2025.11.10

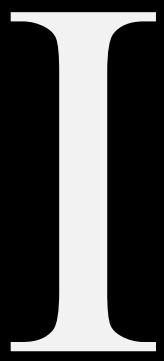
OWASP, CVE

가디언 웹 보안 세미나 7

임준서

About CVE

OWASP, CVE



OWASP

Open Worldwide Application Security Project

웹 애플리케이션 보안 프로젝트

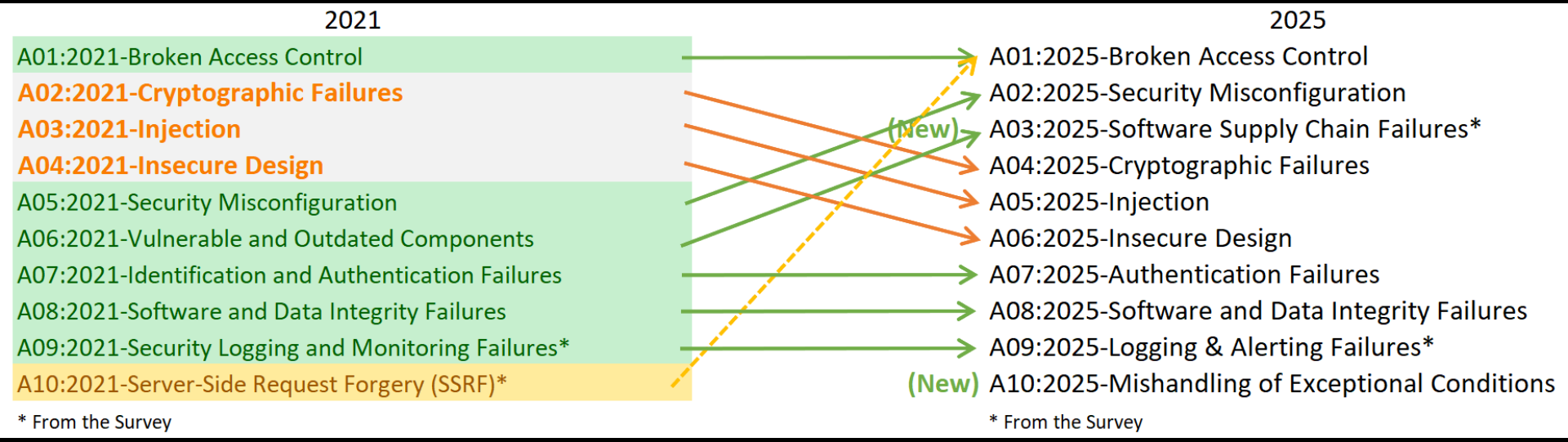
10대 웹앱 취약점 발표

웹 보안을 위한 프로젝트, 툴 제공

참고: https://cheatsheetseries.owasp.org/

OWASP

Open Worldwide Application Security Project



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

Guardian 2025

OWASP

2025

1. Broken Access Control

OWASP

2025

2. Security Misconfiguration

OWASP

2025

3. Supply Chain Failure

OWASP

2025

4. Cryptographic Failure

OWASP

2025

5. Injection

OWASP

2025

6. Insecure Design

OWASP

2025

7. Authentication Failure

OWASP

2025

8. Software Integrity Failure

OWASP

2025

9. Logging, Alerting Failure

OWASP

2025

10. Mishandling Exception

Common Vulnerabilities & Exposures

Concept

CVE: 보안 취약점을 식별하기 위한 프로젝트

CVE-년도-번호

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

미국 MITRE에서 운영

www.cve.org, cvedails.com 등에서 확인 가능하다.

Common Vulnerabilities & Exposures

Example

Redis » Redis » 8.2.1 : Security Vulnerabilities, CVEs

cpe:2.3:a:redis:redis:8.2.1:*:*:*:*:*:*:*

Published in: 2025 January February March April May June July August September October November

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2025-62507

Redis is an open source, in-memory database that persists on disk. In versions 8.2.0 and above, a user can run the XACKDEL command with multiple ID's and trigger a stack buffer overflow, which may potentially lead to remote code execution. This issue is fixed in version 8.2.3. To workaround this issue without patching the redis-server executable is to prevent users from executing XACKDEL operation. This can be done using ACL to restrict XACKDEL command.

Source: GitHub, Inc.

Max CVSS	7.7
EPSS Score	0.32%
Published	2025-11-04
Updated	2025-11-06

CVE-2025-49844

Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.

Source: GitHub, Inc.

Max CVSS	9.9
EPSS Score	5.50%
Published	2025-10-03
Updated	2025-11-12

2000.00.00

Q&A

질문이 있다면 하십시오

발표자

2.5cm-3.5cm 떨어진 제목 36px

제목 하단의 부제목 18px

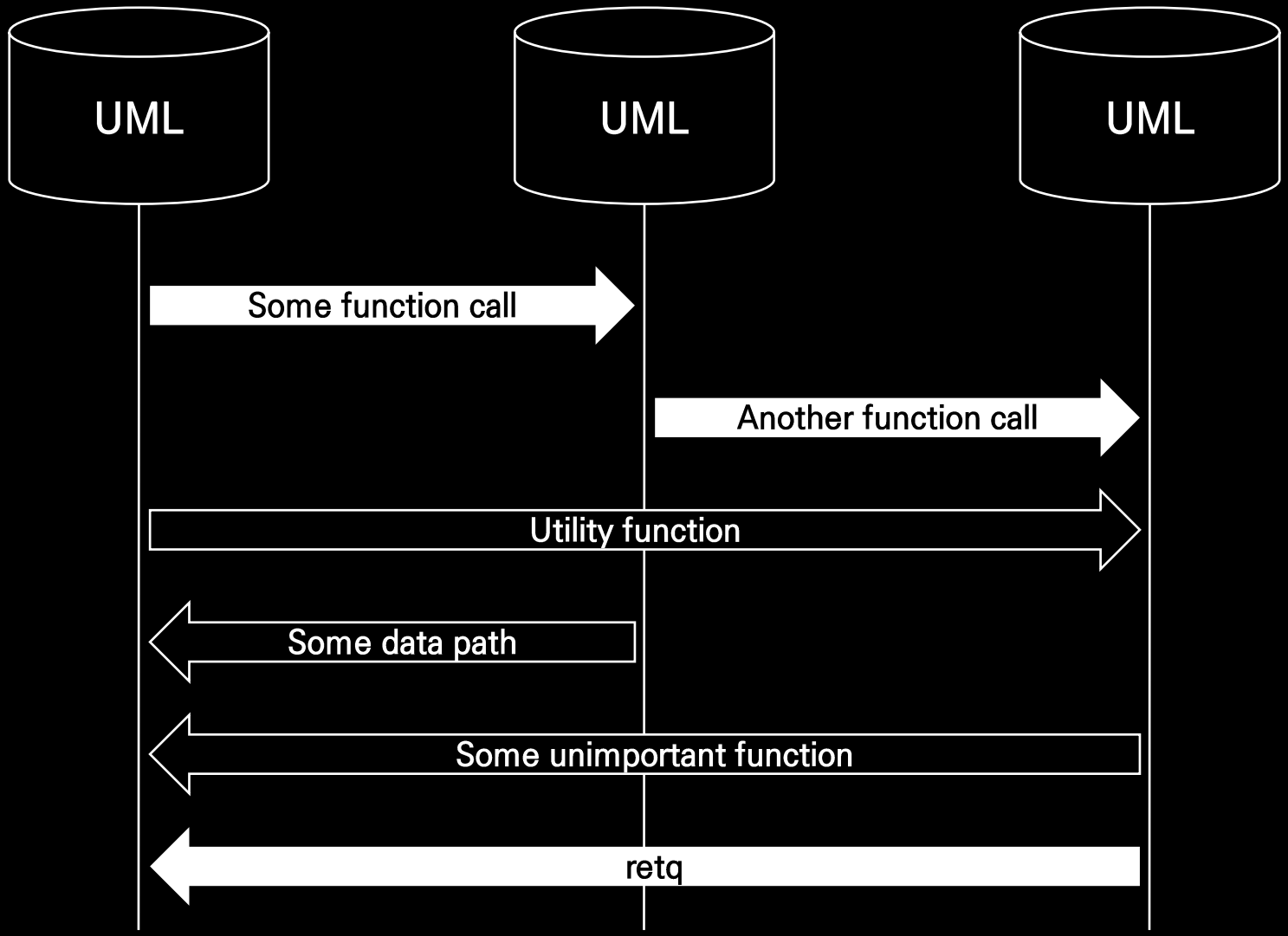
3.5cm 떨어진 내용 1 32px

```
Git init
Git status
Git add text.txt
Git add .
Git commit
Ctrl+C
Git commit -m “genesis”
Git log
Git log --oneline
```

```
Git add .
Git reset .
Git commit -m “add README”
Git log --oneline -n 3
Git commit –a –m “hello”
```

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px



Guardian 2025

Extensible Markup Language

XML

3.5cm 떨어진 내용 1 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 2 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 3 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px