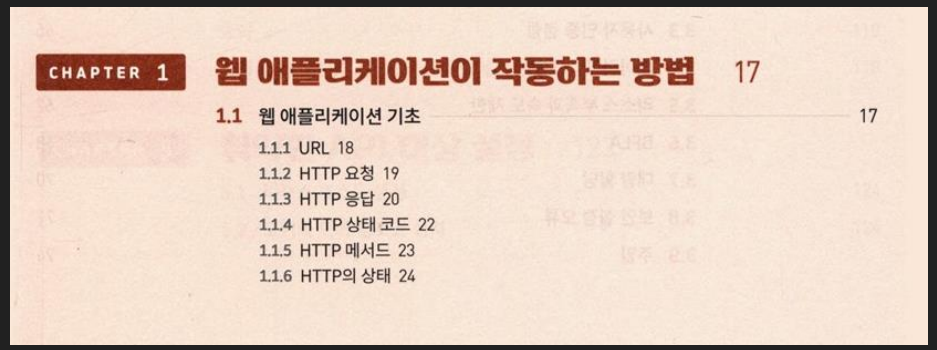
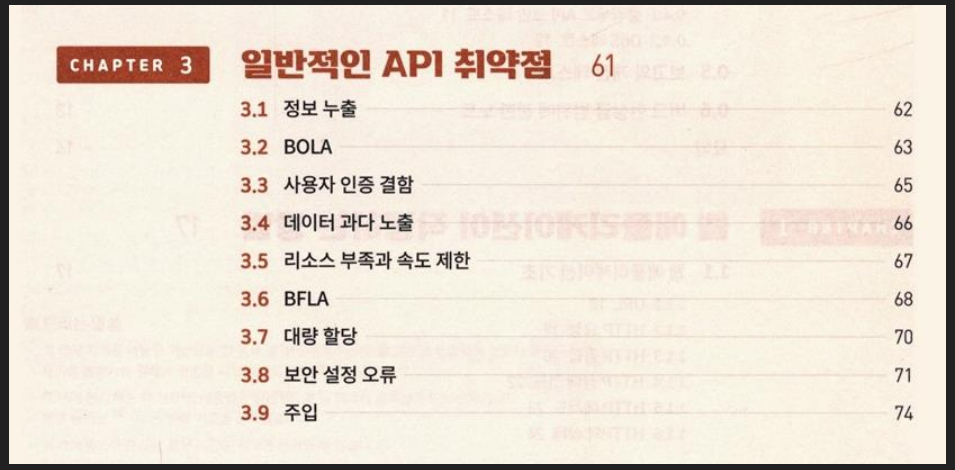
BlackCat 스터디 – Injection

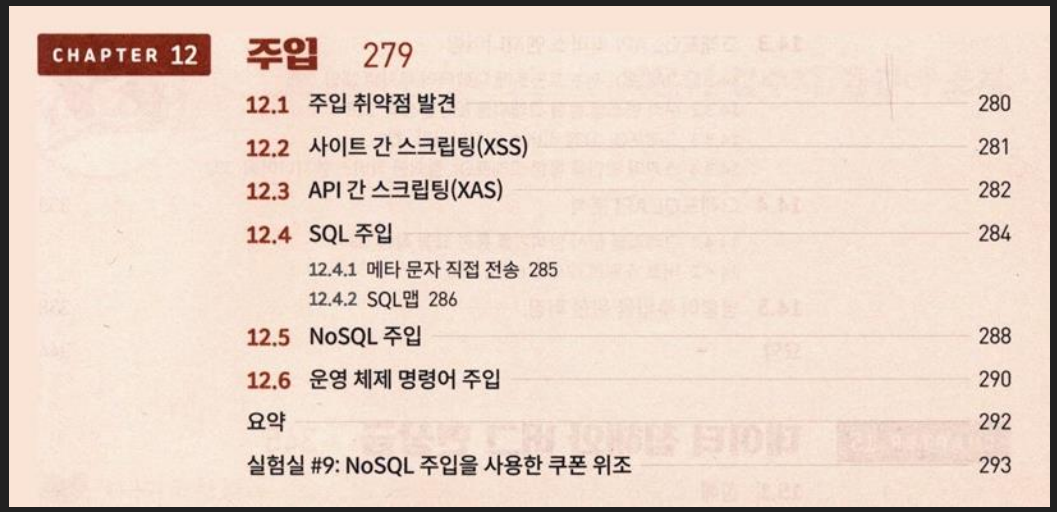
공부 순서



CHAPTER 1 웹 애플리케이션이 작동하는 방법 17



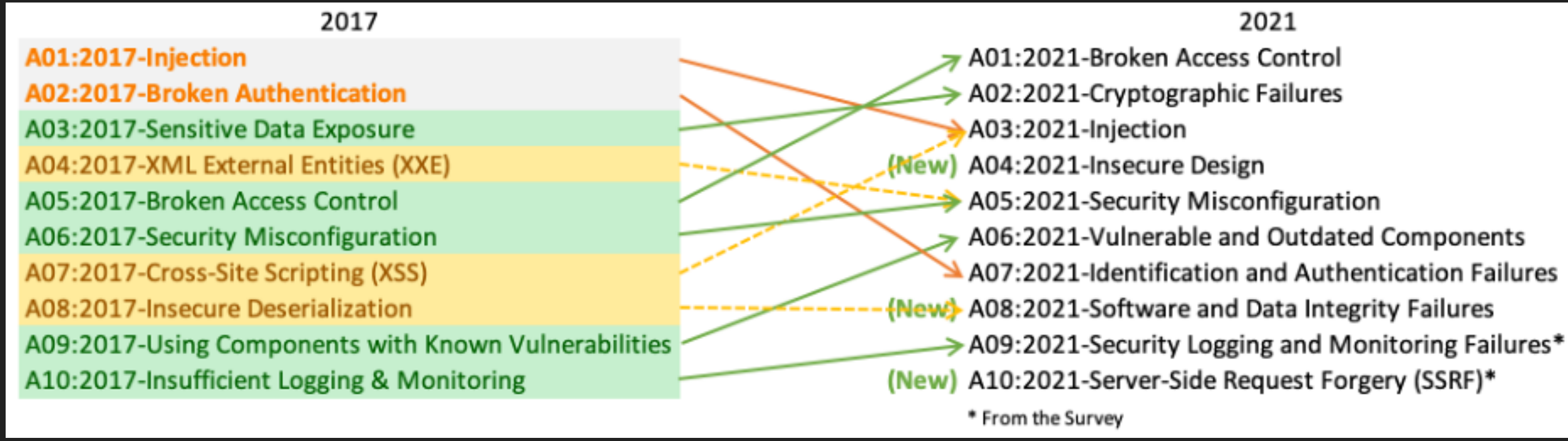
CHAPTER 3 일반적인 API 취약점 61



CHAPTER 12 주입 279

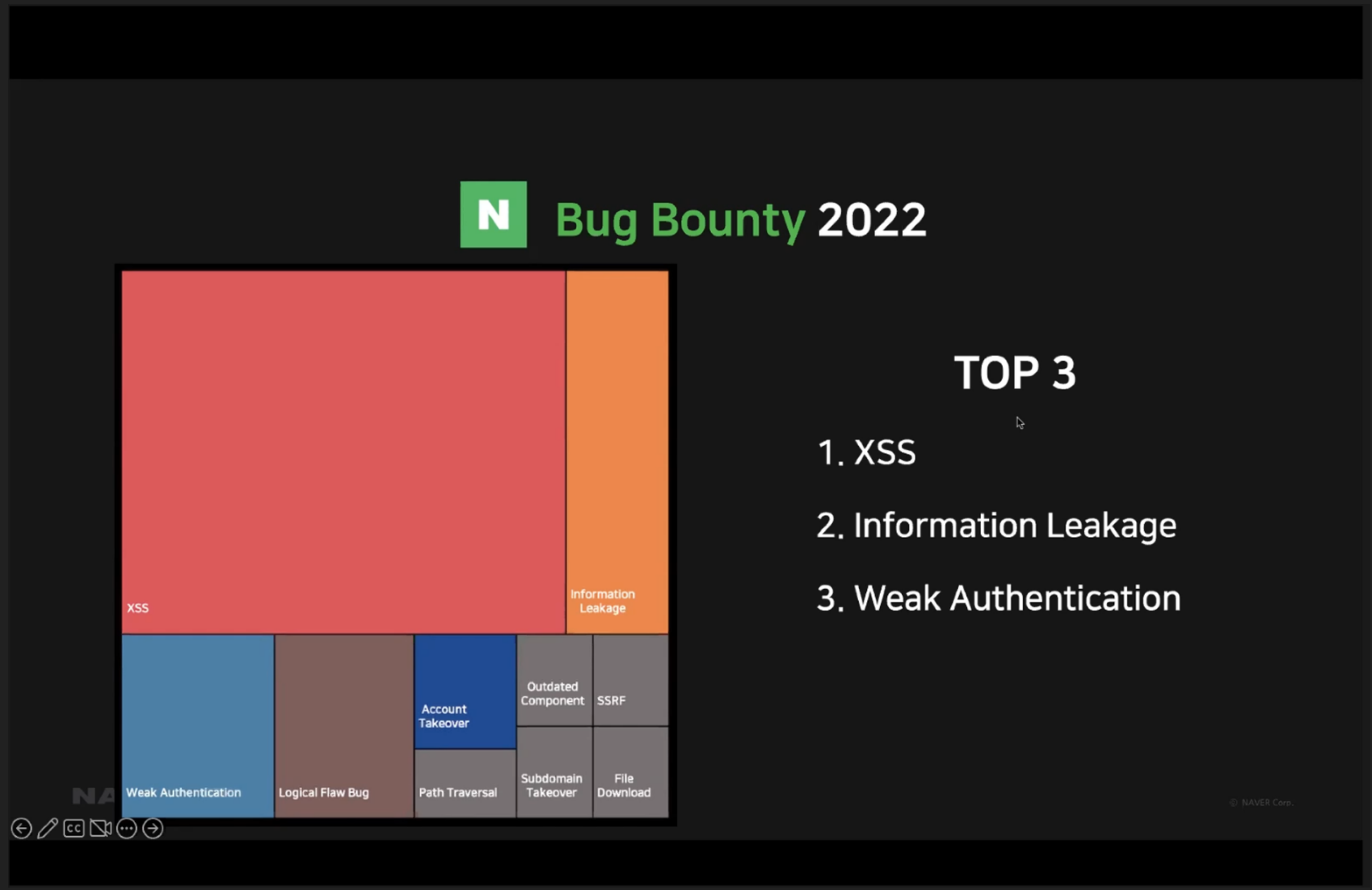
책 챕터대로..

OWASP Top 10



- 1위 : 권한 제어 (ex. 관리자 전용 기능을 일반사용자도 사용가능)
- 2위 : 데이터 노출 (ex. 개인정보 노출 등)
- 4위 : 로직상 문제

In real bug bounty…



Javascript

- HTML 내에서 <script> 태그로 사용 가능
- HTML 내 버튼 element에 event handler로 등록 가능
- <script> 태그를 이용해 외부 스크립트 또한 첨부 가능
- 클릭, 웹페이지 요청, 스크롤, 등등 웬만한 모든 행동이 자바스크립트로 구현 가능
- 인터프리터 방식처럼 동작함 <-> 컴파일 방식

XSS (Cross-Site Scripting)

- 공격자가 스크립트를 심어 피해자가 웹사이트에서 원치않는 행동을 하는 것

- 쿠키 및 각종 스토리지 또한 스크립트를 통해 가져올 수 있으므로 위험함

Stored XSS

- 공격자가 타겟 웹사이트에 스크립트를 심는것
- 글쓰기 본문, 제목, 댓글 등 입력 가능하고 타인이 볼 수 있는 모든 곳이 타겟이 될 수 있음
- 해당 게시글을 본 사람들은 쿠키 탈취 -> 다른 사용자의 세션을 따 해당 사용자처럼 행동 가능

Reflected XSS

- 웹사이트 URL(주로 GET)을 대상으로 하는 XSS 공격
- 공격자가 URL 파라미터에 script를 심어, 해당 URL을 클릭하는 피해자가 공격자가 원하는 행동을 하도록 함
- 검색창 등에서 Reflected XSS 공격 가능

CSRF (Cross site request forgery)

- XSS 가 가능한 상황에서, 피해자가 서버에 이상한 요청을 하도록 스크립트를 실행하는것

- Ex. 해당 사용자가 모르게 (스크립트를 통해) 글 수정, 비밀번호 변경, 상품 구매, 등등등..

- <-> SSRF (Server-Side request forgery)

방어 방법

- 간단한 방어 방법은 모든 입력에 대해서 스크립트가 주입되었는지를 확인하는 것
- 단순히 문자열 검사로는 우회할 수 있는 경우가 너무 많아 주로 라이브러리를 이용함
- 최근 프레임워크(React, Angular, Vue 등) 에는 xss filter가 자동으로 되어 있음
- 국내에서는 네이버에서 개발한 lucy xss filter 등 존재

방어 방법 - 2

- CSRF의 경우 CSRF Token을 이용해 방어
  - CSRF Token : 클라이언트에 제공되는 비밀 값

XSS Game

- http://www.xssgame.com/
- XSS 공부하는 사이트!
- 회원가입 필요 없음!

- URL 인코딩
- https://www.urlencoder.org/
- 참고
- https://www.w3schools.com/js/js_events_examples.asp

In CTF...

- https://dreamhack.io/wargame/challenges/28
- https://tools.dreamhack.games/requestbin/
- location.href = …
- document.cookie

과제

- https://dreamhack.io/wargame/challenges/26/
- Webhacking.kr 23번
- 최대한 문제 분석해보기!!

추가 문제들

- (Advanced)
- https://dreamhack.io/wargame/challenges/268/
- https://dreamhack.io/wargame/challenges/269