

브라우저 기능을 이용하는  
잘못된 보안 권고 사항

(주)시도우 웹표준화 추진팀 팀장

신현석(<http://hyeonseok.com>)

2006년 7월 4일

## 브라우저 주소 입력부분에 URL이 표시되지 않아야 한다는 사항

### URL 표시를 막는 것이 가능한가?

URL 표시를 막기 위해서 사용되는 방법을 살펴보면 웹사이트의 첫페이지(index.html등)를 Frameset문서로 만들어서 주소 부분을 고정시키는 방법을 사용하고 있다. 하지만 브라우저의 페이지 정보에는 해당 페이지의 URL이 정상적으로 표시되기 때문에 URL이 단지 주소 표시줄만 나오지 않을 뿐으로 실제로 페이지 URL을 감출 수는 없다. URL은 브라우저가 페이지를 표시하기 위한 기본적인 정보이기 때문에 현재 보고 있는 페이지의 URL을 표시 안 되게 하는 것은 불가능하다.

그리고 이 방법은 다른 문제점도 가지고 있다. 우선 프레임 구조가 아닌 웹사이트를 불필요하게 프레임 구조로 만들기 때문에 잘못된 HTML사용이다. 그리고 프레임으로 이루어진 웹페이지의 경우 화면 재갱신(refresh)을 할 경우 현재 페이지가 재갱신되는 것이 아니라 프레임 셋의 맨 첫화면(웹사이트의 첫화면)으로 페이지가 이동할 수가 있다. 또한, 사용자가 현재 보고 있는 페이지를 다른 사람과 공유하거나 저장하고자 할 때 URL이 노출되지 않기 때문에 불편을 겪게 된다.

### URL 표시가 보안수준을 낮추는가?

URL이란 Uniform Resource Locators의 약자로서 웹페이지의 위치를 나타내는 고유의 값을 의미 한다. 통상 하나의 웹페이지는 하나의 URL을 가지게 되고 이 URL은 페이지의 위치를 확인, 저장, 공유하는 수단으로 사용되게 된다. 따라서 URL은 감춰야 하는 사항이 아니라 사용자가 보다 명확하게 인식할 수 있게 하여야 하는 중요한 정보이다.

일부, URL이 노출 됨으로 해서 해킹의 빌미를 제공한다는 주장은 URL이 웹페이지를 표시하는 기본 정보라는 것을 인식하지 못한 전혀 근거 없는 주장이다. 보안수준을 높이기 위해서는 URL을 안보이게 해야 하는 것이 아니라 악의를 가진 부적절한 URL 접근이 있을 때 이를 인지하고 서버측에서 효과적으로 접근을 차단해야 한다. 웹서버의 디렉토리 리스팅을 막는다든지 부적절한 파라미터 조작을 방지하는 방법 등이 그 방법이다.

## 마우스 오른쪽 클릭/드래그가 안되게 해야 한다는 사항

### 특정 마우스 기능을 막는 것이 가능한가?

마우스 기능을 제어하는 방법을 살펴보면 oncontextmenu, onselectstart, ondragstart 같은 javascript 이벤트를 제어하여 해당 기능이 작동되지 않게 하는 방법을 사용한다. 하지만 javascript를 제어하는 방식은 브라우저에서 javascript 기능을 꺼버리게 되면 작동하지 않게 된다. 사용자 브라우저 기능을 javascript로 제어하는 것은 불가능 하다.

또한, 마우스 오른쪽 클릭을 했을 때 나오는 메뉴에는 그림 저장과 같은 기능 뿐만 아니라 “뒤로”, “앞으로”, “새로고침”, “인쇄”, “새창에서 열기”와 같은 웹페이지 이용을 위한 기능들도 제공이 되는데 사용자가 이런 기능까지도 이용할 수 없게 되기 때문에 옳지 않은 방법이다.

### 특정 마우스 기능을 막는 것이 보안 수준을 향상시키는가?

인터넷에 올려지는 컨텐츠나 이미지등은 기본적으로 공유를 목적으로 하고 있고 그러한 기반으로 인터넷이 만들어져 있기 때문에 배포에 문제가 있는 컨텐츠는 인터넷을 통해서 공개가 되지 않도록 하는 것이 바람직하다.

그리고 이러한 콘텐츠를 javascript로 보호하는 것은 기술적으로 불가능하다. 웹페이지라는 것 자체가 사용자 화면에서 보여지게 될 단계에 이미 브라우저 캐시나 컴퓨터 메모리에 저장되기 때문에 이를 막는 것을 불가능하고 보호해야 하는 콘텐츠는 웹을 이용하지 않고 브라우저 외의 다른 수단을 통해서 전달해야 한다.

## 상태표시줄에 링크의 경로 나오지 않게 하기

### 상태표시줄의 링크를 제어하는 것이 가능한가?

상태표시줄을 제어하는 방법은 1초에 수십~수백번 상태표시줄에 다른 텍스트를 출력함으로 가려지는 것 처럼 보이게 하는 눈속임이다. 이것 역시 브라우저에서 javascript 기능을 끄면 작동하지 않는다. 그리고 이 상태표시줄을 제어하는 것은 피싱으로 악용 될 수 있기 때문에 최근의 보안이 강화된 브라우저들은 javascript로 상태표시줄을 제어할 수 없게 되어있다.

그리고 상태표시줄은 사용자가 마우스나 키보드를 이용해서 웹페이지를 이용할 때 현재의 상태가 링크 상태이고 해당 URL이 어떠한 것인지를 알려주는 사용자에게는 매우 유용한 정보이기 때문에 이를 사용하지 못하게 하는 것은 바람직 하지않다.

### 상태표시줄의 링크를 감추는 것이 보안 수준을 향상 시키는가?

URL의 경우나 마우스 이용을 제어하는 것과 마찬가지로 javascript 기능을 끄거나 html에 대한 기본적인 지식만 있으면 이러한 정보들은 쉽게 접근할 수 있는 정보들이다. 그리고 이 정보들은 사용자에게 반드시 필요한 것들이기 때문에 보안과는 전혀 상관이 없는 사항이다.

## 결론

javascript를 이용하거나 frame을 이용하는 등, 사용자 브라우저 기능을 이용한 처리는 보안 수준을 향상 시킬 수 없고 웹페이지의 사용성만을 떨어뜨리게 된다. 보안 수준을 향상시키기 위해서는 서버측에서 부적절한 접근을 효과적으로 차단하고 대응해야하고, 정보통신부나 국가정보원 등에서 배포하는 보안 지침을 잘 준수 하여야 할 것이다. 그리고 해킹에 대한 빌미를 제공하는 것을 미리 막겠다는 주장은 HTTP로 전송되어 이미 브라우저 화면에 출력된 웹페이지에는 해당사항이 없다.