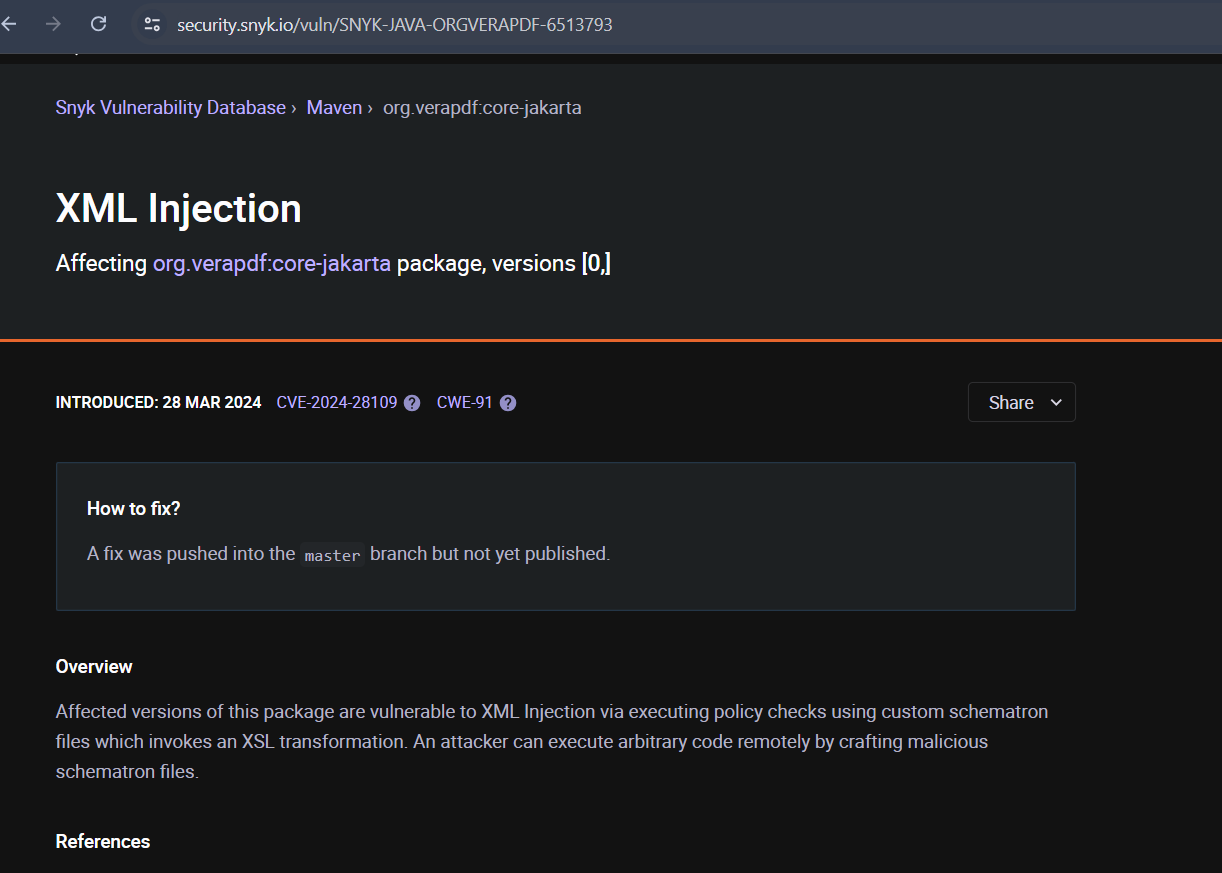
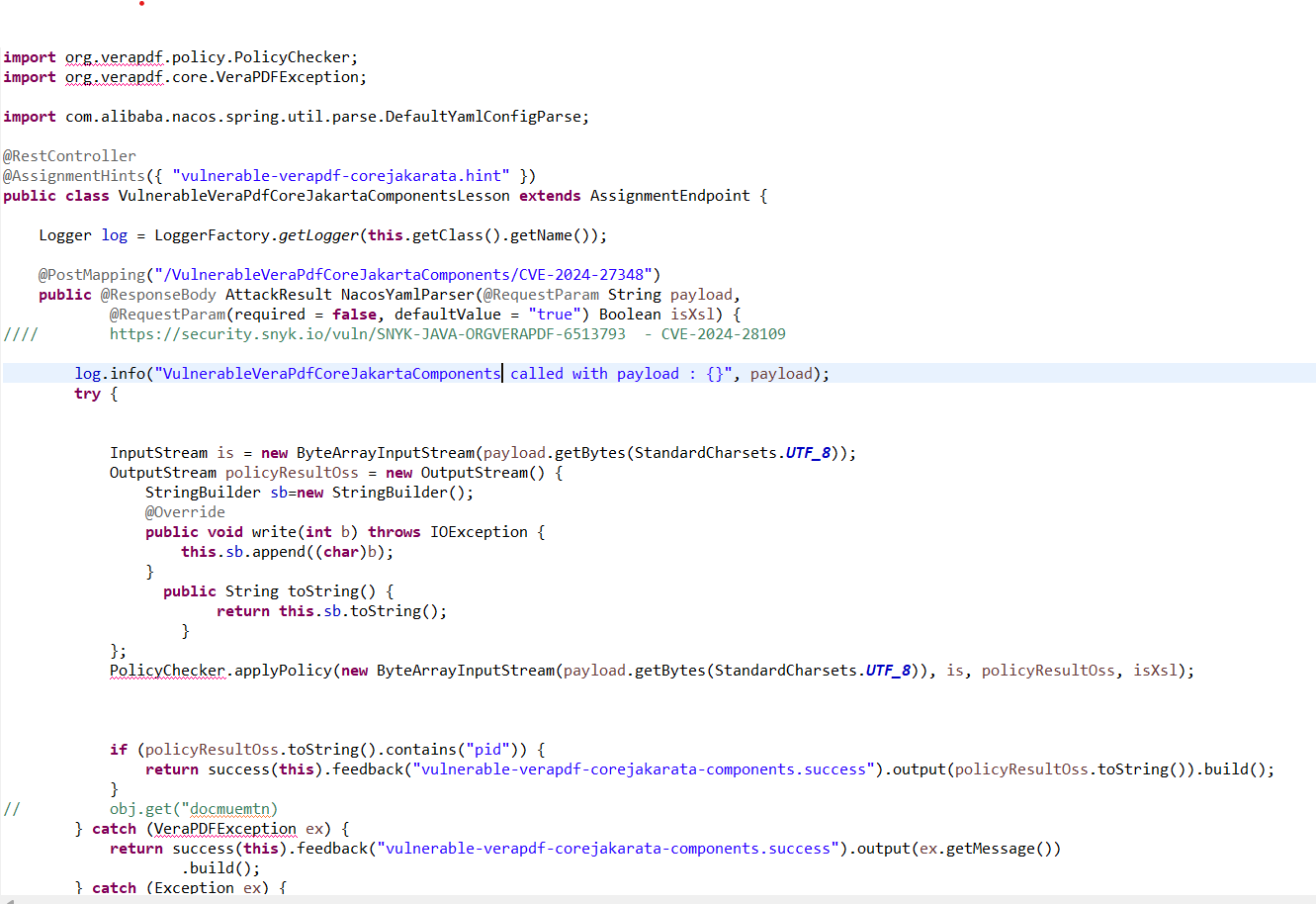
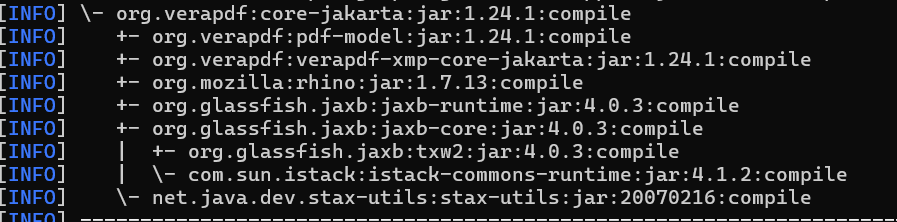
<https://security.snyk.io/vuln/SNYK-JAVA-ORGVERAPDF-6513793> - CVE-2024-28109

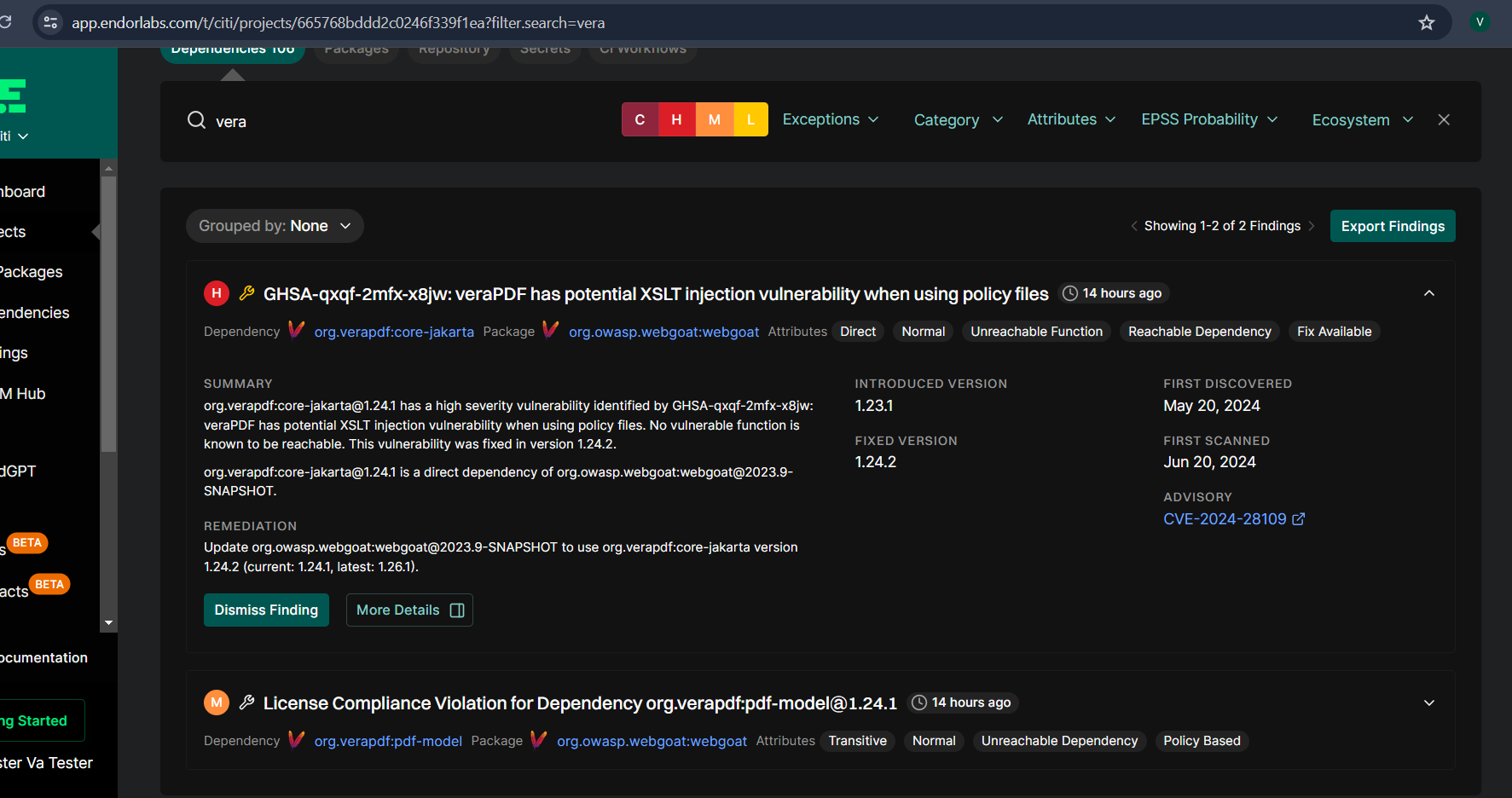


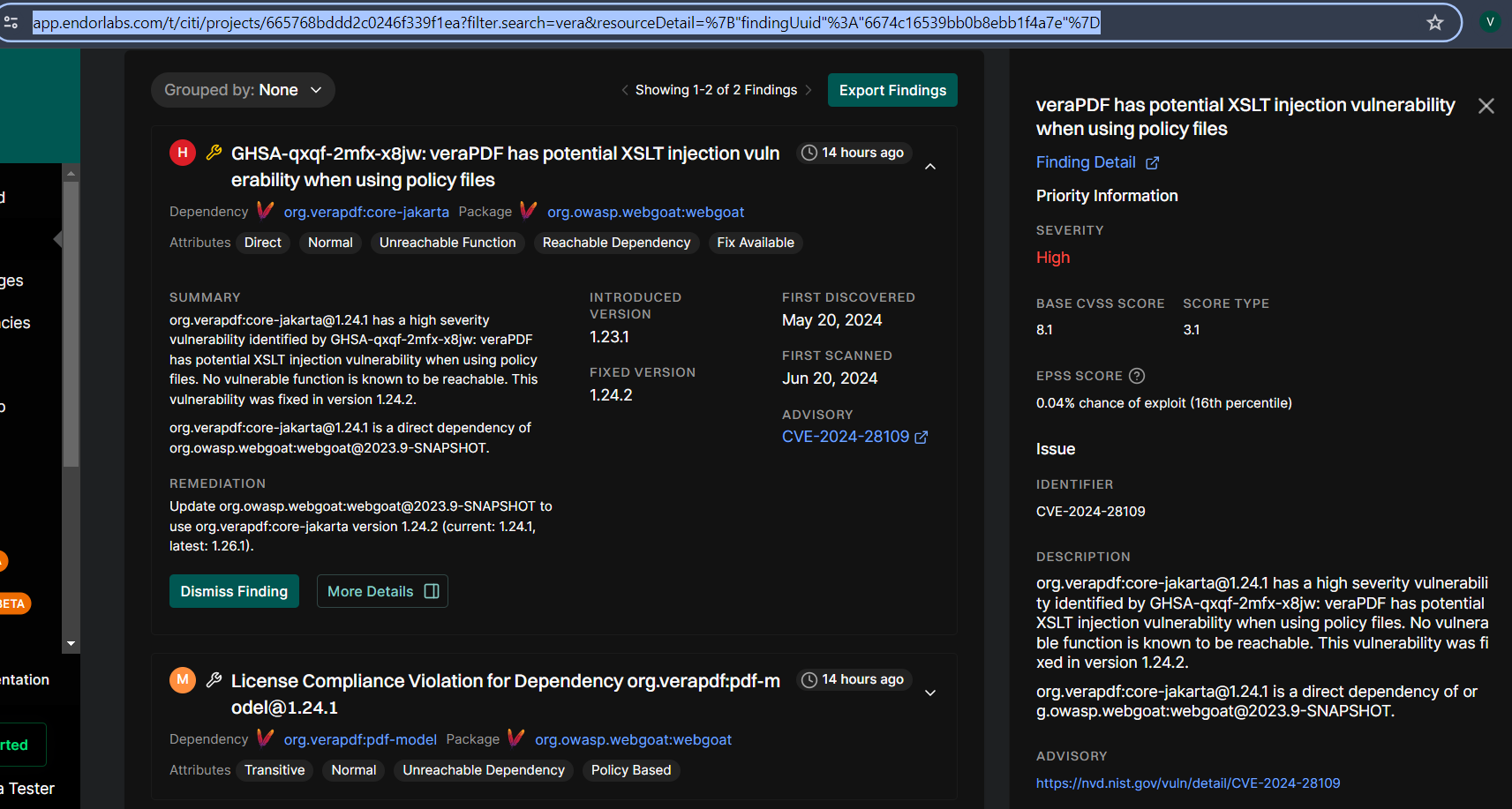




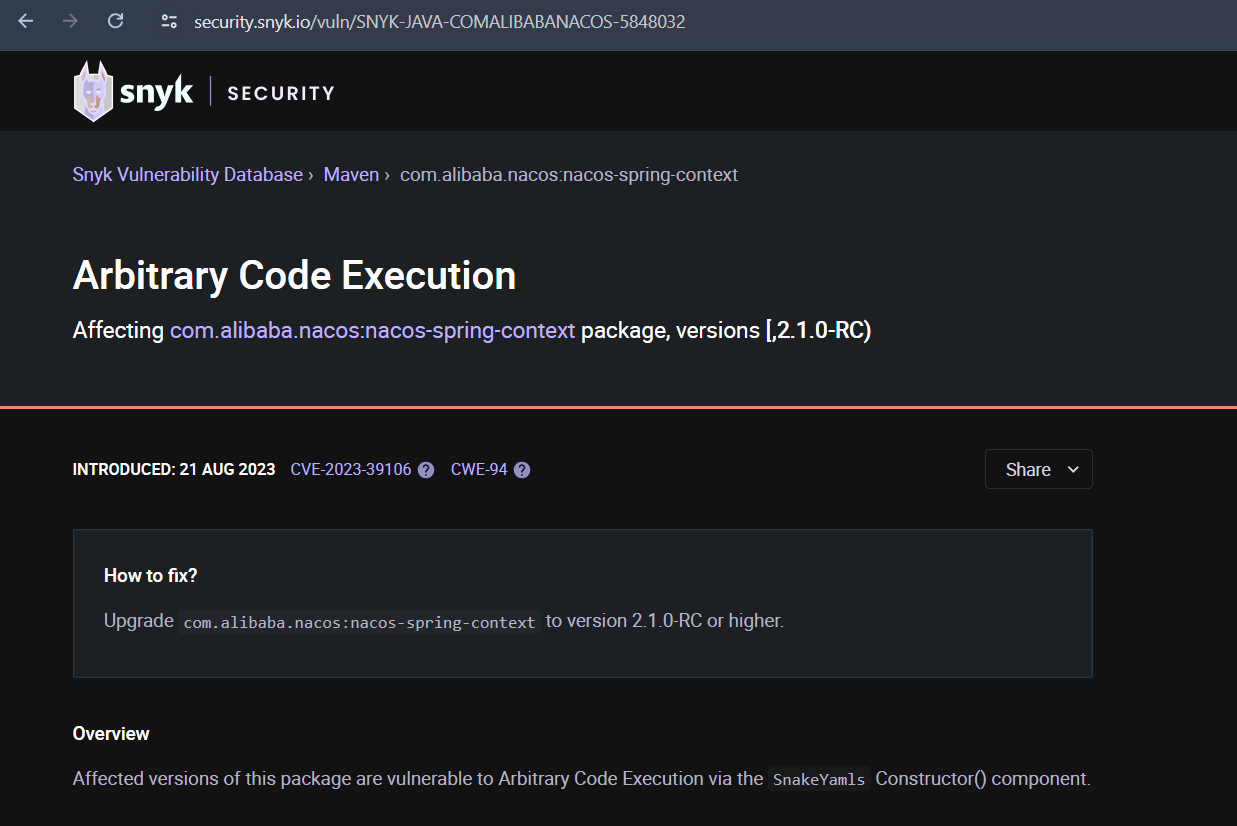


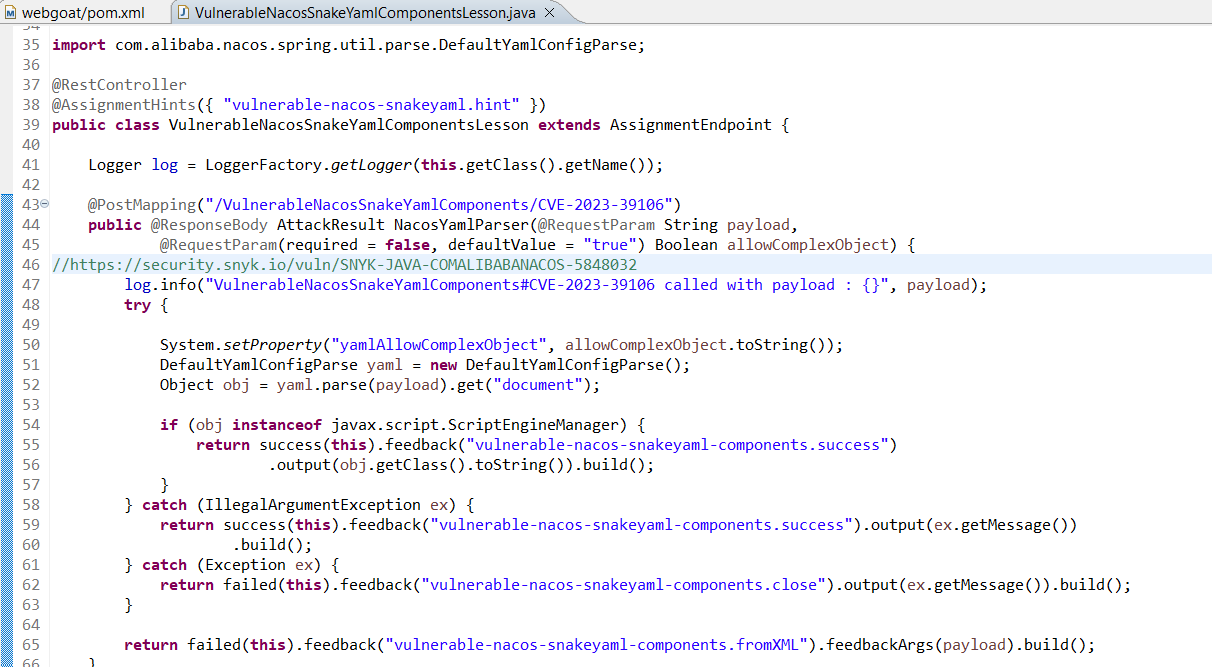
<https://app.endorlabs.com/t/citi/projects/665768bddd2c0246f339f1ea?filter.search=vera&resourceDetail=%7B%22findingUuid%22%3A%226674c16539bb0b8ebb1f4a7e%22%7D>

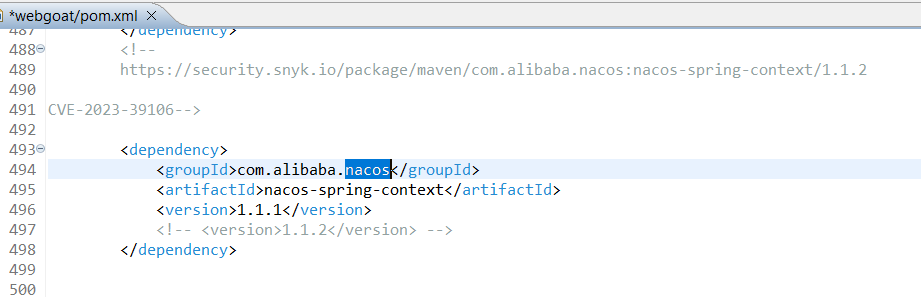


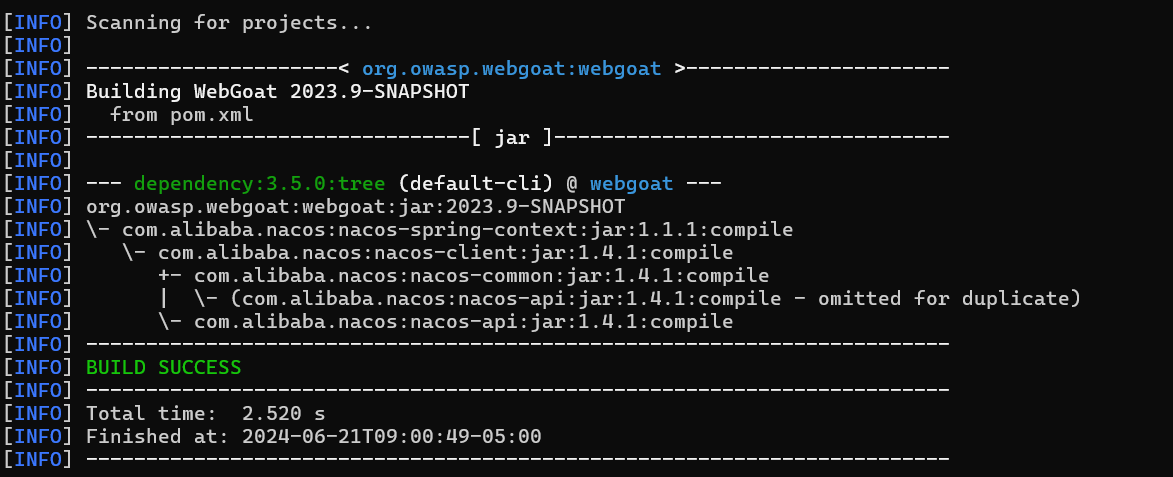


<https://security.snyk.io/vuln/SNYK-JAVA-COMALIBABANACOS-5848032> - CVE-2023-39106

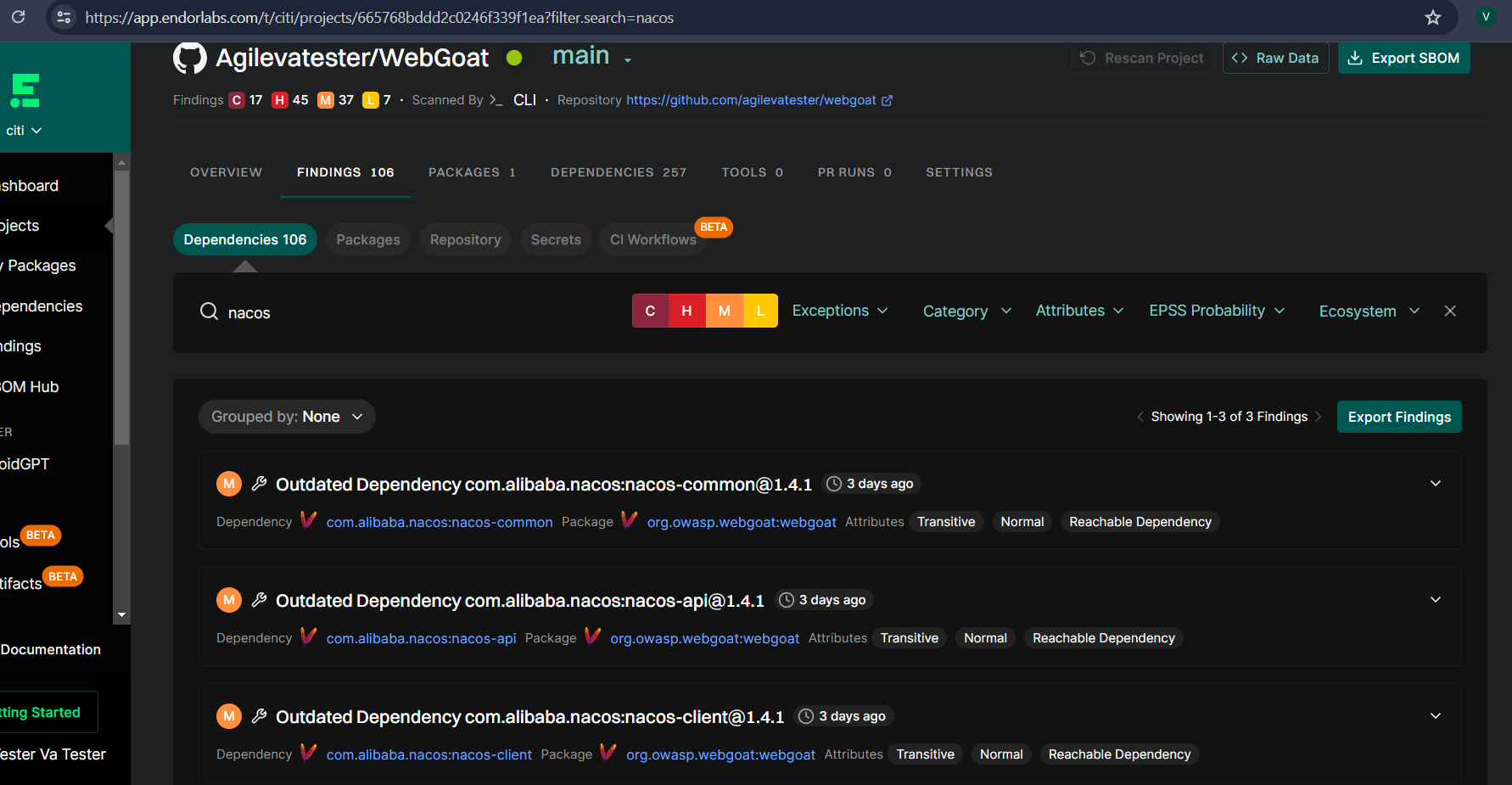




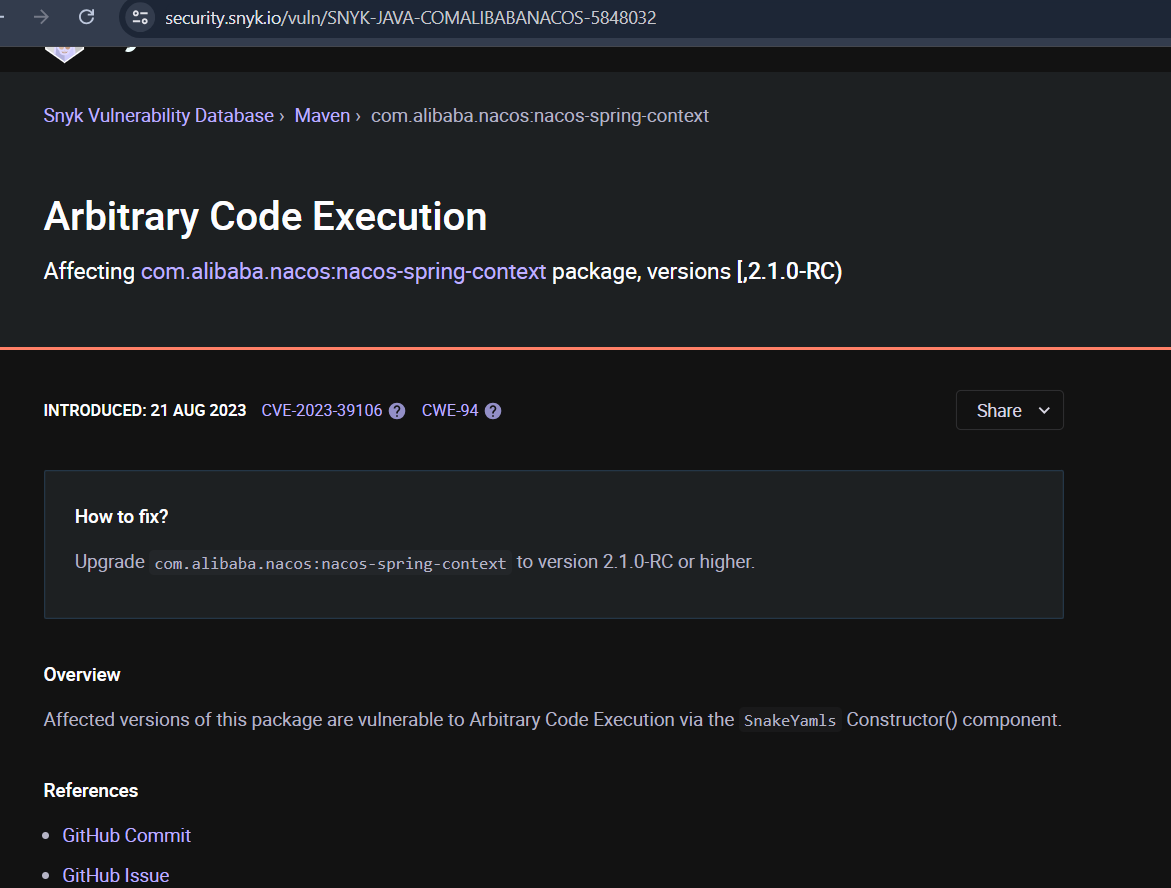




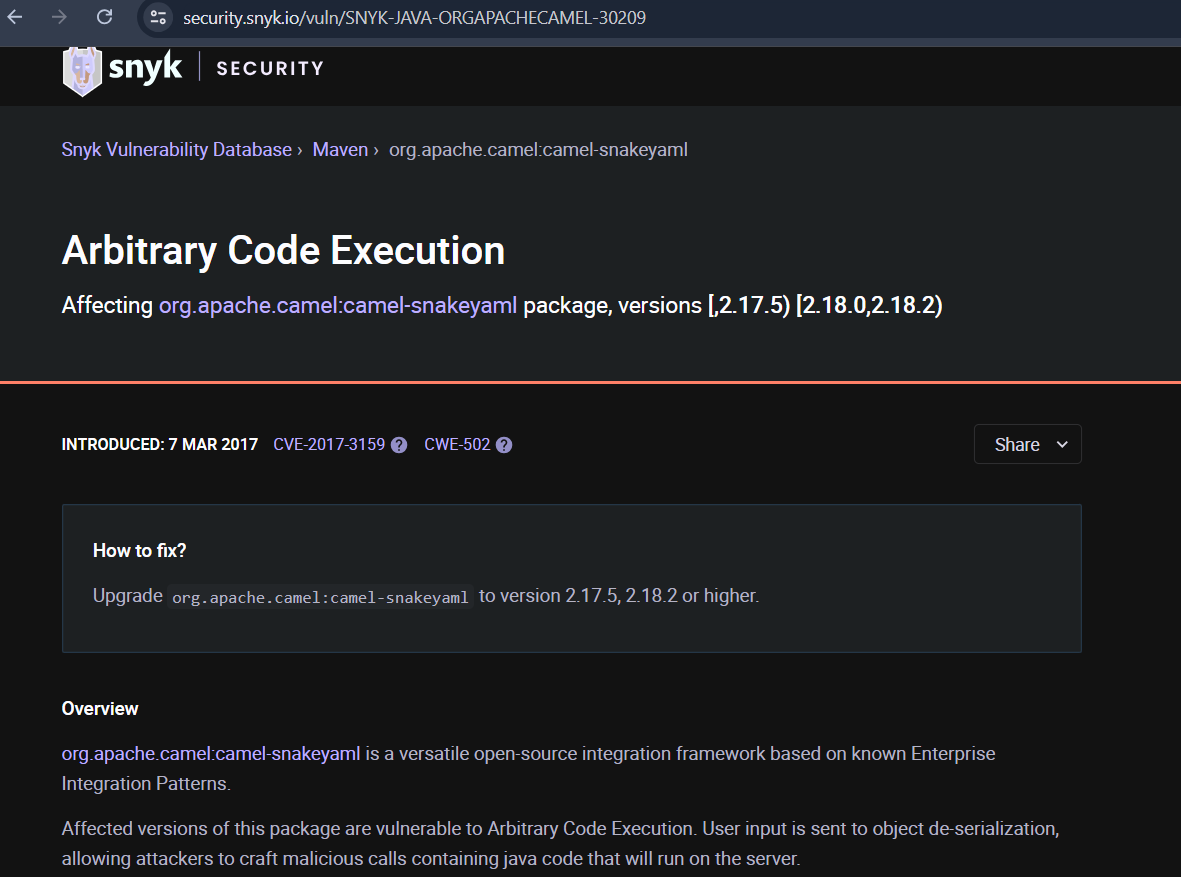
<https://app.endorlabs.com/t/citi/projects/665768bddd2c0246f339f1ea?filter.search=nacos>

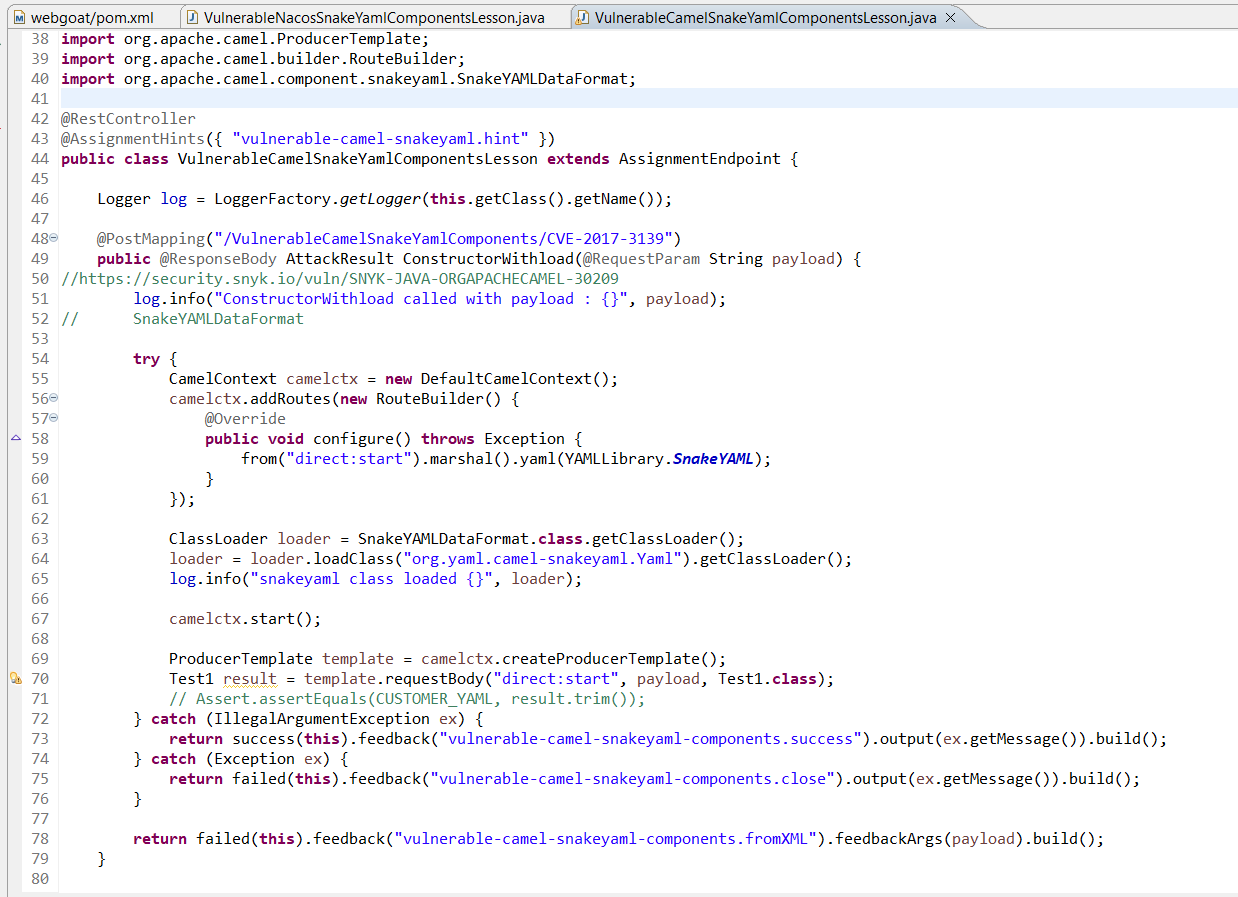


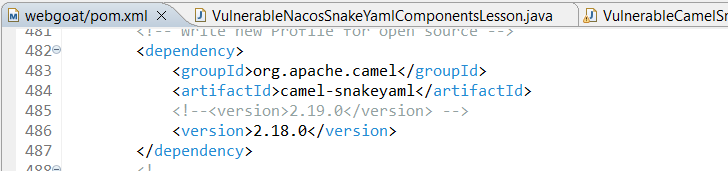
<https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHECAMEL-30209>

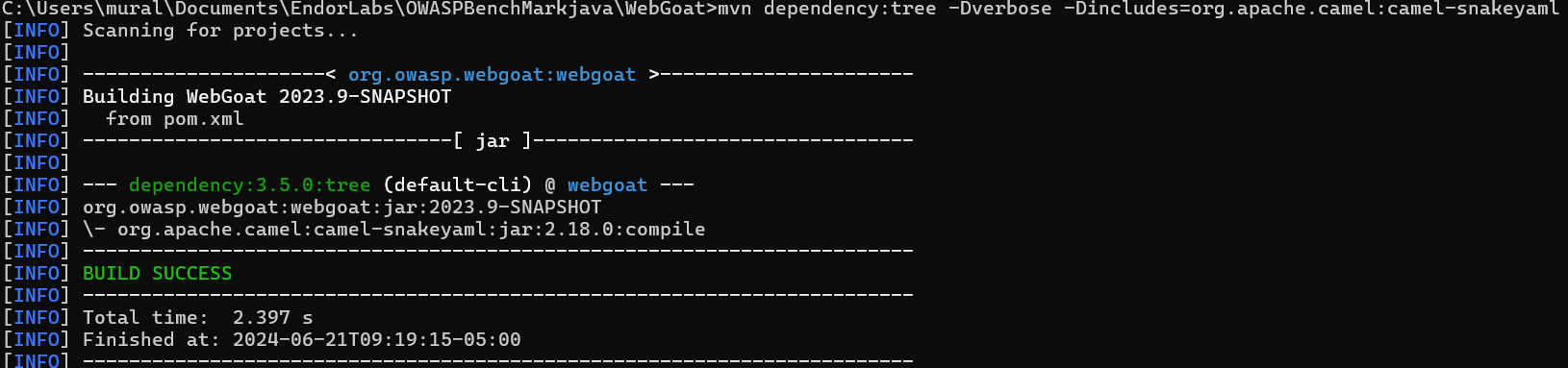


<https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHECAMEL-30209>

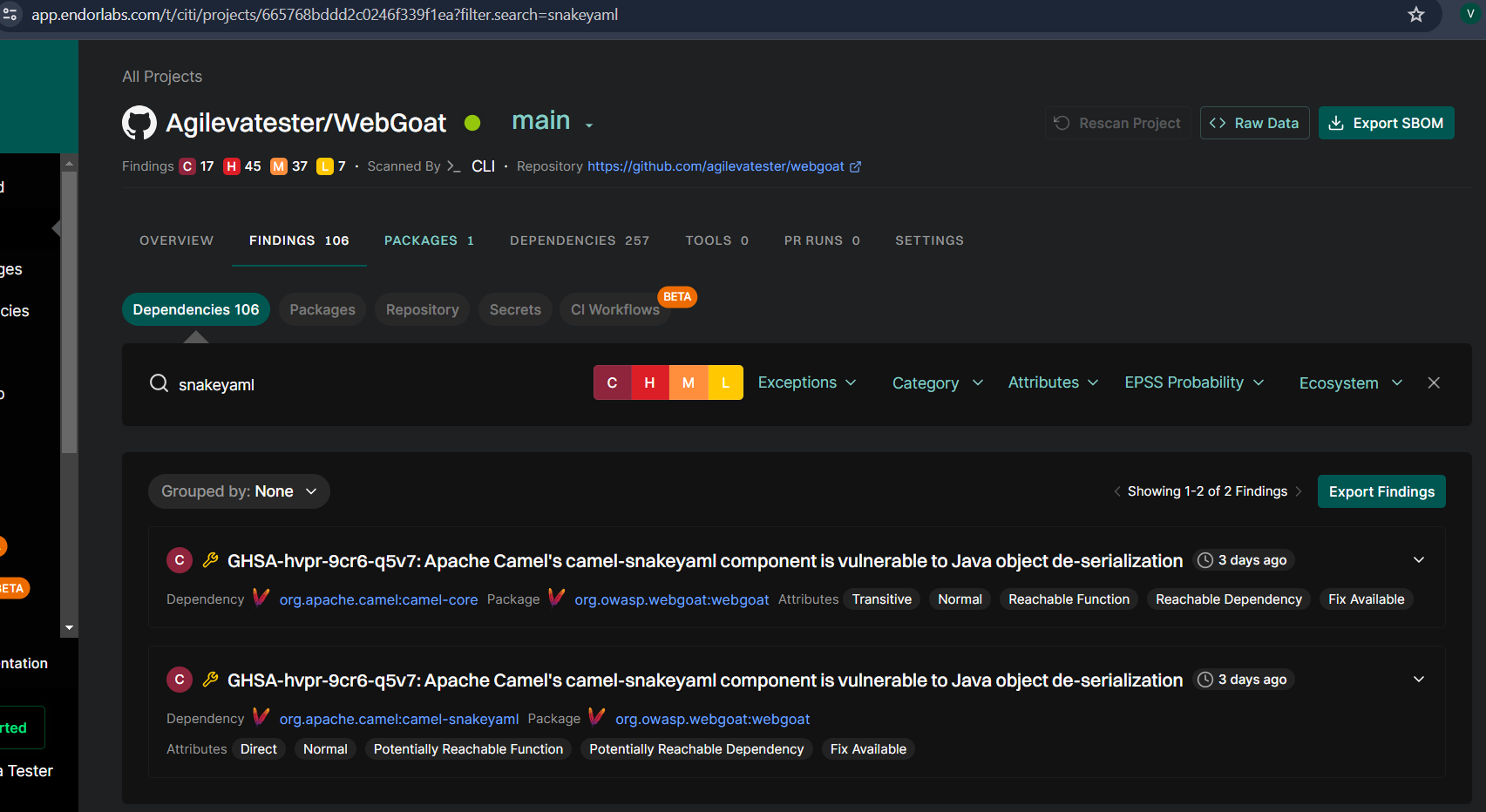


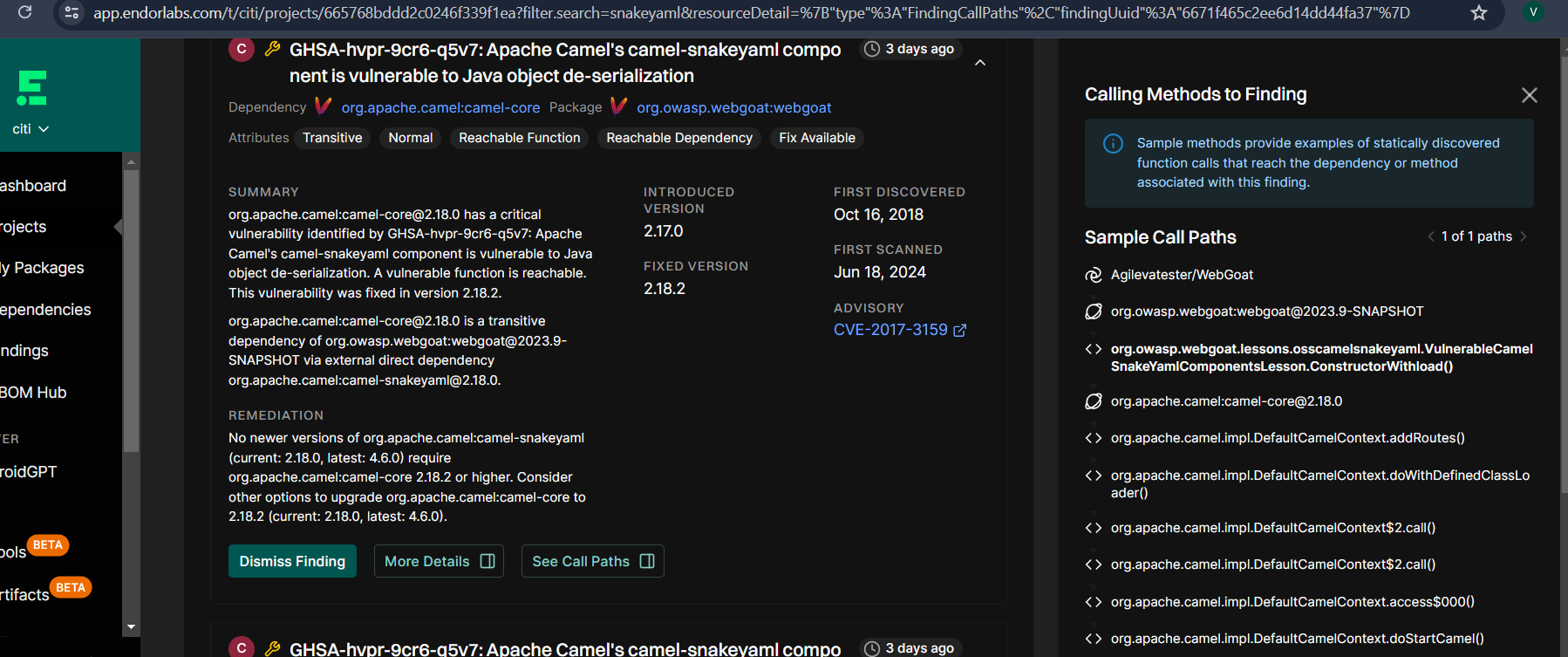


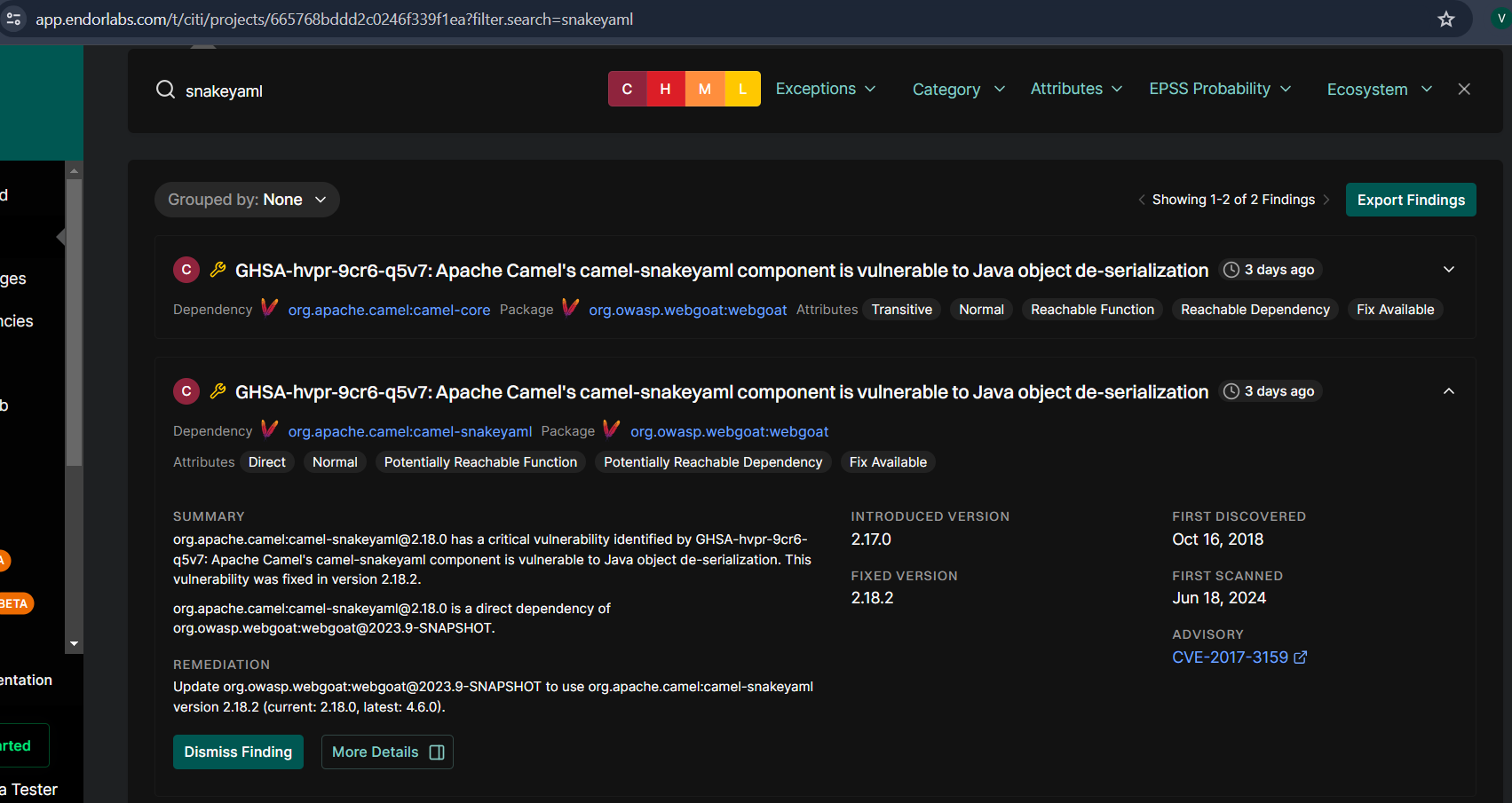




https://app.endorlabs.com/t/citi/projects/665768bddd2c0246f339f1ea?filter.search=snakeyaml





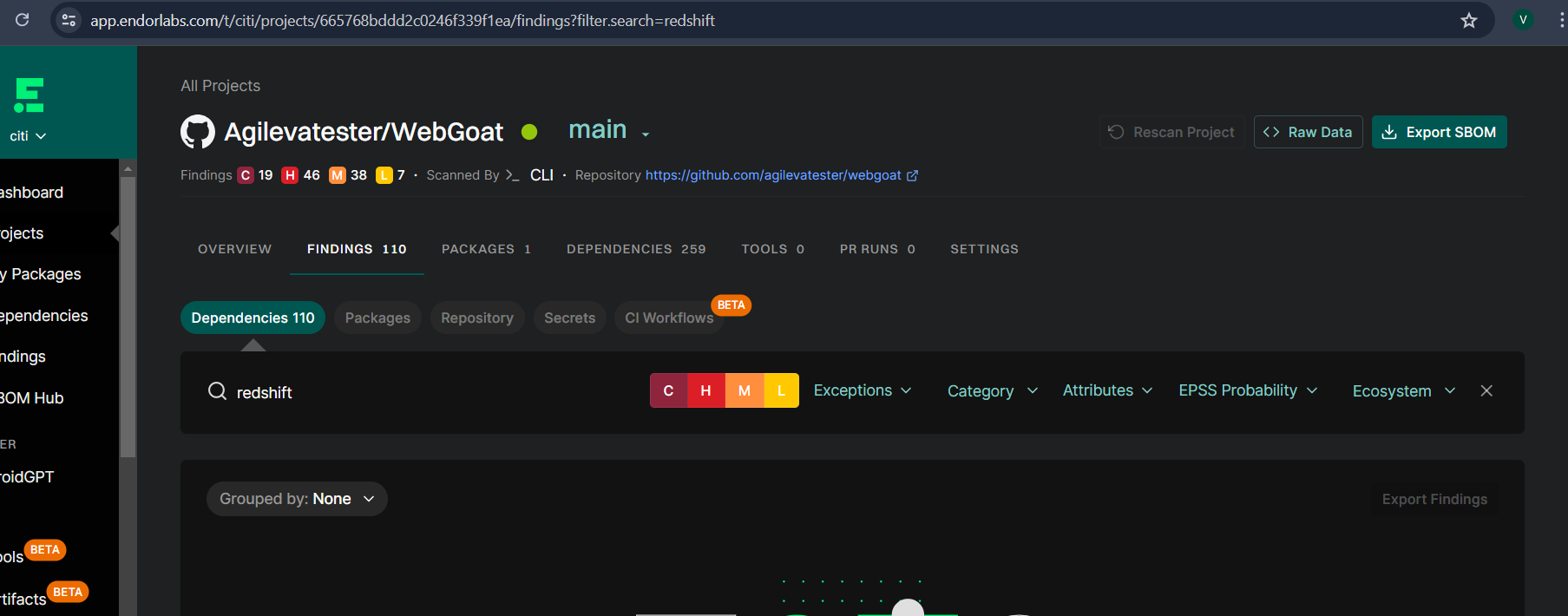


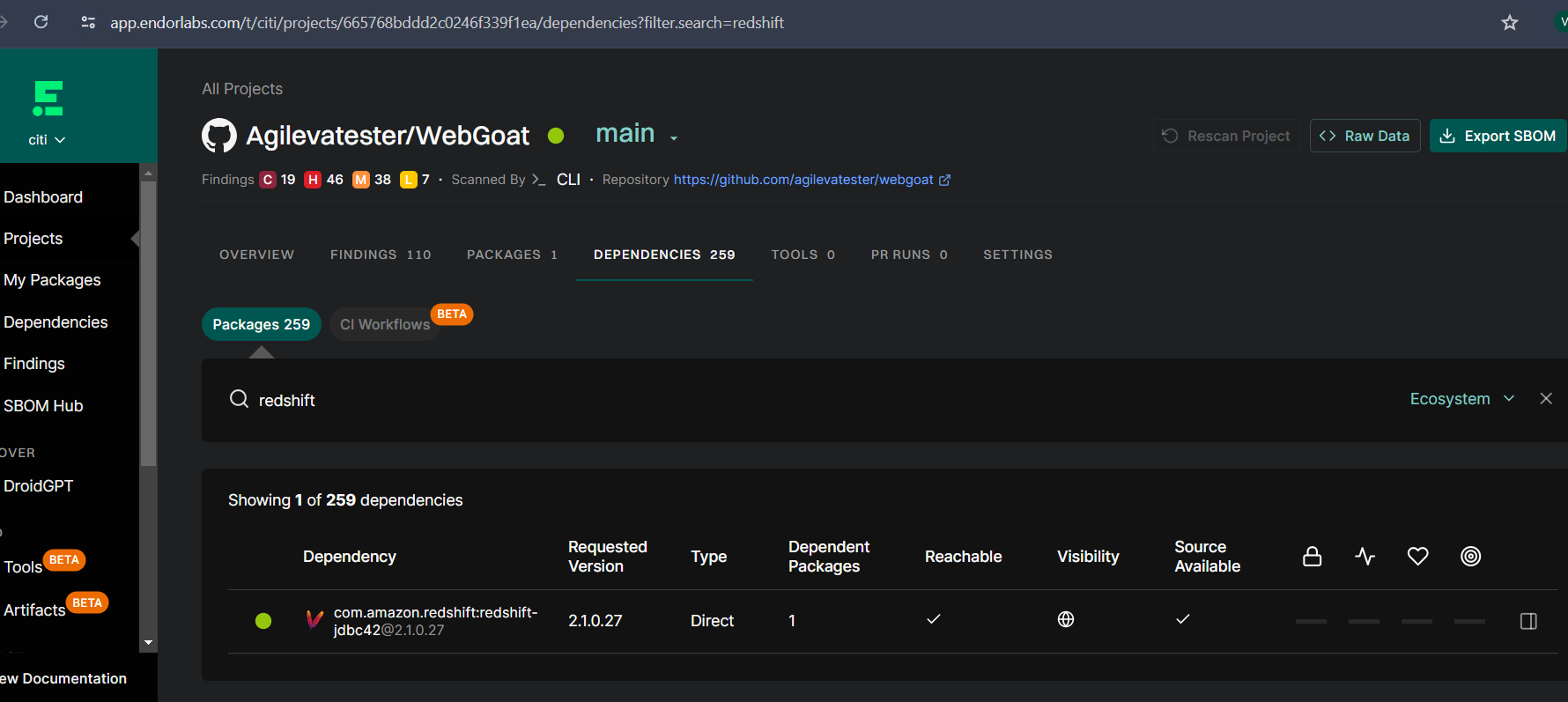
Error after adding the amazon jdbc42 driver

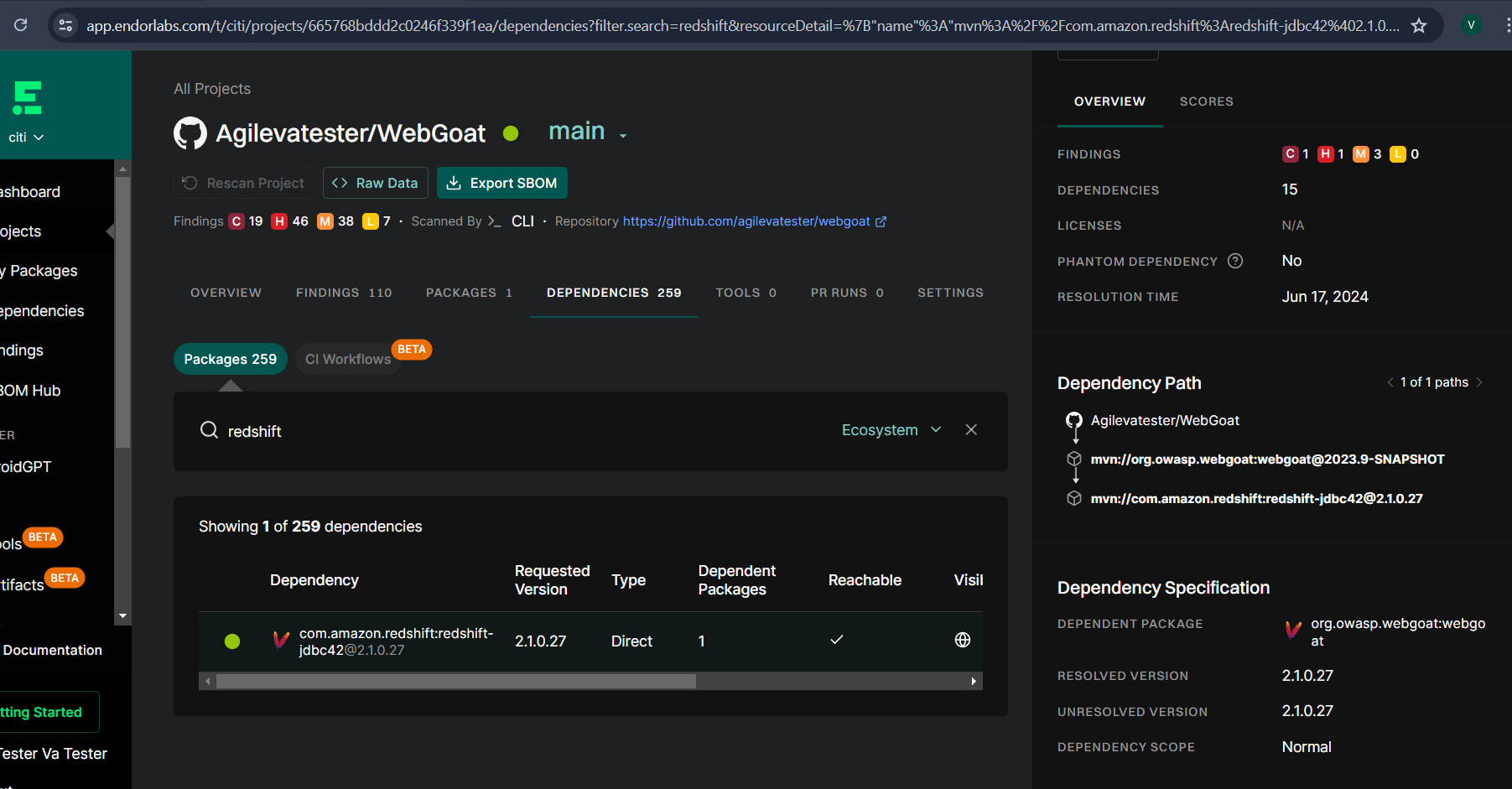
INFO: Initiating full dependency analysis for 'mvn://org.owasp.webgoat:webgoat@2023.9-SNAPSHOT'

ERROR findings-error: Errors processing findings for package version 'mvn://org.owasp.webgoat:webgoat@2023.9-SNAPSHOT' with ref 'e308d7cde7f3c6f50016a7548f078fe481d5de8e' and sha 'main': unable to store findings for method SYSTEM\_EVALUATION\_METHOD\_DEFINITION\_VULNERABILITIES: error while creating message tenant\_meta:{namespace:{value:"citi"}} meta:{name:{value:"dependency\_with\_critical\_vulnerabilities"} description:{value:"CVE-2024-32888: The Amazon JDBC Driver for Redshift is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in the Java Platform, Enterprise Editions. Prior to version 2.1.0.28, SQL injection is possible when using the non-default connection property `preferQueryMode=simple` in combination with application code which has a vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default, extended query mode. Note that `preferQueryMode` is not a supported parameter in Redshift JDBC driver, and is inherited code from Postgres JDBC driver. Users who do not override default settings to utilize this unsupported query mode are not affected. This issue is patched in driver version 2.1.0.28. As a workaround, do not use the connection property `preferQueryMode=simple`. (NOTE: Those who do not explicitly specify a query mode use the default of extended query mode and are not affected by this issue.)"} parent\_uuid:{value:"66576927976b423560072142"} parent\_kind:{value:"PackageVersion"}} spec:{project\_uuid:{value:"665768bddd2c0246f339f1ea"} last\_processed:{seconds:1719178951 nanos:657694800} level:FINDING\_LEVEL\_CRITICAL remediation:{value:"Update org.owasp.webgoat:webgoat@2023.9-SNAPSHOT to use com.amazon.redshift:redshift-jdbc42 version 2.1.0.28 (current: 2.1.0.27, latest: 2.1.0.29)."} finding\_metadata:{vulnerability:{uuid:{value:"664662ca53e1318e61a7dd01"} tenant\_meta:{namespace:{value:"oss"}} meta:{create\_time:{seconds:1715888842 nanos:410000000} update\_time:{seconds:1716074811 nanos:29679941} upsert\_time:{seconds:1716074811 nanos:29679941} name:{value:"CVE-2024-32888"} kind:{value:"Vuln"} version:{value:"v1"} description:{value:"The Amazon JDBC Driver for Redshift is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in the Java Platform, Enterprise Editions. Prior to version 2.1.0.28, SQL injection is possible when using the non-default connection property `preferQueryMode=simple` in combination with application code which has a vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default, extended query mode. Note that `preferQueryMode` is not a supported parameter in Redshift JDBC driver, and is inherited code from Postgres JDBC driver. Users who do not override default settings to utilize this unsupported query mode are not affected. This issue is patched in driver version 2.1.0.28. As a workaround, do not use the connection property `preferQueryMode=simple`. (NOTE: Those who do not explicitly specify a query mode use the default of extended query mode and are not affected by this issue.)"} created\_by:{value:"vulnerabilityingestor@endor.ai@x509"} updated\_by:{value:"vulnerabilityingestor@endor.ai@x509"}} spec:{deepdive:{value:true} disputed:{} cvss\_v3\_severity:{score:{value:10} vector:{value:"CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"} level:LEVEL\_CRITICAL} summary:{value:"The Amazon JDBC Driver for Redshift is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in the Java Platform, Enterprise Editions. Prior to version 2.1.0.28, SQL injection is possible when using the non-default connection property `preferQueryMode=simple` in combination with application code which has a vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default, extended query mode. Note that `preferQueryMode` is not a supported parameter in Redshift JDBC driver, and is inherited code from Postgres JDBC driver. Users who do not override default settings to utilize this unsupported query mode are not affected. This issue is patched in driver version 2.1.0.28. As a workaround, do not use the connection property `preferQueryMode=simple`. (NOTE: Those who do not explicitly specify a query mode use the default of extended query mode and are not affected by this issue.)"} affected:{package:{name:{value:"com.amazon.redshift:redshift-jdbc42"} ecosystem:ECOSYSTEM\_MAVEN purl:{value:"pkg:maven/com.amazon.redshift/redshift-jdbc42"}} ranges:{type:RANGE\_TYPE\_ECOSYSTEM introduced:{value:"2.0.0.3"} fixed:{value:"2.1.0.28"}} versions:"2.0.0.3" versions:"2.0.0.4" versions:"2.0.0.5" versions:"2.0.0.6" versions:"2.0.0.7" versions:"2.1.0.1" versions:"2.1.0.2" versions:"2.1.0.3" versions:"2.1.0.4" versions:"2.1.0.5" versions:"2.1.0.6" versions:"2.1.0.7" versions:"2.1.0.8" versions:"2.1.0.9" versions:"2.1.0.10" versions:"2.1.0.11" versions:"2.1.0.12" versions:"2.1.0.13" versions:"2.1.0.14" versions:"2.1.0.15" versions:"2.1.0.16" versions:"2.1.0.17" versions:"2.1.0.18" versions:"2.1.0.19" versions:"2.1.0.20" versions:"2.1.0.21" versions:"2.1.0.22" versions:"2.1.0.23" versions:"2.1.0.24" versions:"2.1.0.25" versions:"2.1.0.26" versions:"2.1.0.27" affected\_filepaths:"com/amazon/redshift/core/v3/SimpleParameterList.class" affected\_callpath\_uris:"/com.amazon.redshift.core.v3/SimpleParameterList.toString(/java.lang/IntegerType,/java.lang/BooleanType)/java.lang/String" fix\_commits:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/bc93694201a291493778ce5369a72befeca5ba7d" fix\_commits:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/12a5e8ecfbb44c8154fc66041cca2e20ecd7b339" has\_been\_fixed:{value:true} source:SOURCE\_ENDOR} epss\_score:{probability\_score:{value:0.00045} percentile\_score:{value:0.14717}} raw:{endor\_vulnerability:{cve\_id:{value:"CVE-2024-32888"} cve\_description:{value:"The Amazon JDBC Driver for Redshift is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in the Java Platform, Enterprise Editions. Prior to version 2.1.0.28, SQL injection is possible when using the non-default connection property `preferQueryMode=simple` in combination with application code which has a vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default, extended query mode. Note that `preferQueryMode` is not a supported parameter in Redshift JDBC driver, and is inherited code from Postgres JDBC driver. Users who do not override default settings to utilize this unsupported query mode are not affected. This issue is patched in driver version 2.1.0.28. As a workaround, do not use the connection property `preferQueryMode=simple`. (NOTE: Those who do not explicitly specify a query mode use the default of extended query mode and are not affected by this issue.)"} cvss\_score:{value:10} cvss\_vector:{value:"CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"} cwe:{value:"89"} cve\_references:{value:"https://github.com/advisories/GHSA-x3wm-hffr-chwm"} cve\_references:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/security/advisories/GHSA-x3wm-hffr-chwm"} cve\_references:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/blob/master/CHANGELOG.md#v21028-2024-05-14"} package\_name:{value:"amazon-redshift-jdbc-driver"} ecosystem:{value:"maven"} fix\_commit:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/bc93694201a291493778ce5369a72befeca5ba7d"} fix\_commit:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/12a5e8ecfbb44c8154fc66041cca2e20ecd7b339"} additional\_notes:{value:"Note: cvss score /vector data added as per data from security advisory provided by the package maintainer.\n\nIntroduction in 2.0.0(src/main/java/com/amazon/redshift/core/v3/SimpleParameterList.java):https://github.com/aws/amazon-redshift-jdbc-driver/commit/7a1efb19412831bd0b9d20842d172df988664b8f#diff-5218300a195d6f30a0fab97f126b87b27edf63804896c26c3694340b22ae4e55R172"} component:{group\_id:{value:"com.amazon.redshift"} artifact\_id:{value:"redshift-jdbc42"} vulnerable\_versions:{value:"2.0.0.3"} vulnerable\_versions:{value:"2.0.0.4"} vulnerable\_versions:{value:"2.0.0.5"} vulnerable\_versions:{value:"2.0.0.6"} vulnerable\_versions:{value:"2.0.0.7"} vulnerable\_versions:{value:"2.1.0.1"} vulnerable\_versions:{value:"2.1.0.2"} vulnerable\_versions:{value:"2.1.0.3"} vulnerable\_versions:{value:"2.1.0.4"} vulnerable\_versions:{value:"2.1.0.5"} vulnerable\_versions:{value:"2.1.0.6"} vulnerable\_versions:{value:"2.1.0.7"} vulnerable\_versions:{value:"2.1.0.8"} vulnerable\_versions:{value:"2.1.0.9"} vulnerable\_versions:{value:"2.1.0.10"} vulnerable\_versions:{value:"2.1.0.11"} vulnerable\_versions:{value:"2.1.0.12"} vulnerable\_versions:{value:"2.1.0.13"} vulnerable\_versions:{value:"2.1.0.14"} vulnerable\_versions:{value:"2.1.0.15"} vulnerable\_versions:{value:"2.1.0.16"} vulnerable\_versions:{value:"2.1.0.17"} vulnerable\_versions:{value:"2.1.0.18"} vulnerable\_versions:{value:"2.1.0.19"} vulnerable\_versions:{value:"2.1.0.20"} vulnerable\_versions:{value:"2.1.0.21"} vulnerable\_versions:{value:"2.1.0.22"} vulnerable\_versions:{value:"2.1.0.23"} vulnerable\_versions:{value:"2.1.0.24"} vulnerable\_versions:{value:"2.1.0.25"} vulnerable\_versions:{value:"2.1.0.26"} vulnerable\_versions:{value:"2.1.0.27"} fixed\_versions:{value:"2.1.0.28"} vulnerable\_filepath:{value:"com/amazon/redshift/core/v3/SimpleParameterList.class"} versions\_range:{value:"[2.0.0.3,2.1.0.28)"} endor\_uri:{value:"/com.amazon.redshift.core.v3/SimpleParameterList.toString(/java.lang/IntegerType,/java.lang/BooleanType)/java.lang/String"}} deepdive:{value:true} disputed:{} nofix:{} schema\_version:{value:"v1"}} epss\_record:{cve\_id:{value:"CVE-2024-32888"} probability:{value:0.00045} percentile:{value:0.14717} ingestion\_time:{seconds:1716074778 nanos:134446383}} nvd\_vulnerability:{cve:{id:{value:"CVE-2024-32888"} source\_identifier:{value:"security-advisories@github.com"} vuln\_status:{value:"Awaiting Analysis"} vuln\_typed\_status:NVD\_STATUS\_AWAITING\_ANALYSIS published:{seconds:1715742912 nanos:627000000} last\_modified:{seconds:1715791219 nanos:330000000} descriptions:{lang:{value:"en"} value:{value:"The Amazon JDBC Driver for Redshift is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in the Java Platform, Enterprise Editions. Prior to version 2.1.0.28, SQL injection is possible when using the non-default connection property `preferQueryMode=simple` in combination with application code which has a vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default, extended query mode. Note that `preferQueryMode` is not a supported parameter in Redshift JDBC driver, and is inherited code from Postgres JDBC driver. Users who do not override default settings to utilize this unsupported query mode are not affected. This issue is patched in driver version 2.1.0.28. As a workaround, do not use the connection property `preferQueryMode=simple`. (NOTE: Those who do not explicitly specify a query mode use the default of extended query mode and are not affected by this issue.)"}} descriptions:{lang:{value:"es"} value:{value:"El controlador Amazon JDBC para Redshift es un controlador JDBC de tipo 4 que proporciona conectividad de bases de datos a través de las interfaces de programas de aplicación (API) JDBC estándar disponibles en Java Platform, Enterprise Editions. Antes de la versión 2.1.0.28, la inyección SQL es posible cuando se usa la propiedad de conexión no predeterminada `preferQueryMode=simple` en combinación con código de aplicación que tiene un SQL vulnerable que niega el valor de un parámetro. No hay vulnerabilidad en el controlador cuando se utiliza el modo de consulta extendido predeterminado. Tenga en cuenta que `preferQueryMode` no es un parámetro admitido en el controlador JDBC de Redshift y es un código heredado del controlador JDBC de Postgres. Los usuarios que no anulen la configuración predeterminada para utilizar este modo de consulta no compatible no se verán afectados. Este problema se solucionó en la versión del controlador 2.1.0.28. Como workaround, no utilice la propiedad de conexión `preferQueryMode=simple`. (NOTA: Aquellos que no especifican explícitamente un modo de consulta utilizan el modo de consulta extendido predeterminado y no se ven afectados por este problema)."}} references:{url:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/0d354a5f26ca23f7cac4e800e3b8734220230319"} source:{value:"security-advisories@github.com"}} references:{url:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/12a5e8ecfbb44c8154fc66041cca2e20ecd7b339"} source:{value:"security-advisories@github.com"}} references:{url:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/commit/bc93694201a291493778ce5369a72befeca5ba7d"} source:{value:"security-advisories@github.com"}} references:{url:{value:"https://github.com/aws/amazon-redshift-jdbc-driver/security/advisories/GHSA-x3wm-hffr-chwm"} source:{value:"security-advisories@github.com"}} references:{url:{value:"https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-24rp-q3w6-vc56"} source:{value:"security-advisories@github.com"}} metrics:{cvss\_metric\_v31:{source:{value:"security-advisories@github.com"} type:NVD\_METRIC\_TYPE\_SECONDARY cvss\_data:{version:{value:"3.1"} vector\_string:{value:"CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"} attack\_vector:NVD\_ATTACK\_VECTOR\_NETWORK attack\_complexity:NVD\_ATTACK\_COMPLEXITY\_LOW privileges\_required:NVD\_PRIVILEGES\_REQUIRED\_NONE user\_interaction:NVD\_USER\_INTERACTION\_NONE scope:NVD\_SCOPE\_CHANGED confidentiality\_impact:NVD\_IMPACT\_HIGH integrity\_impact:NVD\_IMPACT\_HIGH availability\_impact:NVD\_IMPACT\_HIGH base\_score:{value:10} base\_severity:NVD\_SEVERITY\_CRITICAL} exploitability\_score:{value:3.9} impact\_score:{value:6}}} weaknesses:{source:{value:"security-advisories@github.com"} type:{value:"Secondary"} description:{lang:{value:"en"} value:{value:"CWE-89"}}}}}} additional\_endor\_notes:"Note: cvss score /vector data added as per data from security advisory provided by the package maintainer.\n\nIntroduction in 2.0.0(src/main/java/com/amazon/redshift/core/v3/SimpleParameterList.java):https://github.com/aws/amazon-redshift-jdbc-driver/commit/7a1efb19412831bd0b9d20842d172df988664b8f#diff-5218300a195d6f30a0fab97f126b87b27edf63804896c26c3694340b22ae4e55R172"}}} summary:{value:"com.amazon.redshift:redshift-jdbc42@2.1.0.27 has a critical vulnerability identified by CVE-2024-32888: The Amazon JDBC Driver for Redshift is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs) available in the Java Platform, Enterprise Editions. Prior to version 2.1.0.28, SQL injection is possible when using the non-default connection property `preferQueryMode=simple` in combination with application code which has a vulnerable SQL that negates a parameter value. There is no vulnerability in the driver when using the default, extended query mode. Note that `preferQueryMode` is not a supported parameter in Redshift JDBC driver, and is inherited code from Postgres JDBC driver. Users who do not override default settings to utilize this unsupported query mode are not affected. This issue is patched in driver version 2.1.0.28. As a workaround, do not use the connection property `preferQueryMode=simple`. (NOTE: Those who do not explicitly specify a query mode use the default of extended query mode and are not affected by this issue.). A vulnerable function is reachable. This vulnerability was fixed in version 2.1.0.28.\ncom.amazon.redshift:redshift-jdbc42@2.1.0.27 is a direct dependency of org.owasp.webgoat:webgoat@2023.9-SNAPSHOT."} finding\_tags:FINDING\_TAGS\_DIRECT finding\_tags:FINDING\_TAGS\_NORMAL finding\_tags:FINDING\_TAGS\_REACHABLE\_FUNCTION finding\_tags:FINDING\_TAGS\_REACHABLE\_DEPENDENCY finding\_tags:FINDING\_TAGS\_FIX\_AVAILABLE target\_uuid:{value:"66788c6787c1de64ea720db1"} extra\_key:{value:"CVE-2024-32888"} method:SYSTEM\_EVALUATION\_METHOD\_DEFINITION\_VULNERABILITIES target\_dependency\_package\_name:{value:"mvn://com.amazon.redshift:redshift-jdbc42@2.1.0.27"} target\_dependency\_name:{value:"com.amazon.redshift:redshift-jdbc42"} target\_dependency\_version:{value:"2.1.0.27"} explanation:{value:"A critical severity known vulnerability has been assessed against this version of the software package according to the information in OSV.dev"} remediation\_action:FINDING\_REMEDIATION\_UPGRADE source\_code\_version:{sha:{value:"e308d7cde7f3c6f50016a7548f078fe481d5de8e"} ref:{value:"main"}} reachable\_paths:{nodes:{function\_ref:{language:{value:"java"} registry:{} product:{value:"org.owasp.webgoat:webgoat"} version:{value:"2023.9-SNAPSHOT"} namespace:{value:"org.owasp.webgoat.lessons.sqlinjection.mitigation"} language\_specific:{value:"SqlInjectionLesson13.completed(/java.lang/String)/org.owasp.webgoat.container.assignments/AttackResult"} classname:{value:"SqlInjectionLesson13"} function\_or\_attribute\_name:{value:"completed"} args:"/java.lang/String" return\_type:{value:"/org.owasp.webgoat.container.assignments/AttackResult"} declared\_type:{value:"/org.owasp.webgoat.lessons.sqlinjection.mitigation/SqlInjectionLesson13"} signature:{value:"completed(/java.lang/String)/org.owasp.webgoat.container.assignments/AttackResult"}} package\_version:{value:"mvn://org.owasp.webgoat:webgoat@2023.9-SNAPSHOT"} internal:{value:true}} nodes:{function\_ref:{language:{value:"java"} registry:{} product:{value:"com.amazon.redshift:redshift-jdbc42"} version:{value:"2.1.0.27"} namespace:{value:"com.amazon.redshift.jdbc"} language\_specific:{value:"RedshiftConnectionImpl.prepareStatement(/java.lang/String)/java.sql/PreparedStatement"} classname:{value:"RedshiftConnectionImpl"} function\_or\_attribute\_name:{value:"prepareStatement"} args:"/java.lang/String" return\_type:{value:"/java.sql/PreparedStatement"} declared\_type:{value:"/com.amazon.redshift.jdbc/RedshiftConnectionImpl"} signature:{value:"prepareStatement(/java.lang/String)/java.sql/PreparedStatement"}} package\_version:{value:"mvn://com.amazon.redshift:redshift-jdbc42@2.1.0.27"}} nodes:{function\_ref:{language:{value:"java"} registry:{} product:{value:"com.amazon.redshift:redshift-jdbc42"} version:{value:"2.1.0.27"} namespace:{value:"com.amazon.redshift.jdbc"} language\_specific:{value:"RedshiftPreparedStatement.toString()/java.lang/String"} classname:{value:"RedshiftPreparedStatement"} function\_or\_attribute\_name:{value:"toString"} return\_type:{value:"/java.lang/String"} declared\_type:{value:"/com.amazon.redshift.jdbc/RedshiftPreparedStatement"} signature:{value:"toString()/java.lang/String"}} package\_version:{value:"mvn://com.amazon.redshift:redshift-jdbc42@2.1.0.27"}} nodes:{function\_ref:{language:{value:"java"} registry:{} product:{value:"com.amazon.redshift:redshift-jdbc42"} version:{value:"2.1.0.27"} namespace:{value:"com.amazon.redshift.core.v3"} language\_specific:{value:"SimpleQuery.toString(/com.amazon.redshift.core/ParameterList)/java.lang/String"} classname:{value:"SimpleQuery"} function\_or\_attribute\_name:{value:"toString"} args:"/com.amazon.redshift.core/ParameterList" return\_type:{value:"/java.lang/String"} declared\_type:{value:"/com.amazon.redshift.core.v3/SimpleQuery"} signature:{value:"toString(/com.amazon.redshift.core/ParameterList)/java.lang/String"}} package\_version:{value:"mvn://com.amazon.redshift:redshift-jdbc42@2.1.0.27"}} nodes:{function\_ref:{language:{value:"java"} registry:{} product:{value:"com.amazon.redshift:redshift-jdbc42"} version:{value:"2.1.0.27"} namespace:{value:"com.amazon.redshift.core"} language\_specific:{value:"NativeQuery.toString(/com.amazon.redshift.core/ParameterList)/java.lang/String"} classname:{value:"NativeQuery"} function\_or\_attribute\_name:{value:"toString"} args:"/com.amazon.redshift.core/ParameterList" return\_type:{value:"/java.lang/String"} declared\_type:{value:"/com.amazon.redshift.core/NativeQuery"} signature:{value:"toString(/com.amazon.redshift.core/ParameterList)/java.lang/String"}} package\_version:{value:"mvn://com.amazon.redshift:redshift-jdbc42@2.1.0.27"}} nodes:{function\_ref:{language:{value:"java"} registry:{} product:{value:"com.amazon.redshift:redshift-jdbc42"} version:{value:"2.1.0.27"} namespace:{value:"com.amazon.redshift.core.v3"} language\_specific:{value:"SimpleParameterList.toString(/java.lang/IntegerType,/java.lang/BooleanType)/java.lang/String"} classname:{value:"SimpleParameterList"} function\_or\_attribute\_name:{value:"toString"} args:"/java.lang/IntegerType" args:"/java.lang/BooleanType" return\_type:{value:"/java.lang/String"} declared\_type:{value:"/com.amazon.redshift.core.v3/SimpleParameterList"} signature:{value:"toString(/java.lang/IntegerType,/java.lang/BooleanType)/java.lang/String"}} package\_version:{value:"mvn://com.amazon.redshift:redshift-jdbc42@2.1.0.27"}}} ecosystem:ECOSYSTEM\_MAVEN finding\_categories:FINDING\_CATEGORY\_SECURITY finding\_categories:FINDING\_CATEGORY\_VULNERABILITY relationship:{value:"com.amazon.redshift:redshift-jdbc42@2.1.0.27 is a direct dependency of org.owasp.webgoat:webgoat@2023.9-SNAPSHOT."} latest\_version:{value:"2.1.0.29"} dependency\_file\_paths:"pom.xml" approximation:{} proposed\_version:{value:"2.1.0.28"}} context:{type:CONTEXT\_TYPE\_MAIN id:{value:"default"}}: rpc error: code = InvalidArgument desc = invalid Finding.Meta: embedded message failed validation | caused by: invalid Meta.Description: value length must be at most 1024 bytes

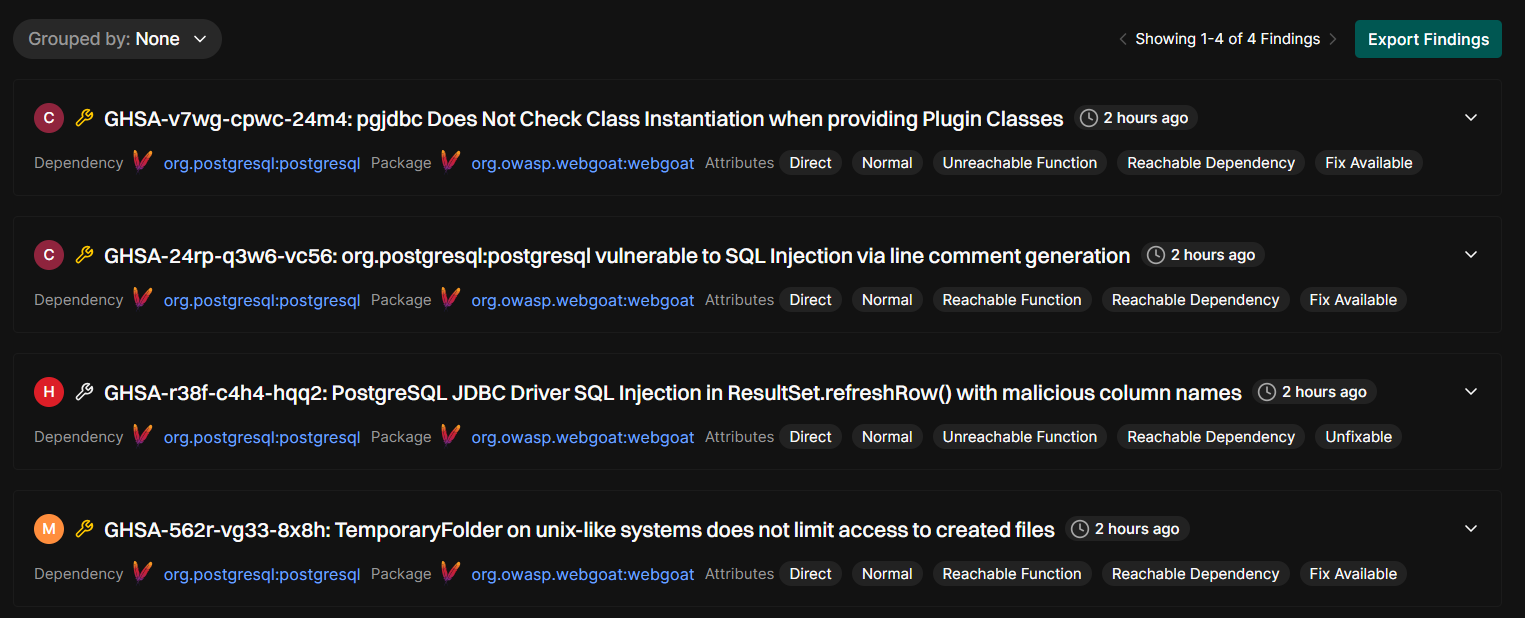
INFO: Finding processing complete ; 59.00s

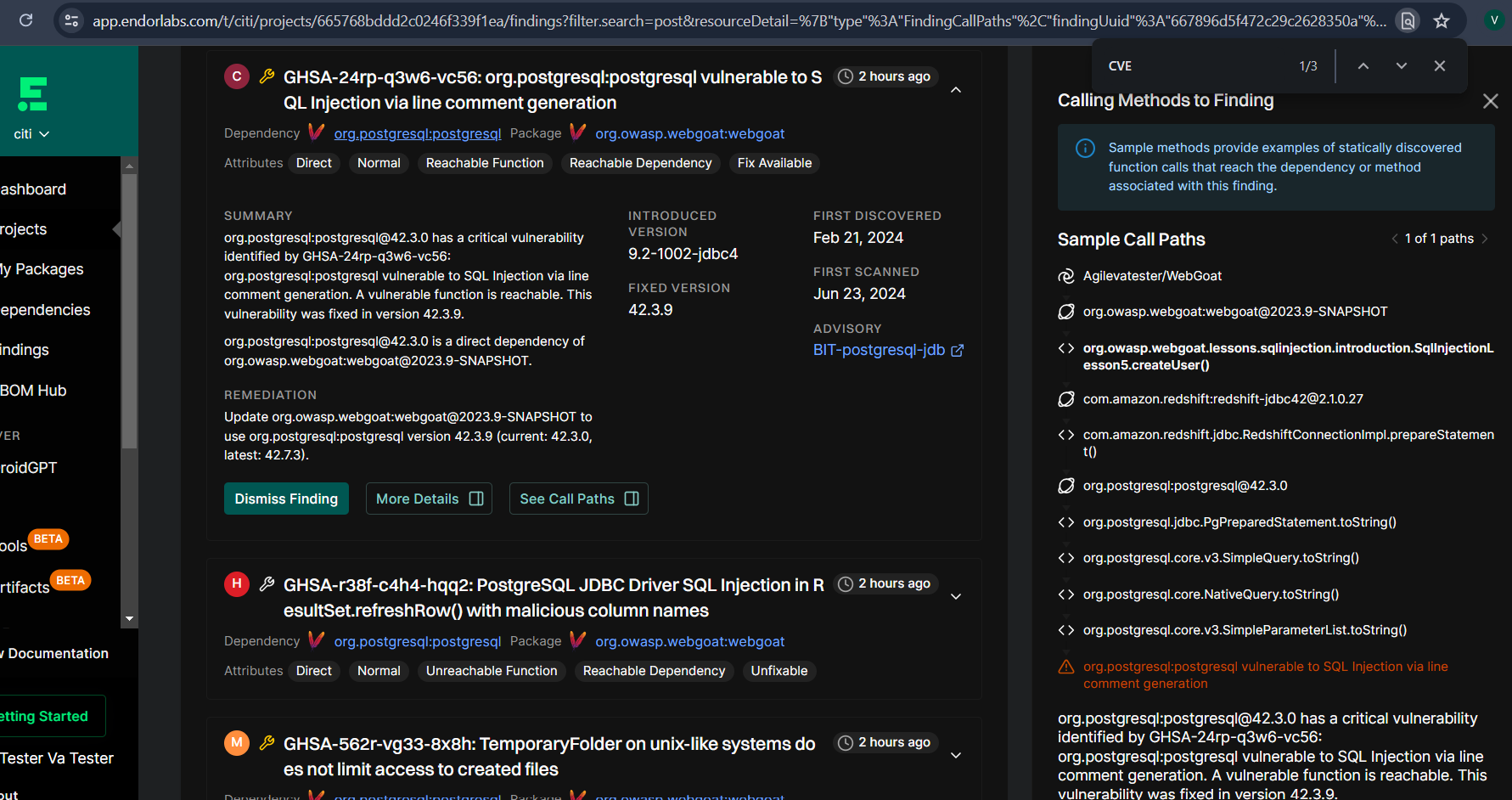




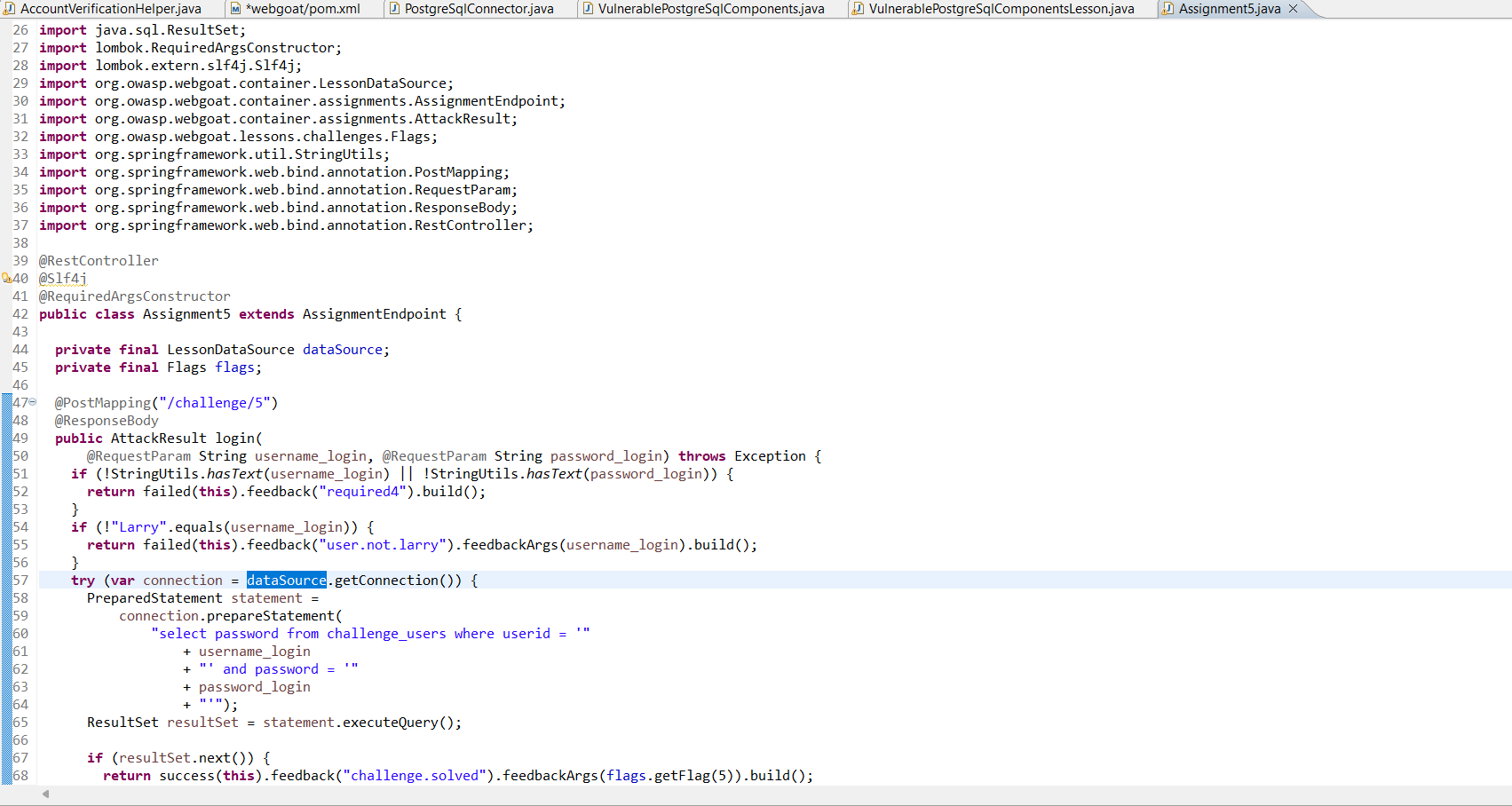


https://app.endorlabs.com/t/citi/projects/665768bddd2c0246f339f1ea/findings?filter.search=post

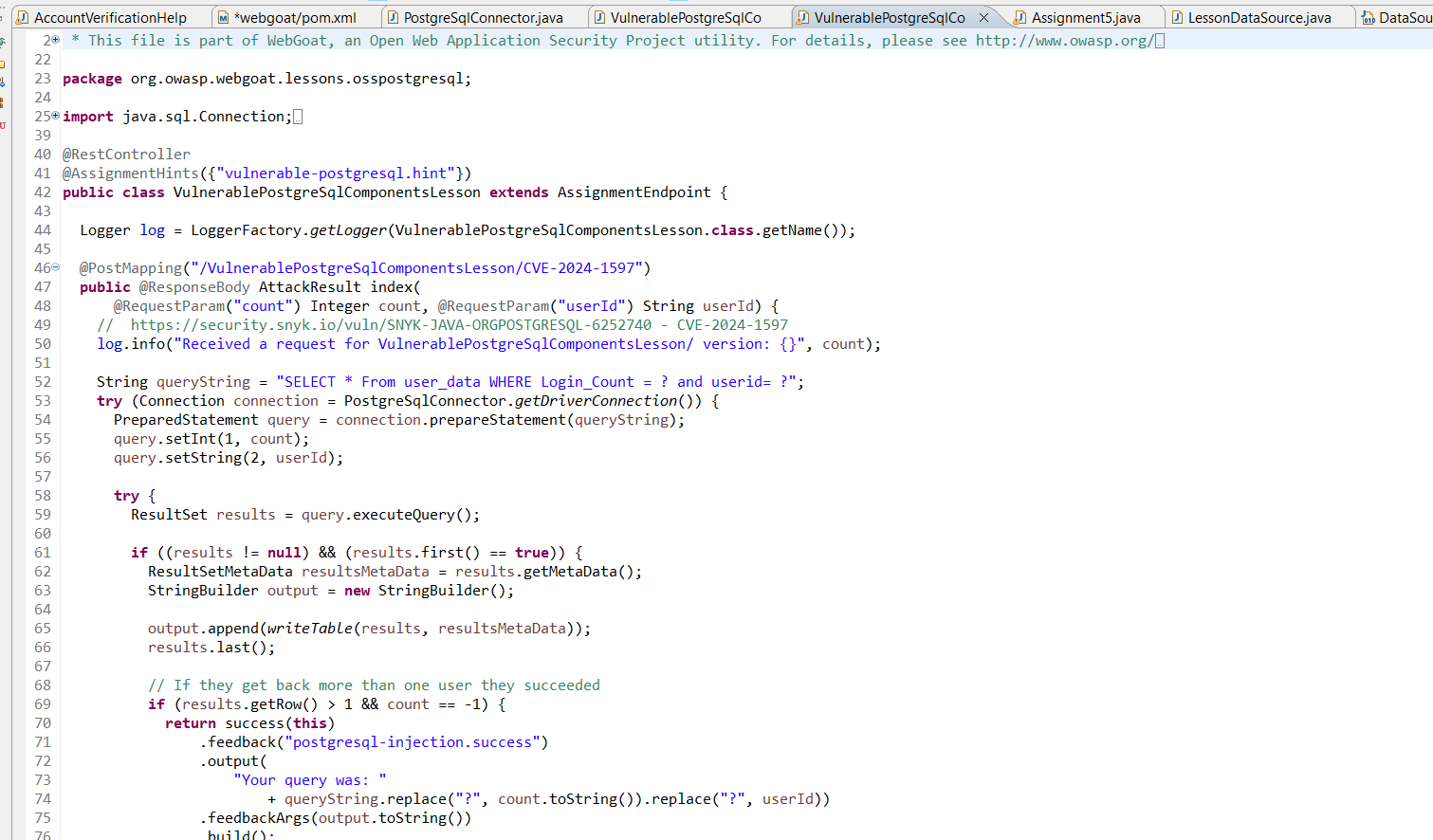


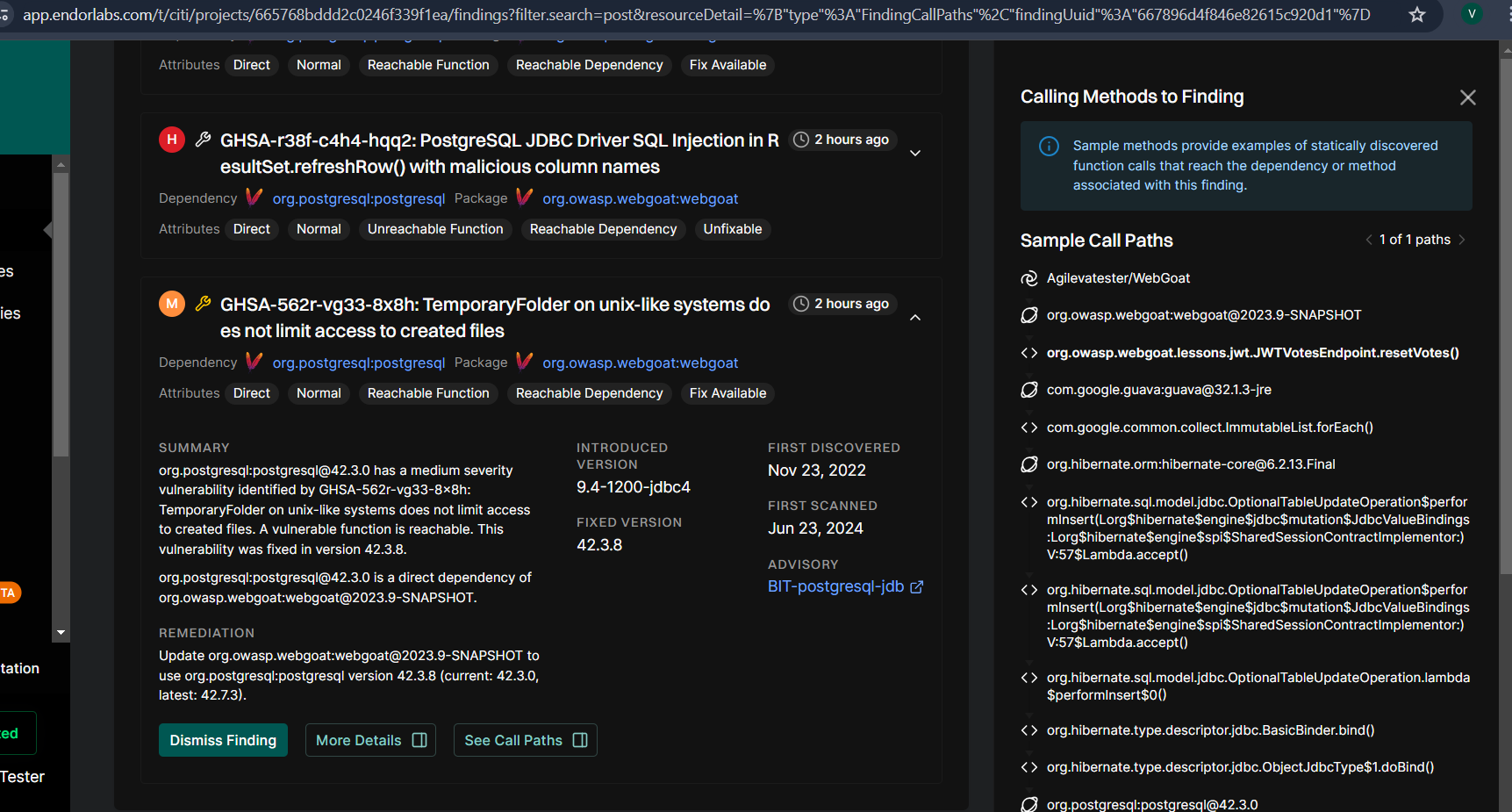


As per finding, Assignment5 is reported in callpath but LessonDataSource is implemented by JDBC Datasoruce



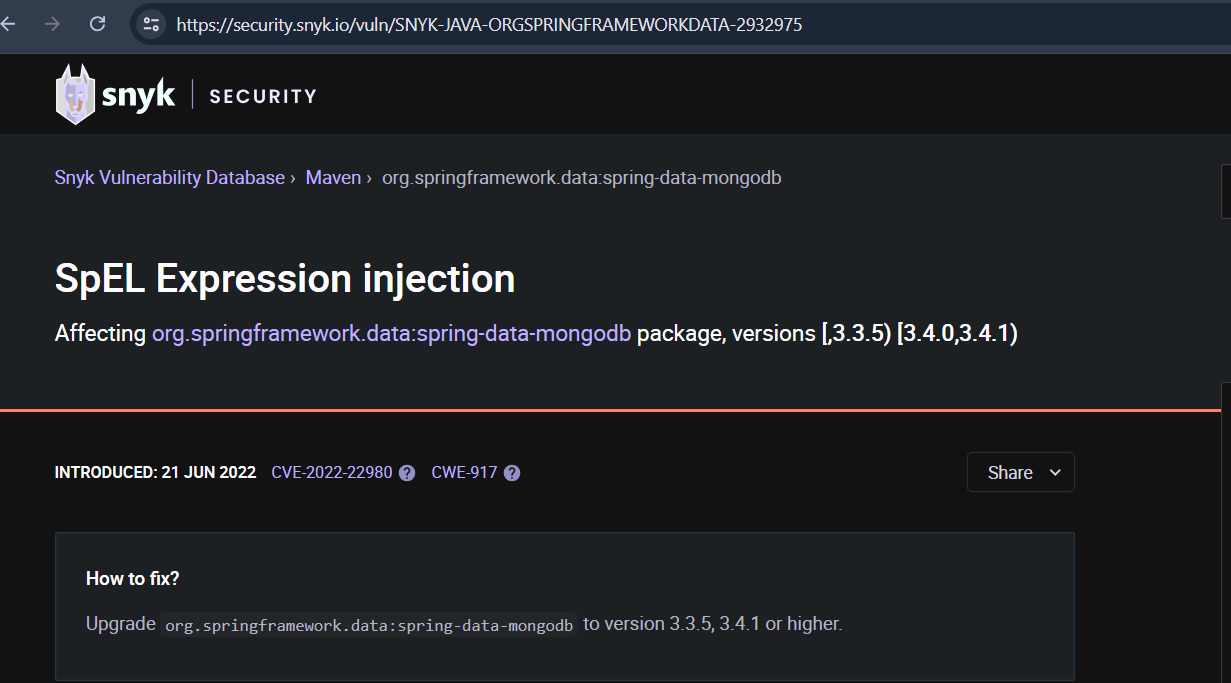
But vulnerable call path is



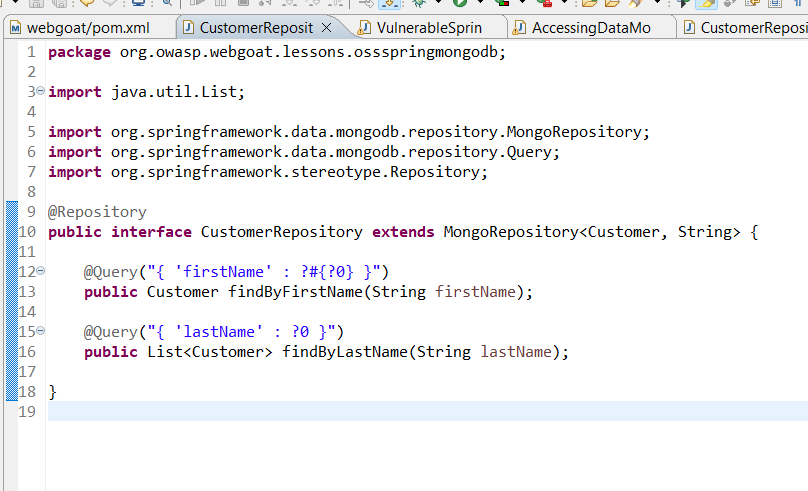


Spring-mongo-db Not reporting finding

<https://security.snyk.io/vuln/SNYK-JAVA-ORGSPRINGFRAMEWORKDATA-2932975>

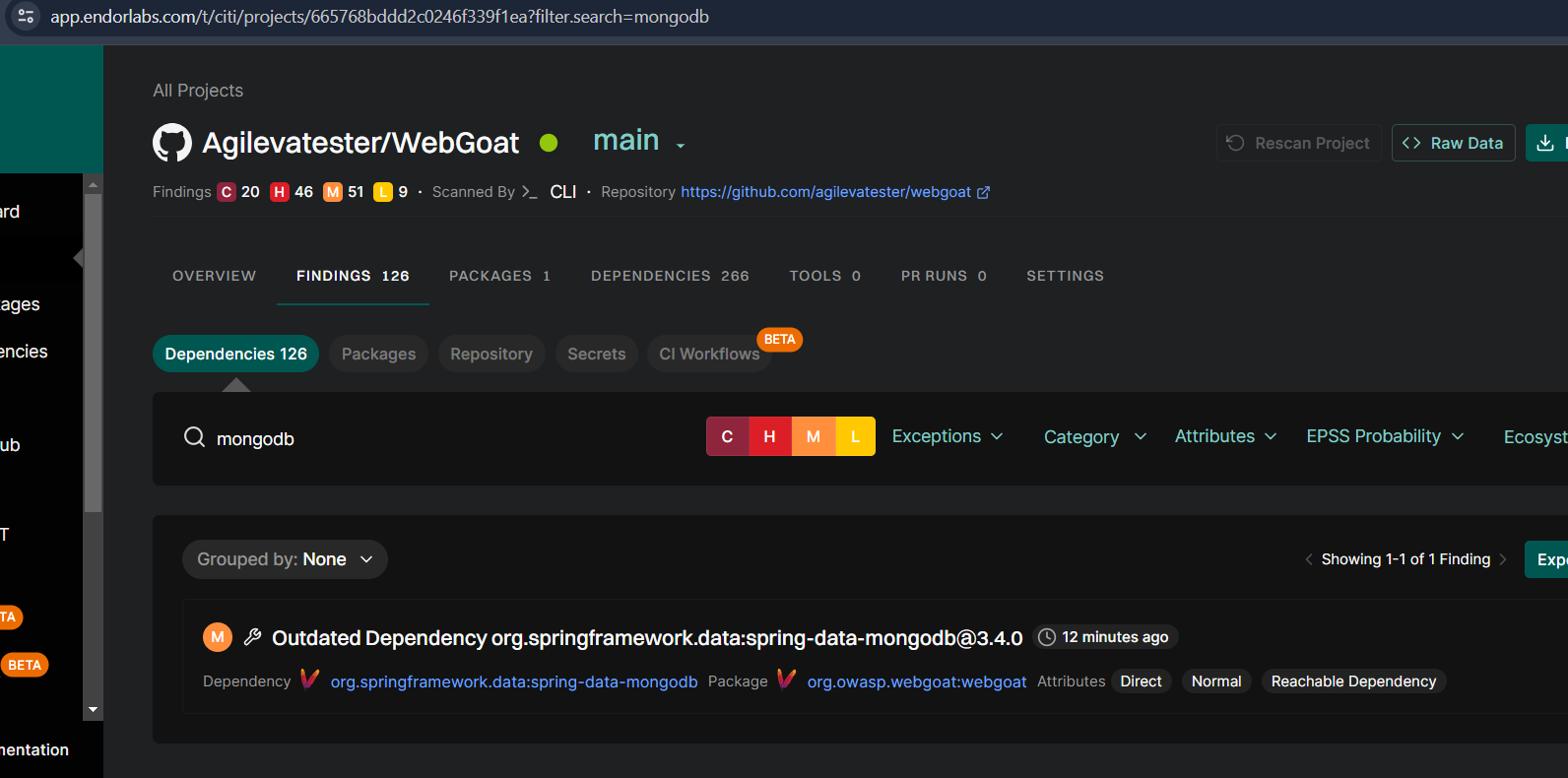


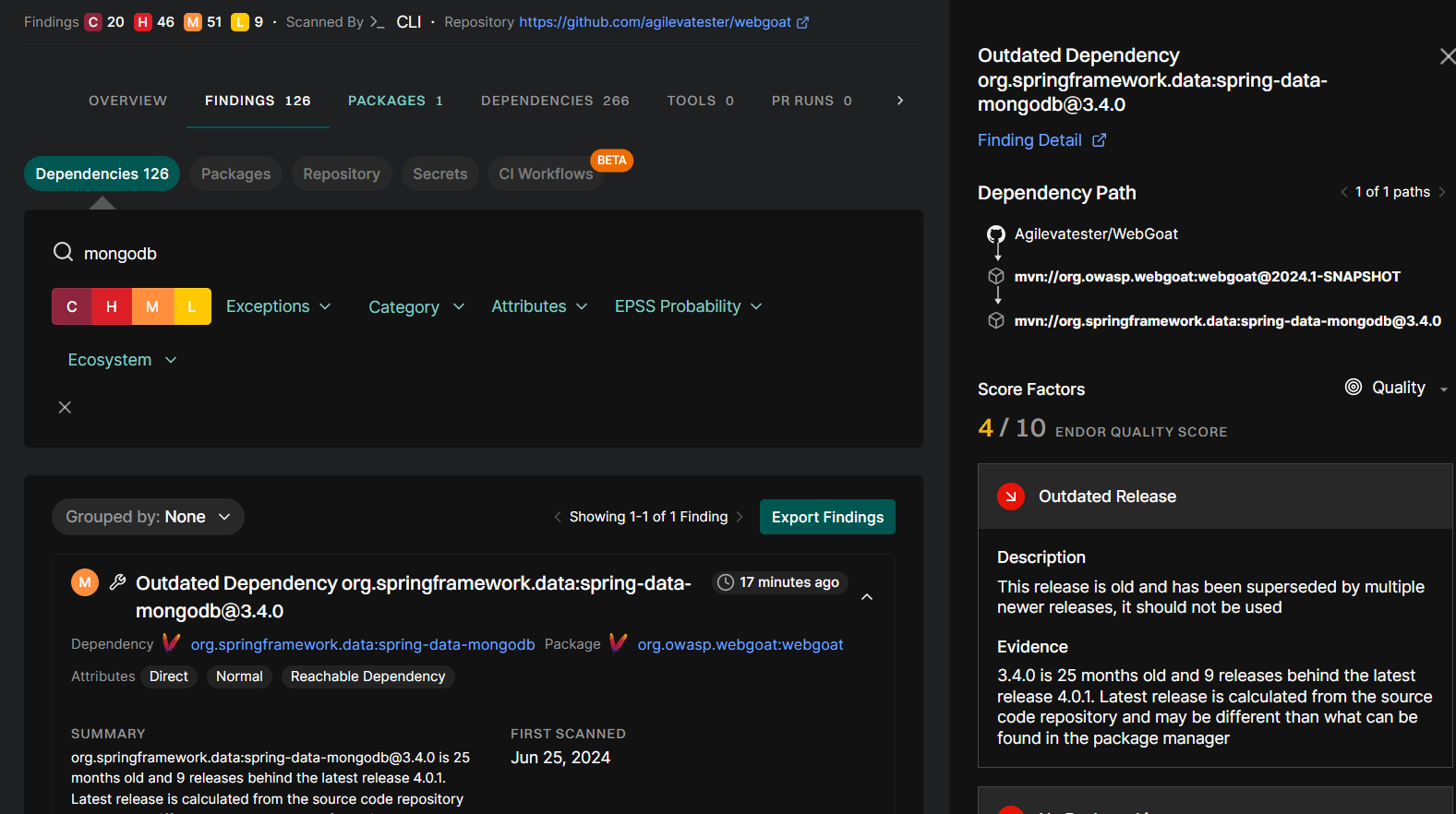




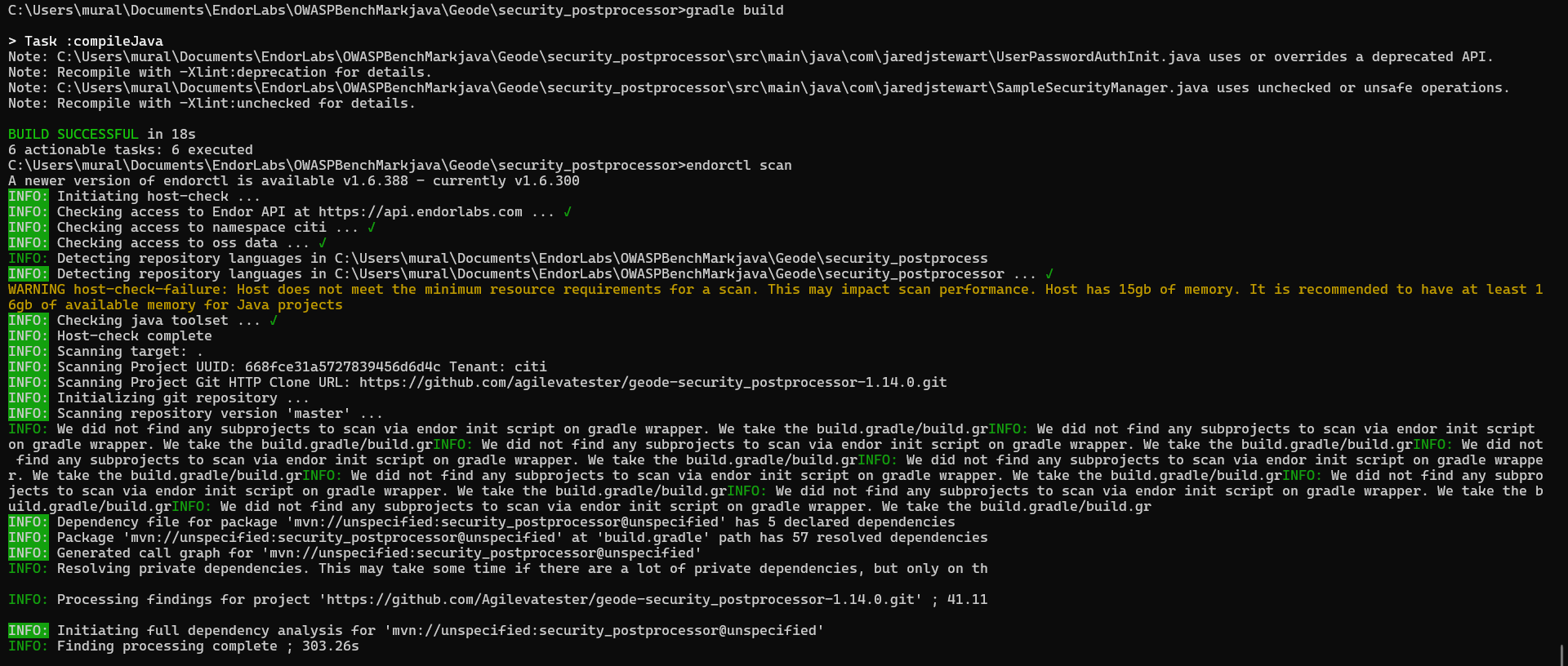
<https://app.endorlabs.com/t/citi/projects/665768bddd2c0246f339f1ea?filter.search=mongodb&resourceDetail=%7B%22findingUuid%22%3A%22667b9969247356e3b127e55c%22%7D>

<https://app.endorlabs.com/t/citi/projects/665768bddd2c0246f339f1ea?filter.search=mongodb>





Took 306 second to scan Gradle Project :



Gradle.build

plugins {

id 'application'

id 'java'

}

repositories {

mavenCentral()

}

dependencies {

testImplementation 'junit:junit:4.11'

testRuntimeOnly 'org.junit.platform:junit-platform-launcher'

implementation 'com.google.guava:guava:21.0'

implementation 'org.apache.geode:geode-core:1.14.0'

implementation 'org.apache.geode:geode-cq:1.14.0'

implementation group: 'com.fasterxml.jackson.core', name: 'jackson-databind', version: '2.17.1'

// https://mvnrepository.com/artifact/com.fasterxml.jackson.core/jackson-core

implementation group: 'com.fasterxml.jackson.core', name: 'jackson-core', version: '2.17.1'

}

application {

mainClass = 'com.jaredjstewart.HelloWorld'

}

tasks.named('test') {

useJUnitPlatform()

}