JUMIA.CO.KE

Technologies	Vulnerability ID	Severity Score	Explanation
Ruby on Rails	CVE-2017-17920 SQL injection vulnerability in the 'reorder' method in Ruby on Rails 5.1.4 and earlier allows remote attackers to execute arbitrary SQL commands via the 'name' parameter.	8.1 (HIGH)	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data.
	CVE-2017-17919 SQL injection vulnerability in the 'order' method in Ruby on Rails 5.1.4 and earlier allows remote attackers to execute arbitrary SQL commands via the 'id desc' parameter.	8.1 (HIGH)	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could

			modify the intended SQL command when it is sent to a downstream component. Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data.
	CVE-2013-0333 lib/active_support/json/backends/yaml.rb in Ruby on Rails 2.3.x before 2.3.16 and 3.0.x before 3.0.20 does not properly convert JSON data to YAML data for processing by a YAML parser, which allows remote attackers to execute arbitrary code, conduct SQL injection attacks, or bypass authentication via crafted data that triggers unsafe decoding, a different vulnerability than CVE-2013-0156.		Ruby on Rails JSON Processor YAML exploit/multi/http/rails_json_yaml_code_exec This module exploits a remote code execution vulnerability in the JSON request processor of the Ruby on Rails application framework. This vulnerability allows an attacker to instantiate a remote object, which in turn can be used to execute any ruby code remotely in. Ruby on Rails JSON Processor YAML Deserialization Scanner auxiliary/scanner/http/rails_json_yaml_scanner This module attempts to identify Ruby on Rails instances vulnerable to an arbitrary object instantiation flaw in the JSON request processor.

	CVE-2020-11023 In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	6.9 (MEDIUM)	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
jQuery 1.8.1	CVE-2020-11022 In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	6.9 (MEDIUM)	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

	CVE-2012-6708 jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.	6.1 (MEDIUM)	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
Apache 2.4	CVE-2024-40898 SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious	9.1 (HIGH)	CWE-918 Server-Side Request Forgery (SSRF) The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

	requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.		
	CVE-2023-25690 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request	9.8 (HIGH)	CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') The product acts as an intermediary HTTP agent (such as a proxy or firewall) in the data flow between two entities such as a client and server, but it does not interpret malformed HTTP requests or responses in ways that are consistent with how the messages will be processed by those entities that are at the ultimate destination.

	CVE-2022-36760 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.	9.0 (HIGH)	CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') The product acts as an intermediary HTTP agent (such as a proxy or firewall) in the data flow between two entities such as a client and server, but it does not interpret malformed HTTP requests or responses in ways that are consistent with how the messages will be processed by those entities that are at the ultimate destination.