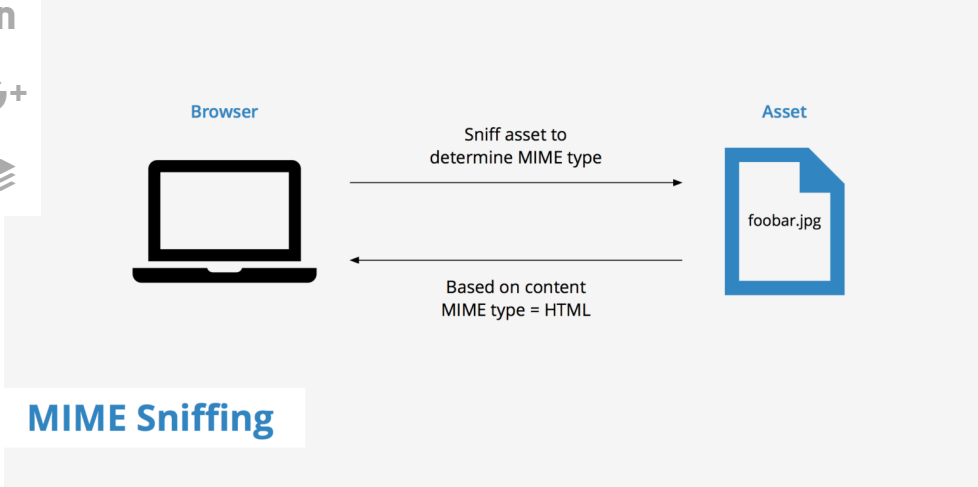
Knowledge Base

Search ...

What is MIME Sniffing?

Updated: April 19, 2017



MIME sniffing was, and still is, a technique used by some web browsers (primarily Internet Explorer) to examine the content of a particular asset. This is done for the purpose of **determining an asset's file format**. This technique is useful in the event that

there is not enough metadata information present for a particular asset, thus leaving the possibility that the browser interprets the asset incorrectly.

Although MIME sniffing can be useful to determine an asset's correct file format, it can also cause a security vulnerability. This vulnerability can be quite dangerous both for site owners as well as site visitors. This is because an attacker can **leverage MIME sniffing** to send an XSS (Cross Site Scripting) attack. This article will explain how to protect your site against MIME sniffing vulnerabilities.

To read more about further securing your sites against XSS attacks, read our Content Security Policy article.

How Does MIME Sniffing Work?

ME sniffing is quite straightforward in the way that it works. e following provides a brief description of each step involved the MIME sniffing process.

1. A web browser requests a particular asset which responds with either no content-type or a content-type previously set at the origin server.

2. The web browser "sniffs" the content to analyze what file format that particular asset is.

3. Once the browser has completed its analysis, it compares what it found against what the web server provided in the content-type header (if anything). If there is a mismatch, the browser uses the MIME type that **it determined to be associated with the asset.**

How To Avoid MIME Sniffing Vulnerabilities

MIME sniffing vulnerabilities can occur when a website allows users to **upload data to the server**. The vulnerability comes into play when an attacker disguises an HTML file as a different file type (e.g. a jpg, zip file, etc). Doing so would allow the attacker to successfully upload the file to the web server, assuming the web server accepts JPGs. Consequently, the browser will render it as an HTML file therefore providing the attacker with the possibility to execute XSS.

There are a couple of ways to avoid these kinds of attacks caused by MIME sniffing.

- You may implement the use of the `X-Content-Type-Options: nosniff` HTTP header. This header is IE and Chrome specific and forces the browser to disabling MIME sniffing. Therefore, the browser is required to use the MIME type sent by the server. Making use of this header means that the website owner should ensure they are **sending the appropriate MIME information**. This is important as the browser will no longer analyze the file.
- As an alternative method to avoid XSS attacks due to MIME sniffing, it is suggested to **use a separate sub-domain** to host and deliver all user uploaded content. Doing so will help ensure that none of the uploaded content will come in contact with your primary web application domain.

In summary, although MIME sniffing can be a useful feature provided by web browsers it can also cause security issues. Being aware of these vulnerabilities and knowing how to mitigate is vital. Through the use of the two suggestions mentioned above, you will not only help improve the security of your website but also of your visitors.

Additional Resources

- Secure Content Sniffing for Web Browsers