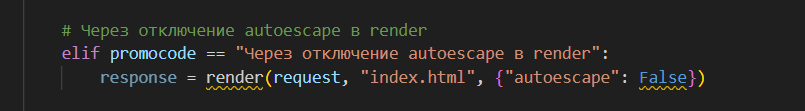
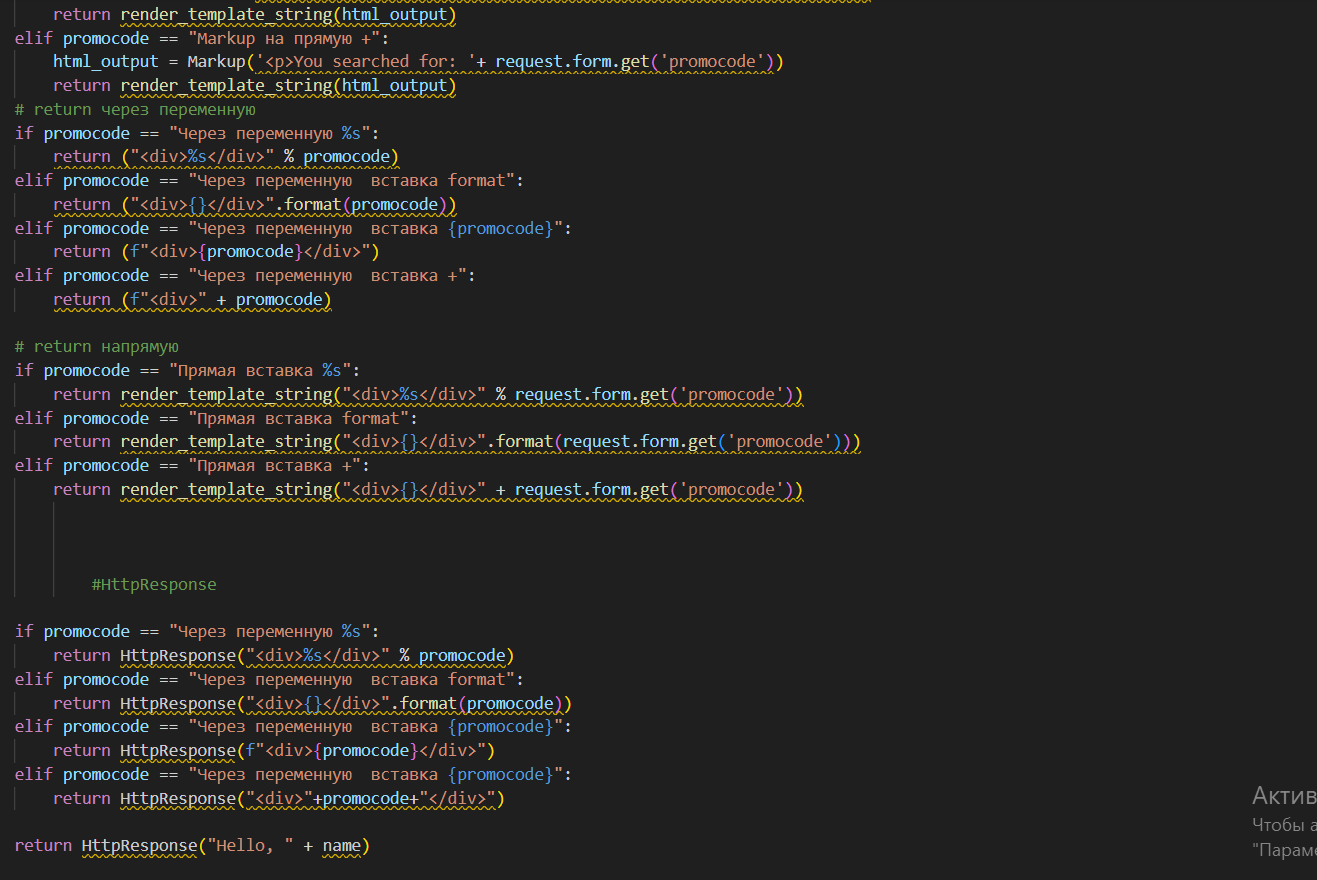
**Итог:**

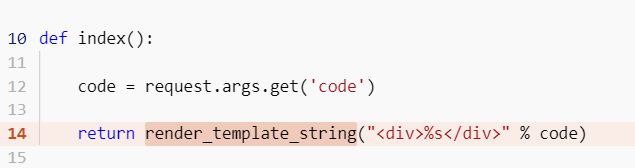
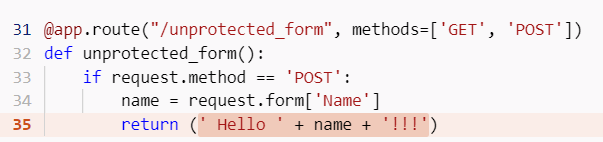
|  |  |  |  |
| --- | --- | --- | --- |
| **XSS** | | | |
| Render\_template\_string (%) прямая/переменная | - | +/+ | -/+ |
| Render\_template\_string ({}.format) прямая/переменная | - | +/+ | -/- |
| Render\_template\_string (f{}) прямая/переменная | - | +/+ | -/- |
| Markup (+) прямая/переменная | - | +/+ | -/- |
| Markup (%) прямая/переменная | - | +/+ | -/- |
| Markup ({}.format) прямая/переменная | - | +/+ | -/- |
| Markup (f{}) переменная | - | - | - |
| Return (+) прямая/переменная | - | +/+ | -/- |
| Return (%) прямая/переменная | - | +/+ | -/- |
| Return ({}.format) прямая/переменная | - | +/+ | -/- |
| Return (f{}) переменная | - | - | - |
| HttpResponse (+) переменная | - | + | - |
| HttpResponse (%) переменная | - | + | - |
| HttpResponse ({}.format) переменная | - | + | - |
| HttpResponse (f{}) переменная | - | - | - |
| Render AutoEscape=False | - | + | - |
| {% autoescape\_false %} | - | + | - |
| Href | - | + | - |
| <div>{{promocode}}</div> | - | - | - |
| **Итог:** | **0 из 28** | **24 из 28** | **1 из 28** |
| **SQL** | | | |
| (%) прямая/переменная | -/- | +/+ | +/+ |
| ({}.format) прямая/переменная | -/- | +/+ | +/+ |
| (f{}) прямая/переменная | -/- | +/+ | +/+ |
| (+) прямая/переменная | -/- | +/+ | +/+ |
| **Итог:** | **0 из 8** | **8 из 8** | **8 из 8** |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SSRF** | | | | | | | | | | | |
| Re.match | | | - | | | + | | | + | | |
| Requests.get | | | - | | | + | | | + | | |
| White list (False) | | | - | | | - | | | - | | |
| **Итог:** | | | **0 из 3** | | | **2 из 3** | | | **2 из 3** | | |
| **Race\_condition** | | | | | | | | | | |
| Low time | | - | | | - | | | - | | |
| Roleback | | - | | | - | | | - | | |
| **Итог:** | | **0 из 2** | | | **0 из 2** | | | **0 из 2** | | |
| **Traversal** | | | | | | | | | | | |
| File open | | | - | | | + | | | + | | |
| **Итог:** | | | **0 из 1** | | | **1 из 1** | | | **0 из 1** | | |
| **redirect** | | | | | | | | | | |
| Redirect переменная | | - | | | + | | | + | | |
| Redirect прямой | | - | | | - | | | - | | |
| **Итог:** | | **0 из 2** | | | **1 из 2** | | | **1 из 2** | | |
| **Cookie** | | | | | | | | | | |
| HttpOnly | | - | | | + | | | - | | |
| Secure | | - | | | + | | | - | | |
| Samesite | | - | | | + | | | - | | |
| **Итог:** | | **0 из 3** | | | **3 из 3** | | | **0 из 3** | | |
| **CRLF** | | | | | | | | | | |
| HttpOnly | | - | | | + | | | - | | |
| **Итог:** | | **0 из 1** | | | **1 из 1** | | | **0 из 1** | | |
| **Deserialize** | | | | | | | | | | |
| pickle.loads | | - | | | + | | | + | | |
| pickle.dumps | | - | | | + | | | + | | |
| **Итог:** | | **0 из 2** | | | **2 из 2** | | | **2 из 2** | | |
| **Arbitrary File Reading** | | | | | | | | | | |
| Re.match | | - | | | + | | | - | | |
| **Итог:** | | **0 из 1** | | | **1 из 1** | | | **0 из 1** | | |
| **Os\_Injection** | | | | | | | | | | |
| Subprocess.call (%) | | | - | | | + | | | + | |
| Subprocess.call ({}.format) | | | - | | | + | | | + | |
| Subprocess.call (f{}) | | | - | | | + | | | + | |
| Subprocess.call (+) | | | - | | | + | | | + | |
| Subprocess.popen (%) | | | - | | | + | | | + | |
| Subprocess.popen ({}.format) | | | - | | | + | | | + | |
| Subprocess.popen (f{}) | | | - | | | + | | | + | |
| Subprocess.popen (+) | | | - | | | + | | | + | |
| Os.system (%) | | | - | | | + | | | + | |
| Os.system ({}.format | | | - | | | + | | | + | |
| Os.system (f{}) | | | - | | | + | | | + | |
| Os.system (+) | | | - | | | + | | | + | |
| Subprocess\_shell | | | - | | | - | | | + | |
| Subprocess\_exec | | | - | | | - | | | - | |
| Subprocess.popen (+) | | | - | | | - | | | - | |
| Subprocess.call | | | - | | | + | | | - | |
| **CSRF** | | | **Fortify** | | | **Semgrep** | | | **Snyk** | |
| @csrf\_exempt | | | - | | | + | | | + | |
| html | | | + | | | + | | | - | |
| Итог: | | | 1 из 2 | | | 2 из 2 | | | 1 из 2 | |
| **Итог общий:** | | | **2/73** | | | **62/73** | | | **32/73** | |
| **Процентное отношение:** | | | **2.4%** | | | **84.5%** | | | **43.7%** | |

**XSS**

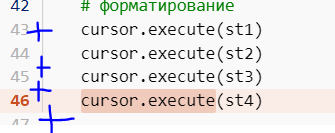
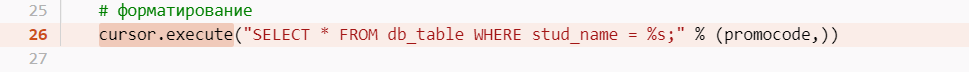
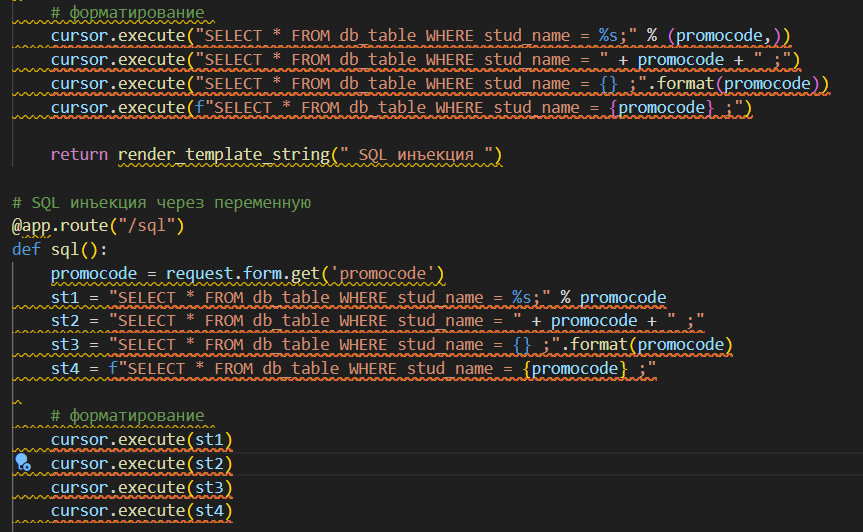
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Render\_template\_string (%) прямая/переменная | - | +/+ | -/+ |
| Render\_template\_string ({}.format) прямая/переменная | - | +/+ | -/- |
| Render\_template\_string (f{}) прямая/переменная | - | +/+ | -/- |
| Markup (+) прямая/переменная | - | +/+ | -/- |
| Markup (%) прямая/переменная | - | +/+ | -/- |
| Markup ({}.format) прямая/переменная | - | +/+ | -/- |
| Markup (f{}) переменная | - | - | - |
| Return (+) прямая/переменная | - | +/+ | -/- |
| Return (%) прямая/переменная | - | +/+ | -/- |
| Return ({}.format) прямая/переменная | - | +/+ | -/- |
| Return (f{}) переменная | - | - | - |
| HttpResponse (+) переменная | - | + | - |
| HttpResponse (%) переменная | - | + | - |
| HttpResponse ({}.format) переменная | - | + | - |
| HttpResponse (f{}) переменная | - | - | - |
| Render AutoEscape=False | - | + | - |
| {% autoescape\_false %} | - | + | - |
| Href | - | + | - |
| <div>{{promocode}}</div> | - | - | - |
| **Итог:** | **0 из 28** | **24 из 28** | **1 из 28** |

**Semgep** 



**SQL**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| (%) прямая/переменная | -/- | +/+ | +/+ |
| ({}.format) прямая/переменная | -/- | +/+ | +/+ |
| (f{}) прямая/переменная | -/- | +/+ | +/+ |
| (+) прямая/переменная | -/- | +/+ | +/+ |
| Итог: | 0 из 8 | 8 из 8 | 8 из 8 |

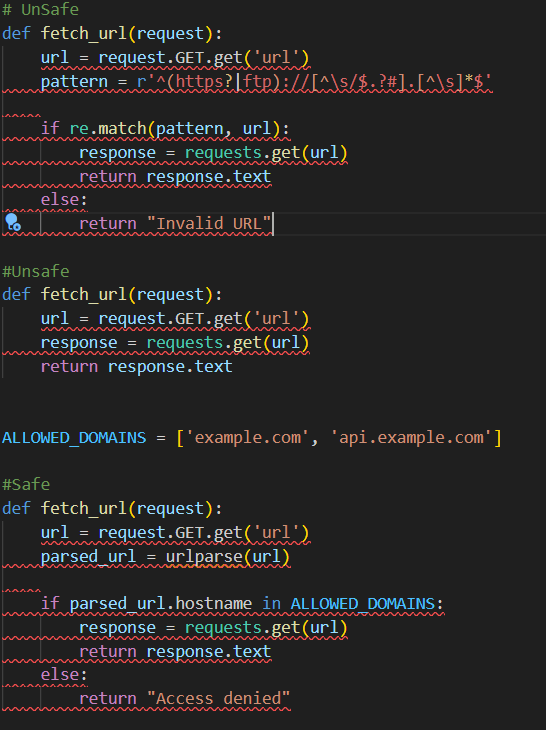


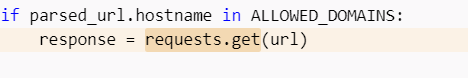
**Race\_condition**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Low time | - | - | - |
| Roleback | - | - | - |
| **Итог:** | **0 из 2** | **0 из 2** | **0 из 2** |

**SSRF**

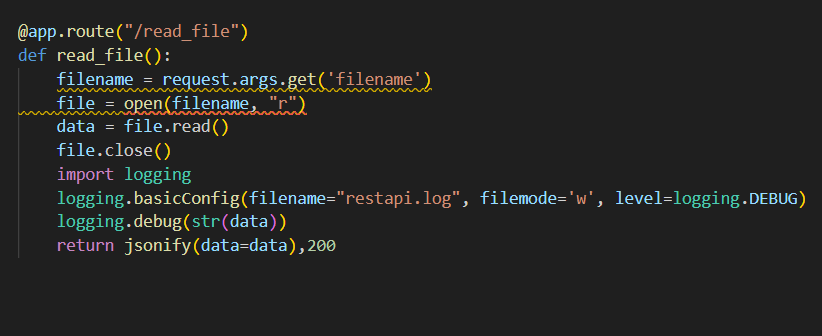
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Re.match | - | + | + |
| Requests.get | - | + | + |
| White list (False) | - | - | - |
| **Итог:** | **0 из 3** | **2 из 3** | **0 из 3** |





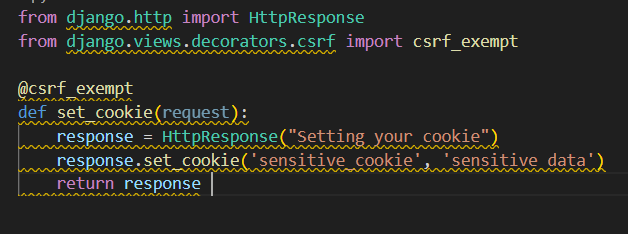
**Arbitrary File Reading**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Re.match | - | + | - |
| **Итог:** | **0 из 1** | **1 из 1** | **0 из 1** |



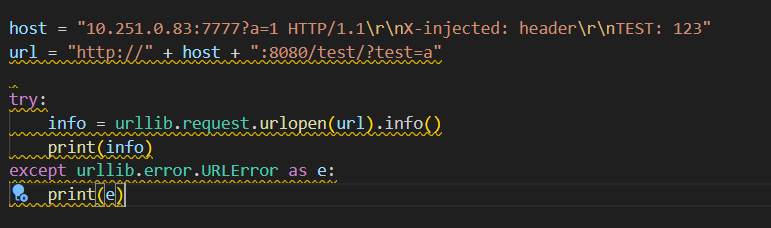
**Cookie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| HttpOnly | - | + | - |
| Secure | - | + | - |
| Samesite | - | + | - |
| **Итог:** | **0 из 3** | **3 из 3** | **0 из 3** |



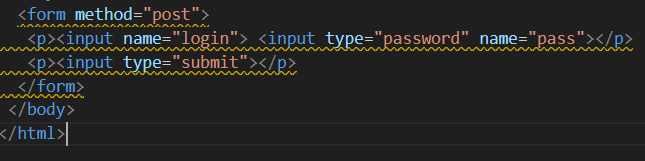
**CRLF**

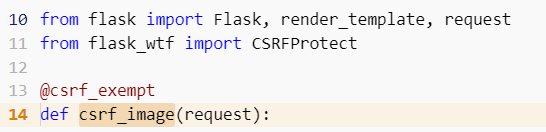
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| HttpOnly | - | + | - |
| **Итог:** | **0 из 1** | **1 из 1** | **0 из 1** |



**CSRF**

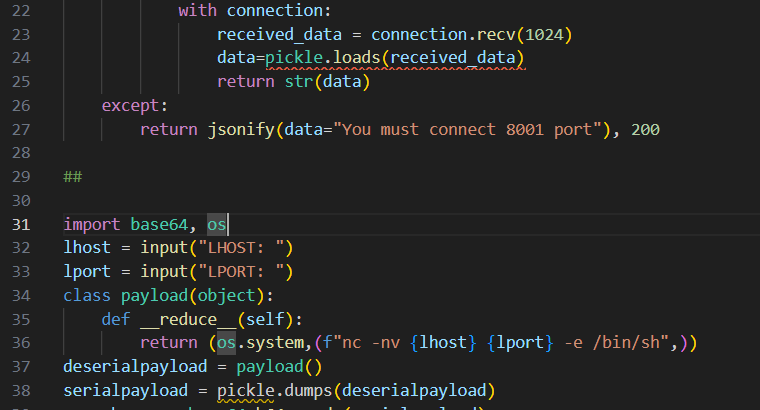
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| @csrf\_exempt | - | + | + |
| html | - | + | - |
| Итог: | 0 из 2 | 2 из 2 | 1 из 2 |





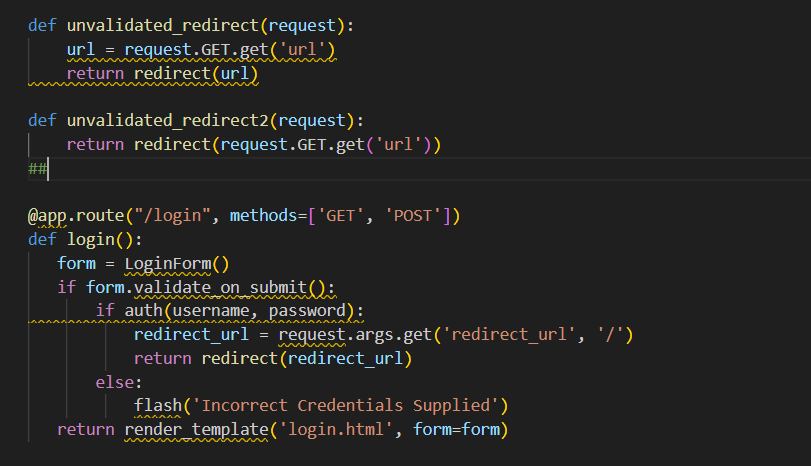
**Deserialize**

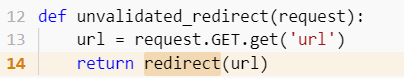
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| pickle.loads | - | + | + |
| pickle.dumps | - | + | + |
| **Итог:** | **0 из 2** | **2 из 2** | **2 из 2** |



**\_redirect**

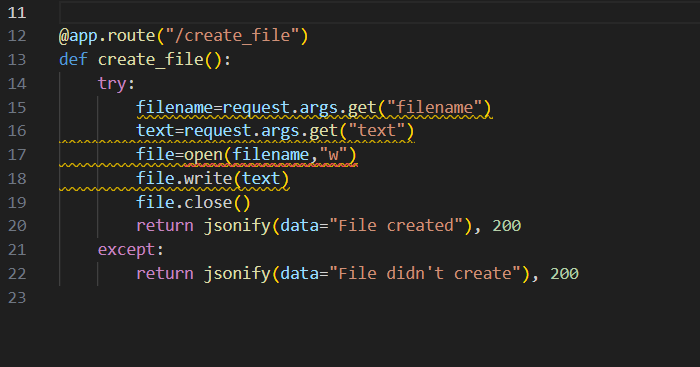
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Redirect переменная | - | + | + |
| Redirect прямой | - | - | - |
| **Итог:** | **0 из 2** | **1 из 2** | **1 из 2** |





**Treversal**

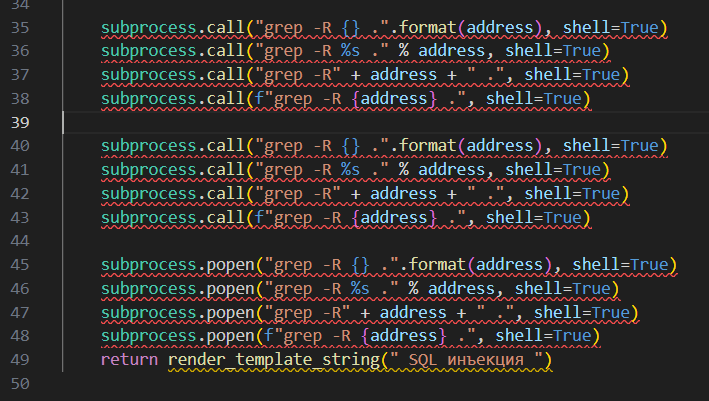
|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| File open | - | + | - |
| **Итог:** | **1 из 1** | **1 из 1** | **1 из 1** |

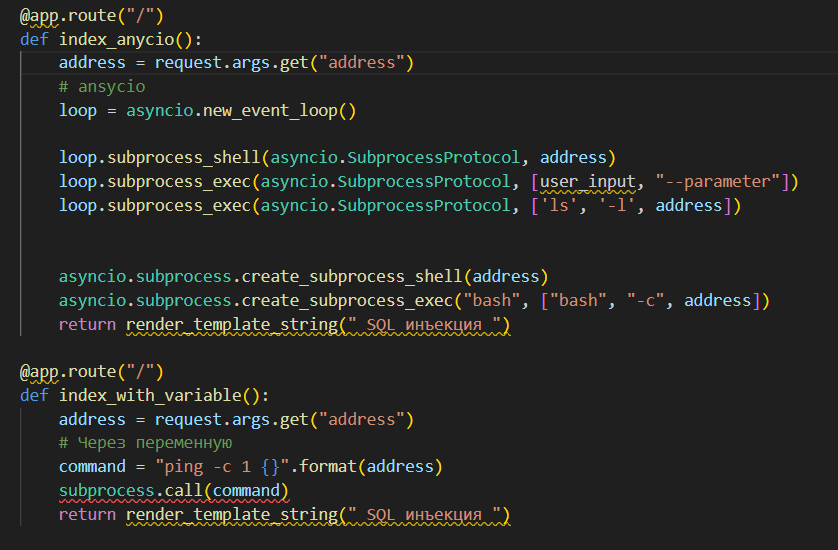


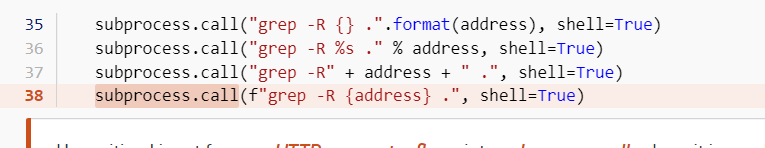
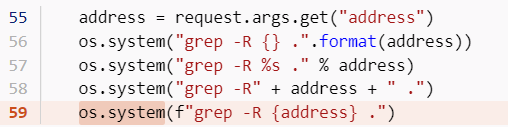
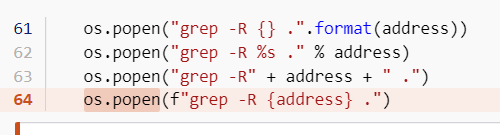


**Os\_Injection**

|  |  |  |  |
| --- | --- | --- | --- |
| **Уязвимость** | **Fortify** | **Semgrep** | **Snyk** |
| Subprocess.call (%) | - | + | + |
| Subprocess.call ({}.format) | - | + | + |
| Subprocess.call (f{}) | - | + | + |
| Subprocess.call (+) | - | + | + |
| Subprocess.popen (%) | - | + | + |
| Subprocess.popen ({}.format) | - | + | + |
| Subprocess.popen (f{}) | - | + | + |
| Subprocess.popen (+) | - | + | + |
| Os.system (%) | - | + | + |
| Os.system ({}.format | - | + | + |
| Os.system (f{}) | - | + | + |
| Os.system (+) | - | + | + |
| Subprocess\_shell | - | - | + |
| Subprocess\_exec | - | - | - |
| Subprocess.popen (+) | - | - | - |
| Subprocess.call | - | + | - |
| **Итог:** | **0 из 20** | **17 из 20** | **17 из 20** |

****

****

****

