			_		
Ataque	Nombre del Lab	Nivel	Encargado	Realizado	Captura del Lab Comentarios
SQL injection	SQL injection vulnerability in WHERE clause allowing retrieval of hidden da		Oscar	Sí	(Control control of Coll Standard Stand
SQL injection	SOL injection vulnerability allowing login bypass	1 - APPRENTICE	Rubí	Sí	(a) (a) palant a statistic description (a)
SQL injection	SOL injection UNION attack, determining the number of columns returned		Alonso	Sí	(ARE 90), injection (ANDM attack, determining the number of columns networks for guery >
SQL injection		2 - PRACTITIONER	Alonso	Sí	LNE SQL ripcton LNOCN attack, finding a calum containing loci : A Solved
SQL injection		2 - PRACTITIONER	Oscar	Sí	and the latter and th
SQL injection		2 - PRACTITIONER	Oscar	Sí	Mark 100 miles (Mill and undergraphy of the control
SQL injection	SQL injection attack, querying the database type and version on Oracle	2 - PRACTITIONER	Oscar	Sí	Bully on the partyles relating at the orients.
SQL injection	SQL injection attack, querying the database type and version on MySQL an	2 - PRACTITIONER	Oscar	Sí	(it specially complete strongers was which per blanch
SQL injection	SOL injection attack, listing the database contents on non-Oracle database	2 - PRACTITIONER	Oscar	Sí	The State of the S
SQL injection	SOL injection attack, listing the database contents on Oracle	2 - PRACTITIONER	Oscar	Sí	(E) Spin AA, Shipha Salama casaa origan :
SQL injection	Blind SQL injection with conditional responses	2 - PRACTITIONER	Rubí	Sí	Op Spell and antidep descriptions :
SQL injection	Blind SOL injection with conditional errors	2 - PRACTITIONER	Rubí	Sí	(in National Addition, description as approximate appr
SQL injection	Blind SOL injection with time delays	2 - PRACTITIONER	Rubí	Sí	(M. (1) selected and physique (
SQL injection	Blind SQL injection with time delays and information retrieval	2 - PRACTITIONER	Rubí	Sí	are the characteristic party from the origin and come of from:
SQL injection		2 - PRACTITIONER	Rubí	Sí	A to the state of
	Blind SQL injection with out-of-band interaction  Blind SQL injection with out-of-band data exfiltration	2 - PRACTITIONER			(a) the SET date, desire yellow date in the place in the second of the s
SQL injection			Rubí	Sí	LABI Reference 2006 into HTML (content with nothing encoded > A Stored
Cross-site scripting	Reflected XSS into HTML context with nothing encoded	1 - APPRENTICE	Alonso	Sí	LAB Parlicid XSS into an base with angle branches in M.C. encoded >
Cross-site scripting	Reflected XSS into attribute with angle brackets HTML-encoded	1 - APPRENTICE	Alonso	Sí	
Cross-site scripting	Stored XSS into anchor href attribute with double quotes HTML-encoded	1 - APPRENTICE	Axel	Sí	LAS Stand XSS Ho andron to at all delicale with double quales NTIIL encoded ()
Cross-site scripting	Reflected XSS into a JavaScript string with angle brackets HTML encoded	1 - APPRENTICE	Axel	Sí	LAS Parlieded 155 into a JavaScript seting with angle brookes HTML encoded >
Cross-site scripting	Stored XSS into HTML context with nothing encoded	1 - APPRENTICE	Alonso	Sí	LNA Stared XSS into HTML contact with nathing encoded > ▲ Stared XSS into HTML contact with nathing encoded >
Cross-site scripting	DOM XSS in document.write sink using source location.search	1 - APPRENTICE	David	Sí	(AB DOW/X55 in documents, sector sink soling season bocastion, exacts):
Cross-site scripting	DOM XSS in innerHTML sink using source location.search	1 - APPRENTICE	David	Sí	LAME CONTEST OF CONTEST ON STORY CONTEST ON STORY CONTEST CONT
Cross-site scripting		1 - APPRENTICE	Jaime	Sí	COU XSS in plumy window save although made using scenarios, executs storate in A Sound
Cross-site scripting		2 - PRACTITIONER	Axel	Sí	LANE Perfected Kitch into HTML cornect with most toge and attitudes blacked :
Cross-site scripting	Reflected XSS into HTML context with all tags blocked except custom one	2 - PRACTITIONER	Axel	Sí	UNB Perfected XSS into 1976L contact with all large blocked except content over > Solved
Cross-site scripting	Reflected XSS with some SVG markup allowed	2 - PRACTITIONER	Axel	Sí	LAB Parliaded XSS With some SVS markup allowed :
Cross-site scripting	Reflected XSS in canonical link tag	2 - PRACTITIONER	Axel	Sí	LAB Purfected XSS in committed finish tag ()
Cross-site scripting	Reflected XSS into a JavaScript string with single quote and backslash esc	2 - PRACTITIONER	Axel	Sí	LAB Purflued XSS into a JavaScript atring with single qualit and backstark except >
Cross-site scripting	Reflected XSS into a JavaScript string with angle brackets and double quo	2 - PRACTITIONER	Axel	Sí	Reflected XES into a JavaScript stong with angle brackles and double quotes HTML- exceeded and dingle-guates encaged >
Cross-site scripting	Stored XSS into onclick event with angle brackets and double quotes HTM		Alonso	Sí	Use 2 More 1955 this result is a word with range in truckets and drubble quates NTML-encoded and simple quates and devictions excepted in
Cross-site scripting	Reflected XSS into a template literal with angle brackets, single, double qu		Alonso	Sí	Refinision XXS from an inequilate literal with supple brackets, single, double quoties, bucketan's and bucklots Window excepted 1
Cross-site scripting		2 - PRACTITIONER	Alonso	Sí	(MA) Set to Comment. and the string National Least Line, research, fields a select decision of the string National Least Line, research, fields a select decision of the string National Least Line, research, fields a select decision of the string National Least Line, research, fields and select decision of the string National Least Line, research, fields and select decision of the string National Least Line, research, fields and select decision of the string National Least Line, research, fields and select decision of the string National Least Line, research, fields and select decision of the string National Least Line, research, fields and select decision of the string National Least Line, research, researc
Cross-site scripting	DOM XSS in AngularJS expression with angle brackets and double quotes	2 - PRACTITIONER	David	Sí	Minimized to Age and Annual residence and complete deviction and deviction person (Trial.  Account 1:
Cross-site scripting	Reflected DOM XSS	2 - PRACTITIONER	David	Sí	Managinatis : American
Cross-site scripting	Stored DOM XSS	2 - PRACTITIONER	David	Sí	(all how 104 OIL - g how
Cross-site scripting	Exploiting cross-site scripting to steal cookies	2 - PRACTITIONER	Brenda	Sí	Basado en: https://www.youtube.com/watch?v=zs1OsfL0z4o
Cross-site scripting	Exploiting cross-site scripting to capture passwords	2 - PRACTITIONER	Brenda	Sí	Basado en: https://www.youtube.com/watch?v=zs1osiLoz40  Basado en: https://www.youtube.com/watch?v=KA4Esd0tSPC
	Reflected XSS protected by CSP, with dangling markup attack	2 - PRACTITIONER	Alonso	Sí	A See ocupa una versión de paga
Cross-site scripting Cross-site scripting	Exploiting XSS to perform CSRF	2 - PRACTITIONER	Alonso	Sí	Se ocupa una version de paga
Cross-site scripting  Cross-site scripting	Reflected XSS with event handlers and href attributes blocked	3 - EXPERT	Axel	Sí	LAS Perfected Kids with event handless and save a stributes blocked :-
	Reflected ASS with event handlers and hier attributes blocked  Reflected XSS in a JavaScript URL with some characters blocked	3 - EXPERT	Rubí	Sí	(see Androit 2011 Audit 2014 Audi
Cross-site scripting	Reflected XSS with Angular JS sandbox escape without strings				
Cross-site scripting		3 - EXPERT	Oscar	Sí	
Cross-site scripting	Reflected XSS with AngularJS sandbox escape and CSP	3 - EXPERT	Tuz	Sí	
Cross-site scripting	Reflected XSS protected by very strict CSP, with dangling markup attack	3 - EXPERT	Aimeé	Sí	(UAD: Reflected 3555 protected by CSP, with dampling markup albeds.)
Cross-site scripting	Reflected XSS protected by CSP, with CSP bypass	3 - EXPERT	Alonso	Sí	[MA   Palmodel XSS protected by CSP, with CSP bytems in
Cross-site request forgery (CSRF)	CSRF vulnerability with no defenses	1 - APPRENTICE	Aimeé	Sí	(AB) CSS submitted with conditioned 1:
Cross-site request forgery (CSRF)	CSRF where token validation depends on request method	2 - PRACTITIONER	Edrey	Sí	LAS COT after State validation deposits as request reduct : A State of
Cross-site request forgery (CSRF)	CSRF where token validation depends on token being present	2 - PRACTITIONER	Edrey	Sí	LAG CSS share sales validation depends on taken being present > 6 Served
Cross-site request forgery (CSRF)	CSRF where token is not tied to user session	2 - PRACTITIONER	Brenda	Sí	Basado en: https://www.youtube.com/watch?v=JKwTX9wjeec
Cross-site request forgery (CSRF)		2 - PRACTITIONER	Jacob	Sí	USE CASE when their is fact to translation cooks >
Cross-site request forgery (CSRF)	CSRF where token is duplicated in cookie	2 - PRACTITIONER	Jacob	Sí	(AB) COSS where twice is displaced in cooks > A Grained
Cross-site request forgery (CSRF)	CSRF where Referer validation depends on header being present	2 - PRACTITIONER	Edrey	Sí	LSB CSBS where Stations understand depends on header being present ::
Cross-site request forgery (CSRF)	CSRF with broken Referer validation	2 - PRACTITIONER	Jacob	Sí	LAB CRY when Police randed on-depends on header larner proceed in
Clickjacking	Basic clickjacking with CSRF token protection	1 - APPRENTICE	Adrian	Sí	(AM) Then chilephology also CDDF delaw primedon > A Edward
Clickjacking	Clickjacking with form input data prefilled from a URL parameter	1 - APPRENTICE	Adrian	Sí	(Ma) Graphing with him to put aboyund action of the parameter -
Clickjacking	Clickjacking with a frame buster script	1 - APPRENTICE	Aimeé	Sí	Lid Citigating with a force books scopt in a Shored
Clickjacking		2 - PRACTITIONER	Adrian	Sí	(AM Control colouring university in tigger (1004 desert 100 )
Clickjacking		2 - PRACTITIONER	Adrian	Sí	(pt) (Addition (column))
DOM-based vulnerabilities		2 - PRACTITIONER	Adrian	Sí	(and 3100000 and nonlique ) A time
DOM-based vulnerabilities	DOM XSS using web messages and a JavaScript URL	2 - PRACTITIONER	Adrian	Sí	(CAE) COCCOS cords and an investigate and a land control PL >
DOM-based vulnerabilities	DOM XSS using web messages and JSON parse	2 - PRACTITIONER	Adrian	Sí	(AM DOUGH anywell remays and cores quarter 1
DOM-based vulnerabilities	DOM-based open redirection	2 - PRACTITIONER	Adrian	Sí	(M. State State State State )
DOM-based vulnerabilities	DOM-based cookie manipulation	2 - PRACTITIONER	Edrey	Sí	LAS DOW haved cooks manipulation > A Stored
DOM-based vulnerabilities	Exploiting DOM clobbering to enable XSS	3 - EXPERT	Adrian	Sí	(SEE Equitivy/2004 Accounty E-viride 1003 > ACCOUNT
DOM-based vulnerabilities	Clobbering DOM attributes to bypass HTML filters	3 - EXPERT	Edrey	Sí	MAI Clobbering DOM arribuses to bigues HTML Stees > g Stowed
Cross-origin resource sharing (CORS)	CORS vulnerability with basic origin reflection	1 - APPRENTICE	Magno	Sí	LAB CCRS schembley with basic origin reflection > A Solved
Cross-origin resource sharing (CORS)	CORS vulnerability with trusted null origin	1 - APPRENTICE	Kenneth	Sí	LAB. COPS wherebilly with tripled mill origin >
Cross-origin resource sharing (CORS)	CORS vulnerability with trusted insecure protocols	2 - PRACTITIONER	Aimeé	Sí	LAS COST Amendady will studed money publicals : A fined
Cross-origin resource sharing (CORS)  Cross-origin resource sharing (CORS)	CORS vulnerability with trusted insecure protocols  CORS vulnerability with internal network pivot attack	3 - EXPERT	Almee	Sí	Las COSS unequity with interest reference point strick 1:  A Name of the COSS unequity with interest reference point strick 1:  A Name of the COSS unequity with interest reference point strick 1:  A Name of the COSS unequity with interest reference point strick 1:
					Se ocupa una version de paga
XML external entity (XXE) injection  XML external entity (XXE) injection	Exploiting XXE using external entities to retrieve files Exploiting XXE to perform SSRF attacks	1 - APPRENTICE 1 - APPRENTICE	Calvin Calvin	Sí Sí	(LAB Equitory DE or perform 560° stocks : A Sound )
XML external entity (XXE) injection		2 - PRACTITIONER	Magno	Sí	LAB Bird XX with subcloted records >
XML external entity (XXE) injection XML external entity (XXE) injection	Blind XXE with out-of-band interaction Blind XXE with out-of-band interaction via XML parameter entities	2 - PRACTITIONER	Magno Magno	Sí	Use Elect XX with and-clear invention in A parameter ordina >
XML external entity (XXE) injection	Exploiting blind XXE to exfiltrate data using a malicious external DTD  Exploiting blind XXE to retrieve data via error messages	2 - PRACTITIONER	Magno	Sí	Expending bloot 100 is written a data verigi a relational relative verigi a relational relative verigi a relational relative verigi a relational verification of the data verification of the verification of
XML external entity (XXE) injection XML external entity (XXE) injection		2 - PRACTITIONER	Calvin	Sí	Library Text CCS in travel class as and reasonable >
		2 - PRACTITIONER 2 - PRACTITIONER	Calvin	Sí	Cas Eurory Oti vo insperie unas > Assess
XML external entity (XXE) injection	Exploiting XXE via image file upload Exploiting XXE to retrieve data by repurposing a local DTD		Calvin	Sí	Totals but in season early abstract a remain (1) Totals the season of th
XML external entity (XXE) injection Server-eide request forgery (SSRE)	Exploiting XXE to retrieve data by repurposing a local DTD  Basic SSRF against the local server	3 - EXPERT 1 - APPRENTICE	Calvin	Sí Sí	LAS Stock SSTF agrees the hoof server >
Server-side request forgery (SSRF)			Edrey		Like Box: 5507 agent the local server ()  Like Box: 5507 agent the local server ()  Like Box: 5507 agent the local server ()  A bloom
Server-side request forgery (SSRF)	Basic SSRF against another back-end system  SSRF with blocklist based input filter	1 - APPRENTICE	Magno	Sí	UB 500-507F agent earther book ord system >
Server-side request forgery (SSRF)	SSRF with blacklist-based input filter	2 - PRACTITIONER 2 - PRACTITIONER	Magno Magno	Sí Sí	LAB SSF with ther bypass via open refrector vulnerability >
Server-side request forgery (SSRF)	SSRF with filter bypass via open redirection vulnerability		-		
Server-side request forgery (SSRF)	Blind SSRF with out-of-band detection SSRF with whiteliet based input filter	2 - PRACTITIONER		Sí	(M) Seed SSE4 with suit of based detection in A Seeding (M)
Server-side request forgery (SSRF)	SSRF with whitelist-based input filter	3 - EXPERT	David	Sí	LAM Bird 5555 will Stellance equinous to
Server-side request forgery (SSRF)	Blind SSRF with Shellshock exploitation	3 - EXPERT	Magno	Sí	
HTTP request smuggling	OS command injection, simple case	1 - APPRENTICE	Kenneth	Sí	(AB) OS comment rejector, simple case >
HTTP request smuggling		2 - PRACTITIONER	Edrey	Sí	nt or response managempt, some call to (INTRODUCE)
HTTP request smuggling	HTTP request smuggling, basic TE.CL vulnerability	2 - PRACTITIONER	Tuz	Sí	Basado en: https://www.youtube.com/watch?v=mZW_Y-sZOJ
HTTP request smuggling		2 - PRACTITIONER	Edrey	Sí	LAB HTTP request shruggling, observabling the TE header > & brinket
HTTP request smuggling	HTTP request smuggling, confirming a CL.TE vulnerability via differential r		Kenneth	Sí	LAB httP request amuggling, confirming a CLTE valuesability risk differential responses >
				Sí	LAB HTTP request strucygling, confirming a TE.CL valvereability via differential responses >
HTTP request smuggling	Exploiting HTTP request smuggling to bypass front-end security controls,		Kenneth	Sí	Explaining HTTP request amongsting to bypass from end security controls, CL.TE withroughly :
HTTP request smuggling	Exploiting HTTP request smuggling to bypass front-end security controls,	2 - PRACTITIONER	Kenneth	Sí	Exploiting HTTP registed strangeling in types to fore end security currons, Till, CI, and Street in submittably :
		2 - PRACTITIONER	Kenneth	Sí	LABI Exploiting HTTP request smuggling to reveal frost-end request reverting >
HTTP request smuggling HTTP request smuggling HTTP request smuggling			Kenneth	Sí	LAB Exploiting HTTP request consigning to supraw other users' requests :
HTTP request smuggling HTTP request smuggling HTTP request smuggling HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests	2 - PRACTITIONER		1	
HTTP request smuggling HTTP request smuggling HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS	2 - PRACTITIONER 2 - PRACTITIONER	Aimeé	Sí	Ladi Colintry (10) research amoging to deliver reference (105 >
HTTP request smuggling HTTP request smuggling HTTP request smuggling HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS			Sí	Contry CTP-seat multiply bits inflanciols :
HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS	2 - PRACTITIONER	Aimeé		
HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS Blind OS command injection with time delays	2 - PRACTITIONER 2 - PRACTITIONER	Aimeé Emmanuel	Sí	Code Bind Cli command agestor-unit time adequ >
HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS Blind OS command injection with time delays Blind OS command injection with output redirection Blind OS command injection with output redirection	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER	Aimeé Emmanuel Emmanuel	Sí Sí	(as the Committee of the bays . A see
HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS Blind OS command injection with time delays Blind OS command injection with output redirection Blind OS command injection with out-for the interaction Blind OS command injection with out-for the interaction Blind OS command injection with out-of-band data exhibitation	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER	Aimeé Emmanuel Emmanuel Emmanuel Jacob	Sí Sí Sí	The contraction of the basis     The contraction of the basis     The contraction of the basis basis
HTTP request smuggling	Exoloiting HTTP request smuggling to reveal front-end request rewriting  Exploiting HTTP request smuggling to capture other users' requests  Exploiting HTTP request smuggling to deliver reflected XSS  Blind OS command injection with time delays  Blind OS command injection with output redirection  Blind OS command injection with output redirection  Blind OS command injection with out-of-band distraction  Blind OS command injection with out-of-band distraction  Exploiting HTTP request smuggling to perform web cache poisoning	2 - PRACTITIONER 3 - EXPERT	Aimeé Emmanuel Emmanuel Emmanuel Jacob Kenneth	Sí Sí Sí Sí	to the consect gather and to steps ( )  The consect gather and the defendance ( )  The consect gather and and defendance ( )  The consect gather and defendance ( )  The consect gather and and consect gather ( )  The consect gather and and consect gather ( )  The consect gather and and consect gather ( )  The
HTTP request smuggling	Exploiting HTTP request smuggling to reveal front-end request rewriting Exploiting HTTP request smuggling to capture other users' requests Exploiting HTTP request smuggling to deliver reflected XSS Blind OS command injection with time delays Blind OS command injection with output redirection Blind OS command injection with output redirection Blind OS command injection with out-of-band interaction Blind OS command injection with out-of-band interaction Blind OS command injection with out-of-band pate explication to Exploiting HTTP request smuggling to perform web cache poisoning Exploiting HTTP request smuggling to perform web cache deception	2 - PRACTITIONER 3 - EXPERT 3 - EXPERT	Aimeé Emmanuel Emmanuel Emmanuel Jacob Kenneth Jaime	Sí Sí Sí Sí Sí	The state of the s
HTTP request smuggling	Exoloiting HTTP request smuggling to reveal front-end request rewriting  Exploiting HTTP request smuggling to capture other users' requests  Exploiting HTTP request smuggling to deliver reflected XSS  Blind OS command injection with time delays  Blind OS command injection with output redirection  Blind OS command injection with output redirection  Blind OS command injection with out-of-band distraction  Blind OS command injection with out-of-band distraction  Exploiting HTTP request smuggling to perform web cache poisoning	2 - PRACTITIONER 3 - EXPERT	Aimeé Emmanuel Emmanuel Emmanuel Jacob Kenneth	Sí Sí Sí Sí	to the consect gather and to steps ( )  The consect gather and the defendance ( )  The consect gather and and defendance ( )  The consect gather and defendance ( )  The consect gather and and consect gather ( )  The consect gather and and consect gather ( )  The consect gather and and consect gather ( )  The

Server-side template injection						
	Server-side template injection in an unknown language with a documented	2 - PRACTITIONER	Ricardo	Sí	LAN Tener sub-template symbol or annother transpage with a documented explicit in	A total
Server-side template injection	Server-side template injection with information disclosure via user-supplie	2 - PRACTITIONER	Ricardo	Sí	CMS (Server distribution) and information describes as such expenses opens or	á SAN
Server-side template injection	Server-side template injection in a sandboxed environment	3 - EXPERT	Ricardo	Sí	LAB Server oldersmylate injection in a sandrowed environment is	A.C.
Server-side template injection	Server-side template injection with a custom exploit	3 - EXPERT	Aimeé	Sí	LAS Sever-old template injection with a custom exploit in	<u>a</u> Solved
Directory traversal	File path traversal, simple case	1 - APPRENTICE	Edrey	Sí	LAM File path traversal, simple case >-	& GOVERS
Directory traversal		2 - PRACTITIONER	Calvin	Sí	LAB   File path traversal, traversal sequences blocked with absolute path bypass >	∆ Solved
Directory traversal	File path traversal, traversal sequences stripped with superfluous URL-dec	2 - PRACTITIONER	Calvin	Sí	LAS File path towersal, towersal sequences stripped with superfusion URL-decode :-	à Street
Directory traversal	File path traversal, validation of start of path	2 - PRACTITIONER	Calvin	Sí	(A6) File path hoursel, validation of start of path (	& String
Directory traversal	File path traversal, validation of file extension with null byte bypass	2 - PRACTITIONER	Calvin	Sí	CAB File path towards, validation of the extension with null byte bypass >	å 50m3
Access control vulnerabilities	Unprotected admin functionality	1 - APPRENTICE	Jaime	Sí	LAB Unprotected admin functionality >	∆ Solves
Access control vulnerabilities	Unprotected admin functionality with unpredictable URL	1 - APPRENTICE	Jacob	Sí	Disposed admin functionally with urproduction UFL in	<u>&amp;</u> Street
Access control vulnerabilities	User role controlled by request parameter	1 - APPRENTICE	Jacob	Sí	LNE User sale controlled by required parameter >	<b>△</b> 20040
Access control vulnerabilities	User role can be modified in user profile	1 - APPRENTICE	Aimeé	Sí	(LAB   Uservole can be modified in user profile >	& Count
Access control vulnerabilities	User ID controlled by request parameter	1 - APPRENTICE	Rodrigo	Sí	Class Char III combolled by regard parameter >-	& Control
Access control vulnerabilities	User ID controlled by request parameter, with unpredictable user IDs	1 - APPRENTICE	Rodrigo	Sí	LAB User D controlled by request parameter, with unpredictable user IDs :-	∆ Salved )
Access control vulnerabilities	User ID controlled by request parameter with data leakage in redirect	1 - APPRENTICE	Rubí	Sí	LAM Dow III controlled by request parameter with data backage in restreet >	Dasado en. https://yodd.berniyoji i i qw
Access control vulnerabilities	User ID controlled by request parameter with password disclosure	1 - APPRENTICE	Oscar	Sí		Basado en: https://youtu.be/erLHrDmf2gE
Access control vulnerabilities	Insecure direct object references	1 - APPRENTICE	Emmanuel	Sí	LAB Involve dred digot elements >	∆ 50m3
Access control vulnerabilities	URL-based access control can be circumvented	2 - PRACTITIONER		Sí	_	A Count
Access control vulnerabilities	Method-based access control can be circumvented	2 - PRACTITIONER		Sí	(Minutesed access criticion te diconverted >	& Street
Access control vulnerabilities	Multi-step process with no access control on one step	2 - PRACTITIONER		Sí	LAG Multi-step process with no access control on one step ::	& Solved
Access control vulnerabilities	Referer-based access control	2 - PRACTITIONER		Sí	EAST Pethon Lased access cartral :-	≜ total
Authentication	Username enumeration via different responses	1 - APPRENTICE	Isaac	Sí	LAB Userame enumention via different responses >  LAB 3/A imple types >	& Gallery
Authentication	2FA simple bypass	1 - APPRENTICE	Isaac	Sí		\$ (************************************
Authentication	Password reset broken logic	1 - APPRENTICE	Isaac	Sí	LNR Passand seat trikes topic >	<u>A</u> those
Authentication	Username enumeration via subtly different responses	2 - PRACTITIONER		Sí	LANE Charterine enumeration via subtly different enganeses >	
Authentication	Username enumeration via response timing	2 - PRACTITIONER		Sí	LAS States bruse protection, 12 requires String >	
Authentication	Broken brute-force protection, IP block	2 - PRACTITIONER		Sí	CAR Denime enumeration in account text :	à total
Authentication	Username enumeration via account lock	2 - PRACTITIONER		Sí	Denima enumeration de account bux >  (34) 274 troden logic >	\$ (000)
Authentication Authentication	2FA broken logic Brute-forcing a stay-logged-in cookie	2 - PRACTITIONER 2 - PRACTITIONER		Sí Sí	LAS State-forcing a stary-logger-in cookie (i)	₫ Colored )
Authentication	Offline password cracking	2 - PRACTITIONER		Sí	LAS Office processed creating :	& Barrier
	Password reset poisoning via middleware	2 - PRACTITIONER		Sí		A TANK
Authentication Authentication	Password brute-force via password change	2 - PRACTITIONER		Sí	LAS Processistations in processistance is	& Street
Authentication	Broken brute-force protection, multiple credentials per request	3 - EXPERT	Isaac	Sí	LAS Broken trade-layou protection, multiple credentials per request :	& Street
Authentication	2FA bypass using a brute-force attack	3 - EXPERT	Isaac	Sí		<u>A</u> Soul
WebSockets	Manipulating WebSocket messages to exploit vulnerabilities	1 - APPRENTICE	Isaac	Sí	(AB) Manipulating Vhid Socket messages to exploit submedicities :	& Street
WebSockets	Manipulating the WebSocket handshake to exploit vulnerabilities	2 - PRACTITIONER		Sí	LAB Marquising the Published Nandandar In sepirit colorada (see	<u>a</u> (me)
WebSockets	Cross-site WebSocket hijacking	2 - PRACTITIONER		Sí	UAB Cross-allo WebSocket hjunking >	& Street
Web cache poisoning	Web cache poisoning with an unkeyed header	2 - PRACTITIONER		Sí	LAB Web-cache poliuring with an unkeyed header >	& Saland
Web cache poisoning	Web cache poisoning with an unkeyed cookie	2 - PRACTITIONER		Sí	LAB Visit-scrite processing with an unkeyed cooker in	& String
Web cache poisoning	Web cache poisoning with multiple headers	2 - PRACTITIONER		Sí	LES Visit such converse with multiple headers :	& Conet
Web cache poisoning	Targeted web cache poisoning using an unknown header	2 - PRACTITIONER		Sí	LAD Targeted web cache polisoning using an unknown header in	& SOUND
Web cache poisoning	Web cache poisoning via an unkeyed query string	2 - PRACTITIONER		Sí	LASE N/46 cuche palasning via an unknyed query string :	<b>≜</b> 50003
Web cache poisoning	Web cache poisoning via an unkeyed query parameter	2 - PRACTITIONER	Emmanuel	Sí	Data - Data cache pononing va.an-unitryed query parameter >	& Table 1
Web cache poisoning	Parameter cloaking	2 - PRACTITIONER		Sí	EXE Parameter counting :-	& nove
Web cache poisoning	Web cache poisoning via a fat GET request	2 - PRACTITIONER	Rodrigo	Sí	LAS This cache policoning via a fet CET request: >	▲ Sever
Web cache poisoning	URL normalization	2 - PRACTITIONER	Rodrigo	Sí	LAS USI normalization >:	à Sonot
Web cache poisoning	Web cache poisoning to exploit a DOM vulnerability via a cache with strict	3 - EXPERT	Rodrigo	Sí	Visit- seche processing to exploit a ECM valinerability viz a seche with other cacheals otheria:	∆ tolero
Web cache poisoning	Combining web cache poisoning vulnerabilities	3 - EXPERT	Ashwin	Sí	LAG Combining web cache policoring substrabilities >-	Se ocupa una versión de paga
Web cache poisoning	Cache key injection	3 - EXPERT	Emmanuel	Sí	LASE Cache key rejection >	∆ SOME
Web cache poisoning	Internal cache poisoning	3 - EXPERT	Ashwin	Sí	LAB Internal cache posoning >	Se ocupa una versión de paga
Insecure deserialization	Modifying serialized objects	1 - APPRENTICE	Emmanuel	Sí	LAR Modifies smallerd streets in	
Insecure deserialization	Modifying serialized data types	2 - PRACTITIONER	David			<u>á</u> Solved
Insecure deserialization	Using application functionality to exploit insecure deserialization			Sí	Mail Mail provided designs 1	A toni
Insecure deserialization		2 - PRACTITIONER	David	Sí	Land to distribute or state of the special state of	A 100 L
	Arbitrary object injection in PHP	2 - PRACTITIONER	David Rodrigo	Sí Sí	Last interpretation acque :  (Last interpretation function is experimented desirable > 1  (Last Addrey signal nightfore in PHP :	Anni
Insecure deserialization	Arbitrary object injection in PHP Exploiting Java deserialization with Apache Commons	2 - PRACTITIONER 2 - PRACTITIONER	David Rodrigo Rodrigo	Sí Sí Sí	Last provinces designs :  (48) Imaging policidor/scholarshy is report resource desertation :  (48) Addrey depth (rigidos is FEP ::  (48) Imaging desertation with Against Commerce ::	A min
Insecure deserialization Insecure deserialization	Arbitrary object injection in PHP Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain.	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime	Sí Sí Sí	Last Displaced Format Angels  (188 Strong specimen fordings is updat describ abundantier i  (188 Addary elgist produce in Pri Pri  (188 Displaced Strong Strong Angels Comments i  (188 Displaced Strong	
Insecure deserialization Insecure deserialization Insecure deserialization	Arbitrary object injection in PHP Exploiting, Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime Aimeé	Sí Sí Sí Sí	The second secon	And
Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization	Arbitrary object injection in PHP Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT	David Rodrigo Rodrigo Jaime Aimeé Tuz	Sí Sí Sí Sí Sí	The second	Basado en: https://www.youtube.com/watch?v=uaPrzydKdg
Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization	Arbitrary object injection in PHP Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac	\$i \$i \$i \$i \$i \$i \$i \$i	The special content of	A see Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization	Arbitrary object injection in PHP Exploiting Jawa deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Jawa deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deoloy a custom gadget chain	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac	\$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$	The second control of	Basado en: https://www.youtube.com/watch?v=uqPrrzydKdq
Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Information disclosure	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo	\$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$i \$	The second control of	Basado en: https://www.youtube.com/watch?v=uqPrrzydKdq
Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Insecure deserialization Information disclosure Information disclosure	Arbitrary object hiection in PHP Exploiting Java deserialization with Apache Commons Exploiting HPI deserialization with a pre-built padget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure on erebug page	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second secon	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure	Arbitrary object injection in PHP Exploiting, Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built padget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for PHP deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure on debug page Source code disclosure on debug page	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built paddet chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to dealow a custom gadget chain Information disclosure in error messages Information disclosure on debug page Source code disclosure via backup files Source code disclosure in formation disclosure	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE	David Rodrigo Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second secon	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure	Arbitrary object injection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for JAva deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain information disclosure in error messages information disclosure on debug page Source code disclosure via backup files Authentication bypass via information disclosure information disclosure in version control history	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo	Si S	The second management of the second management	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built paddet chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to dealow a custom gadget chain Information disclosure in error messages Information disclosure on debug page Source code disclosure via backup files Source code disclosure in formation disclosure	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE	David Rodrigo Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for PHP deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain information disclosure on debug page Information disclosure on debug page Source code disclosure with abellum files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo	Si S	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for PHP deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain information disclosure on debug page Information disclosure on debug page Source code disclosure with abellum files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho Chucho	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vunerabilities Business logic vunerabilities Business logic vunerabilities	Arbitrary object injection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built padget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for JAva deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain information disclosure in error messages information disclosure in debug page Source code disclosure wia backup files Authentication bypass via information disclosure information disclosure in version control history Excessive trust in client-side controls High-level logic vulnerability Inconsistent security controls	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE	David Rodrigo Rodrigo Jaime Almeé Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho Chucho Chucho	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities Business logic vulnerabilities Business logic vulnerabilities Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting Ruby deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deoloy a custom gadget chain Information disclosure in error messages Information disclosure in the state of the stat	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Chucho Chucho Chucho Chucho Chucho	Si Si Si Si Si Si Si Si Si Si Si Si Si S	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities	Arbitrary object hiection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in or messages Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls High-level logic underability Inconsistent security controls Flawed enforcement of business rules Lovel-evel logic flaw	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime Almeé Tuz Isaac Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$1 \$	The second control of	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities	Arbitrary object hiection in PHP Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with Apache Commons Exploiting PHP deserialization with a pre-built padget chain Exploiting Ruby deserialization using a documented padget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for Java deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in or messages Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls High-level logic vulnerability Unconsistent security controls Flaved enforcement of business rules Low-level logic flaw Inconsistent handling of exceptional input Weak isolation on dual-use endpoint Insufficient workflow validation	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$2 \$1 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to desloy a custom gadget chain Information disclosure in error messages Information disclosure in order messages Information disclosure in order messages Information disclosure in information disclosure Information disclosure in version control history Excessive trust in client-side controls I-iigh-level logic vulnerability Inconsistent security controls Flaved enforcement of business rules Lovel-evel logic flaw Inconsistent handling of exceptional input Weak isolation on dual-use endpoint Insufficient worktion validation Authentication bypass via flaved state machine	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 4 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built paddet chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in or messages Information disclosure on debug page Source code disclosure on debug page Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-aide controls High-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Low-level logic flaw Inconsistent handling of exceptional input Weak isolation on dual-use endopoint Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 3 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTITIONE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$1 \$1 \$1 \$2 \$1 \$2 \$1 \$2 \$1 \$2 \$1 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in abelug page Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in information disclosure Information disclosure in presion control history Excessive trust in client-side controls High-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Veak isolation on dual-use endpoint Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via encryption oracle	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 3 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTIT	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Chucho Chuch	\$1 \$1 \$2 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second material of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Business logic vulnerabilities	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting Nuby deserialization with a pre-built paddet chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to dealoy a custom gadget chain formation disclosure in error messages Information disclosure in the second deservation of the second disclosure in the second disclosure in formation disclosure in formation disclosure in formation disclosure in version control history Excessive trust in client-side controls High-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Usine Second disclosure in version disclosure Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via encryption oracle	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 2 - PRACTITIONER 3 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONER 6 - PRACTITIONER 6 - PRACTITIONER 7 - PRACTITIONER 8 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 1 - PRACTITIONER	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Chucho Aimeé Jaime	\$1 \$1 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITP Host header attacks	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built paddet chain Exploiting PHP deserialization using a documented gadget chain Developing a custom gadget chain for JAPA deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in orm cessages Information disclosure on debug page Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls Injuly-level logic vulnerability Inconsistent security controls Lawde enforcement of business rules Loy-level logic filaw Inconsistent handling of exceptional input Weak isolation on dual-use endopoint Insufficient workflow validation Authentication bypass via encryption oracle Basic password reset polsoning Host header authentication bypass	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 3 - PRACTITIONER 4 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONE	David Rodrigo Rodrigo Jaime Aimeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$1 \$1 \$1 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2	The second content of	Basado en https://www.youtube.com/watch?v=uqPrzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITP Host header attacks HITP Host header attacks	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in order messages Information disclosure in error messages Information disclosure in information disclosure Information disclosure in version control history Excessive trust in client-side controls Information disclosure in version control history Excessive trust in client-side controls Flawed enforcement of business rules Low-level logic flaw Inconsistent handling of exceptional input Weak isolation on dual-use endpoint Insufficient workflow validation Authentication bypass via Enawed state machine Infinite money logic flaw Authentication bypass via encryption oracle Basic password reset poisoning Host header authentication bypass	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 1 - PRACTITIONER 2 - PRACTITIONER 1 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - APPRENTICE 4 - APPRENTICE 4 - APPRENTICE 5 - APPRENTICE 6 - APPRENTICE 6 - APPRENTICE 6 - APPRENTICE 6 - APPRENTICE 7 - APPRENTICE 8 - APPRENTICE 8 - APPRENTICE 9 - APPRENT	David Rodrigo Rodrigo Jaime Almeé Tuz Isaac Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$2 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second control of	Basado en: https://www.youtube.com/watch?v=uaPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITP Host header attacks HITP Host header attacks HITP Host header attacks	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with a pre-built paddet chain Exploiting Ruby deserialization with a pre-built paddet chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP developing the publication observation of the publication o	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 3 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONER 7 - PR	David Rodrigo Rodrigo Jaime Almeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$1 \$1 \$1 \$2 \$1 \$2 \$1 \$2 \$1 \$2 \$1 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITTP Host header attacks HITTP Host header attacks HITTP Host header attacks HITTP Host header attacks	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built padget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in or messages Information disclosure in debug page Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls Ingh-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Inconsistent handling of exceptional input Weak isolation on dual-use endopoint Insufficient workflow validation Authentication bypass via encryption oracle Basic password reset polsoning Host header authentication bypass Web scache poisoning via ambiguous requests Routing-based SSRE SSRE via flawed request parsing	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 3 - APPRENTICE 4 - APPRENTICE 5 - PRACTITIONER	David Rodrigo Rodrigo Jaime Almeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho Chu	\$1 \$1 \$2 \$2 \$2 \$2 \$3 \$3 \$3 \$3 \$4 \$3 \$4 \$3 \$4 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITP Host header attacks	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting Ruby deserialization with a pre-built paddet chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deoloy a custom gadget chain fromation disclosure in corressages Information disclosure in corressages Information disclosure in the second disclosure Information disclosure in the second disclosure Information disclosure in version control history Excessive trust in client-side controls Flawder deforcement of business rules Love-level logic vulnerability Inconsistent and ling of exceptional input Weak isolation on dual-use endpoint Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via encryption oracle Basic password reset polsoning Host header authentication bypass Routing-based SSRE SSRF via flawed request parsing Password reset poisoning via dangling markup	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERITIONER 4 - EXPERITIONER 5	David Rodrigo Rodrigo Jaime Aimeé Truz Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2 \$2	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Business logic vulnerabilities Business logic vu	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built paddet chain Exploiting PHP deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to decloy a custom gadget chain Information disclosure in error messages Information disclosure on debug page Source code disclosure in the state of	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERTICE 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERTIONER 4 - EXPERTIONER 5	David Rodrigo Rodrigo Jaime Almeé Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Chucho C	\$1 \$1 \$2 \$2 \$2 \$3 \$3 \$3 \$4 \$3 \$4 \$3 \$4 \$3 \$4 \$3 \$4 \$3 \$4 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$4 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5 \$5	The second content of	Basado en https://www.youtube.com/watch?v=uqPrzydKdg
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITTP Host header attacks OAuth authentication OAuth authentication	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built added chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Developing a custom gadget chain for PHP deserialization Ising PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in order messages Information disclosure in explain to the second page of the second page Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls Isind-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Love-level logic flaw User and the security controls Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via encryption oracle Basic password reset poisoning Host header authentication bypass SNF via flawed request parsing Password reset poisoning via ambiguous requests Routing-based SSRE SNF via flawed request parsing Password reset poisoning via dangling markup Authentication bypass via OAuth implicit flow Forced OAuth profile linking	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 3 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITION	David Rodrigo Rodrigo Jaime Almeé Tuz Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities Business	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with a pre-built padget chain Exploiting Ruby deserialization with a pre-built padget chain Exploiting Ruby deserialization using a documented gadget chain Developing a custom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in the second padget chain Information disclosure in the second padget chain Information disclosure in the second padget chain Information disclosure in version control history Excessive trust in client-side controls High-level logic vulnerability Inconsistent security controls Elawed enforcement of business rules Lov-level logic flaw Unconsistent handling of exceptional input Weak isolation on dual-use endoont Insufficient workflow validation Authentication bypass via encryption practle Basic password reset poisoning Host header authentication bypass Web cache poisoning via ambiguous requests Routing-based SSRE SSRF via flawed request parsing Password reset poisoning via adagling markup Authentication bypass via Portific linking OAuth account hijacking via redirect_uri	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERITIONER 2 - PRACTITIONER 3 - EXPERITIONER 2 - PRACTITIONER 3 - EXPERITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONER 7 - PRACTITIONER 7 - PRACTITIONER 8 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERITIONER 3 - EXPERITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONER 7 - PRACTITIONER 7 - PRACTITIONER 9 - PRACTITION	David Rodrigo Rodrigo Jaime Rodrigo Jaime Tuz Isaae Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Ricardo Chucho	\$1 \$1 \$2 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities HITP Host header attacks OAUth authentication OAuth authentication OAuth authentication OAuth authentication	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ribby deserialization using a documented gadget chain Developing a usustom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in error messages Information disclosure in abelug page Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls High-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Unconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Weak isolation on dual-use endpoint Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via encryption oracle Basic password reset poisoning Password reset poisoning via ambiguous requests Routing-based SSRE SSRF via flawed request parsing Password reset poisoning via dangling markup Authentication bypass via OAUth implicit flow Forced OAuth profile linking OAuth account hijacking via redirect uni Stealing OAUth access tokens via an open redirect	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERT 3 - APPRENTICE 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - APPRENTICE 2 - PRACTITIONER 3 - EXPERT 4 - APPRENTICE 2 - PRACTITIONER 3 - EXPERT 4 - PRACTITIONER 3 - EXPERT 5 - PRACTITIONER 4 - PRACTITIONER 5 - PRACTITIONER	David Rodrigo Rodrigo Jaime Rodrigo Jaime Rodrigo Jaime Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho Ch	\$1 \$1 \$2 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq
Insecure deserialization Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Information disclosure Business logic vulnerabilities Business	Arbitrary object miection in PHP Exploiting Java deserialization with Apache Commons Exploiting Java deserialization with Apache Commons Exploiting PHP deserialization with a pre-built gadget chain Exploiting Ribby deserialization using a documented gadget chain Developing a usustom gadget chain for Java deserialization Developing a custom gadget chain for PHP deserialization Using PHAR deserialization to deploy a custom gadget chain Information disclosure in error messages Information disclosure in error messages Information disclosure in abelug page Source code disclosure via backup files Authentication bypass via information disclosure Information disclosure in version control history Excessive trust in client-side controls High-level logic vulnerability Inconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Unconsistent security controls Flawed enforcement of business rules Lov-level logic flaw Weak isolation on dual-use endpoint Insufficient workflow validation Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via flawed state machine Infinite money logic flaw Authentication bypass via encryption oracle Basic password reset poisoning Password reset poisoning via ambiguous requests Routing-based SSRE SSRF via flawed request parsing Password reset poisoning via dangling markup Authentication bypass via OAUth implicit flow Forced OAuth profile linking OAuth account hijacking via redirect uni Stealing OAUth access tokens via an open redirect	2 - PRACTITIONER 2 - PRACTITIONER 2 - PRACTITIONER 3 - EXPERT 3 - EXPERT 3 - EXPERT 3 - EXPERT 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERITIONER 2 - PRACTITIONER 3 - EXPERITIONER 2 - PRACTITIONER 3 - EXPERITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONER 7 - PRACTITIONER 7 - PRACTITIONER 8 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 9 - PRACTITIONER 1 - APPRENTICE 1 - APPRENTICE 2 - PRACTITIONER 3 - EXPERITIONER 3 - EXPERITIONER 4 - PRACTITIONER 5 - PRACTITIONER 5 - PRACTITIONER 6 - PRACTITIONER 7 - PRACTITIONER 7 - PRACTITIONER 9 - PRACTITION	David Rodrigo Rodrigo Jaime Rodrigo Jaime Rodrigo Jaime Tuz Isaac Isaac Ricardo Ricardo Ricardo Ricardo Ricardo Chucho Ch	\$1 \$1 \$2 \$2 \$2 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3 \$3	The second content of	Basado en: https://www.youtube.com/watch?v=uqPrzydKdq