|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Codebase** | **Vulnerability Type** | **Severity** | **File** | **Vulnerable Lines** | **Fix** |
| .\gateway\app.py:83:17 | B104:hardcoded\_bind\_all\_interfaces | Medium | app.py | 82,83 | We can fix this issue by changing 0.0.0.0 to local host(127.0.0.1) and bandit will not able to recognize it but while deploying our app on docker in production we will let docker and k8s to handle this vulnerability .  We can ignore at the moment. |
| .\math\_py\app.py:66:17 | [B104:hardcoded\_bind\_all\_interfaces] | Medium | app.py | 65,66 | We can fix this issue by changing 0.0.0.0 to local host(127.0.0.1) and bandit will not able to recognize it but while deploying our app on docker in production we will let docker and k8s to handle this vulnerability .  We can ignore at the moment. |
| .\stats\_py\app.py:8:11 | [B105:hardcoded\_password\_string] | Low | app.py | 7,8,9,10 | To resolve this issue we created a config.jason file and put our secrets there and then added config file in .gitignore |
| .\stats\_py\app.py:110:17 | [B104:hardcoded\_bind\_all\_interfaces] | Medium | app.py | 109,110 | We can fix this issue by changing 0.0.0.0 to local host(127.0.0.1) and bandit will not able to recognize it but while deploying our app on docker in production we will let docker and k8s to handle this vulnerability .  We can ignore at the moment. |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |