**IIS:**

|  |  |
| --- | --- |
| Vulnerabilidad CWE | Rule |
| CWE-117: Improper Output Neutralization for Logs | [Logging should not be vulnerable to injection attacks](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=javasecurity%3AS5145&rule_key=javasecurity%3AS5145) |
| CWE-22: Improper limitation of a pathname to a restricted directory ('path traversal') | [Accessing files should not lead to filesystem oracle attacks](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=javasecurity%3AS6549&rule_key=javasecurity%3AS6549)  [Extracting archives should not lead to zip slip vulnerabilities](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=javasecurity%3AS6096&rule_key=javasecurity%3AS6096)  [I/O function calls should not be vulnerable to path injection attacks](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=javasecurity%3AS2083&rule_key=javasecurity%3AS2083) |
| CWE-209: Information Exposure through an Error Message |  |
| CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | [Database queries should not be vulnerable to injection attacks](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=javasecurity%3AS3649&rule_key=javasecurity%3AS3649) |
| CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | [OS commands should not be vulnerable to command injection attacks](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=javasecurity%3AS2076&rule_key=javasecurity%3AS2076) |
| CWE-120: Classic Buffer Overflow |  |

**GRA:**

|  |  |
| --- | --- |
| Vulnerabilidad CWE | Rule |
| CWE-404: Improper Resource Shutdown or Release |  |
| CWE-434: Unrestricted Upload of File with Dangerous Type |  |
| CWE-770. Allocation of resources without limits or throttling |  |
| CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |  |
| CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) |  |
| CWE-319: Cleartext Transmission of Sensitive Information |  |
| CWE-307: Improper Restriction of Excessive Authentication Attempts |  |
| CWE-327: Use of a Broken or Risky Cryptographic Algorithm | [Cipher algorithms should be robust](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS5547&rule_key=java%3AS5547)  [Cipher Block Chaining IVs should be unpredictable](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS3329&rule_key=java%3AS3329)  [Encryption algorithms should be used with secure mode and padding scheme](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS5542&rule_key=java%3AS5542)  [Weak SSL/TLS protocols should not be used](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS4423&rule_key=java%3AS4423) |
| CWE-328: Reversible One-Way Hash |  |

**SP:**

|  |  |
| --- | --- |
| Vulnerabilidad CWE | Rule |
| CWE-732: Incorrect Permission Assignment for Critical Resource |  |
| CWE-285: Improper Authorization | ["HttpSecurity" URL patterns should be correctly ordered](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS4601&rule_key=java%3AS4601)  [Authorizations should be based on strong decisions](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS5808&rule_key=java%3AS5808) |
| CWE-272: Least privilege violation |  |
| CWE-807: Reliance on Untrusted Inputs in a Security Decision | ["HttpServletRequest.getRequestedSessionId()" should not be used](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS2254&rule_key=java%3AS2254) |
| CWE-798: Use of Hard-coded Credentials | [Credentials should not be hard-coded](https://sonarcloud.io/organizations/oscarardaizunavarra/rules?open=java%3AS6437&rule_key=java%3AS6437) |
| CWE-306: Missing Authentication for Critical Function |  |

**LINKS:**

* Corregido: https://sonarcloud.io/project/overview?id=eduardoezponda\_highscorescorregido
* Vulnerabilidades: https://sonarcloud.io/summary/overall?id=eduardoezponda\_vulnerabilities