



## **INFORME SONARQUBE**

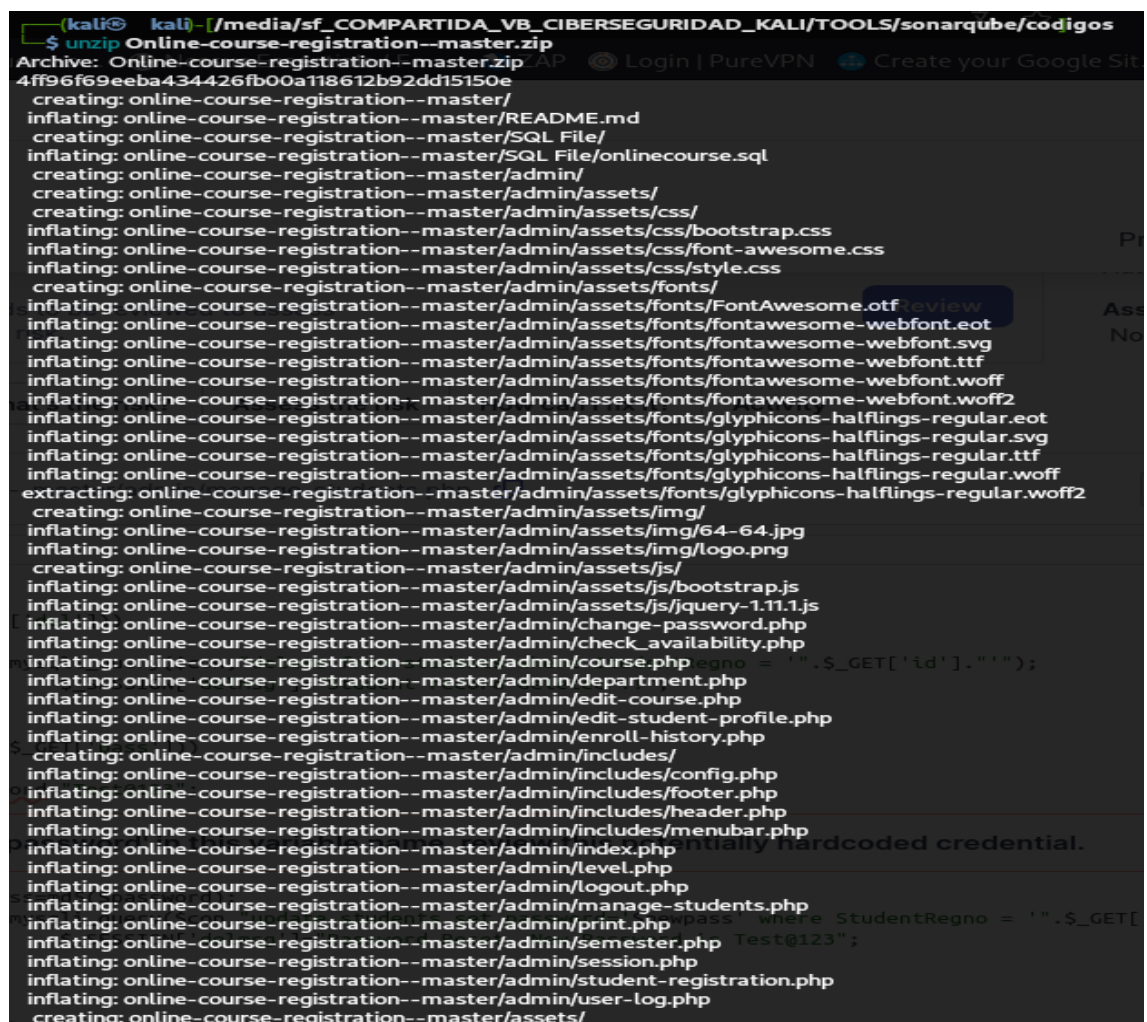
**Online-course-registration--master**

## 1.- INTRODUCCIÓN

SonarQube es una plataforma de código abierto, compatible con múltiples lenguajes de programación, usada para la revisión automática de errores y vulnerabilidades en el código fuente de las aplicaciones, integrándose con diversas herramientas, entre la que se encuentra SonarScanner, la cual, se utiliza para escanear el código fuente, enviando los resultados a un servidor de SonarQube para su análisis y visualización.

## 2.- PROCESO DE ESCANEO DEL CODIGO

En primer lugar, vamos a proceder a la descomprimir el archivo facilitado “Onlinecourse-registration—master”:



```
(kali) kali-[/media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/TOOLS/sonarqube/codigos]
$ unzip Online-course-registration--master.zip
Archive: Online-course-registration--master.zip
4ff96f69eeba434426fb00a118612b92dd15150e
  creating: online-course-registration--master/
  inflating: online-course-registration--master/README.md
  creating: online-course-registration--master/SQL File/
  inflating: online-course-registration--master/SQL File/onlinecourse.sql
  creating: online-course-registration--master/admin/
  creating: online-course-registration--master/admin/assets/
  creating: online-course-registration--master/admin/assets/css/
  inflating: online-course-registration--master/admin/assets/css/bootstrap.css
  inflating: online-course-registration--master/admin/assets/css/font-awesome.css
  inflating: online-course-registration--master/admin/assets/css/style.css
  creating: online-course-registration--master/admin/assets/fonts/
  inflating: online-course-registration--master/admin/assets/fonts/FontAwesome.otf
  inflating: online-course-registration--master/admin/assets/fonts/fontawesome-webfont.eot
  inflating: online-course-registration--master/admin/assets/fonts/fontawesome-webfont.svg
  inflating: online-course-registration--master/admin/assets/fonts/fontawesome-webfont.ttf
  inflating: online-course-registration--master/admin/assets/fonts/fontawesome-webfont.woff
  inflating: online-course-registration--master/admin/assets/fonts/fontawesome-webfont.woff2
  inflating: online-course-registration--master/admin/assets/fonts/glyphicons-halflings-regular.eot
  inflating: online-course-registration--master/admin/assets/fonts/glyphicons-halflings-regular.svg
  inflating: online-course-registration--master/admin/assets/fonts/glyphicons-halflings-regular.ttf
  inflating: online-course-registration--master/admin/assets/fonts/glyphicons-halflings-regular.woff
  extracting: online-course-registration--master/admin/assets/fonts/glyphicons-halflings-regular.woff2
  creating: online-course-registration--master/admin/assets/img/
  inflating: online-course-registration--master/admin/assets/img/64-64.jpg
  inflating: online-course-registration--master/admin/assets/img/logo.png
  creating: online-course-registration--master/admin/assets/js/
  inflating: online-course-registration--master/admin/assets/js/bootstrap.js
  inflating: online-course-registration--master/admin/assets/js/jquery-1.11.1.js
  inflating: online-course-registration--master/admin/change-password.php
  inflating: online-course-registration--master/admin/check_availability.php
  inflating: online-course-registration--master/admin/course.php $regno = $_GET['id'].");
  inflating: online-course-registration--master/admin/departament.php
  inflating: online-course-registration--master/admin/edit-course.php
  inflating: online-course-registration--master/admin/edit-student-profile.php
  inflating: online-course-registration--master/admin/enroll-history.php
  creating: online-course-registration--master/admin/includes/
  inflating: online-course-registration--master/admin/includes/config.php
  inflating: online-course-registration--master/admin/includes/footer.php
  inflating: online-course-registration--master/admin/includes/header.php
  inflating: online-course-registration--master/admin/includes/menubar.php
  inflating: online-course-registration--master/admin/index.php
  inflating: online-course-registration--master/admin/level.php
  inflating: online-course-registration--master/admin/logout.php
  inflating: online-course-registration--master/admin/manage-students.php
  inflating: online-course-registration--master/admin/print.php $pass" where StudentRegno = $_GET[
  inflating: online-course-registration--master/admin/semester.php Test@123";
  inflating: online-course-registration--master/admin/session.php
  inflating: online-course-registration--master/admin/student-registration.php
  inflating: online-course-registration--master/admin/user-log.php
  creating: online-course-registration--master/assets/
```

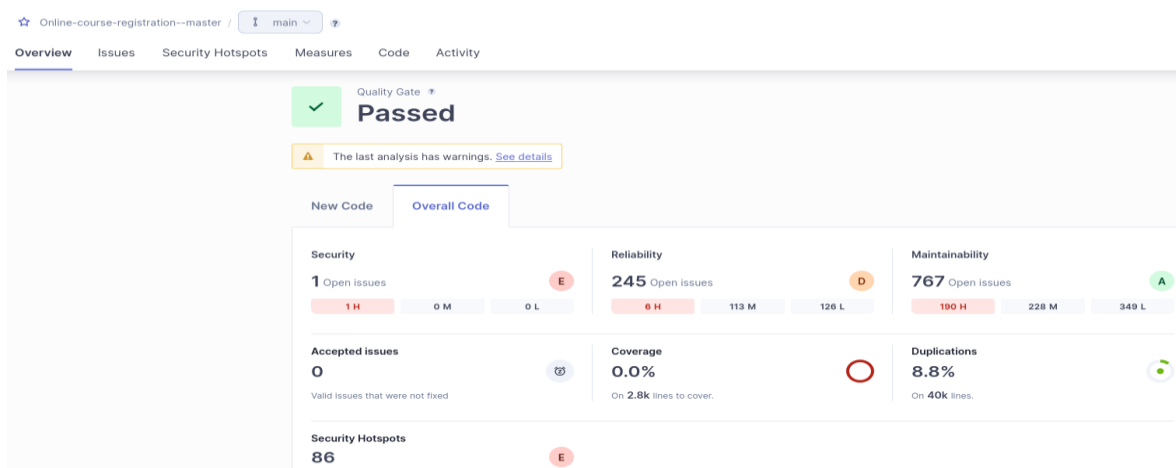
Esto es una muestra de la información, siendo el código PHP.

Después, se procede al análisis mediante la herramienta sonnar-scanner, dando como resultado un informe que envía al servidor de la aplicación SonarQube:

```
(kali) kali-[/media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/TOOLS/sonarqube/codigos]
$ sonar-scanner \
-Dsonar.projectKey=Online-course-registration--master \
-Dsonar.sources=. \
-Dsonar.host.url=http://localhost:9000 \
-Dsonar.token=sqp_69b9fe648881bf5c987cb67cb1b09954083c3fb3
```

```
01:14:42.059 INFO Using git CLI to retrieve untracked files
01:14:42.060 WARN Analyzing only language associated files, make sure to run the analysis inside a git repository
01:14:42.117 INFO 60 source files to be analyzed
01:14:42.358 INFO 60/60 source files have been analyzed
01:14:42.359 INFO Sensor TextAndSecretsSensor [text] (done) | time=543ms
01:14:42.362 INFO ----- Run sensors on project
01:14:42.380 INFO Sensor Zero Coverage Sensor
01:14:42.551 INFO Sensor Zero Coverage Sensor (done) | time=172ms
01:14:42.552 INFO SCM Publisher No SCM system was detected. You can use the 'sonar.scm.provider' property to explicitly specify it.
01:14:42.559 INFO CPD Executor 15 files had no CPD blocks
01:14:42.559 INFO CPD Executor Calculating CPD for 37 files
01:14:42.622 INFO CPD Executor CPD calculation finished (done) | time=64ms
01:14:43.371 INFO Analysis report generated in 239ms, dir size=2.3 MB
01:14:46.348 INFO Analysis report compressed in 2975ms, zip size=747.3 kB
01:14:46.424 INFO Analysis report uploaded in 75ms
01:14:46.428 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=Online-course-registration--master
01:14:46.431 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
01:14:46.432 INFO More about the report processing at http://localhost:9000/api/ce/task?id=3d8b7ec5-a3ec-468b-96aa-edbaef284b105
01:15:44.279 INFO Analysis total time: 2:42.139 s
01:15:44.280 INFO SonarScanner Engine completed successfully
01:15:44.707 INFO EXECUTION SUCCESS
01:15:44.708 INFO Total time: 2:44.097s
```

### 3.- PROCESO DE ANALISIS DEL RESULTADO



Dentro del campo de la ciberseguridad, concretamente en la pestaña de “Security Hotspots” podemos observar que el código tiene presuntas vulnerabilidades altas, medias y bajas, que deben ser verificadas:

Review priority: 🔴 High	
🔴 Authentication	1 >
🔴 SQL Injection	40 >
Review priority: 🟡 Medium	
🟡 Weak Cryptography	2 >
Review priority: 🟢 Low	
🟢 Others	43 >

86 of 86 shown

### 3.1.- RIESGO ALTO

- 3.1.1.- La vulnerabilidad de Autenticación detectada de prioridad alta, se debe a que dentro del código aparece una contraseña legible:

```
if(isset($_GET['del']))
{
    mysqli_query($con,"delete from students where StudentRegno = '".$_GET['id']."'");
    $_SESSION['delmsg']="Student record deleted !!";
}

if(isset($_GET['pass']))
{
    $password="Test@123";
}
```

Detected 'password' in this variable name, review this potentially hardcoded credential.

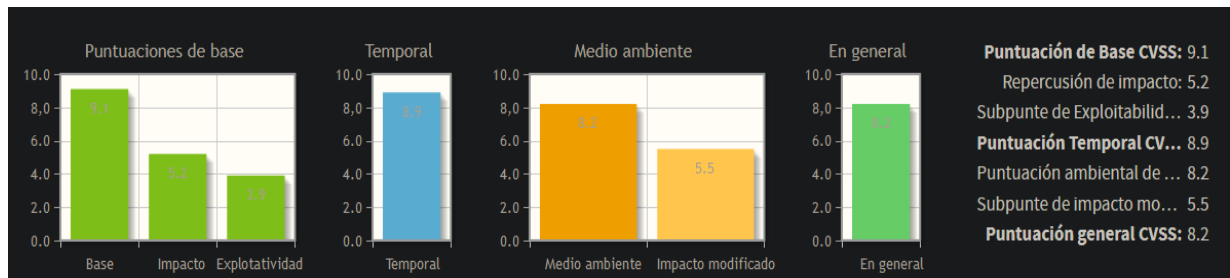
Esta vulnerabilidad podría permitir a atacantes malintencionados el acceso a datos sensibles y confidenciales (BBDD, APIs, servicios, etc), recomendándose su verificación y corrección, en su caso, por otras prácticas de codificación más seguras, como, el almacenamiento las credenciales en un archivo de configuración fuera del repositorio y usar los servicios iCloud para almacenar datos sensibles, encontrándose en el OWASP Top 10 2021, en la categoría número 7 llamada “Identificación y autenticación”.

#### Compliant Solution

```
$user = getUser();
$password = getPassword(); // Compliant

$httpUrl = "https://example.domain?user=$user&password=$password" // Compliant
$sshUrl = "ssh://$user:$password@example.domain" // Compliant
```

Esta vulnerabilidad podría tener una puntuación CVSS alta, adjuntando grafico del resultado:



-3.1.2.- Se han detectado 40 posibles fallos en la codificación que podrían permitir a los atacantes realizar inyecciones SQL maliciosas al concatenar valores que no son de confianza en la misma consulta, recomendando su verificación y corrección, en este caso, usando consultas parametrizadas y/o declaraciones preparadas, como en este caso:

#### Compliant Solution

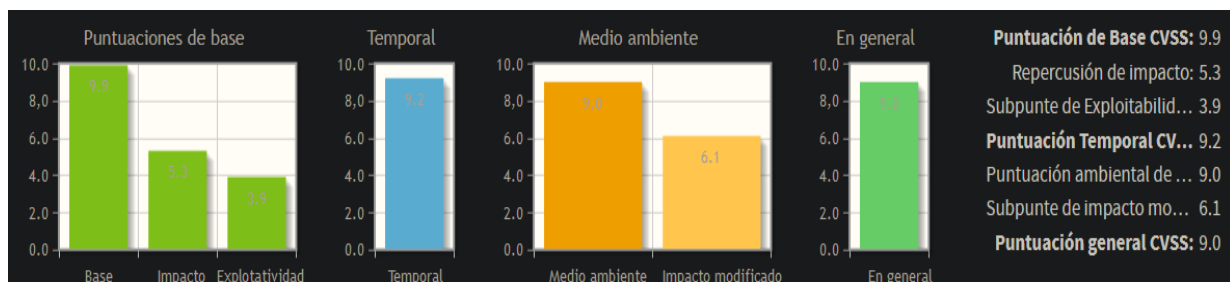
```
$id = $_GET['id'];
try {
    $conn = new PDO('mysql:host=localhost;dbname=myDatabase', $username, $password);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

    $stmt = $conn->prepare('SELECT * FROM myTable WHERE id = :id');
    $stmt->execute(array('id' => $id));

    while($row = $stmt->fetch(PDO::FETCH_OBJ)) {
        echo $row->name;
    }
} catch(PDOException $e) {
    echo 'ERROR: ' . $e->getMessage();
}
```

Estas vulnerabilidades se encuentran en el OWASP – Top 10 2021 en la tercera categoría denominada “Inyección”.

Esta vulnerabilidad podría tener una puntuación CVSS alta, adjuntando grafico del resultado:





### 3.2.- RIESGO MEDIO

Se han encontrado 2 presuntas debilidades criptográficas, concretamente en 2 partes del código:

```
26         if(mysqli_num_rows($result_email)>0){
27             echo '<script type="text/javascript">';
28             echo 'setTimeout(function () { sweetAlert("Oops...", "Email Address '. $email_address.
' is already exists!","error");';
29             echo '}, 500);</script>';
30         }
31         else if(mysqli_num_rows($result_mobile)>0){
32             echo '<script type="text/javascript">';
33             echo 'setTimeout(function () { sweetAlert("Oops...", "Mobile number '. $mobile_number.
' is already exists!","error");';
34             echo '}, 500);</script>';
35         }else{
36             $activation_code = hash('sha256',mt_rand(0,1000));
```

Make sure that using this pseudorandom number generator is safe here.

```
5         {
6         header('location:index.php');
7         }
8         else{
9
10        if(isset($_POST['submit']))
11        {
12        $studentname=$_POST['studentname'];
13        $studentregno=$_POST['studentregno'];
14        $password=md5($_POST['password']);
15        $pincode = rand(100000,999999);
```

Make sure that using this pseudorandom number generator is safe here.

Estas vulnerabilidades podrían ser usada por atacantes para adivinar valores pseudoaleatorios producidos por funciones PHP (RAND) mediante ataques de fuerza bruta, debiendo ser verificado, y corregido, en caso afirmativo, recomendando el uso de funciones que se basen en un generador de valores aleatorios fuertes y seguros (*Random\_int()*, *Random\_bytes()*, etc). En caso que desee continuar usando la función *Random\_pseudo\_bytes ()* verifique el parámetro *crypto\_strong*, el cual permite verificar si los bytes pseudoaleatorios generados pueden ser utilizados de manera segura en operaciones criptográficas (generación de claves o tokens de autenticación), indicando:

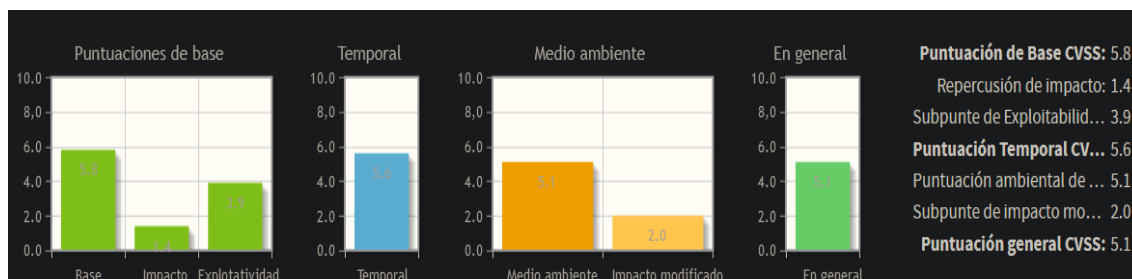
- ✓ true: si los datos aleatorios generados son criptográficamente seguros.
- ✓ false: si la fuente aleatoria no es suficientemente fuerte para fines criptográficos, aunque si lo sean para otros propósitos menos críticos.

#### Compliant Solution

```
$randomInt = random_int(0,99); // Compliant; generates a cryptographically secure random integer
```

Estas debilidades pertenecen a la OWASP – Top 10 2021, dentro de la categoría 2 llamada “Fallos Criptográficos”.

Estas vulnerabilidades podrían tener una puntuación CVSS medio, adjuntando grafico del resultado:



### 3.3.- RIESGO BAJO

Se han encontrado 43 supuestas vulnerabilidades de riesgo bajo que podrían afectar a los algoritmos hash criptográficos (MD2, MD4, MD5, MD6, HAVAL-128, HMAC-MD5, etc), siendo éstos, usados para el almacenamiento de datos sensibles (contraseñas) , generadores de token de seguridad o para el calculo de la integridad de los mensajes, por lo que se recomienda su verificación, y el uso de alternativas más seguras (SHA-256, SHA-512, SHA-3, bcrypt, scrypt, etc), siendo algoritmos más fuertes ante ataques de fuerza bruta.

#### Compliant Solution

```
// for a password
$hash = password_hash($password, PASSWORD_BCRYPT); // Compliant

// other context
$hash = hash("sha512", $data);
```

Estas debilidades pertenecen a la OWASP – Top 10 2021, dentro de la categoría 2 llamada “Fallos Criptográficos”.