파라미터 위조, 변조 방지를 위한 URL 암호화 기술

신준석 [1] 이덕규
[1]서원대학교 소프트웨어학과
James990729@gmail.com , deokgyulee@seowon.ac.kr

Jun-Seok Shin[1]
[1]Department of Software, Seo-Won University

요 약

url 은 사용자들에게 편의성을 제공하지만 이로 인해 발생하는 보안 문제점들이 있다. 파라미터 값을 변조해 발생하는 온라인 쇼핑몰 해킹이나 회사 내부망에서 관리자 페이지나 사내 기밀 게시판 등 평소라면 접근할 수 없는 숨겨진 페이지에 접근을 시도하는 문제점들이 발생해 이를 방지할 AES 방식의 url 암호화 기술을 구상해 보았다.

1. 서론

URL 파라미터 위조,변조로 인해 발생하는 보안 사고를 방지하기 위해 URL 요청자에게 주소를 노출 시키 지 않고 API 단계에서 이를 처리하는 URL 암호화 방식을 소개해 보려고 한다.

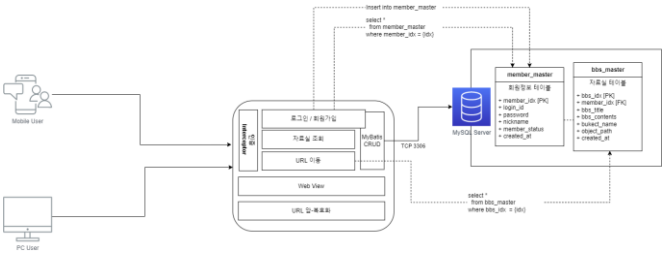
2. 현재까지의 URL 암호화 기술

웹 서비스를 운영하는 일반 사용자들에게 조금 더 안정성 있는 웹 보안이 필요하다. 현재까지 url 을 웹 이용자에게 노출시키지 않기 위해 개발된 기술들이 있다. 대표적인 방식으로 [1]OTAC 이 기술은 token 이라고 하는 Hash 함수로 암호화된 url 을 생성하게 된다. url 과 sessionid, timestamp, salt 값을 더해 암호화를 하고 1 회용 토큰으로 구성되어 url 노출 방지에 효과적인 기술이다. 하지만 DB 에 url 주소가 그대로 저장되어 있어 url 값을 암호화 해서 저장하는 방식을 구상해 보았다.

3. API url 암호화 기술

API 에서는 암호화, 복호화, Gateway, DB 정보 확인 및 불러오기 등의 역할을 수행한다. 데이터베이스에서 불러온 암호화된 URL 을 복호화 시킨 후 사용자에게 URL 을 넘겨주지 않고 해당 링크로 요청자를 보내주게 되어 접근 권한을 가진 사용자에게도 URL 노출을 방지 시킬 수 있다. 암호화 방식은 복호화가 필요하기 때문에 AES 256 방식을 사용한다.

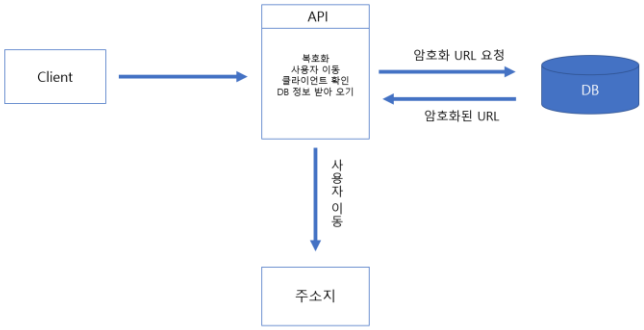
4. 설계도



<표 1>암호화 url 설계도

url 암호화 방식은 복호화가 필요하기 때문에 AES 256 방식을 사용하고 DB 에서 불러온 url 을 복호화 시킨 후 사용자에게 url 을 노출시키지 않고 해당 링크로 요청자를 보내주게 된다.

5. 흐름도



<표 2>흐름도

사용자가 서비스를 이용할 때 해당 페이지로 이동을 할 경우 HTML <a href> 태그에 암호화된 url 로 넘어갈 수 있는 링크를 넣어주게 되고 해당 링크를 통해 API 에서는 사용자를 식별하고 url 을 복호화 해 사용자를 해당 요청지로 이동시켜 주게 된다.

6. 결론

AES 방식의 url 암호화를 적용하게 된다면 DB 에도 암호화된 url 값을 저장하기 때문에 조금 더 안정성을 강화할 수 있다.

참고문헌

[1] Guiseok Kim, Seungjoo Kim " OTACUS: Parameter-Tampering Prevention Techniques using Clean URL ", 55-64 , 2014. Dec.: 15