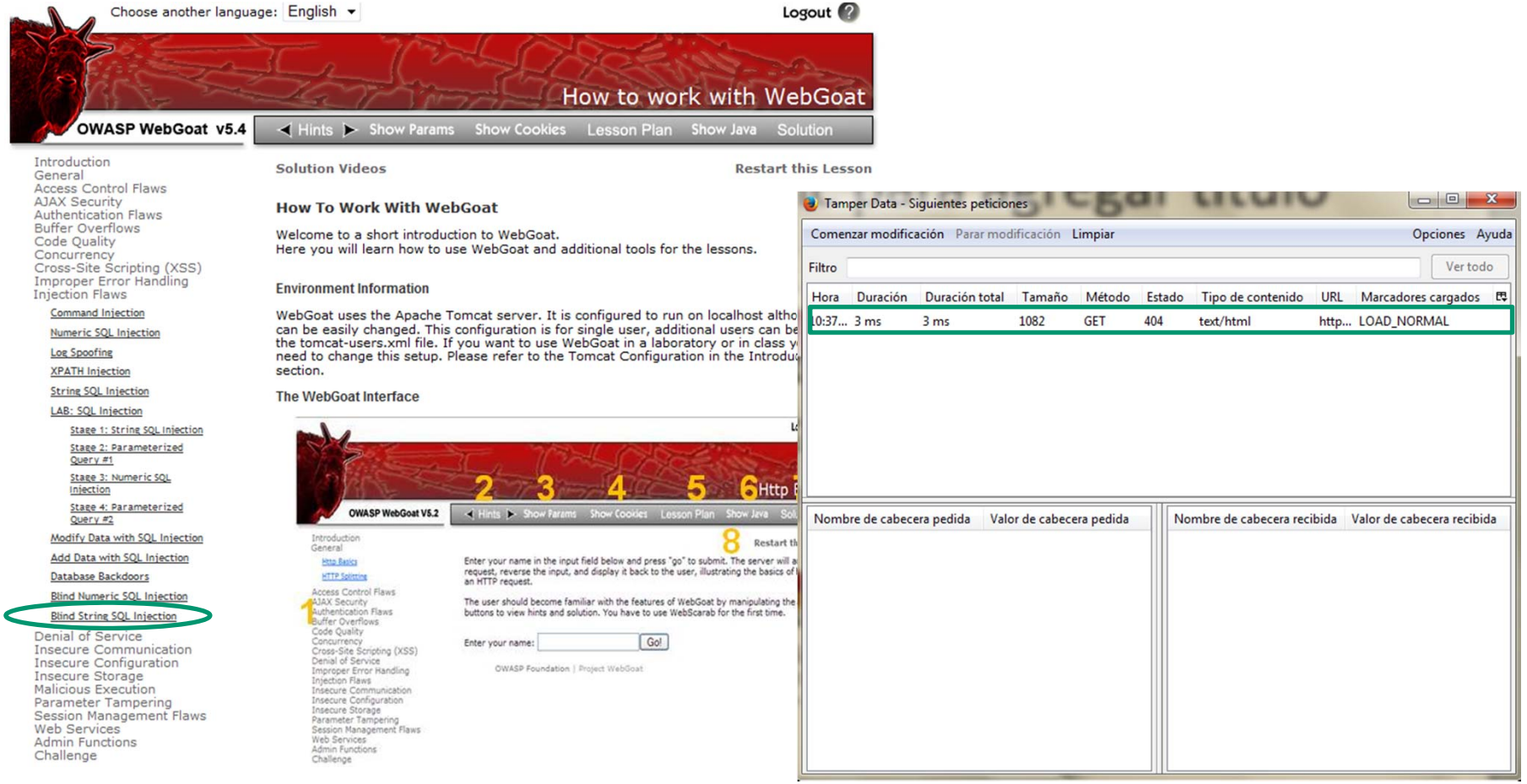




Firefox Tamper Data - Prueba

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

- Al interactuar con la aplicación, en Firefox Tamper Data aparecerá la información de las peticiones



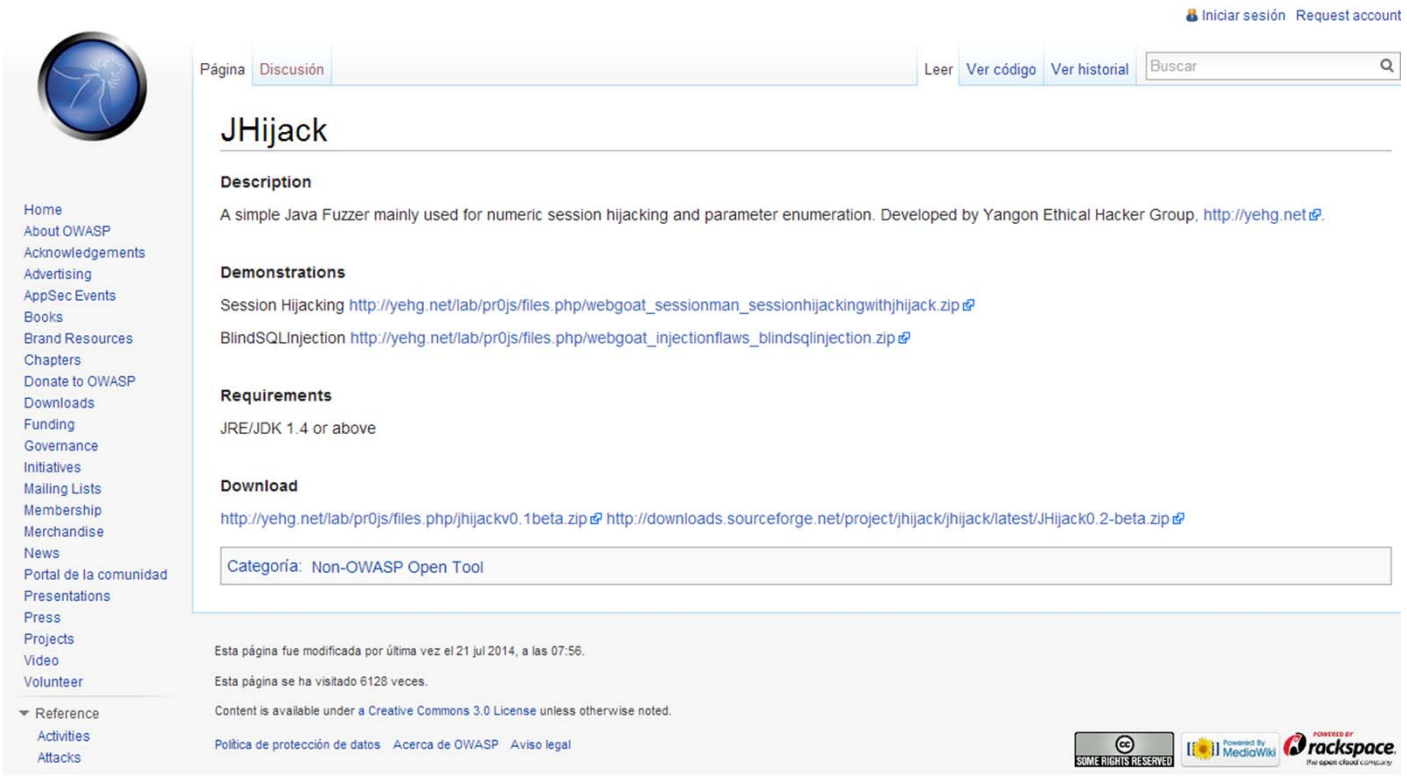
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

JHijack

JHijack – Sitio web

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

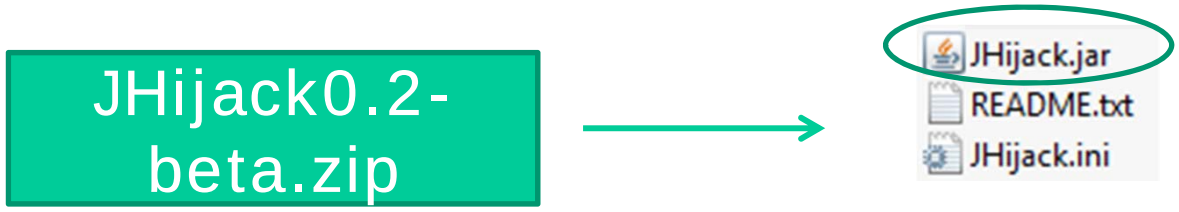
- Herramienta Java para simular la apropiación de sesiones
- https://www.owasp.org/index.php/JHijack



JHijack - Descarga

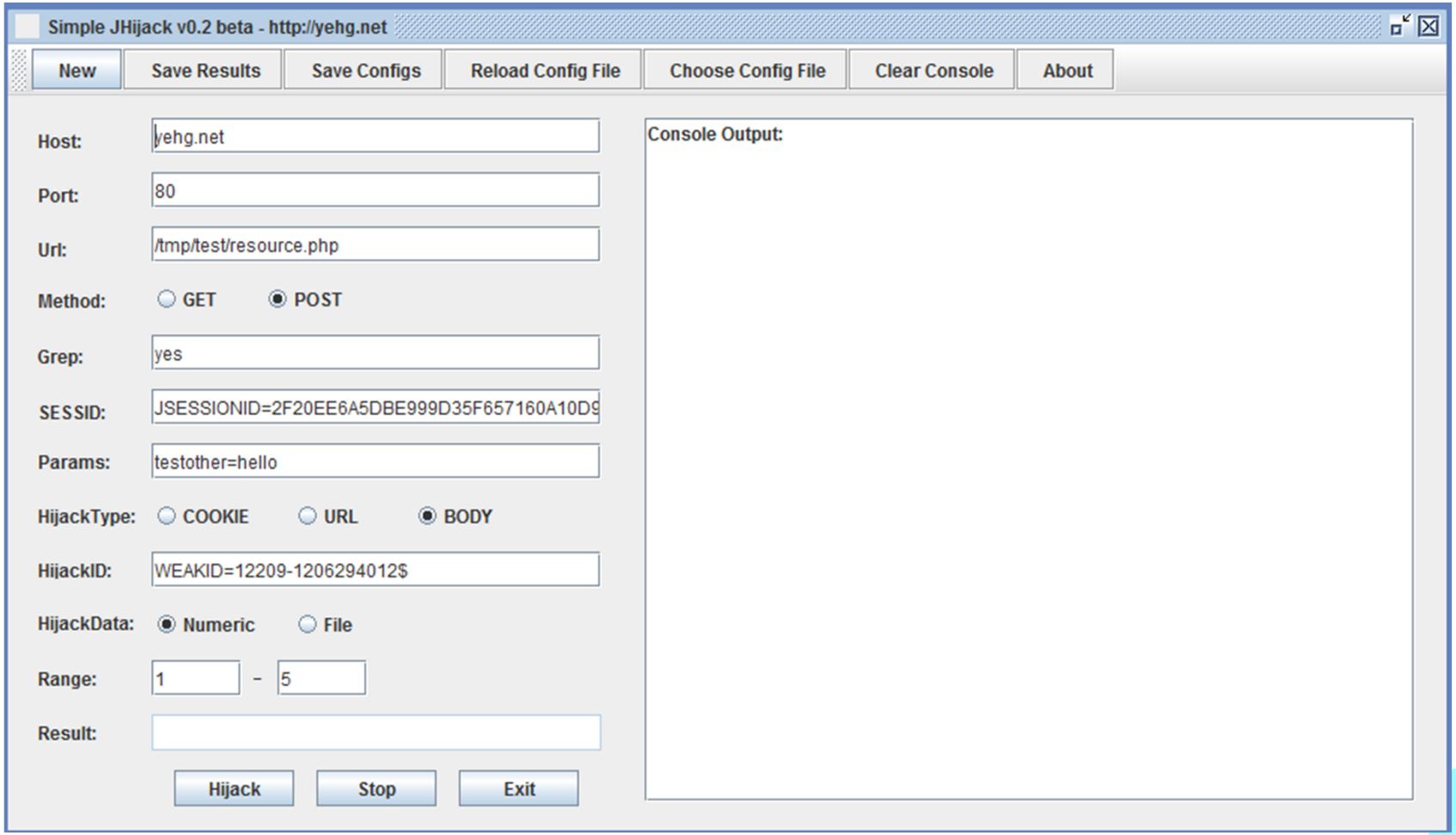
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

- Descarga: http://downloads.sourceforge.net/project/jhijack/jhijack/latest/JHijack0.2-beta.zip



JHijack - Interfaz

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

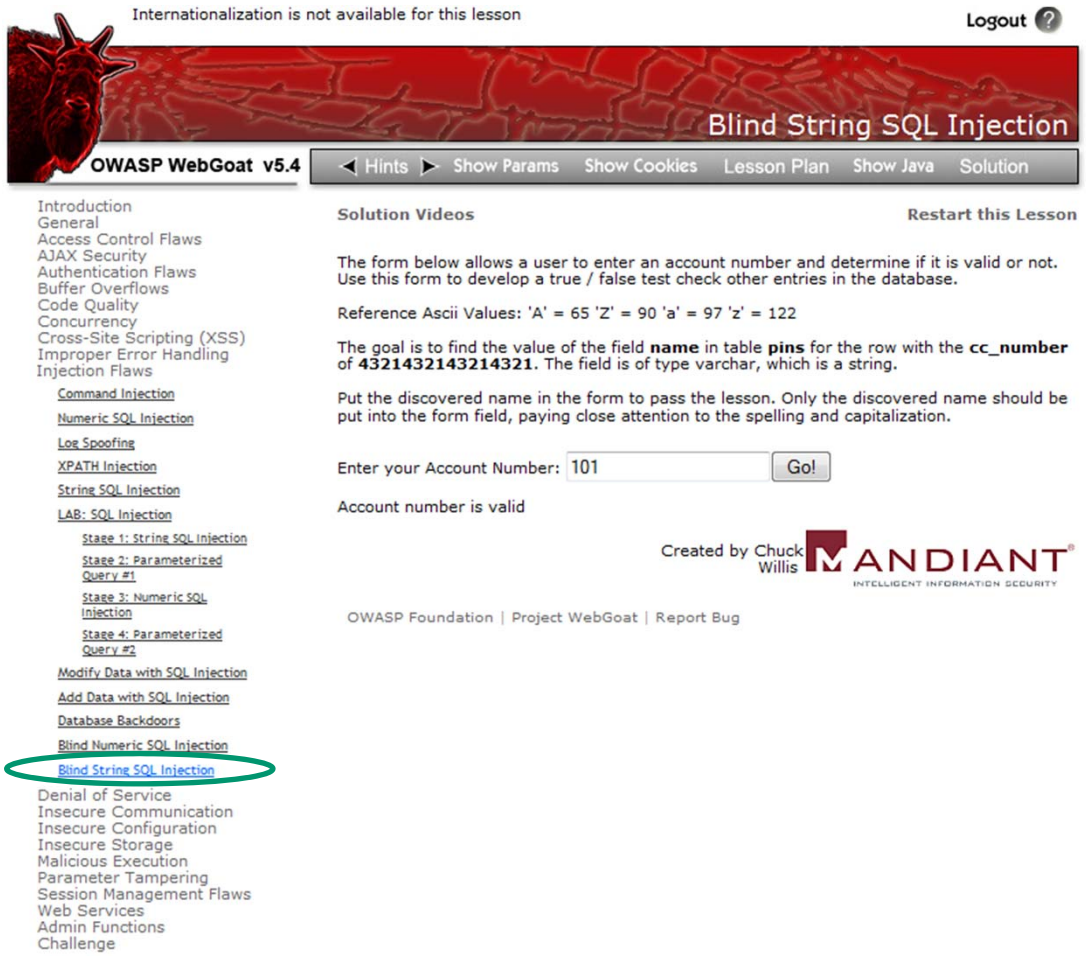


UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Práctica WebGoat
Blind String SQL Injection

1. Abrir la lección en WebGoat con Firefox

- http://localhost/WebGoat/attack

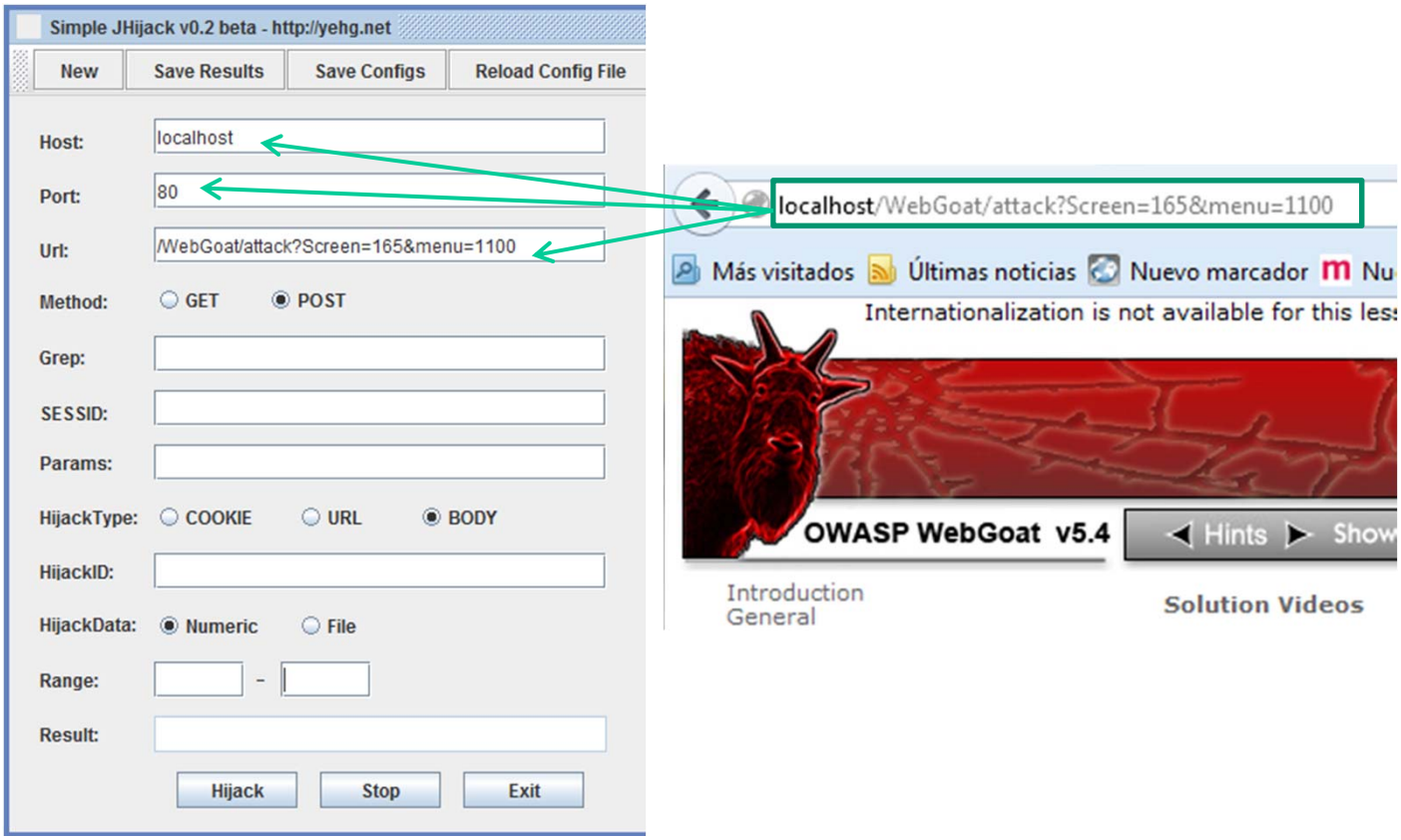


- Aplicación que devuelve si un número de cuenta es o no válido
- Se aprovechará las vulnerabilidades para obtener el nombre del titular de la cuenta 4321432143214321

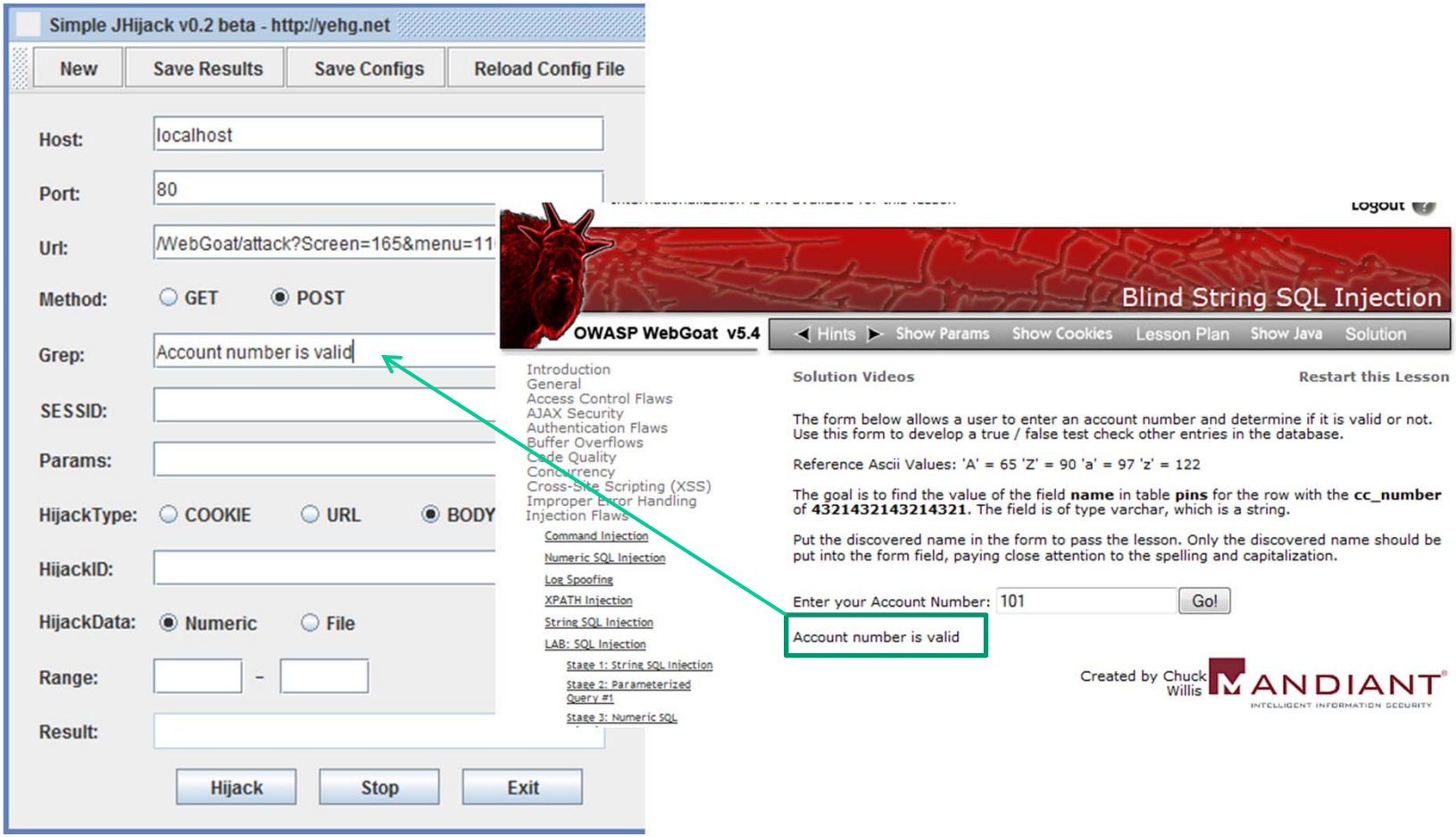
2. Configuración

Configura JHijack para lanzar la consulta:

- Host: localhost
- Port: 80
- Url:



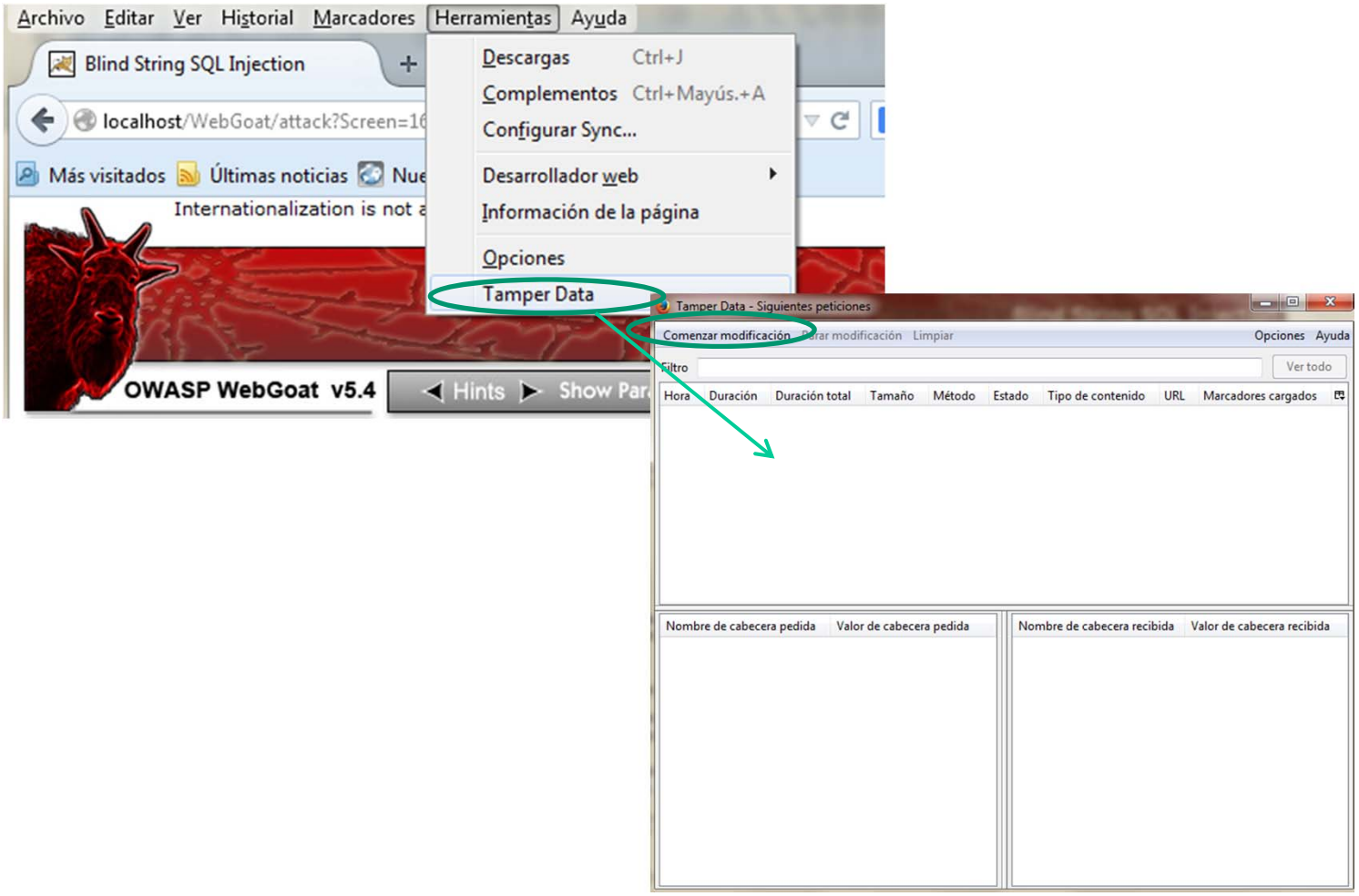
2. Configuración



3. Obtención de la cookie

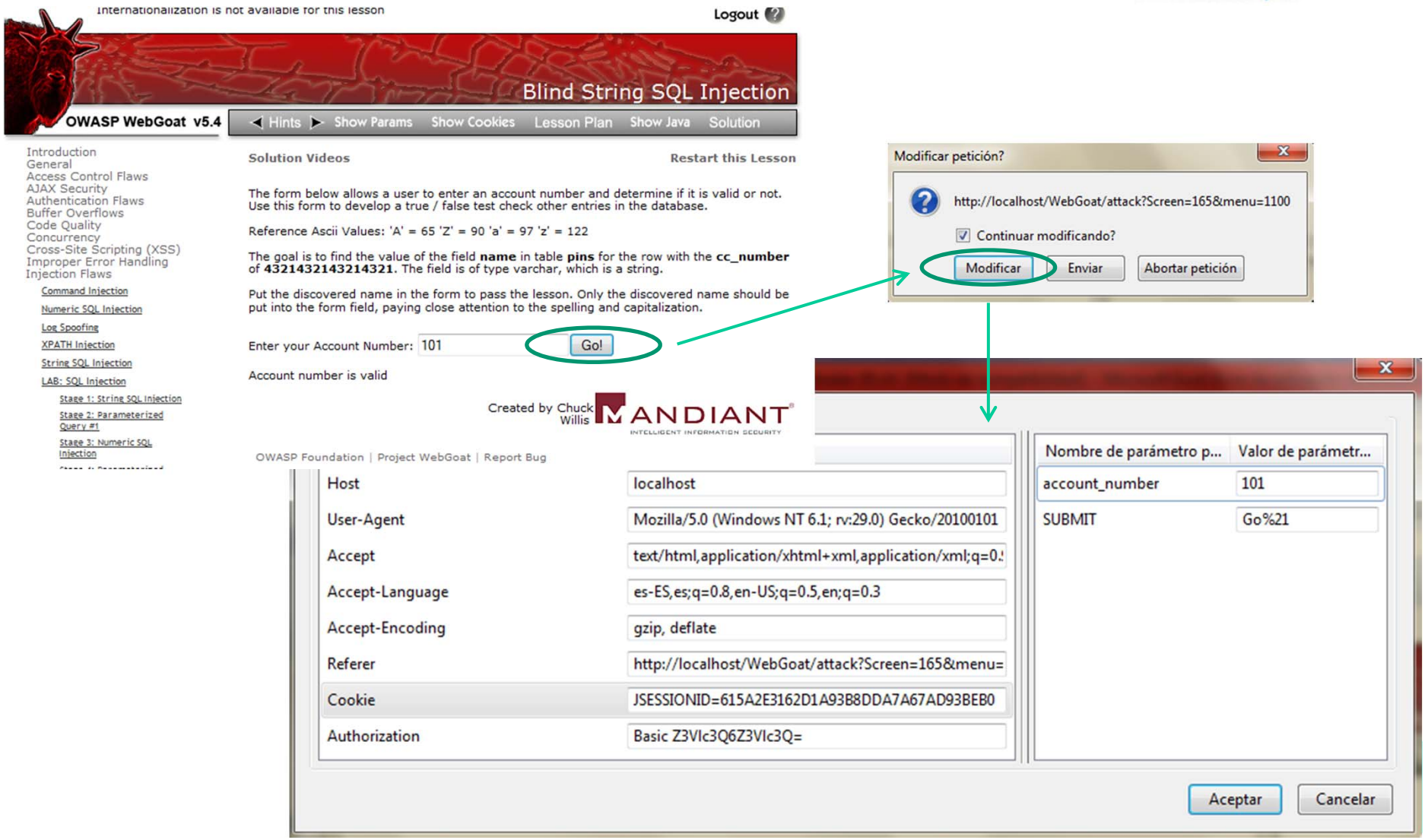
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

- Obtener cookie
  - Activar Firefox Tamper Data



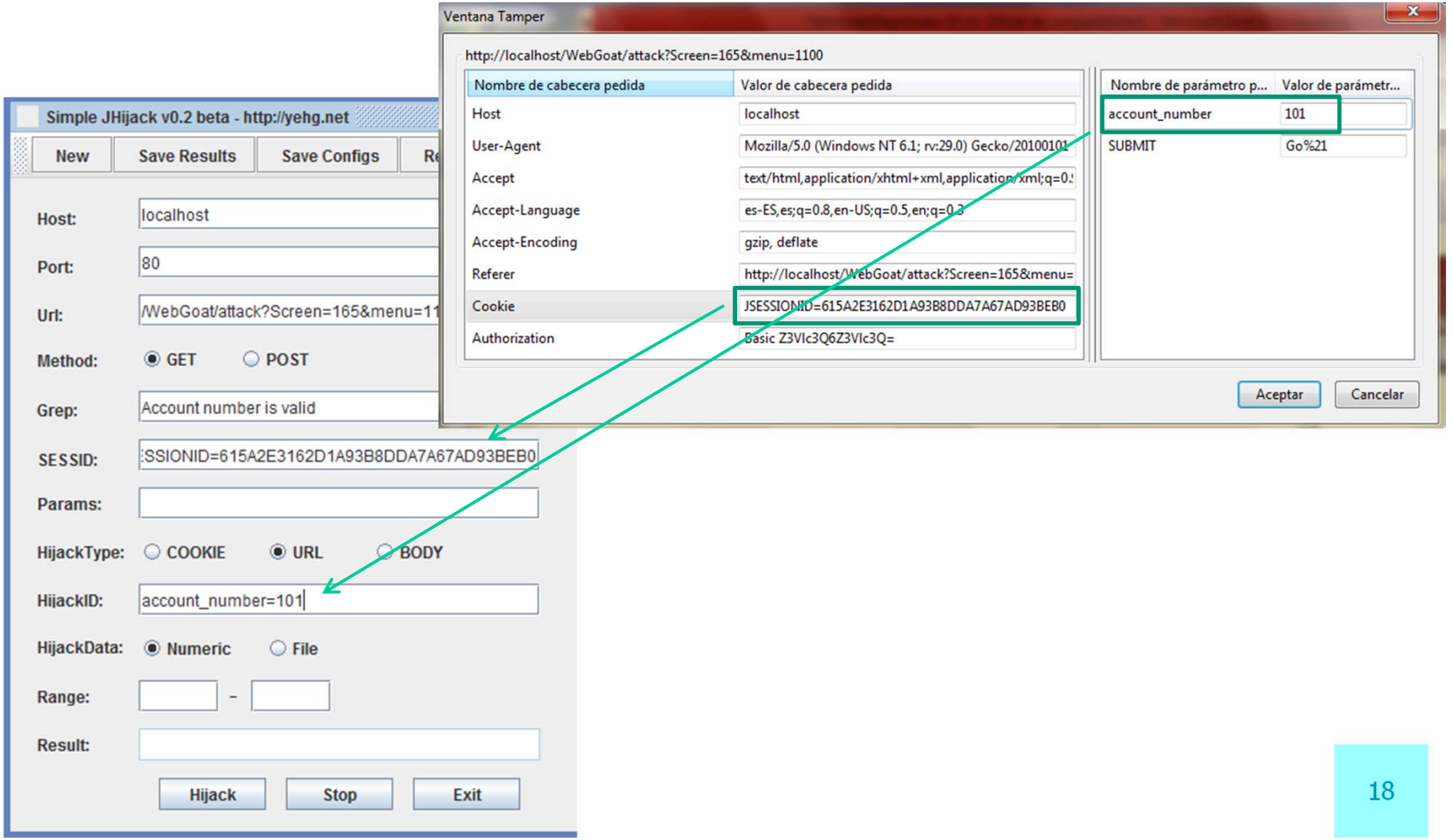
3. Obtención de la cookie

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

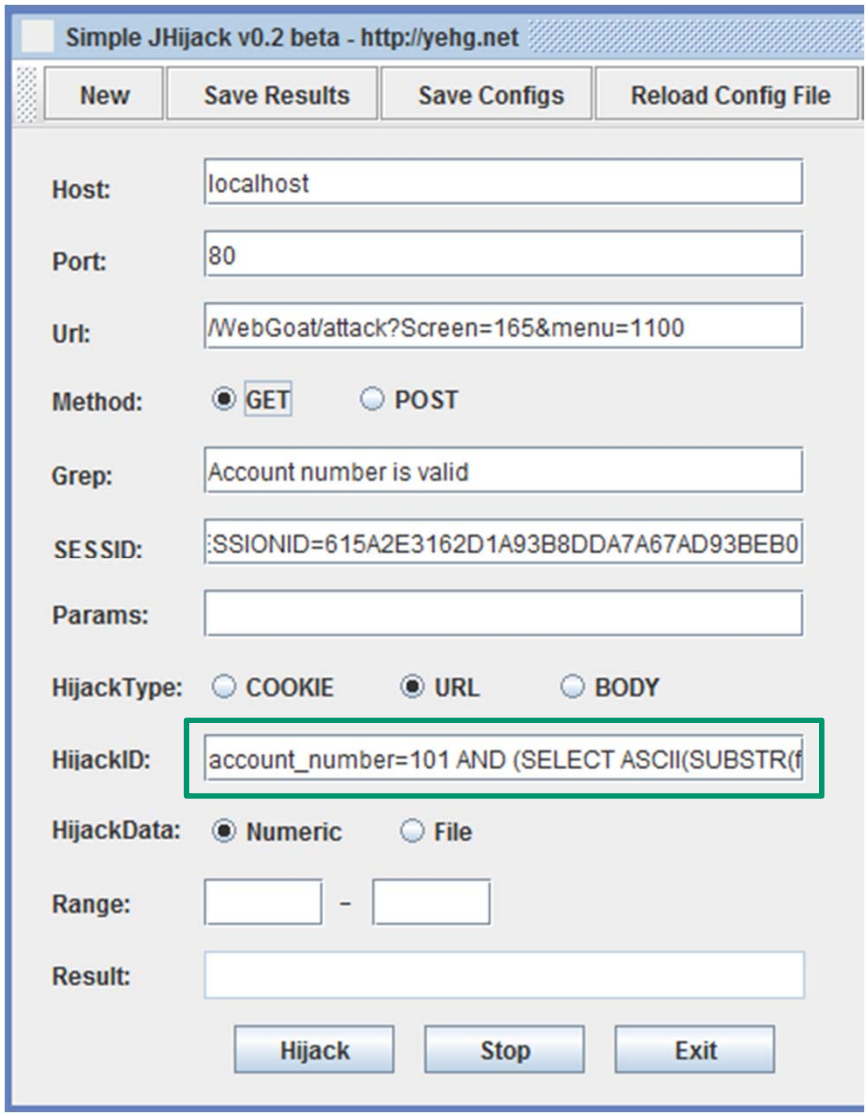


3. Obtención de la cookie

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

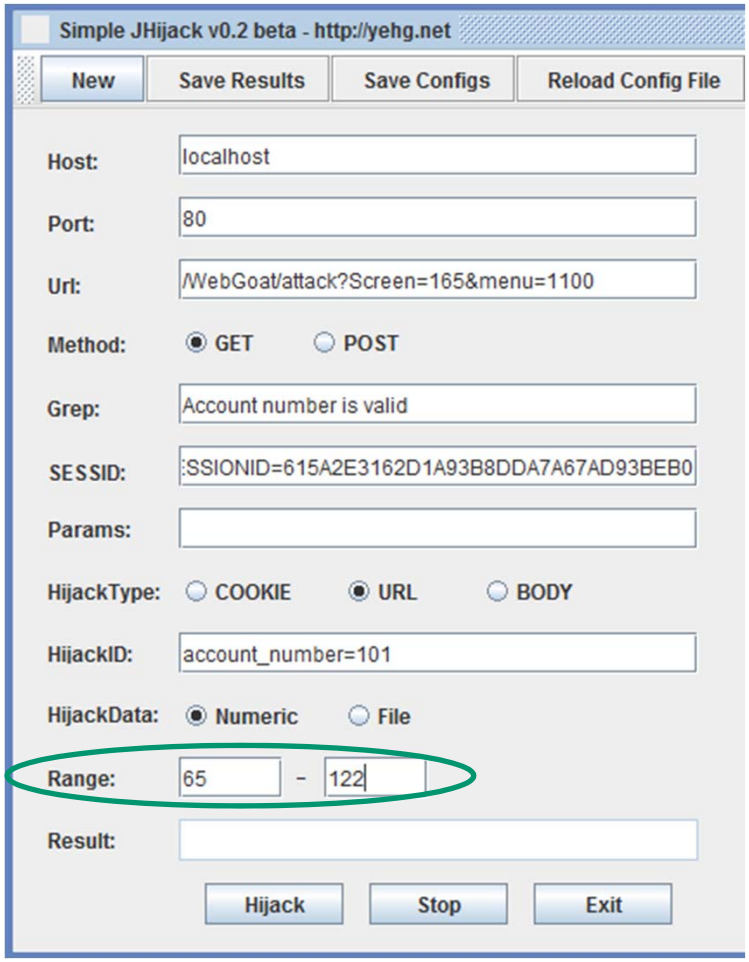


4. Inyección de Código SQL



- Modificar la query para ir obteniendo las letras del nombre:
  - Actual: … account_number=101
  - Nuevo: … account_number=101 AND (SELECT ASCII(SUBSTR(name,1,1)) FROM pins WHERE cc_number=4321432143214321) =$ --

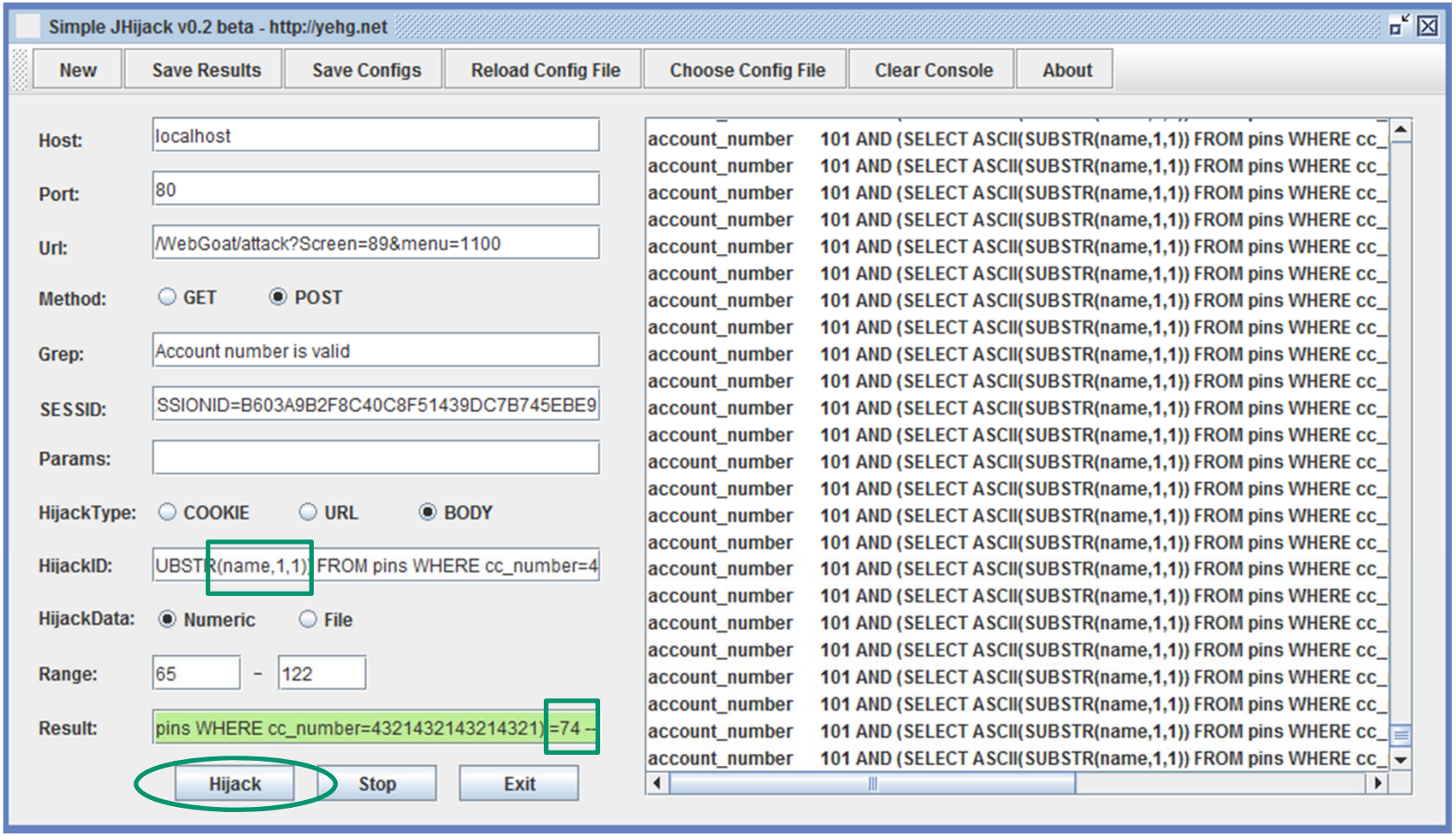
5. Rango de caracteres válidos



- Codificación UTF-8
  - A: 65
  - …
  - Z: 90
  - a: 97
  - …
  - z: 122

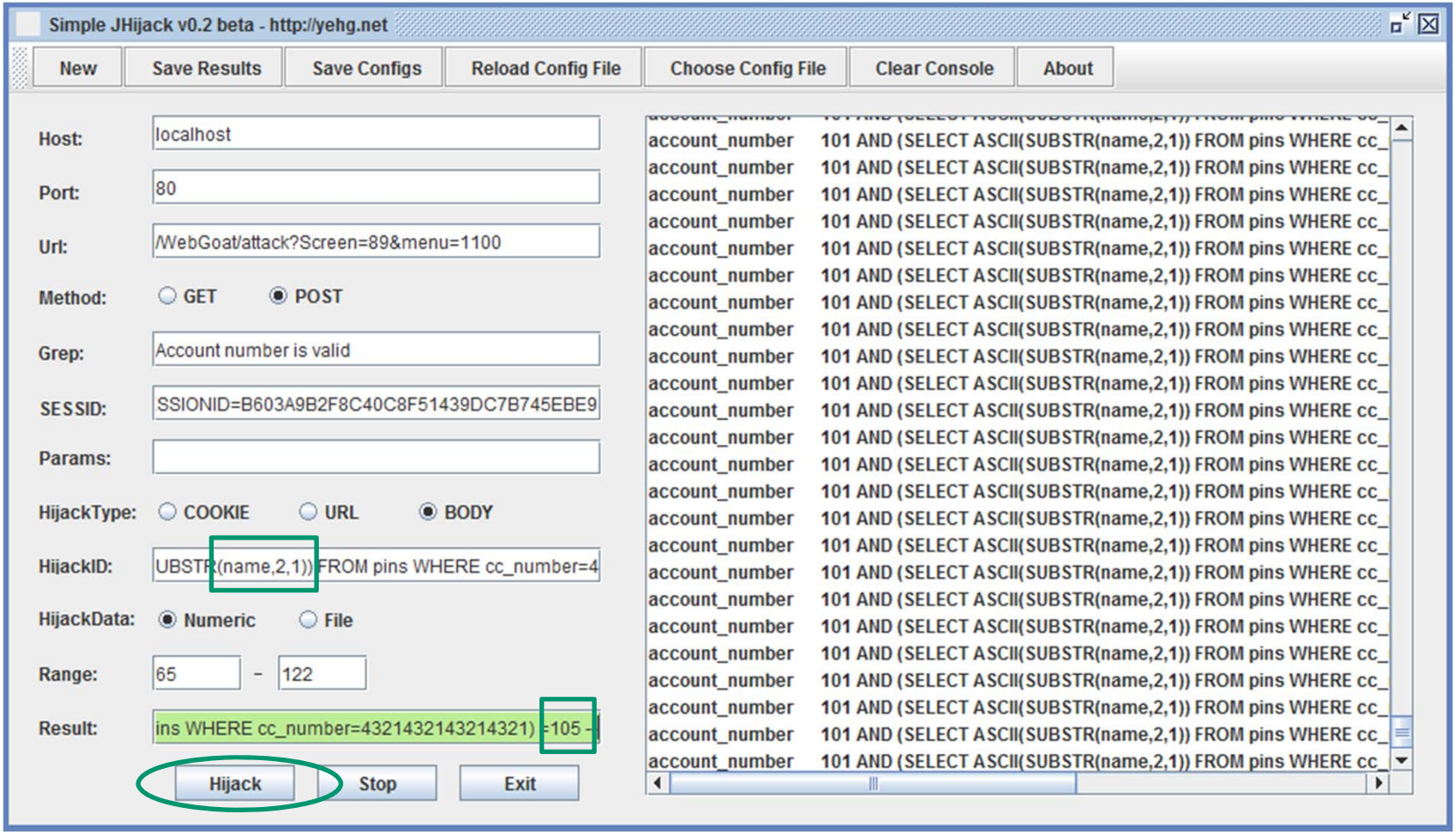
6. Lanzar ataque

- Paso 1: 1ª letra → 74



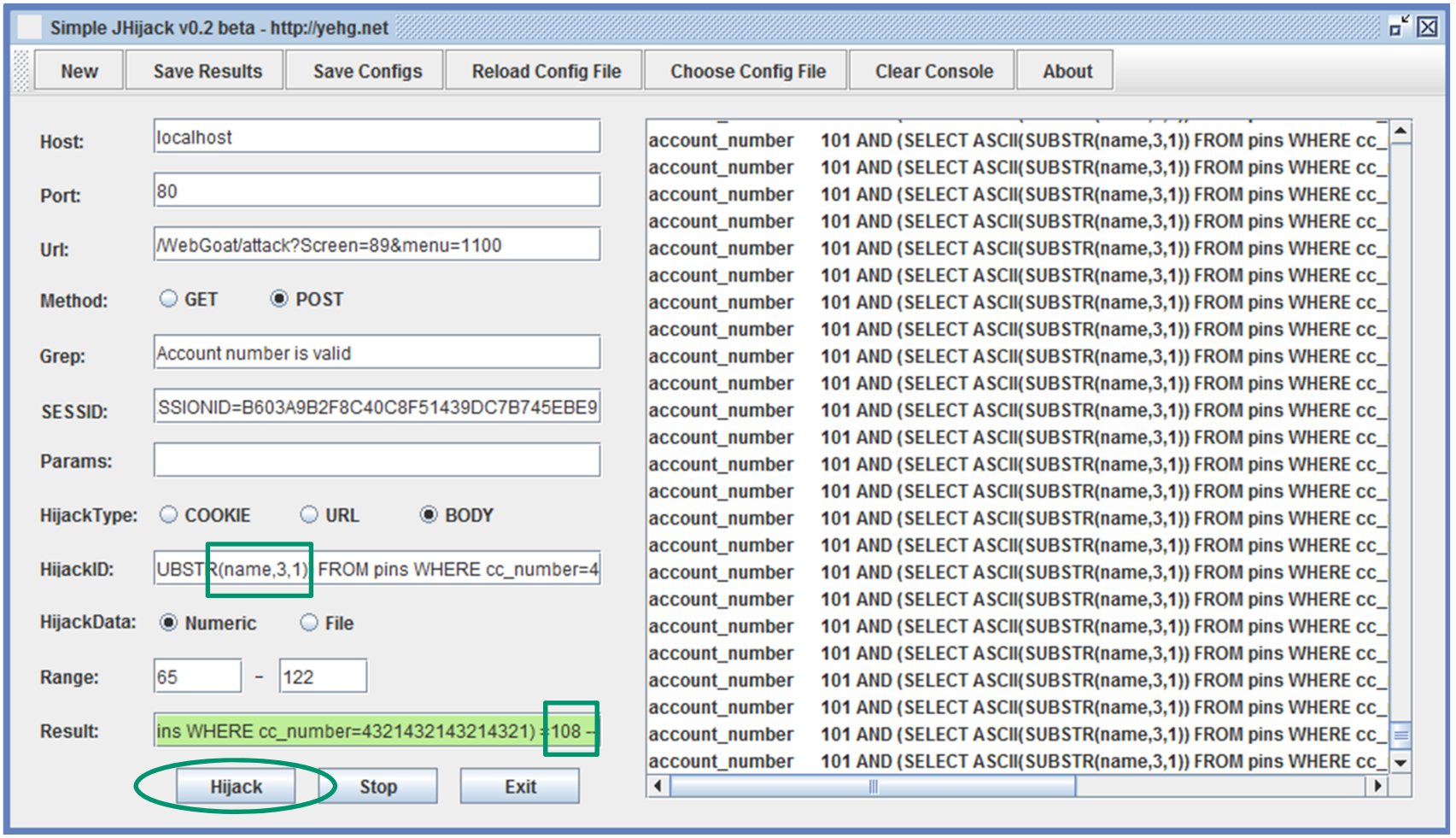
6. Lanzar ataque

- Paso 2: 2ª letra → 105



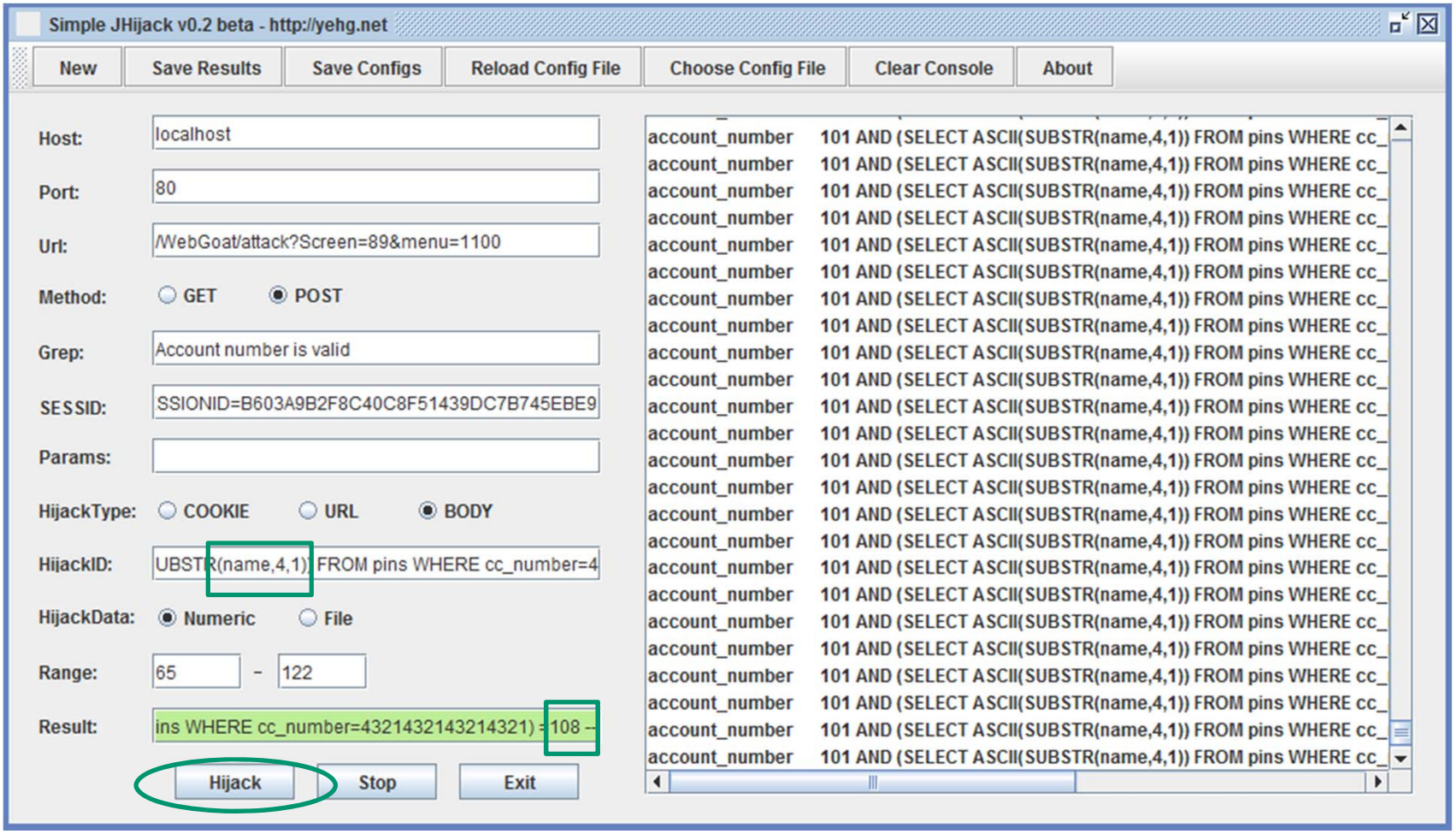
6. Lanzar ataque

- Paso 3: 3ª letra → 108



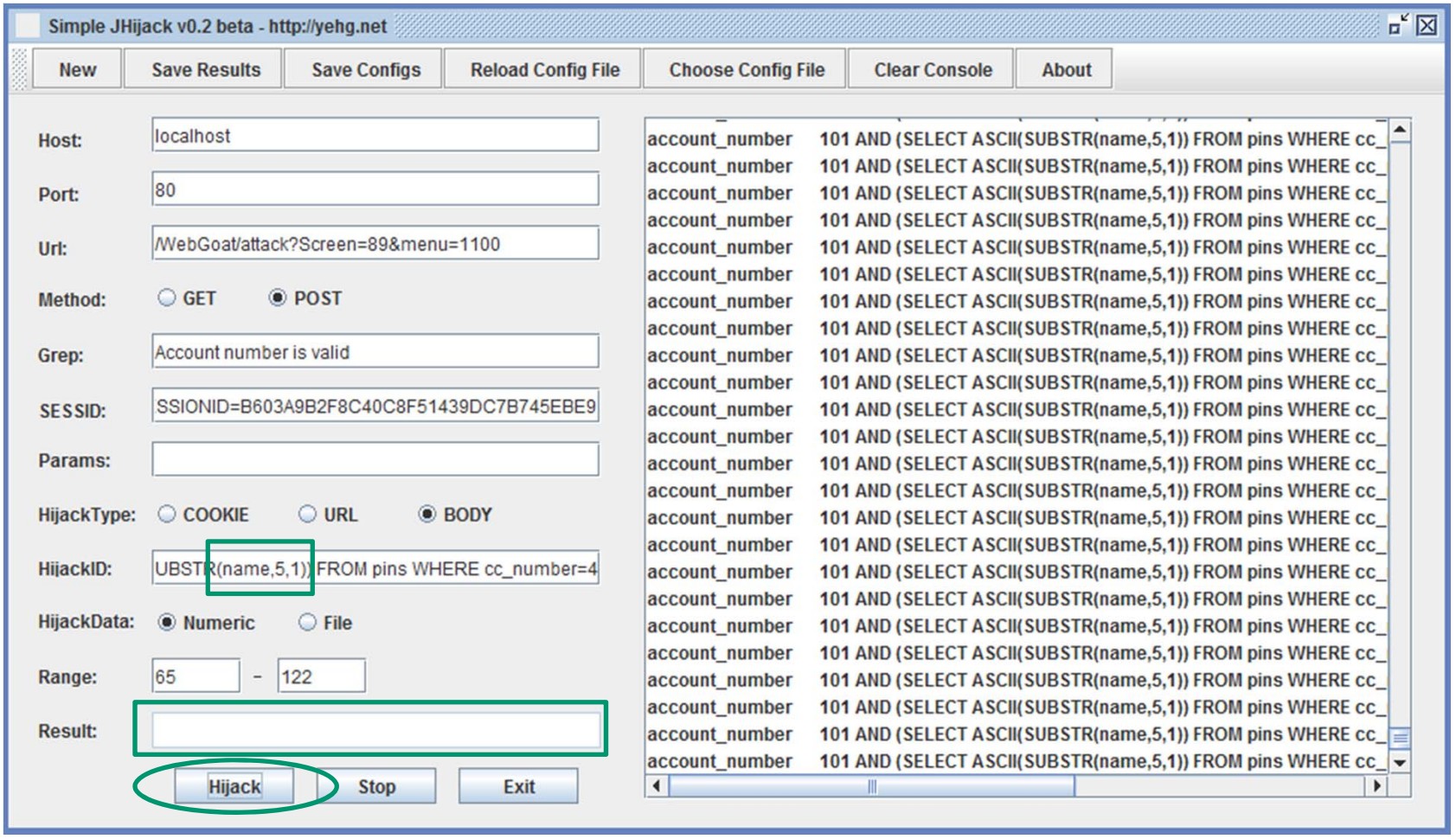
6. Lanzar ataque

- Paso 4: 4ª letra → 108



6. Lanzar ataque

- Paso 5: 5ª letra → No hay



7. Obtención de resultados

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

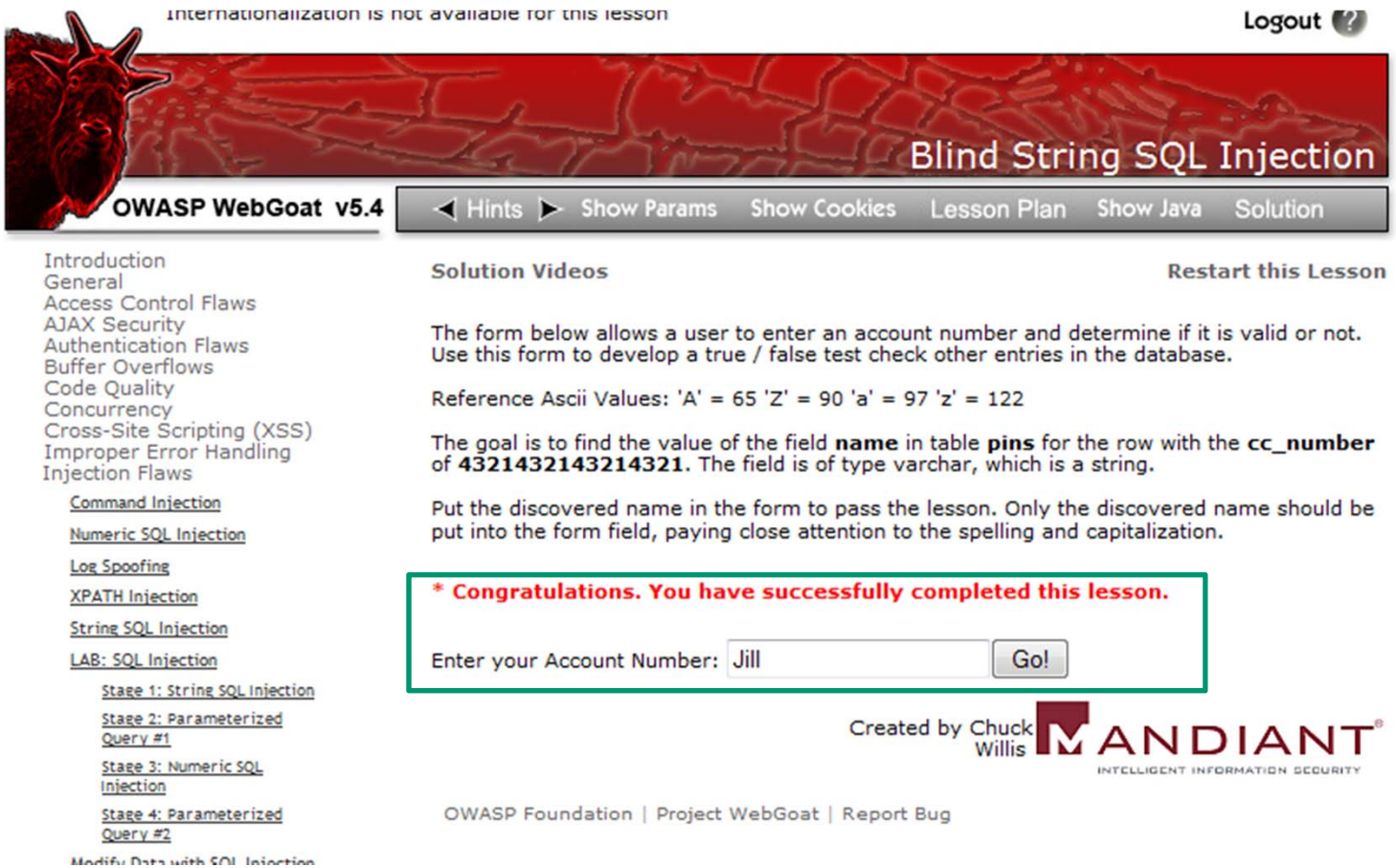
- Letras:
  - 74: J
  - 105: i
  - 108: l
  - 108: l
- Nombre: Jill

Caracteres ASCII imprimibles

32	espacio	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

7. Obtención de resultados

UNIVERSIDAD INTERNACIONAL DE LA RIOJA



UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Seguridad en la Web

Práctica opcional

Proxy HTTP

La Universidad en Internet

Javier Parra