잠깐!

아직 음소거 하지 말아주세요!

여러분은 도메인 주소에 대해 얼마나 아시나요?

cross-origin에 관해 설명해주실 수 있나요?

same-origin과 cross-origin, same-site는 무엇인가요?

CS Study 11주차

Origin & Site

김신아

1. Origin

https://www.example.com:443

scheme

host name

port

1. Origin -> same-origin & cross-origin

origin

https://www.example.com:443

cross-origin

https://www.example.com:443/foo

동일한 scheme, host name, port로 구성된 웹 사이트는 **same-origin** 이다.
다른 웹사이트는 **cross-origin** 이다.

1. Origin -> same-origin & cross-origin

Origin A : https://www.example.com:443 (기준 URL)

Origin B	same-origin or cross-origin	reason
https://**www.evil.com**:443	cross-origin	domains 불일치
https://example.com:443	cross-origin	subdomains 불일치
https://**login**.example.com:443	cross-origin	subdomains 불일치
http://www.example.com:443	cross-origin	schemes 불일치
https://www.example.com:**80**	cross-origin	port 번호 불일치
https://www.example.com:443	same-origin	정확한 일치
https://www.example.com	same-origin	암시적 port 번호(443) 일치

2. Site

.com .org

최상위 도메인(TLDs)은 Root Zone Database에 나열되어있다.
TLD와 그 앞의 도메인 부분의 조합을 Site 라 한다.
e.g) https://www.example.com:443/foo

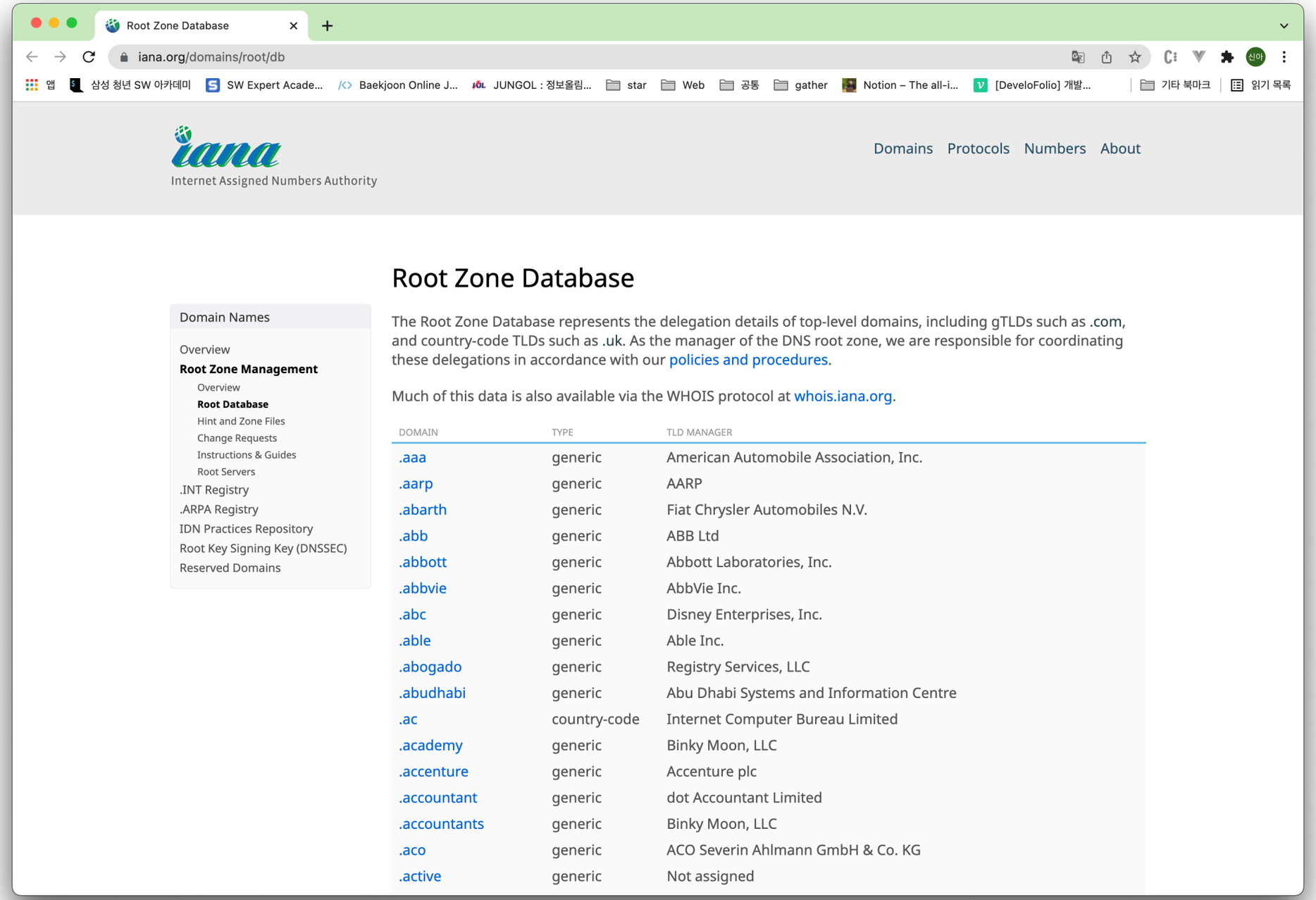
2. Site

.co.jp .github.io

TLD를 사용하는 것만으로는 Site를 식별할 수 있을만큼 세분화되지 않았다.
특정 TLD에 대해 등록 가능한 도메인의 레벨을 알고리즘적으로 결정할 방법이 없다.
이러한 이유로 effective TLDs(eTLD) 목록이 만들어졌다.
Public Suffix List에 정의되어 있다. eTLDs 목록은 publicsuffix.org/list에서 관리된다.
전체 Site 이름은 eTLD+1 로 알려져 있다.

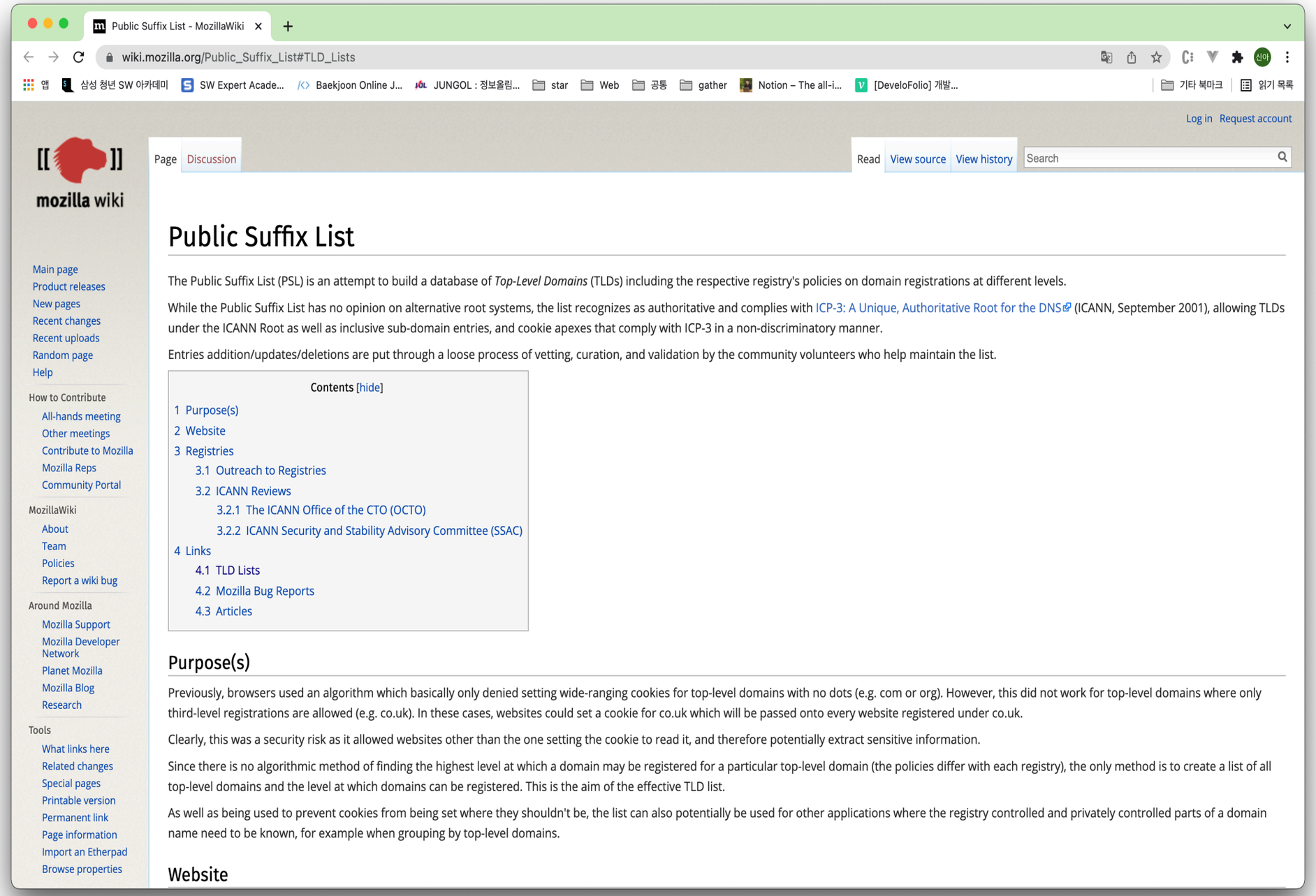
동일한 eTLD + 1이 있는 웹사이트는 same-site 이다.
다른 eTLD + 1이 있는 웹사이트는 cross-site 이다.

2. Site



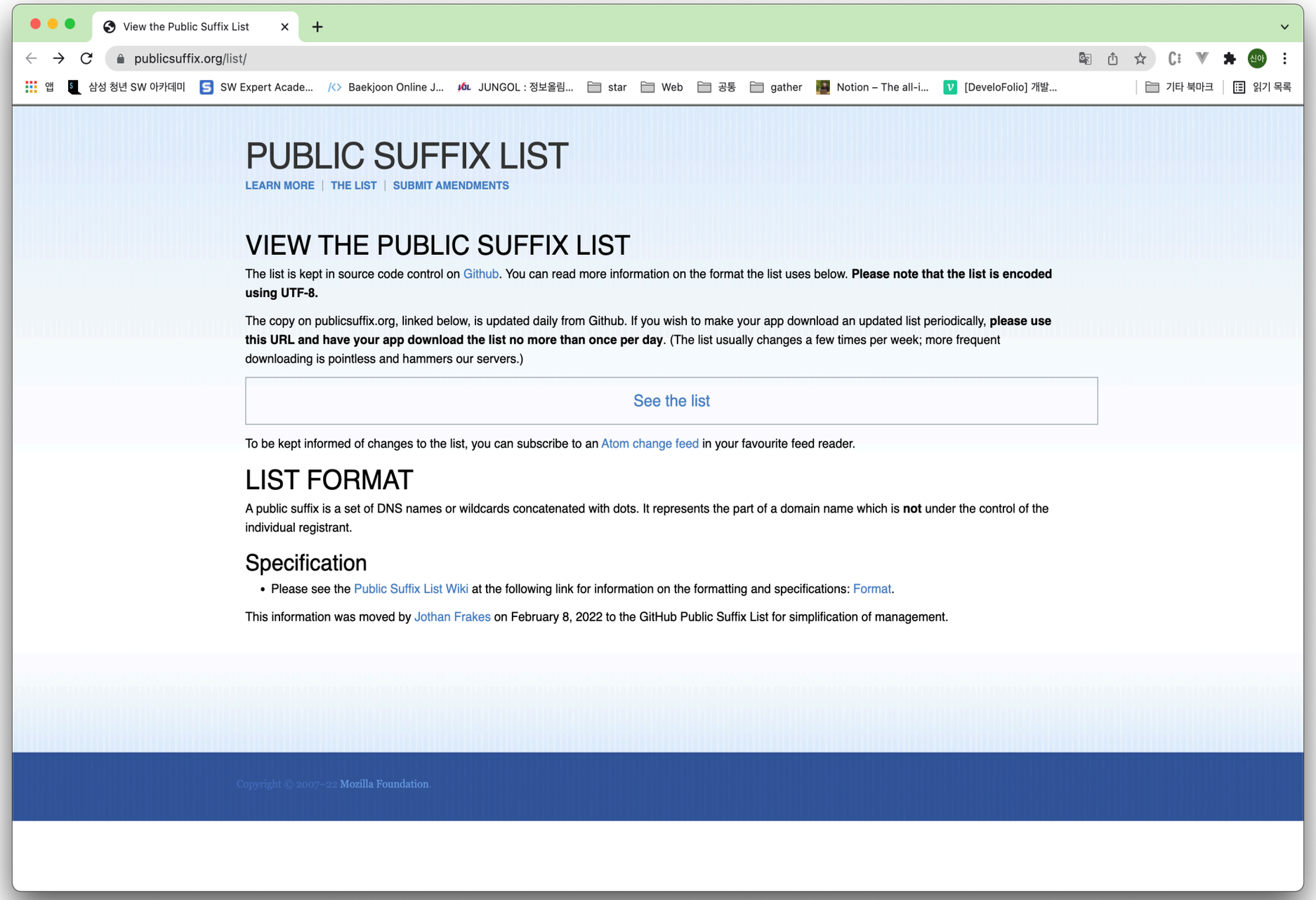
https://www.iana.org/domains/root/db

2. Site



https://publicsuffix.org/list/

2. Site



https://wiki.mozilla.org/Public_Suffix_List#TLD_Lists

2. Site -> same-site & cross-site

Origin A : https://www.example.com:443 (기준 URL)

Origin B	same-site or cross-site	reason
https://**www.evil.com**:443	cross-site	domains 불일치
https://**login**.example.com:443	same-site	다른 subdomains 상관없음
http://login.example.com:443	same-site	다른 schemes은 상관없음
https://www.example.com:**80**	same-site	다른 port 번호는 상관없음
https://www.example.com:443	same-site	정확한 일치
https://www.example.com	same-site	port 번호 상관없음

3. schemeful same-site

http://www.example.com

https://www.example.com

same-site는 scheme를 무시하고 있지만,
http의 취약점을 방어하기 위해 URL scheme 을 Site의 일부로 간주하도록 진화하고 있다.
schemes가 일치하지 않기 때문에 cross-site 로 간주한다.

3. schemeful same-site

Origin A : https://www.example.com:443 (기준 URL)

Origin B	schemeful same-site	reason
https://**www.evil.com**:443	cross-site	domains 불일치
https://**login**.example.com:443	schemeful same-site	다른 subdomains 상관없음
http://login.example.com:443	cross-site	schemes 불일치
https://www.example.com:**80**	schemeful same-site	다른 port 번호는 상관없음
https://www.example.com:443	schemeful same-site	정확한 일치
https://www.example.com	schemeful same-site	port 번호 상관없음

4. ‘same-site’, ‘same-origin’, ‘cross-site’ 확인하는 방법

Chrome은 Sec-Fetch-Site HTTP header와 함께 요청을 보낸다.
(다른 브라우저는 지원하지 않을수도 있다.)
이것은 더 큰 Fetch Metadata Request Headers 목적의 일부이다.
Sec-Fetch-Site는 다음의 값들 중 하나를 가지고 있다.

- cross-site
- same-site
- same-origin
- none

‘schemeful-same-site’는 Sec-Fetch-Site로 알 수 없다.
cf. Fetch Metadata Request Headers -> https://www.w3.org/TR/fetch-metadata/

4. ‘same-site’, ‘same-origin’, ‘cross-site’ 확인하는 방법

```
▼ Request Headers
    :authority: developer.mozilla.org
    :method: GET
    :path: /ko/docs/Web/HTTP/Headers/Referer
    :scheme: https
    accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
    application/signed-exchange;v=b3;q=0.9
    accept-encoding: gzip, deflate, br
    accept-language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
    cache-control: max-age=0
    cookie: _ga=GA1.2.1555481756.1644224392; _gid=GA1.2.1633546348.1645979419; lux_uid=164599384781348624
    if-modified-since: Sun, 27 Feb 2022 01:10:52 GMT
    if-none-match: W/"e391f69b70f7a2868041320b2cfca2d0"
    referer: https://ogaeng.com/http-referrer/
    sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
    sec-ch-ua-mobile: ?0
    sec-ch-ua-platform: "macOS"
    sec-fetch-dest: document
    sec-fetch-mode: navigate
    sec-fetch-site: same-origin
    sec-fetch-user: ?1
    upgrade-insecure-requests: 1
    user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
    e/98.0.4758.109 Safari/537.36
```

Thank You

별첨

https://minjung-jeon.github.io/same-site-same-origin/

https://www.iana.org/domains/root/db

https://publicsuffix.org/list/

https://wiki.mozilla.org/Public_Suffix_List#TLD_Lists

https://www.w3.org/TR/fetch-metadata/#sec-fetch-user-header