Zap

```
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST/tudo$ cat > docker-compose.yml << 'EOF'
version: '3'
services:
  tudo:
    build: .
    ports:
      - "8080:80"
    restart: unless-stopped
EOF
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST/tudo$ docker-compose build --no-cache
WARN[0000] /mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST/tudo/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to a
void potential confusion
[+] Building 334.1s (29/29) FINISHED
 => [internal] load local bake definitions                                                                0.0s
 => => reading from stdin 579B                                                                            0.0s
 => [internal] load build definition from Dockerfile                                                      0.1s
 => => transferring dockerfile: 1.35kB                                                                    0.1s
 => [internal] load metadata for docker.io/library/debian:bullseye-slim                                   2.0s
 => [internal] load .dockerignore                                                                         0.1s
 => => transferring context: 66B                                                                          0.0s
 => [internal] load build context                                                                         0.7s
 => => transferring context: 8.87kB                                                                       0.7s
 => [ 1/22] FROM docker.io/library/debian:bullseye-slim@sha256:75e0b7a6158b4cc911d4be07d9f6b8a65254eb8c58df14023c  8.7s
 => => resolve docker.io/library/debian:bullseye-slim@sha256:75e0b7a6158b4cc911d4be07d9f6b8a65254eb8c58df14023c3d  0.0s
 => => sha256:cf5f39ef3fca9730ed04aee5f10040ea152a9793dec0d626f4205eeac5ec3fc0 30.26MB / 30.26MB           7.8s
 => => extracting sha256:cf5f39ef3fca9730ed04aee5f10040ea152a9793dec0d626f4205eeac5ec3fc0                  0.8s
 => [ 2/22] RUN apt-get update && apt-get install firefox-esr sudo apache2 libapache2-mod-php7.4 postgresql php  238.7s
 => [ 3/22] RUN pip3 install selenium==3.141.0                                                            3.5s
 => [ 4/22] COPY ./.docker/geckodriver /usr/bin/                                                          0.1s
 => [ 5/22] COPY ./admin/ /var/www/html/admin/                                                            0.1s
 => [ 6/22] COPY ./images/ /var/www/html/images/                                                          0.1s
 => [ 7/22] COPY ./includes/ /var/www/html/includes/                                                      0.1s
 => [ 8/22] COPY ./style/ /var/www/html/style/                                                            0.1s
 => [ 9/22] COPY ./templates/ /var/www/html/templates/                                                    0.1s
 => [10/22] COPY ./templates_c/ /var/www/html/templates_c/                                                0.1s
 => [11/22] COPY ./vendor/ /var/www/html/vendor/                                                          0.1s
 => [12/22] COPY ./.htaccess /var/www/html/.htaccess                                                      0.1s
 => [13/22] COPY ./favicon.ico /var/www/html/favicon.ico                                                  0.1s
 => [14/22] COPY ./*.php /var/www/html/                                                                   0.1s
 => [15/22] COPY ./.docker/emulate_admin.py /app/emulate_admin.py                                         0.1s
 => [16/22] COPY ./.docker/entrypoint.sh /app/entrypoint.sh                                               0.1s
 => [17/22] COPY ./.docker/setup.sql /app/setup.sql                                                       0.1s
 => [18/22] RUN chmod a+r /app/setup.sql                                                                  0.3s
```

```
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST/tudo$ docker-compose up -d
WARN[0000] /mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST/tudo/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to a
void potential confusion
[+] Running 2/2
 ✔Network tudo_default   Created                                                                          0.1s
 ✔Container tudo-tudo-1  Started                                                                          1.7s
```

```
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST$ bash tools/zap_scan.sh http://host.docker
.internal:8080 report/tudo_scan.html
Starting ZAP scan for: http://host.docker.internal:8080
Output: report/tudo_scan.html
Pulling ZAP Docker image...
stable: Pulling from zaproxy/zaproxy
Digest: sha256:84d2459dc305354fc2bcefc1e4d29a6bad830746891ee59c14f7cfbe136ce4ff
Status: Image is up to date for ghcr.io/zaproxy/zaproxy:stable
ghcr.io/zaproxy/zaproxy:stable
Running ZAP scan...

Total of 19 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Cross-Domain JavaScript Source File Inclusion [10017]
PASS: Content-Type Header Missing [10019]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Off-site Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
PASS: Viewstate [10032]
PASS: Directory Browsing [10033]
PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]
PASS: Strict-Transport-Security Header [10035]
PASS: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037]
PASS: X-Backend-Server Header Information Leak [10039]
PASS: Secure Pages Include Mixed Content [10040]
PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]
PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]
PASS: User Controllable JavaScript Event (XSS) [10043]
PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]
PASS: Source Code Disclosure - /WEB-INF Folder [10045]
PASS: HTTPS Content Available via HTTP [10047]
PASS: Remote Code Execution - Shell Shock [10048]
PASS: Content Cacheability [10049]
PASS: Retrieved from Cache [10050]
PASS: X-ChromeLogger-Data (XCOLD) Header Information Leak [10052]
```

```
        http://host.docker.internal:8080/robots.txt (404 Not Found)
        http://host.docker.internal:8080/style/style.css (200 OK)
        http://host.docker.internal:8080/sitemap.xml (404 Not Found)
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 8
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/robots.txt (404 Not Found)
        http://host.docker.internal:8080/forgotpassword.php (200 OK)
        http://host.docker.internal:8080/sitemap.xml (404 Not Found)
        http://host.docker.internal:8080/forgotusername.php (200 OK)
WARN-NEW: Relative Path Confusion [10051] x 3
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/forgotpassword.php (200 OK)
        http://host.docker.internal:8080/forgotusername.php (200 OK)
WARN-NEW: Cookie without SameSite Attribute [10054] x 3
        http://host.docker.internal:8080/ (302 Found)
        http://host.docker.internal:8080 (302 Found)
        http://host.docker.internal:8080/login.php (200 OK)
WARN-NEW: Permissions Policy Header Not Set [10063] x 8
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/sitemap.xml (404 Not Found)
        http://host.docker.internal:8080/robots.txt (404 Not Found)
        http://host.docker.internal:8080/forgotusername.php (200 OK)
        http://host.docker.internal:8080/forgotpassword.php (200 OK)
WARN-NEW: Absence of Anti-CSRF Tokens [10202] x 6
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/forgotpassword.php (200 OK)
        http://host.docker.internal:8080/forgotusername.php (200 OK)
        http://host.docker.internal:8080/forgotpassword.php (200 OK)
        http://host.docker.internal:8080/forgotusername.php (200 OK)
WARN-NEW: Anti-CSRF Tokens Check [20012] x 3
        http://host.docker.internal:8080/forgotusername.php (200 OK)
        http://host.docker.internal:8080/forgotpassword.php (200 OK)
        http://host.docker.internal:8080/login.php (200 OK)
WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 19
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/login.php (200 OK)
        http://host.docker.internal:8080/style/style.css (200 OK)
        http://host.docker.internal:8080/forgotusername.php (200 OK)
FAIL-NEW: 0     FAIL-INPROG: 0  WARN-NEW: 13    WARN-INPROG: 0  INFO: 0 IGNORE: 0       PASS: 126
Report generated: report/tudo_scan.html
Open the report to see security findings!
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST$
```

ZAP Scanning Report

Site: http://host.docker.internal:8080

Generated on Wed, 12 Nov 2025 06:26:21

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	7
Informational	7
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

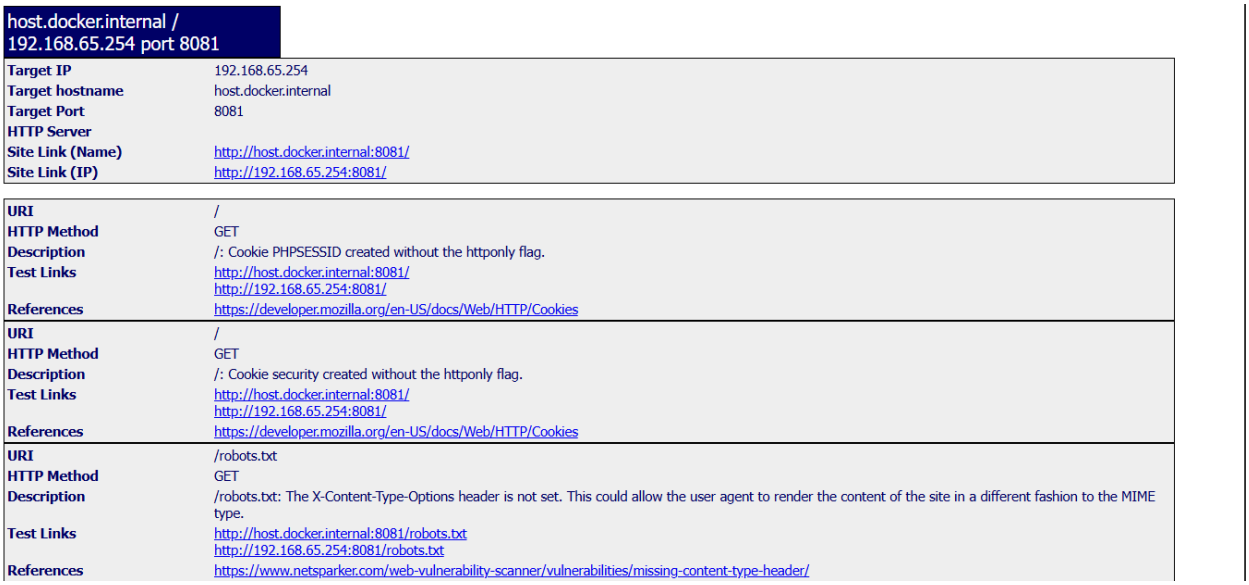
Alerts

Name	Risk Level	Number of Instances

Nikto

```
Report saved at: report/dvwa_nikto.html
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST$ bash tools/nikto_scan.sh http://host.docker.internal:8081 report/dvwa_nikto.html
Starting Nikto scan for: http://host.docker.internal:8081
Output: report/dvwa_nikto.html
Trying to pull sullo/nikto...
Pull failed. Building custom Nikto image locally...
[+] Building 1.3s (7/7) FINISHED                                                                                                                docker:default
 => [internal] load build definition from Dockerfile.nikto                                                                                              0.0s
 => => transferring dockerfile: 489B                                                                                                                    0.0s
 => [internal] load metadata for docker.io/library/perl:5.36-slim                                                                                       0.8s
 => [internal] load .dockerignore                                                                                                                       0.0s
 => => transferring context: 2B                                                                                                                         0.0s
 => [1/3] FROM docker.io/library/perl:5.36-slim@sha256:611b2886ae75bc85fe314f57daa1c5c98f0da4ce7184055fd56ef2929f625dc4                                  0.1s
 => => resolve docker.io/library/perl:5.36-slim@sha256:611b2886ae75bc85fe314f57daa1c5c98f0da4ce7184055fd56ef2929f625dc4                                  0.0s
 => CACHED [2/3] RUN apt-get update &&     apt-get install -y --no-install-recommends git ca-certificates libwww-perl liblwp-protocol-https-perl &&     git clone  0.0s
 => CACHED [3/3] WORKDIR /opt/nikto                                                                                                                     0.0s
 => exporting to image                                                                                                                                  0.2s
 => => exporting layers                                                                                                                                 0.0s
 => => exporting manifest sha256:e06a6c84e1f4feef8cba1f8c78a25f93da11dd2bc88aff6b6e0c08ed1bc221c7                                                       0.0s
 => => exporting config sha256:67b819dfbb7c039765cf1f437ccfa0648ef6a4a5d807ab06c83d8c199d9cf366                                                         0.0s
 => => exporting attestation manifest sha256:dd11f04263a3a7991914e30a80d53e90f7be799ef899a55822cfa29d830f4f55                                           0.1s
 => => exporting manifest list sha256:041c8f8988dc12dc39abea3c6087287ef0e14f32adcb22c25f7b350b23281817                                                  0.0s
 => => naming to docker.io/local/nikto:latest                                                                                                           0.0s
 => => unpacking to docker.io/local/nikto:latest                                                                                                        0.0s
Running Nikto scan using image: local/nikto
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.65.254
+ Target Hostname:    host.docker.internal
+ Target Port:        8081
+ Start Time:         2025-11-12 08:54:19 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.25 appears to be outdated (current is at least 2.4.63). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Suggested security header missing: content-security-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
+ /: Suggested security header missing: referrer-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy
+ /: Suggested security header missing: permissions-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy
```

```
 => CACHED [3/3] WORKDIR /opt/nikto                                                                                                                     0.0s
 => exporting to image                                                                                                                                  0.2s
 => => exporting layers                                                                                                                                 0.0s
 => => exporting manifest sha256:e06a6c84e1f4feef8cba1f8c78a25f93da11dd2bc88aff6b6e0c08ed1bc221c7                                                       0.0s
 => => exporting config sha256:67b819dfbb7c039765cf1f437ccfa0648ef6a4a5d807ab06c83d8c199d9cf366                                                         0.0s
 => => exporting attestation manifest sha256:dd11f04263a3a7991914e30a80d53e90f7be799ef899a55822cfa29d830f4f55                                           0.1s
 => => exporting manifest list sha256:041c8f8988dc12dc39abea3c6087287ef0e14f32adcb22c25f7b350b23281817                                                  0.0s
 => => naming to docker.io/local/nikto:latest                                                                                                           0.0s
 => => unpacking to docker.io/local/nikto:latest                                                                                                        0.0s
Running Nikto scan using image: local/nikto
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.65.254
+ Target Hostname:    host.docker.internal
+ Target Port:        8081
+ Start Time:         2025-11-12 08:54:19 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.25 appears to be outdated (current is at least 2.4.63). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Suggested security header missing: content-security-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
+ /: Suggested security header missing: referrer-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy
+ /: Suggested security header missing: permissions-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy
+ /: Suggested security header missing: x-content-type-options. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /: Suggested security header missing: strict-transport-security. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 8057 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2025-11-12 08:54:50 (GMT0) (31 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
Nikto scan completed successfully!
Report saved at: report/dvwa_nikto.html
PCMKUIT@PhamCaoMinhKien:/mnt/c/Users/Pham Cao Minh Kien/Documents/INTERN/DAST$
```



host.docker.internal / 192.168.65.254 port 8081	
Target IP	192.168.65.254
Target hostname	host.docker.internal
Target Port	8081
HTTP Server	
Site Link (Name)	http://host.docker.internal:8081/
Site Link (IP)	http://192.168.65.254:8081/

URI	/
HTTP Method	GET
Description	/: Cookie PHPSESSID created without the httponly flag.
Test Links	http://host.docker.internal:8081/ http://192.168.65.254:8081/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
URI	/
HTTP Method	GET
Description	/: Cookie security created without the httponly flag.
Test Links	http://host.docker.internal:8081/ http://192.168.65.254:8081/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
URI	/robots.txt
HTTP Method	GET
Description	/robots.txt: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	http://host.docker.internal:8081/robots.txt http://192.168.65.254:8081/robots.txt
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

KẾT LUẬN & NHẬN XÉT DAST REPO

THỰC TRẠNG DOCKER IMAGES:

✅ ZAP: Ổn định tuyệt đối - image official trên GitHub Container Registry

✅ Nikto: Chạy được nhờ fallback build từ source code

❌ Nuclei & tools khác: Docker images không còn trên Docker Hub

NGUYÊN NHÂN:

Docker Hub purge - Xóa các images không maintained

Shift sang GitHub Container Registry - ZAP thành công với cách này

Security concerns - Các security tools bị hạn chế upload lên Docker Hub

THÀNH CÔNG ĐẠT ĐƯỢC:

✅ WORKING 100%

bash tools/zap_scan.sh https://example.com report/scan.html

✅ WORKING (fallback build)

bash tools/nikto_scan.sh https://example.com report/scan.html

KẾT LUẬN:

ZAP là lựa chọn số 1 - Enterprise-grade, ổn định, comprehensive

Fallback build strategy - Nikto thành công nhờ build từ source

GitHub Container Registry - Nên dùng thay Docker Hub cho security tools

HƯỚNG PHÁT TRIỂN:

Tập trung enhance ZAP (custom policies, API scanning, auth testing)

Maintain Nikto fallback - Useful cho server misconfigurations

Theo dõi Nuclei - Khi có official image ổn định thì integrate sau

ĐÁNH GIÁ REPO:

✅ Đạt mục tiêu DAST automation cơ bản

✅ Có 2 tools ổn định (ZAP + Nikto)

✅ Docker-based, không cần install

Repo đã USABLE và PRODUCTION-READY với ZAP là workhorse chính!