**웹 시스템 설계 – 14주차 학습 보고서 5 (2020년 12월 16일까지 제출)**

|  |  |  |
| --- | --- | --- |
| 성명 : 유 상 정 | 학과 : 사이버보안학과 | 학번 : 201602641 |

※ 본 학습보고서를 작성함에 있어 다른 학생의 문서로부터 일부 또는 전체를 복사하였습니까?

예( ) 아니오(✓) (복사 하였다면 예에 체크하고 아니라면 아니오에 체크하시오)

**I. Objectives**

* SOP(Same-Origin Policy)를 해결하는 방법에 대해서 학습한다.

**II. Exercises**

* 14주차 학습과제 수행 시, CORS(Cross Origin Resource Sharing)가 활용된 부분의 코드를 복사 및 붙여넣기 하고 CORS에 대해서 자세히 설명하시오.

|  |  |
| --- | --- |
| **코드에서 CORS가 활용된 부분과 설명** | var app = express();  var reviewRouter = require('./routes/review');  app.use(cors());  교차 출처 리소스 공유(Croos-Origin Resource Sharing, CORS) 는 추가 HTTP 헤더를 사용하여 한 출처에서 실행 중인 웹 애플리케이션이 다른 출처의 선택한 자원에 접근할 수 있는 권한을 부여하도록 브라우저에 알려주는 체제이다. 웹 애플리케이션은 리소스가 자신의 출처(도메인, 프로토콜, 포트)와 다를 때, 교차 출처 HTTP 요청을 실행한다. 이때, same origin 규칙은 protocol, port, host가 모두 같은 경우이다.    CORS 예시: https://domain-a.com 의 frontend JavaScript Code가 XMLHttpRequest를 사용하여 <https://domain-b.com/data.json>을 요청하는 경우.  보안상의 이유로, browser는 스크립트에서 시작한 Cross-origin HTTP 요청을 제한한다.  CORS 체제는 브라우저와 서버 간의 안전한 교차 출처 요청 및 데이터 전송을 지원한다. 최신 브라우저는 XMLHttpRequest 또는 [Fetch](https://developer.mozilla.org/ko/docs/Web/API/Fetch_API)와 같은 API에서 CORS를 사용하여 교차 출처 HTTP 요청의 위험을 완화한다. |