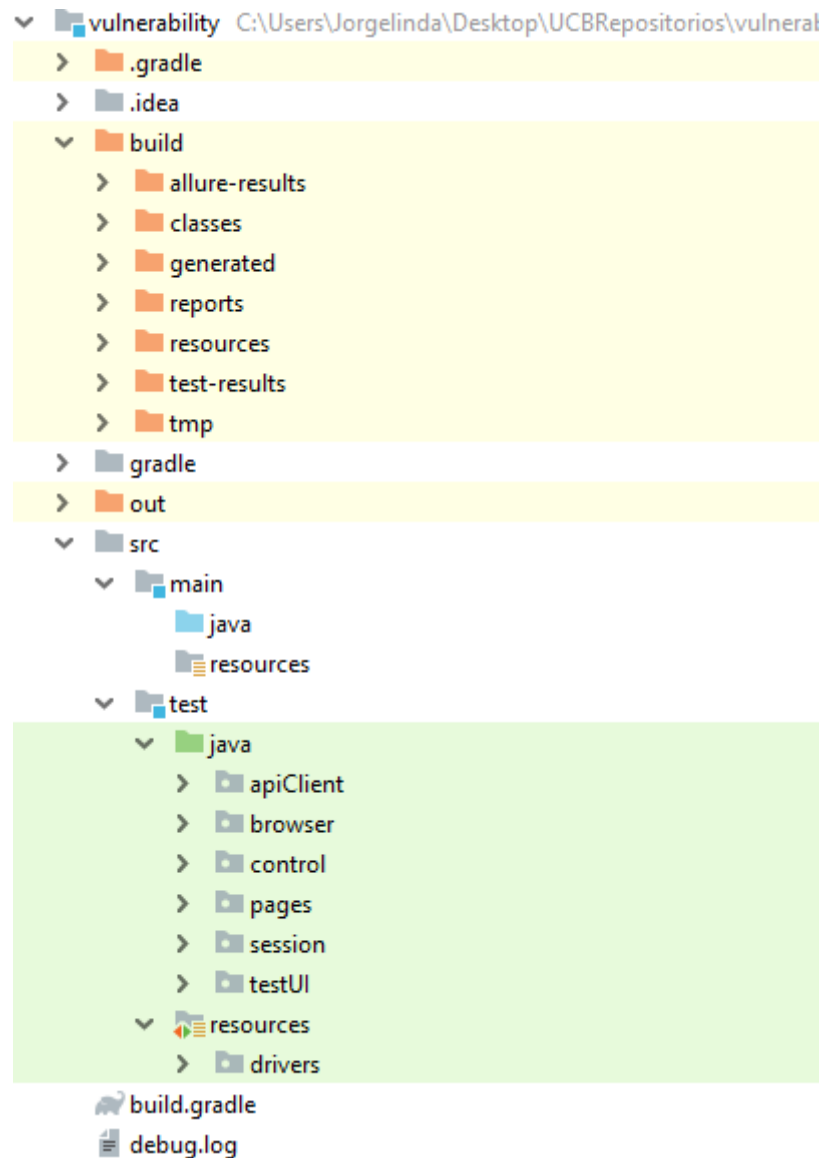


TODO IST PRUEBAS DE VULNERABILIDAD OWASP

1.	CREACION DEL PROYECTO PRINCIPAL.....	2
2.	ADICIONANDO LAS DEPENDENCIAS.....	3
3.	AGREGANDO LAS PRUEBAS Y LAS CLASES PRINCIPALES.....	3
4.	CORRIDA DE LAS PRUEBAS CREADAS.....	4
5.	GENERACION DEL REPORTE ALLURE	4
6.	REPORTE ALLURE – SECCION PRINCIPAL.....	4
7.	REPORTE ALLURE – SECCION “SUITES”	5
8.	REPORTE ALLURE – SECCION “TEST – LOGIN TODO IST TEST”	5
9.	REPORTE ALLURE – SECCION “TEST – VULNERABILITY TEST”	6
10.	REPORTE ALLURE – SECCION “REPORTE VULNERABILITY”	6
11.	REPORTE ALLURE – SECCION “SUMMARY REPORT”	7
12.	REPORTE ALLURE – SECCION “GRAFICOS”	8
13.	REPORTE ALLURE – SECCION “BEHAVIOR – TEST: VERIFY THE LOGIN USING EMAIL, PASSWORD AND NAME”	8
14.	REPORTE ALLURE – SECCION “BEHAVIOR – TEST: VERIFY THE VULNERABILITY TEST USING OWASP”	9
15.	PROGRESO TERMINADO – OWASP ZAP	10
16.	REPOSITORIO GITHUB CON EL CODIGO DISPONIBLE.....	10

TODO.IST – PRUEBAS OWASP

1. CREACION DEL PROYECTO PRINCIPAL



2. ADICIONANDO LAS DEPENDENCIAS

```
}dependencies {
    testCompile group: 'junit', name: 'junit', version: '4.12'

    // https://mvnrepository.com/artifact/org.seleniumhq.selenium/selenium-java
    compile group: 'org.seleniumhq.selenium', name: 'selenium-java', version: '3.141.59'

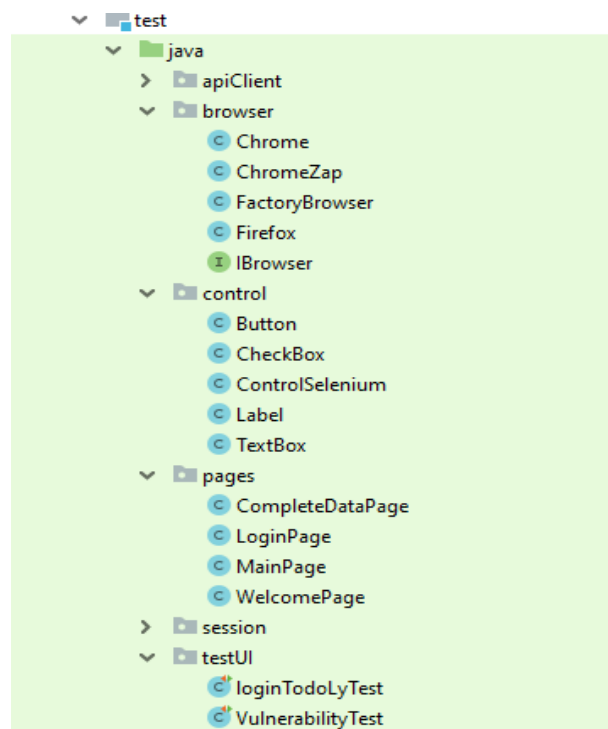
    // https://mvnrepository.com/artifact/io.rest-assured/rest-assured
    testCompile group: 'io.rest-assured', name: 'rest-assured', version: '4.3.1'
    // https://mvnrepository.com/artifact/io.rest-assured/json-path
    compile group: 'io.rest-assured', name: 'json-path', version: '4.3.1'
    // https://mvnrepository.com/artifact/io.rest-assured/json-schema-validator
    compile group: 'io.rest-assured', name: 'json-schema-validator', version: '4.3.1'
    // https://mvnrepository.com/artifact/io.rest-assured/rest-assured-common
    compile group: 'io.rest-assured', name: 'rest-assured-common', version: '4.3.1'
    // https://mvnrepository.com/artifact/io.rest-assured/rest-assured-all
    compile group: 'io.rest-assured', name: 'rest-assured-all', version: '4.3.1'

    // https://mvnrepository.com/artifact/io.qameta.allure/allure-junit4
    testCompile group: 'io.qameta.allure', name: 'allure-junit4', version: '2.13.5'
}

allure {
    autoconfigure = true
    version = '2.6.0'
    aspectjweaver = true
}

// gradle clean test
// allure serve ${PATH}/allure-results
```

3. AGREGANDO LAS PRUEBAS Y LAS CLASES PRINCIPALES



4. CORRIDA DE LAS PRUEBAS CREADAS

```
> Task :compileTestJava
Note: C:\Users\Jorgelinda\Desktop\UCBRepositorios\vulnerability\src\test\java\browser\ChromeZap.java uses or overrides a deprecated API.
Note: Recompile with -Xlint:deprecation for details.
<=====--> 87% EXECUTING [1m 52s]

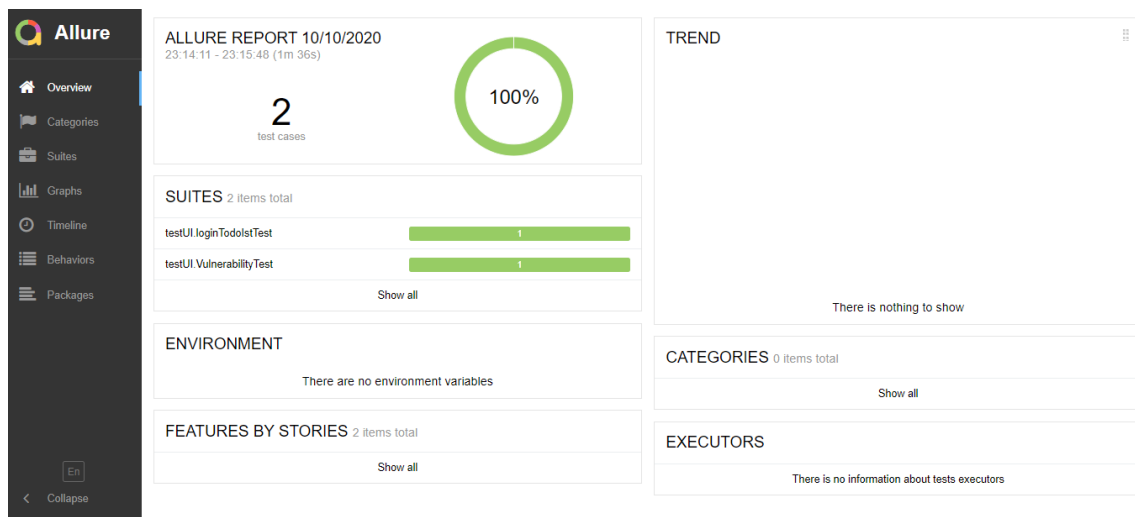
Deprecated Gradle features were used in this build, making it incompatible with Gradle 7.0.
Use '--warning-mode all' to show the individual deprecation warnings.
See https://docs.gradle.org/6.6.1/userguide/command\_line\_interface.html#sec:command\_line\_warnings

BUILD SUCCESSFUL in 2m 9s
4 actionable tasks: 4 executed
```

5. GENERACION DEL REPORTE ALLURE

```
C:\Users\Jorgelinda\Desktop\UCBRepositorios\vulnerability>allure serve build\allure-results
Generating report to temp directory...
Report successfully generated to C:\Users\JORGEL~1\AppData\Local\Temp\5298669854545821424\allure-report
Starting web server...
2020-10-10 23:09:18.027:INFO::main: Logging initialized @4366ms to org.eclipse.jetty.util.log.StdErrLog
Server started at <http://192.168.56.1:65322/>. Press <Ctrl+C> to exit
```

6. REPORTE ALLURE – SECCION PRINCIPAL



7. REPORTE ALLURE – SECCION “SUITES”

The screenshot shows the Allure Suites report page. On the left is a dark sidebar with navigation links: Overview, Categories, Suites (highlighted), Graphs, Timeline, Behaviors, and Packages. The main area has a header with the Allure logo and the title 'Suites'. Below the header is a table with columns: order, name, duration, status, and a status summary bar showing 0 failures, 0 errors, 2 warnings, and 0 skipped. The table lists two suites: 'testUI.loginTodoIstTest' and 'testUI.VulnerabilityTest', both with a green '1' icon indicating one test passed.

8. REPORTE ALLURE – SECCION “TEST – LOGIN TODO IST TEST”

The screenshot shows the Allure Test report page for the test 'verify The Login Using Email, Password And Name'. The left sidebar is the same as in the previous screenshot. The main area has a header with the test name and a 'Passed' status. Below the header is a table with columns: order, name, duration, status, and a status summary bar showing 0 failures, 0 errors, 2 warnings, and 0 skipped. The table lists one test: '#1 verify The Login Using Email, Password And Name' with a duration of 30s 970ms and a green '1' icon. The right panel shows the test details: Severity: normal, Duration: 30s 970ms, Description: This test case is to verify The Login Using Email, Password And Name, Owner: Grecia Machaca, and Execution: Click on [Regístrate] Button on Main Page 1 parameter 3ms, Type value : 'grace.lopez.martinez@gmail.com' on [email] textbox on Login Page 1 parameter 0s, Click on [signup] button on Login Modal Page 1 parameter 0s, Type value : 'Grace' on [name] textbox on completeData Page 1 parameter 0s, Type value : 'l0pezGr4c3123' on [password] textbox on completeData Page 1 parameter 0s, Click on [signup] button on completeData Page 1 parameter 0s.

9. REPORTE ALLURE – SECCION “TEST – VULNERABILITY TEST”

Suites

order

name

duration

status

Status: 0 0 2 0 0

Marks:

testUI.loginTodoistTest

#1 verify The Login Using Email, Password And Name30s 970ms

testUI.VulnerabilityTest

#1 Verify the vulnerability test using OWASP1m 05s

testUI.VulnerabilityTest.verifyVulnerabilityScanTest

Passed

Verify the vulnerability test using OWASP

OverviewHistoryRetries

Severity: normal

Duration: 0 1m 05s

Description

This test case is to verify the attack of vulnerability using owasp with the last pluggins

Owner

Grecia Machaca

Execution

Test body

Start Vulnerability Test using OWASP ZAP4s 786ms

Monitoring Scan of OWASP ZAP 100% 1 parameter1m 00s

OWASP Report Vulnerability Detail371.2 KB

OWASP Summary Report38.3 KB

10. REPORTE ALLURE – SECCION “REPORTE VULNERABILITY”

OWASP Report Vulnerability Detail

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	8
Low	13
Informational	17

Alert Detail

Medium (High)	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	https://analytics.google.com/g/collect?v=2&tid=G-HCDW2MG61G&utm=2oe9u1&p=928984875&sr=1366x768&gaze=1&ul=es-es&cid=339312235.1602384068&s=3&dt=https%3A%2F%2Ftodoist.com%2Fes&dr=&dt=Todoist%3A%20La%20%22to%20do%20list%22%20para%20organizar%20tus%20proyec
Method	POST
Parameter	sid
Evidence	1602384067374.miekbsbv
URL	https://analytics.google.com/g/collect?v=2&tid=G-HCDW2MG61G&utm=2oe9u1&p=1990064371&sr=1366x768&gaze=1&ul=es-es&cid=1424924324.1602384507&s=2&dt=https%3A%2F%2Ftodoist.com%2Fes&dr=&dt=Todoist%3A%20La%20%22to%20do%20list%22%20para%20organizar%20tus%20proyec
Method	POST
Parameter	sid
Evidence	1602384509814.304e5b&ct=1&seg=0&en=user_engagement&_fv=1&_ss=1&ep.daypart=Night%20-%2021-23&ep.weekday_num=Weekend&ep.hit_timestamp=2020-10-10T22%3A48%3A29.814-04%3A00&ep.mmfw_version=MMFW%20-%20031219%20-%20GTM-MF4CZSB&ep.all_data=true&ep.debug_mode=true

11. REPORTE ALLURE – SECCION “SUMMARY REPORT”

OWASP Summary Report

scanProgress

idhttps://todoist.com

HostProcess

Plugin

namePath Traversal

id6

qualityrelease

statusComplete

timeInMs4

reqCount0

alertCount0

Plugin

nameRemote File Inclusion

id7

qualityrelease

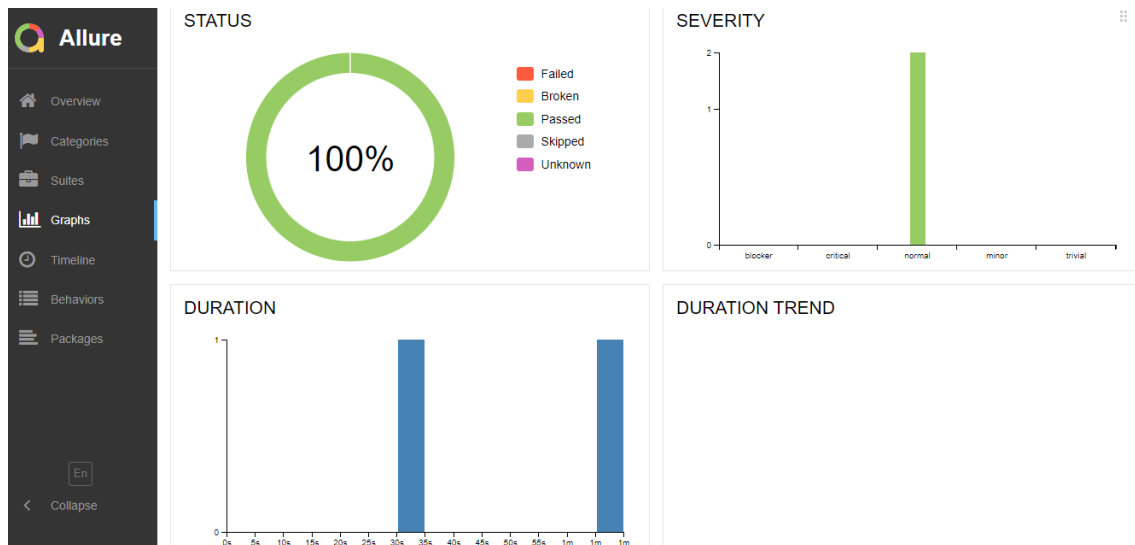
statusComplete

timeInMs4

reqCount0

alertCount0

12. REPORTE ALLURE – SECCION “GRAFICOS”



13. REPORTE ALLURE – SECCION “BEHAVIOR – TEST: VERIFY THE LOGIN USING EMAIL, PASSWORD AND NAME”

Behaviors

order name duration status Status: 0 0 2 0 0

Marks: [icon] [icon]

order	name	duration	status
#1	verify The Login Using Email, Password And Name	30s 970ms	Passed
#2	Verify the vulnerability test using OWASP	1m 05s	Passed

Passed **verify The Login Using Email, Password And Name**

Overview History Retries

Severity: normal

Duration: 30s 970ms

Description

This test case is to verify The Login Using Email, Password And Name

Owner

Grecia Machaca

Execution

Test body

- Click on [Regístrate] Button on Main Page 1 parameter 3ms
- Type value : 'grace.lopez.martinez@gmail.com' on [email] textbox on Login Page 1 parameter 0s
- Click on [signup] button on Login Modal Page 1 parameter 0s
- Type value : 'Grace' on [name] textbox on completeData Page 1 parameter 0s
- Type value : 'l0pezGr4c3123' on [password] textbox on completeData Page 1 parameter 0s
- Click on [signup] button on completeData Page 1 parameter 0s

14. REPORTE ALLURE – SECCION “BEHAVIOR – TEST: VERIFY THE VULNERABILITY TEST USING OWASP”

Behaviors



order

name

duration

status

Status: 00200

Marks:  

✓ #1 verify The Login Using Email, Password And Name30s 970ms

✓ #2 Verify the vulnerability test using OWASP1m 05s

Passed

Verify the vulnerability test using OWASP

Overview

History

Retries

Severity: normal

Duration: 1m 05s

Description

This test case is to verify the attack of vulnerability using owasp with the last pluggins

Owner

Grecia Machaca

Execution

Test body

✓ Start Vulnerability Test using OWASP ZAP4s 786ms

> Monitoring Scan of OWASP ZAP 100% 1 parameter1m 00s

> OWASP Report Vulnerability Detail371.2 KB✕

> OWASP Summary Report38.3 KB✕

15. PROGRESO TERMINADO – OWASP ZAP

https://todoist.com/es Progreso del escaneo

Progreso Tabla de respuesta

Sitio: https://todoist.com

	Fuerza	Progreso	Transcurrido	Requis...	Alertas	Est...
Analizador			00:00.000	0		
Plugin						
Path Traversal	Medio	<div></div>	00:00.004	0	0	✓
Remote File Inclusion	Medio	<div></div>	00:00.004	0	0	✓
Source Code Disclosure - /WEB-INF folder	Medio	<div></div>	00:07.840	13	0	✓
External Redirect	Medio	<div></div>	00:07.839	0	0	✓
Server Side Include	Medio	<div></div>	00:00.015	0	0	✓
Cross Site Scripting (Reflected)	Medio	<div></div>	00:00.000	0	0	✓
Cross Site Scripting (Persistent) - Prime	Medio	<div></div>	00:00.000	0	0	✓
Cross Site Scripting (Persistent) - Spider	Medio	<div></div>	00:01.001	1	0	✓
Cross Site Scripting (Persistent)	Medio	<div></div>	00:00.015	0	0	✓
SQL Injection	Medio	<div></div>	00:00.000	0	0	✓
Server Side Code Injection	Medio	<div></div>	00:00.000	0	0	✓
Remote OS Command Injection	Medio	<div></div>	00:00.000	0	0	✓
Directory Browsing	Medio	<div></div>	00:01.342	1	0	✓
Buffer Overflow	Medio	<div></div>	00:00.000	0	0	✓
Error de formato de cadena	Medio	<div></div>	00:00.016	0	0	✓
CRLF Injection	Medio	<div></div>	00:00.000	0	0	✓
Parameter Tampering	Medio	<div></div>	00:00.000	0	0	✓
Reglas de búsqueda activadas para el Scri...	Medio	<div></div>	00:00.000	0	0	✗
Source Code Disclosure - Git	Medio	<div></div>	00:00.000	0	0	✓
Source Code Disclosure - File Inclusion	Medio	<div></div>	00:00.000	0	0	✓
Ejecución remota de código - Shell Shock	Medio	<div></div>	00:00.000	0	0	✓
Httpoxy - Proxy Header Misuse	Medio	<div></div>	00:07.767	10	0	✓
Anti-CSRF Tokens Check	Medio	<div></div>	00:00.000	0	0	✓
Vulnerabilidades de OpenSSL HeartBleed	Medio	<div></div>	00:00.885	3	0	✓
Desconfiguración de Dominio cruzado	Medio	<div></div>	00:01.170	2	0	✓
Divulgación del código fuente - CVE-2012-...	Medio	<div></div>	00:02.451	1	0	✓
Ejecución remota de código - CVE-2012-1...	Medio	<div></div>	00:01.141	2	0	✓
Fijación de Sesión	Medio	<div></div>	00:00.000	0	0	✓
Inyección SQL - MySQL	Medio	<div></div>	00:00.000	0	0	✓
Inyección SQL - SQL hipersónico	Medio	<div></div>	00:00.000	0	0	✓
Inyección SQL - Oráculo	Medio	<div></div>	00:00.000	0	0	✓
Inyección SQL - PostgreSQL	Medio	<div></div>	00:00.000	0	0	✓
SQL Injection - SQLite	Medio	<div></div>	00:00.015	0	0	✓
SQL Injection - MsSQL	Medio	<div></div>	00:00.000	0	0	✓

Copiar al portapapeles cerrar

16. REPOSITORIO GITHUB CON EL CODIGO DISPONIBLE

<https://github.com/Greciamy/todoIstVulnerability.git>