IIS:

Vulnerabilidad CWE	Rule
CWE-117: Improper Output Neutralization for Logs	Logging should not be vulnerable to injection attacks
CWE-22: Improper limitation of a pathname to a restricted directory ('path traversal')	Accessing files should not lead to filesystem oracle attacks Extracting archives should not lead to zip slip vulnerabilities I/O function calls should not be vulnerable to path injection attacks
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
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
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 Cipher Block Chaining IVs should be unpredictable Encryption algorithms should be used with secure mode and padding scheme Weak SSL/TLS protocols should not be used
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 Authorizations should be based on strong decisions
CWE-272: Least privilege violation	
CWE-807: Reliance on Untrusted Inputs in a Security Decision	"HttpServletRequest.getRequestedSessionId()" should not be used
CWE-798: Use of Hard-coded Credentials	Credentials should not be hard-coded
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