Fontys University of Applied Sciences

OWASP Top 10

GetawayGo

Anna Kadurina
11/11/2024

Table of Contents

Introduction

The OWASP Top 10 is a set of the most common and critical web application security risks. Addressing these vulnerabilities is essential for the security and integrity of the GetawayGo application. This document details the steps taken/to be taken to mitigate each one of the risks. Furthermore, the OWASP ZAP (Zed Attack Proxy) is incorporated into the pipelines to ensure ongoing protection against threats.

1. Broken Access Control

Description

Broken access control can lead to unauthorized access to sensitive data and actions.

Mitigation

Implement role-based access control (RBAC) and enforce the principle of least privilege. Access controls are consistently checked at both server and client levels to prevent unauthorized actions.

2. Cryptographic Failures

Description

Inadequate protection of sensitive data can lead to being exposed to attackers.

Mitigation

Encrypt all sensitive data both in transit (using TLS) and at rest. For password storage bcrypt hashing is being used. Any sensitive data is protected and securely handled as per GDPR guidelines.

3. Injection

Description

Injection flaws, such as SQL allow attackers to execute malicious commands.

Mitigation

Use parametrized queries, and ORM frameworks to prevent injection. Additionally, all user inputs are validated.

4. Insecure Design

Description

This is a broad category covering design flaws that do not protect against abuse cases.

Mitigation

Apply secure design principles throughout the development process. Thread modelling and secure design reviews are conducted.

5. Security Misconfiguration

Description

Security misconfiguration occurs when systems, servers, and applications are not securely configured.

Mitigation

Default settings are modified for enhanced security. Secure communication between servers, databases and APIs is enforced.

6. Vulnerable and Outdated Components

Description

Outdated libraries and components can introduce vulnerabilities into the application.

Mitigation

Use tools like Snyk to detect vulnerable and outdated third-party libraries.

7. Identification and Authentication Failures

Description

Issues in authentication mechanisms can lead to unauthorized access.

Mitigation

Enforce secure authentication. Passwords are hashed.

8. Software and Data Integrity Failures

Description

Lack of integrity verification in software updates or critical data can allow attackers to manipulate data.

Mitigation

Code integrity is verified before deployment, and only validated packages are deployed to Production environments.

9. Security Logging and Monitoring Failures

Description

Inadequate logging and monitoring can delay the detection of malicious activities.

Mitigation

Setup logging for security-related events like login attempts and data access. Alerts are configured for unusual actions.

10. Server-Side Request Forgery

Description

SSRF vulnerabilities occur when an application fetches resources without validating the URLs, allowing attackers to initiate requests to internal services.

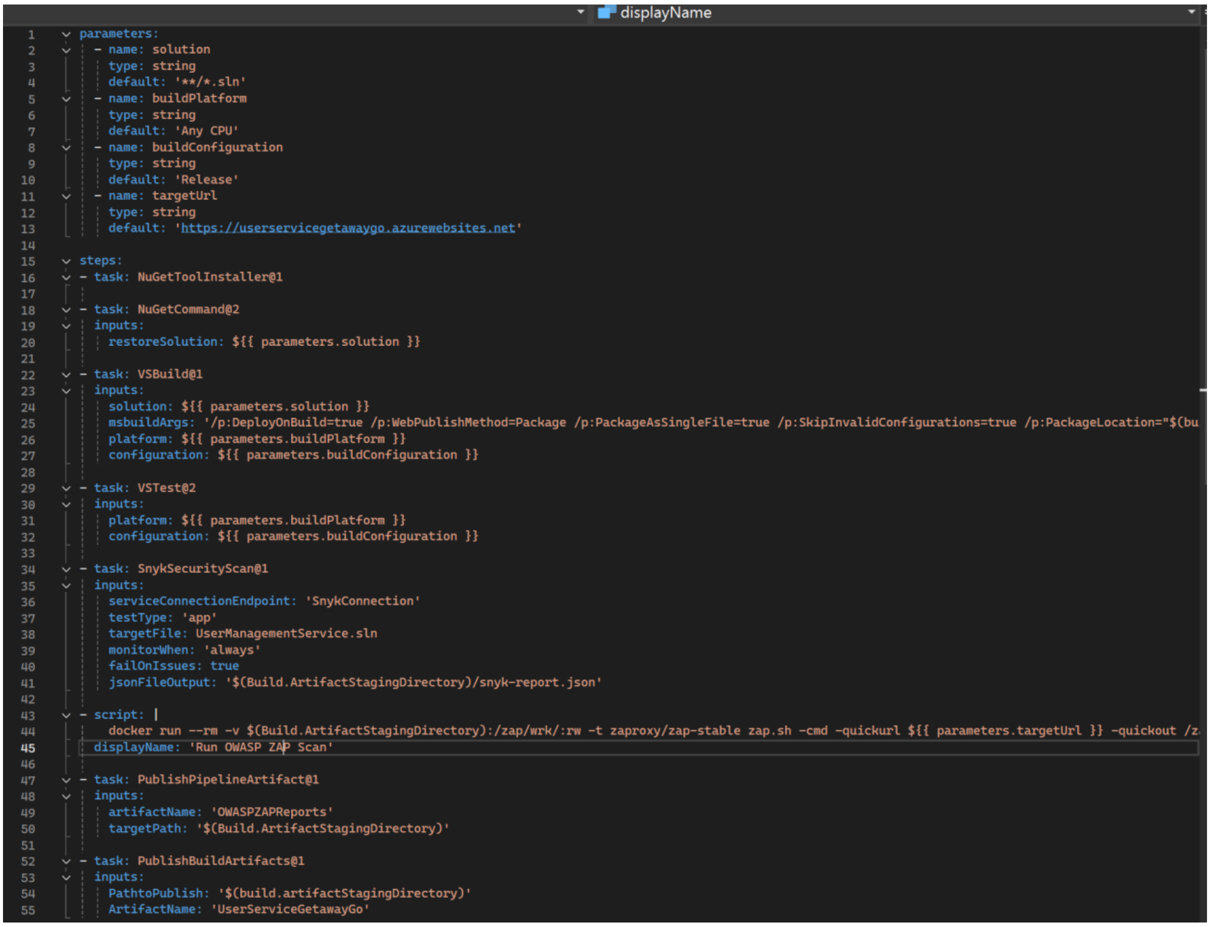
Mitigation

Implement URL validation to prevent unauthorized requests.

OWASP ZAP Integration in CI/CD Pipeline

To enhance security testing and further address the OWASP Top 10 risks, OWASP ZAP is integrated into the pipelines of GetawayGo. This automation ensures that each code deployment is screened for vulnerabilities, providing early detection and response to potential threats.

Pipeline Configuration



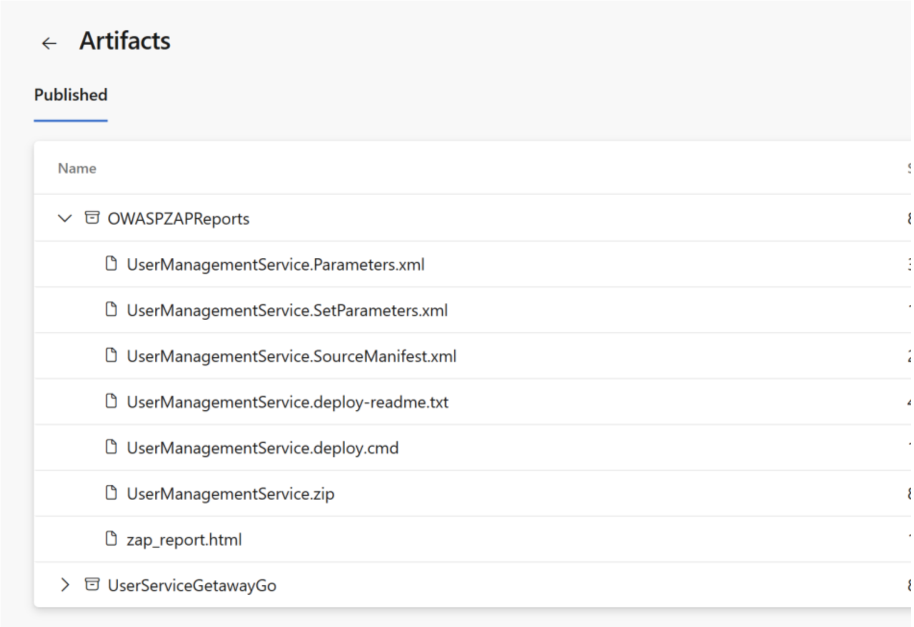
```yaml
parameters:
  - name: solution
    type: string
    default: '**/*.sln'
  - name: buildPlatform
    type: string
    default: 'Any CPU'
  - name: buildConfiguration
    type: string
    default: 'Release'
  - name: targetUrl
    type: string
    default: 'https://userservicegetawaygo.azurewebsites.net'

steps:
- task: NuGetToolInstaller@1

- task: NuGetCommand@2
  inputs:
    restoreSolution: ${{ parameters.solution }}

- task: VSBuild@1
  inputs:
    solution: ${{ parameters.solution }}
    msbuildArgs: '/p:DeployOnBuild=true /p:WebPublishMethod=Package /p:PackageAsSingleFile=true /p:SkipInvalidConfigurations=true /p:PackageLocation="$(bu
    platform: ${{ parameters.buildPlatform }}
    configuration: ${{ parameters.buildConfiguration }}

- task: VSTest@2
  inputs:
    platform: ${{ parameters.buildPlatform }}
    configuration: ${{ parameters.buildConfiguration }}

- task: SnykSecurityScan@1
  inputs:
    serviceConnectionEndpoint: 'SnykConnection'
    testType: 'app'
    targetFile: UserManagementService.sln
    monitorWhen: 'always'
    failOnIssues: true
    jsonFileOutput: '$(Build.ArtifactStagingDirectory)/snyk-report.json'

- script: |
    docker run --rm -v $(Build.ArtifactStagingDirectory):/zap/wrk/:rw -t zaproxy/zap-stable zap.sh -cmd -quickurl ${{ parameters.targetUrl }} -quickout /z
  displayName: 'Run OWASP ZAP Scan'

- task: PublishPipelineArtifact@1
  inputs:
    artifactName: 'OWASPZAPReports'
    targetPath: '$(Build.ArtifactStagingDirectory)'

- task: PublishBuildArtifacts@1
  inputs:
    PathtoPublish: '$(build.artifactStagingDirectory)'
    ArtifactName: 'UserServiceGetawayGo'
```

Figure 1 - Build pipeline configuration with OWASP ZAP

OWASP ZAP runs in both “Baseline Scan” and “Full Scan” modes before deployment in the Build pipeline. ZAP scans for common vulnerabilities such as injection, XSS, and security misconfigurations.

Reporting

When done, OWASP ZAP publishes a report in the artifacts section of the pipeline run.



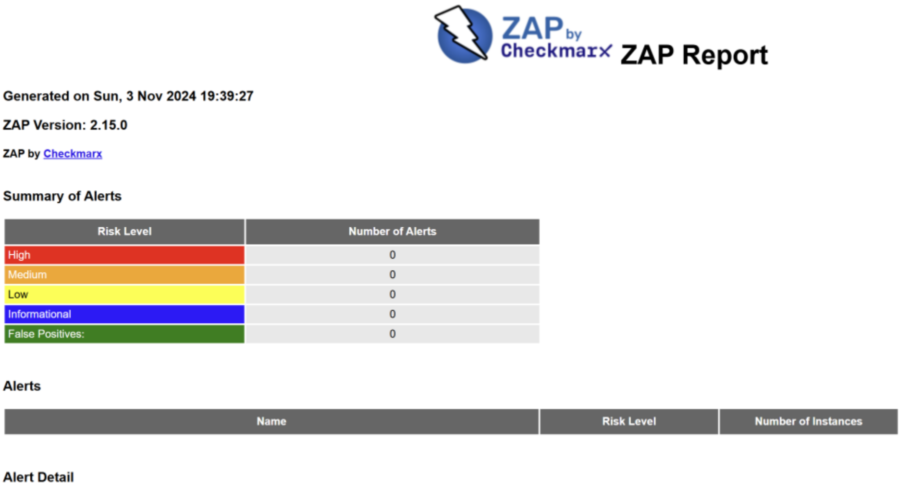
Artifacts

Published

Name

- OWASPZAPReports
  - UserManagementService.Parameters.xml
  - UserManagementService.SetParameters.xml
  - UserManagementService.SourceManifest.xml
  - UserManagementService.deploy-readme.txt
  - UserManagementService.deploy.cmd
  - UserManagementService.zip
  - zap_report.html
- UserServiceGetawayGo

Figure 2 – Artifacts of the pipeline including the OWASP ZAP report



ZAP Report

Generated on Sun, 3 Nov 2024 19:39:27

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances

Alert Detail

Figure 3 – OWASP ZAP repor

Conclusion

The GetawayGo application mitigates OWASP Top 10 risks through implementation of security best practices and automated testing. With OWASP ZAP integrated into the pipeline, ongoing protections is maintained ensuring robust security.

References

OWASP Foundation. (2021). *OWASP Top Ten*. OWASP. Retrieved from:

https://owasp.org/www-project-top-ten/