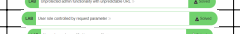
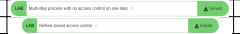
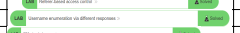
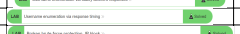
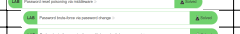
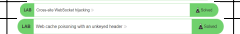
| Ataque | Nombre del Lab | Nivel | Encargado | Realizado | Captura del Lab | Comentarios |
|---|---|---|---|---|---|---|
| SQL injection | SQL injection vulnerability in WHERE clause allowing retrieval of hidden da | 1 - APPRENTICE | Oscar | Sí |  | |
| SQL injection | SQL injection vulnerability allowing login bypass | 1 - APPRENTICE | Rubí | Sí |  | |
| SQL injection | SQL injection UNION attack, determining the number of columns returned | 2 - PRACTITIONER | Alonso | Sí |  | |
| SQL injection | SQL injection UNION attack, finding a column containing text | 2 - PRACTITIONER | Alonso | Sí |  | |
| SQL injection | SQL injection UNION attack, retrieving data from other tables | 2 - PRACTITIONER | Oscar | Sí |  | |
| SQL injection | SQL injection UNION attack, retrieving multiple values in a single column | 2 - PRACTITIONER | Oscar | Sí |  | |
| SQL injection | SQL injection attack, querying the database type and version on Oracle | 2 - PRACTITIONER | Oscar | Sí |  | |
| SQL injection | SQL injection attack, querying the database type and version on MySQL an | 2 - PRACTITIONER | Oscar | Sí |  | |
| SQL injection | SQL injection attack, listing the database contents on non-Oracle database | 2 - PRACTITIONER | Oscar | Sí |  | |
| SQL injection | SQL injection attack, listing the database contents on Oracle | 2 - PRACTITIONER | Oscar | Sí |  | |
| SQL injection | Blind SQL injection with conditional responses | 2 - PRACTITIONER | Rubí | Sí |  | |
| SQL injection | Blind SQL injection with conditional errors | 2 - PRACTITIONER | Rubí | Sí |  | |
| SQL injection | Blind SQL injection with time delays | 2 - PRACTITIONER | Rubí | Sí |  | |
| SQL injection | Blind SQL injection with time delays and information retrieval | 2 - PRACTITIONER | Rubí | Sí |  | |
| SQL injection | Blind SQL injection with out-of-band interaction | 2 - PRACTITIONER | Rubí | Sí |  | |
| SQL injection | Blind SQL injection with out-of-band data exfiltration | 2 - PRACTITIONER | Rubí | Sí |  | |
| Cross-site scripting | Reflected XSS into HTML context with nothing encoded | 1 - APPRENTICE | Alonso | Sí |  | |
| 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 |  | |
| Cross-site scripting | Reflected XSS into a JavaScript string with angle brackets HTML encoded | 1 - APPRENTICE | Axel | Sí |  | |
| Cross-site scripting | Stored XSS into HTML context with nothing encoded | 1 - APPRENTICE | Alonso | Sí |  | |
| Cross-site scripting | DOM XSS in document.write sink using source location.search | 1 - APPRENTICE | David | Sí |  | |
| Cross-site scripting | DOM XSS in innerHTML sink using source location.search | 1 - APPRENTICE | David | Sí |  | |
| Cross-site scripting | DOM XSS in jQuery anchor href attribute sink using location.search source | 1 - APPRENTICE | Jaime | Sí |  | |
| Cross-site scripting | Reflected XSS into HTML context with most tags and attributes blocked | 2 - PRACTITIONER | Axel | Sí |  | |
| Cross-site scripting | Reflected XSS into HTML context with all tags blocked except custom one | 2 - PRACTITIONER | Axel | Sí |  | |
| Cross-site scripting | Reflected XSS with some SVG markup allowed | 2 - PRACTITIONER | Axel | Sí |  | |
| Cross-site scripting | Reflected XSS in canonical link tag | 2 - PRACTITIONER | Axel | Sí |  | |
| Cross-site scripting | Reflected XSS into a JavaScript string with single quote and backslash es | 2 - PRACTITIONER | Axel | Sí |  | |
| Cross-site scripting | Reflected XSS into a JavaScript string with angle brackets and double quo | 2 - PRACTITIONER | Axel | Sí |  | |
| Cross-site scripting | Stored XSS into onclick event with angle brackets and double quotes HTM | 2 - PRACTITIONER | Alonso | Sí |  | |
| Cross-site scripting | Reflected XSS into a template literal with angle brackets, single, double qu | 2 - PRACTITIONER | Alonso | Sí |  | |
| Cross-site scripting | DOM XSS in document.write sink using source location.search inside a se | 2 - PRACTITIONER | Alonso | Sí |  | |
| Cross-site scripting | DOM XSS in AngularJS expression with angle brackets and double quotes | 2 - PRACTITIONER | David | Sí |  | |
| Cross-site scripting | Reflected DOM XSS | 2 - PRACTITIONER | David | Sí |  | |
| Cross-site scripting | Stored DOM XSS | 2 - PRACTITIONER | David | Sí |  | |
| 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=KA4Esd0tSPQ |
| Cross-site scripting | Reflected XSS protected by CSP, with dangling markup attack | 2 - PRACTITIONER | Alonso | Sí |  | Se ocupa una versión de paga |
| Cross-site scripting | Exploiting XSS to perform CSRF | 2 - PRACTITIONER | Alonso | Sí |  | |
| Cross-site scripting | Reflected XSS with event handlers and href attributes blocked | 3 - EXPERT | Axel | Sí |  | |
| Cross-site scripting | Reflected XSS in a JavaScript URL with some characters blocked | 3 - EXPERT | Rubí | Sí |  | Basado en: https://youtu.be/1PowdKzFYYA |
| Cross-site scripting | Reflected XSS with AngularJS sandbox escape without strings | 3 - EXPERT | Oscar | Sí |  | Basado en: https://youtu.be/niUiUTuBJxQ |
| Cross-site scripting | Reflected XSS with AngularJS sandbox escape and CSP | 3 - EXPERT | Tuz | Sí |  | Basado en: https://www.youtube.com/watch?v=K6gll9Ru_Pw |
| Cross-site scripting | Reflected XSS protected by very strict CSP, with dangling markup attack | 3 - EXPERT | Aimeé | Sí |  | |
| Cross-site scripting | Reflected XSS protected by CSP, with CSP bypass | 3 - EXPERT | Alonso | Sí |  | |
| Cross-site request forgery (CSRF) | CSRF vulnerability with no defenses | 1 - APPRENTICE | Aimeé | Sí |  | |
| Cross-site request forgery (CSRF) | CSRF where token validation depends on request method | 2 - PRACTITIONER | Edrey | Sí |  | |
| Cross-site request forgery (CSRF) | CSRF where token validation depends on token being present | 2 - PRACTITIONER | Edrey | Sí |  | |
| 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) | CSRF where token is tied to non-session cookie | 2 - PRACTITIONER | Jacob | Sí |  | |
| Cross-site request forgery (CSRF) | CSRF where token is duplicated in cookie | 2 - PRACTITIONER | Jacob | Sí |  | |
| Cross-site request forgery (CSRF) | CSRF where Referer validation depends on header being present | 2 - PRACTITIONER | Edrey | Sí |  | |
| Cross-site request forgery (CSRF) | CSRF with broken Referer validation | 2 - PRACTITIONER | Jacob | Sí |  | |
| Clickjacking | Basic clickjacking with CSRF token protection | 1 - APPRENTICE | Adrian | Sí |  | |
| Clickjacking | Clickjacking with form input data prefilled from a URL parameter | 1 - APPRENTICE | Adrian | Sí |  | |
| Clickjacking | Clickjacking with a frame buster script | 1 - APPRENTICE | Aimeé | Sí |  | |
| Clickjacking | Exploiting clickjacking vulnerability to trigger DOM-based XSS | 2 - PRACTITIONER | Adrian | Sí |  | |
| Clickjacking | Multistep clickjacking | 2 - PRACTITIONER | Adrian | Sí |  | |
| DOM-based vulnerabilities | DOM XSS using web messages | 2 - PRACTITIONER | Adrian | Sí |  | |
| DOM-based vulnerabilities | DOM XSS using web messages and a JavaScript URL | 2 - PRACTITIONER | Adrian | Sí |  | |
| DOM-based vulnerabilities | DOM XSS using web messages and JSON.parse | 2 - PRACTITIONER | Adrian | Sí |  | |
| DOM-based vulnerabilities | DOM-based open redirection | 2 - PRACTITIONER | Adrian | Sí |  | |
| DOM-based vulnerabilities | DOM-based cookie manipulation | 2 - PRACTITIONER | Edrey | Sí |  | |
| DOM-based vulnerabilities | Exploiting DOM clobbering to enable XSS | 3 - EXPERT | Adrian | Sí |  | |
| DOM-based vulnerabilities | Clobbering DOM attributes to bypass HTML filters | 3 - EXPERT | Edrey | Sí |  | |
| Cross-origin resource sharing (CORS) | CORS vulnerability with basic origin reflection | 1 - APPRENTICE | Magno | Sí |  | |
| Cross-origin resource sharing (CORS) | CORS vulnerability with trusted null origin | 1 - APPRENTICE | Kenneth | Sí |  | |
| Cross-origin resource sharing (CORS) | CORS vulnerability with trusted insecure protocols | 2 - PRACTITIONER | Aimeé | Sí |  | |
| Cross-origin resource sharing (CORS) | CORS vulnerability with internal network pivot attack | 3 - EXPERT | Alonso | Sí |  | Se ocupa una versión de paga |
| XML external entity (XXE) injection | Exploiting XXE using external entities to retrieve files | 1 - APPRENTICE | Calvin | Sí |  | |
| XML external entity (XXE) injection | Exploiting XXE to perform SSRF attacks | 1 - APPRENTICE | Calvin | Sí |  | |
| XML external entity (XXE) injection | Blind XXE with out-of-band interaction | 2 - PRACTITIONER | Magno | Sí |  | |
| XML external entity (XXE) injection | Blind XXE with out-of-band interaction via XML parameter entities | 2 - PRACTITIONER | Magno | Sí |  | |
| XML external entity (XXE) injection | Exploiting blind XXE to exfiltrate data using a malicious external DTD | 2 - PRACTITIONER | Magno | Sí |  | |
| XML external entity (XXE) injection | Exploiting blind XXE to retrieve data via error messages | 2 - PRACTITIONER | Calvin | Sí |  | |
| XML external entity (XXE) injection | Exploiting XInclude to retrieve files | 2 - PRACTITIONER | Calvin | Sí |  | |
| XML external entity (XXE) injection | Exploiting XXE via image file upload | 2 - PRACTITIONER | Calvin | Sí |  | |
| XML external entity (XXE) injection | Exploiting XXE to retrieve data by repurposing a local DTD | 3 - EXPERT | Calvin | Sí |  | |
| Server-side request forgery (SSRF) | Basic SSRF against the local server | 1 - APPRENTICE | Edrey | Sí |  | |
| Server-side request forgery (SSRF) | Basic SSRF against another back-end system | 1 - APPRENTICE | Magno | Sí |  | |
| Server-side request forgery (SSRF) | SSRF with blacklist-based input filter | 2 - PRACTITIONER | Magno | Sí |  | |
| Server-side request forgery (SSRF) | SSRF with filter bypass via open redirection vulnerability | 2 - PRACTITIONER | Magno | Sí |  | |
| Server-side request forgery (SSRF) | Blind SSRF with out-of-band detection | 2 - PRACTITIONER | Magno | Sí |  | |
| Server-side request forgery (SSRF) | SSRF with whitelist-based input filter | 3 - EXPERT | David | Sí |  | |
| 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 |  | |
| HTTP request smuggling | HTTP request smuggling, basic CL.TE vulnerability | 2 - PRACTITIONER | Edrey | Sí |  | |
| HTTP request smuggling | HTTP request smuggling, basic TE.CL vulnerability | 2 - PRACTITIONER | Tuz | Sí |  | Basado en: https://www.youtube.com/watch?v=mZW_Y-sZOJk |
| HTTP request smuggling | HTTP request smuggling, obfuscating the TE header | 2 - PRACTITIONER | Edrey | Sí |  | |
| HTTP request smuggling | HTTP request smuggling, confirming a CL.TE vulnerability via differential r | 2 - PRACTITIONER | Kenneth | Sí |  | |
| HTTP request smuggling | HTTP request smuggling, confirming a TE.CL vulnerability via differential r | 2 - PRACTITIONER | Kenneth | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to bypass front-end security controls, | 2 - PRACTITIONER | Kenneth | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to bypass front-end security controls, | 2 - PRACTITIONER | Kenneth | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to reveal front-end request rewriting | 2 - PRACTITIONER | Kenneth | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to capture other users' requests | 2 - PRACTITIONER | Kenneth | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to deliver reflected XSS | 2 - PRACTITIONER | Aimeé | Sí |  | |
| HTTP request smuggling | Blind OS command injection with time delays | 2 - PRACTITIONER | Emmanuel | Sí |  | |
| HTTP request smuggling | Blind OS command injection with output redirection | 2 - PRACTITIONER | Emmanuel | Sí |  | |
| HTTP request smuggling | Blind OS command injection with out-of-band interaction | 2 - PRACTITIONER | Emmanuel | Sí |  | |
| HTTP request smuggling | Blind OS command injection with out-of-band data exfiltration | 2 - PRACTITIONER | Jacob | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to perform web cache poisoning | 3 - EXPERT | Kenneth | Sí |  | |
| HTTP request smuggling | Exploiting HTTP request smuggling to perform web cache deception | 3 - EXPERT | Jaime | Sí |  | |
| Server-side template injection | Basic server-side template injection | 2 - PRACTITIONER | Ricardo | Sí |  | |
| Server-side template injection | Basic server-side template injection (code context) | 2 - PRACTITIONER | Ricardo | Sí |  | |
| Server-side template injection | Server-side template injection using documentation | 2 - PRACTITIONER | Ricardo | Sí |  | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Server-side template injection | Server-side template injection in an unknown language with a documented | 2 - PRACTITIONER | Ricardo | Sí |  | |
| Server-side template injection | Server-side template injection with information disclosure via user-supplie | 2 - PRACTITIONER | Ricardo | Sí |  | |
| Server-side template injection | Server-side template injection in a sandboxed environment | 3 - EXPERT | Ricardo | Sí |  | |
| Server-side template injection | Server-side template injection with a custom exploit | 3 - EXPERT | Aimeé | Sí |  | |
| Directory traversal | File path traversal, simple case | 1 - APPRENTICE | Edrey | Sí |  | |
| Directory traversal | File path traversal, traversal sequences blocked with absolute path bypass | 2 - PRACTITIONER | Calvin | Sí |  | |
| Directory traversal | File path traversal, traversal sequences stripped with superfluous URL-dec | 2 - PRACTITIONER | Calvin | Sí |  | |
| Directory traversal | File path traversal, validation of start of path | 2 - PRACTITIONER | Calvin | Sí |  | |
| Directory traversal | File path traversal, validation of file extension with null byte bypass | 2 - PRACTITIONER | Calvin | Sí |  | |
| Access control vulnerabilities | Unprotected admin functionality | 1 - APPRENTICE | Jaime | Sí |  | |
| Access control vulnerabilities | Unprotected admin functionality with unpredictable URL | 1 - APPRENTICE | Jacob | Sí |  | |
| Access control vulnerabilities | User role controlled by request parameter | 1 - APPRENTICE | Jacob | Sí |  | |
| Access control vulnerabilities | User role can be modified in user profile | 1 - APPRENTICE | Aimeé | Sí |  | |
| Access control vulnerabilities | User ID controlled by request parameter | 1 - APPRENTICE | Rodrigo | Sí |  | |
| Access control vulnerabilities | User ID controlled by request parameter, with unpredictable user IDs | 1 - APPRENTICE | Rodrigo | Sí |  | |
| Access control vulnerabilities | User ID controlled by request parameter with data leakage in redirect | 1 - APPRENTICE | Rubí | Sí |  | Basado en: https://youtu.be/nrlv0iHYFqM. |
| Access control vulnerabilities | User ID controlled by request parameter with password disclosure | 1 - APPRENTICE | Oscar | Sí |  | Basado en: https://youtu.be/erLHrDmf2qE. |
| Access control vulnerabilities | Insecure direct object references | 1 - APPRENTICE | Emmanuel | Sí |  | |
| Access control vulnerabilities | URL-based access control can be circumvented | 2 - PRACTITIONER | David | Sí |  | |
| Access control vulnerabilities | Method-based access control can be circumvented | 2 - PRACTITIONER | Rodrigo | Sí |  | |
| Access control vulnerabilities | Multi-step process with no access control on one step | 2 - PRACTITIONER | Jaime | Sí |  | |
| Access control vulnerabilities | Referer-based access control | 2 - PRACTITIONER | Jaime | Sí |  | |
| Authentication | Username enumeration via different responses | 1 - APPRENTICE | Isaac | Sí |  | |
| Authentication | 2FA simple bypass | 1 - APPRENTICE | Isaac | Sí |  | |
| Authentication | Password reset broken logic | 1 - APPRENTICE | Isaac | Sí |  | |
| Authentication | Username enumeration via subtly different responses | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Username enumeration via response timing | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Broken brute-force protection, IP block | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Username enumeration via account lock | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | 2FA broken logic | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Brute-forcing a stay-logged-in cookie | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Offline password cracking | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Password reset poisoning via middleware | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Password brute-force via password change | 2 - PRACTITIONER | Isaac | Sí |  | |
| Authentication | Broken brute-force protection, multiple credentials per request | 3 - EXPERT | Isaac | Sí |  | |
| Authentication | 2FA bypass using a brute-force attack | 3 - EXPERT | Isaac | Sí |  | |
| WebSockets | Manipulating WebSocket messages to exploit vulnerabilities | 1 - APPRENTICE | Isaac | Sí |  | |
| WebSockets | Manipulating the WebSocket handshake to exploit vulnerabilities | 2 - PRACTITIONER | Isaac | Sí |  | |
| WebSockets | Cross-site WebSocket hijacking | 2 - PRACTITIONER | Isaac | Sí |  | |
| Web cache poisoning | Web cache poisoning with an unkeyed header | 2 - PRACTITIONER | Jaime | Sí |  | |
| Web cache poisoning | Web cache poisoning with an unkeyed cookie | 2 - PRACTITIONER | Emmanuel | Sí |  | |
| Web cache poisoning | Web cache poisoning with multiple headers | 2 - PRACTITIONER | Aimeé | Sí |  | |
| Web cache poisoning | Targeted web cache poisoning using an unknown header | 2 - PRACTITIONER | Jaime | Sí |  | |
| Web cache poisoning | Web cache poisoning via an unkeyed query string | 2 - PRACTITIONER | Emmanuel | Sí |  | |
| Web cache poisoning | Web cache poisoning via an unkeyed query parameter | 2 - PRACTITIONER | Emmanuel | Sí |  | |
| Web cache poisoning | Parameter cloaking | 2 - PRACTITIONER | Rodrigo | Sí |  | |
| Web cache poisoning | Web cache poisoning via a fat GET request | 2 - PRACTITIONER | Rodrigo | Sí |  | |
| Web cache poisoning | URL normalization | 2 - PRACTITIONER | Rodrigo | Sí |  | |
| Web cache poisoning | Web cache poisoning to exploit a DOM vulnerability via a cache with strict | 3 - EXPERT | Rodrigo | Sí |  | |
| Web cache poisoning | Combining web cache poisoning vulnerabilities | 3 - EXPERT | Ashwin | Sí |  | Se ocupa una versión de paga |
| Web cache poisoning | Cache key injection | 3 - EXPERT | Emmanuel | Sí |  | |
| Web cache poisoning | Internal cache poisoning | 3 - EXPERT | Ashwin | Sí |  | Se ocupa una versión de paga |
| Insecure deserialization | Modifying serialized objects | 1 - APPRENTICE | Emmanuel | Sí |  | |
| Insecure deserialization | Modifying serialized data types | 2 - PRACTITIONER | David | Sí |  | |
| Insecure deserialization | Using application functionality to exploit insecure deserialization | 2 - PRACTITIONER | David | Sí |  | |
| Insecure deserialization | Arbitrary object injection in PHP | 2 - PRACTITIONER | Rodrigo | Sí |  | |
| Insecure deserialization | Exploiting Java deserialization with Apache Commons | 2 - PRACTITIONER | Rodrigo | Sí |  | |
| Insecure deserialization | Exploiting PHP deserialization with a pre-built gadget chain | 2 - PRACTITIONER | Jaime | Sí |  | |
| Insecure deserialization | Exploiting Ruby deserialization using a documented gadget chain | 2 - PRACTITIONER | Aimeé | Sí |  | |
| Insecure deserialization | Developing a custom gadget chain for Java deserialization | 3 - EXPERT | Tuz | Sí |  | Basado en: https://www.youtube.com/watch?v=uqPrrzydKdg |
| Insecure deserialization | Developing a custom gadget chain for PHP deserialization | 3 - EXPERT | Isaac | Sí |  | |
| Insecure deserialization | Using PHAR deserialization to deploy a custom gadget chain | 3 - EXPERT | Isaac | Sí |  | |
| Information disclosure | Information disclosure in error messages | 1 - APPRENTICE | Ricardo | Sí |  | |
| Information disclosure | Information disclosure on debug page | 1 - APPRENTICE | Ricardo | Sí |  | |
| Information disclosure | Source code disclosure via backup files | 1 - APPRENTICE | Ricardo | Sí |  | |
| Information disclosure | Authentication bypass via information disclosure | 1 - APPRENTICE | Ricardo | Sí |  | |
| Information disclosure | Information disclosure in version control history | 2 - PRACTITIONER | Ricardo | Sí |  | |
| Business logic vulnerabilities | Excessive trust in client-side controls | 1 - APPRENTICE | Chucho | Sí |  | |
| Business logic vulnerabilities | High-level logic vulnerability | 1 - APPRENTICE | Chucho | Sí |  | |
| Business logic vulnerabilities | Inconsistent security controls | 1 - APPRENTICE | Chucho | Sí |  | |
| Business logic vulnerabilities | Flawed enforcement of business rules | 1 - APPRENTICE | Chucho | Sí |  | |
| Business logic vulnerabilities | Low-level logic flaw | 2 - PRACTITIONER | Chucho | Sí |  | |
| Business logic vulnerabilities | Inconsistent handling of exceptional input | 2 - PRACTITIONER | Chucho | Sí |  | |
| Business logic vulnerabilities | Weak isolation on dual-use endpoint | 2 - PRACTITIONER | Chucho | Sí |  | |
| Business logic vulnerabilities | Insufficient workflow validation | 2 - PRACTITIONER | Chucho | Sí |  | |
| Business logic vulnerabilities | Authentication bypass via flawed state machine | 2 - PRACTITIONER | Chucho | Sí |  | |
| Business logic vulnerabilities | Infinite money logic flaw | 2 - PRACTITIONER | Aimeé | Sí |  | |
| Business logic vulnerabilities | Authentication bypass via encryption oracle | 2 - PRACTITIONER | Jaime | Sí |  | |
| HTTP Host header attacks | Basic password reset poisoning | 1 - APPRENTICE | Chucho | Sí |  | |
| HTTP Host header attacks | Host header authentication bypass | 1 - APPRENTICE | Chucho | Sí |  | |
| HTTP Host header attacks | Web cache poisoning via ambiguous requests | 2 - PRACTITIONER | Chucho | Sí |  | |
| HTTP Host header attacks | Routing-based SSRF | 2 - PRACTITIONER | Chucho | Sí |  | |
| HTTP Host header attacks | SSRF via flawed request parsing | 2 - PRACTITIONER | Aimeé | Sí |  | |
| HTTP Host header attacks | Password reset poisoning via dangling markup | 3 - EXPERT | Chucho | Sí |  | |
| OAuth authentication | Authentication bypass via OAuth implicit flow | 1 - APPRENTICE | Chucho | Sí |  | |
| OAuth authentication | Forced OAuth profile linking | 2 - PRACTITIONER | Chucho | Sí |  | |
| OAuth authentication | OAuth account hijacking via redirect_uri | 2 - PRACTITIONER | Jacob | Sí |  | |
| OAuth authentication | Stealing OAuth access tokens via an open redirect | 2 - PRACTITIONER | Jacob | Sí |  | |
| OAuth authentication | SSRF via OpenID dynamic client registration | 2 - PRACTITIONER | Aimeé | Sí |  | |
| OAuth authentication | Stealing OAuth access tokens via a proxy page | 3 - EXPERT | Jacob | Sí |  | |