Web 취약점

1. OWASP Top 10

- OWASP(The Open Web Application Security Project)
- 웹 애플리케이션 보안에 대한 정보를 공유하고 체계를 세우는 자발적인 온라인 정보 공유 사이트
- 국제 웹보안 분야 비영리기구
- 2001년 12월 마크 커페이와 데니스 그로브스 등에 의해 탄생
- 2004년 ‘OWASP Top 10’이라는 웹 애플리케이션상의 10대 주요 취약점 발표
  - 웹 애플리케이션을 중심으로 공격 빈도가 가장 많은 상위 10가지 항목을 3년 단위로 업데이트
- 우리나라는 2011년 1월 OWASP Korea Chapter 이사회가 조직되어 활동 전개

http://www.owasp.org

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

OWASP Top 10 – 2017	OWASP Top 10 – 2021
A1 – Injection	A1 – Broken Access Control
A2 – Broken Authentication	A2 – Cryptographic Failures
A3 – Sensitive Data Exposure	A3 – Injection
A4 – XML External Entities (XXE)	A4 – Insecure Design
A5 – Broken Access Control	A5 – Security Misconfiguration
A6 – Security Misconfiguration	A6 – Vulnerable and Outdated Components
A7 – Cross-Site Scripting (XSS)	A7 – Identification and Authentication Failures
A8 – Insecure Deserialization	A8 – Software and Data Integrity Failures
A9 – Using Components with Known Vulnerabilities	A9 – Security Logging and Monitoring Failures
A10 – Insufficient Logging & Monitoring	A10 – Server-Side Request Forgery

OWASP Top 10

A01 : Broken Access Control (접근 제어 취약점)

- 접근제어는 사용자가 권한을 벗어나 행동할 수 없도록 정책을 시행
- 접근 제어가 취약하면 사용자는 주어진 권한을 벗어나 모든 데이터를 무단으로 열람, 수정 혹은 삭제 등의 행위로 수행

A02 : Cryptographic Failures (암호화 오류)

- Sensitive Data Exposure의 명칭이 2021년 Cryptographic Failures(암호화 오류)로 변경
- 적절한 암호화가 이루어지지 않으면 민감 데이터가 노출될 수 있음

A03: Injection (인젝션)

- 신뢰할 수 없는 데이터가 명령어나 쿼리문의 일부분으로써 인터프리터로 보내질 때 취약점이 발생

A04: Insecure Design (안전하지 않은 설계)

- 누락되거나 비효율적인 제어 설계로 나타나는 취약점

OWASP Top 10

A05: Security Misconfiguration (보안설정오류)

- 불필요한 기능이 활성화 되거나 설치되었을 때, 기본계정 및 암호화가 변경되지 않았을 때, 지나치게 상세한 오류 메세지를 노출할 때, 최신 보안기능이 비활성화 되거나 안전하지 않게 구성되었을 때 발생

A06: Vulnerable and Outdated Components (취약하고 오래된 요소)

- 지원이 종료되었거나 오래된 버전을 사용할 때 발생
- 애플리케이션 뿐만 아니라, DBMS, API 및 모든 구성요소 들이 포함

A07: Identification and Authentication Failures (식별 및 인증 오류)

- Broken Authentication로 알려졌던 해당 취약점은 identification failures(식별 실패)까지 포함하여 더 넓은 범위를 포함할 수 있도록 변경
- 사용자의 신원확인, 인증 및 세션관리가 적절히 되지 않을 때 취약점이 발생할 수 있음

OWASP Top 10

A08: Software and Data Integrity Failures(소프트웨어 및 데이터 무결성 오류, 2021)

–무결성을 확인하지 않고 소프트웨어 업데이트, 중요 데이터 및 CI/CD 파이프라인과 관련된 가정을 하는데 중점을 둠

A09: Security Logging and Monitoring Failures (보안 로깅 및 모니터링 실패)

- Insufficient Logging & Monitoring의 명칭변경
- 해당 카테고리는 진행중인 공격을 감지 및 대응하는데 도움이 됨

A10: Server-Side Request Forgery (서버 측 요청 위조, 2021)

- 웹 애플리케이션이 사용자가 제공한 URL의 유효성을 검사하지 않고 원격 리소스를 가져올 때마다 발생
- 이를 통해 공격자는 방화벽, VPN 또는 다른 유형의 네트워크 ACL(액세스 제어 목록)에 의해 보호되는 경우에도 응용 프로그램이 조작된 요청을 예기치 않은 대상으로 보내도록 강제할 수음

2. 주요 Web 공격

- 구글해킹(google hacking)
- Injection
- XSS (Cross-Site Scripting)
- CSRF(Cross Site Request Forgery)
- Identification and Authentication Failures
- Security Misconfiguration (보안설정오류)
- Broken Access Control (접근 제어 취약점)
- Cryptographic Failures (암호화 오류)
- Drive By Download(DBD)

구글해킹(Google Hacking)

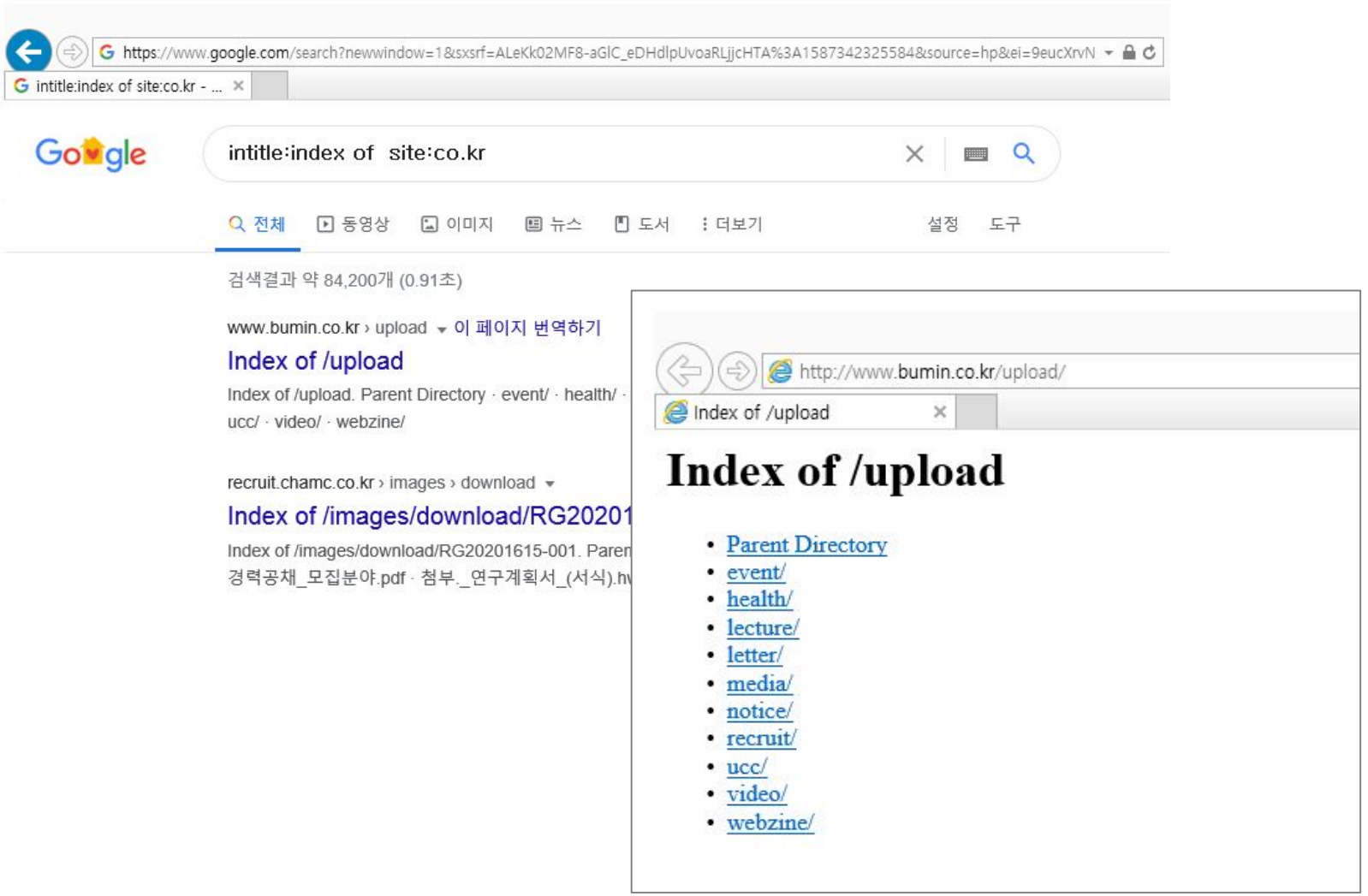
- FootPriting ：공격 대상의 정보 취득
  - IT 기술을 기반
  - IT 기술 없이도 가능한 공격 기법 (사회공학적 기법)
- 검색 서비스를 이용하여 서비스를 해킹하는 기술
- 검색 연산자를 이용하여 Hacking

❶ 주요 검색 인자


intitle
구글해킹 - Google 검색 - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
site
inurl
주소(D) http://www.google.co.kr/search?complete=1/google.ppt
Google 구글해킹 실행 즐겨찾기 PageRank 팝업 허용
filetype
ZDNet Korea,..구글을 통한 해킹 기법, googledork
물론 그 반대의 경우도 가능하다. 해킹과 보안은 그야말로 양날의 칼과 같다. 무엇이 옳다 그르다의 관점보다는 누가
::: 구글을 통한 해킹 기법, googledork (2.67MB, PDF) ...
www.zdnet.co.kr/microsite/aspiri 19,00.htm - 70k - 저장된 페이지 - 유사한 페이지
numrange
ZDNet Korea,..해킹 툴로 전락한 구글, 보안 개선 「안간힘」
웹사이트에서 정보를 찾아내는 구글의 능력에 의존해 보안 전문가들과 공격자들은 똑같이 구글의 사이트 검색
다. 구글 해킹으로 알려진 이러한 활동은 구글의 특정 결함에 대한 사인이나 민감한 정보에 ...
www.zdnet.co.kr/news/internet/0,39031 ,00.htm - 89k - 저장된 페이지 - 유사한 페이지
intext
해커스랩 프리해킹존에 오신걸 환영합니다.
[mud님 日] 오레일리의 구글해킹 책 살 돈이 없어서 속상하던 참에 눈이 번쩍 뜨이는 사이트를 발견했습니다. 구글
쉽게 할 수 있는 방법들을 모아놓은 것 같습니다. 구글 검색 팁에 관한 다른 사이트도 ...

- intitle:index of site:co.kr
- intitle:admin site:co.kr
- intitle:admin|관리자 site:co.kr
- 대외비 filetype:ppt site:co.kr
- 대외비 filetype:doc site.co.kr

intitle:index of site:co.kr



- filetype `site:wishfree.com admin`

  예) ‘wishfree.com’ 도메인이 있는 페이지에서 ‘admin’ 문자열 찾기

- filetype `filetype:txt password`

  – 특정 파일 유형을 검색할 때 사용.

  예) 파일 확장자가 txt이고 문자열 password가 들어간 파일 검색하기

- intitle `intitle:index.of admin`

  – 디렉터리 리스팅 취약점이 존재하는 사이트를 찾을 수 있어 정보 수집 시 유용.

  예) 수많은 사이트의 디렉터리 리스팅 확인하기

❷ robots.txt 검색 엔진의 검색을 피하는 방법

- 웹 서버의 홈 디렉터리에 'robots.txt' 파일을 만들어 크롤링을 제한
  - User-agent: robots.txt 에서 지정하는 크롤링 규칙이 적용되어야 할 크롤러를 지정
  - Allow: 크롤링을 허용할 경로 (/ 부터의 상대 경로)
  - Disallow: 크롤링을 제한할 경로(/ 부터의 상대 경로)

```
User-agent: googlebot                  // 구글 검색 엔진의 검색을 막는다.
User-agent: *                          // 모든 검색 로봇의 검색을 막는다.
Disallow: dbconn.ini                   // dbconn.ini 파일을 검색하지 못하게 한다.
Disallow: /admin/                      // admin 디렉터리에 접근하지 못하게 한다.
```

- 크롤러들은 robots.txt 에서 액세스가 허용되지 않은 디렉토리를 발견한다면 원칙적으로는 크롤링하지 않음

```
# 대상: 네이버 크롤러 (Naverbot) & Google 크롤러 (GoogleBot)
# 제한 디렉토리 1: /not-for-find-1/ 이하
# 제한 디렉토리 2: /not-for-find-2/ 이하
# 제한 디렉토리 3: /not-for-find-3/ 이하

# 대상: 다음 크롤러 (Daum)
# 제한 디렉토리 1: /not-for-daum-1/ 이하
# 제한 디렉토리 2: /not-for-daum-2/ 이하

User-agent: Yeti
User-agent: GoogleBot
Disallow: /not-for-find-1/
Disallow: /not-for-find-2/
Disallow: /not-for-find-3/

User-agent: Daum
Disallow: /not-for-daum1/
Disallow: /not-for-daum2/
```

- ·Robots.txt의 내용을 따를지 말지를 결정하는 것은 웹로봇에 달려 있음
  - 합법적인 로봇은 robots.txt 내용을 준수하여 수집을 진행하지만 악의적으로 제작된 로봇은 내용을 무시하고 정보수집
  - Disallowed 로 차단 내용을 정보 수집에 오히려 활용
  - robots.txt를 통해 오히려 중요한 경로가 노출 될 수 있음을 주의해야 함