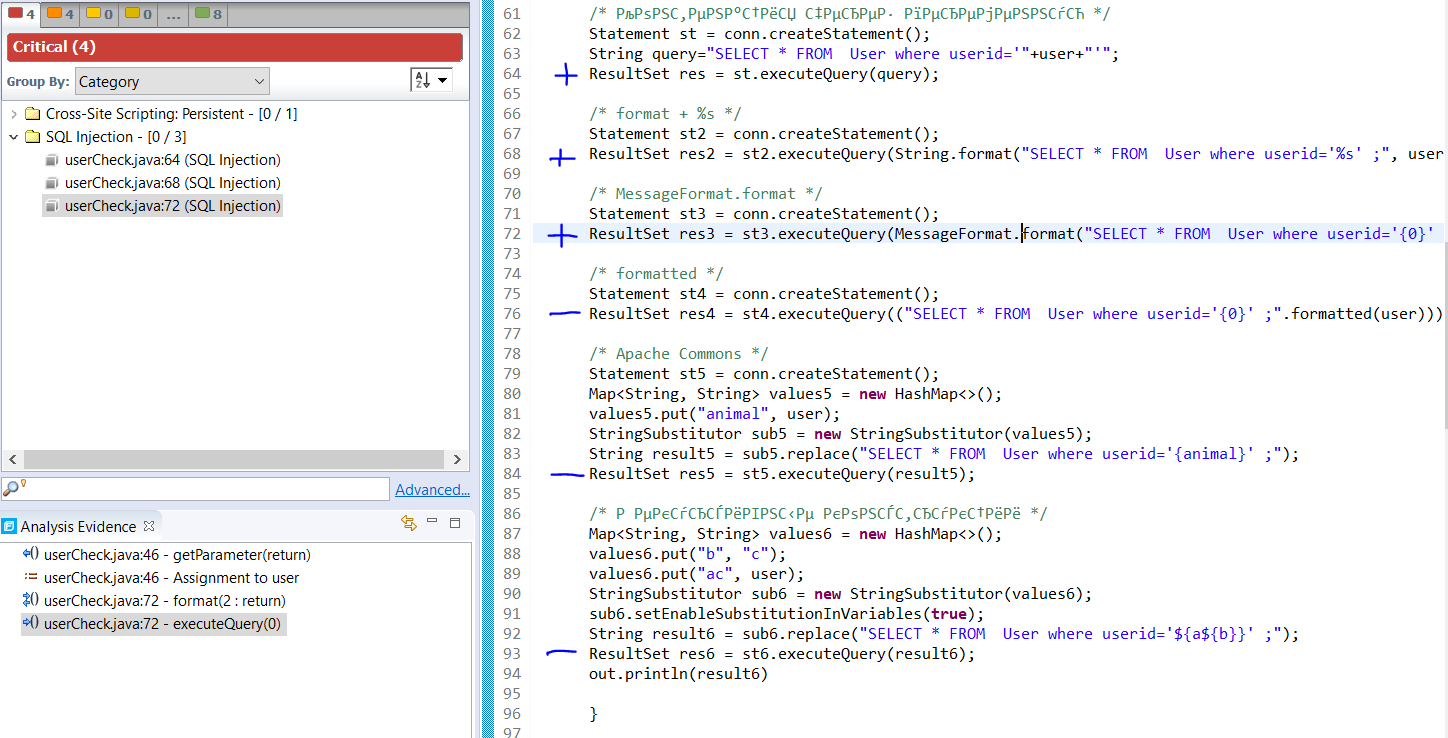
**Сводная таблица**

|  |  |  |  |
| --- | --- | --- | --- |
| **SQL** | **Fortify** | **Semgrep** | **Snyk** |
| Конкатенация ( + переменная) | + | + | + |
| Format | + | + | - |
| MessageFormat | + | + | - |
| Formatted | - | + | - |
| Replace | - | + | - |
| Em | - | + | - |
| Apache Commons | - | + | - |
| AplicationJbdcTemplate.query | - | + | + |
| Apache Commons рекурсивное | - | - | - |
| **Итог:** | **3 из 9** | **7 из 9** | **2 из 9** |
| **XSS + SSTI** | | | |
| Конкатенация + (переменная) | + | + | + |
| String.format + %s | + | + | + |
| MessageFormat.format | - | + | - |
| formatted | - | + | - |
| replace | - | + | - |
| Apache Commons | - | + | - |
| ResponseEntity | - | + | + |
| Document.getEl().innerHtml  DetailTitle.innerHTML  postDiv.innerHTML  span.HTML | - | +/+/+/+ | - |
| Apache Commons Рекурсивные конструкции | - | - | - |
| HTML | - | + | - |
| VelocityContext | - | - | - |
| Return | - | - | + |
| **Итог:** | **2 из 16** | **12 из 16** | **4 из 16** |
| **Command Injection** | | | |
| ProcessBuilder | - | + | + |
| ScriptEngine | - | + | - |
| GroovyShell | - | + | - |
| StandatrEvalutionContext | - | + | - |
| **Итог** | **0 из 4** | **4 из 4** | **1 из 4** |
| **Docker** | | | |
| no-new-privileges | - | + | - |
| **Итог:** | **0 из 1** | **1 из 1** | **0 из 1** |
| **Hardcode** | | | |
| Private key | - | + | - |
| JWT Token | - | + | - |
| Password | + | - | + |
| **Итог:** | **0 из 3** | **2 из 3** | **1 из 3** |
| **SSRF** | | | |
| URL | - | + | + |
| HttpRequest | - | + | + |
| Jsoup | - | + | + |
| SecurityUtil | - | - | - |
| HttpUtil | - | - | + |
| HttpService | - | - | + |
| **Итог** | **0 из 6** | **3 из 6** | **5 из 6** |
| **RFI** | | | |
| getForObject | - | + | + |
| FileInputStream | - | + | + |
| **Итог:** | **0 из 2** | **2 из 2** | **1 из 2** |
| **Debug** | | | |
| Exception | - | + | - |
| **Итог:** | **0 из 1** | **1 из 1** | **0 из 1** |
| **CSRF** | | | |
| CSRF token | +- | + | - |
| **Итог:** | **0.5 из 1** | **1 из 1** | **0 из 1** |
| **LFI** | | | |
| Exception | + | + | + |
| **Итог:** | **1 из 1** | **1 из 1** | **1 из 1** |
| **Cors** | | | |
| Access-Control.. : \* | - | + | + |
| Пользовательский ввод в origin | + | - | + |
| **Итог** | **1 из 2** | **1 из 2** | **2 из 2** |
| **CRLF** | | | |
| addHeader | + | + | + |
| setHeader | + | + | + |
| cookie | + | + | - |
| Использование переменной | + | + | + |
| **Итог** | **4 из 4** | **4 из 4** | **3 из 4** |
| **Deserialize** | | | |
| Json | - | + | - |
| ObjectInputStream | - | + | + |
| Yaml | - | + | + |
| **Итог** | **0 из 3** | **3 из 3** | **2 из 3** |
| **Traversal** | | | |
| Patchs.get | - | + | + |
| File | - | - | + |
| **Итог** | **0 из 2** | **2 из 2** | **2 из 2** |
| **Cookie** | | | |
| HttpOnly | - | + | + |
| Secure | - | + | + |
| Patch | + | – | - |
| **Итог** | **1 из 3** | **2 из 3** | **1 из 3** |
| **OpenRedirect** | | | |
| Redirect | - | + | + |
| SetHendler | + | - | + |
| Response.sendRedirect | + | + | + |
| Forward Safe (False) | + | + | + |
| SecurityUtil | + | + | - |
| WhiteList (False) | + | + | - |
| **Итог** | **5 из 6** | **5 из 6** | **4 из 6** |
| **WebSocket** | | | |
| Socket | - | - | + |
| **Итог** | **0 из 1** | **0 из 1** | **1 из 1** |
| **XXE** | | | |
| DocumentBulder | - | + | + |
| SAXParser | - | + | - |
| XMLReader | - | + | - |
| **Итог** | **0 из 3** | **3 из 3** | **1 из 3** |
| **СУПЕР ИТОГ:** | **17.5 / 68** | **54 / 68** | **31/68** |
| **Процентное:** | **25.7%** | **79%** | **54.5%** |

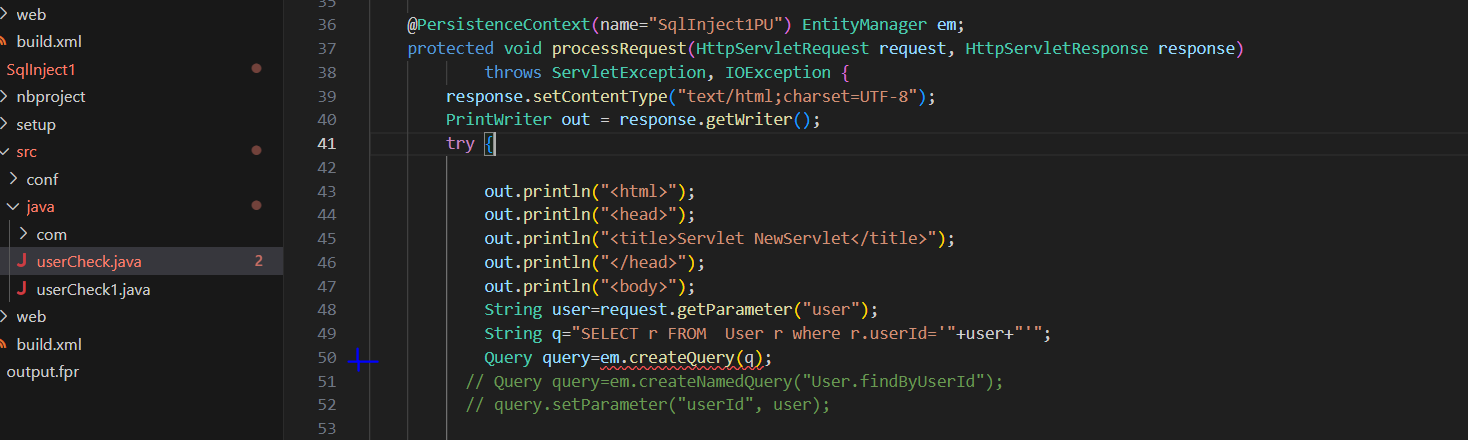
**SQL Injection**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Конкатенация ( + переменная) | + | + | + |
| Format | + | + | - |
| MessageFormat | + | + | - |
| Formatted | - | + | - |
| Replace | - | + | - |
| Em | - | + | - |
| Apache Commons | - | + | - |
| AplicationJbdcTemplate.query | - | + | + |
| Apache Commons рекурсивное | - | - | - |
| **Итог:** | **3 из 9** | **7 из 9** | **2 из 9** |

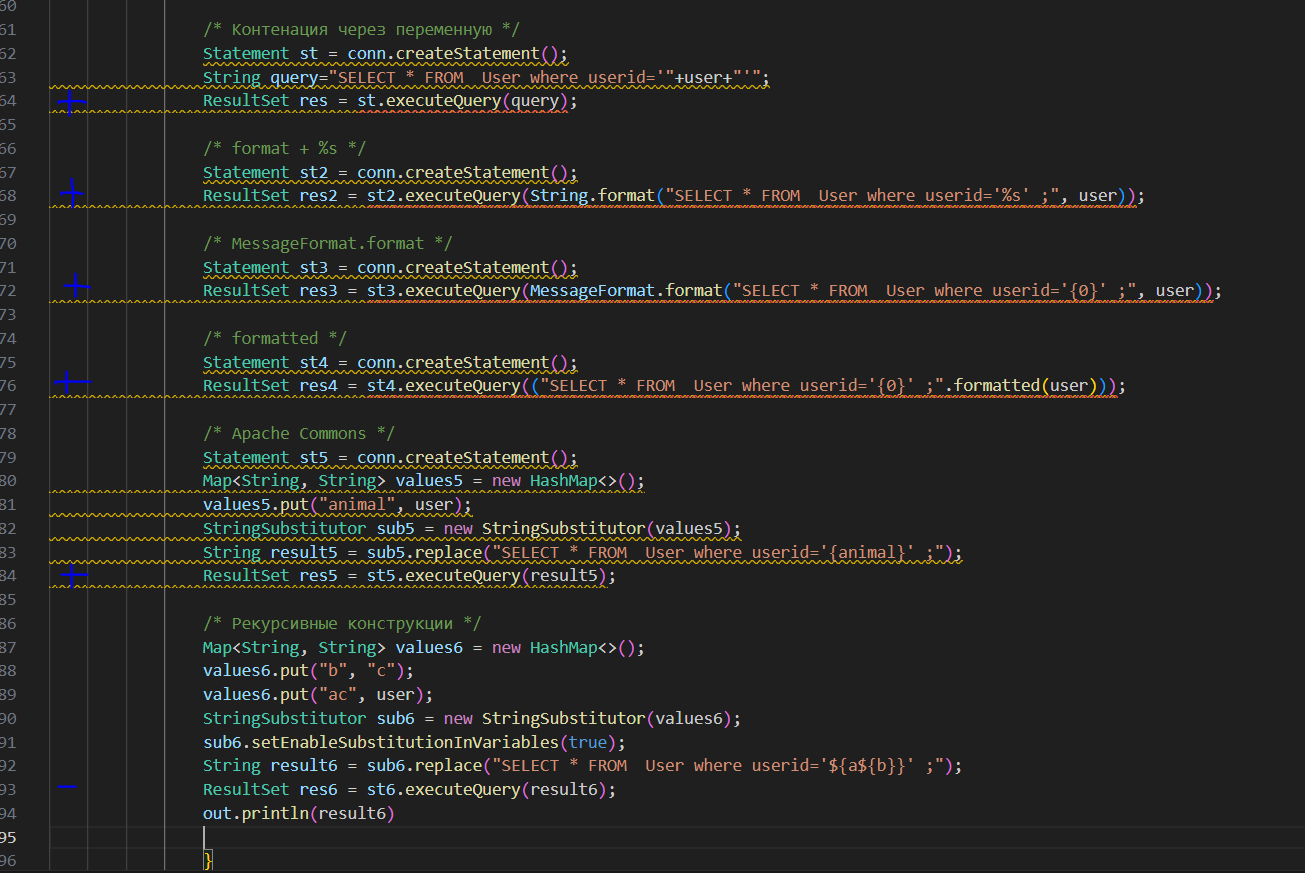
**Fortify:**

**Semgrep:**

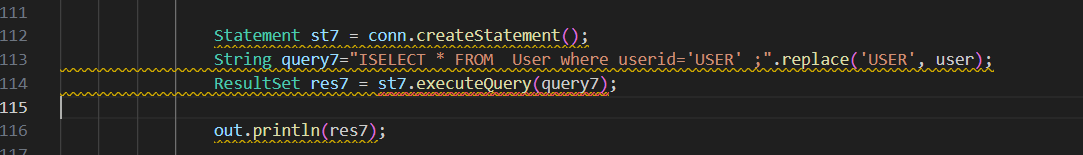
**Em**



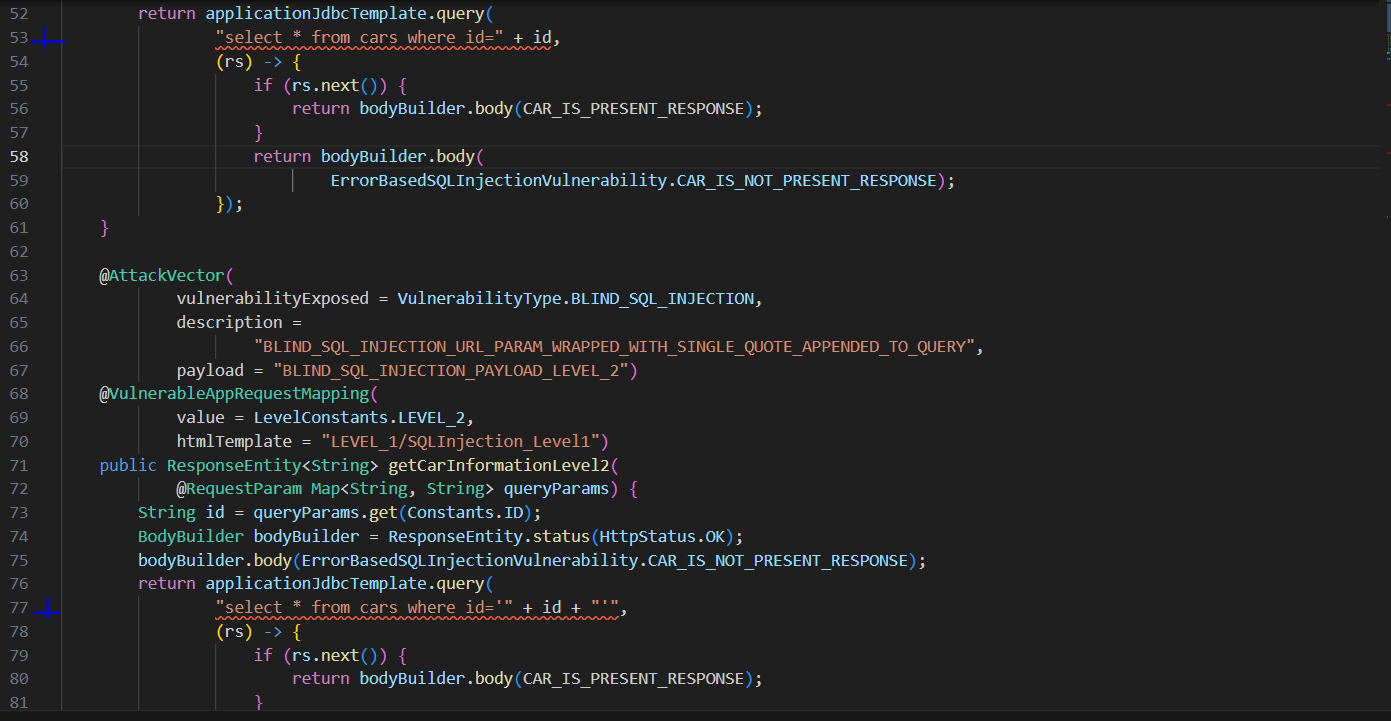
**Конкатенация, Format, MessageFormat, Formatted, Apache Commons**



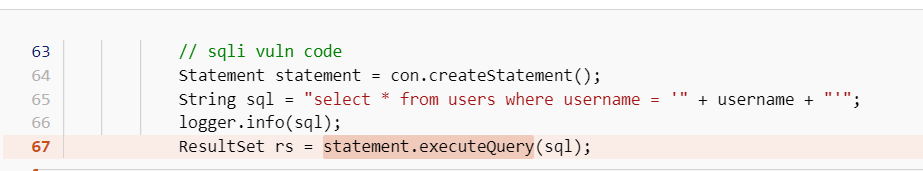
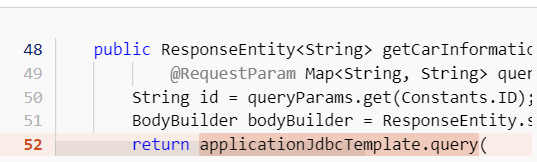
**Replace**



**AplicationJbdcTemplate.query**

****

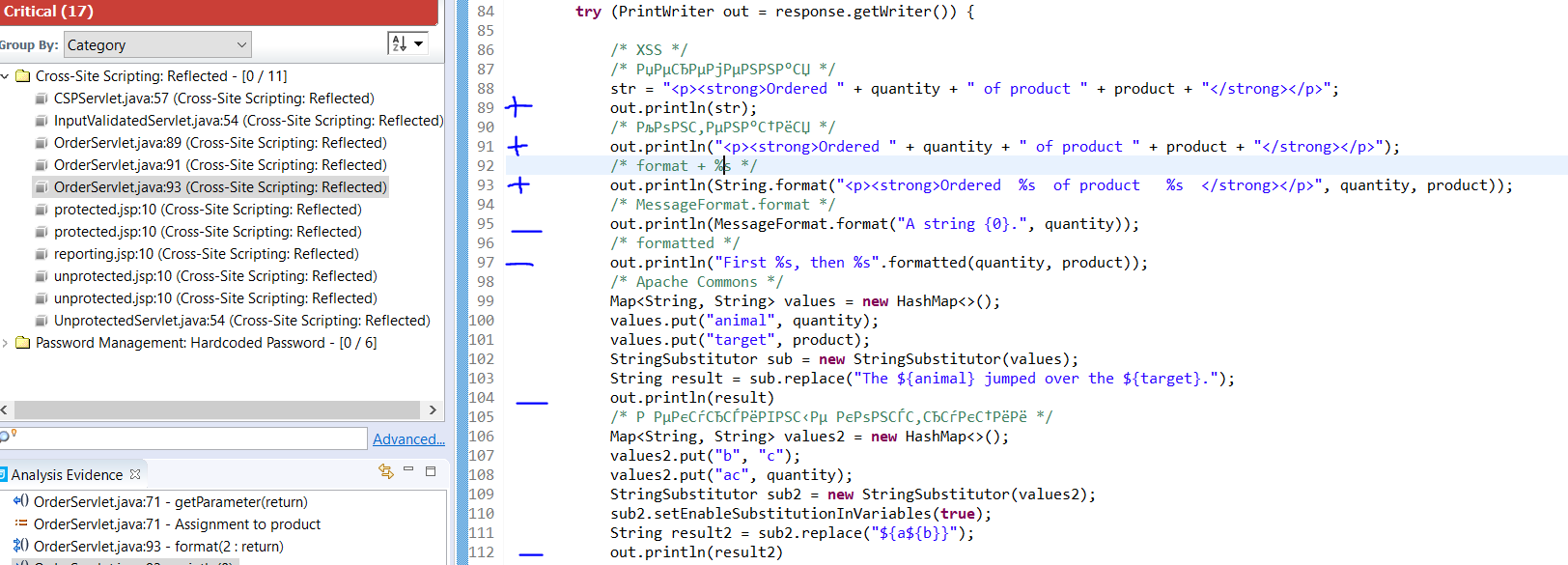
**Snyk**

****

**XSS + SSTI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Конкатенация + (переменная) | + | + | + |
| String.format + %s | + | + | + |
| MessageFormat.format | - | + | - |
| formatted | - | + | - |
| replace | - | + | - |
| Apache Commons | - | + | - |
| ResponseEntity | - | + | + |
| Document.getEl().innerHtml  DetailTitle.innerHTML  postDiv.innerHTML  span.HTML | - | +/+/+/+ | - |
| Apache Commons Рекурсивные конструкции | - | - | - |
| HTML | - | + | - |
| VelocityContext | - | - | - |
| Return | - | - | + |
| **Итог:** | **2 из 16** | **12 из 16** | **4 из 16** |

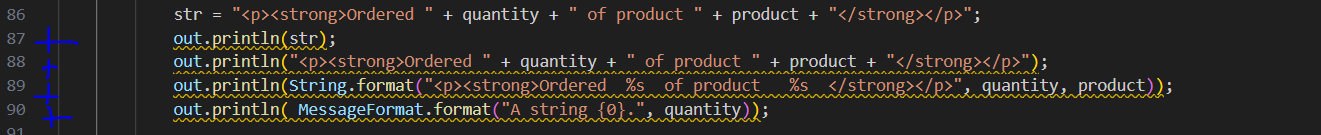
**Fortify:**

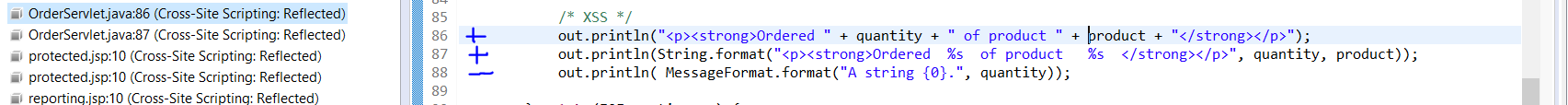
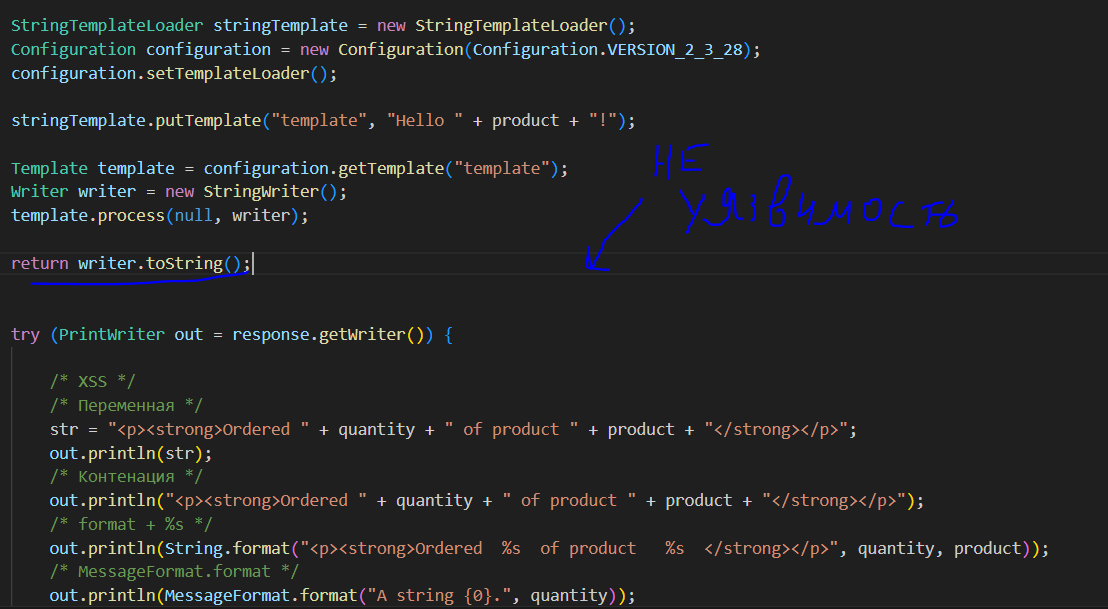
****

****

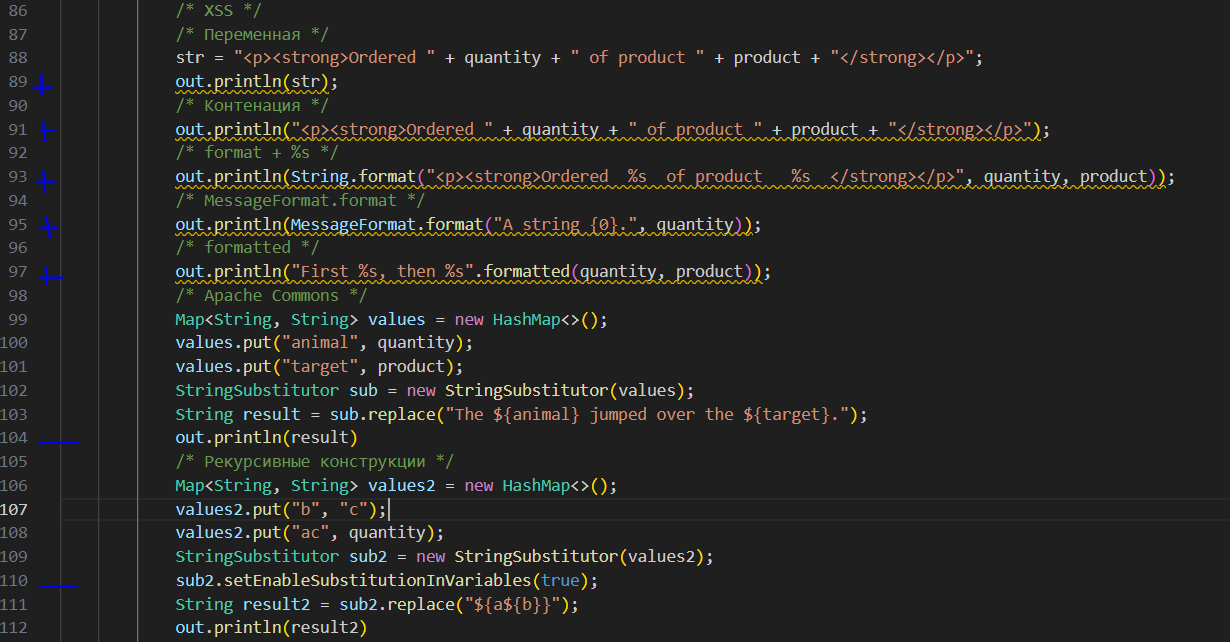
**Semgrep:**

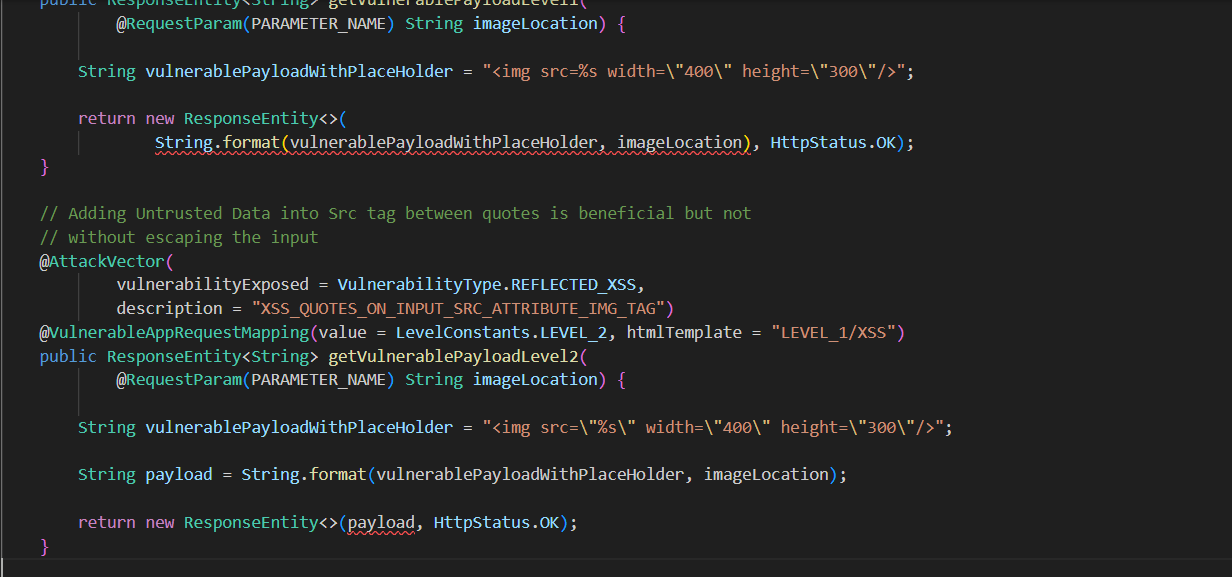
**Конкатенация, String.format, MessageFormat.format**

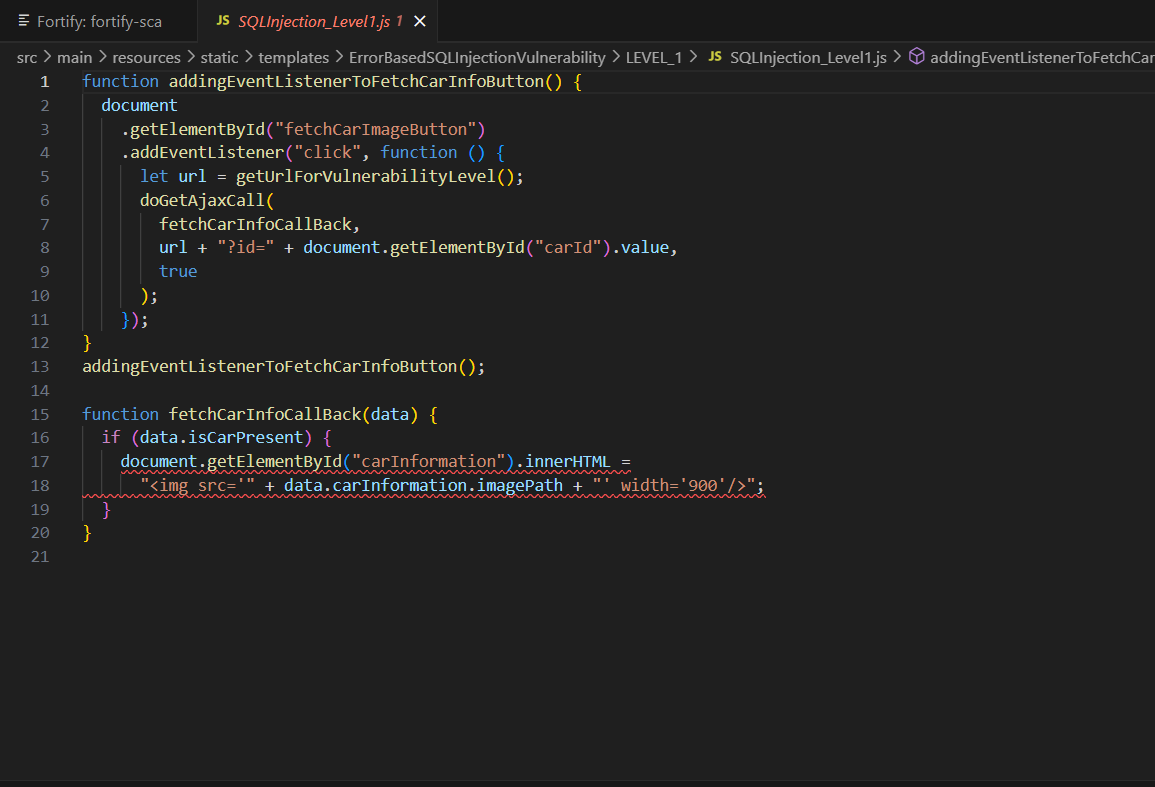
****

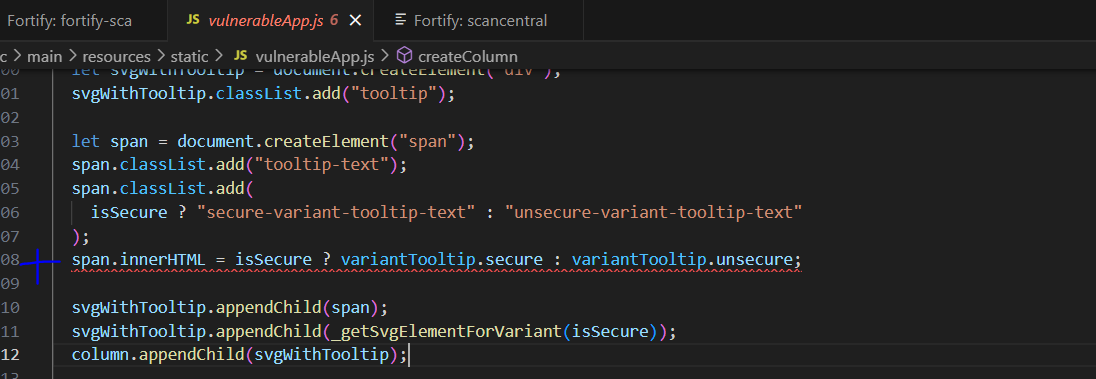
**Проверка на потоки **

Replace**,** Apache Commons, Apache Commons Рекурсивные конструкции

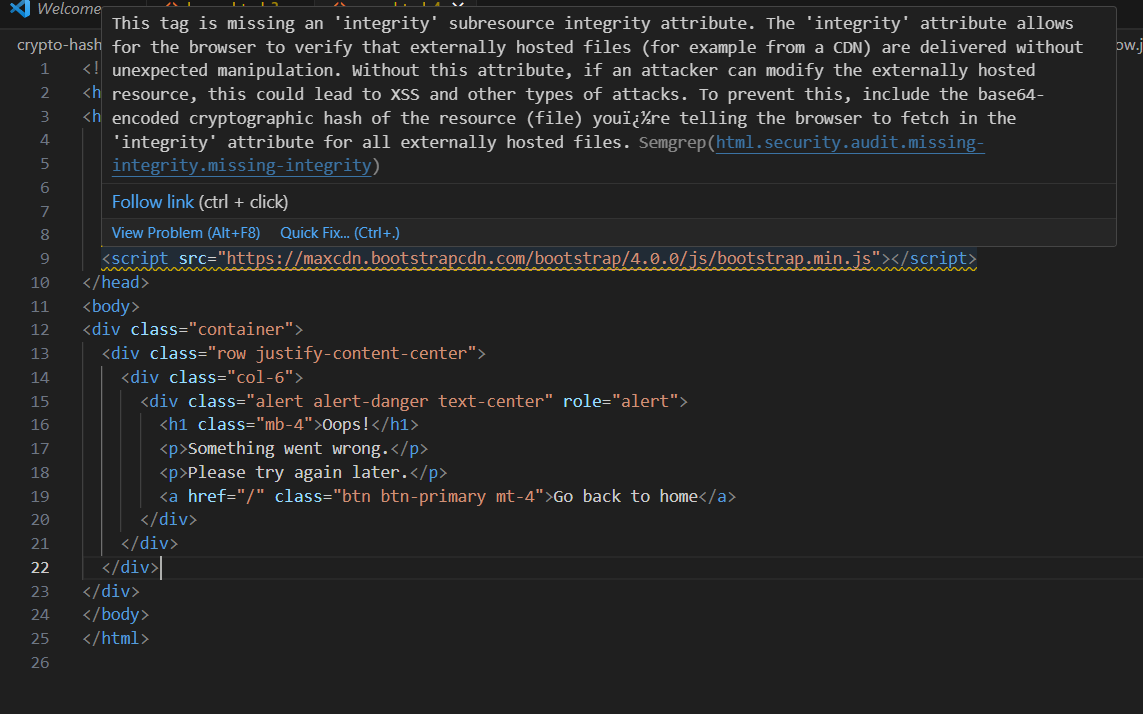
****

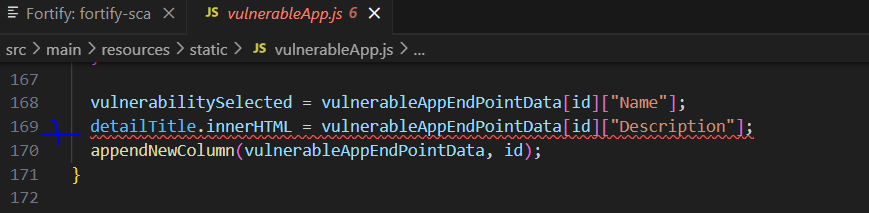
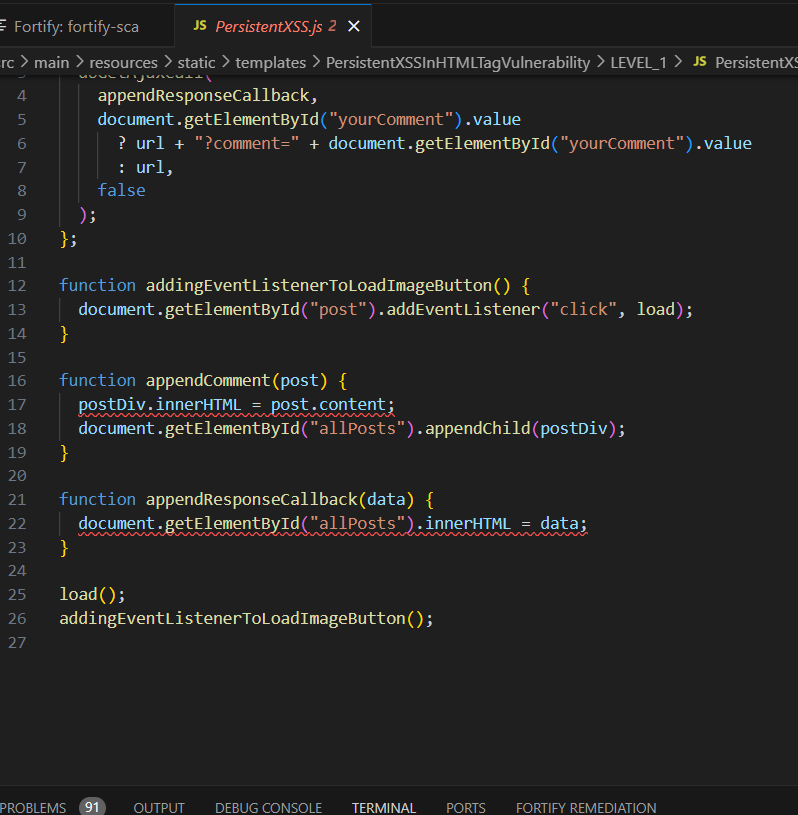
**ResponseEntity **

**Document.getEl().innerHtml**

**span.HTML** 

**HTML**

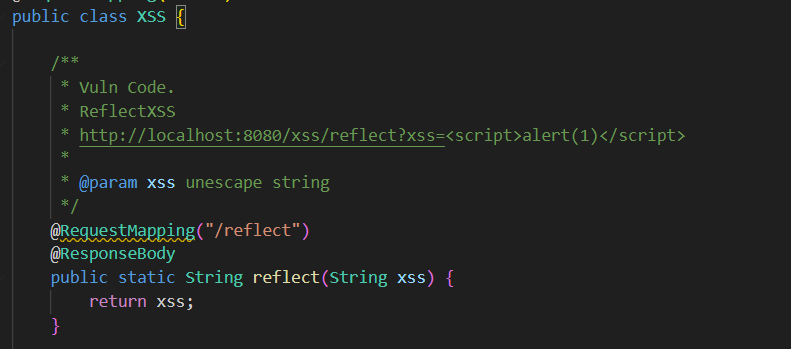
****

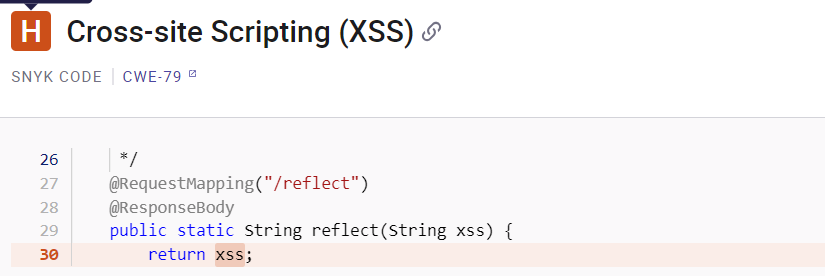
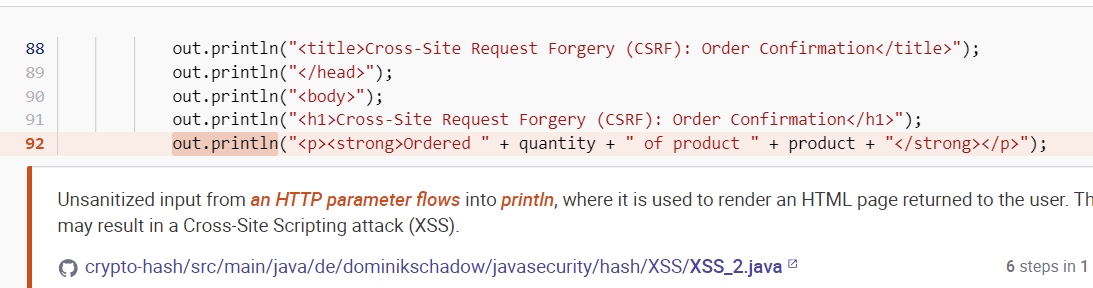
**DetailTitle.innerHTML, postDiv.innerHTML**

**VelocityContext**

****

**Return**

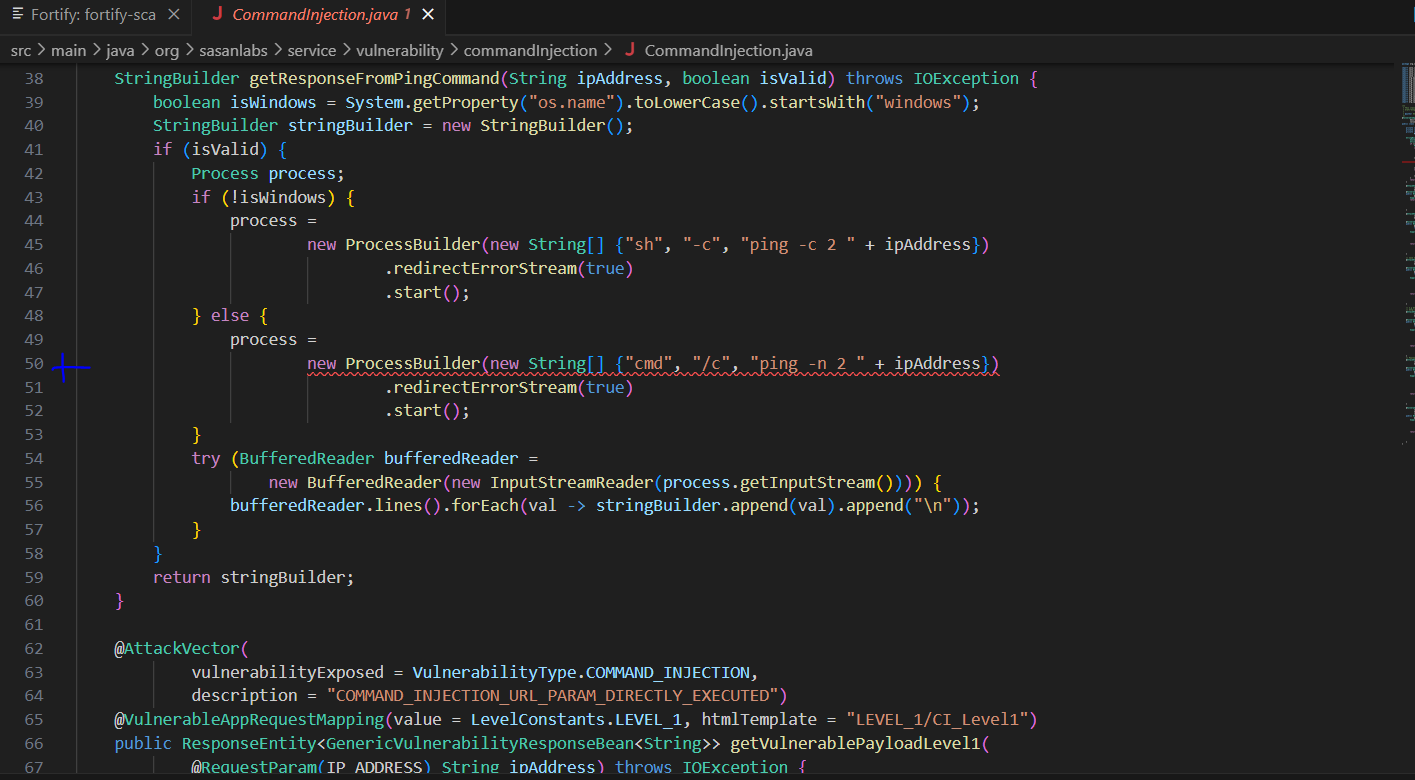
****

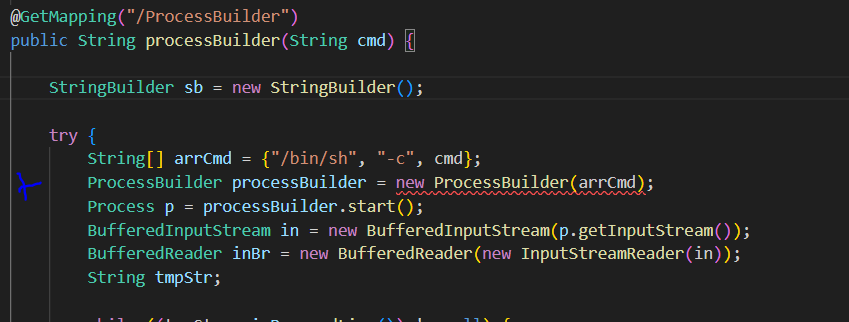
**Snyk **

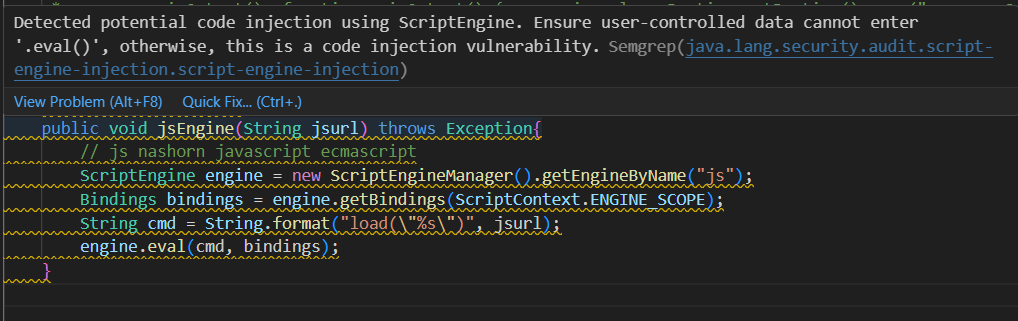
**Command injection**

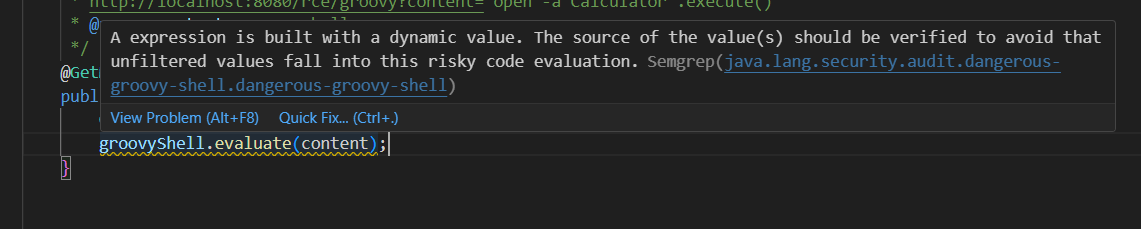
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| ProcessBuilder | - | + | + |
| ScriptEngine | - | + | - |
| GroovyShell | - | + | - |
| StandatrEvalutionContext | - | + | - |
| **Итог** | **0 из 4** | **4 из 4** | **1 из 4** |

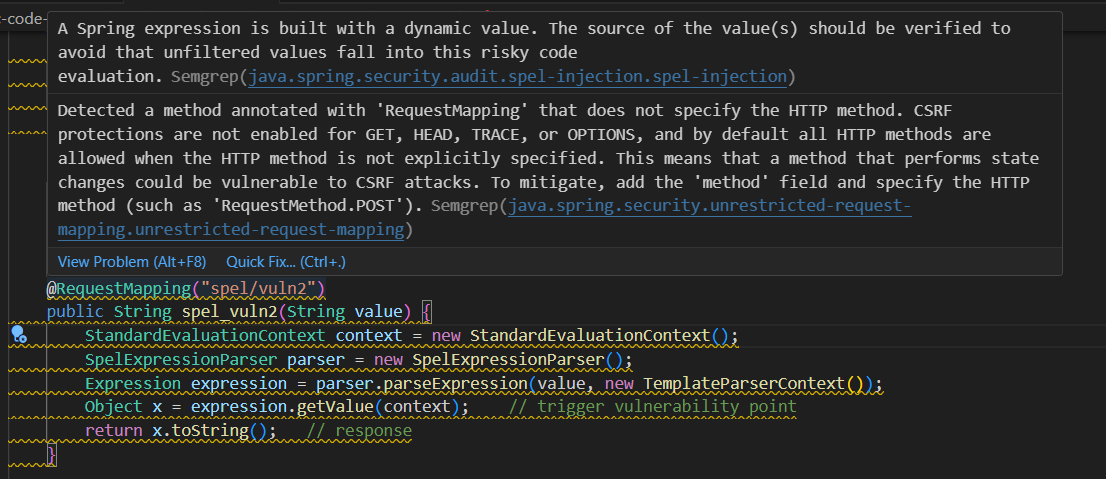
**Semgrep**

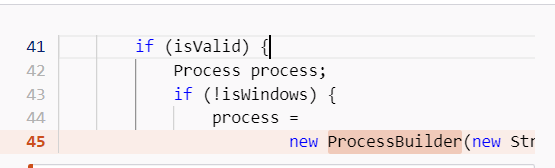


****

****

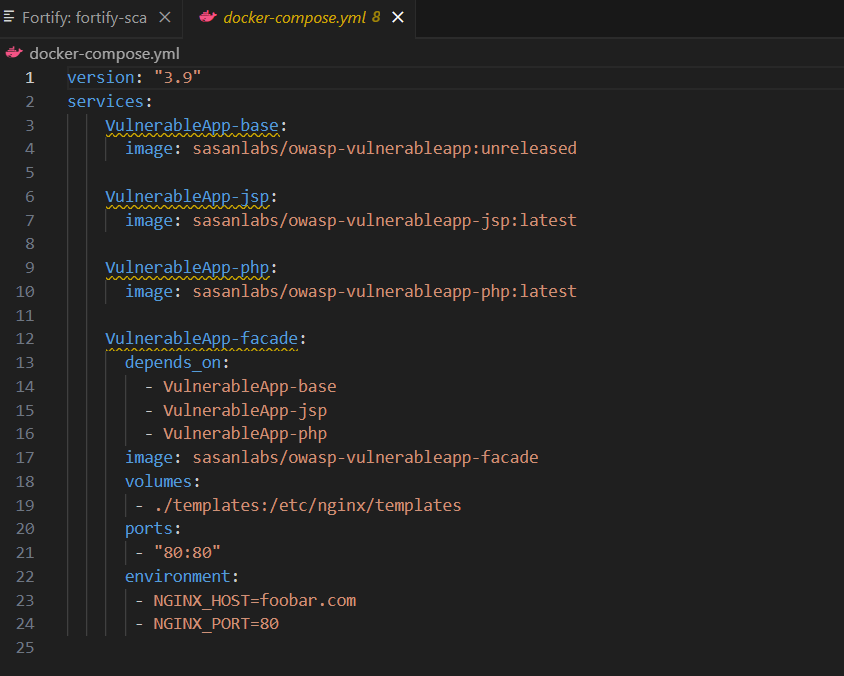
****

****

**Snyk **

**Docker**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| no-new-privileges | - | + | - |
| **Итог:** | **0 из 1** | **1 из 1** | **0 из 1** |

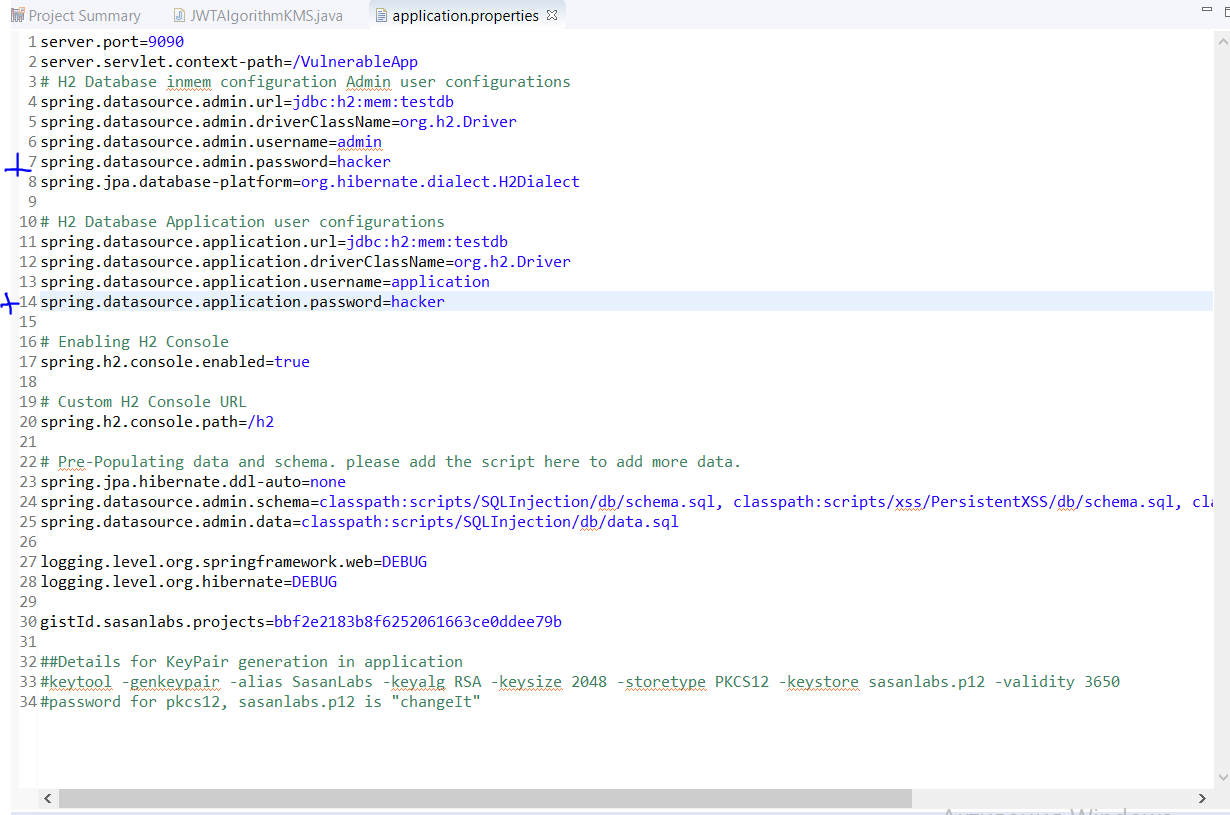
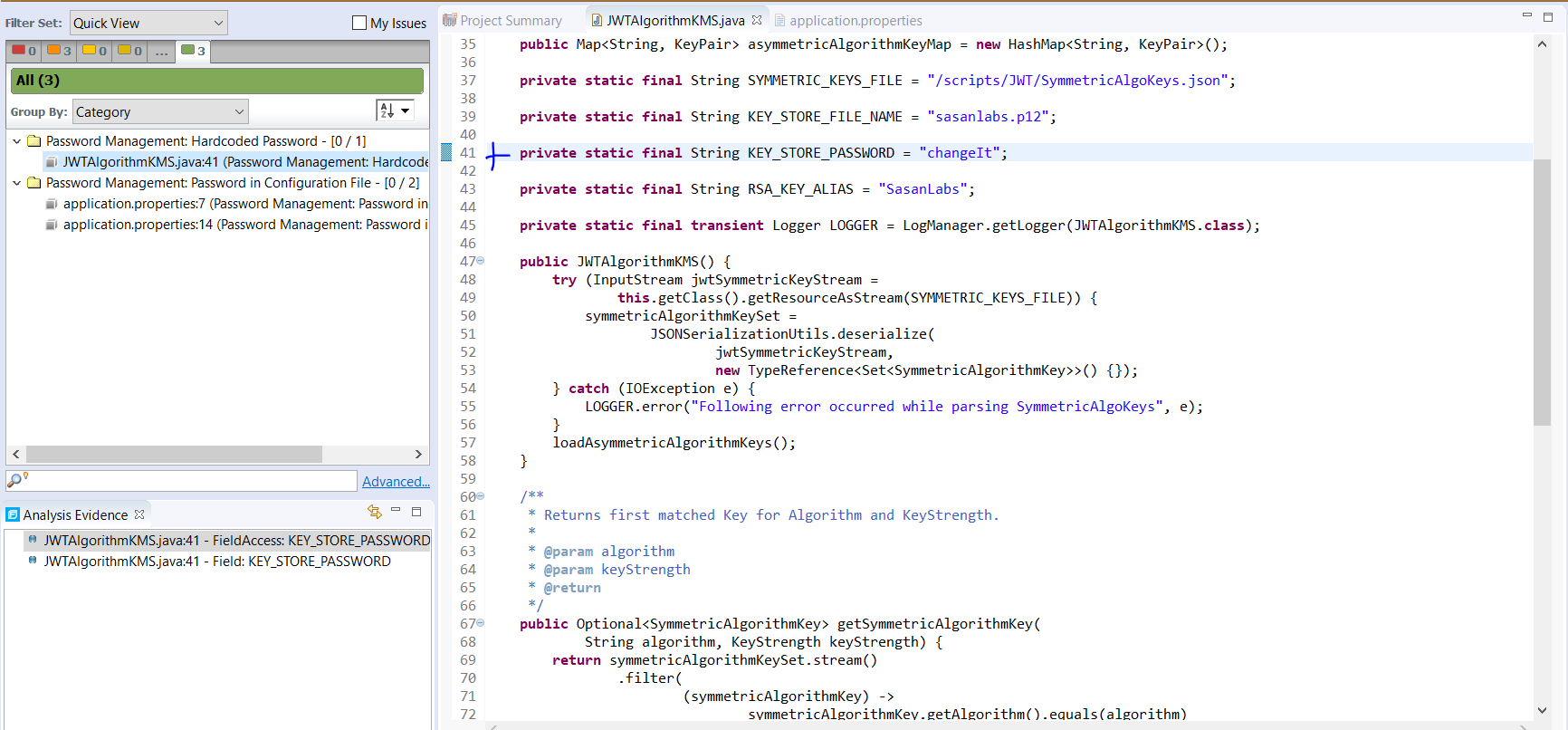
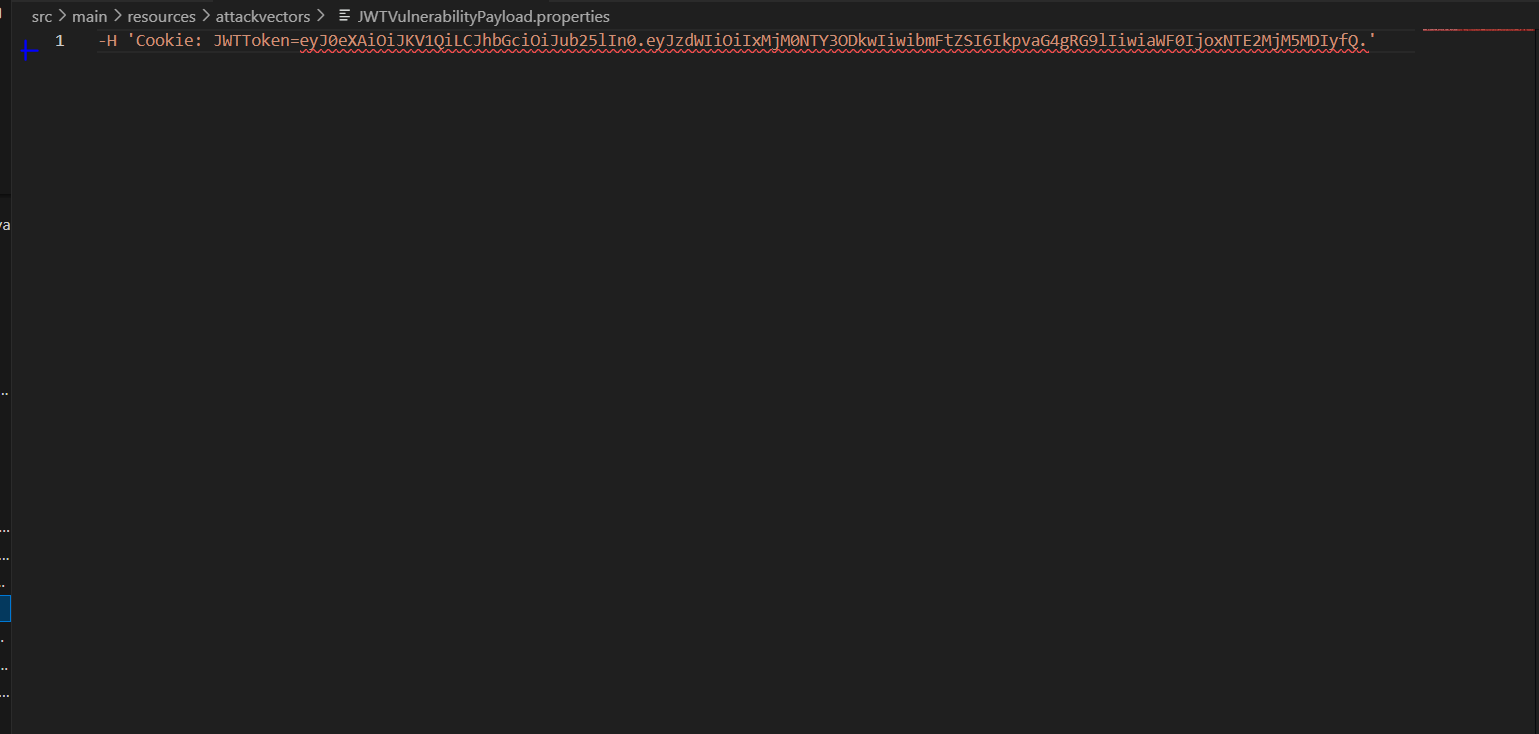
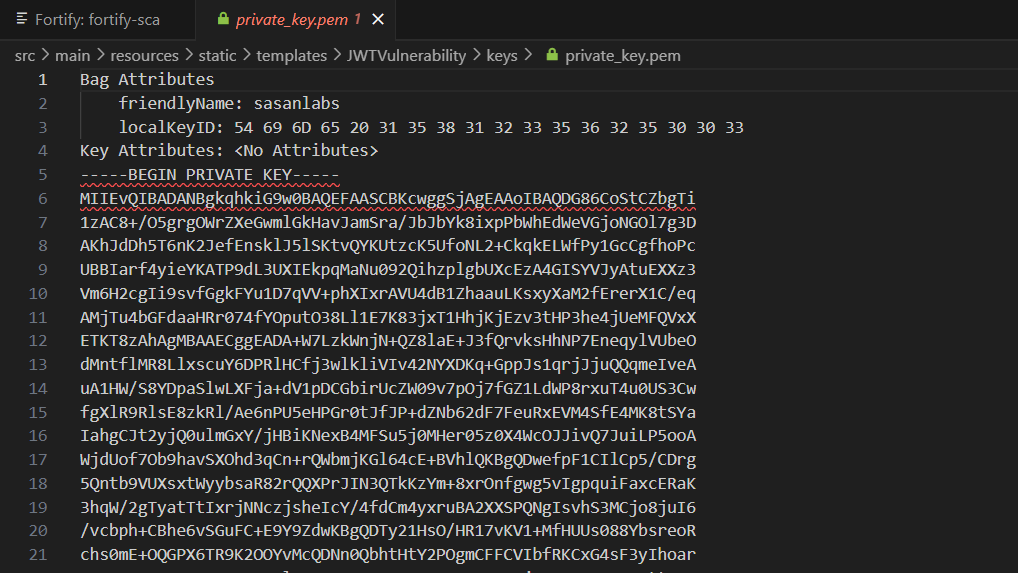
****

Service 'VulnerableApp-base' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security\_opt' to prevent this.Semgrep[yaml.docker-compose.security.no-new-privileges.no-new-privileges](https://sg.run/0n8q)

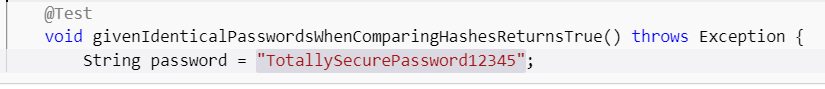
Service 'VulnerableApp-base' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read\_only: true' to this service to prevent this.

**Hardcode**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Private key | - | + | - |
| JWT Token | - | + | - |
| Password | + | - | + |
| **Итог:** | **0 из 3** | **2 из 3** | **1 из 3** |

****

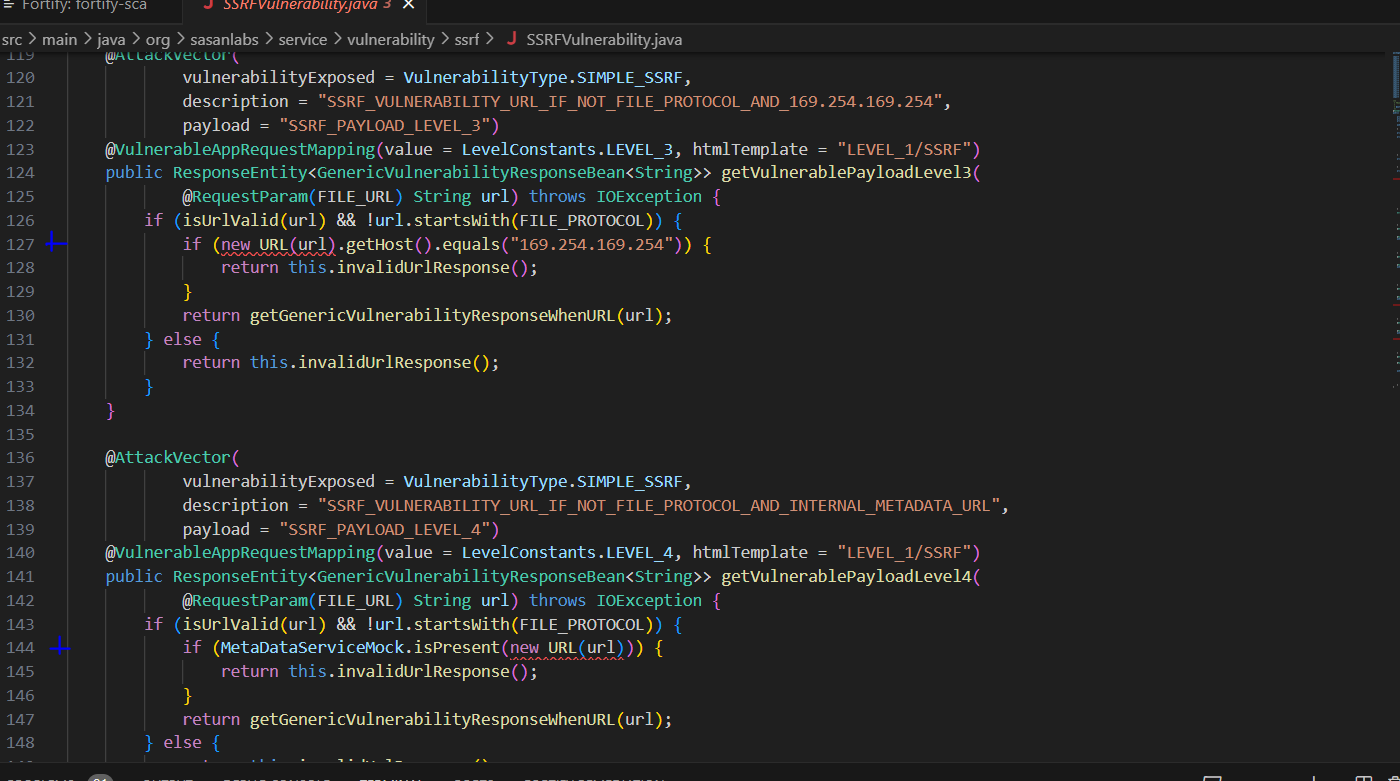
**Snyk**

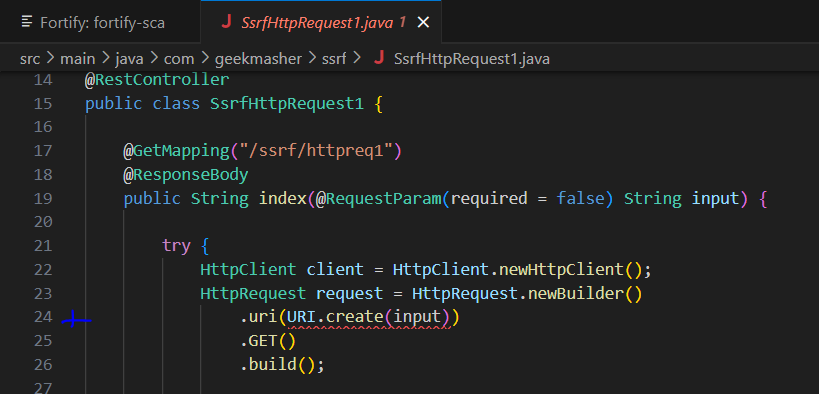
****

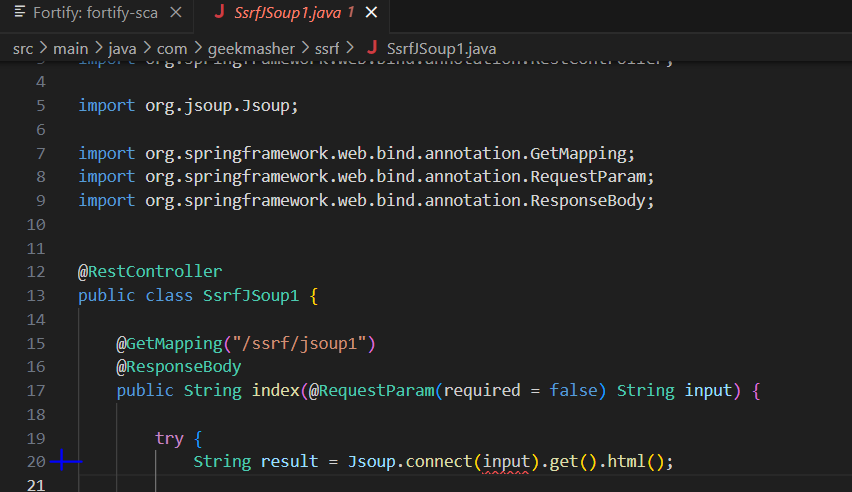
**SSRF**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| URL | - | + | + |
| HttpRequest | - | + | + |
| Jsoup | - | + | + |
| SecurityUtil | - | - | - |
| HttpUtil | - | - | + |
| HttpService | - | - | + |
| **Итог** | **0 из 6** | **3 из 6** | **5 из 6** |

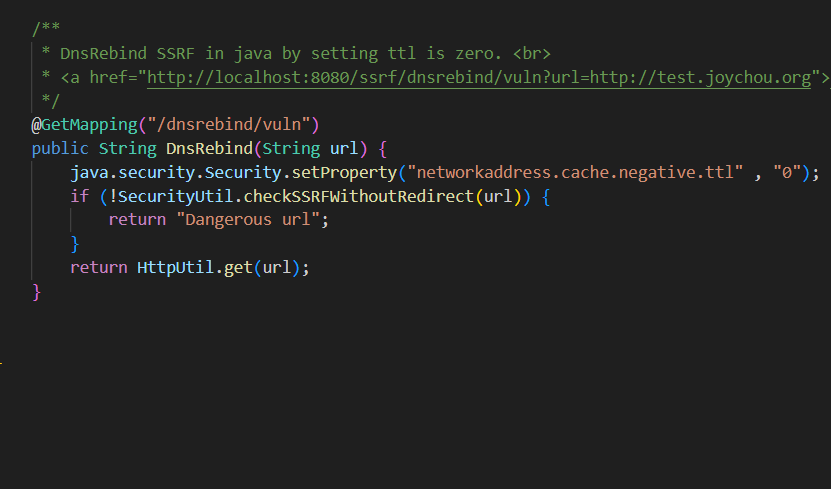
**URL**

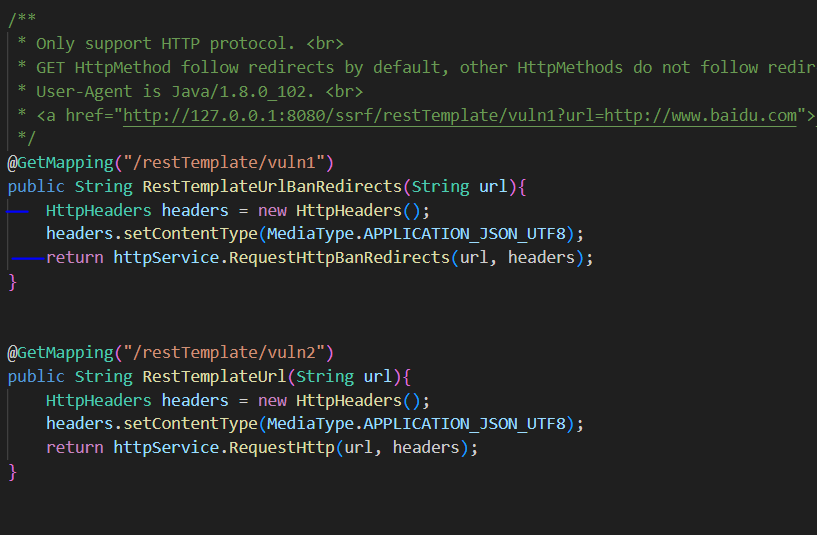
****

**HttpRequest**

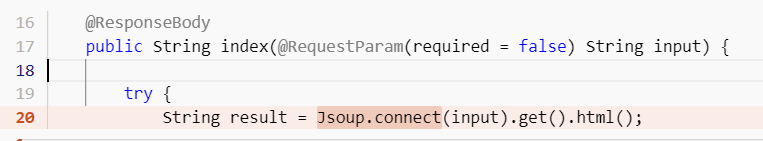
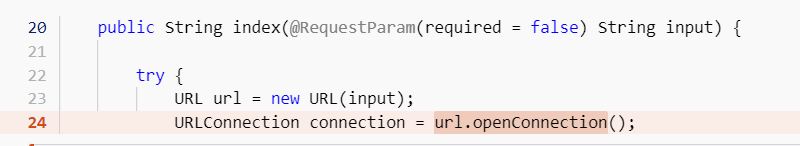
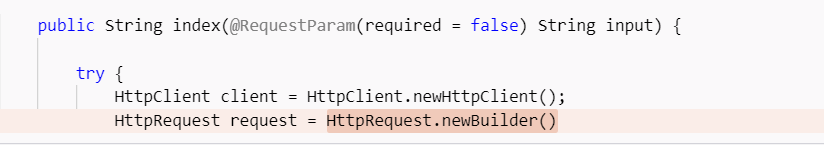
**Jsoup**

**SecurityUtil**

**HttpUtil**

**HttpService**

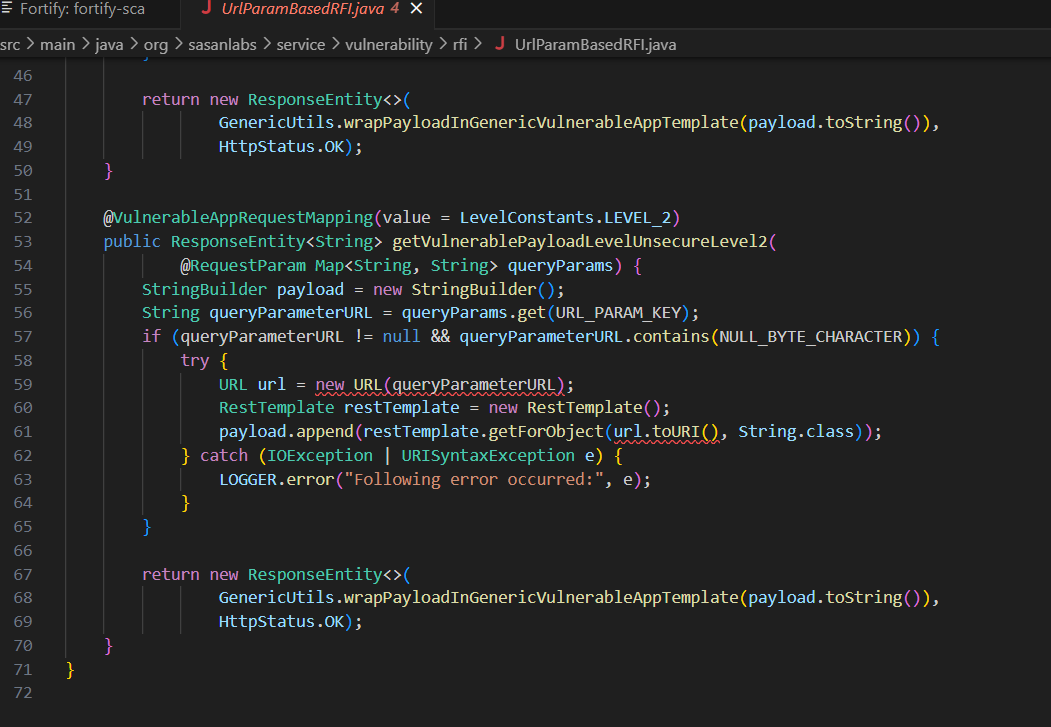
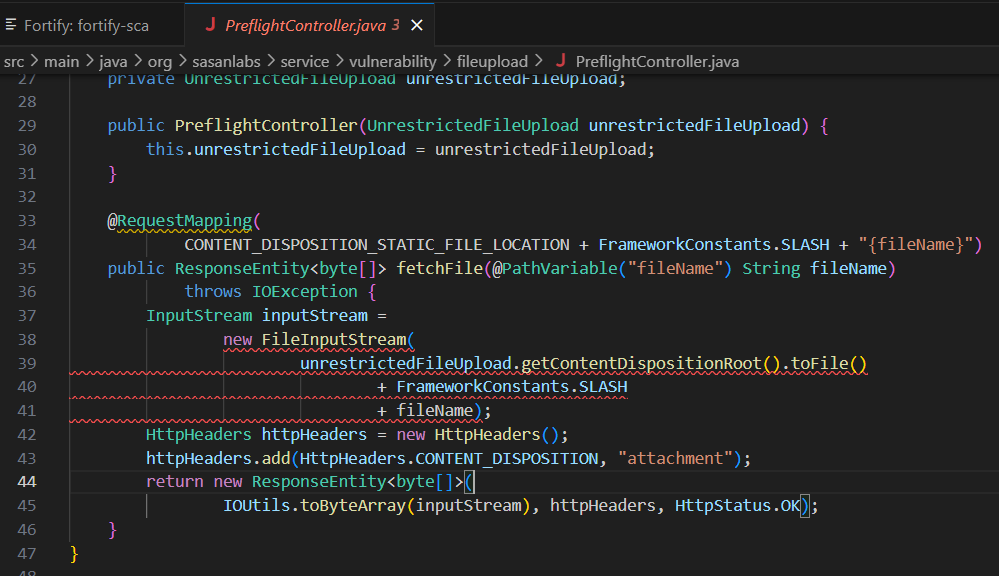
**Snyk**

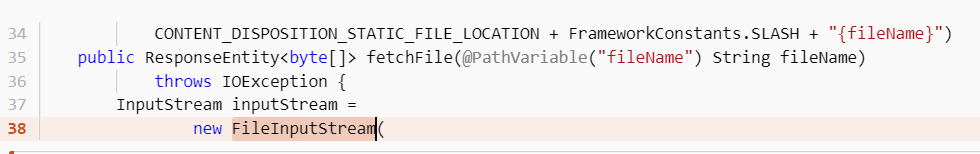
****

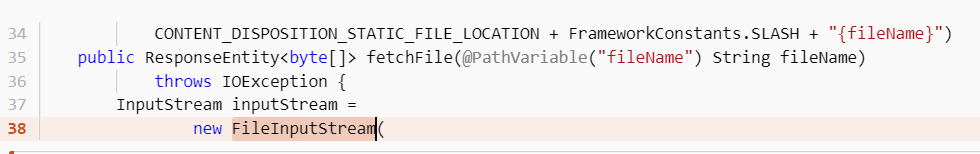
**RFI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| getForObject | - | + | + |
| FileInputStream | - | + | + |
| **Итог:** | **0 из 2** | **2 из 2** | **1 из 2** |

**Semgrep**

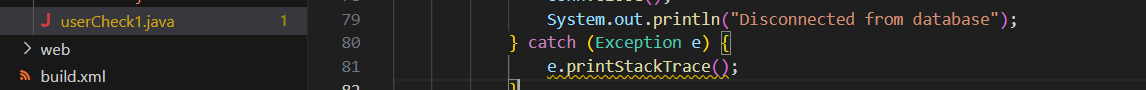
****

**Snyk**

****

**Debug**

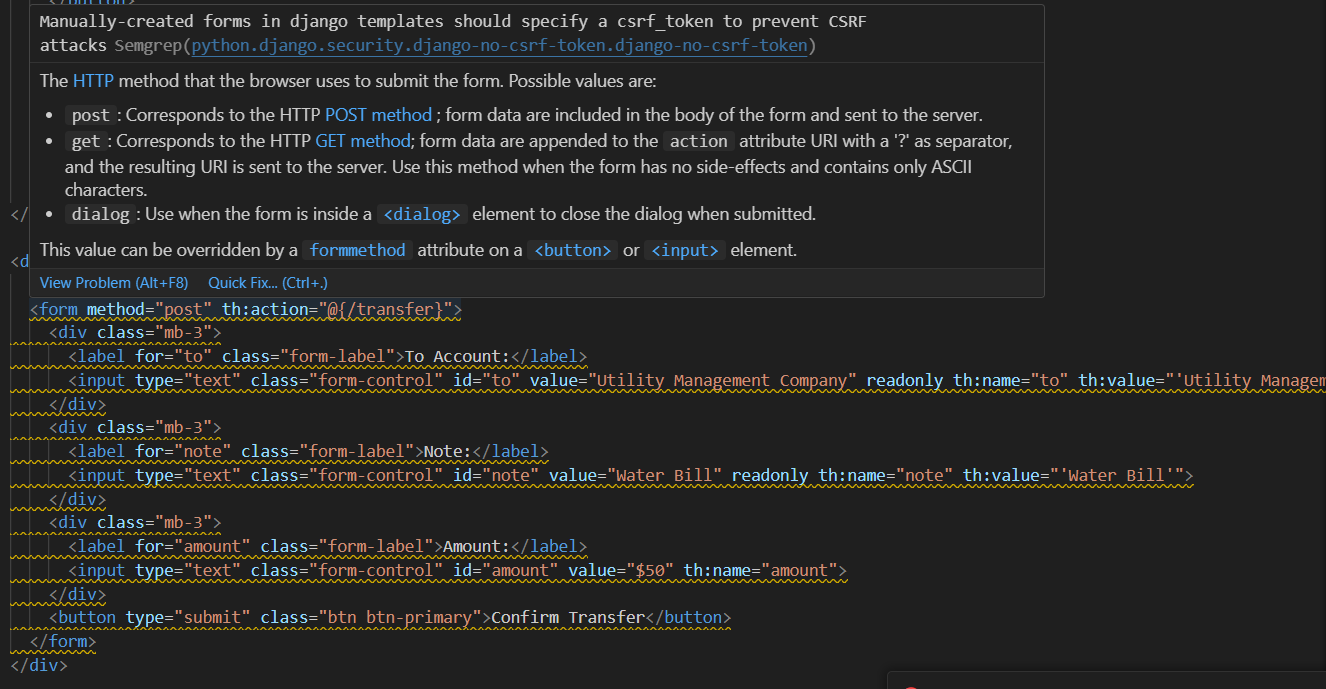
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Exception | - | + | - |
| **Итог:** | **0 из 1** | **1 из 1** | **0 из 1** |

****

**CSRF**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| CSTF token | +- | + | - |
| **Итог:** | **0.5 из 1** | **1 из 1** | **0 из 1** |

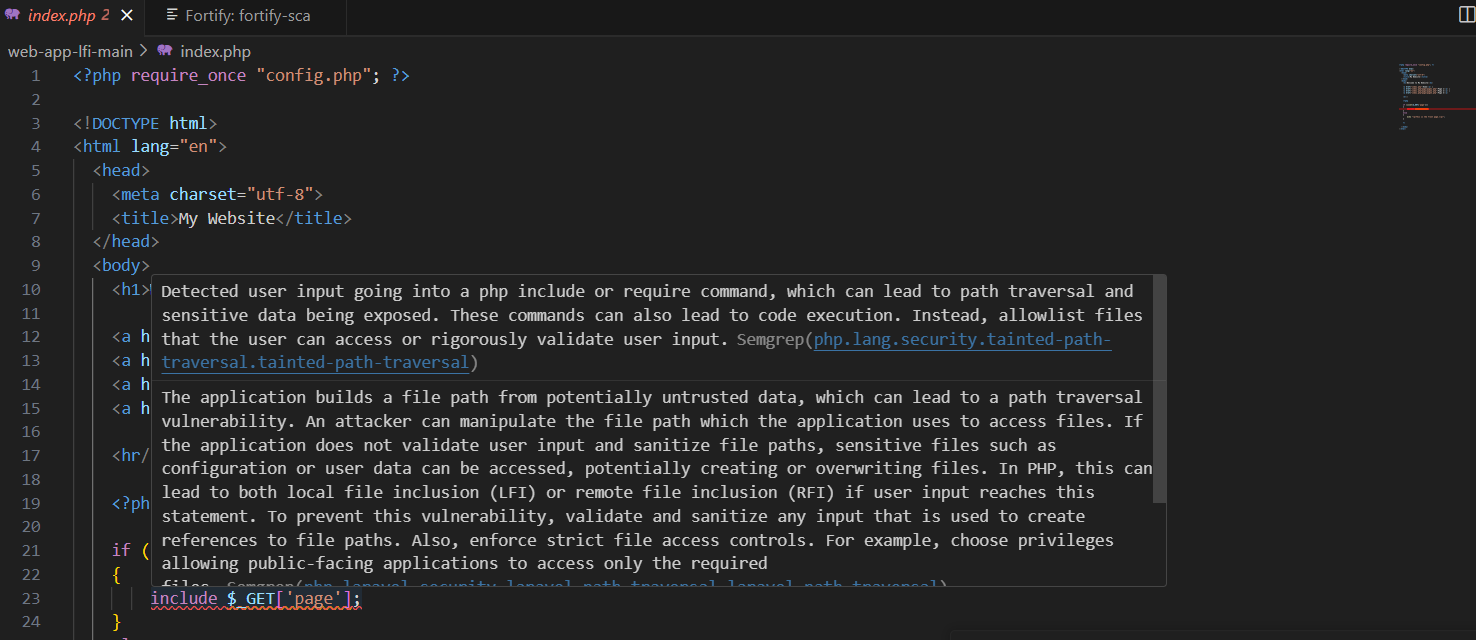
**CSRF token**

****

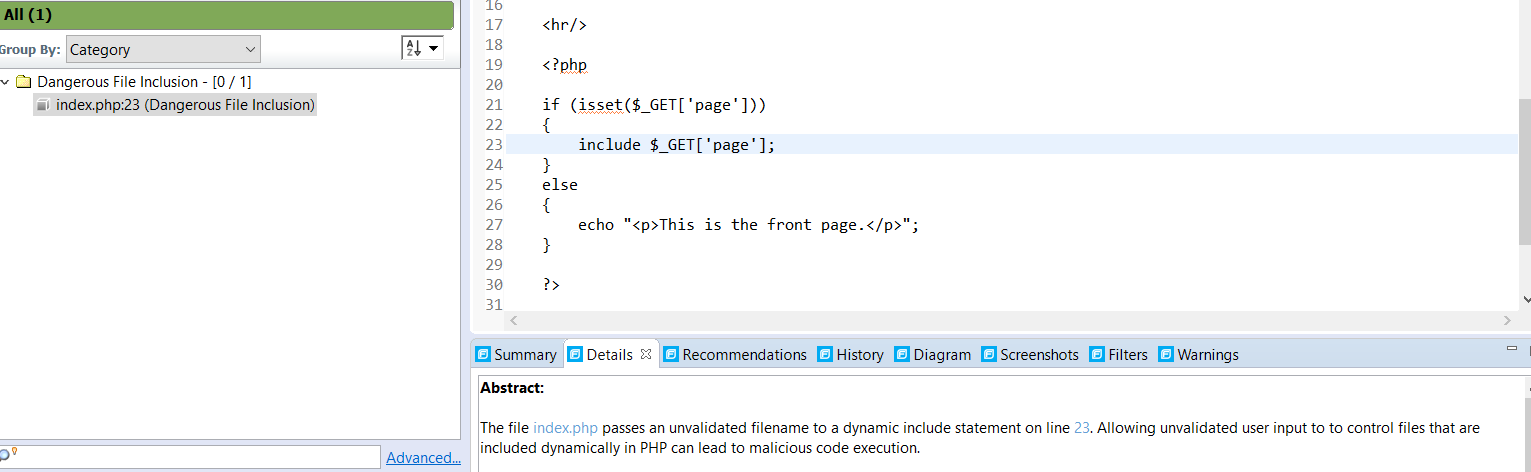
**LFI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Exception | + | + | + |
| **Итог:** | **1 из 1** | **1 из 1** | **1 из 1** |

**Semgrep**

****

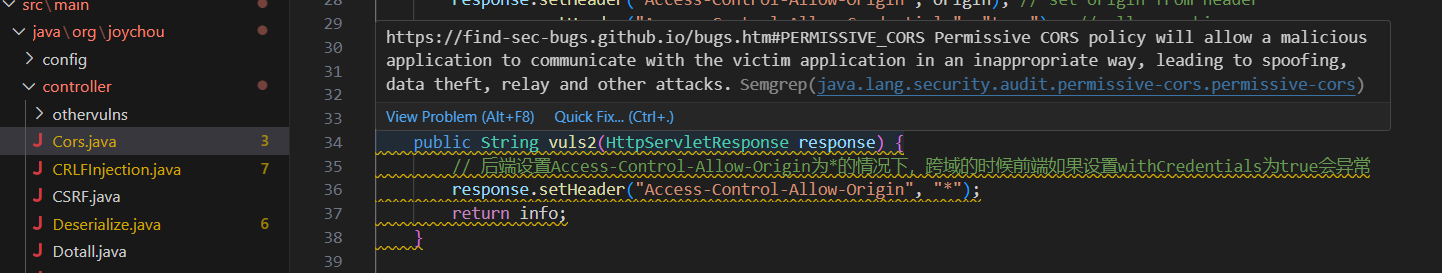
**Fortify**

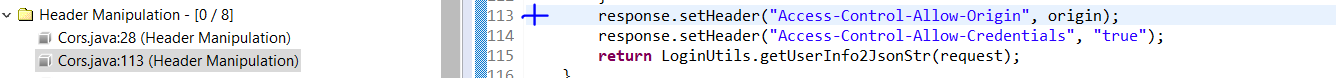
****

**Snyk **

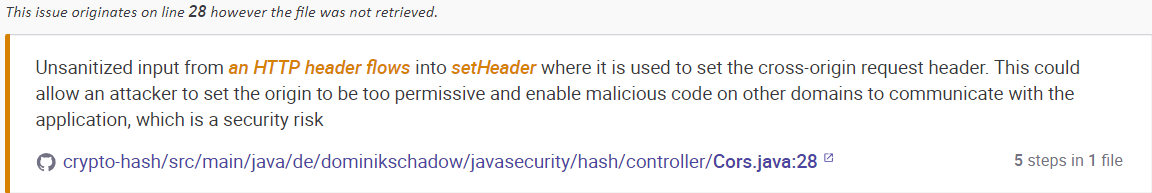
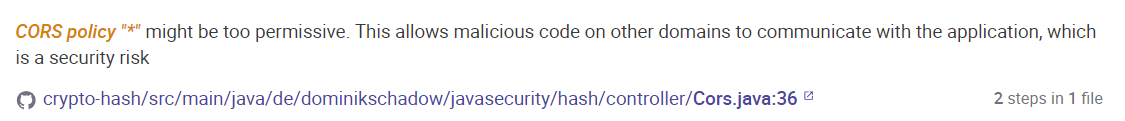
**CORS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Access-Control.. : \* | - | + | + |
| Пользовательский ввод в origin | + | - | + |
| **Итог** | **1 из 2** | **1 из 2** | **2 из 2** |

**Semgrep Fortify**

****

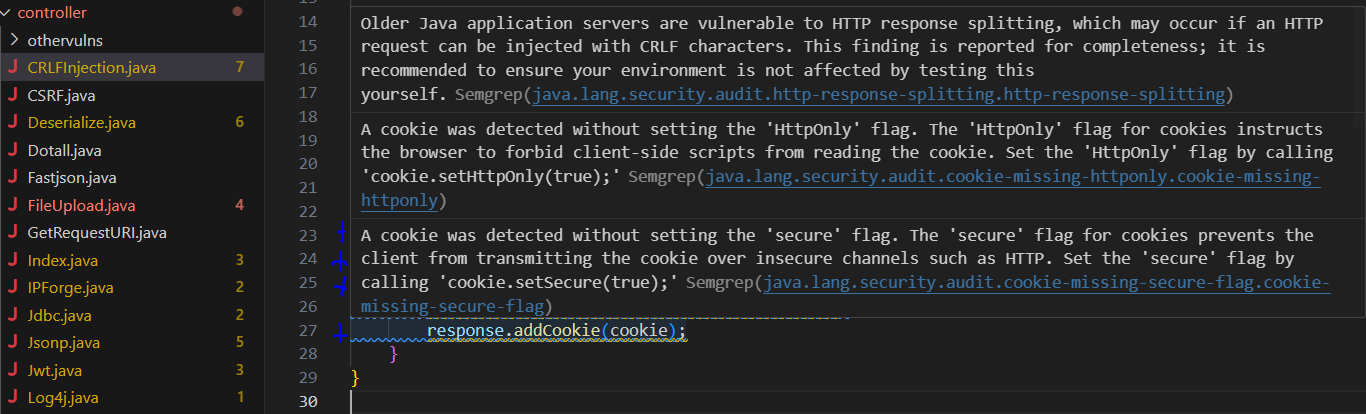
**Snyk**

****

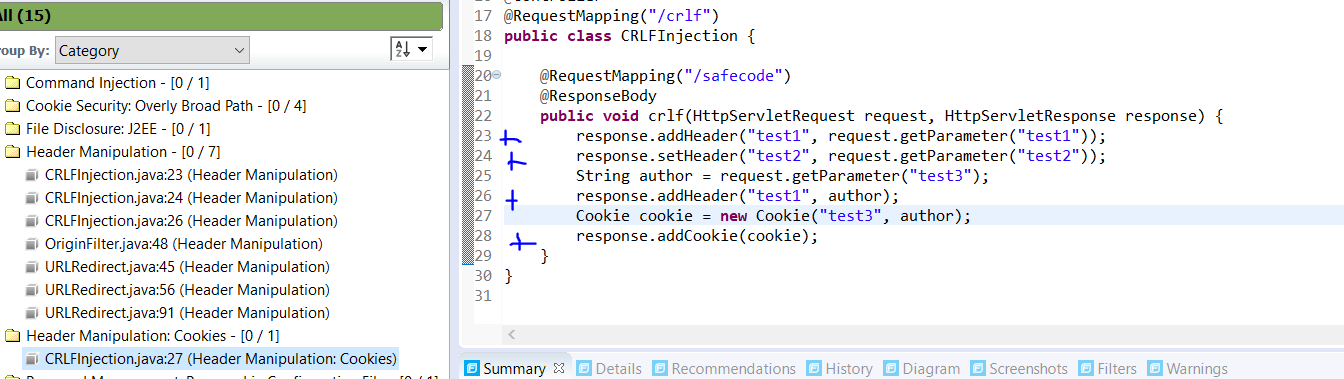
**CRLF**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| addHeader | + | + | + |
| setHeader | + | + | + |
| cookie | + | + | - |
| Использование переменной | + | + | + |
| **Итог** | **4 из 4** | **4 из 4** | **3 из 4** |

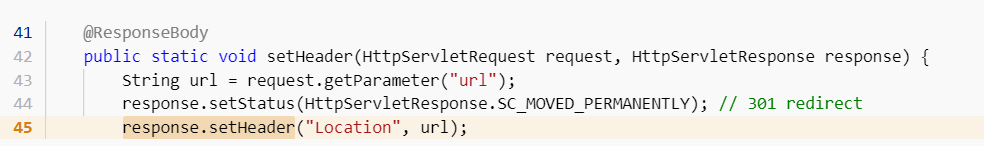
**Semgrep**

****

**Forify**

****

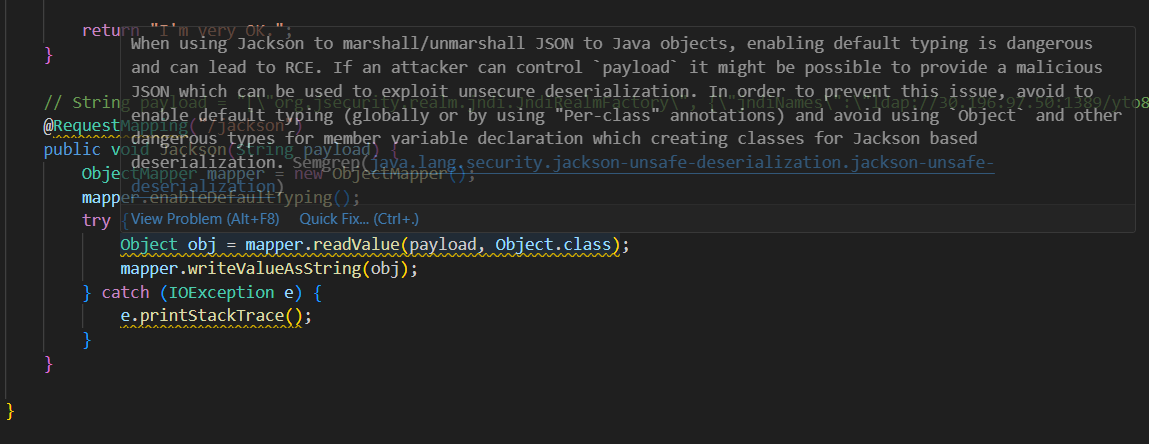
**Snyk**

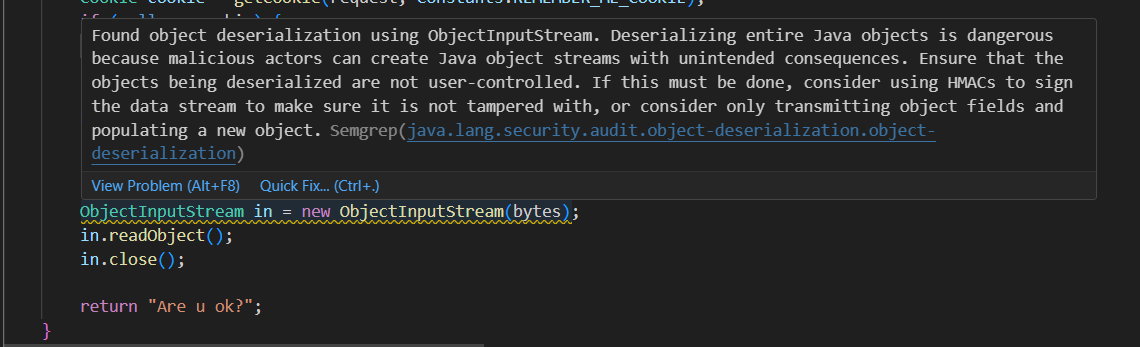
****

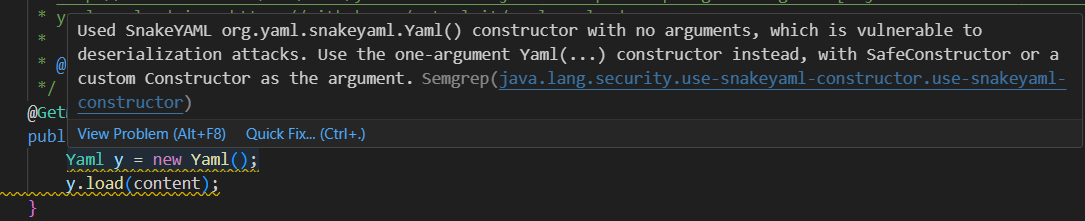
**Deserialize**

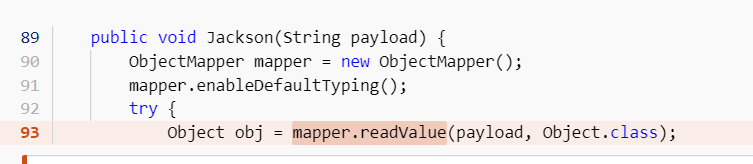
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Json | - | + | - |
| ObjectInputStream | - | + | + |
| Yaml | - | + | + |
| **Итог** | **0 из 2** | **3 из 3** | **2 из 3** |

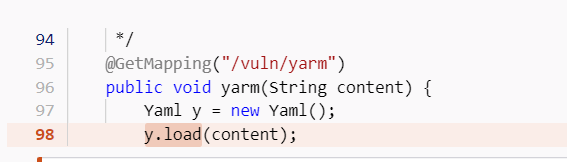
**Semgrep (приводит к RCE)**

****

****

****

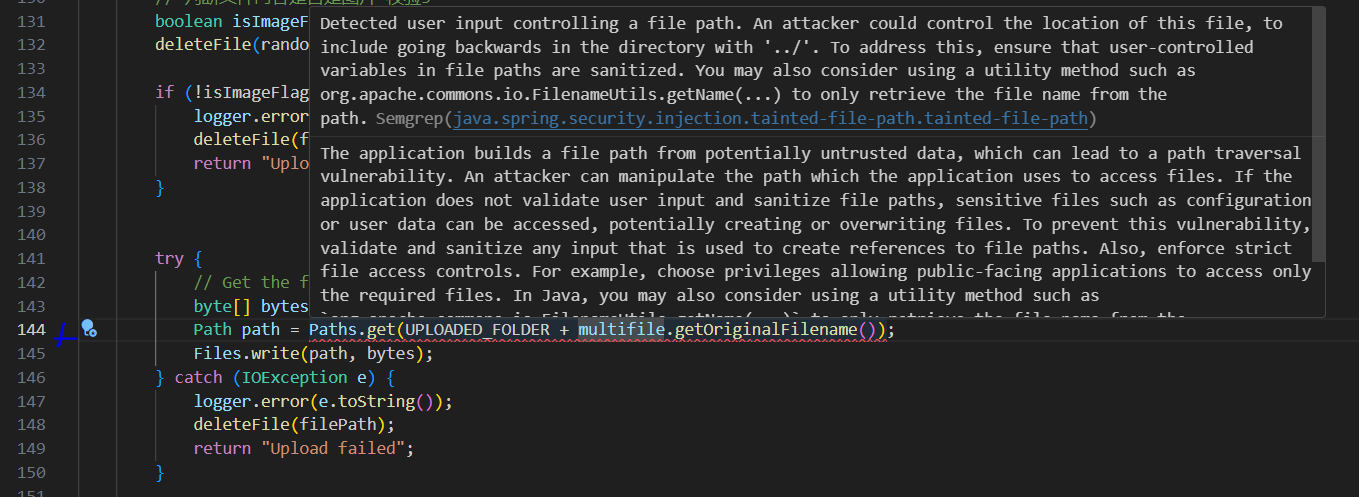
**Snyk **

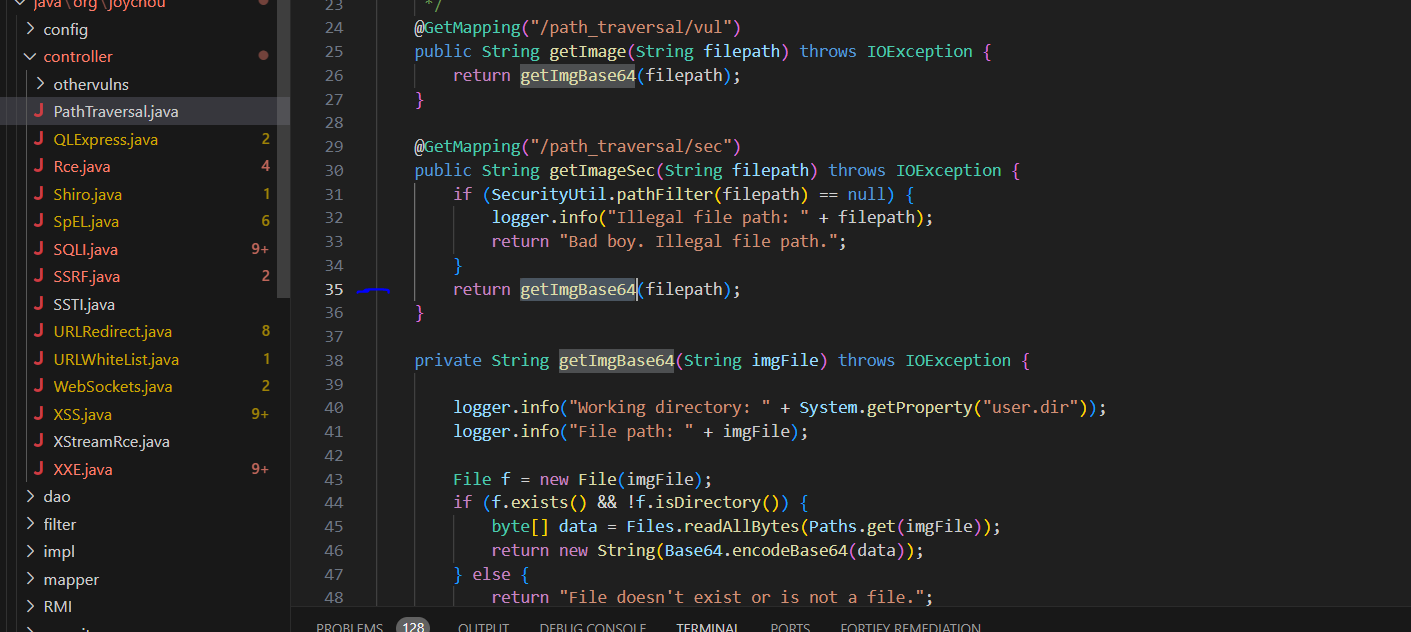
****

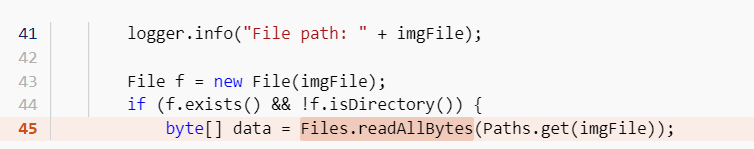
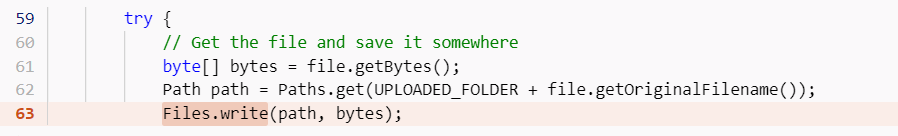
**Traversal**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Patchs.get | - | + | + |
| File | - | - | + |
| **Итог** | **0 из 2** | **2 из 2** | **2 из 2** |

**Semgrep**

****

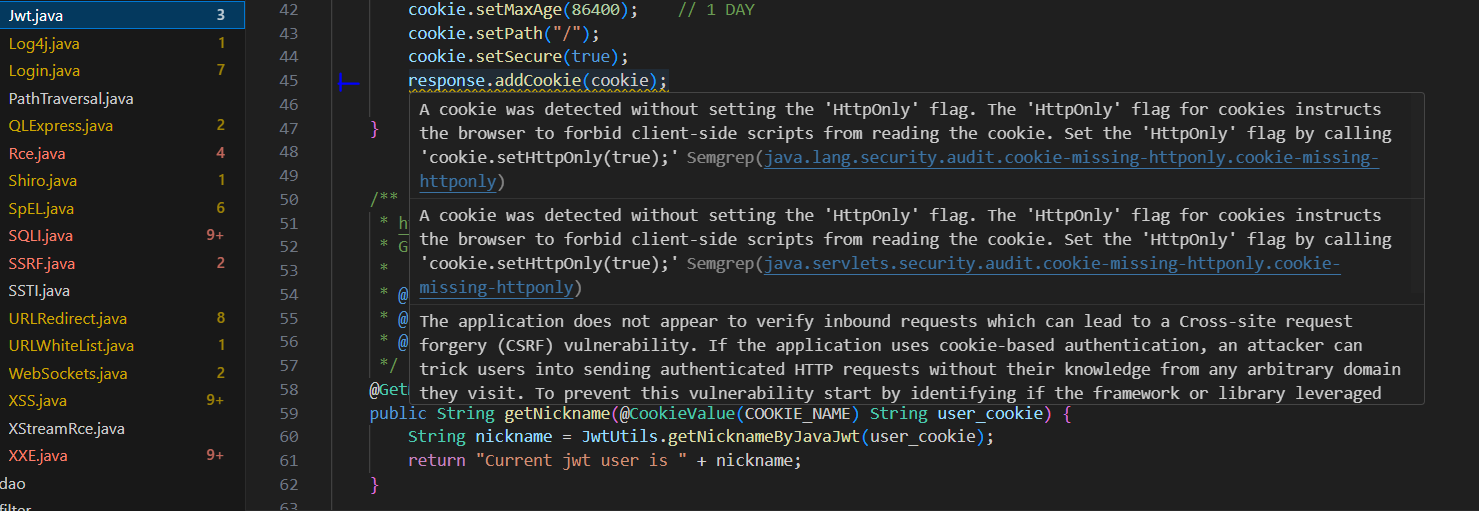
****

**Snyk **

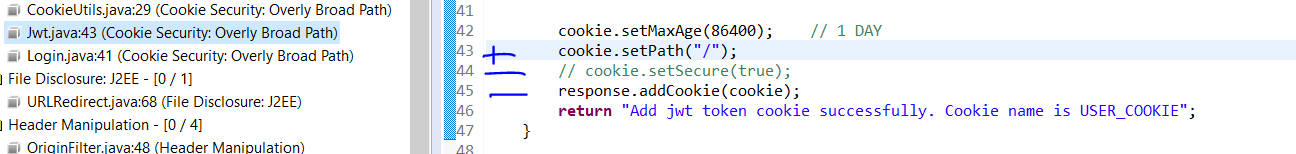
**Cookie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| HttpOnly | - | + | + |
| Secure | - | + | + |
| Patch | + | – | - |
| **Итог** | **1 из 3** | **2 из 3** | **1 из 3** |

**Semgrep**

****

**Fortify**

****

**Snyk**

****

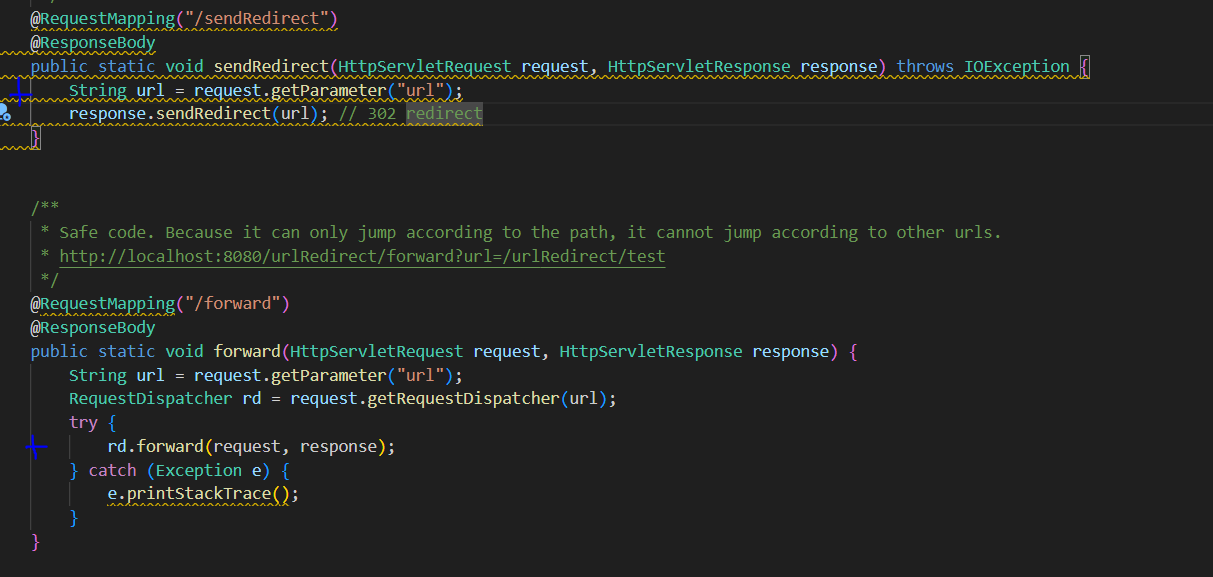
**OpenRedirect**

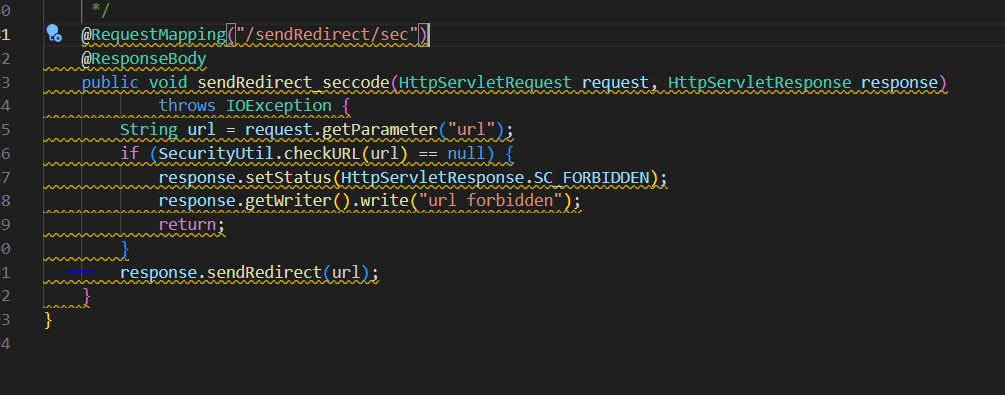
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Redirect | - | + | + |
| SetHendler | + | - | + |
| Response.sendRedirect | + | + | + |
| Forward Safe (False) | + | + | + |
| SecurityUtil | + | + | - |
| WhiteList (False) | + | + | - |
| **Итог** | **5 из 6** | **5 из 6** | **4 из 6** |

**Semgrep**

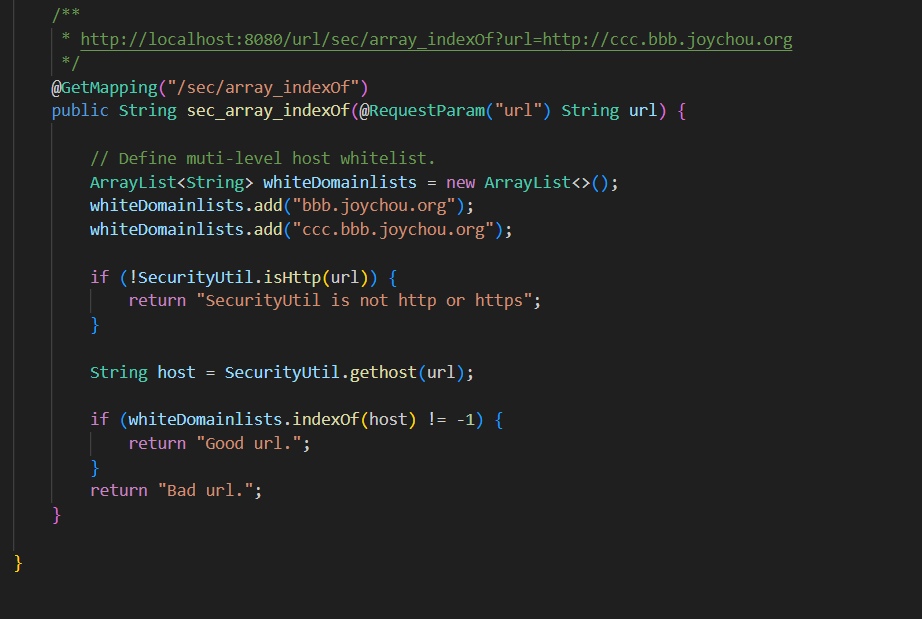
**Redirect и SetHendler**

****

**SendRedirect + Forward Safe (False)**

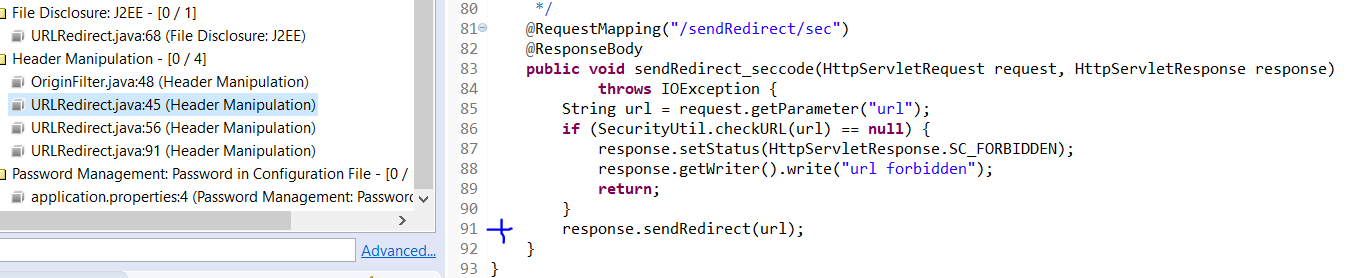
****

**WhiteList**

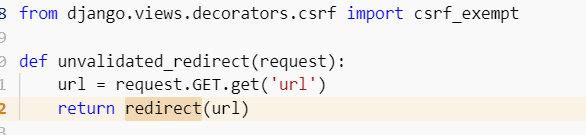
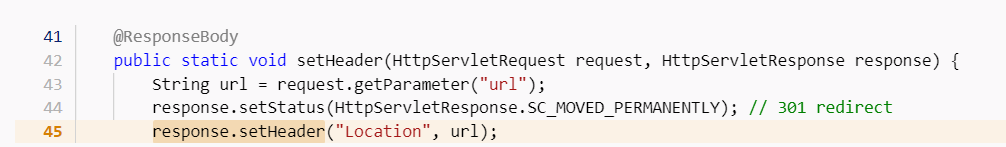
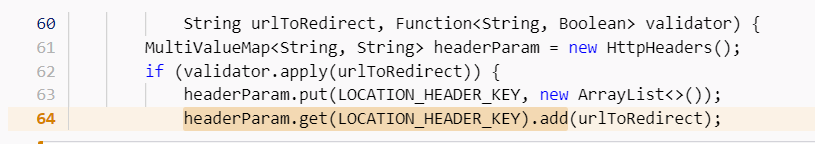
****

**Fortify**

****

****

**Snyk**

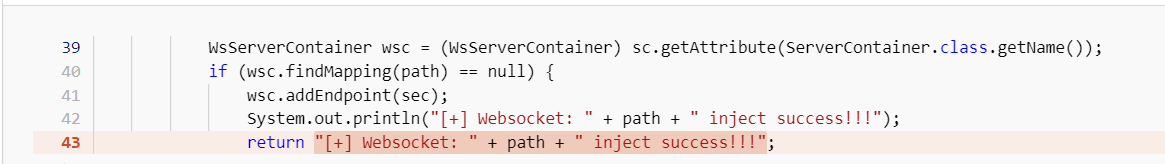
****

**WebSocket**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Socket | - | - | + |
| **Итог** | **0 из 1** | **0 из 1** | **1 из 1** |

**Semgrep**

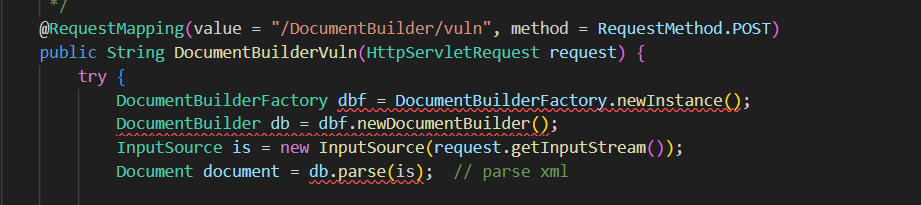
****

**Snyk**

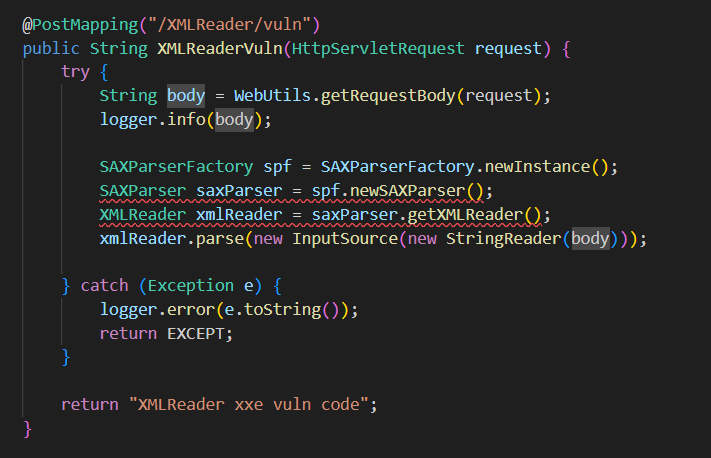
**XXE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| DocumentBulder | - | + | + |
| SAXParser | - | + | - |
| XMLReader | - | + | - |
| **Итог** | **0 из 3** | **3 из 3** | **1 из 3** |

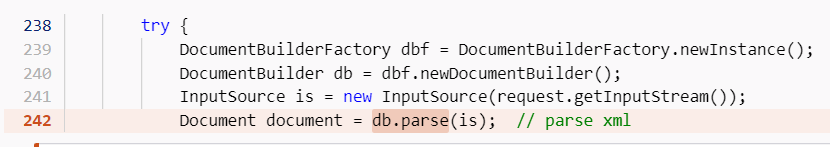
**DocumentBuilder**

****

**SAXParser + XMLReader**

****

**Snyk**

****