



#5 / What is mixed content?

Mixed content occurs when initial HTML is loaded over a secure HTTPS connection, but other resources (such as images, videos, stylesheets, scripts) are loaded over an insecure HTTP connection.

Mixed content 는 초기 HTML 이 보안된 HTTPS 연결을 통해 로드되지만, 다른 리소스 (이비지, 비디오, stylesheet, scripts 등) 들이 보안되지 않은 HTTP 연결을 통해 로드될 때 발생합니다.

This is called mixed content because both HTTP and HTTPS content are being loaded to display the same page, and the initial request was secure over HTTPS.

초기 요청은 분명 보안된 HTTPS 였으나 같은 페이지를 보여주기 위해 HTTP 와 HTTPS 연결을 사용하는 컨텐츠가 로드되기 때문에 이를 mixed content 라고 부릅니다.

Requesting subresources using the insecure HTTP protocol weakens the security of the entire page, as these requests are vulnerable to on-path attacks, where an attacker eavesdrops on a network connection and views or modifies the communication between two parties.

sub 리소스들을 보안되지 않은 HTTP 프로토콜을 사용해서 요청하는 것은 이러한 요청들이 공격자가 네트워크 연결을 도청하거나 서버와 사용자간의 통신을 보거나 수정할 수 있다는 점에서 on-path attacks 에 취약하기 때문에, 전체 페이지의 보안을 약화시킵니다.

Using these resources, attackers can track users and replace content on a website,
and in the case of active mixed content,
take complete control over the page,
not just the insecure resources.

이러한 리소스들을 사용하면,
공격자들은 사용자를 추적하고 웹사이트의 컨텐츠를 바꿀 수 있게 되며,
active mixed content 의 경우에는
단지 보안되지 않은 리소스에서 멈추는 것이 아니라
페이지의 통제권을 완전히 가져갈 수 있습니다.

Although many browsers report mixed content warnings to the user, by the time this happens, it is too late:
the insecure requests have already been performed and the security of the page is compromised.

비록 많은 브라우저들이 mixed content 의 위험을 사용자에게 알려주지만,
그때는 너무 늦었습니다:
안전하지 않은 요청이 이미 수행되었고 페이지의 보안은 약화되었습니다.

This is why browsers are increasingly blocking mixed content.
이것이 바로 많은 브라우저들이 점점 mixed content 를 막는 이유입니다.

If you have mixed content on your site,
then fixing it will ensure the content continues to load
as browsers become more strict.

만약 당신의 사이트가 mixed content 를 가지고 있다면,
그것을 고치는 것은 브라우저들이 점점 엄격해짐에도
컨텐츠가 계속 로드될 수 있도록 보장할 것입니다.

The two types of mixed content

mixed content 의 두가지 유형

The two types of mixed content are: active and passive.

mixed content에는 두가지 유형이 있습니다: 적극적인 것과 수동적인 것.

Passive mixed content refers to content that doesn't interact with the rest of the page, and thus a man-in-the-middle attack is restricted to what they can do if they intercept or change that content.

Passive mixed content란 페이지의 나머지 부분들과 상호작용하지 않는 컨텐츠를 말하며, 따라서 중간에서 공격자가 컨텐츠를 가로채거나 바꾸더라도 그들이 할 수 있는 공격이 제한됩니다.

Passive mixed content is defined as images, video, and audio content.

Passive mixed content는 이미지, 비디오, 음성 컨텐츠들로 정의됩니다.

Active mixed content interacts with the page as a whole and allows an attacker to do almost anything with the page.

Active mixed content는 페이지 전체와 상호작용하며 공격자들이 그 페이지에서 거의 모든 것을 할 수 있도록 합니다.

Active mixed content includes scripts, stylesheets, iframes, and other code that the browser can download and execute.

Active mixed content는 스크립트, 스타일시트, 아이프레임, 그리고 브라우저가 다운로드하고 실행할 수 있는 여러 코드들을 포함합니다.

Passive mixed content

수동적 혼합된 컨텐츠

Passive mixed content is seen as less problematic yet still poses a security threat to your site and your users.

Passive mixed content는 덜 문제가 있는 것으로 간주되지만, 여전히 사이트와 사용자에게 보안 위협을 가하고 있습니다.

For example,
an attacker can intercept HTTP requests for images on your site and swap
or replace these images;
the attacker can swap the save and delete button images,
causing your users to delete content without intending to;
replace your product diagrams with lewd or pornographic content, defacing
your site;
or replace your product pictures with ads for a different site or product.

예를 들어,
공격자가 HTTP 요청을 중간에서 가로채어 당신의 사이트의 이미지를 변경할 수 있습니다;
공격자가 save 와 delete 버튼 이미지를 바꾸어
사용자가 의도치 않았는데도 컨텐츠를 삭제하도록 할 수 있습니다;
당신의 상품 그림을 무례하고 외설적인 컨텐츠로 바꾸어
당신 사이트를 망칠 수 있습니다;
또는 당신의 상품 그림을 다른 사이트의 상품이나 광고로 바꿀 수 있습니다;

Even if the attacker doesn't alter the content of your site, an attacker
can track users via mixed content requests.

공격자가 당신의 사이트의 컨텐츠를 수정하지 않을지라도,
공격자는 mixed content 요청을 통해 사용자들을 추적할 수 있습니다.

The attacker can tell which pages a user visits and which products they
view based on images or other resources that the browser loads.

공격자는 이미지 또는 브라우저가 로드하는 다른 리소스들을 통해
사용자가 어떤 페이지를 방문하고 어떤 상품을 보는지 알 수 있습니다.

The following Glitch demo contains examples of passive mixed content.

다음 Glitch demo 는 passive mixed content 의 예시를
담고 있습니다.

Passive mixed content

Audio file

▶ 0:00 / 0:01 ━━ ◀ ▶ ⏱

Image file



 passive-mixed-content by 

[Share](#) [View Source](#)



If passive mixed content is present most browsers will indicate in the URL bar that page is not secure, even when the page itself was loaded over HTTPS.

만약 passive mixed content 가 있는 경우,
대부분의 브라우저들은 지금의 페이지가 HTTPS 를 통해 로드되었더라도
URL 막대에서 이 페이지는 안전하지 않다고 말할 것입니다.

Until recently passive mixed content was loaded in all browsers, as to block it would have broken many websites.

최근까지 passive mixed content 는 모든 브라우저들에서 로드되었기에,
그것을 막는 것은 아마 많은 웹사이트들을 망가뜨릴 것입니다.

This is now beginning to change and so it is vital to update any instances of mixed content on your site.

지금 이러한 변화는 막 시작되었기 때문에
당신의 사이트의 모든 mixed content 요소를 업데이트하는 것이
꼭 필요합니다.

Chrome is currently rolling out automatic upgrading of passive mixed content where possible.

크롬은 현재 passive mixed content 의 업그레이드가 가능하다면,
이를 자동으로 업그레이드 해주는 것을 개발하고 있습니다.

Automatic upgrading means that if the asset is available over HTTPS, but has been hardcoded as HTTP, the browser will load the HTTPS version.

여기서 자동 업그레이드는

만약 컨텐츠를 HTTPS로 로드하는 것이 가능하지만 HTTP로 하드코딩된 경우, 브라우저가 HTTPS로 로드하는 것을 뜻합니다.

If no secure version can be found the asset will not load.

만약 보안된 버전이 발견되지 않을 경우, 컨텐츠는 로드되지 않을 것입니다.

Chrome logs messages to its DevTools Console whenever it detects mixed content or auto-upgrades passive mixed content.

크롬은 mixed content를 발견하고 자동 업그레이드가 가능한 것을 발견하면, 이를 개발도구 콘솔창에다 메시지를 남깁니다.



The screenshot shows the 'Issues' tab in Chrome DevTools. A message at the top says 'Issues detected. The new Issues tab displays information about deprecations, breaking changes and other potential problems.' There are five yellow warning messages listed:

- Mixed Content: The page at '<https://passive-mixed-content.glitch.me/>' was loaded over HTTPS, but requested an insecure image '<http://cdn.glitch.com/446ca0ec-cc52-4774-889a-6dc040eac6ef%2Fpuppy.jpg?v=1600261043278>'. This content should also be served over HTTPS.
- Mixed Content: The page at '<https://passive-mixed-content.glitch.me/>' was loaded over HTTPS, but requested an insecure element '<http://cdn.glitch.com/446ca0ec-cc52-4774-889a-6dc040eac6ef%2Fsleep.mp3?v=1600261050178>'. This request was automatically upgraded to HTTPS. For more information see <https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html>.
- Mixed Content: The page at '<https://passive-mixed-content.glitch.me/>' was loaded over HTTPS, but requested an insecure element '<http://cdn.glitch.com/446ca0ec-cc52-4774-889a-6dc040eac6ef%2Fchrome.webm?v=1600260322137>'. This request was automatically upgraded to HTTPS. For more information see <https://blog.chromium.org/2019/10/no-more-mixed-messages-about-https.html>.
- Mixed Content: The page at '<https://passive-mixed-content.glitch.me/>' was loaded over HTTPS, but requested an insecure audio file '<http://cdn.glitch.com/446ca0ec-cc52-4774-889a-6dc040eac6ef%2Fsleep.mp3?v=1600261050178>'. This content should also be served over HTTPS.
- Mixed Content: The page at '<https://passive-mixed-content.glitch.me/>' was loaded over HTTPS, but requested an insecure video '<http://cdn.glitch.com/446ca0ec-cc52-4774-889a-6dc040eac6ef%2Fchrome.webm?v=1600260322137>'. This content should also be served over HTTPS.

Active mixed content

적극적 혼합된 컨텐츠

Active mixed content poses a greater threat than passive mixed content.

Active mixed content는 passive mixed content 보다 더 큰 위협을 제기합니다.

An attacker can intercept and rewrite active content,
thereby taking full control of your page or even your entire website.

공격자는 active 컨텐츠를 가로채서 다시 쓸 수 있으며,
따라서 그 페이지, 심지어 전체 웹사이트의 제어권을 완전히 가져갈 수 있습니다.

This allows the attacker to change anything about the page, including displaying entirely different content, stealing user passwords or other login credentials, stealing user session cookies, or redirecting the user to a different site entirely.

이를 통해 공격자는 완전히 다른 컨텐츠를 보여주거나,
사용자의 패스워드나 다른 로그인에 관련된 증명정보를 훔치거나,
사용자 세션 쿠키를 도용하거나,
사용자를 완전히 다른 사이트로 리다이렉트하는 등
페이지에 대한 모든 것을 변경할 수 있습니다.

Due to the severity of this threat, most browsers already block this type of content by default to protect users,
but functionality varies between browser vendors and versions.

이러한 심각한 위협으로 인해, 대부분의 브라우저들은 사용자를 보호하기 위해 이미 이러한 타입의 컨텐츠를 막았습니다만, 브라우저 공급업체나 버전마다 관련 기능이 달라집니다.

The following contains examples of active mixed content.

다음은 active mixed content 를 포함하고 있는 예시입니다.

Active mixed content

Several examples of active mixed content. When viewed over HTTPS most browsers block this content and display errors in the JavaScript console.

Insecure stylesheet

Insecure background image



 active-mixed-content by 

Share

View Source

▶

◀

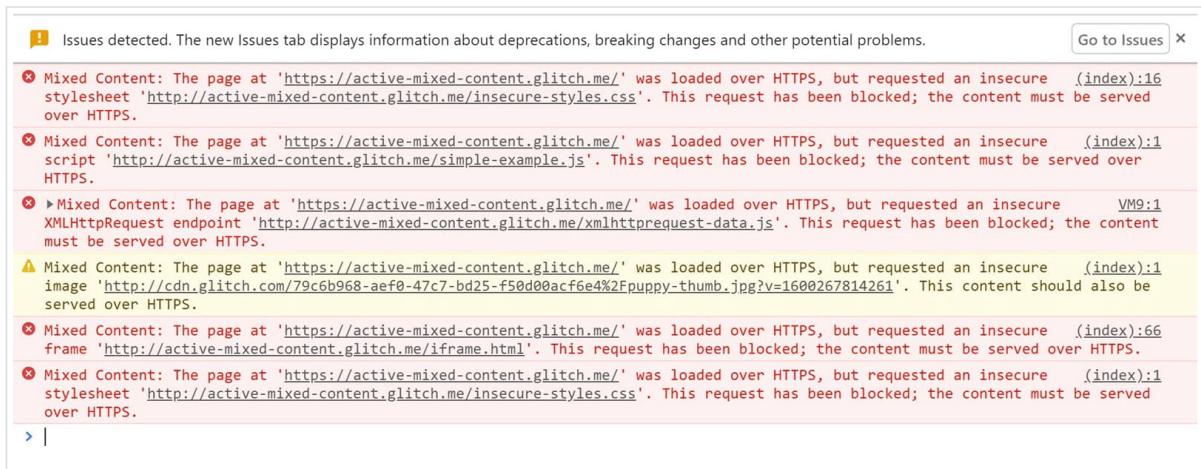
▶

Load the example over HTTP to see the content that's blocked when you load the example over HTTPS.

HTTPS 를 통해 예시를 로드할 때 차단되는 컨텐츠를 보려면
HTTP 를 통해 예시를 로드하십시오.

Block content will be detailed in the Chrome DevTools Console.

제한된 컨텐츠는 크롬 개발도구 콘솔에 자세히 설명되어 있습니다.



The mixed content specification

mixed content 구체화

Browsers follow the mixed content specification, which defines the `optionally blockable content` and `blockable content` categories.

브라우저는 `optionally blockable content` 와 `blockable content` 를 정의한 mixed content specification 을 따릅니다.

From the spec, a resource qualifies as optionally blockable content "when the risk of allowing its usage as mixed content is outweighed by the risk of breaking significant portions of the web"; this is subset of the passive mixed content category described above.

구체적인 명세에서, "mixed content"로 사용을 허가해주는 데 수반하는 위험이 웹의 중요한 부분을 파괴할 위험보다 클 때" 이러한 리소스들은 optionally blockable content를 만족합니다. 이는 앞에서 설명된 passive mixed content의 하위집합입니다.

All content that is not **optionally blockable** is considered **blockable**, and should be blocked by the browser.

optionally blockable이 아닌 모든 컨텐츠는 **blockable**로 간주되며, 브라우저에서 차단되어야만 합니다.

There is a Level 2 of the Mixed Content specification in progress, which will add automatic upgrading to the spec.

Mixed Content 명세 Level 2가 진행중이며, 자동 업그레이드가 그 명세에 추가될 예정입니다.

In recent years, HTTPS usage has risen dramatically, and has become the clear default on the web.

최근들어 HTTPS의 사용이 급격하게 증가했고 웹에 있어 기본이 된 것은 명확합니다.

This makes it more feasible now for browsers to consider blocking all mixed content, even those subresource types defined in the mixed content specification as **optionally blockable**.

이는 현재 브라우저가 모든 mixed content를 차단하는, 심지어 mixed content 명세에서 optionally blockable로 정의된 서브 리소스들도 차단하는 것을 더욱더 실현가능도록 만들고 있습니다.

This is why we now see Chrome taking a stricter approach to these subresources.

이는 크롬이 지금 이러한 서브 리소스들을 엄격하게 취급하는 이유입니다.

Older browsers

오래된 브라우저들

It is important to remember that not every visitor to your website uses the most up-to-date browsers.

당신의 사이트를 방문하는 모든 사람들이 최신버전의 브라우저를 사용하는 것이 아니라는 것을 기억하는 것은 중요합니다.

Different versions from different browser vendors each treat mixed content differently.

각양각색의 브라우저와 버전은 mixed content 를 서로 다른 방식으로 다루고 있습니다.

At worst, older browsers and versions don't block any mixed content at all, which is very unsafe for the user.

최악인 점은 오래된 브라우저나 버전의 경우 사용자들에게 있어 굉장히 안전하지 않은 mixed content 를 전혀 차단하지 않는다는 것입니다.

By fixing your mixed content problems you ensure that your content is visible in new browsers.

당신의 mixed content 문제들을 고침으로서, 당신의 컨텐츠가 새로운 브라우저에서도 보일 수 있도록 할 것입니다.

You also help protect users from dangerous content that isn't blocked by older browsers.

또한 오래된 브라우저들은 차단하지 않는 위험한 컨텐츠들로부터 유저를 보호하는데 도움을 줄 것입니다.