세션과 쿠키

- description : CAPTCHA
- author : 오션
- email : shlim@repia.com
- lastupdate : 2020-09-10

Session과 Cookie

웹은 대다수가 HTTP 기반으로 동작합니다. HTTP가 구현된 방식에서 웹 서버와 클라이언트는 지속적으로 연결을 유지한 상태가 아니라, 요청(request) – 응답(response)의 반복일 뿐이기 때문에, 이전 요청과 새로운 요청이 같은 사용자(같은 브라우저)에서 이루어졌는지를 확인하는 방법이 필요하며, 이때 '쿠키(cookies)'와 '세션(session)'이 필요합니다.

쿠키(cookies)는 유저가 웹 사이트를 방문할 때 사용자의 브라우저에 심겨지는 작은 파일인데, Key - Value 형식으로 로컬 브라우저에 저장됩니다. 서버는 이 쿠키의 정보를 읽어 HTTP 요청에 대해 브라우저를 식별합니다.

그러나, 쿠키는 로컬에 저장된다는 근원적인 문제로 인해 악의적 사용자가 쿠키를 변조하거나 탈취해 정상적이지 않은 쿠키로 서버에 요청을 보낼 수 있습니다. 만약 '로그인 하였음'이라는 식별을, 로컬 쿠키만을 신뢰해 로그인을 한 상태로 서버가 인식한다면 쿠키 변조를 통해 마치 관리자나 다른 유저처럼 행동할 수도 있습니다.

이를 방지하기 위해 서버측에서 클라이언트를 식별하는 '세션'을 주로 이용하게 됩니다.

세션은 브라우저가 웹 서버에 요청을 한 경우 서버 내에 해당 세션 정보를 파일이나 DB에 저장하고 클라이언트의 브라우저에 seesion-id라는 임의의 긴 문자열을 줍니다. 이때 사용는 쿠키는 클라이언트와 서버간 연결이 끊어진 경우 삭제된는 메모리 쿠키를 이용합니다.

쿠키, Cookie from TTA

웹 서버가 웹 브라우저에게 보내어 저장했다가 서버의 부가적인 요청이 있을 때 다시 서버로 보내주는 문자열 정보, 예를 들면, 어떤 사용자가 특정 웹사이트에 접속한 후 그 사이트 내에서 어떤 정보를 보았는지 등에 관련된 기록을 남겨 놓았다가 다음에 접속하였을 때 그것을 읽어 이전의 상태로 유지하면서 검색할 수 있게 하는 역할을 한다.

세션, Session from TTA

1. 망 환경에서 사용자 간 또는 컴퓨터 간의 대화를 위한 논리적 연결.Fix Me!
2. 프로세스들 사이에서 통신을 수행하기 위해서 메시지 교환을 통해 서로를 인식 이후부터 통신을 마칠 때까지의 기간.Fix Me!

세션 식별자, Session Identification, Session ID, SID from TTA

웹 서버가 다수의 웹 페이지 요청자를 구별하기 위하여 각 사용자의 세션에 대해서 부여하는 임의의 긴 문자열 값. 사용자가 홈 페이지를 방문하거나 인증 로그인할 때에 생성된다. 일반적으로 세션 식별자(session ID)에는 사용자의 계정, 암호, 그 밖의 IP주소, 타임 스탬프 등의 여러 파라미터들이 조합되어 생성된다. HTTP는 기본적으로 비연결 유지(stateless) 프로토콜이어서 웹 페이지를 방문할 때마다 새로운 로그인이 필요하다. 이러한 불편함을 해결하는 방안으로 세션 ID가 사용되며, 처음 로그인 시 아이디(ID), 비밀번호 입력, 또는 기타 인증 절차에 의하여 사용자가 확인되면 그 이후 방문에는 서버에 저장되어 있는 세션 ID 정보에 의하여 인증이 유지된다. 세션 ID는 쿠키(cookie)에 저장되는 것이 일반적이다. 그러나 가끔은 웹 브라우저 주소창 URL이나 HTML 페이지 폼 소스상의 히든(hidden) 필드에 포함되어 해커의 공격 대상이 되기도 한다.

Ref

Session을 이용해 로그인하기

오션, 세션과, 쿠키,, Session,, Cookie

From:
http://125.132.25.164/dokuwiki/ - **문제를 잘 정의하는 것은 문제를 절반 해결한 것이다. - 2023.12**

Permanent link:
http://125.132.25.164/dokuwiki/doku.php?id=wiki:miscellaneous:session_and_cookie&rev=1599710732

Last update: **2022/03/10 19:52**