woohyun212 / 박우현

박우현 입니다! 😍

- 국립창원대학교 정보보안동아리 CASPER
- KITRI Whitehat School 3기
- 적응인공지능 연구실 학부연구생
- 컴퓨터공학과 교직이수
- KVE-2025-0238 // 광주광역시교육청

안산 / 창원

github.com/woohyun212

linkedin.com/in/woohyun212

개발 # 보안 # 인공지능 # 클라우드 # 교육 # 정책 # 🎧🎵💿

목차

APPLICATION SECURITY
VERIFICATION STANDARD

01 | ASVS 가 뭐에요?


왜 필요하죠?

애플리케이션 보안의 현실

- OWASP Top 10만으로는 부족
  - 약점 유형 중심 → 예방보다는 사후 대응
  - 설계와 아키텍처 수준의 요구사항 부족

“Application Security Verification Standard”

- 애플리케이션과 서비스의 **보안 요구사항 표준**
- 안전한 설계, 개발, 유지보수, 보안 평가에 활용 가능
- OWASP에서 관리하는 **보안 통제 프레임워크**

Scope of ASVS

Application - 최종 결과물로서의 제품

- 구현되고, 개발되고, 빌드되고, 구성되어야 할 것

Security - 해결해야할 보안 문제

- 해당 요구사항이 위험의 발생 가능성, 영향도를 어떻게 줄이는지 명시

Verification - 보안 검증의 “fail or pass” 요구사항

- 애플리케이션 구성 요소 및 문서에 대한 전체 접근을 통해 검증 가능해야 함

Standard - *“달성되어야 할 보안 원칙”*

- 검증 요구사항 중심
- 테스트 가이드(“어떻게 테스트할 것인가”)가 아니며, 구현 가이드(“어떻게 구현할 것인가”)도 아님

“That is out of scope”
*- **Said no attacker ever***

“Out of scope for ASVS"
does not mean
Not important (for security)

Requirement

달성해야 할 보안 목표

- 특정 구현 방식이나 기술에 종속되지 않을 것
- 구현 방법, 검증 방법을 설명해서는 안 됨

> *"Verify that the security principle X is achieved to prevent attack Y."*

초점과 메시지

- 왜 존재하는지 스스로 설명할 수 있어야 함
- 문맥 밖에서도 이해 가능해야 함 (독립적으로 명확해야 함)

참/거짓으로 평가 가능한 요구사항

- "Verify that" == "해당 애플리케이션이 반드시 이 기능을 수행해야 한다(MUST)."
- RFC2119 용어 정의:
  - MUST = 필수(REQUIRED), 반드시(SHALL)
  - SHOULD = 권장(RECOMMENDED)
- ASVS에서는 모두 소문자 형식으로 사용됨 (must, should)

Requirement level

일반 사항

- 요구사항 수준은 지표로 받아들여야 함
- **우선순위 기반 평가**에 따라 결정됨
- 수준은 1, 2, 3
- 해당 수준부터는 해당 요구사항이 **"반드시 충족해야 할"** 항목으로 간주됨
- 그 이전 수준에서는 **권장사항** 으로 간주 가능
  - 하나의 요구사항에 여러 수준(L1, L2, L3)이 함께 명시될 수 있음

L1 – 첫 단계
L2 – 표준 보안 수준
L3 – 한 단계 더 나아간 수준

정의

- **Level 1** – 우선순위 지정의 첫 단계
  - 이 수준이 없으면 **보안이 제공될 수 없음** == 최초 방어선
- **Level 2** – 표준 보안 수준
  - 모든 애플리케이션이 **달성 목표로 삼아야 할 수준**
- **Level 3** – 고급 보안 수준
  - 한 걸음 더 나아간 **심화된 통제 수준**

02 ASVS 5.0 가 나왔어요!

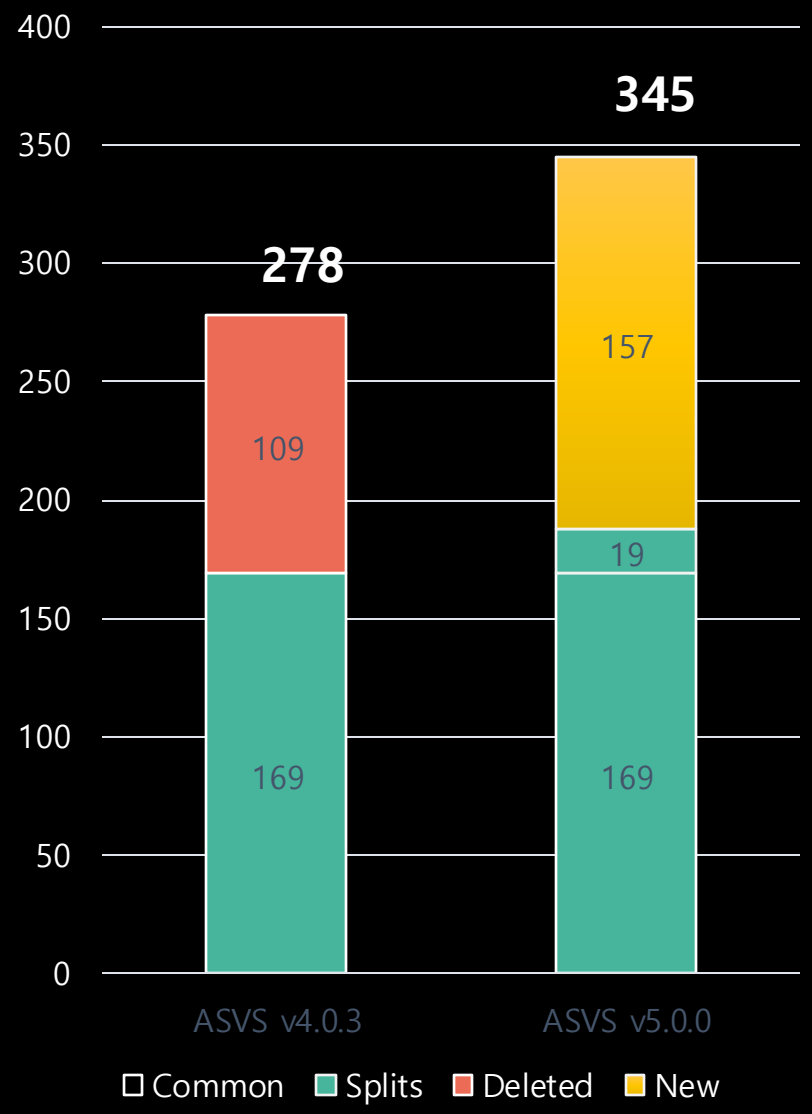
The scale of changes

In v4.0.3 - **278** 요구사항

- **109개 요구사항 (38%)** 은 v5.0.0에서 **별도 항목으로 유지되지 않음**
  - **50개**: 범위 재정의로 삭제
  - **28개**: 중복 또는 다른 항목에서 이미 다루어져 삭제
  - **31개**: 다른 요구사항에 병합

In v5.0.0 - **345** 요구사항

- **157개는 신규 요구사항**
  - v4.0에서 분할, 수정, 병합된 것이 아닌 완전히 새로운 항목
- 일부 항목은 기존 요구사항에서 분리
  - 보안 원칙, 수준, 섹션이 다른 경우
- 변경되지 않은 항목은 11개, 문법만 수정된 항목 15개
- 모든 요구사항은 새 번호 체계로 재정렬



V1 Encoding and Sanitization

요구 사항 30 개, 신규 사항 8 개

"Process input safely"

"Input Validation" moved away

섹션

- **V1.1** 인코딩 및 정제 아키텍처 (Encoding and Sanitization Architecture)
- **V1.2** 인젝션 방지 (Injection Prevention)
- **V1.3** 정제(Sanitization)
- **V1.4** 메모리, 문자열, 비관리 코드 처리 (Memory, String, and Unmanaged Code)
- **V1.5** 안전한 역직렬화 (Safe Deserialization)

V2 Validation and Business Logic

요구 사항 13 개, 신규 사항 3 개

섹션

- V2.1 검증 및 비즈니스 로직 문서화 (Validation and Business Logic Documentation)
- V2.2 입력 검증 (Input Validation)
- V2.3 비즈니스 로직 보안 (Business Logic Security)
- V2.4 자동화 공격 방지 (Anti-automation)

"Accept only valid input"
"Provide expected business logic"

Documentation requirements

"Input Validation" moved hereZ

V3 Web Frontend Security

요구 사항 31 개, 신규 사항 12 개

"Accept only valid input"
"Provide expected business logic"

Documentation requirements

"Input Validation" moved here

섹션

- **V3.1** 웹 프론트엔드 보안 문서화 (Web Frontend Security Documentation)
- **V3.2** 비의도적 콘텐츠 해석 방지 (Unintended Content Interpretation)
- **V3.3** 쿠키 설정 (Cookie Setup)
- **V3.4** 브라우저 보안 메커니즘 헤더 (Browser Security Mechanism Headers)
- **V3.5** 브라우저 출처(origin) 분리 (Browser Origin Separation)
- **V3.6** 외부 리소스 무결성 (External Resource Integrity)
- **V3.7** 기타 브라우저 보안 고려사항 (Other Browser Security Considerations)

V4 API and Web Service

요구 사항 16 개, 신규 사항 12 개

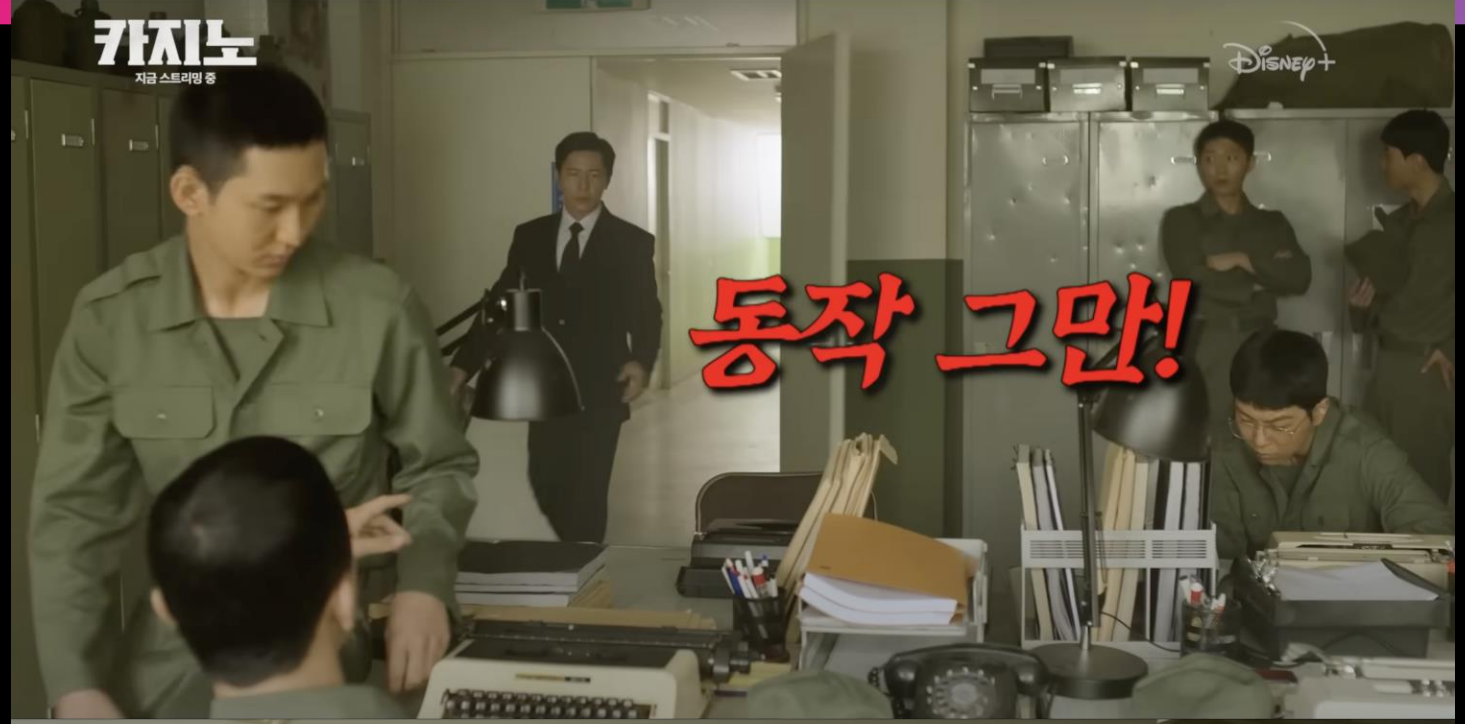
> *"General requirements for API and Web Service that are not browser-specific"*

섹션

- **V4.1** 일반 웹 서비스 보안 (Generic Web Service Security)
- **V4.2** HTTP 메시지 구조 검증 (HTTP Message Structure Validation)
- **V4.3** GraphQL
- **V4.4** WebSocket

03 | 번역해요~

요약


카지노
지금 스트리밍 중
Disney+
동작 그만!

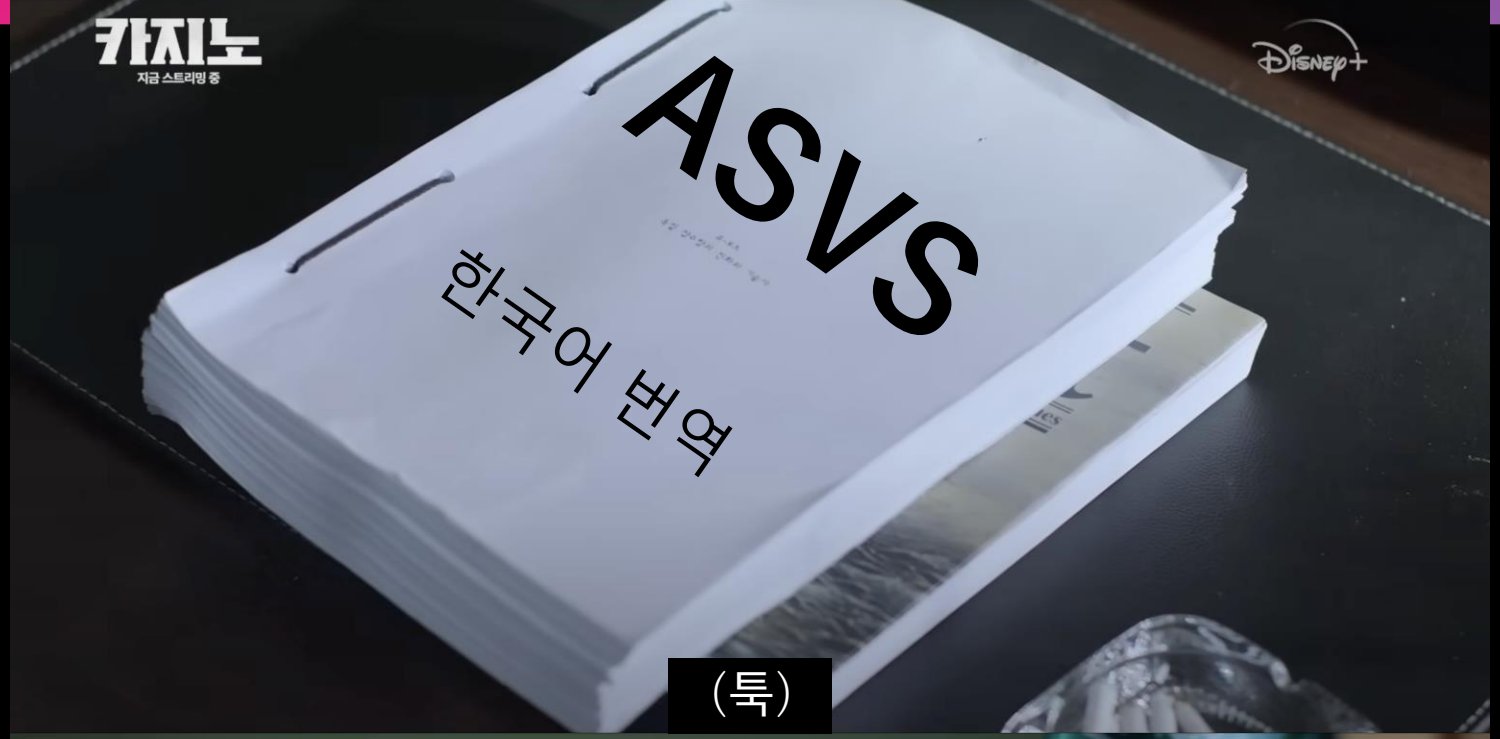

카지노
지금 스트리밍 중
Disney+
사장님 명령이다


카지노
지금 스트리밍 중
Disney+
다들 하던일을 멈추고


카지노
지금 스트리밍 중
Disney+
타자기 앞에 앉는다

- 그것은 너무 직역체 입니다. 수정해주세요.

- 마춤뻡이 틀렷읍니다.



(툭)

- 이걸 다 한거야?
- 네


카지노
지금 스트리밍 중
Disney+
- 너 혼자?


카지노
지금 스트리밍 중
Disney+
- 주변인들의 자원을 받았습니다.
무보수로 일을 하겠다고 했습니다.

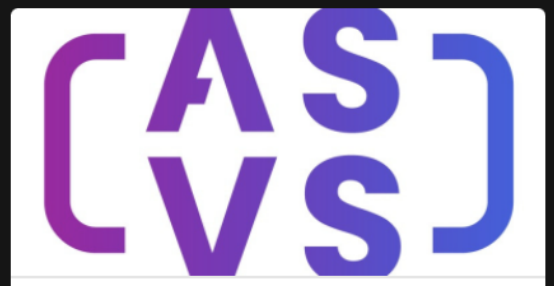
서막

김동현 (Ben)

OWASP에서 2008년부터 시작된 Application security verificaiton standard 5.0이 3주전에 런칭 되었습니다. 웹 어플리케이션에 관련한 기술적 보안 테스트를 위한 기반을 제공하고, 안전한 개발을 위한 요구사항을 제공하는 프로젝트입니다.

현재 터키어, 페르시안, 우크라이나, 포루투칼(브라질)어, 프랑스어, 중국어로 번역이 진행되고 있습니다.

관심 있으신분들은 말씀주시면 적극 지원해 드리도록 하겠습니다 :)
현재 진행중인 번역은 아래에서 확인하실 수 있습니다.
https://github.com/OWASP/ASVS/blob/master/CONTRIBUTING.md#translations



안녕하십니까
김동현 멤토님
WHS 23반 박우현 이라고합니다

OWASP Seoul chapter 에 이번 ASVS 번역에 관심이 생겨서 연락드렸습니다.

저희 동아리에서 여름 방학 프로젝트 중 하나로 진행하면 어떨까 싶어서 관련 자료 요청드릴 수 있겠습니까?

오후 12:24

김동현 (Ben)

안녕하세요. 우현님
서울챕터가 재 빌딩되고 아직 번역가이드가 완성되진 않았는데요.

오후 12:29

김동현 (Ben)

PR부터 같이 열어서 진행해보면 어떨까 싶어요.

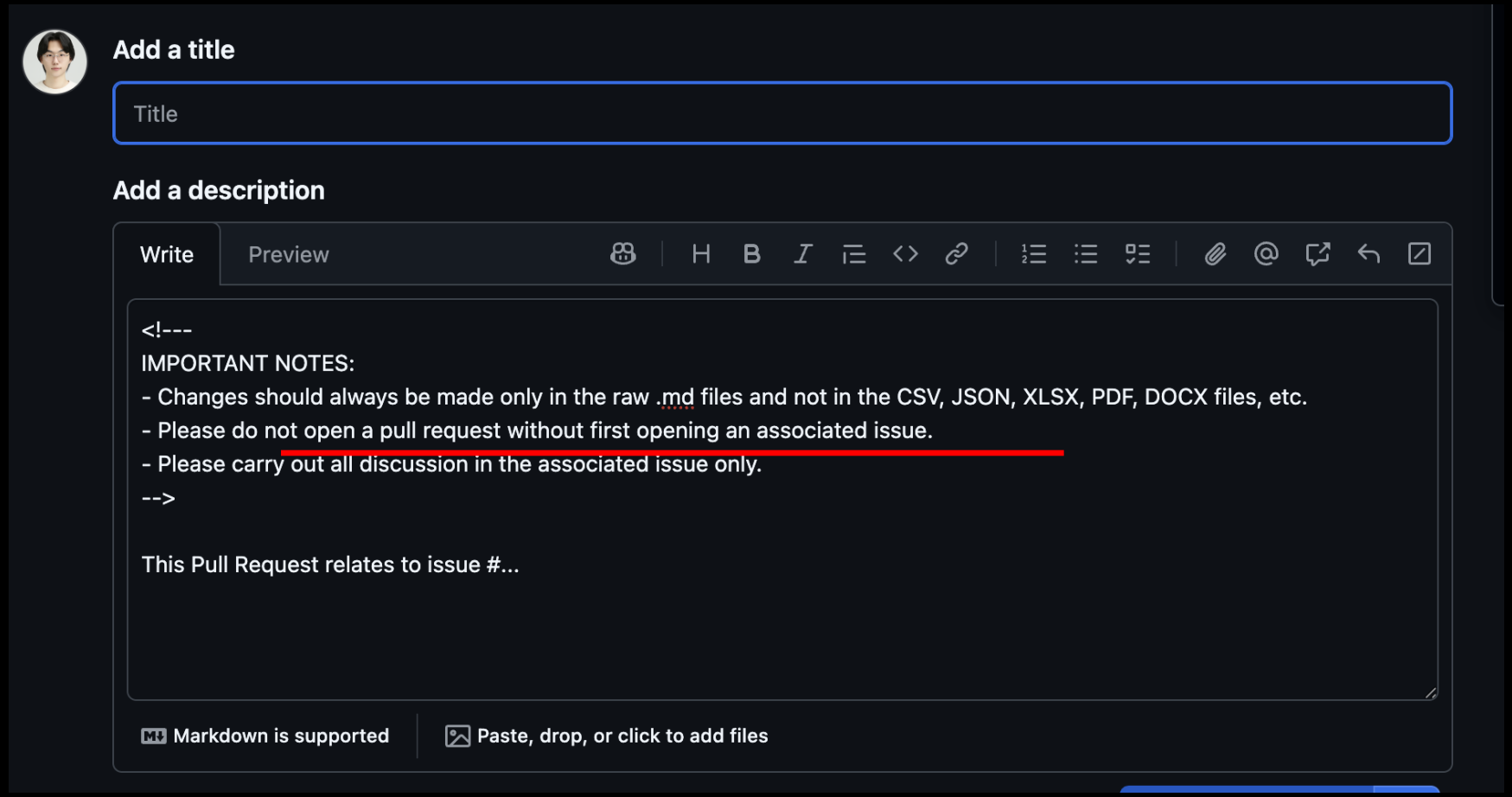
김동현 (Ben)

네, 기여하시는데 있어서 제한은 없습니다 :) 서울챕터가 뭐 하지말라/해라 하진 않아요.ㅎㅎ

대신에 언어나 문맥 통일 정도는 같이 하면 좋을 것 같아서, 저희가 구어체나 문어체 등 가이드를 만들어서 제공해드리도록 하겠습니다.

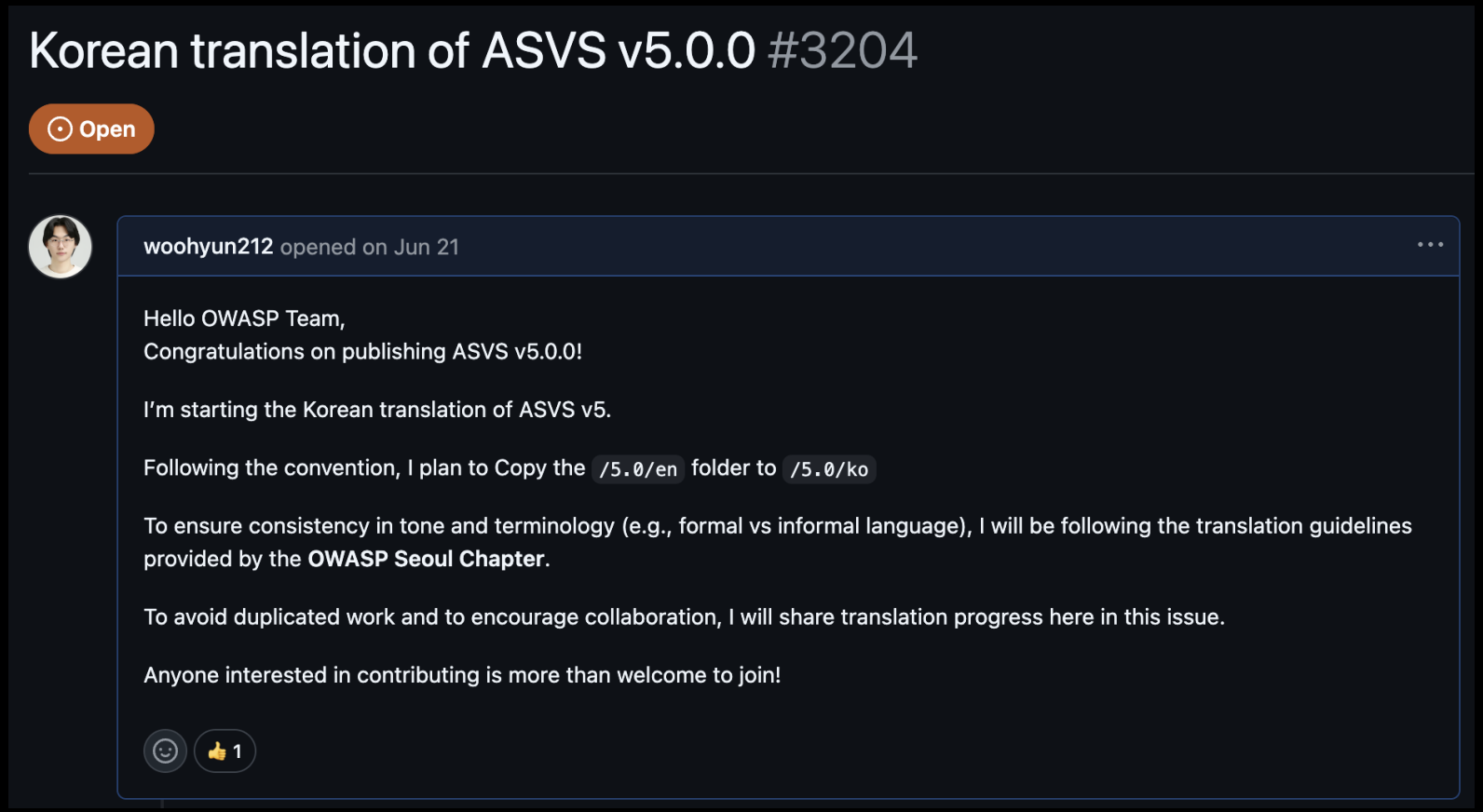
PR 부터 만들기

Issue 생성 부터



기여의 시작은 이슈

Issue 생성 부터



Korean translation of ASVS v5.0.0 #3204

Open

woohyun212 opened on Jun 21

Hello OWASP Team,
Congratulations on publishing ASVS v5.0.0!

I'm starting the Korean translation of ASVS v5.

Following the convention, I plan to Copy the `/5.0/en` folder to `/5.0/ko`

To ensure consistency in tone and terminology (e.g., formal vs informal language), I will be following the translation guidelines provided by the **OWASP Seoul Chapter**.

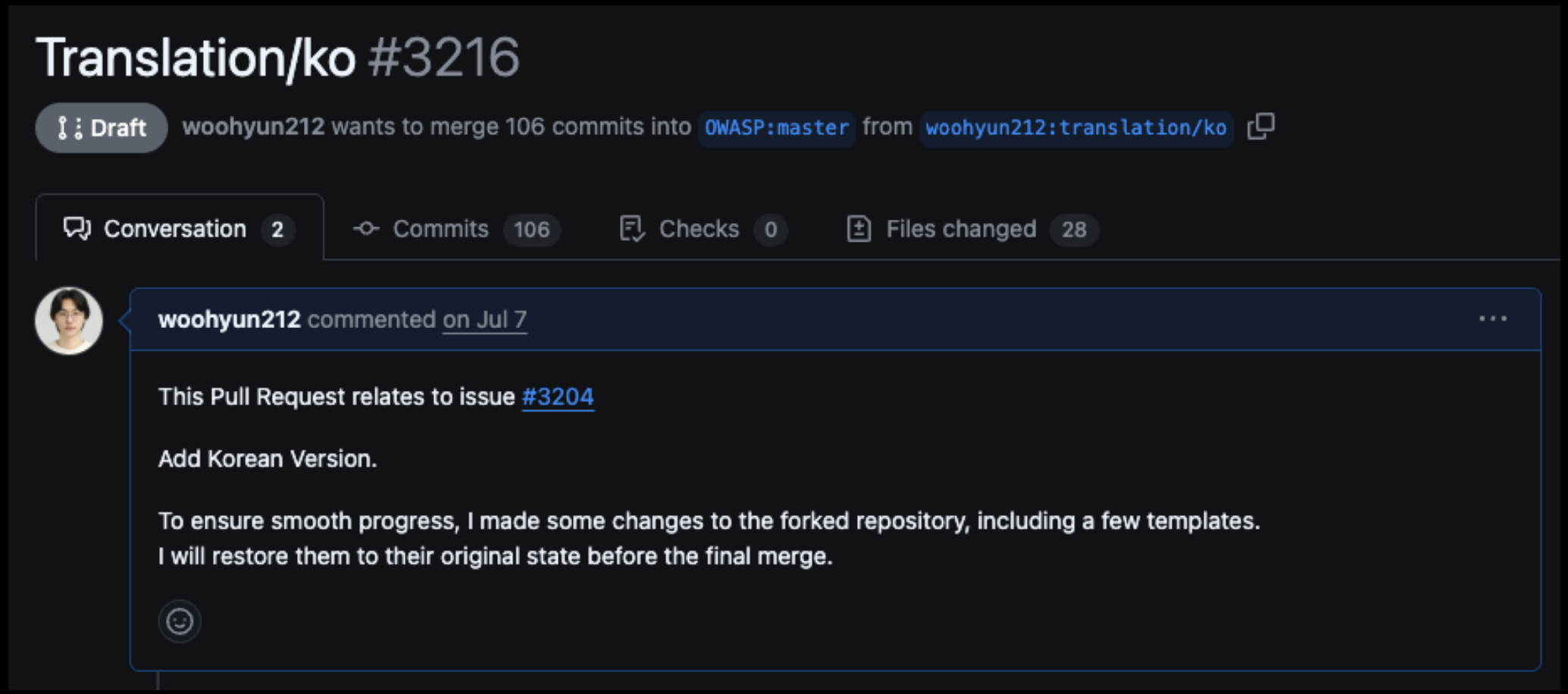
To avoid duplicated work and to encourage collaboration, I will share translation progress here in this issue.

Anyone interested in contributing is more than welcome to join!

1

부족한 영어는 GPT

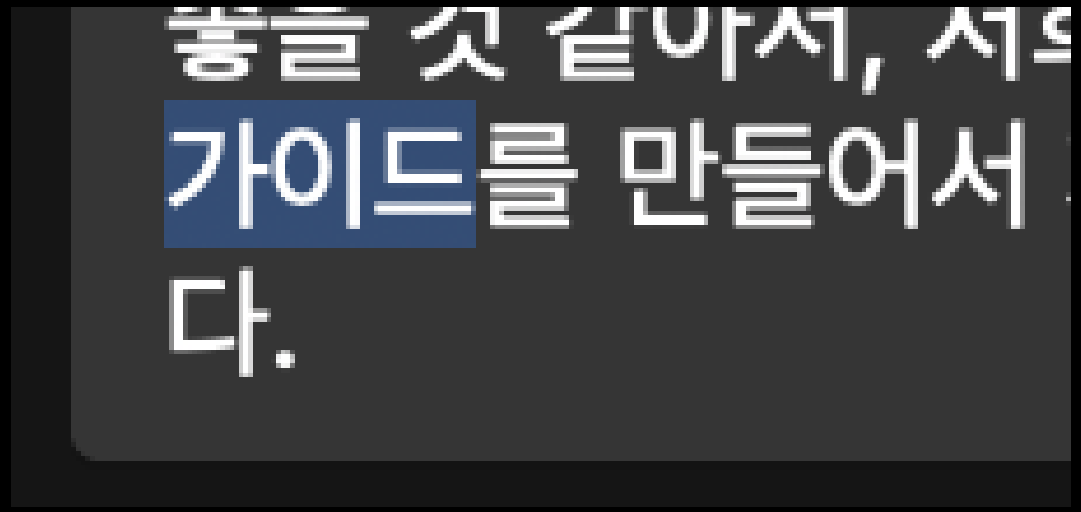
PR 등록


Translation/ko #3216
Draft
woohyun212 wants to merge 106 commits into OWASP:master from woohyun212:translation/ko
Conversation 2
Commits 106
Checks 0
Files changed 28
woohyun212 commented on Jul 7
This Pull Request relates to issue #3204
Add Korean Version.
To ensure smooth progress, I made some changes to the forked repository, including a few templates.
I will restore them to their original state before the final merge.

기여자 등록

```
112           * Portuguese, see [#3182](https://github.com/OWASP/ASVS/issues/3182)
113           * French, see [#3188](https://github.com/OWASP/ASVS/issues/3188)
114           * Simplified Chinese, see [#3191](https://github.com/OWASP/ASVS/issues/3191)
115 +         * Korean, see [#3204](https://github.com/OWASP/ASVS/issues/3204)
116       * v5.0.0
117           * None
118   * If the language you are interested in appears, it would be great if you could reach
      you can help them.
```

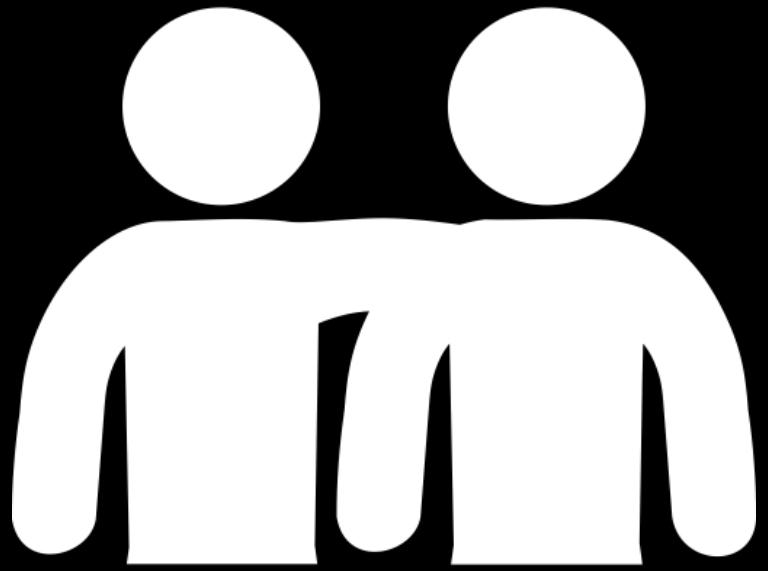
제가 기여는 처음이라…


가이드를 만들어서
다.

가이드라인이 필요하다.

너희 누님
번역해보셨잖아

그런 편이지



조언을 구하고 싶은 질문

1. 문체/문맥 관련

- 이런 기술 문서는 직역해주는 게 좋은지, 아니면 의역을 해주는 게 좋은지 궁금합니다.
- 이런 기술 문서 번역에서는 보통 어떤 톤을 사용하는 것이 자연스러울까요
(해야 한다. / 해야 합니다. 같은)?
- "해야 한다" / "권장한다" / "할 수 있다" 같은 표현에 일관성을 주기 위해 어떤 기준을 잡는 게 좋을까요?
- 번역 시, 원문의 문체를 최대한 유지하는 게 좋을까요, 아니면 한국어로 자연스럽게 풀어쓰는 게 좋을까요?
  (예를 들어, "The application must..."를 "애플리케이션은 반드시..." / "애플리케이션은 ~해야 합니다." 중 무엇으로 번역하는 것이 맞을지.?)

2. 스타일 가이드 관련

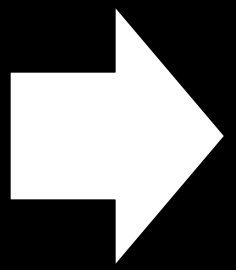
- 여러 사람이 번역할 때, 표현 통일을 위해 가장 먼저 정해야 할 기준은 무엇이 있을까요?
- 고유 명사나 전문 용어는 번역하는 게 좋을지, 원어를 유지하는 게 좋을지 판단 기준이 있을까요?
- 본인의 경험상 '번역 가이드라인'에서 반드시 포함되어야 한다고 느낀 항목이 있으신가요?

3. 리뷰/검수 관련

- 번역 검수나 리뷰 시, 어떤 구조나 프로세스를 사용하셨나요?
- 하나의 문서는 한 사람이 번역했나요? 하나의 문서를 여러 사람이 번역했나요?
  중복 작업을 허용하는 환경이었는지, 그러했다면 어떻게 병합하였는지 궁금합니다.
  (두 명 이상이 하나의 문서를 완전히 번역하여 두 가지 이상 번역본이 나온 경우)
- 검수나 리뷰 시 자주 발생하는 번역 스타일의 흔들림을 방지하려면 어떤 구조가 도움이 될까요?
- 두 사람이 동일한 문장을 다르게 번역했을 때, 어떤 기준으로 조율하면 좋을까요?
  - 그냥 개인이 선호하는 표현을 따르는 게 좋을까요?

4. 그 외

- 이런 번역 협업에서 자주 간과되는 문제나 조심해야 할 포인트가 있을까요?
- 유사한 협업 번역 경험이 있다면, 어떤 방식으로 조직화했는지 간단히 공유해주시면 감사하겠습니다.
- 마지막으로 번역 하시는 입장에서 리더가 이런 건 좀 관리해줬으면 좋겠다 싶은 부분이 있으셨나요?



조언을 구하고 싶은 질문

1. 문체/문맥 관련

- 이런 기술 문서는 직역해주는 게 좋은지, 아니면 의역을 해주는 게 좋은지 궁금합니다.
  > 기술 문서는 보통 필드에서 사용하는 용어나 표현이 굳어져있는 편이 많아, 보통 직역을 하는 편입니다. 다만, 단어 대 단어로 번역해서 번역투처럼 읽히는 것이 아니라, 업계에서 사용하는 표현으로 읽혀야 합니다. 의역하는 경우, 일반인은 이해하기 쉽지만, 업계 종사자의 입장에서는 어색하게 느껴지는 경우가 있을 수 있습니다.
- 이런 기술 문서 번역에서는 보통 어떤 톤을 사용하는 것이 자연스러울까요
(해야 한다. / 해야 합니다. 같은)?
  > 기술 문서는 보통 '-이다'체를 사용합니다.
- "해야 한다" / "권장한다" / "할 수 있다" 같은 표현에 일관성을 주기 위해 어떤 기준을 잡는 게 좋을까요?
  > 원문이 무엇이냐에 따라 다릅니다.
- 번역 시, 원문의 문체를 최대한 유지하는 게 좋을까요, 아니면 한국어로 자연스럽게 풀어쓰는 게 좋을까요?
  (예를 들어, "The application must..."를 "애플리케이션은 반드시..." / "애플리케이션은 ~해야 합니다." 중 무엇으로 번역하는 것이 맞을지.?)
  > 다국어로 번역되는 문서는 최대한 원문의 문체를 유지하는 것이 좋습니다.

2. 스타일 가이드 관련

- 여러 사람이 번역할 때, 표현 통일을 위해 가장 먼저 정해야 할 기준은 무엇이 있을까요?
  > 용어집을 작성하여 전문용어 및 고유명사를 정의해 주어야 합니다.
- 고유 명사나 전문 용어는 번역하는 게 좋을지, 원어를 유지하는 게 좋을지 판단 기준이 있을까요?
  > 국내 업계에서 통용하고 있는 표현이 있다면 그 표현을 사용하고, 없는 경우 음차한 후 원문을 병기합니다. 두문자어(acronym)의 경우에는 원문을 그대로 사용합니다. 예시) 두문자어: HTML -> HTML, SVG를 설명하는 경우 -> 처음 나왔을 때는 확장 가능한 벡터 그래픽(Scalable Vector Graphics; SVG)으로 풀어쓰고 이후에는 SVG로만 씁니다.
- 본인의 경험상 '번역 가이드라인'에서 반드시 포함되어야 한다고 느낀 항목이 있으신가요?
  > 용어집과 어체 (스타일) 가이드가 필수입니다. 작업 시작 전 합의 또는 통보해 두어야 두 번 일하지 않습니다. 가능하다면 참고 가능한 사전(Dictionary) 링크는 주는 것도 좋습니다.

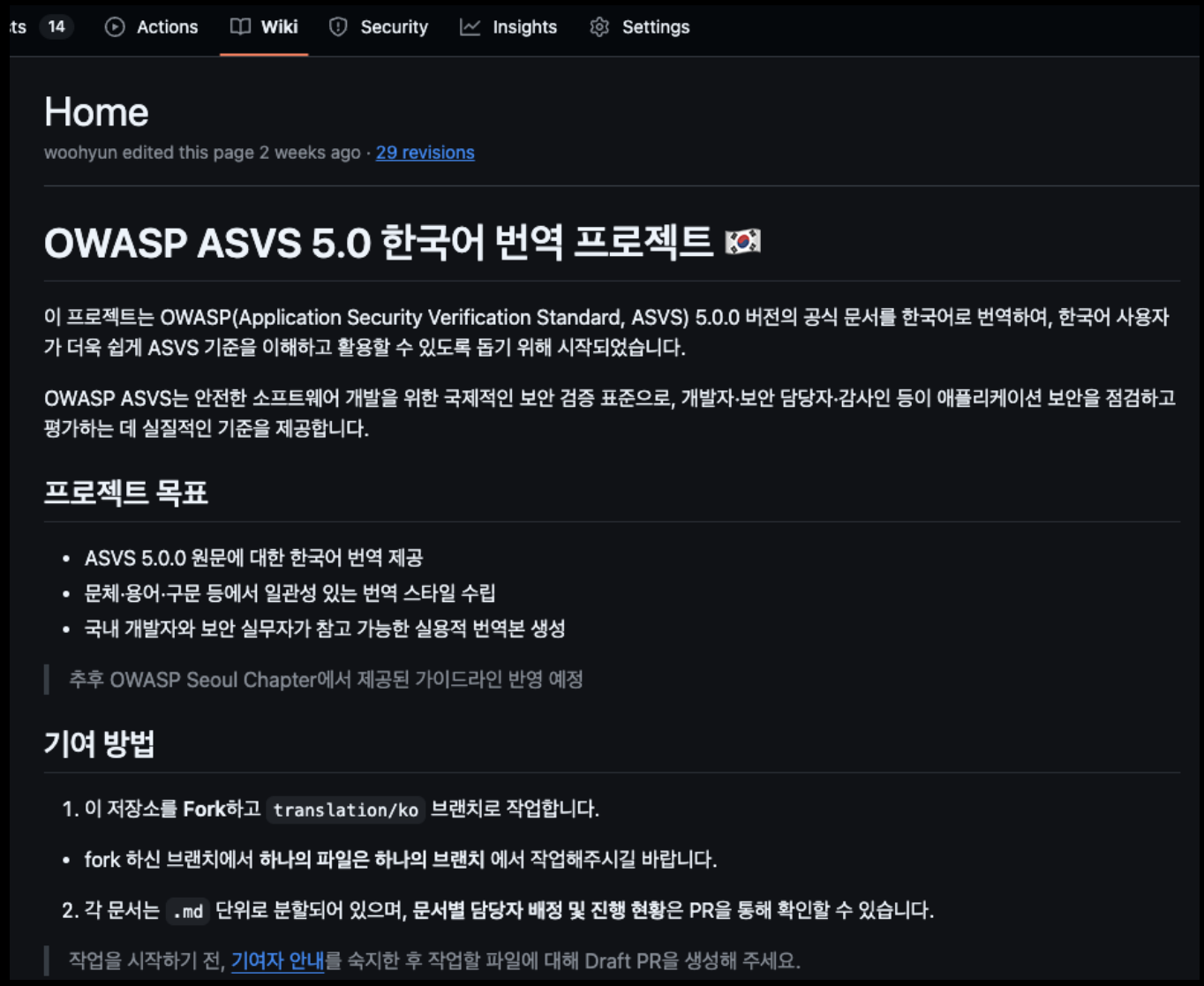
3. 리뷰/검수 관련

- 번역 검수나 리뷰 시, 어떤 구조나 프로세스를 사용하셨나요?
  > 보통 전문번역사들은 피어리뷰(동료검토) 절차를 탑니다. 서로의 작업물을 교차로 읽어보고 피드백 또는 수정하는 것인데, 이 작업은 전문성이 확보된 번역사끼리는 신뢰할 만하나, 비전문가라면 오히려 기계번역을 활용한 역번역으로 검증하는 것이 좋습니다.
  > 역번역 검증은 LLM 또는 번역 모델을 사용하여 번역문을 출발어로 번역한 뒤 자연어처리로 원문과 역번역문의 일치도를 확인합니다.
- 하나의 문서는 한 사람이 번역했나요? 하나의 문서를 여러 사람이 번역했나요?
  중복 작업을 허용하는 환경이었는지, 그러했다면 어떻게 병합하였는지 궁금합니다.
  (두 명 이상이 하나의 문서를 완전히 번역하여 두 가지 이상 번역본이 나온 경우)
  > 하나의 문서를 여러 사람이 번역하는 경우, 작업 구간이 겹치지 않게 합니다. 여러 명이 하나의 문서를 번역하는 것은 분량이 많은 문서의 작업 시간을 단축하기 위함이므로, 굳이 같은 부분을 작업할 필요가 없습니다. 병합하는 작업은 보통 한 사람이 취합합니다.
- 검수나 리뷰 시 자주 발생하는 번역 스타일의 흔들림을 방지하려면 어떤 구조가 도움이 될까요?
  > 위에서 언급한 스타일 가이드를 정해주어야 합니다.
- 두 사람이 동일한 문장을 다르게 번역했을 때, 어떤 기준으로 조율하면 좋을까요?
  - 그냥 개인이 선호하는 표현을 따르는 게 좋을까요?
  > 여러 작업자가 동일한 구간을 작업하는 경우가 없게 하는 것이 가장 좋습니다.

4. 그 외

- 이런 번역 협업에서 자주 간과되는 문제나 조심해야 할 포인트가 있을까요?
- 유사한 협업 번역 경험이 있다면, 어떤 방식으로 조직화했는지 간단히 공유해주시면 감사하겠습니다.
- 마지막으로 번역 하시는 입장에서 리더가 이런 건 좀 관리해줬으면 좋겠다 싶은 부분이 있으셨나요?
  > 저는 개인 작업을 할 때 외에는 주로 프로젝트를 관리하는 입장입니다. 관리자의 입장에서 몇 가지 이야기해보자면,
  > 1) 납기일을 준수하는 것이 가장 중요하기 때문에 주요 마일스톤마다 작업자들에게 리마인드 공지를 합니다.
  > 2) 납기일을 확인하여 1인당 하루에 처낼 수 있는 분량을 확인하고 필요 시, 인원 수를 늘립니다.
  > 3) 작업자들이 용어나 표현을 자의적으로 판단하지 않도록, 유의해야 하는 표현이나 표현을 작업자가 번역하기 어려워하는 구간은 정례회의나 구글 스프레드시트 (그 외 공유

github Wiki



Powered By

기여 방법

번역 가이드라인

용어집

기여 방법을 작성할 때 고려사항

프로젝트 목표 → 공동의 목표

github 활용 수준 → PR, branch, fork, …

작업 방식 → 최대한 상세하게

가이드라인을 작성할 때 고려사항

>>>※ 외우기 쉬워야 함 ※<<<

+ 예시가 있으면 좋다.

3. 원문 모달(MUST/SHOULD/MAY) 표현 기준

원문 표현	번역 예시
MUST / SHALL	반드시 ~해야 한다
MUST NOT / SHALL NOT	~해서는 안 된다 / ~하지 않아야 한다
SHOULD	~하는 것이 권장된다
SHOULD NOT	~하지 않는 것이 권장된다
MAY / OPTIONAL	~할 수 있다 / 선택 사항이다

※ 가능한 한 위 예시 형식을 따르는 것이 좋으나, **가독성을 해치지 않는 범위 내에서 유연하게 적용할 수 있다.**
- 예) ~ 설정되어 있는지 확인하는 것이 권장된다 -> 설정한다. / 설정되어 있는지 확인한다.

※ 필요시 괄호로 원문을 병기할 수 있다: 예) `~해야 한다 (MUST)`

6. 기술 문장 작성 예시

원문	번역 예
The application must validate input.	애플리케이션은 입력을 반드시 검증해야 한다.
Sessions should be terminated after logout.	로그아웃 이후 세션을 종료하는 것이 권장된다.
The system may store logs for up to 90 days.	시스템은 로그를 최대 90일간 저장할 수 있다.

용어집 을 작성할 때 고려사항

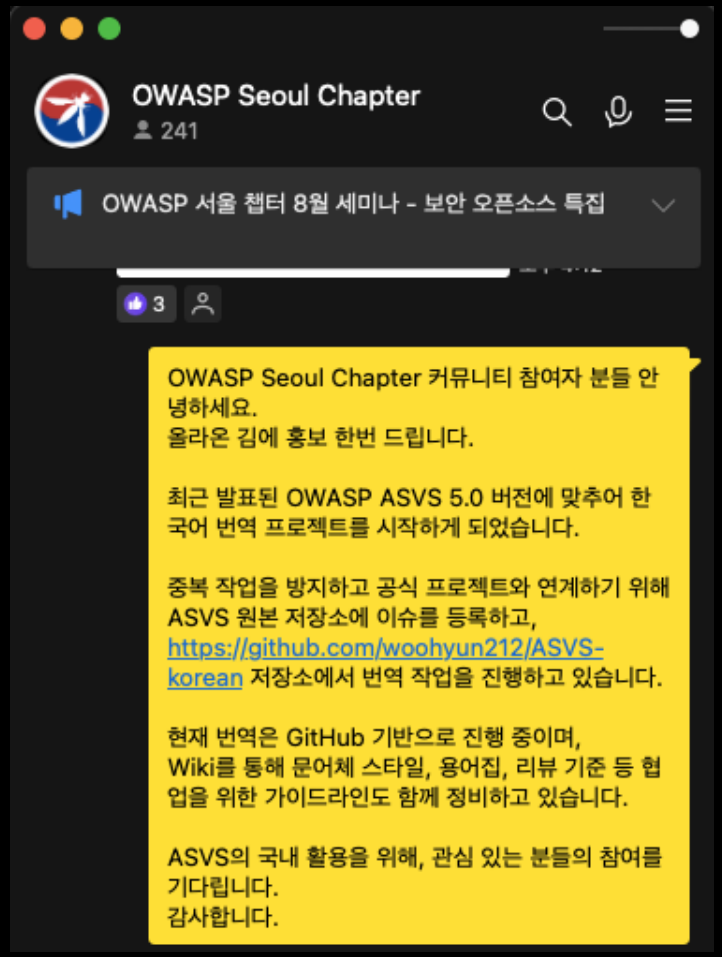
용어집

영어 원문 (EN)	한국어 번역 (KO)	약어(Acronym)	설명 / 맥락	상태	비고 / 참고
application	애플리케이션			승인	
infrastructure	인프라스트럭처	infra		승인	문서 내 번역 시, 축약형 "인프라"는 문맥상 반복이나 가독성을 위해 제한적으로 허용
query	쿼리				필요에 따라 queries / 쿼리들 복수 표기 가능
Application Security Verification Standar	애플리케이션 보안 검증 표준	ASVS			
business logic	비즈니스 로직			승인	사업 논리' 보다 비즈니스 로직 그대로 사용
parameterized	파라미터화된		Verify that the application prot		

사람이 필요하다.

(feat. 너 내 동료가 되라.)

함께 하실 분 계신가요?~


OWASP Seoul Chapter
241
OWASP 서울 챕터 8월 세미나 - 보안 오픈소스 특집
3
OWASP Seoul Chapter 커뮤니티 참여자 분들 안녕하세요.
올라온 김에 홍보 한번 드립니다.
최근 발표된 OWASP ASVS 5.0 버전에 맞추어 한국어 번역 프로젝트를 시작하게 되었습니다.
중복 작업을 방지하고 공식 프로젝트와 연계하기 위해 ASVS 원본 저장소에 이슈를 등록하고, https://github.com/woohyun212/ASVS-korean 저장소에서 번역 작업을 진행하고 있습니다.
현재 번역은 GitHub 기반으로 진행 중이며, Wiki를 통해 문어체 스타일, 용어집, 리뷰 기준 등 협업을 위한 가이드라인도 함께 정비하고 있습니다.
ASVS의 국내 활용을 위해, 관심 있는 분들의 참여를 기다립니다.
감사합니다.


놀라울 만큼,
그 누구도 관심을
주지 않았다.

OWASP

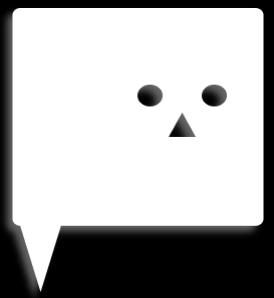
OWASP Seoul

Whitehat School

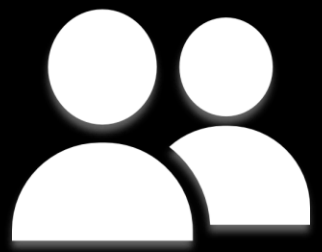
Network

CWNU

제발 해주세요



CASPER



peer

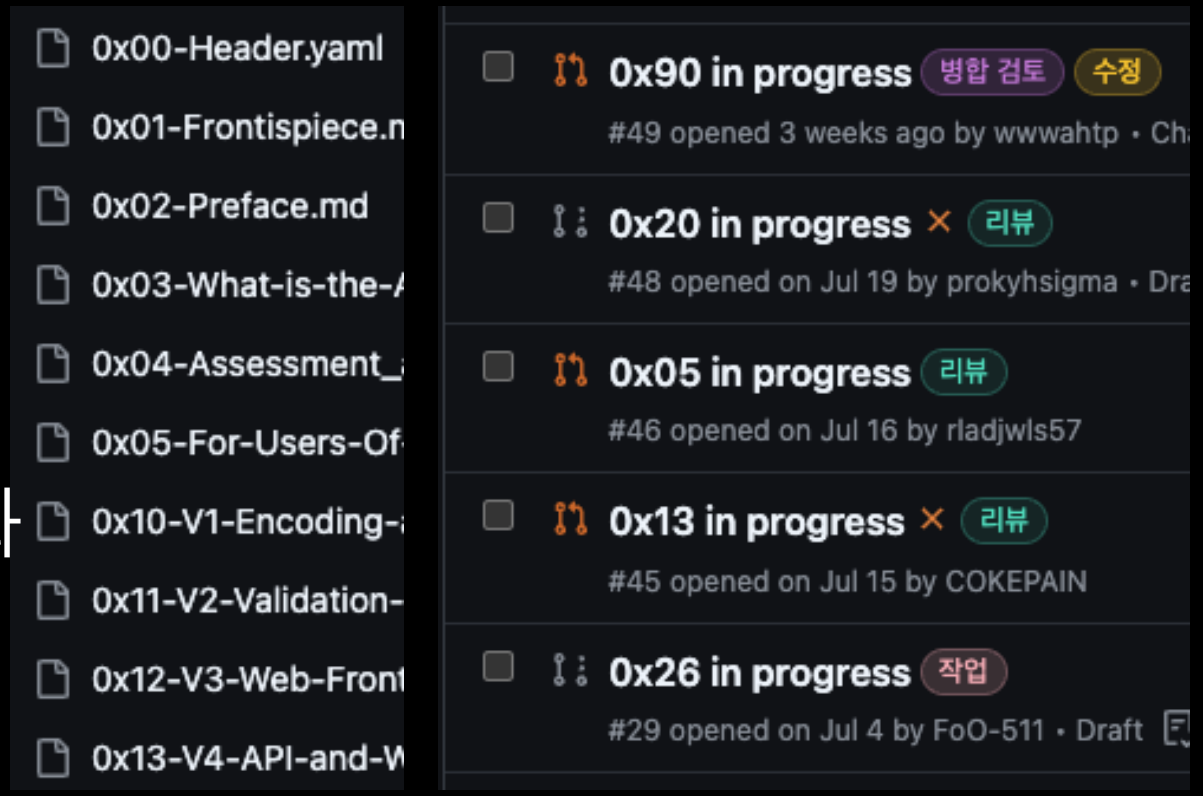
대학생 커뮤니티

생각보다 하고자하는 사람은 많다!

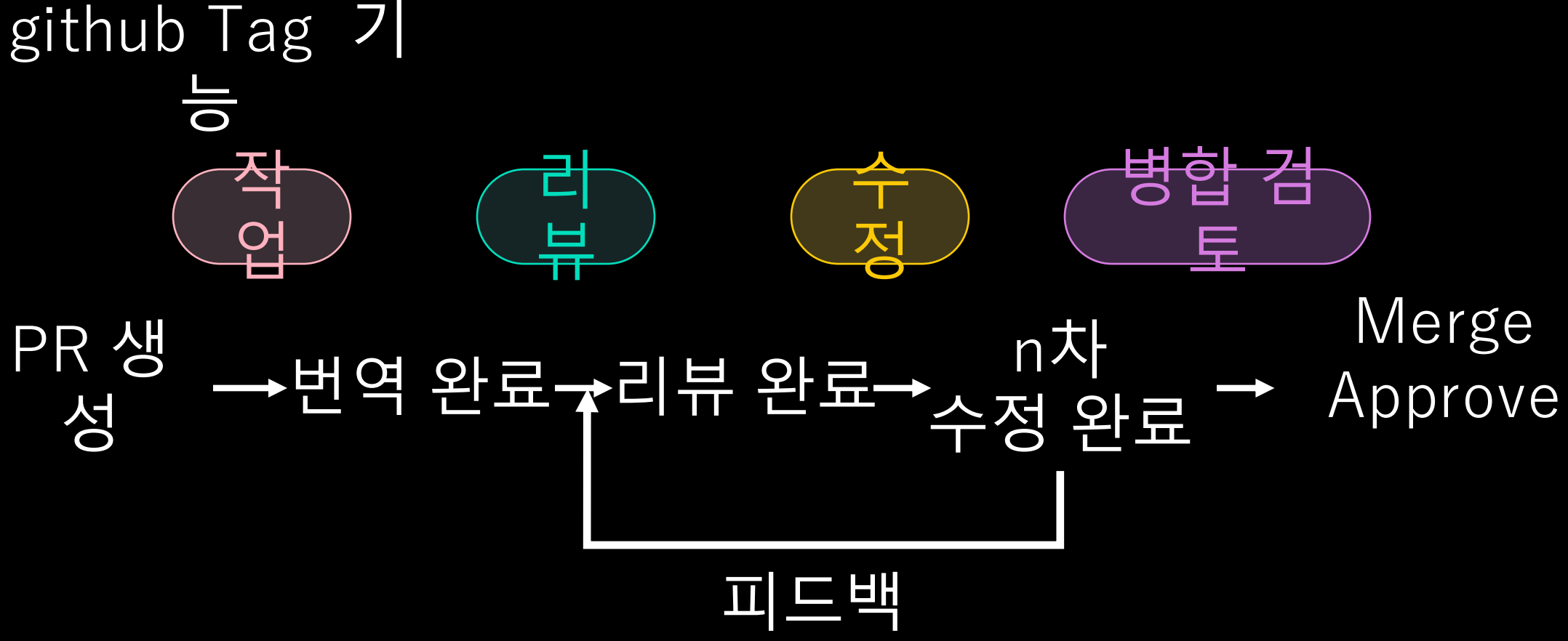
작업 방식

문서 번호를 이용한 **PR 형식** 통일

Draft PR을 이용한 작업 현황 최신화

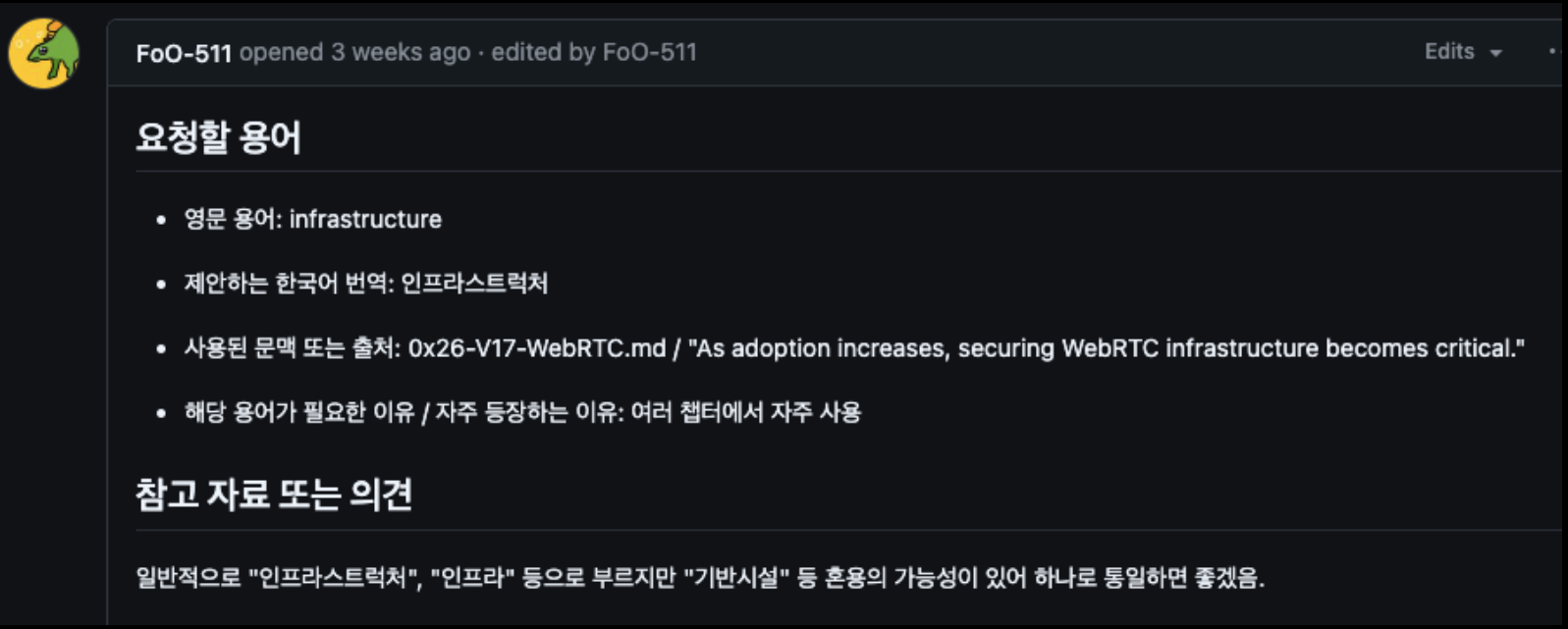


작업 과정


github Tag 기능
작업
리뷰
수정
병합 검토
PR 생성
번역 완료
리뷰 완료
n차 수정 완료
Merge Approve
피드백

용어집 등록

- [ ] [용어집] infrastructure / 인프라스트럭처
  #52 · by FoO-511 was closed 2 weeks ago
- [ ] [용어집] Sanitization / 정제
  #43 · by prokyhsigma was closed on Jul 15
- [ ] [용어집] Identity Provider / ID 공급자
  #62 · zsxen opened last week
- [ ] [용어집] memcache / 메모리 캐시
  #40 · Survey05 opened on Jul 8



FoO-511 opened 3 weeks ago · edited by FoO-511 Edits

요청할 용어

- 영문 용어: infrastructure
- 제안하는 한국어 번역: 인프라스트럭처
- 사용된 문맥 또는 출처: 0x26-V17-WebRTC.md / "As adoption increases, securing WebRTC infrastructure becomes critical."
- 해당 용어가 필요한 이유 / 자주 등장하는 이유: 여러 챕터에서 자주 사용

참고 자료 또는 의견

일반적으로 "인프라스트럭처", "인프라" 등으로 부르지만 "기반시설" 등 혼용의 가능성이 있어 하나로 통일하면 좋겠음.

github Template 기능

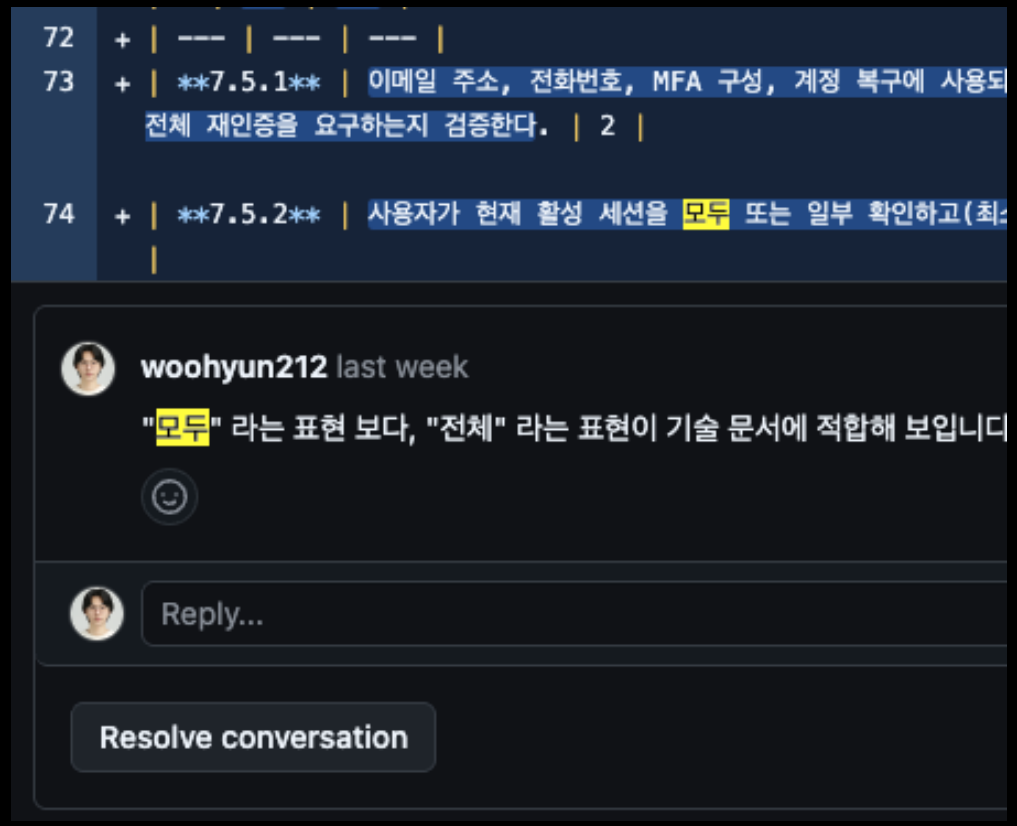
Add a description

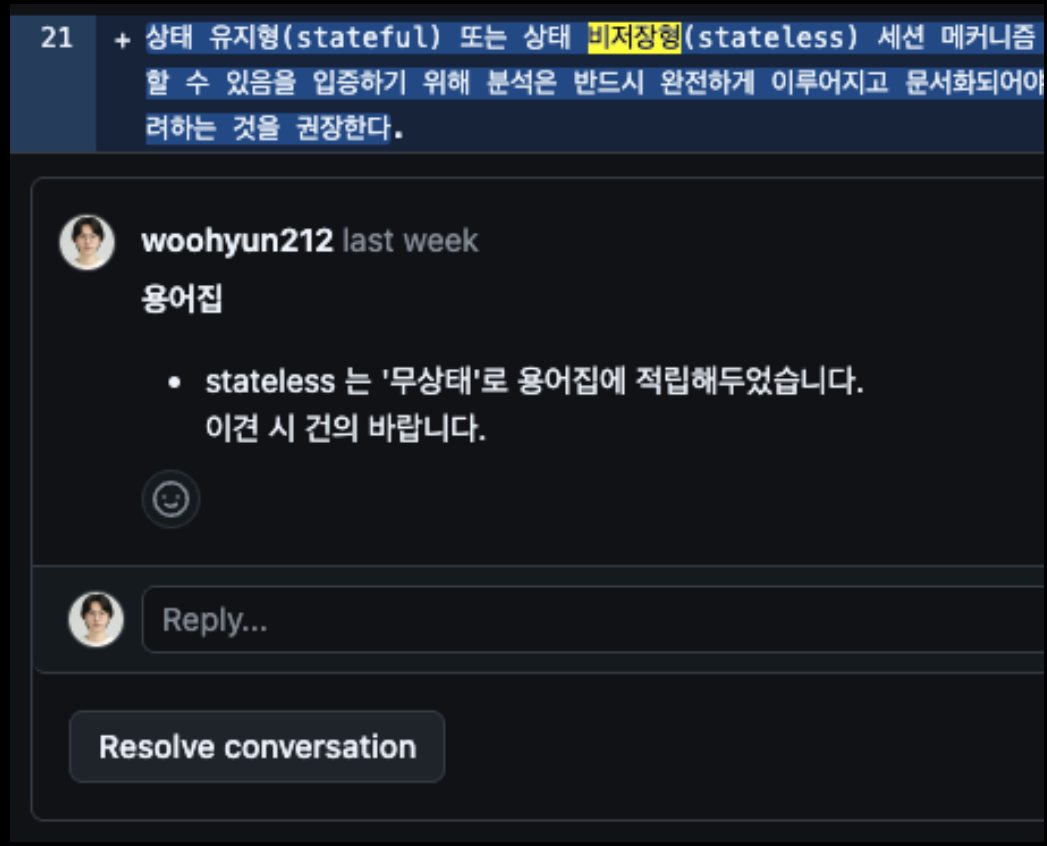
Write | Preview

```
<!--
이슈를 올리기전에 확인해주세요:
- 유사한 요청이 이미 논의된 적이 있는지 이슈(issues)를 먼저 검색해 주세요.
- [최신 버전](https://github.com/OWASP/ASVS/tree/master/5.0)을 참고하고 있는지 확인해 주세요.
- 이슈 제목은 요청할 용어의 `영문 용어/제안 번역` 으로 입력해주세요.
- 이슈 승인되면 용어집 스프레드시트에 반영 됩니다.
-->
## 요청할 용어

- 영문 용어:
  <!--(예: credential)-->

- 제안하는 한국어 번역:
  <!--(예: 자격 증명)-->

- 사용된 문맥 또는 출처:
  <!--(예: 0x03-Authentication.md / "The user must provide valid credentials.")-->

- 해당 용어가 필요한 이유 / 자주 등장하는 이유:
  <!--(예: 여러 챕터에서 반복 사용되며 다양한 번역이 혼용되고 있음)-->

## 참고 자료 또는 의견

<!-- - (예: 국내 보안 커뮤니티에서 일반적으로 '자격 정보' 또는 '자격 증명'이라는 표현을 사용함)-->
<!-- - (예: OWASP 번역 사례 중 AppSensor, Top 10 등에서는 credential → 자격 증명으로 통일됨)-->
```

리뷰 방식

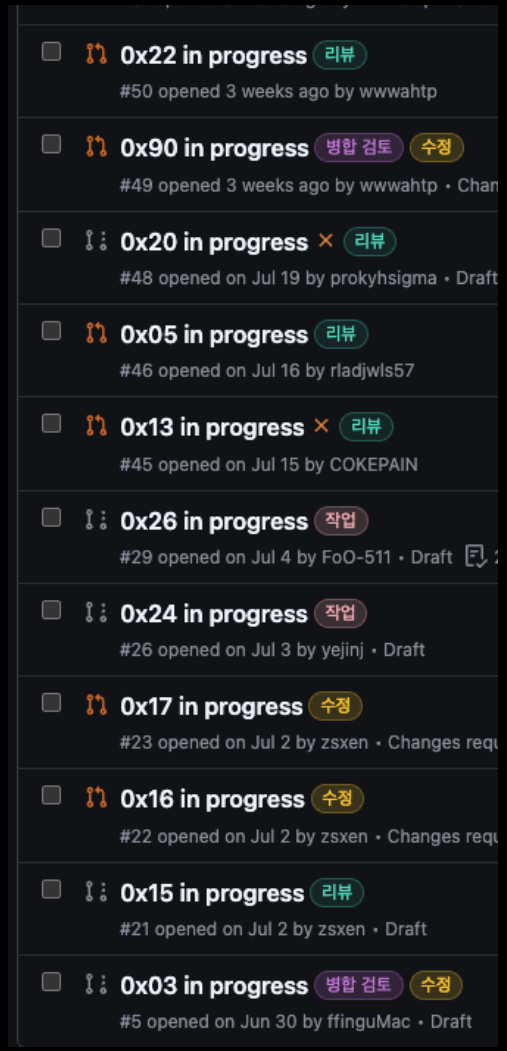
github Files changed 기능





나 혼자만 리뷰어

번역은 여럿이 리뷰는 혼자?



문서당 적게는 60줄 많게는 200줄 가까이

모든 문서를 가이드라인, 용어집과 비교하며
2,3 번씩 보고 리뷰하기엔 소요가 너무 큼

diff 를 이용한 번역 리뷰 자동화

PR에는 파일의 변경 사항을 구조화한 diff를 볼 수 있음

```
diff --git a/5.0/ko/0x93-Appendix-D_Recommendations.md b/5.0/ko/0x93-Appendix-D_Recommendations.
index 496dd5ba61..d6e51250b9 100644
--- a/5.0/ko/0x93-Appendix-D_Recommendations.md
+++ b/5.0/ko/0x93-Appendix-D_Recommendations.md
@@ -1,47 +1,47 @@
-# Appendix D: Recommendations
+# 부록 D: 권장 사항

-## Introduction
+## 소개

-Whilst preparing version 5.0 of the Application Security Verification Standard (ASVS), it becam
because they were not in scope for ASVS as per the definition for 5.0 or alternatively it was fe
+애플리케이션 보안 검증 표준(Application Security Verification Standard; ASVS) 버전 5.0을 준비하면서, 몇 가지
수 사항으로 지정하기에는 어려움이 있기 때문이다.

-Not wanting to lose all these items entirely, some have been captured in this appendix.
+해당 항목들이 누락되지 않도록 일부 항목을 본 부록에 수록하였다.

-## Recommended, in-scope mechanisms
+## 권장되는 범위 내 매커니즘

-The following items are in-scope for ASVS. They should not be made mandatory but it is strongly
+다음 항목들은 ASVS의 범위 내에 있으며, 필수적이지는 않으나 안전한 애플리케이션의 일부로서 고려하는 것이 강력하게 권장된다.

-* A password strength meter should provided to help users set a stronger password.
-* Create a publicly available security.txt file at the root or .well-known directory of the app
-* Client-side input validation should be enforced in addition to validation at a trusted servic
-* Prevent accidentally accessible and sensitive pages from appearing in search engines using a
-* When using GraphQL, implement authorization logic at the business logic layer instead of the
+* 사용자들이 더 강력한 비밀번호를 설정할 수 있도록 패스워드 스트렝스 미터(password strength meter)를 제공하는 것이 권
+* 애플리케이션의 루트 또는 .well-known 디렉터리에 공개적으로 접근 가능한 security.txt 파일을 생성하여, 보안 문제에 관
+* 신뢰할 수 있는 서비스 계층에서의 검증과 함께 클라이언츠 측에서의 입력값 검증을 강제하는 것이 권장된다. 이는 누군가가 애플리
+* robots.txt 파일, X-Robots-Tag 응답 헤더 또는 robots html meta tag를 사용하여 우연히 접근될 수 있는 민감한 페
+* GraphPL을 사용하는 경우, 모든 개별 인터페이스마다의 권한 부여를 관리하지 않아도 않도록 GraphQL이나 리졸버 계층이 아닌
```

→ 원문과 번역문이 줄 단위로 매칭

diff 를 이용한 번역 리뷰 자동화

diff 가이드라인

- ✅ 중복 표현
- ✅ 너무 긴 문장(가독성)
- ✅ 오탈자

❗ [오타] “검검증하는” → “검증하는”

diff 복사

```
+요구사항이 누락되면 애플리케이션의 보안 수준이 저하되며, 요구사항을 구현하면 보안 위험의 발생 가능성 또는
```

💬 [긍정적] 원문의 `likelihood or impact`를 적절히 “발생 가능성 또는 영향”으로 번역한 점 좋습니다.

diff 복사

```
+요구사항은 구현이나 기술에 너무 구애받지 않으면서도 존재하는 이유를 자명하게 설명하면서...
```

진행 사항 관리

- 0x25 in progress 수정
  #51 opened 3 weeks ago by wwwahtp • Changes requested
- 0x22 in progress 리뷰
  #50 opened 3 weeks ago by wwwahtp
- 0x90 in progress 병합 검토 수정
  #49 opened 3 weeks ago by wwwahtp • Changes requested
- 0x20 in progress ✕ 리뷰
  #48 opened on Jul 19 by prokyhsigma • Draft
- 0x05 in progress 리뷰
  #46 opened on Jul 16 by rladjwls57
- 0x13 in progress ✕ 리뷰
  #45 opened on Jul 15 by COKEPAIN
- 0x26 in progress 작업
  #29 opened on Jul 4 by FoO-511 • Draft 2 tasks

Progress

	subject_id	assignee	state
1	0x00-Header.yaml	woohyun212	Done
2	0x01-Frontispiece.md	breakpack	Done
3	0x02-Preface.md	typemnm	Done
4	0x03-What-is-the-ASVS.md	ffinguMacc	Merge R...
5	0x04-Assessment_and_Certification.md	kimchiudon	Done
6	0x05-For-Users-Of-4.0.md	rladjwls577	Review
7	0x10-V1-Encoding-and-Sanitization.md	survey05	Done
8	0x11-V2-Validation-and-Business-Logic.md	COKEPAIN	Done
9	0x12-V3-Web-Frontend-Security.md	typemnm	Done
10	0x13-V4-API-and-Web-Service.md	COKEPAIN	Review

Total Progess

작업 파일 정렬 및 작업자, 진행 사항 대시보드

데드라인의 필요성

오픈 소스 형식

참여자	관리자
장점	단점
자율성	자율성
다양한 기여자들	다양한 기여자들

Name	Github ID	Email
박우현(Park WooHyun)	woohyun212	woohyun212@gmail.com
김용환(Kim YongHwan)	prokyhsigma	prokyhsigma@naver.com
조예진(Jo YeJin)	yejinj	sitting077@gmail.com
이본영(Lee BonYeong)	FoO-511	5thofnovmbr@gmail.com
박재욱(Park JaeWook)	ffinguMacc	parkjaewook228@gmail.com
박준범(Park JunBeom)	blatter95	gomwer678@gmail.com
차원제(Cha WonJe)	breakpack	198799879a@gmail.com
신승민(Shin SeungMin)	COKEPAIN	tlstmdals05@gmail.com
이준서(Lee JunSeo)	typemnm	ljunseo1334@gmail.com
박민균(Park MinGyun)	survey05	ismingyun01@gmail.com
윤현정(Youn HyunJung)	kimchiudon	yoon45544@gmail.com
이지훈(Lee JiHun)	effortjh1112	kchimney1112@gmail.com
김어진(Kim EoJin)	rladjwls57	marijohn57@naver.com
오모세(O Moses)	wwwahtp	wwwmoses@g.skku.edu
정수진(Jeong SooJin)	zsxen	useaf7ernoon@gmail.com
이하린(Lee HaRin)	sari-harin	1303sari@gmail.com
양 진(Yang Jin)	yjiiny	yjiiny01@gmail.com
정민석(Jung MinSuk)	j93es	j93es.jung@gmail.com

+ 홍성진
+ 김동현
+ 이다혜

결론

- ASVS 는 단순한 문서가 아니라, 실무 보안의 기준점
- 문서를 번역하는 것이 아니라, 도메인 지식으로 문맥과 의도를 해석하는 작업이었다.
- 생각 이상으로 대학생 커뮤니티는 아주 활발함.
- 프로젝트 규모가 커지니 가이드라인, 용어집, GitHub 이슈와 PR 관리 등 체계적인 협업 구조 없이는
  불가능하다고 느꼈음.
- 오픈소스 협업과 자율성은 강점이지만, 그만큼 관리자의 지속적인 관찰과 피드백이 필요하다.

감사합니다!