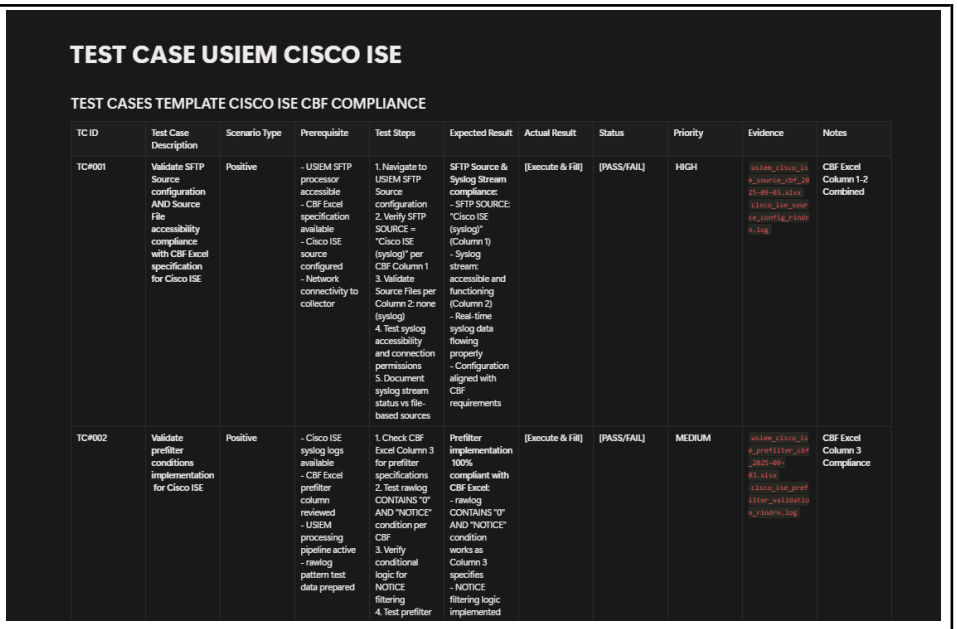
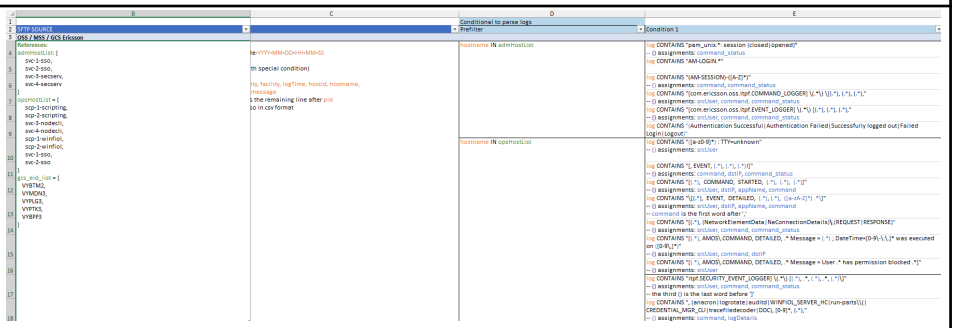
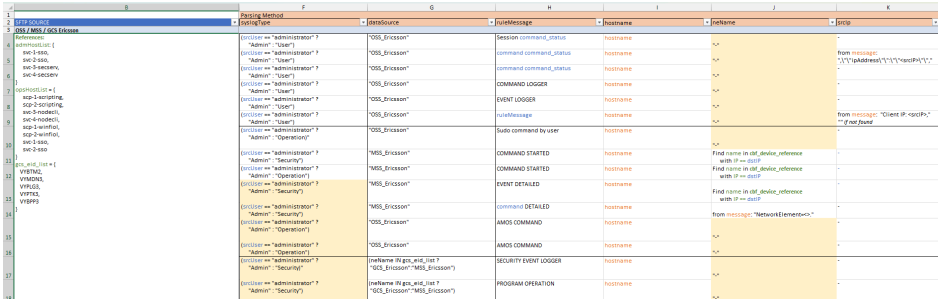
Log Book KP

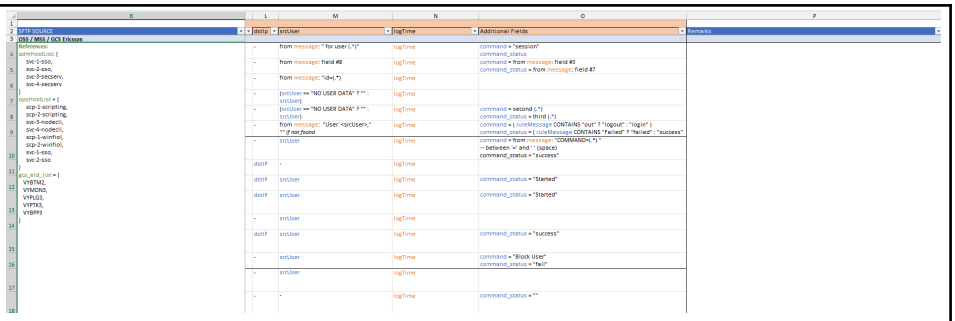
JURUSAN : TEKNIK KOMPUTER DAN INFORMATIKA	PROGRAM STUDI : (D3) TEKNIK INFORMATIKA

No : 11	Periode : 8 September s.d. 12 September 2025
Sub No : 11.1	Hari/Tanggal : Senin, 8 September 2025
Proyek	Nama Proyek : USIEM Tsel Project
	Project Manager : Irfan Nurdin Salman
	Technical Leader : Regina Christiany
Tugas	Writing Test Cases for USIEM Tsel Project
Waktu dan Kegiatan Harian	08.00 WIB Hadir di Meja Kerja Menyelesaikan test case cisco_ise sesuai dengan parsing cbf excel --- 12.00 WIB Istirahat makan siang di rumah karena WFH --- 13.00 WIB Mengeksplor penggunaan Jenkins dan OWASP ZAP --- 17.00 WIB Merapikan barang-barang karena jam kerja sudah selesai
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google Docs/Words • Wiki Tritronik • Notion • GlobalProtect

Hasil Kerja	 - Berhasil menyelesaikan test case untuk cisco_ise apakah pass atau terdapat defect pada masing-masing event sample di processor cisco_ise - Mendapatkan eksplorasi terkait penggunaan Jenkins dan OWASP di lingkup general
Lesson Learned	Quote of the day: There's no audience to impress. No people to please. No applause to chase. Do everything for yourself. Stop comparing your journey to others and move at your own pace.
Keterangan	-

No : 11	Periode : 8 September s.d. 12 September 2025
Sub No : 11.2	Hari/Tanggal : Selasa, 9 September 2025
Proyek	Nama Proyek : USIEM Tsel Project
	Project Manager : Irfan Nurdin Salman
	Technical Leader : Regina Christiany
Tugas	Finding Test Cases Sample for USIEM Tsel Project based on excel file Parsing CBF
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3

	Melakukan revisi pada test case mss_ericsson --- 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor --- 13.00 WIB Mencari sample untuk sgsn_zte --- 17.00 WIB Menyiapkan barang-barang untuk segera pulang
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words/ Google Drive • Notion • Kafka • Excel • Prisma Browser • GlobalProtect
Hasil Kerja	 



TEST CASE USIEM OSS/MSS/GCS ERICSSON

TEST CASES TEMPLATE OSS/MSS/GCS ERICSSON CBF COMPLIANCE

TC ID	Test Case Description	Scenario Type	Prerequisite	Test Steps	Expected Result	Actual Result	Status	Priority	Evidence	Notes
TC#001	Validate SFTP Source configuration AND Source File accessibility compliance with CBF Excel specification for OSS/MSS/GCS Ericsson	Positive	- USIEM SFTP processor accessible - CBF Excel specification available - OSS/MSS/GCS Ericsson source configured - Network connectivity to collector	1. Navigate to USIEM SFTP Source configuration 2. Verify SFTP SOURCE = "OSS/MSS/GCS Ericsson" per CBF Column 1 3. Validate Source Files per Column 2: enm-csv-logfile, svc-1-sso, svc-2-sso, svc-3-secserv, svc-4-secserv 4. Test file accessibility and read permissions for available files 5. Document which files are accessible vs pending	SFTP Source & Source Files compliance: - SFTP SOURCE: "OSS/MSS/GCS Ericsson" (Column 1) - Available Files: enm-csv-logfile accessible (Column 2) - Service files status documented (available/pending) - Configuration aligned with CBF requirements	[Execute & Fill]	[PASS/FAIL]	HIGH	usiem_oss_source_files_cbf_2025-09-02.xlsx oss_source_config_rindrn.log	CBF Excel Column 1-2 Combined
TC#002	Validate prefilter conditions implementation for OSS/MSS/GCS Ericsson	Positive	- OSS/MSS/GCS Ericsson logs available - CBF Excel prefilter column reviewed - USIEM processing	1. Check CBF Excel Column 3 for prefilter specifications 2. Test "hostname IN opsHostList" condition per CBF 3. Verify	Prefilter implementation 100% compliant with CBF Excel: - "hostname IN opsHostList" condition works as Column 3	[Execute & Fill]	[PASS/FAIL]	MEDIUM	usiem_oss_prefilter_cbf_2025-09-02.xlsx oss_prefilter_validation_rindrn.log	CBF Excel Column 3 Compliance

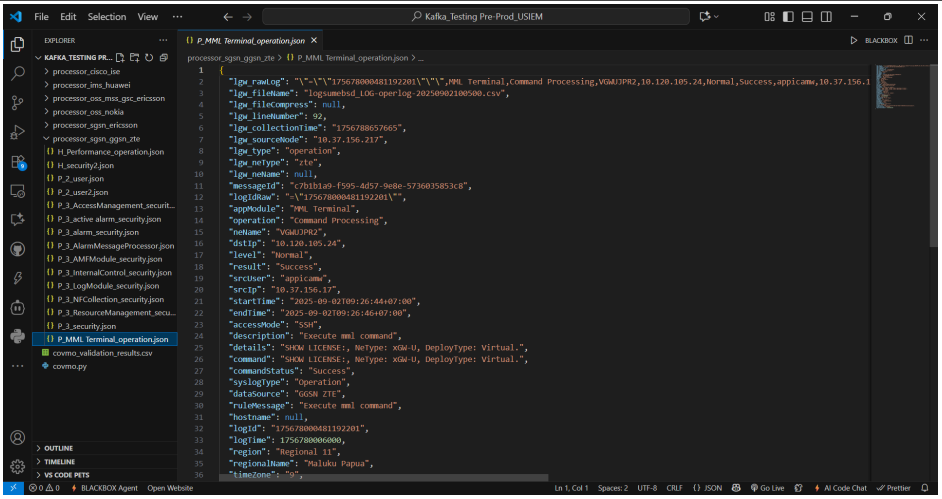
ZTE

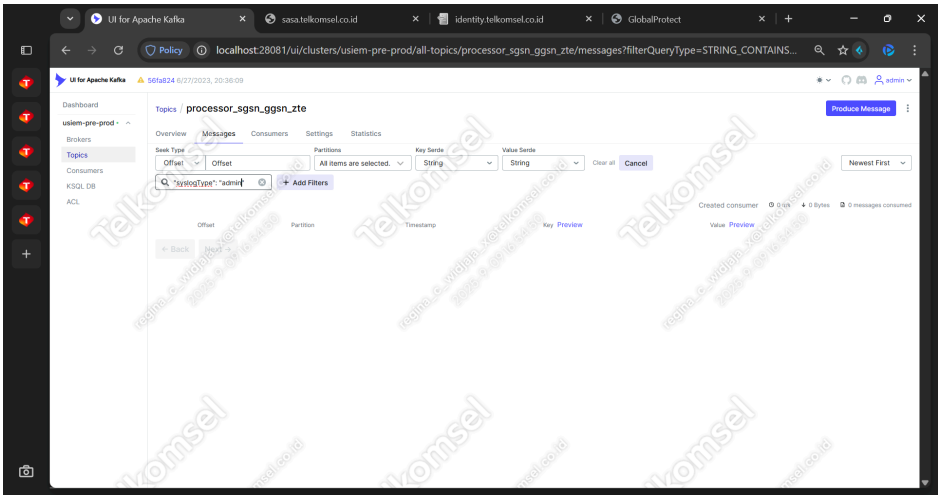
Collection Schedule:
hourly @hh:30 (file is started at hh:05)
Directory:
/logsumebsd
/logsumeprivatecore
/logsumeuso
Reference: zteUserSystemList =
{
access-api-operation,
vnfm, vnf_to_vnfm, VCHRBSD1,
SMDGWC_TO_VNFM, SMDGWU_TO_VNFM,
BPPGWU_TO_VNFM, BPPGWC_TO_VNFM,
PTKGWU_TO_VNFM, PTKGWC_TO_VNFM,
MDOGWU_TO_VNFM, MDOGWC_TO_VNFM,
TMKGWC_TO_VNFM, TMKGWU_TO_VNFM,
PALGWC_TO_VNFM, PALGWU_TO_VNFM,
NFV-U-VNFM-TO-NFVO, NFV-U-VNFM-TO-NFVO,
SMDCG1, BPPCG1, PTKCG1, MDOCG1
}

Filename:
LOG-operlog-YYYYMMDDhhmmss.csv
Log format:
csv with header
Field assignments:
logID, appModule, operation, neName, dstIP, level, result, srcUser, srcIP, startTime, logTime, accessMode, description, details

Filename:
LOG-seclog-YYYYMMDDhhmmss.csv
Log format:
csv with header
Field assignments:
logID, ruleMessage, srcUser, level, logTime, result, srcIP, accessMode, detail

Filename:
LOG-syslog-YYYYMMDDhhmmss.csv
Log format:
csv with header
Field assignments:
logID, ruleMessage, level, appModule, startTime, logTime, srcIP, details

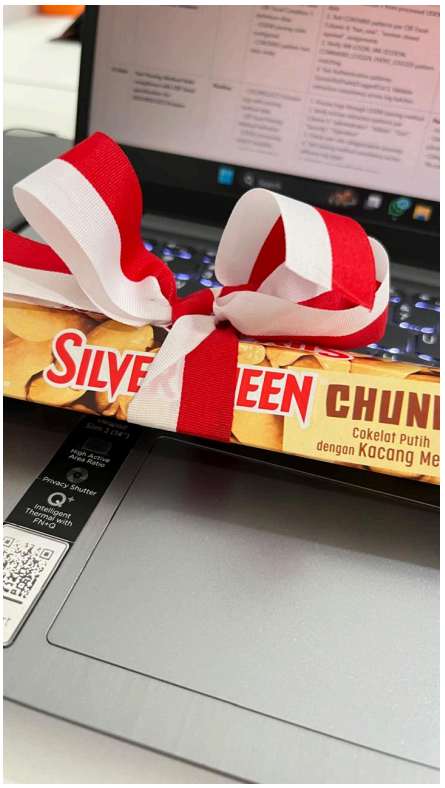
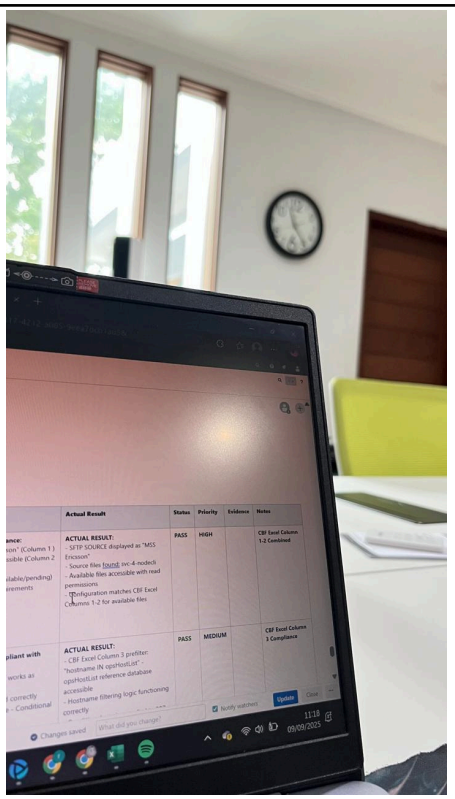
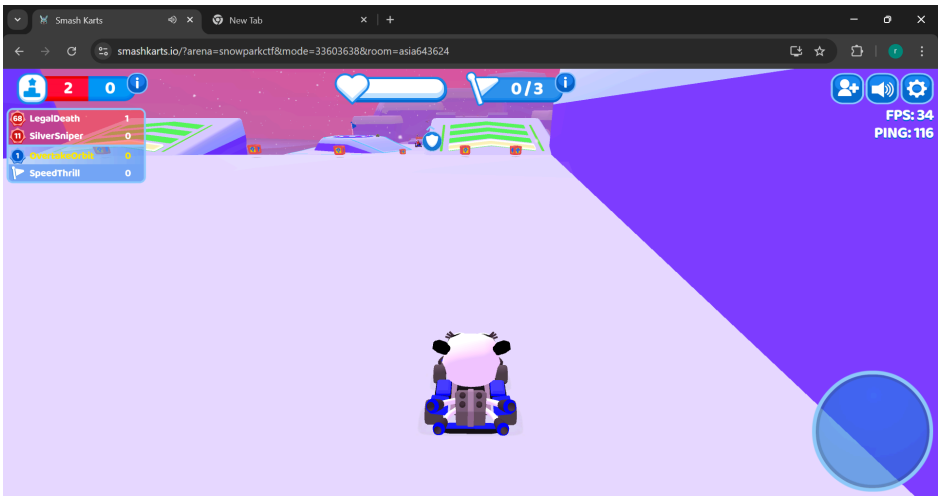




• Berhasil menerapkan revisi pada test case mss_ericsson yang sudah ada sebelumnya

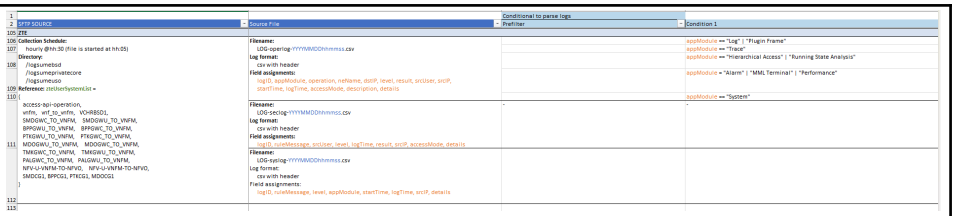
• Berhasil menemukan sampel pada topik sgsn_zte yang cocok sesuai dengan spesifikasi pada parsing cbf pada excel

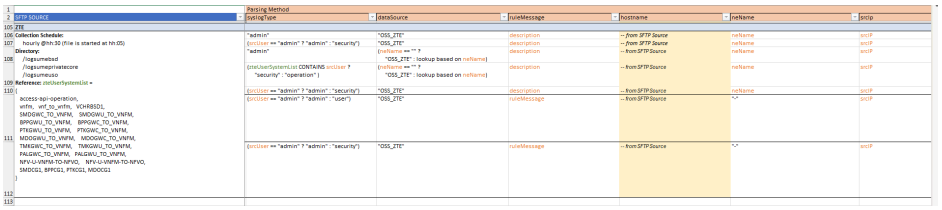
Lesson Learned	Quote of the day: Fear is “What if.” Faith is “Even if.”

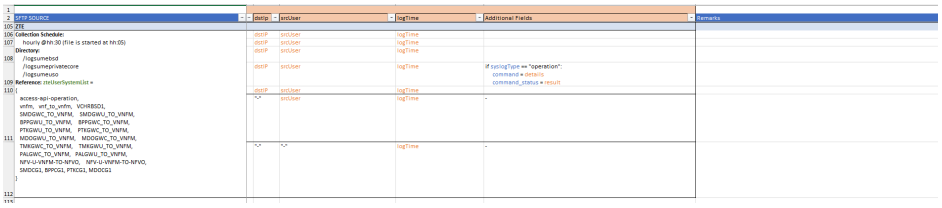
	  Mendapat rewards karena membantu dokumentasi badminton Additional:  Saya diajak main smashkart oleh teman-teman kantor seusai jam kerja.
Keterangan	-

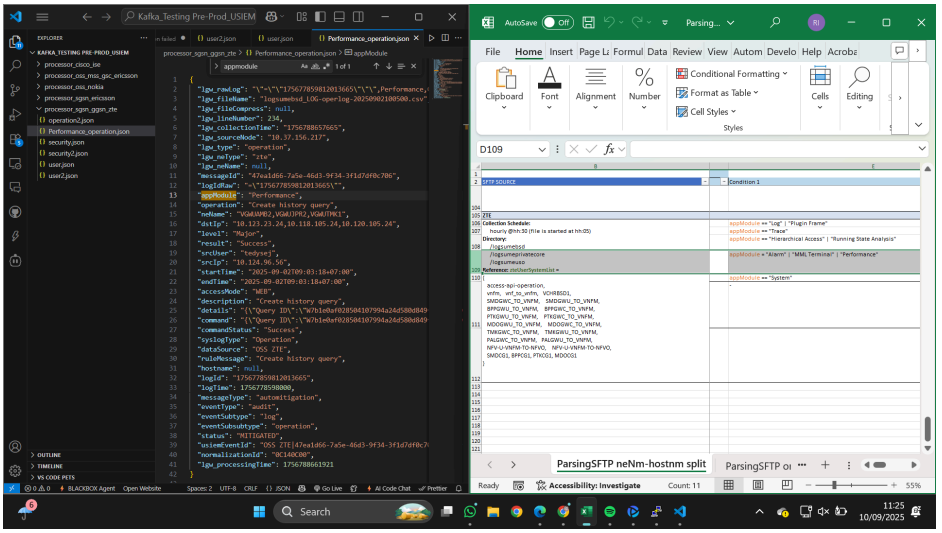
No : 11	Periode : 8 September s.d. 12 September 2025
Sub No : 11.3	Hari/Tanggal : Rabu, 10 September 2025
Proyek	Nama Proyek : USIEM Tsel Project Project Manager : Irfan Nurdin Salman Technical Leader : Regina Christiany
Tugas	Execute Test Cases Sample for USIEM Tsel Project based on excel file Parsing CBF
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3 Membuat test case untuk topik sgsn_zte _____ 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor _____ 13.00 WIB Mencari sampel untuk topik sgsn_zte _____ 15.00 WIB Melakukan execute test case topik sgsn_zte _____ 17.00 WIB Menyiapkan barang-barang untuk segera pulang
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words/ Google Drive • Notion • Kafka • VS Code • Excel • Prisma Browser • Putty • GlobalProtect

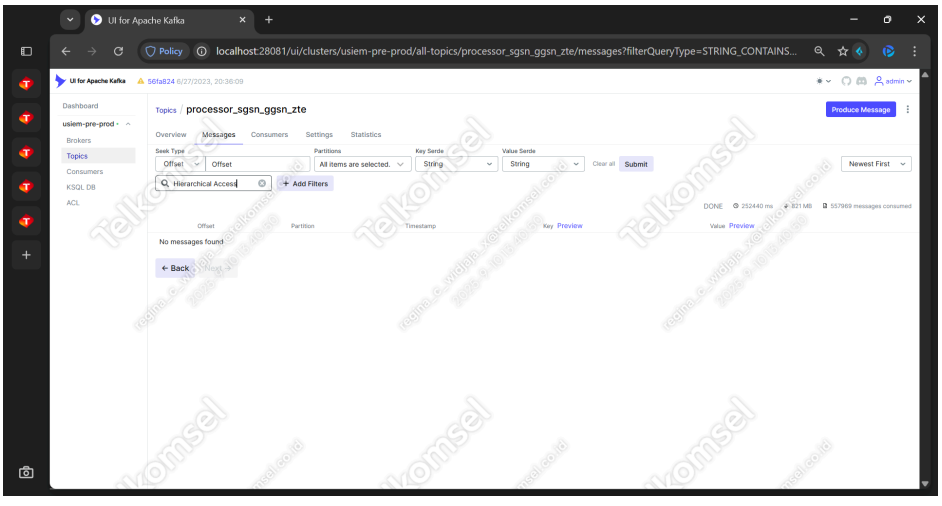
Hasil Kerja

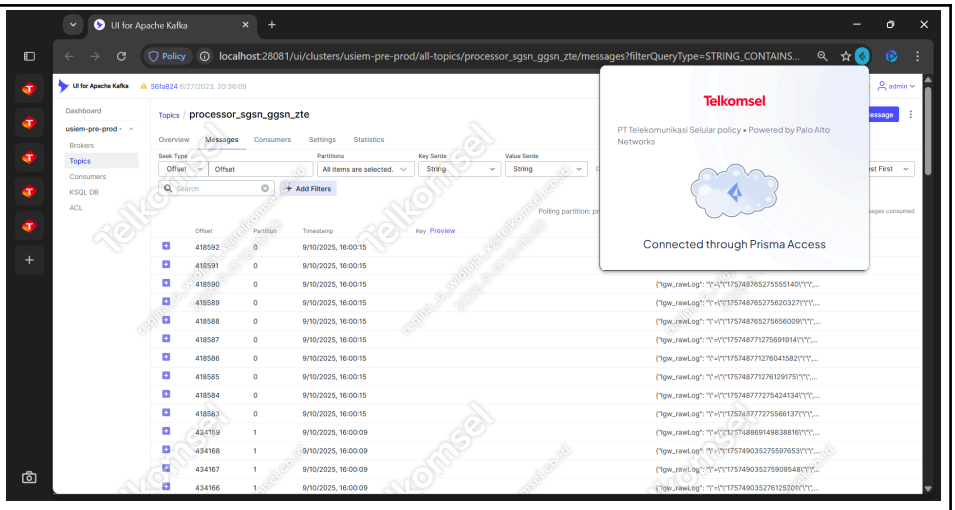
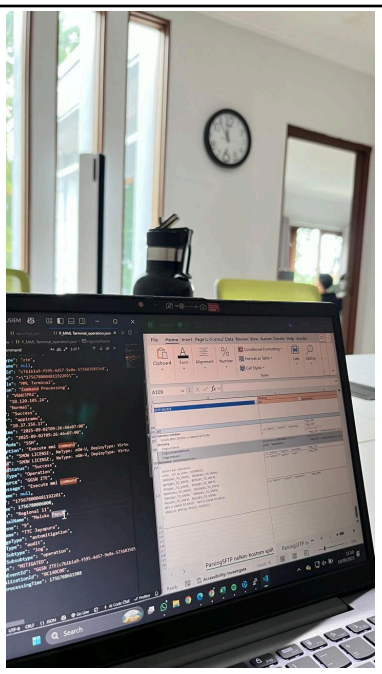
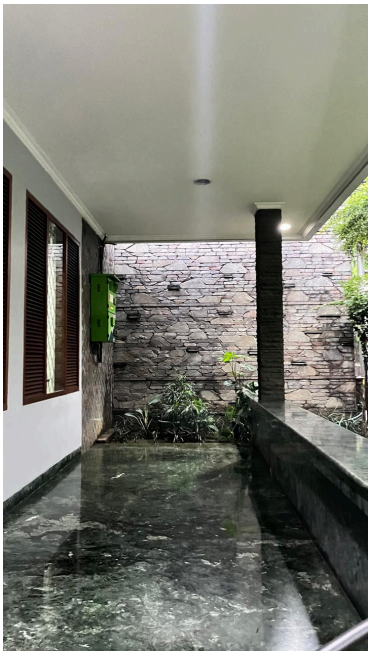






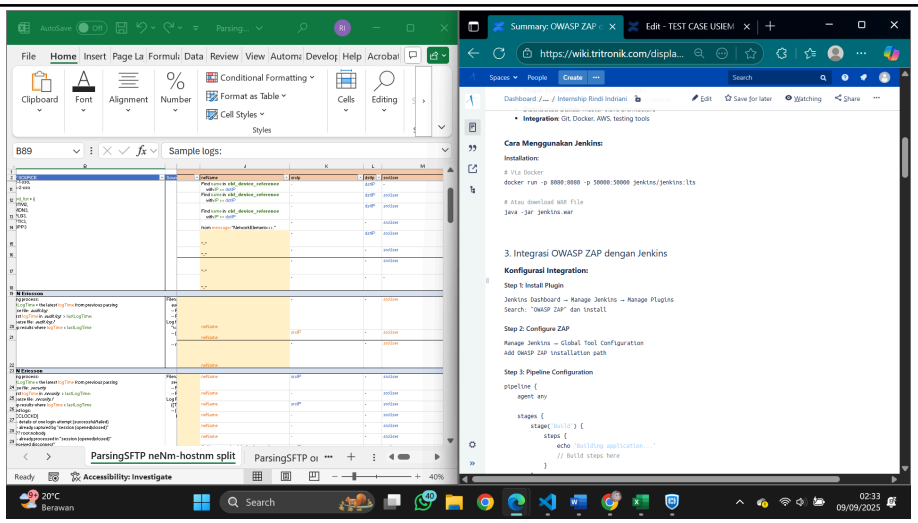


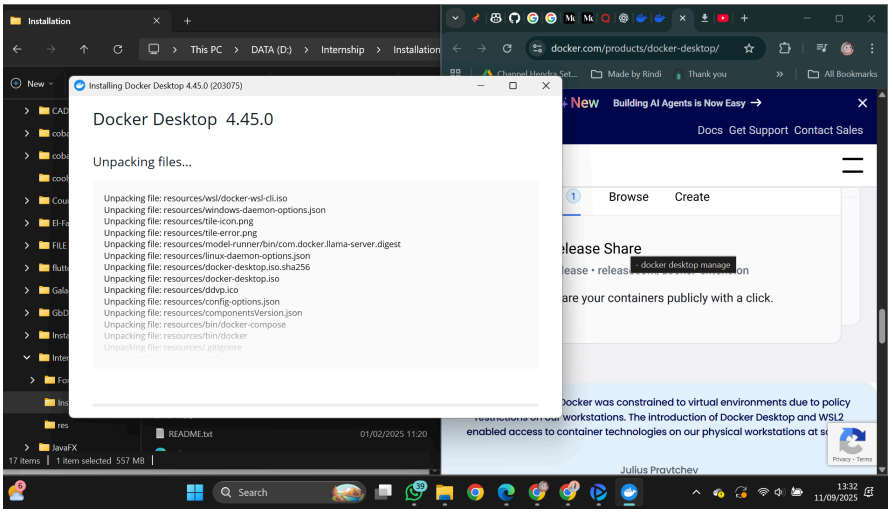


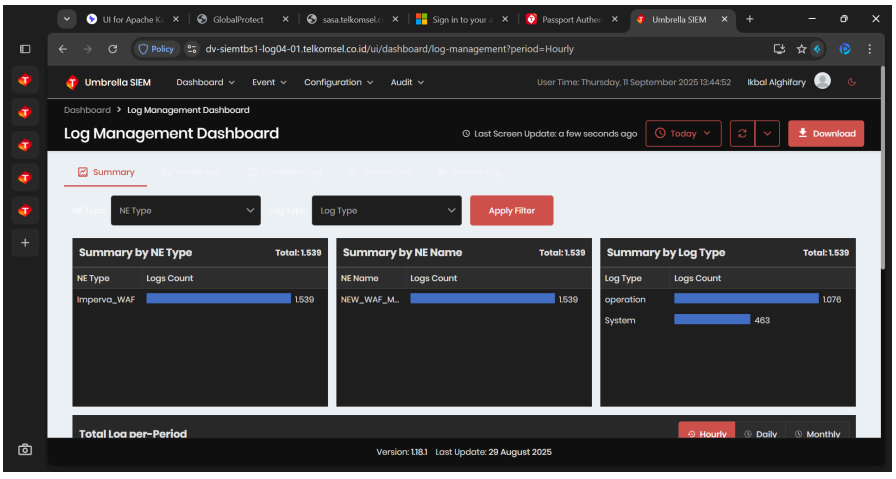
	 • Memiliki test case untuk menuangkan hasil temuan pada topik sgsn_zte baik pun itu failed maupun pass • Menemukan sampel pada topik sgsn_zte lainnya • Melakukan execute test pada test case topik sgsn_zte
Lesson Learned	Quotes of the day: The grass is greener on my side because I wake up. everyday. and. water. it.
Keterangan	 

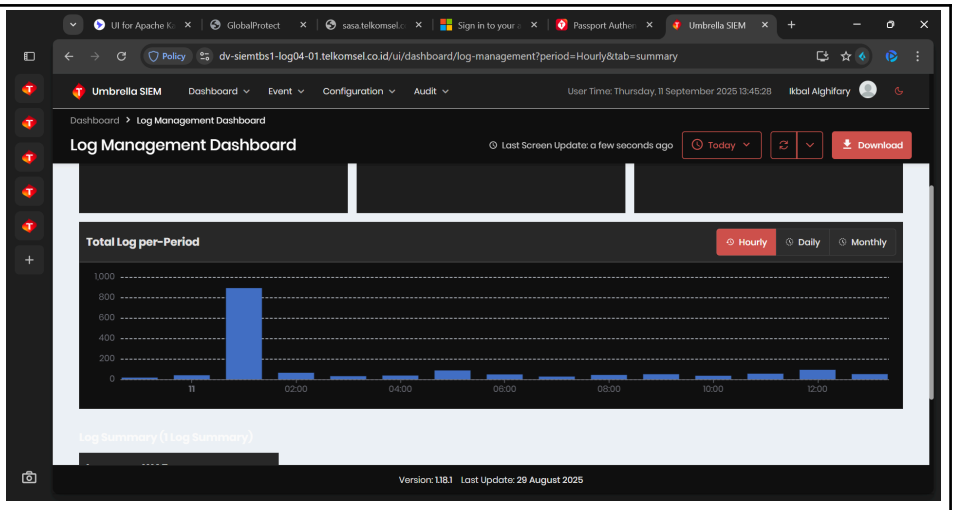
No : 11	Periode : 8 September s.d. 12 September 2025
Sub No : 11.4	Hari/Tanggal : Kamis, 11 September 2025
Proyek	Nama Proyek : USIEM Tsel Project Project Manager : Irfan Nurdin Salman Technical Leader : Regina Christiany
Tugas	Write Test Cases and finding sample for testing USIEM Tsel Project Topics sgsn_ericcson based on excel file Parsing CBF
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3 Mengeksplorasi lebih dalam terkait OWASP ZAP dan Jenkins serta integrasinya untuk security testing _____ 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor _____ 13.00 WIB Melanjutkan mencari sampel dengan topik sgsn_zte lainnya _____ 15.00 WIB Mencari sampel topik ims_huawei _____ 17.00 WIB Menyiapkan barang-barang untuk segera pulang
Tools yang digunakan	• Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words/ Google Drive • Notion • Kafka • VS Code • Prisma Browser • Putty • Excel • GlobalProtect

Hasil Kerja


Cara Menggunakan Jenkins:
Installation:
3. Integrasi OWASP ZAP dengan Jenkins
Konfigurasi Integration:
Step 1: Install Plugin
Step 2: Configure ZAP
Step 3: Pipeline Configuration


Installing Docker Desktop 4.45.0 (203075)
Docker Desktop 4.45.0
Unpacking files...
Unpacking file: resources/wsl/docker-wsl-cli.iso
Unpacking file: resources/windows-daemon-options.json
Unpacking file: resources/tile-icon.png
Unpacking file: resources/tile-error.png
Unpacking file: resources/model-runner/bin/com.docker.llama-server.digest
Unpacking file: resources/linux-daemon-options.json
Unpacking file: resources/docker-desktop.iso.sha256
Unpacking file: resources/docker-desktop.iso
Unpacking file: resources/ddvp.ico
Unpacking file: resources/config-options.json
Unpacking file: resources/componentsVersion.json
Unpacking file: resources/bin/docker-compose
Unpacking file: resources/bin/docker
Unpacking file: resources/.gitignore


Umbrella SIEM
Log Management Dashboard
Summary by NE Type
Summary by NE Name
Summary by Log Type
Total Log per-Period

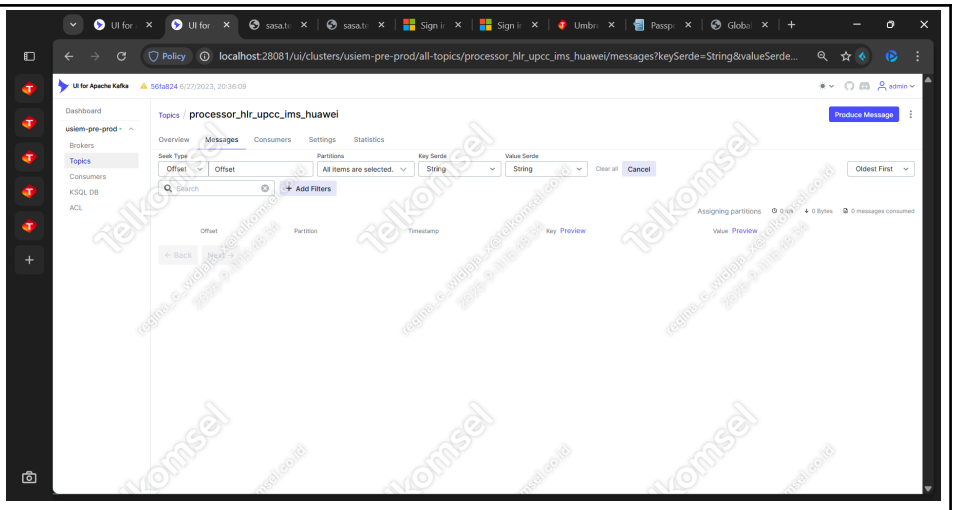
<table>
<tr>
<td></td>
<td>


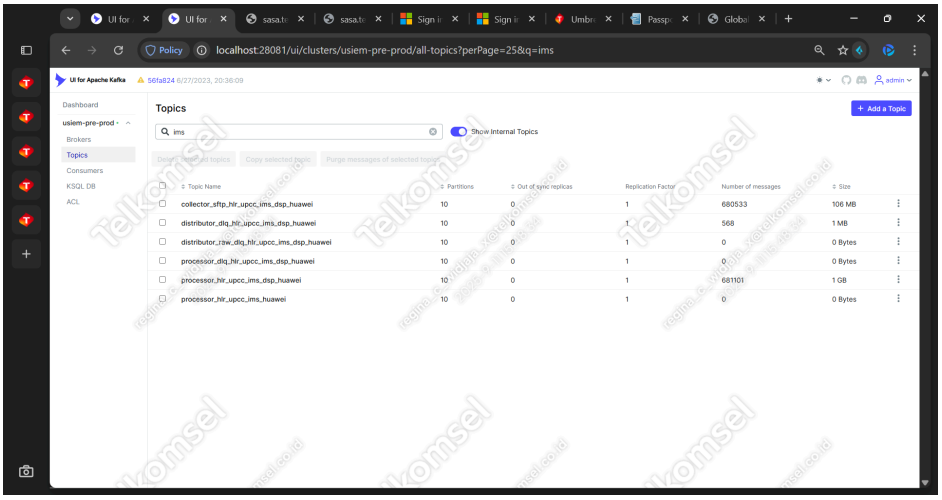
Mendapatkan hasil eksplor yang lebih dalam terkait OWASP ZAP dan Jenkins serta integrasinya untuk security testing
Menemukan sample pada topik sgsn_zte yang terbaru lainnya
Menemukan beberapa sampel pada topik ims_huawei

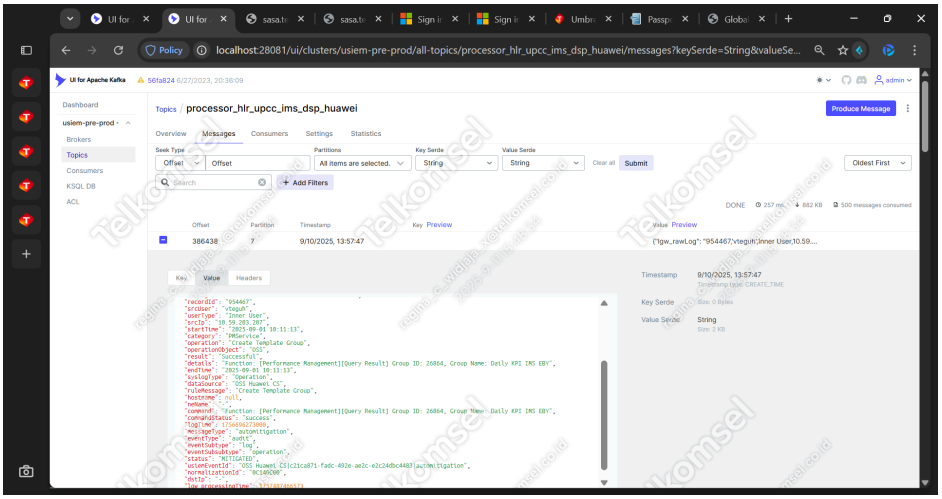
</td>
</tr>
<tr>
<td>Lesson Learned</td>
<td>Some quotes of the day:
Keep going, change looks so beautiful on you.</td>
</tr>
</table>

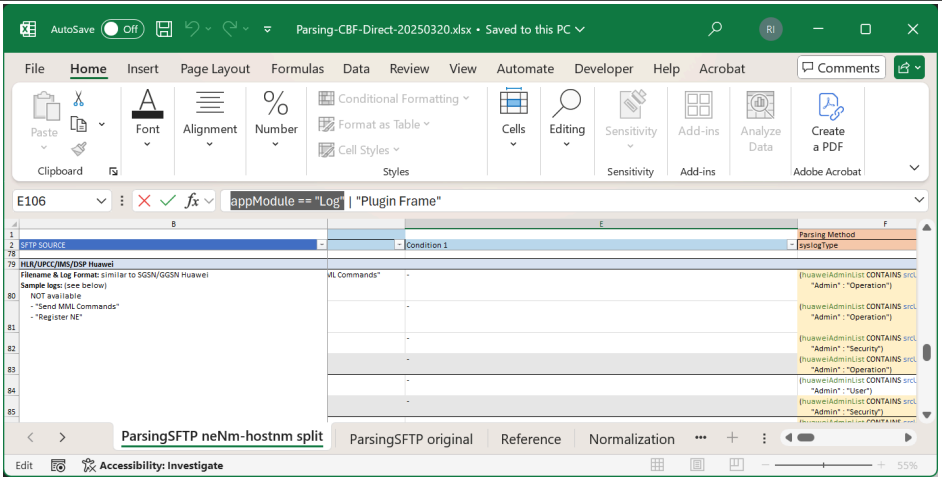
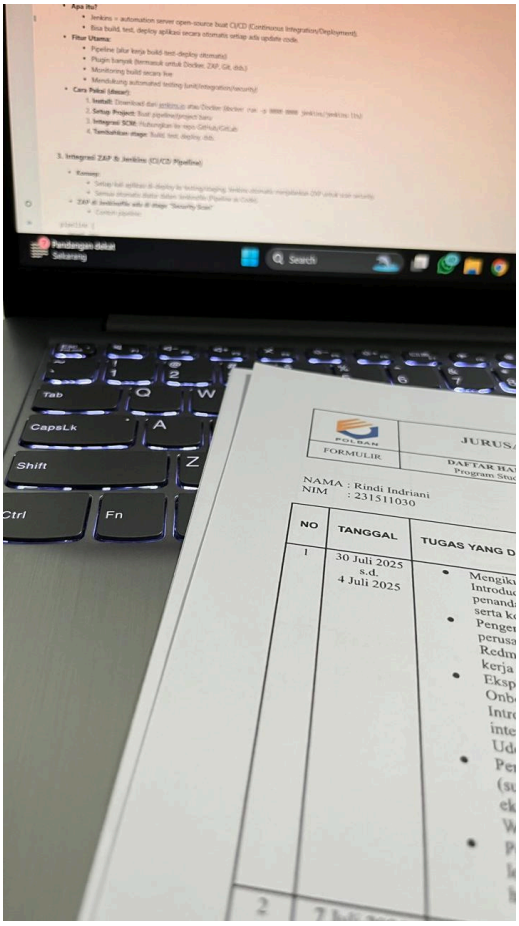
No : 11	Periode : 8 September s.d. 12 September 2025
Sub No : 11.5	Hari/Tanggal : Jumat, 12 September 2025
Proyek	Nama Proyek : USIEM Tsel Project
	Project Manager : Irfan Nurdin Salman
	Technical Leader : Regina Christiany
Tugas	Execute Test Cases Sample for USIEM Tsel Project Topic ssgsn_ericsson based on excel file Parsing CBF
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3 Mencari sampel pada topik ims_huawei yang lainnya --- 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor --- 13.00 WIB Melakukan execute awal test case sample dengan topik ims_huawei yang baru saja ditemukan --- 17.00 WIB Menyiapkan barang-barang untuk segera pulang
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words/ Excel / Google Drive • Notion • Kafka • VS Code • Excel • Prisma Browser • Putty • GlobalProtect

Hasil Kerja


localhost:28081/ui/clusters/usiem-pre-prod/all-topics/processor_hlr_upcc_ims_huawei/messages?keySerde=String&valueSerde...
Topics / processor_hlr_upcc_ims_huawei
Produce Message
Overview
Messages
Consumers
Settings
Statistics
Add Filters
Oldest First


localhost:28081/ui/clusters/usiem-pre-prod/all-topics?perPage=25&q=ims
Topics
Add a Topic
Show Internal Topics
collector_sftp_hlr_upcc_ims_dsp_huawei
distributor_dlq_hlr_upcc_ims_dsp_huawei
distributor_raw_dlq_hlr_upcc_ims_dsp_huawei
processor_dlq_hlr_upcc_ims_dsp_huawei
processor_hlr_upcc_ims_dsp_huawei
processor_hlr_upcc_ims_huawei


localhost:28081/ui/clusters/usiem-pre-prod/all-topics/processor_hlr_upcc_ims_dsp_huawei/messages?keySerde=String&valueSe...
Topics / processor_hlr_upcc_ims_dsp_huawei
Produce Message
Overview
Messages
Consumers
Settings
Statistics
Add Filters
Oldest First
Submit

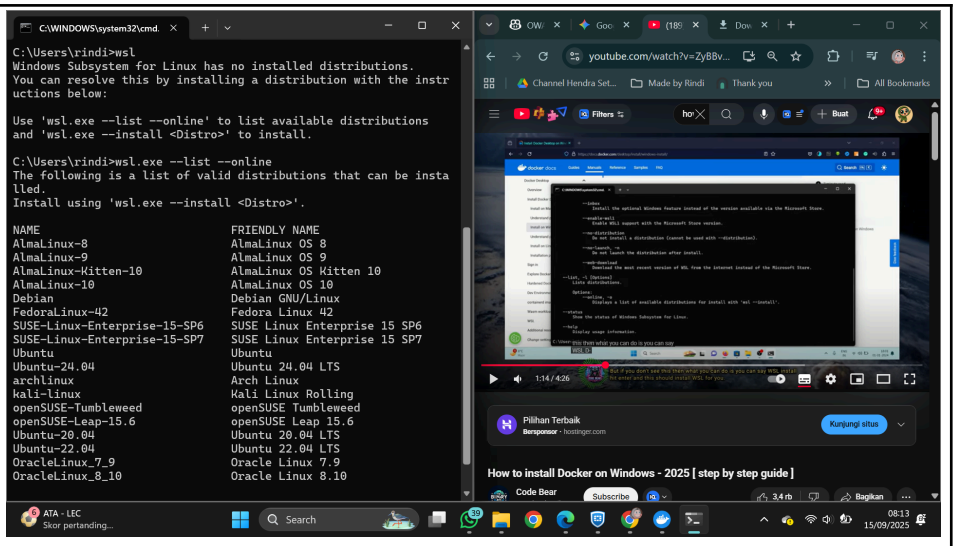
	 • Menemukan beberapa sampel pada topik ims_huawei • Mendapatkan hasil execute sample pada topik ims_huawei yang ada
Lesson Learned	Quote of the day: I don't walk away to teach people a lesson, I walk away cuz I've learned mine. Is the best quote of the year.
Keterangan	

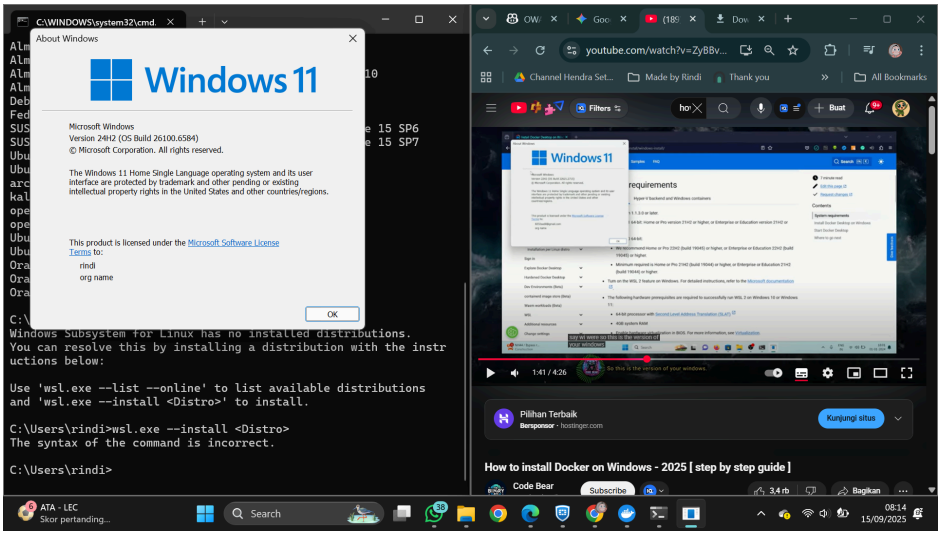
Log Book KP

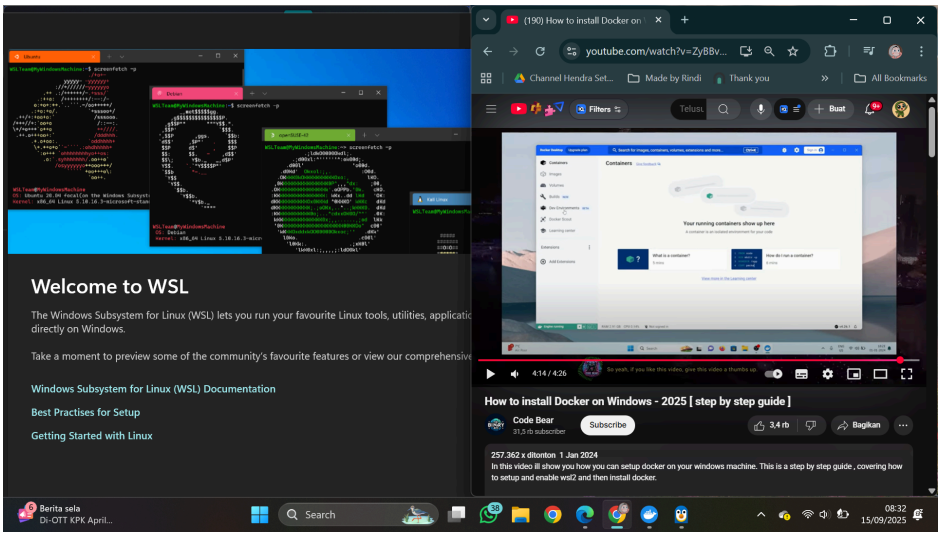
JURUSAN : TEKNIK KOMPUTER DAN INFORMATIKA	PROGRAM STUDI : (D3) TEKNIK INFORMATIKA

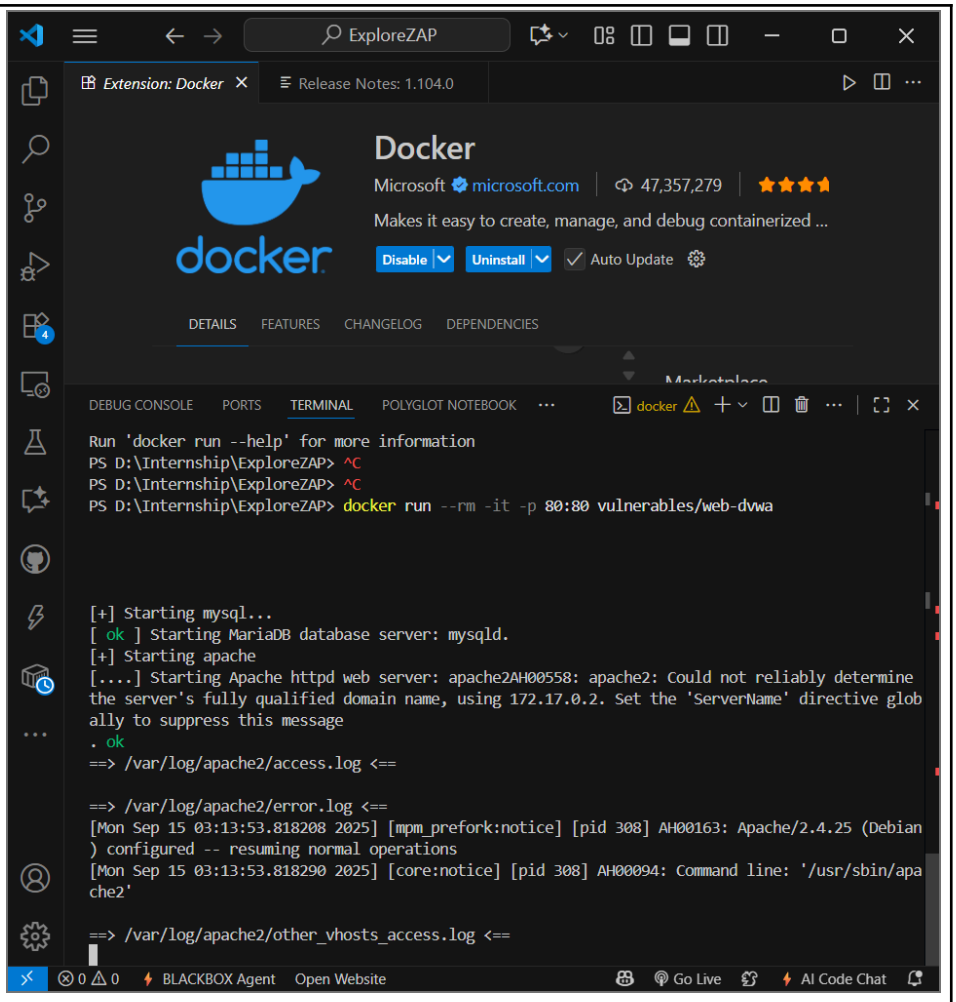
No : 12	Periode : 15 September s.d. 19 September 2025
Sub No :12.1	Hari/Tanggal : Senin, 15 September 2025
Proyek	Nama Proyek : USIEM Tsel Project
	Project Manager : Irfan Nurdin Salman
	Technical Leader : Regina Christiany
Tugas	Setup and configuration tools (Forticlient VPN, Microsoft Office Access Login) for Wiki Tritronik
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3 Implementasi integrasi OWASP ZAP dan Jenkins yang sudah coba di explore --- 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor --- 13.00 WIB Melanjutkan implementasi integrasi OWASP ZAP dan Jenkins yang sedang coba di explore --- 17.00 WIB Menyiapkan barang-barang untuk segera pulang
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words/ Excel / Google Drive • Notion • FortiClient VPN • Wiki Tritronik • GlobalProtect

Hasil Kerja

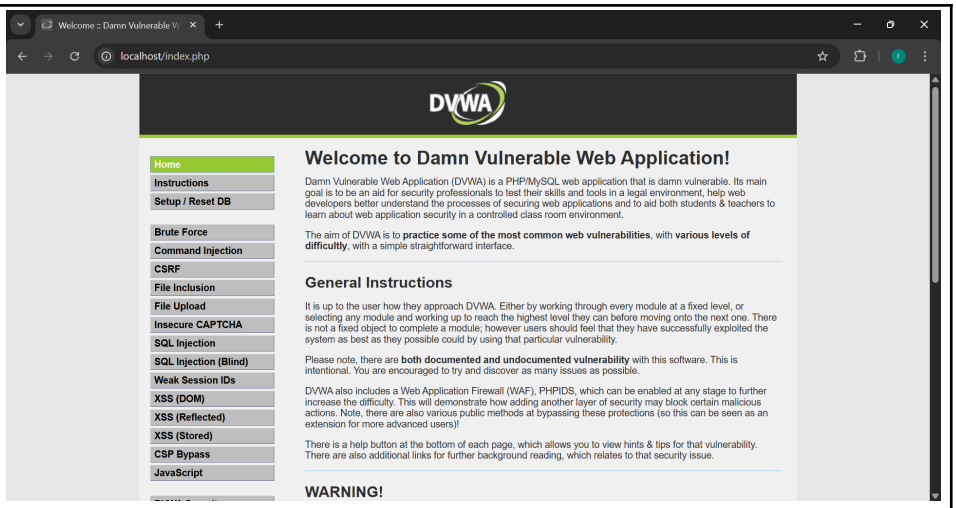

C:\WINDOWS\system32\cmd.
C:\Users\rindi>wsl
Windows Subsystem for Linux has no installed distributions.
You can resolve this by installing a distribution with the instr
uctions below:
Use 'wsl.exe --list --online' to list available distributions
and 'wsl.exe --install <Distro>' to install.
C:\Users\rindi>wsl.exe --list --online
The following is a list of valid distributions that can be insta
lled.
Install using 'wsl.exe --install <Distro>'.
NAME FRIENDLY NAME
AlmaLinux-8 AlmaLinux OS 8
AlmaLinux-9 AlmaLinux OS 9
AlmaLinux-Kitten-10 AlmaLinux OS Kitten 10
AlmaLinux-10 AlmaLinux OS 10
Debian Debian GNU/Linux
FedoraLinux-42 Fedora Linux 42
SUSE-Linux-Enterprise-15-SP6 SUSE Linux Enterprise 15 SP6
SUSE-Linux-Enterprise-15-SP7 SUSE Linux Enterprise 15 SP7
Ubuntu Ubuntu
Ubuntu-24.04 Ubuntu 24.04 LTS
archlinux Arch Linux
kali-linux Kali Linux Rolling
openSUSE-Tumbleweed openSUSE Tumbleweed
openSUSE-Leap-15.6 openSUSE Leap 15.6
Ubuntu-20.04 Ubuntu 20.04 LTS
Ubuntu-22.04 Ubuntu 22.04 LTS
OracleLinux_7_9 Oracle Linux 7.9
OracleLinux_8_10 Oracle Linux 8.10
How to install Docker on Windows - 2025 [step by step guide]
Code Bear
Subscribe
Pilihan Terbaik
Bersponsor · hostinger.com
Kunjungi situs
ATA - LEC
Skor pertanding...
Search
08:13
15/09/2025

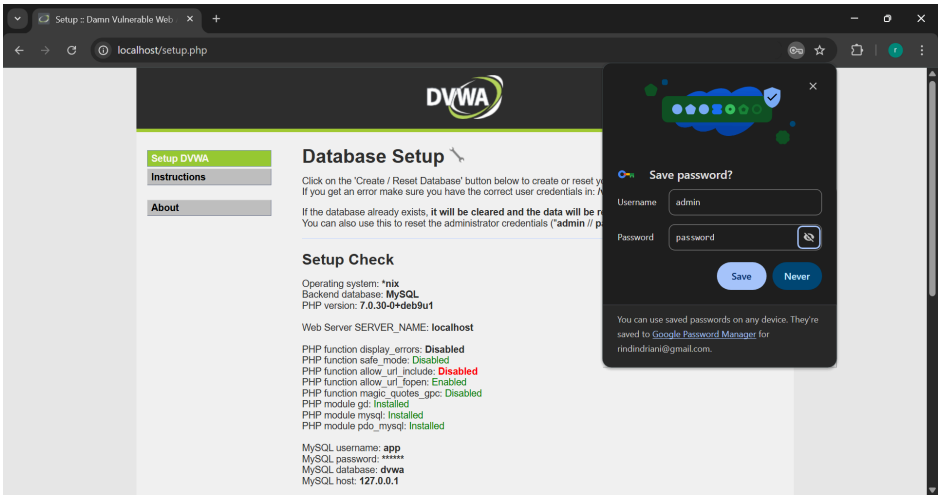

About Windows
Windows 11
Microsoft Windows
Version 24H2 (OS Build 26100.6584)
© Microsoft Corporation. All rights reserved.
The Windows 11 Home Single Language operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
This product is licensed under the Microsoft Software License Terms to:
rindi
org name
OK
C:\Users\rindi>wsl.exe --install <Distro>
The syntax of the command is incorrect.
C:\Users\rindi>
How to install Docker on Windows - 2025 [step by step guide]
Code Bear
Subscribe
Pilihan Terbaik
Bersponsor · hostinger.com
Kunjungi situs
ATA - LEC
Skor pertanding...
Search
08:14
15/09/2025

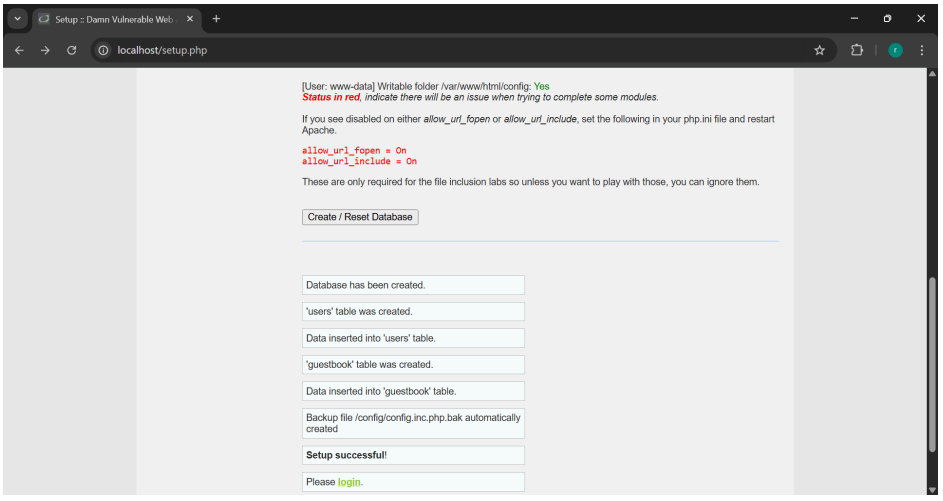

Welcome to WSL
The Windows Subsystem for Linux (WSL) lets you run your favourite Linux tools, utilities, applicatio
directly on Windows.
Take a moment to preview some of the community's favourite features or view our comprehensiv
Windows Subsystem for Linux (WSL) Documentation
Best Practises for Setup
Getting Started with Linux
How to install Docker on Windows - 2025 [step by step guide]
Code Bear
Subscribe
257.362 x ditonton 1 Jan 2024
In this video ill show you how you can setup docker on your windows machine. This is a step by step guide , covering how to setup and enable wsl2 and then install docker.
Berita sela
Di-OTT KPK April...
Search
08:32
15/09/2025

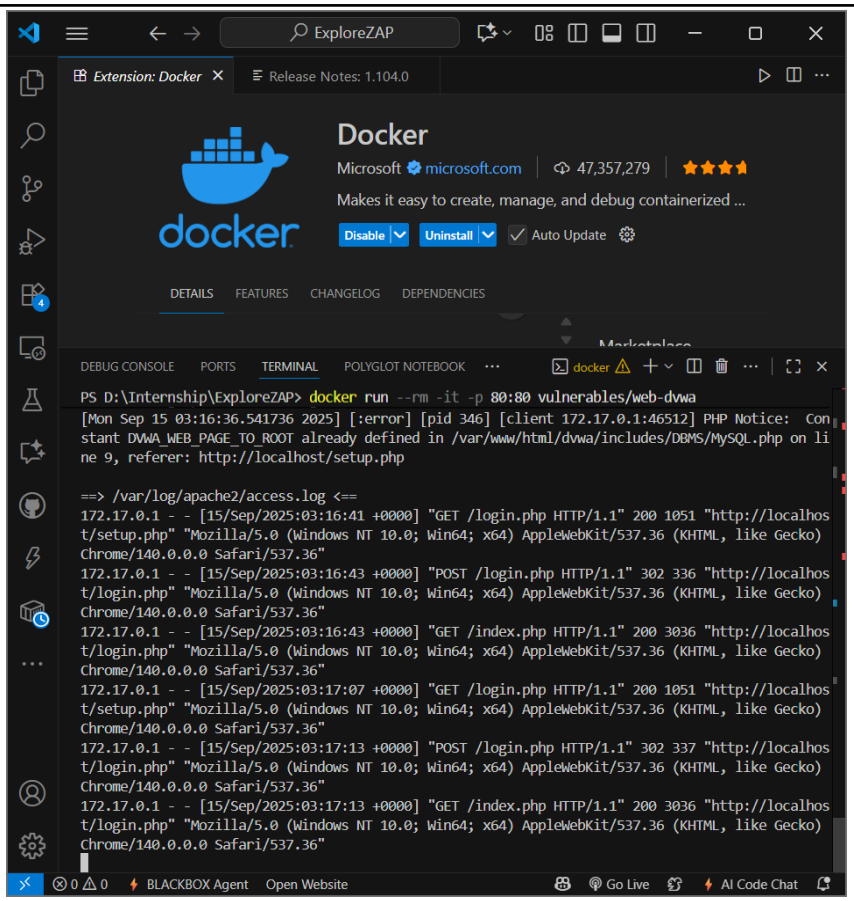

ExploreZAP
Extension: Docker
Release Notes: 1.104.0
Docker
Microsoft microsoft.com
47,357,279
Makes it easy to create, manage, and debug containerized ...
Disable
Uninstall
Auto Update
DETAILS
FEATURES
CHANGELOG
DEPENDENCIES
DEBUG CONSOLE
PORTS
TERMINAL
POLYGLOT NOTEBOOK
docker
Run 'docker run --help' for more information
PS D:\Internship\ExploreZAP> ^C
PS D:\Internship\ExploreZAP> ^C
PS D:\Internship\ExploreZAP> docker run --rm -it -p 80:80 vulnerables/web-dvwa
[+] Starting mysql...
[ok] Starting MariaDB database server: mysqld.
[+] Starting apache
[....] Starting Apache httpd web server: apache2AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message
. ok
==> /var/log/apache2/access.log <==
==> /var/log/apache2/error.log <==
[Mon Sep 15 03:13:53.818208 2025] [mpm_prefork:notice] [pid 308] AH00163: Apache/2.4.25 (Debian) configured -- resuming normal operations
[Mon Sep 15 03:13:53.818290 2025] [core:notice] [pid 308] AH00094: Command line: '/usr/sbin/apache2'
==> /var/log/apache2/other_vhosts_access.log <==
BLACKBOX Agent
Open Website
Go Live
AI Code Chat


Login :: Damn Vulnerable Web
localhost/login.php
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA)

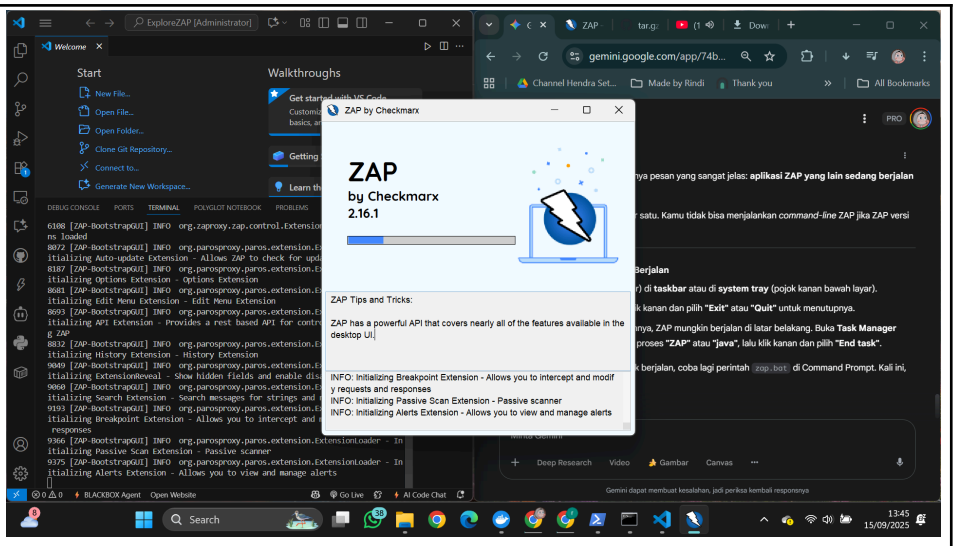

Welcome :: Damn Vulnerable W
localhost/index.php
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!

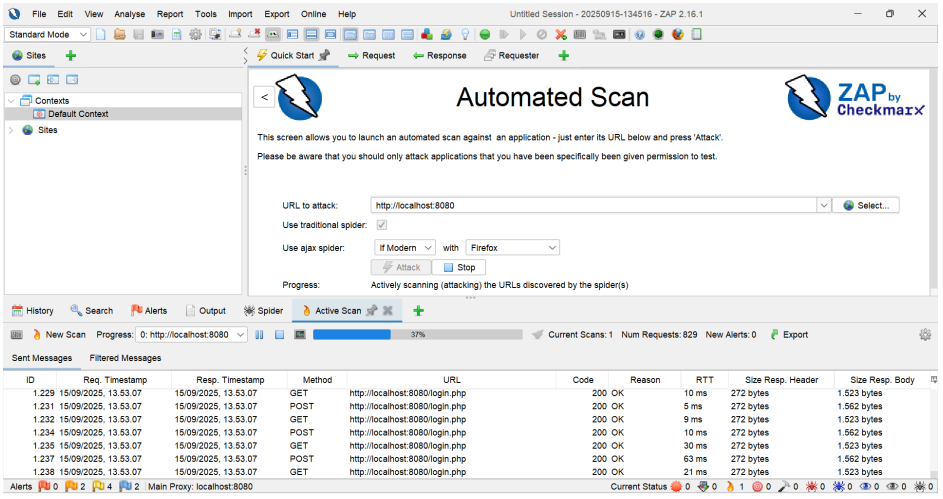

Setup :: Damn Vulnerable Web
localhost/setup.php
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset y
If you get an error make sure you have the correct user credentials in: /
If the database already exists, it will be cleared and the data will be r
You can also use this to reset the administrator credentials ("admin // p
Setup Check
Operating system: *nix
Backend database: MySQL
PHP version: 7.0.30-0+deb9u1
Web Server SERVER_NAME: localhost
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: app
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1
Save password?
Username
admin
Password
password
Save
Never
You can use saved passwords on any device. They're saved to Google Password Manager for rindindriani@gmail.com.

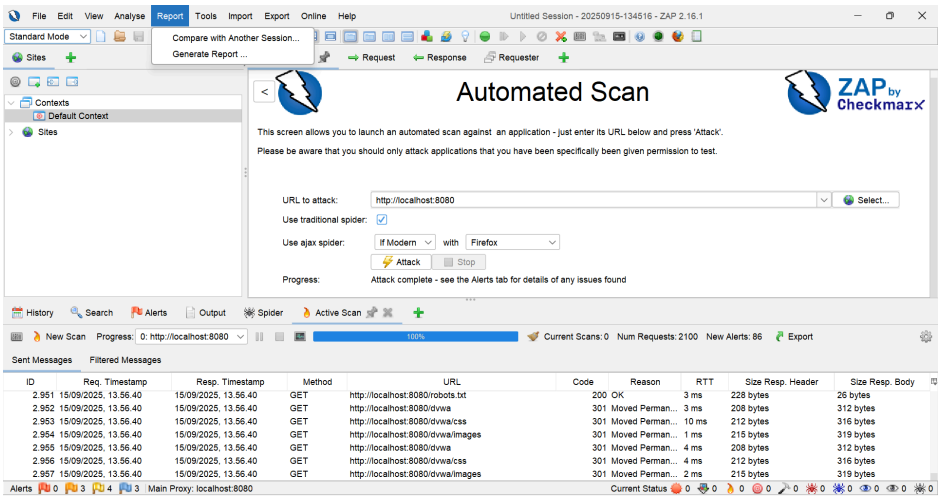

Setup :: Damn Vulnerable Web
localhost/setup.php
[User: www-data] Writable folder /var/www/html/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database
Database has been created.
'users' table was created.
Data inserted into 'users' table.
'guestbook' table was created.
Data inserted into 'guestbook' table.
Backup file /config/config.inc.php.bak automatically created
Setup successful!
Please login.


ExploreZAP
Extension: Docker
Release Notes: 1.104.0
Docker
Microsoft microsoft.com
47,357,279
Makes it easy to create, manage, and debug containerized ...
Disable
Uninstall
Auto Update
DETAILS
FEATURES
CHANGELOG
DEPENDENCIES
DEBUG CONSOLE
PORTS
TERMINAL
POLYGLOT NOTEBOOK
docker
PS D:\Internship\ExploreZAP> docker run --rm -it -p 80:80 vulnerables/web-dvwa
[Mon Sep 15 03:16:36.541736 2025] [:error] [pid 346] [client 172.17.0.1:46512] PHP Notice: Constant DVWA_WEB_PAGE_TO_ROOT already defined in /var/www/html/dvwa/includes/DBMS/MySQL.php on line 9, referer: http://localhost/setup.php
==> /var/log/apache2/access.log <==
172.17.0.1 - - [15/Sep/2025:03:16:41 +0000] "GET /login.php HTTP/1.1" 200 1051 "http://localhost/setup.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
172.17.0.1 - - [15/Sep/2025:03:16:43 +0000] "POST /login.php HTTP/1.1" 302 336 "http://localhost/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
172.17.0.1 - - [15/Sep/2025:03:16:43 +0000] "GET /index.php HTTP/1.1" 200 3036 "http://localhost/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
172.17.0.1 - - [15/Sep/2025:03:17:07 +0000] "GET /login.php HTTP/1.1" 200 1051 "http://localhost/setup.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
172.17.0.1 - - [15/Sep/2025:03:17:13 +0000] "POST /login.php HTTP/1.1" 302 337 "http://localhost/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
172.17.0.1 - - [15/Sep/2025:03:17:13 +0000] "GET /index.php HTTP/1.1" 200 3036 "http://localhost/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
BLACKBOX Agent
Open Website
Go Live
AI Code Chat


ExploreZAP
Extension: Docker
Release Notes: 1.104.0
Docker
Microsoft microsoft.com
47,357,279
Makes it easy to create, manage, and debug containerized ...
Disable
Uninstall
Auto Update
DETAILS
FEATURES
CHANGELOG
DEPENDENCIES
DEBUG CONSOLE
PORTS
TERMINAL
POLYGLOT NOTEBOOK
PROBLEMS
OUTPUT
PS D:\Internship\ExploreZAP> docker login
Your one-time device confirmation code is: RCSV-KMRF
Press ENTER to open your browser or submit your device code here: https://login.docker.com/activate
Waiting for authentication in the browser…
Error response from daemon: Get "https://registry-1.docker.io/v2/": unauthorized: email must be verified before using account
PS D:\Internship\ExploreZAP> docker login
USING WEB-BASED LOGIN
Info → To sign in with credentials on the command line, use 'docker login -u <username>'
Your one-time device confirmation code is: PMXB-QQQM
Press ENTER to open your browser or submit your device code here: https://login.docker.com/activate
Waiting for authentication in the browser…
Login Succeeded
PS D:\Internship\ExploreZAP>
dock...
powersh...
BLACKBOX Agent
Open Website
Go Live
AI Code Chat

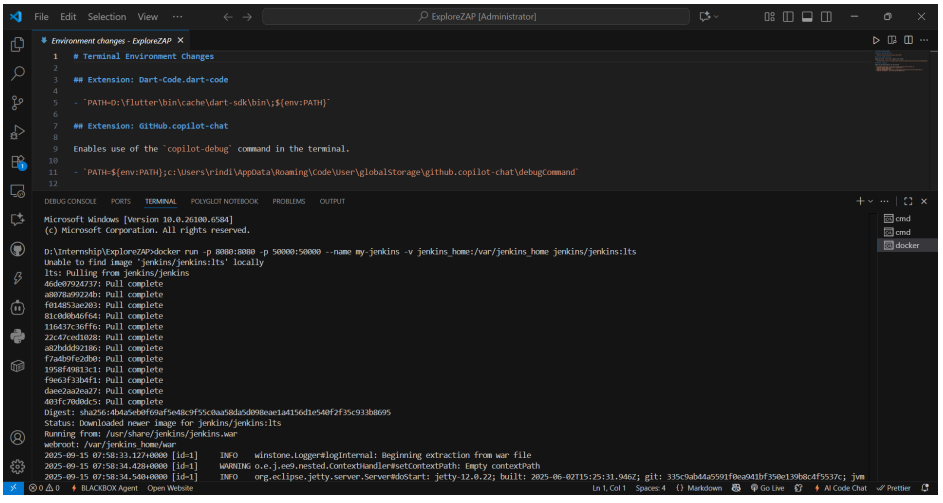

ZAP by Checkmarx
ZAP
by Checkmarx
2.16.1
ZAP Tips and Tricks:
ZAP has a powerful API that covers nearly all of the features available in the desktop UI.
INFO: Initializing Breakpoint Extension - Allows you to intercept and modify requests and responses
INFO: Initializing Passive Scan Extension - Passive scanner
INFO: Initializing Alerts Extension - Allows you to view and manage alerts

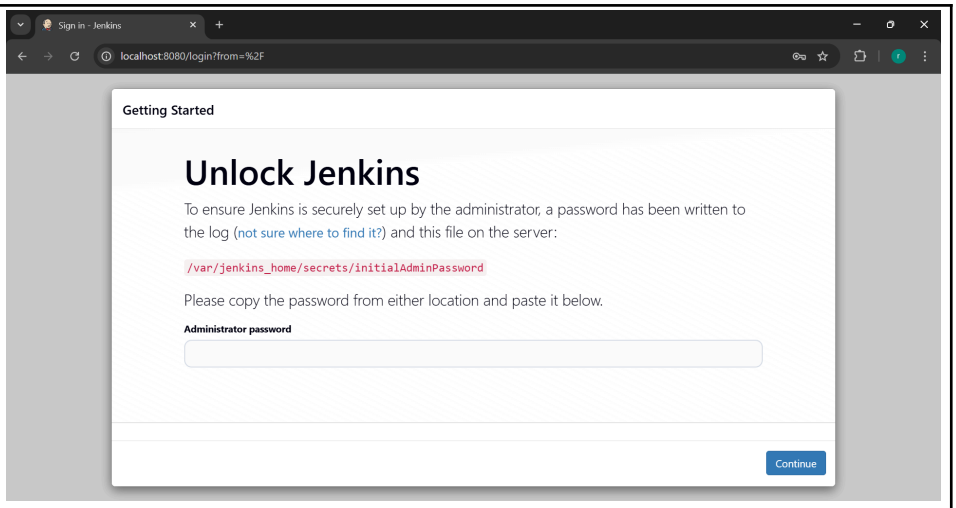

Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://localhost:8080
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

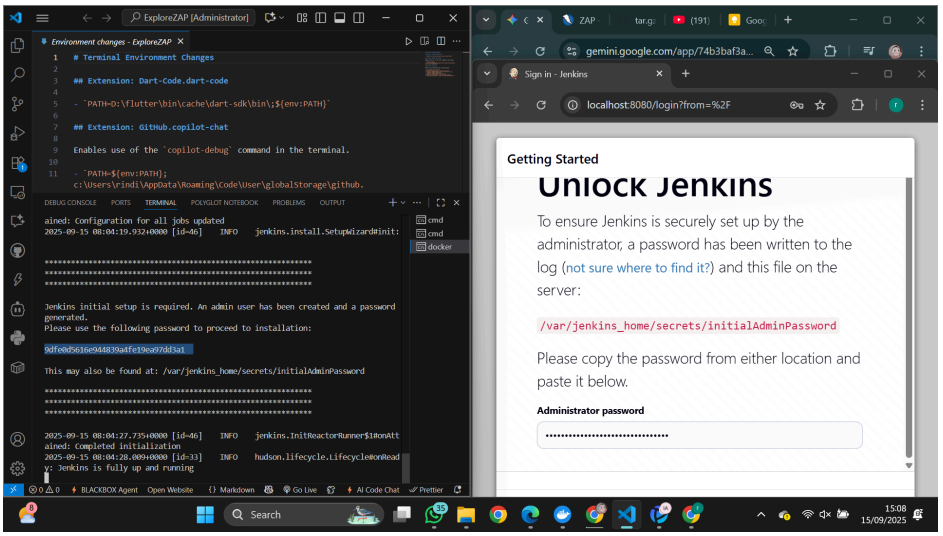

Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://localhost:8080
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found

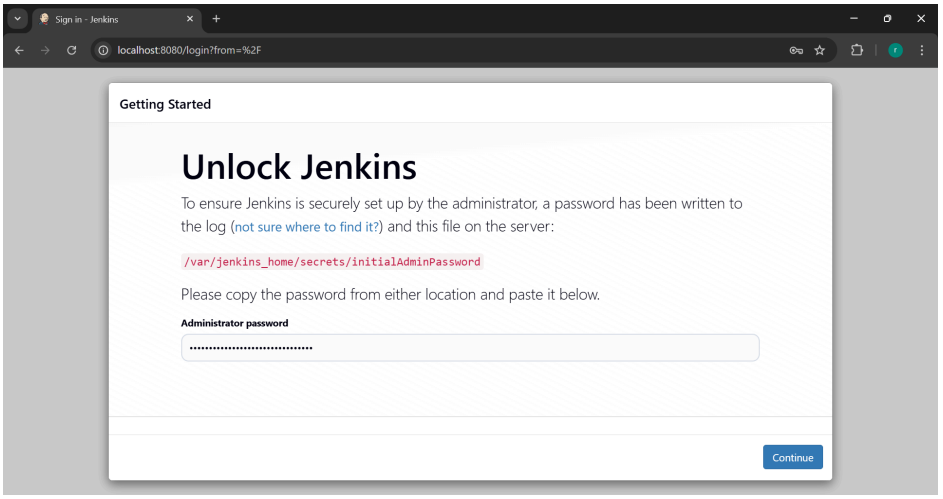
	 - Menemukan cara implementasi dan integrasi antara OWASP ZAP dan Jenkins dengan baik, dan tidak lupa disimpan dilaporan
Lesson Learned	Quote of the day: If you are feeling sad go create somethings because art is magic and it will make everything a little bit better.
Keterangan	

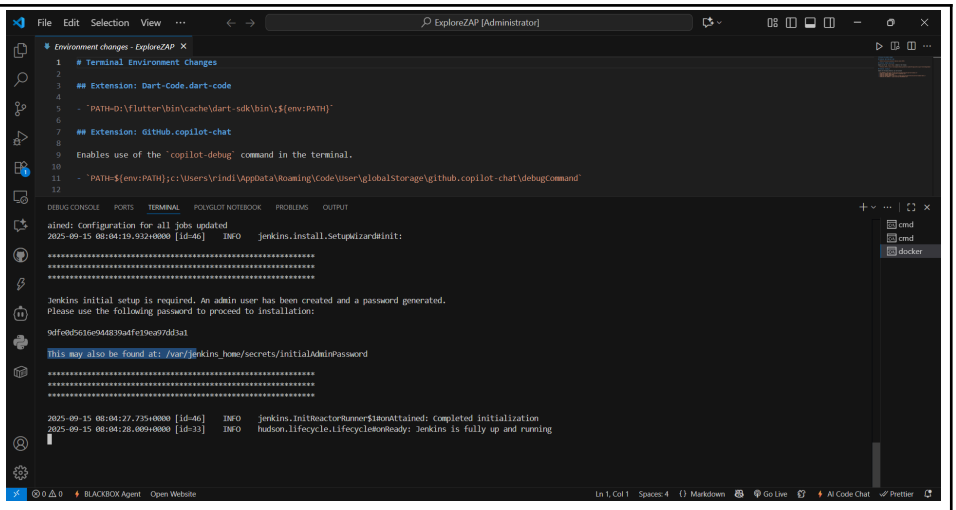
No : 12	Periode : 15 September s.d. 19 September 2025
Sub No : 12.2	Hari/Tanggal : Selasa, 16 September 2025
Proyek	Nama Proyek : USIEM Tsel Project
	Project Manager : Irfan Nurdin Salman
	Technical Leader : Regina Christiany
Tugas	Re-setup and access Wiki Tritronik and moving Notion summary to Wiki
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik)

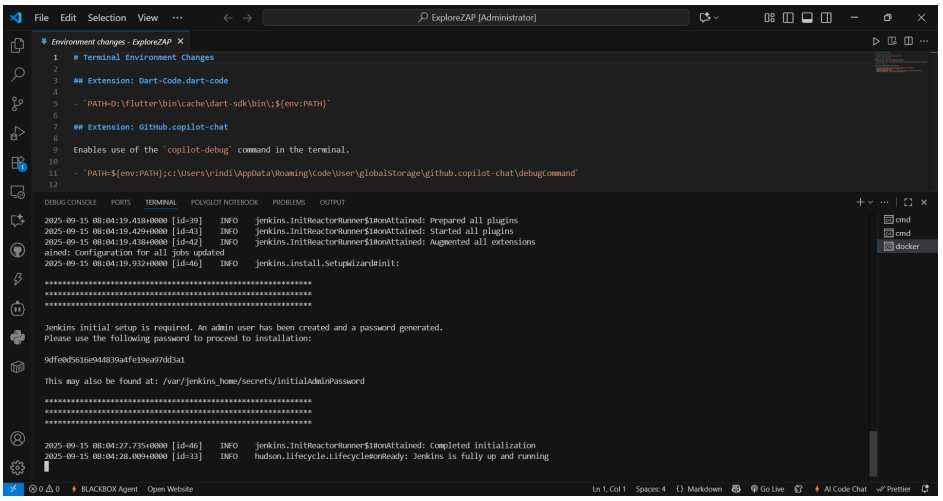
	Memasuki ruangan saya di Lantai 3 Melakukan execute test case ims_huawei --- 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor --- 13.00 WIB Fiksasi implementasi OWASP ZAP dan Jenkins integration --- 17.00 WIB Membereskan barang-barang karena jam kerja sudah selesai
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words/ Excel / Google Drive • Notion • FortiClient VPN • Wiki Tritronik • GlobalProtect
Hasil Kerja	

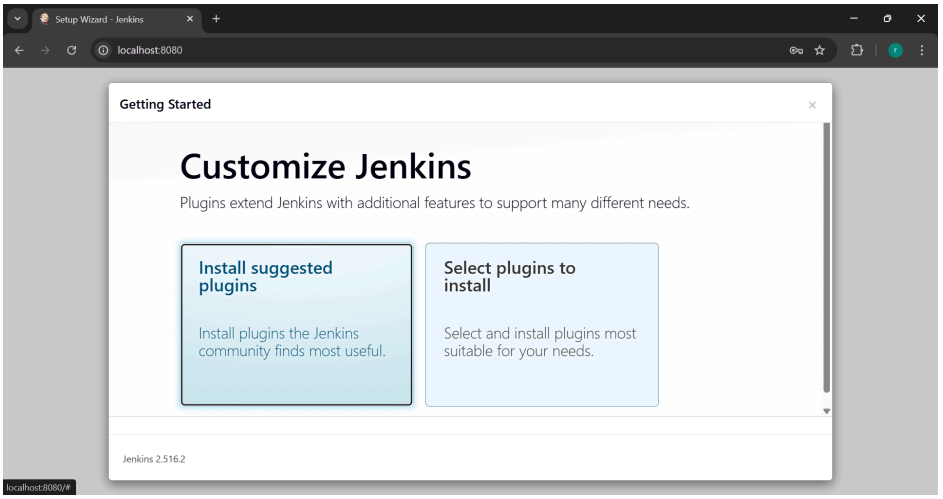

Sign in - Jenkins
localhost:8080/login?from=%2F
Getting Started
Unlock Jenkins
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:
/var/jenkins_home/secrets/initialAdminPassword
Please copy the password from either location and paste it below.
Administrator password
Continue

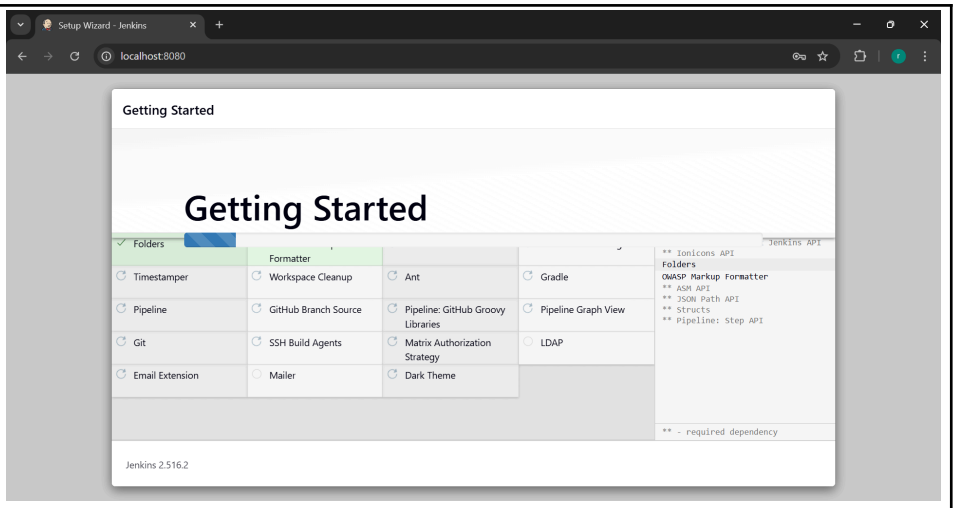

ExploreZAP [Administrator]
Environment changes - ExploreZAP
Terminal Environment Changes
Extension: Dart-Code.dart-code
Extension: GitHub.copilot-chat
Enables use of the `copilot-debug` command in the terminal.
DEBUG CONSOLE
PORTS
TERMINAL
POLYGLOT NOTEBOOK
PROBLEMS
OUTPUT
Jenkins initial setup is required. An admin user has been created and a password generated.
Please use the following password to proceed to installation:
This may also be found at: /var/jenkins_home/secrets/initialAdminPassword
Jenkins is fully up and running
Sign in - Jenkins
localhost:8080/login?from=%2F
Getting Started
Unlock Jenkins
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:
/var/jenkins_home/secrets/initialAdminPassword
Please copy the password from either location and paste it below.
Administrator password
Search
15:08
15/09/2025

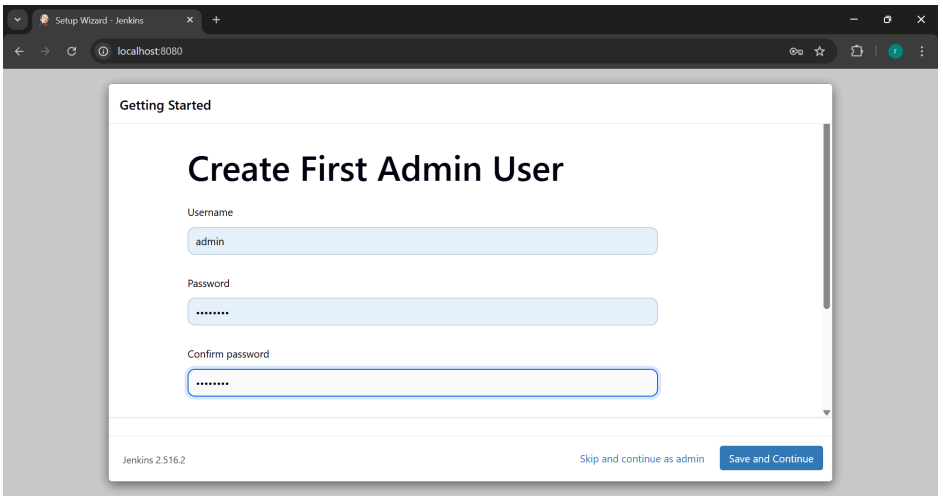

Sign in - Jenkins
localhost:8080/login?from=%2F
Getting Started
Unlock Jenkins
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:
/var/jenkins_home/secrets/initialAdminPassword
Please copy the password from either location and paste it below.
Administrator password
Continue

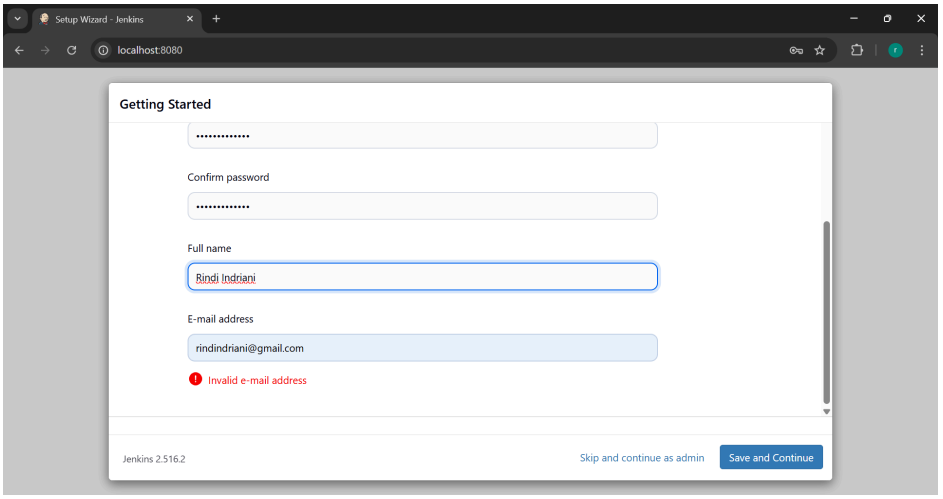

File Edit Selection View
ExploreZAP [Administrator]
Environment changes - ExploreZAP
Terminal Environment Changes
Extension: Dart-Code.dart-code
- `PATH=D:\flutter\bin\cache\dart-sdk\bin\;${env:PATH}`
Extension: GitHub.copilot-chat
Enables use of the `copilot-debug` command in the terminal.
- `PATH=${env:PATH};c:\Users\rindi\AppData\Roaming\Code\User\globalStorage\github.copilot-chat\debugCommand`
DEBUG CONSOLE PORTS TERMINAL POLYGLOT NOTEBOOK PROBLEMS OUTPUT
ained: Configuration for all jobs updated
2025-09-15 08:04:19.932+0000 [id=46] INFO jenkins.install.SetupWizard#init:
Jenkins initial setup is required. An admin user has been created and a password generated.
Please use the following password to proceed to installation:
9dfe0d5616e944839a4fe19ea97dd3a1
This may also be found at: /var/jenkins_home/secrets/initialAdminPassword
2025-09-15 08:04:27.735+0000 [id=46] INFO jenkins.InitReactorRunner$1#onAttained: Completed initialization
2025-09-15 08:04:28.009+0000 [id=33] INFO hudson.lifecycle.Lifecycle#onReady: Jenkins is fully up and running
cmd
cmd
docker
BLACKBOX Agent Open Website
Ln 1, Col 1 Spaces: 4 Markdown Go Live AI Code Chat Prettier

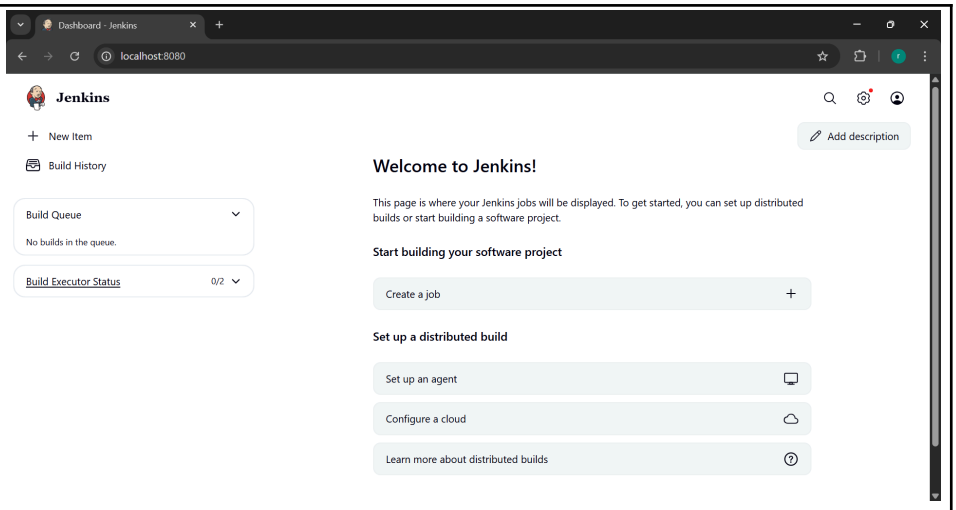

File Edit Selection View
ExploreZAP [Administrator]
Environment changes - ExploreZAP
Terminal Environment Changes
Extension: Dart-Code.dart-code
- `PATH=D:\flutter\bin\cache\dart-sdk\bin\;${env:PATH}`
Extension: GitHub.copilot-chat
Enables use of the `copilot-debug` command in the terminal.
- `PATH=${env:PATH};c:\Users\rindi\AppData\Roaming\Code\User\globalStorage\github.copilot-chat\debugCommand`
DEBUG CONSOLE PORTS TERMINAL POLYGLOT NOTEBOOK PROBLEMS OUTPUT
2025-09-15 08:04:19.418+0000 [id=39] INFO jenkins.InitReactorRunner$1#onAttained: Prepared all plugins
2025-09-15 08:04:19.429+0000 [id=43] INFO jenkins.InitReactorRunner$1#onAttained: Started all plugins
2025-09-15 08:04:19.438+0000 [id=42] INFO jenkins.InitReactorRunner$1#onAttained: Augmented all extensions
ained: Configuration for all jobs updated
2025-09-15 08:04:19.932+0000 [id=46] INFO jenkins.install.SetupWizard#init:
Jenkins initial setup is required. An admin user has been created and a password generated.
Please use the following password to proceed to installation:
9dfe0d5616e944839a4fe19ea97dd3a1
This may also be found at: /var/jenkins_home/secrets/initialAdminPassword
2025-09-15 08:04:27.735+0000 [id=46] INFO jenkins.InitReactorRunner$1#onAttained: Completed initialization
2025-09-15 08:04:28.009+0000 [id=33] INFO hudson.lifecycle.Lifecycle#onReady: Jenkins is fully up and running
cmd
cmd
docker
BLACKBOX Agent Open Website
Ln 1, Col 1 Spaces: 4 Markdown Go Live AI Code Chat Prettier

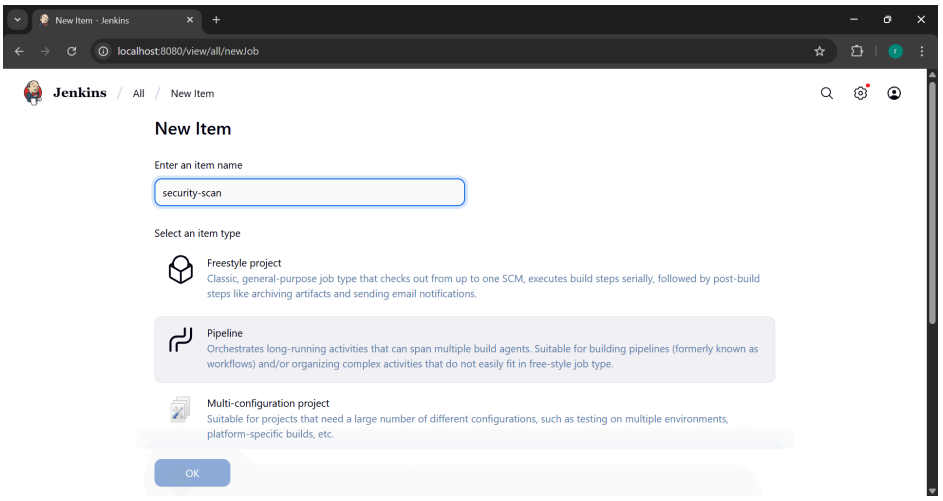

Setup Wizard - Jenkins
localhost:8080
Getting Started
Customize Jenkins
Plugins extend Jenkins with additional features to support many different needs.
Install suggested plugins
Install plugins the Jenkins community finds most useful.
Select plugins to install
Select and install plugins most suitable for your needs.
Jenkins 2.516.2
localhost:8080/#

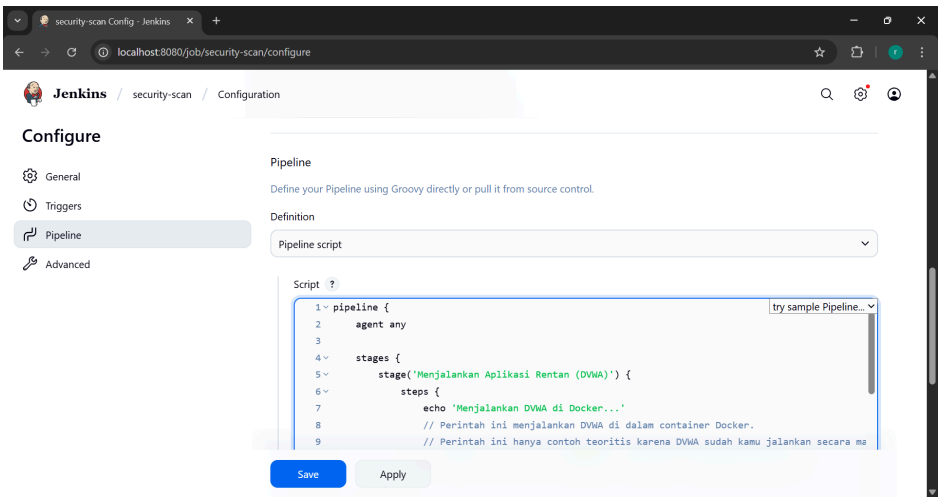

Setup Wizard - Jenkins
localhost:8080
Getting Started
Getting Started
Folders
Formatter
Timestamper
Workspace Cleanup
Ant
Gradle
Pipeline
GitHub Branch Source
Pipeline: GitHub Groovy Libraries
Pipeline Graph View
Git
SSH Build Agents
Matrix Authorization Strategy
LDAP
Email Extension
Mailer
Dark Theme
Jenkins API
** Ionicons API
Folders
OWASP Markup Formatter
** ASM API
** JSON Path API
** Structs
** Pipeline: Step API
** - required dependency
Jenkins 2.516.2

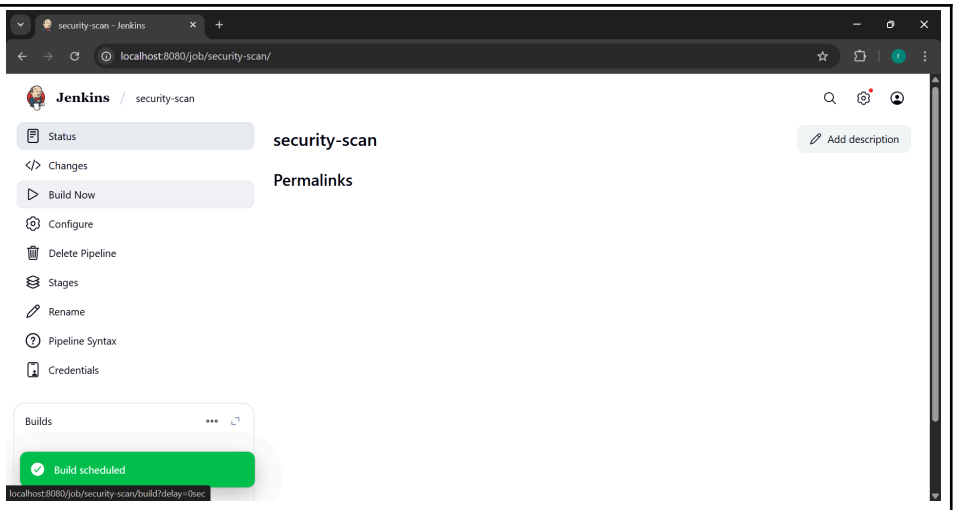

Setup Wizard - Jenkins
localhost:8080
Getting Started
Create First Admin User
Username
admin
Password
Confirm password
Jenkins 2.516.2
Skip and continue as admin
Save and Continue

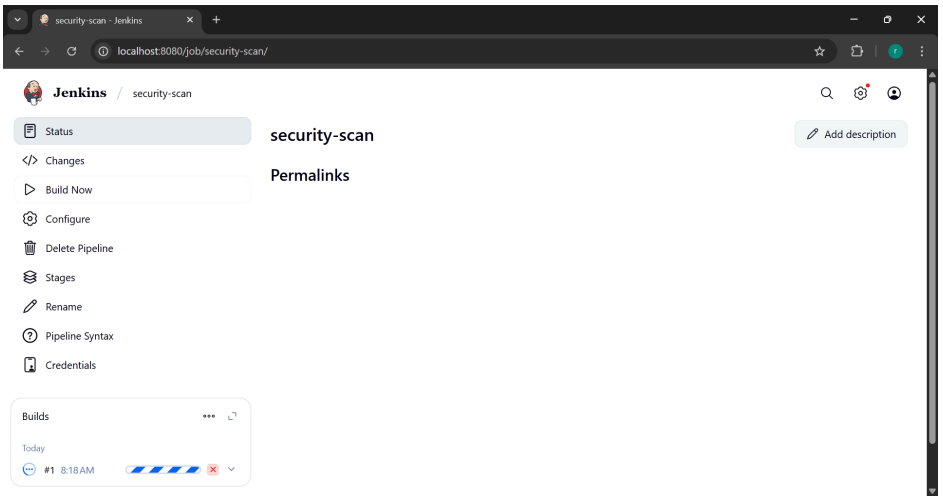

Setup Wizard - Jenkins
localhost:8080
Getting Started
Confirm password
Full name
Rindi Indriani
E-mail address
rindindriani@gmail.com
Invalid e-mail address
Jenkins 2.516.2
Skip and continue as admin
Save and Continue

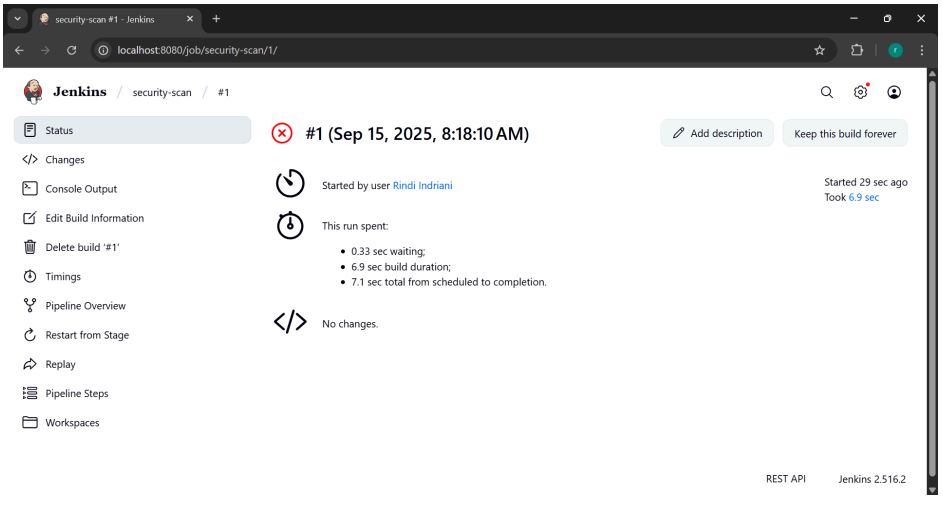

Dashboard - Jenkins
localhost:8080
Jenkins
New Item
Build History
Build Queue
No builds in the queue.
Build Executor Status
0/2
Add description
Welcome to Jenkins!
This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.
Start building your software project
Create a job
Set up a distributed build
Set up an agent
Configure a cloud
Learn more about distributed builds

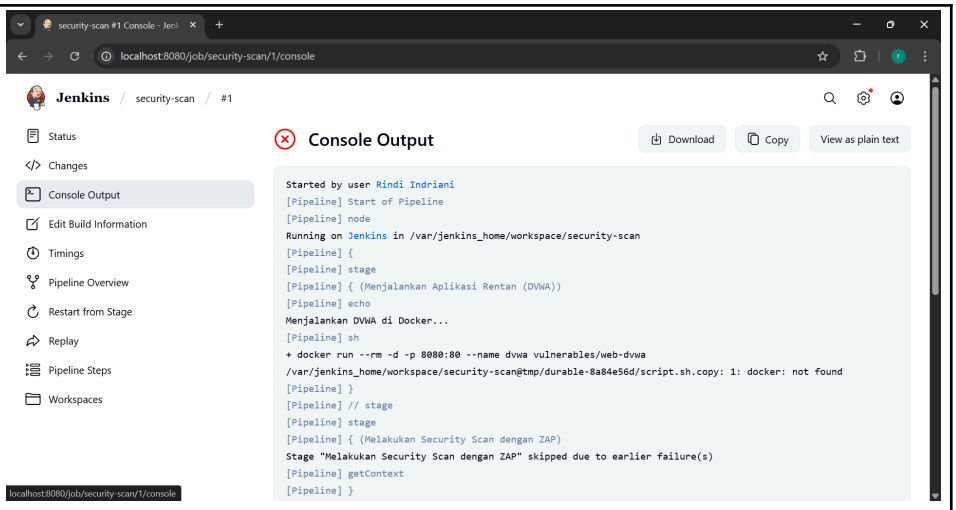

New Item - Jenkins
localhost:8080/view/all/newJob
Jenkins / All / New Item
New Item
Enter an item name
security-scan
Select an item type
Freestyle project
Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.
Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.
Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.
OK

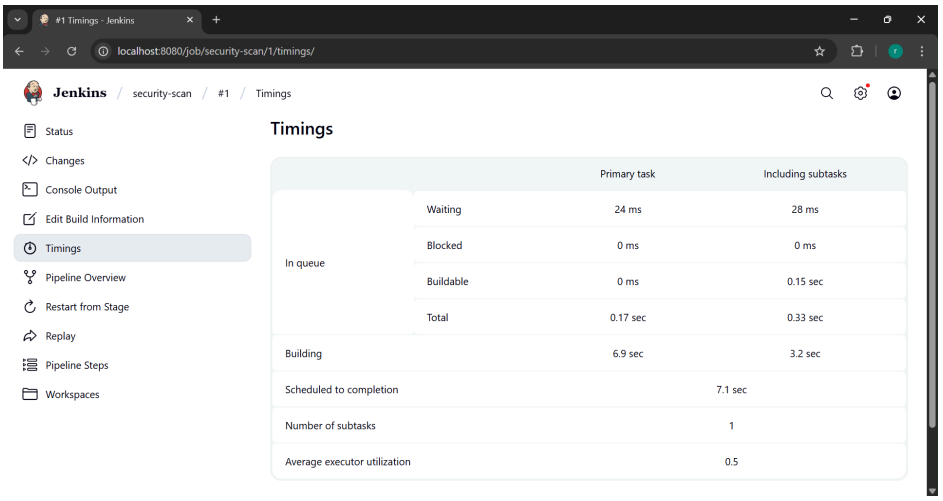

security-scan Config - Jenkins
localhost:8080/job/security-scan/configure
Jenkins / security-scan / Configuration
Configure
General
Triggers
Pipeline
Advanced
Pipeline
Define your Pipeline using Groovy directly or pull it from source control.
Definition
Pipeline script
Script
try sample Pipeline...
pipeline {
agent any
stages {
stage('Menjalankan Aplikasi Rentan (DVWA)') {
steps {
echo 'Menjalankan DVWA di Docker...'
// Perintah ini menjalankan DVWA di dalam container Docker.
// Perintah ini hanya contoh teoritis karena DVWA sudah kamu jalankan secara ma
Save
Apply

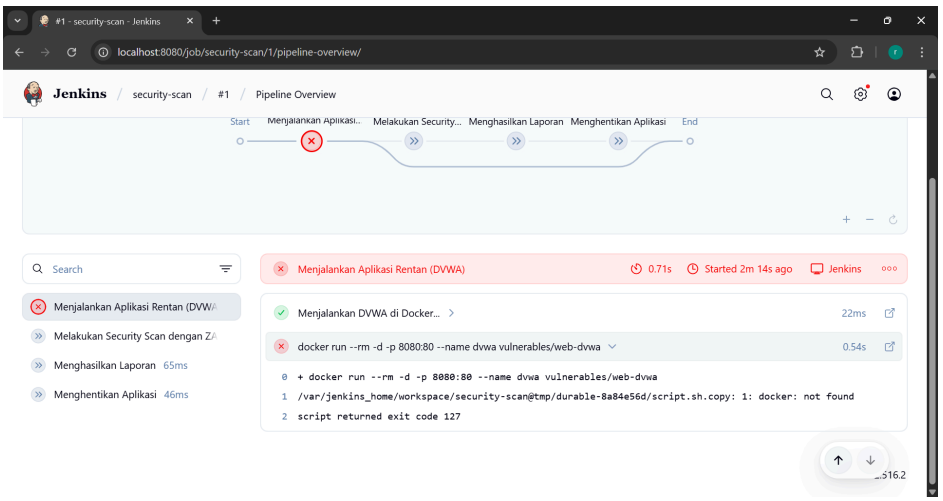

security-scan - Jenkins
localhost:8080/job/security-scan/
Jenkins
security-scan
Status
Changes
Build Now
Configure
Delete Pipeline
Stages
Rename
Pipeline Syntax
Credentials
Builds
Build scheduled
localhost:8080/job/security-scan/build?delay=0sec
security-scan
Add description
Permalinks

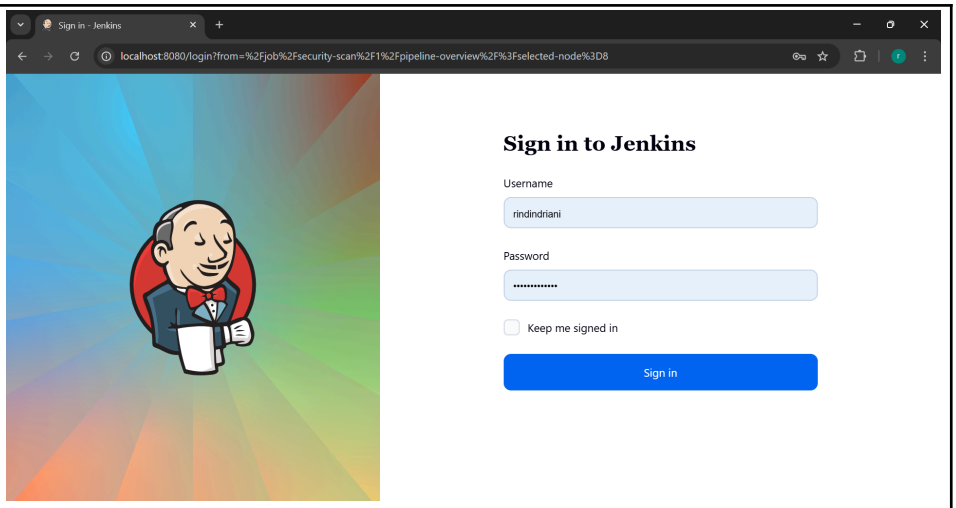

security-scan - Jenkins
localhost:8080/job/security-scan/
Jenkins
security-scan
Status
Changes
Build Now
Configure
Delete Pipeline
Stages
Rename
Pipeline Syntax
Credentials
Builds
Today
#1 8:18 AM
security-scan
Add description
Permalinks

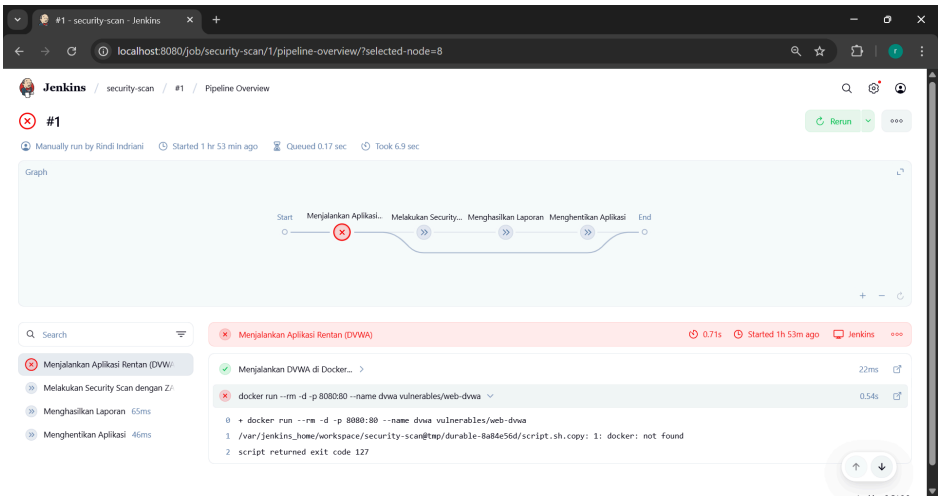

security-scan #1 - Jenkins
localhost:8080/job/security-scan/1/
Jenkins
security-scan
#1
Status
Changes
Console Output
Edit Build Information
Delete build '#1'
Timings
Pipeline Overview
Restart from Stage
Replay
Pipeline Steps
Workspaces
#1 (Sep 15, 2025, 8:18:10 AM)
Add description
Keep this build forever
Started by user Rindi Indriani
Started 29 sec ago
Took 6.9 sec
This run spent:
0.33 sec waiting;
6.9 sec build duration;
7.1 sec total from scheduled to completion.
No changes.
REST API
Jenkins 2.516.2

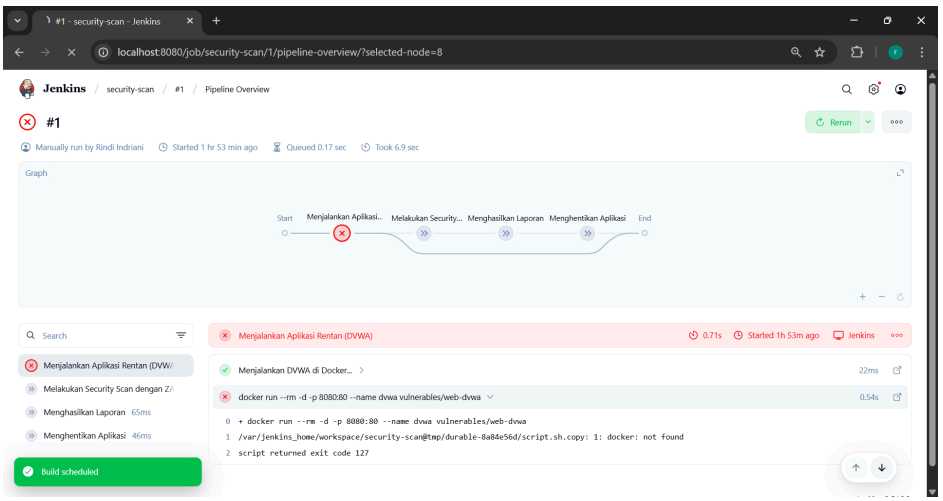

security-scan #1 Console - Jenkins
localhost:8080/job/security-scan/1/console
Jenkins / security-scan / #1
Status
Changes
Console Output
Edit Build Information
Timings
Pipeline Overview
Restart from Stage
Replay
Pipeline Steps
Workspaces
Console Output
Download
Copy
View as plain text
Started by user Rindi Indriani
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in /var/jenkins_home/workspace/security-scan
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Menjalankan Aplikasi Rentan (DVWA))
[Pipeline] echo
Menjalankan DVWA di Docker...
[Pipeline] sh
+ docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa
/var/jenkins_home/workspace/security-scan@tmp/durable-8a84e56d/script.sh.copy: 1: docker: not found
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Melakukan Security Scan dengan ZAP)
Stage "Melakukan Security Scan dengan ZAP" skipped due to earlier failure(s)
[Pipeline] getContext
[Pipeline] }
localhost:8080/job/security-scan/1/console

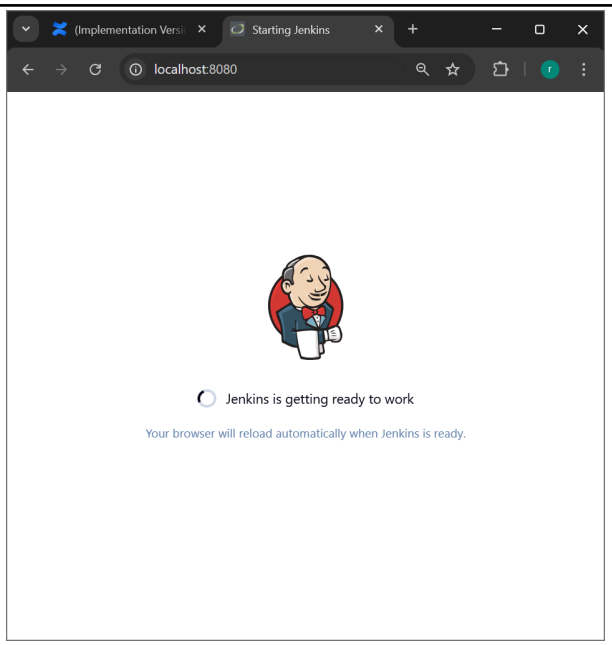

#1 Timings - Jenkins
localhost:8080/job/security-scan/1/timings/
Jenkins / security-scan / #1 / Timings
Status
Changes
Console Output
Edit Build Information
Timings
Pipeline Overview
Restart from Stage
Replay
Pipeline Steps
Workspaces
Timings
Primary task
Including subtasks
In queue
Waiting 24 ms 28 ms
Blocked 0 ms 0 ms
Buildable 0 ms 0.15 sec
Total 0.17 sec 0.33 sec
Building 6.9 sec 3.2 sec
Scheduled to completion 7.1 sec
Number of subtasks 1
Average executor utilization 0.5

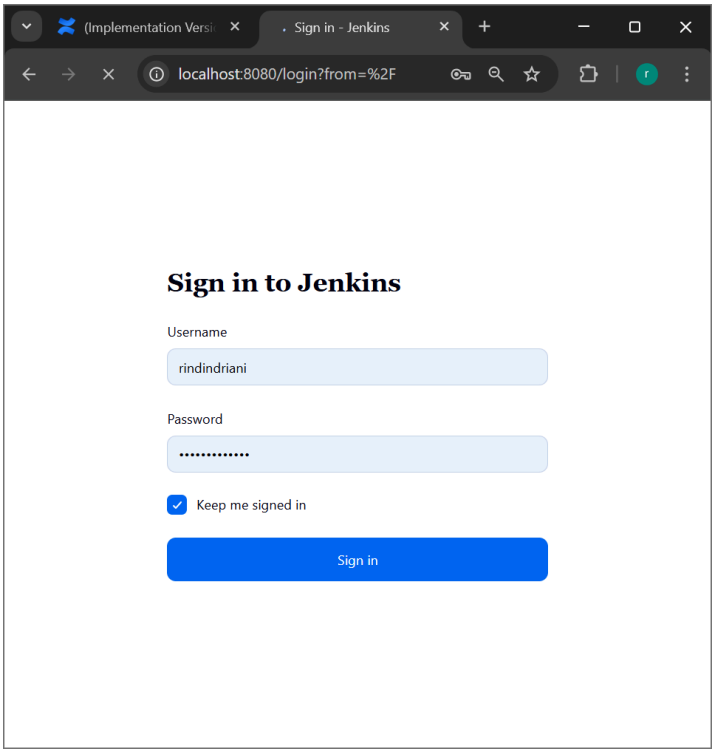

#1 - security-scan - Jenkins
localhost:8080/job/security-scan/1/pipeline-overview/
Jenkins / security-scan / #1 / Pipeline Overview
Start
Menjalankan Aplikasi...
Melakukan Security...
Menghasilkan Laporan
Menghentikan Aplikasi
End
Search
Menjalankan Aplikasi Rentan (DVWA)
Melakukan Security Scan dengan ZA
Menghasilkan Laporan 65ms
Menghentikan Aplikasi 46ms
Menjalankan Aplikasi Rentan (DVWA) 0.71s Started 2m 14s ago Jenkins
Menjalankan DVWA di Docker... 22ms
docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa 0.54s
+ docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa
/var/jenkins_home/workspace/security-scan@tmp/durable-8a84e56d/script.sh.copy: 1: docker: not found
script returned exit code 127

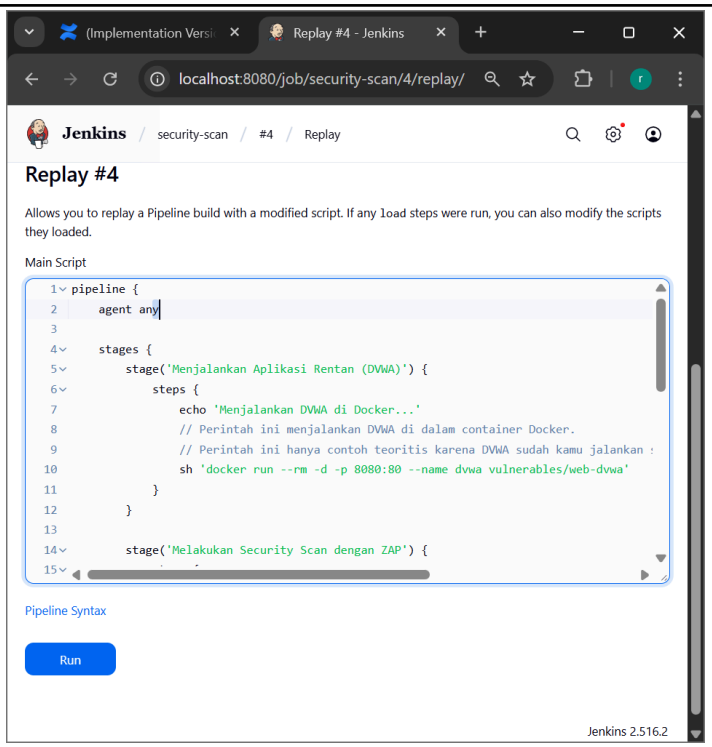

Sign in - Jenkins
localhost:8080/login?from=%2Fjob%2Fsecurity-scan%2F1%2Fpipeline-overview%2F%3Fselected-node%3D8
Sign in to Jenkins
Username
rindindriani
Password
Keep me signed in
Sign in

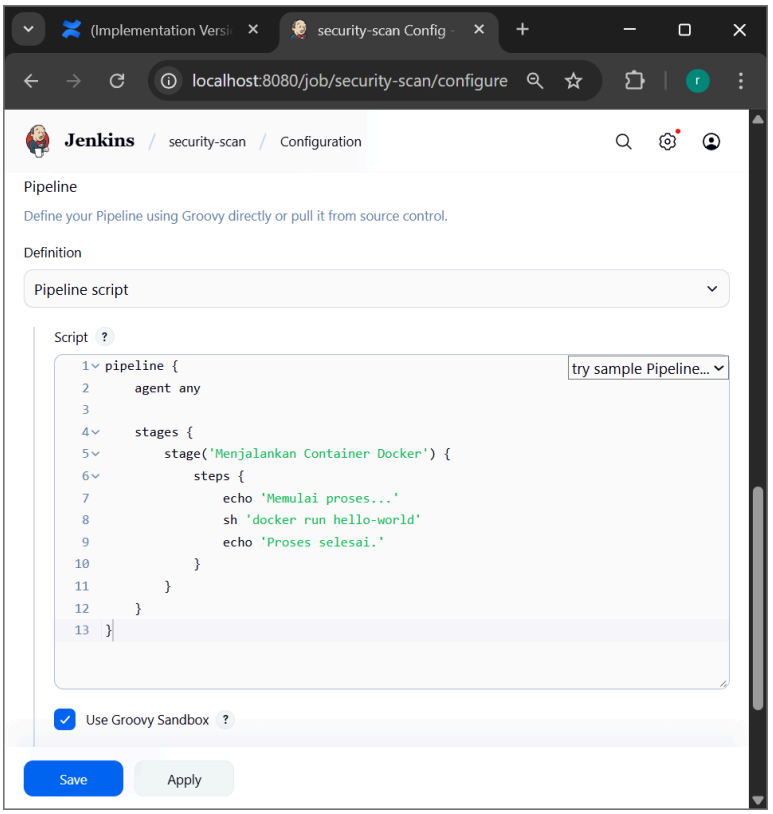

#1 - security-scan - Jenkins
localhost:8080/job/security-scan/1/pipeline-overview/?selected-node=8
Jenkins
security-scan
#1
Pipeline Overview
#1
Rerun
Manually run by Rindi Indriani
Started 1 hr 53 min ago
Queued 0.17 sec
Took 6.9 sec
Graph
Start
Menjalankan Aplikasi...
Melakukan Security...
Menghasilkan Laporan
Menghentikan Aplikasi
End
Search
Menjalankan Aplikasi Rentan (DVWA)
0.71s
Started 1h 53m ago
Jenkins
Menjalankan Aplikasi Rentan (DVW
Melakukan Security Scan dengan Z
Menghasilkan Laporan 65ms
Menghentikan Aplikasi 46ms
Menjalankan DVWA di Docker...
22ms
docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa
0.54s
0 + docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa
1 /var/jenkins_home/workspace/security-scan@tmp/durable-8a84e56d/script.sh.copy: 1: docker: not found
2 script returned exit code 127

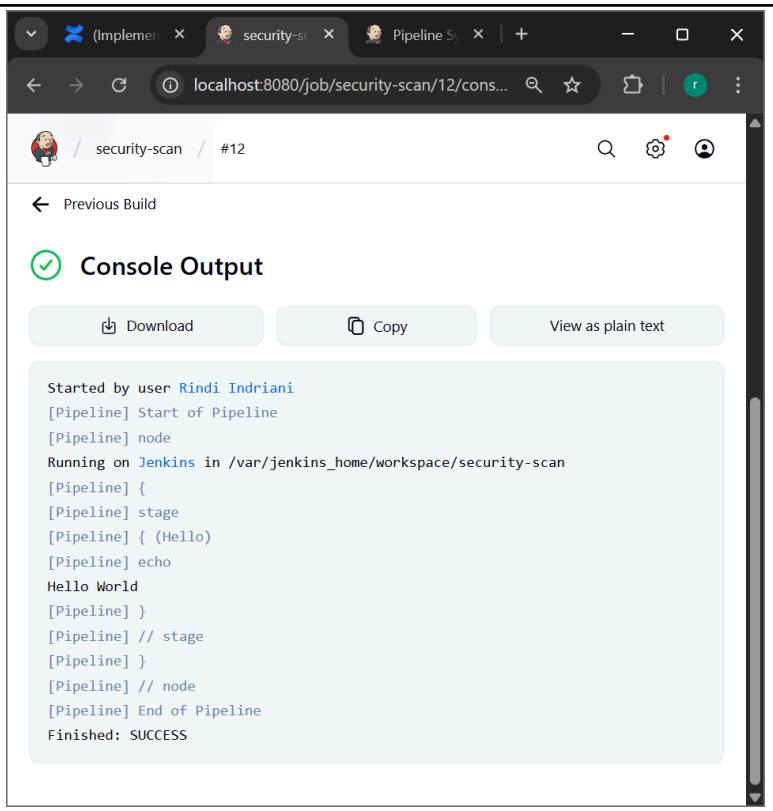

#1 - security-scan - Jenkins
localhost:8080/job/security-scan/1/pipeline-overview/?selected-node=8
Jenkins
security-scan
#1
Pipeline Overview
#1
Rerun
Manually run by Rindi Indriani
Started 1 hr 53 min ago
Queued 0.17 sec
Took 6.9 sec
Graph
Start
Menjalankan Aplikasi...
Melakukan Security...
Menghasilkan Laporan
Menghentikan Aplikasi
End
Search
Menjalankan Aplikasi Rentan (DVWA)
0.71s
Started 1h 53m ago
Jenkins
Menjalankan Aplikasi Rentan (DVW
Melakukan Security Scan dengan Z
Menghasilkan Laporan 65ms
Menghentikan Aplikasi 46ms
Build scheduled
Menjalankan DVWA di Docker...
22ms
docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa
0.54s
0 + docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa
1 /var/jenkins_home/workspace/security-scan@tmp/durable-8a84e56d/script.sh.copy: 1: docker: not found
2 script returned exit code 127

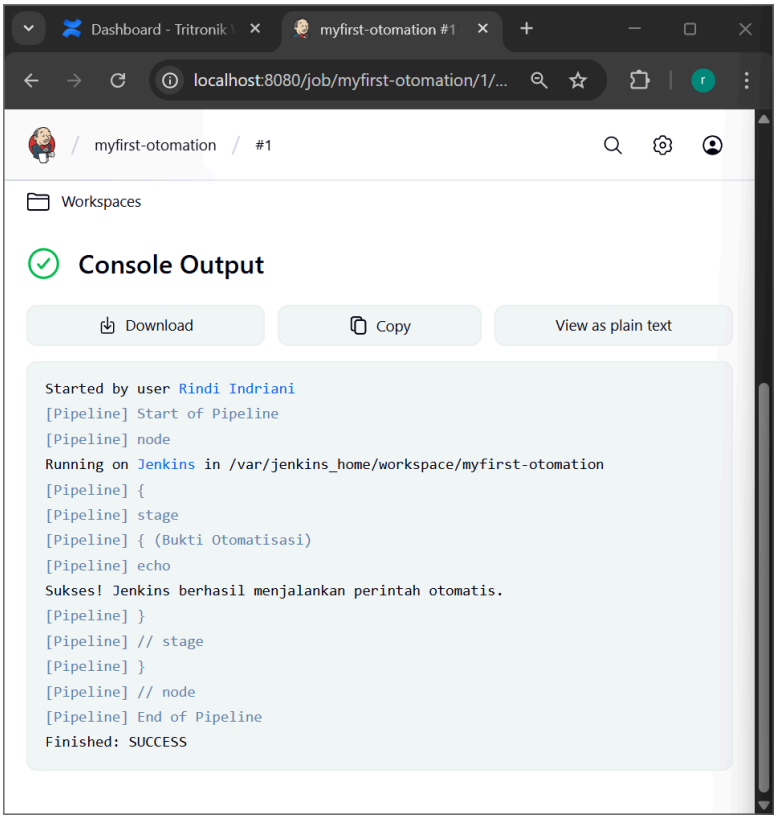

(Implementation Versi
Starting Jenkins
localhost:8080
Jenkins is getting ready to work
Your browser will reload automatically when Jenkins is ready.

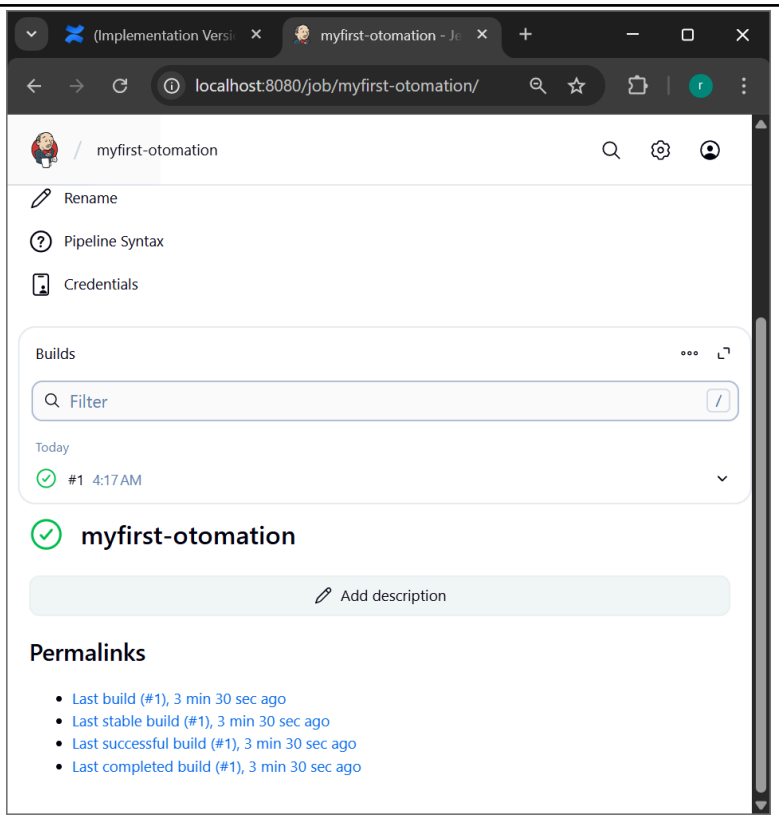

(Implementation Versi
Sign in - Jenkins
localhost:8080/login?from=%2F
Sign in to Jenkins
Username
rindindriani
Password
Keep me signed in
Sign in

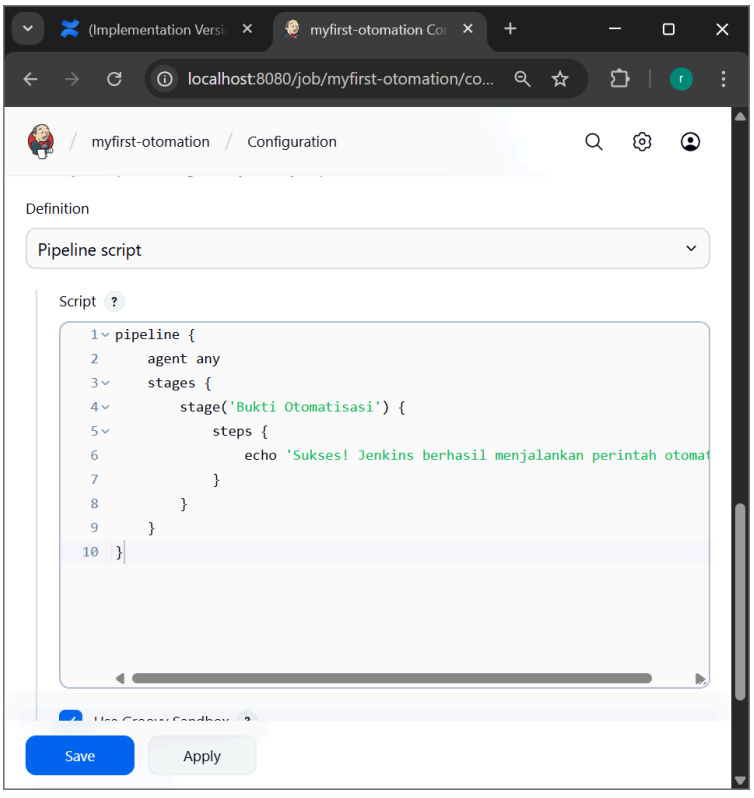

(Implementation Versi
Replay #4 - Jenkins
localhost:8080/job/security-scan/4/replay/
Jenkins
security-scan
#4
Replay
Replay #4
Allows you to replay a Pipeline build with a modified script. If any load steps were run, you can also modify the scripts they loaded.
Main Script
pipeline {
agent any
stages {
stage('Menjalankan Aplikasi Rentan (DVWA)') {
steps {
echo 'Menjalankan DVWA di Docker...'
// Perintah ini menjalankan DVWA di dalam container Docker.
// Perintah ini hanya contoh teoritis karena DVWA sudah kamu jalankan
sh 'docker run --rm -d -p 8080:80 --name dvwa vulnerables/web-dvwa'
}
}
stage('Melakukan Security Scan dengan ZAP') {
Pipeline Syntax
Run
Jenkins 2.516.2

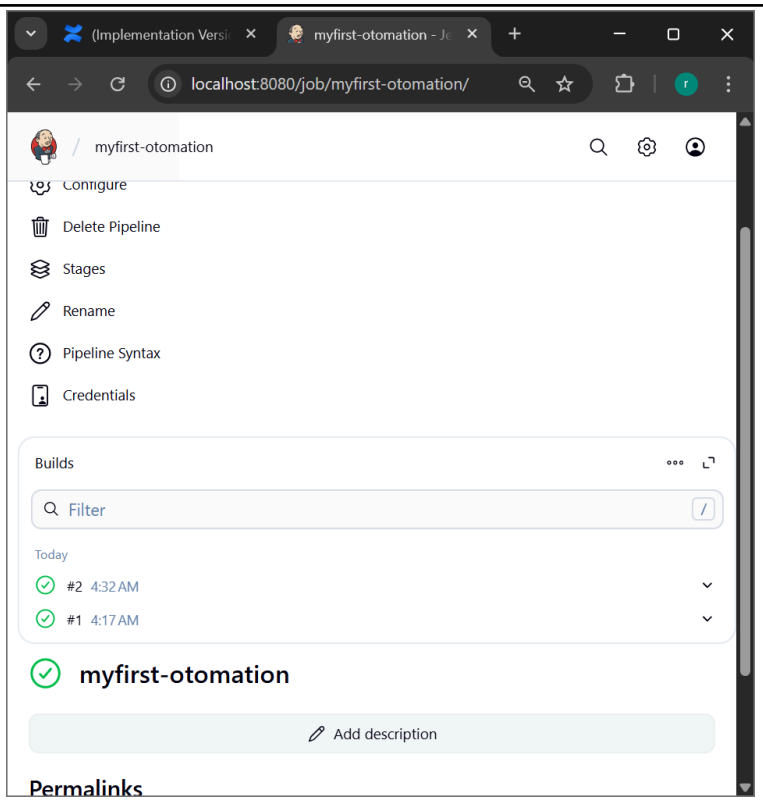

(Implementation Versi
security-scan Config
localhost:8080/job/security-scan/configure
Jenkins
security-scan
Configuration
Pipeline
Define your Pipeline using Groovy directly or pull it from source control.
Definition
Pipeline script
Script
try sample Pipeline...
pipeline {
agent any
stages {
stage('Menjalankan Container Docker') {
steps {
echo 'Memulai proses...'
sh 'docker run hello-world'
echo 'Proses selesai.'
}
}
}
}
Use Groovy Sandbox
Save
Apply

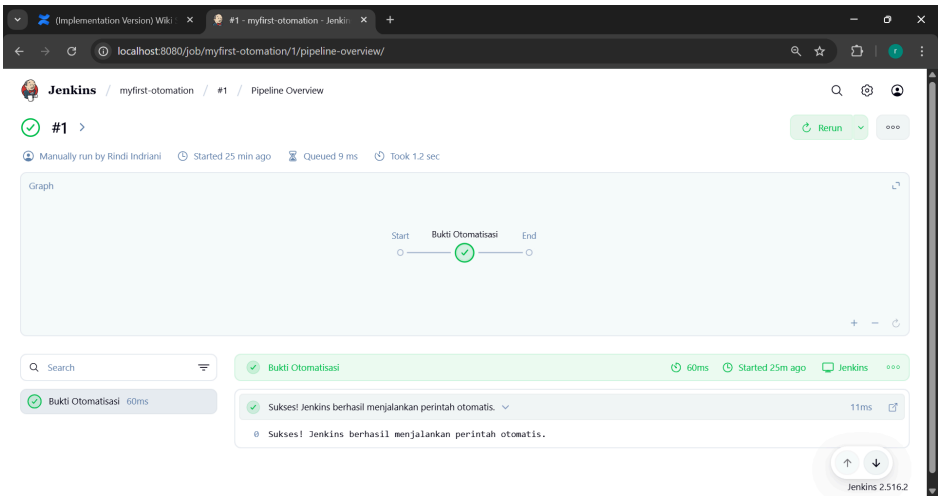

localhost:8080/job/security-scan/12/cons...
security-scan
#12
Previous Build
Console Output
Download
Copy
View as plain text
Started by user Rindi Indriani
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in /var/jenkins_home/workspace/security-scan
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Hello)
[Pipeline] echo
Hello World
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS


Dashboard - Tritronik
myfirst-otomation #1
localhost:8080/job/myfirst-otomation/1/...
myfirst-otomation
#1
Workspaces
Console Output
Download
Copy
View as plain text
Started by user Rindi Indriani
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in /var/jenkins_home/workspace/myfirst-otomation
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Bukti Otomatisasi)
[Pipeline] echo
Sukses! Jenkins berhasil menjalankan perintah otomatis.
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS


(Implementation Versi
myfirst-otomation - Je
localhost:8080/job/myfirst-otomation/
myfirst-otomation
Rename
Pipeline Syntax
Credentials
Builds
Filter
/
Today
#1 4:17 AM
myfirst-otomation
Add description
Permalinks
Last build (#1), 3 min 30 sec ago
Last stable build (#1), 3 min 30 sec ago
Last successful build (#1), 3 min 30 sec ago
Last completed build (#1), 3 min 30 sec ago


(Implementation Versi
myfirst-otomation Cor
localhost:8080/job/myfirst-otomation/co...
myfirst-otomation
Configuration
Definition
Pipeline script
Script
pipeline {
agent any
stages {
stage('Bukti Otomatisasi') {
steps {
echo 'Sukses! Jenkins berhasil menjalankan perintah otomat
}
}
}
}
Save
Apply

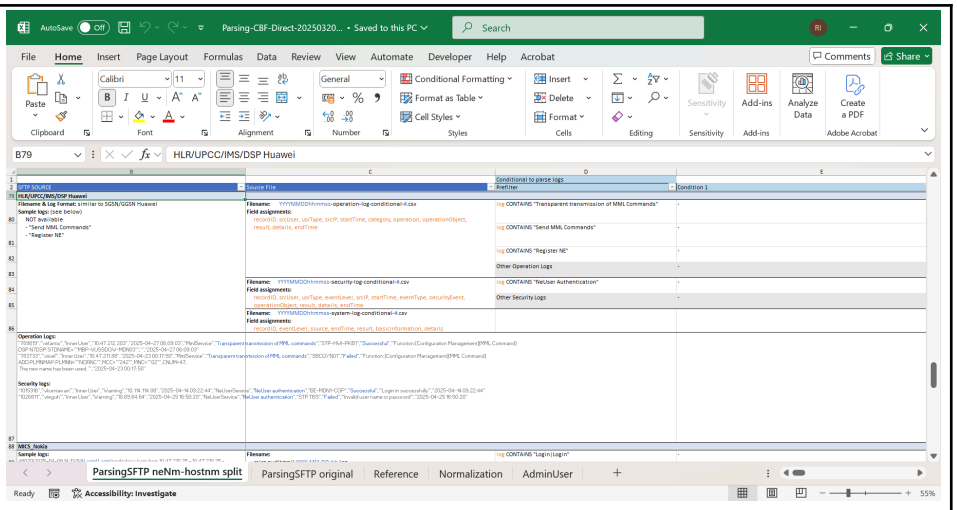
<table>
<tr>
<td></td>
<td>


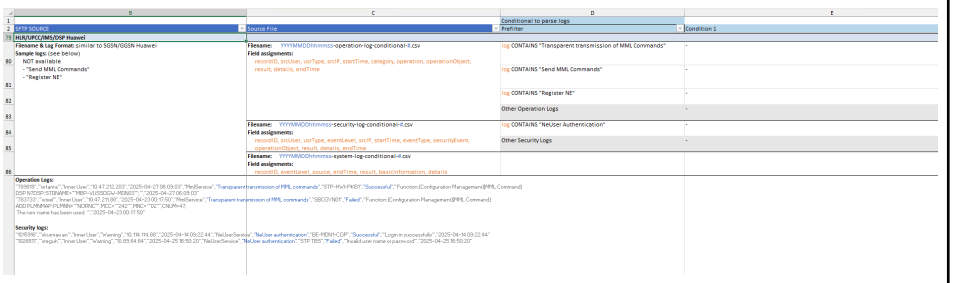


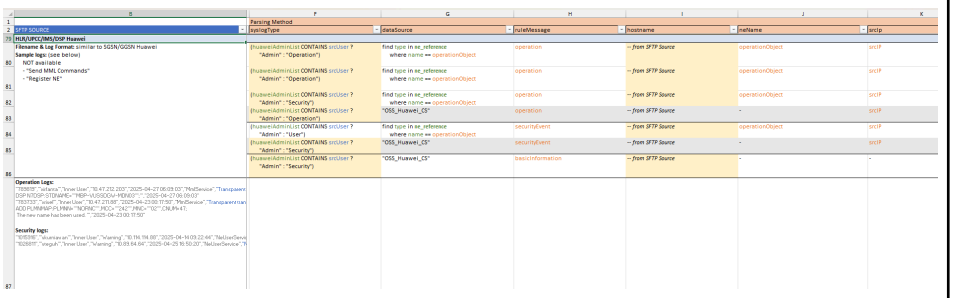
• Berhasil mencari solusi pada error yang ditemukan pada eksplorasi Jenkins
• Selesai melakukan fiksasi pada implementasi OWASP ZAP dan Jenkins integration
</td>
</tr>
<tr>
<td>Lesson Learned</td>
<td>Quote of the day:
Let go of fear and trust the timing of your life.</td>
</tr>
<tr>
<td>Keterangan</td>
<td>-</td>
</tr>
</table>

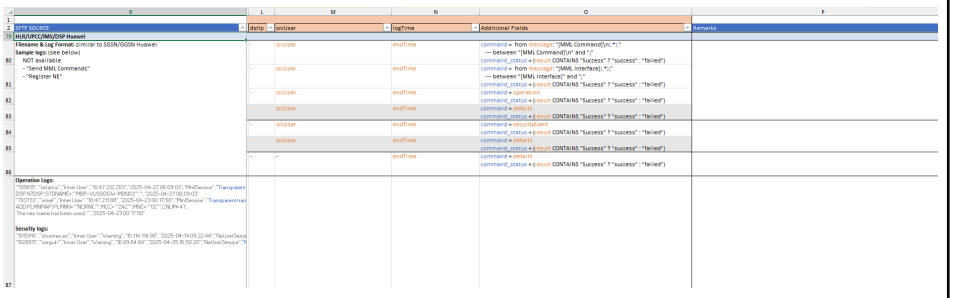
No : 12	Periode : 15 September s.d. 19 September 2025
Sub No : 12.3	Hari/Tanggal : Rabu, 17 September 2025
Proyek	Nama Proyek : USIEM Tsel Project Project Manager : Irfan Nurdin Salman Technical Leader : Regina Christiany
Tugas	Re-finding sample oss_nokia for produce message from collector sftp oss nokia to processor oss nokia
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3 Melanjutkan kembali mencari sampel ims huawei _____ 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor _____ 13.00 WIB Membuat draft test case untuk test case ims_huawei template _____ 17.00 WIB Membereskan barang-barang karena jam kerja sudah selesai
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words • Notion • Wiki • Excel • Prisma Browser • Putty • Kafka • GlobalProtect

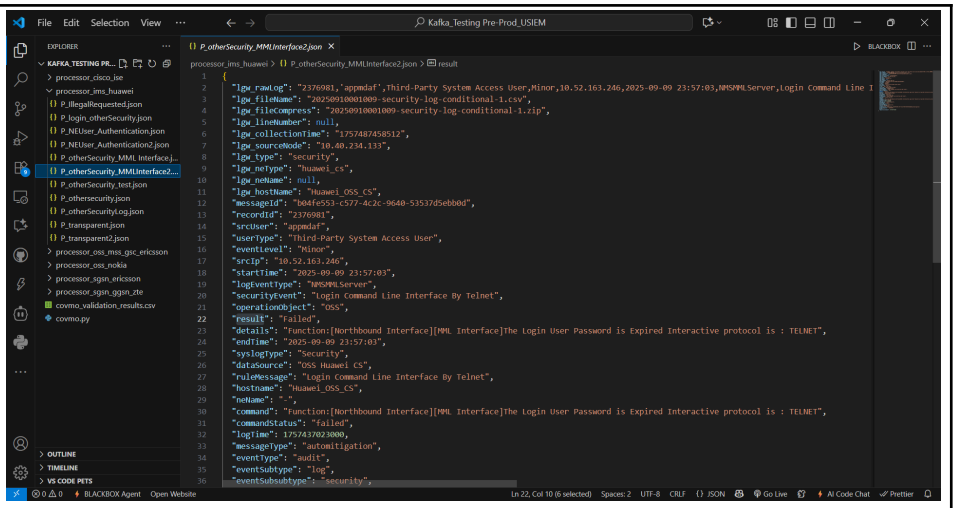
Hasil Kerja


Parsing-CBF-Direct-20250320...
Search
File Home Insert Page Layout Formulas Data Review View Automate Developer Help Acrobat
B79
HLR/UPCC/IMS/DSP Huawei
ParsingSFTP neNm-hostnm split
ParsingSFTP original
Reference
Normalization
AdminUser
Ready
Accessibility: Investigate









TEST CASES TEMPLATE IMS HUAWEI CBF COMPLIANCE

TC ID	Test Case Description	Scenario Type	Prerequisite	Test Steps	Expected Result	Actual Result	Status	Priority	Evidence	Notes
TC#001	Validate SFTP Source configuration AND Source File accessibility compliance with CBF Excel specification for IMS Huawei	Positive	- USEM SFTP processor accessible - CBF Excel specification available - IMS Huawei source configured - Network connectivity to collector	1. Navigate to USIEM SFTP Source configuration 2. Verify SFTP SOURCE = "IMS/UPCF/IMS /DSP Huawei" per CBF Column 1 3. Validate Source Files per Column 2: YYYYMMDD-operation-log-conditional-*.csv, YYYYMMDD-security-log-conditional-*.csv, YYYYMMDD-system-log-conditional-*.csv 4. Test file accessibility and read permissions for available files 5. Document which files are accessible vs pending	SFTP Source & Source Files compliance: - SFTP SOURCE: "IMS/UPCF/IMS /DSP Huawei" (Column 1) - Available Files: operation-log, security-log, system-log accessible (Column 2) - CSV format with header validation - Configuration aligned with CBF requirements	[Execute & Fill]	[PASS/FAIL]	HIGH	usiem_ims_huawei_source_files_cbf_2025-01-10.xlsx ims_huawei_source_config_rindrn.log	CBF Excel Column 1-2 Combined
TC#002	Validate prefilter conditions implementation for IMS Huawei	Positive	- IMS Huawei CSV logs available - CBF Excel prefilter column reviewed - USEM processing pipeline active - Conditional parsing	1. Check CBF Excel Column 3 for prefilter specifications 2. Verify "Transparent transmission of MML Commands" prefilter 3. Test "Send MML	Prefilter implementation 100% compliant with CBF Excel: - "Transparent transmission of MML Commands" filter active - "Send MML Commands"	[Execute & Fill]	[PASS/FAIL]	MEDIUM	usiem_ims_huawei_prefilter_cbf_2025-01-10.xlsx ims_huawei_prefilter_validation_rindrn.log	CBF Excel Column 3 Compliance

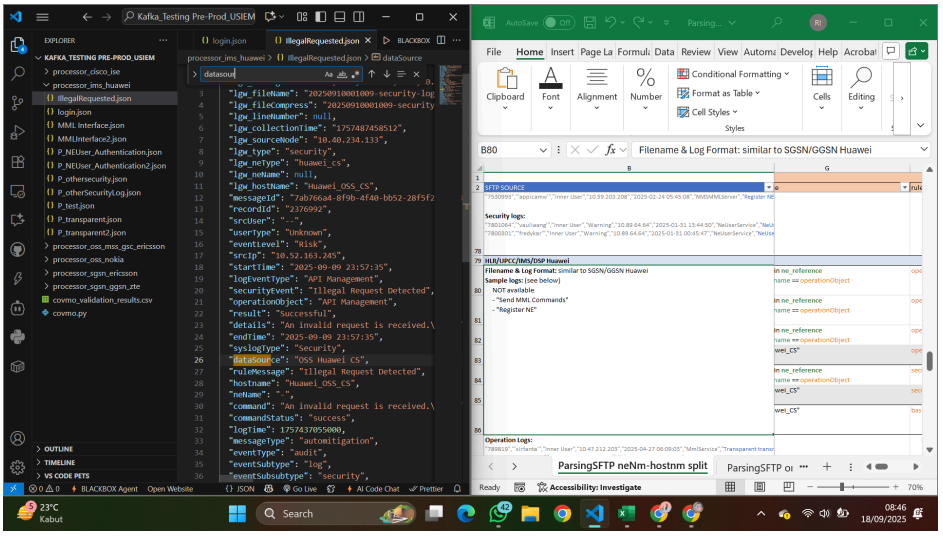
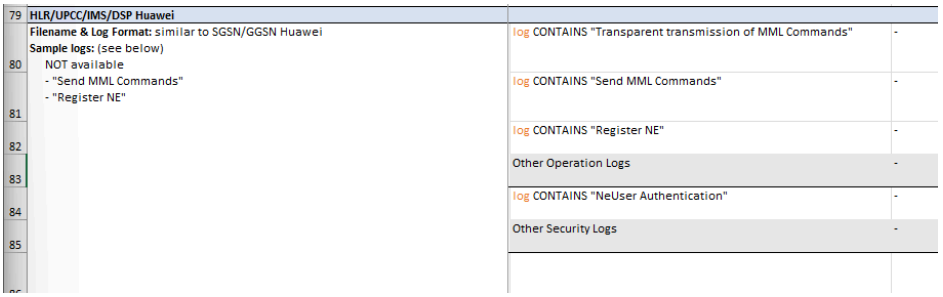
Menemukan kembali sample baru dari ims_huawei

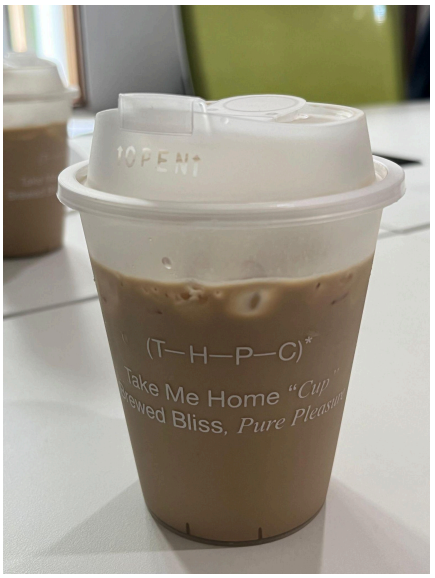
Berhasil membuat draft test case untuk test case ims_huawei template

Lesson Learned	Quote of the day: If you're ready to break the cycle… And rebuild from the inside out - with Allah at the centre.

Keterangan	 Makan diluar kantor (Nasi Telor Ma Edja)

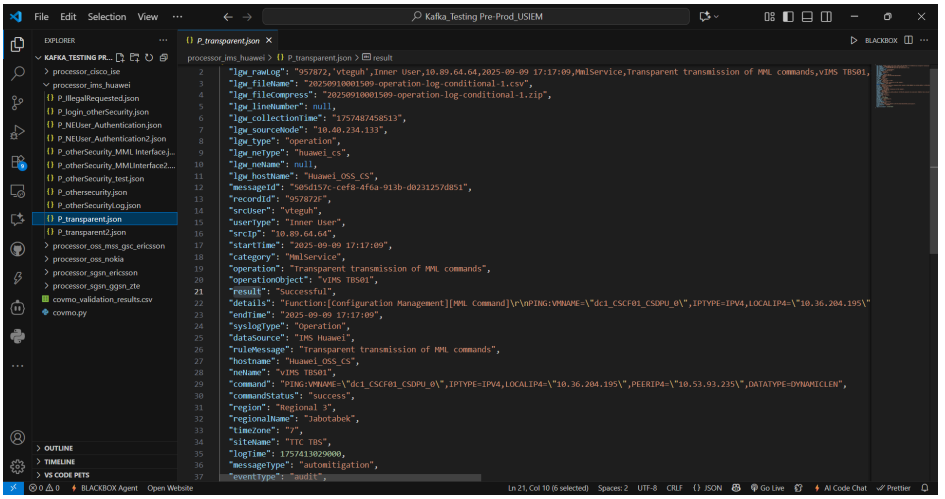
No : 12	Periode : 15 September s.d. 19 September 2025
Sub No : 12.4	Hari/Tanggal :Kamis, 18 September 2025
Proyek	Nama Proyek : USIEM Tsel Project Project Manager : Irfan Nurdin Salman Technical Leader : Regina Christiany
Tugas	Re-finding sample oss_nokia for produce message from collector sftp oss nokia to processor oss nokia PT. 2
Waktu dan Kegiatan Harian	08.00 WIB Hadir di meja kerja untuk melaksanakan KP Membuat test case untuk ims_huawei berdasarkan pedoman excel parsing cbf --- 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor --- 13.00 WIB Melanjutkan pembuatan test case untuk ims_huawei berdasarkan file pedoman excel parsing CBF --- 17.00 WIB Membereskan barang-barang karena jam kerja sudah selesai

Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words • Notion • Wiki • Excel • Prisma Browser • Putty • Kafka • GlobalProtect
Hasil Kerja	 

	TEST CASES TEMPLATE IMS HUAWEI CBF COMPLIANCE TC ID | Test Case Description | Scenario Type | Prerequisite | Test Steps | Expected Result | Actual Result | Status | Priority | Evidence | Notes TC#001 | Validate SFTP Source configuration AND Source File accessibility compliance with CBF Excel specification for IMS Huawei | Positive | - USEM SFTP processor accessible - CBF Excel specification available - IMS Huawei source configured - Network connectivity to collector | 1. Navigate to USEM SFTP Source configuration 2. Verify SFTP SOURCE = "IMS/UPCF/IMS /DSP Huawei" per CBF Column 1 3. Validate Source Files per Column 2: YYYYMMDD-operation-log-conditional-.csv, YYYYMMDD-security-log-conditional-.csv, YYYYMMDD-system-log-conditional-*.csv 4. Test file accessibility and read permissions for available files 5. Document which files are accessible vs pending | SFTP Source & Source Files compliance: - SFTP SOURCE: "IMS/UPCF/IMS /DSP Huawei" (Column 1) - Available Files: operation-log, security-log, system-log accessible (Column 2) - CSV format with header validation - Configuration aligned with CBF requirements | [Execute & Fill] | [PASS/FAIL] | 🔴 HIGH | usiem_ims_huawei_source_files_cbf_2025-01-10.xlsx ims_huawei_source_config_rindrn.log | CBF Excel Column 1-2 Combined TC#002 | Validate prefilter conditions implementation for IMS Huawei | Positive | - IMS Huawei CSV logs available - CBF Excel prefilter column reviewed - USIEM processing pipeline active - Conditional parsing | 1. Check CBF Excel Column 3 for prefilter specifications 2. Verify "Transparent transmission of MML Commands" prefilter 3. Test "Send MML | Prefilter implementation 100% compliant with CBF Excel: - "Transparent transmission of MML Commands" filter active - "Send MML Commands" | [Execute & Fill] | [PASS/FAIL] | 🟠 MEDIUM | usiem_ims_huawei_prefilter_cbf_2025-01-10.xlsx ims_huawei_prefilter_validation_rindrn.log | CBF Excel Column 3 Compliance - Memiliki test case untuk mendokumentasikan sampel yang ada pada ims_huawei
Lesson Learned	Quote of the day: Either it works out, or it turns into poetry. There isn't any losing, I think.
Keterangan	 Mendapat coffee dari teman kantor

	  Menonton Conjuring The Last Rits Bersama Teman Kantor

No : 12	Periode : 15 September s.d. 19 September 2025
Sub No : 12.5	Hari/Tanggal : Jumat, 19 September 2025
Proyek	Nama Proyek : USIEM Tsel Project
	Project Manager : Irfan Nurdin Salman
	Technical Leader : Regina Christiany
Tugas	Execute test c
Waktu dan Kegiatan Harian	08.00 WIB Hadir di PT Tricada Intronik (Tritronik) Memasuki ruangan saya di Lantai 3 Melakukan execute test case pada topik ims_huawei --- 12.00 WIB Istirahat makan siang bersama dengan teman-teman di kantor

	13.00 WIB Memasukkan hasil execute ke dalam test case ims_huawei 17.00 WIB Membereskan barang-barang karena jam kerja sudah selesai
Tools yang digunakan	• Buku tulis kosong • Pulpen • Laptop • Chrome/ Microsoft Edge • Google docs/Words • Notion • Wiki • Excel • Prisma Browser • Putty • Kafka • GlobalProtect
Hasil Kerja	

	IMS HUAWEI CBF COMPLIANCE TEST CASES TC ID: TC#001 Test Case Description: Validate SFTP Source configuration AND Source File accessibility compliance with CBF Excel specification for IMS Huawei Scenario Type: Positive Prerequisite: - USIEM SFTP processor accessible - CBF Excel specification available - IMS Huawei source configured - Network connectivity to collector Test Steps: 1. Navigate to USIEM SFTP Source configuration 2. Verify SFTP SOURCE = "IMS/UPCF/IMS /DSP Huawei" per CBF Column 1 3. Validate Source Files per Column 2: YYYYMMDD-operation-log-conditional-.csv, YYYYMMDD-security-log-conditional-.csv, YYYYMMDD-system-log-conditional-*.csv 4. Test file accessibility and read permissions for available files 5. Document which files are accessible vs pending Expected Result: SFTP Source & Source Files compliance: - SFTP SOURCE: "IMS/UPCF/IMS /DSP Huawei" (Column 1) - Available Files: operation-log, security-log, system-log accessible (Column 2) - CSV format with header validation - Configuration aligned with CBF requirements Actual Result: ACTUAL RESULT: - SFTP SOURCE displayed as "IMS/UPCF/IMS /DSP Huawei" - SFTP connection status: ACTIVE - 20250917-operation-log-conditional-030311.csv: ACCESSIBLE - 20250917-security-log-conditional-030311.csv: ACCESSIBLE - 20250917-system-log-conditional-030311.csv: ACCESSIBLE - CSV header validation: PASSED - File permissions: READ/WRITE - Total files found: 89 operation, 45 security, 23 system files - File size validation: 234MB average - Network connectivity: STABLE - Collector response time: Status: [PASS/FAIL] Priority: HIGH Evidence: Notes: CBF Excel Column 1-2 Combined • Berhasil melakukan execute test case untuk ims_huawei • Memasukkan hasil execute ims_huawei ke dalam test case
Lesson Learned	Quote of the day: It takes time to learn how to be alone without being lonely, but once you do, it's called freedom.
Keterangan	 Ulang Tahun Ibu Vice President