**Strict Transport Layer Security Misconfiguration**

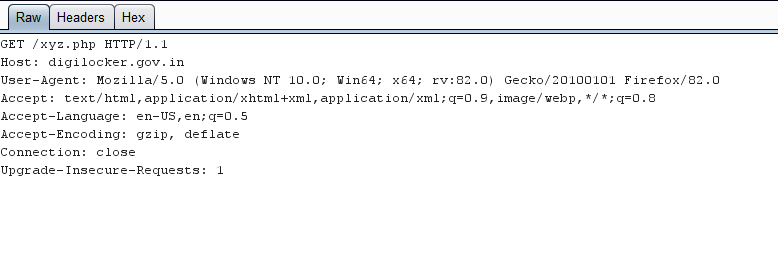
**Summary:** The HTTP strict transport security policy defines timeframe where browser must connect to web server via https. Without strict transport security policy the web application may be vulnerable against several attacks.

1. If web application mixes usage of HTTP and HTTPS, an attacker can manipulate pages in unsecured area of application or change redirection target in a manner that switch to secured page is not performed or done in manner, that the attacker remains between client and server.
2. If there is not HTTP server, an attacker in same network could simulate a HTTP server and motivate user to click on prepared URL by social engineering attack

The protection is effective only for given amount of time. Multiple occurrence of this header could cause undefined behaviour in browsers and should ne avoided

**Severity: Medium**

Request



**Complexity: Easy**

**Impact:**

Multiple occurrences of ‘Strict-Transport-Security’ headers were seen in HTTP response. This could cause undefined with browsers, because it is unclear, which header is used

**Affected Page: -**

<https://digilocker.gov.in/xyz.php> (Chatbot page)

**Recommendations:**

There should be only one header defining a strict transport security policy. The time frame be set at minimum to 7776000

**References:**

<https://www.leviathansecurity.com/blog/the-double-edged-sword-of-hsts-persistence-and-privacy>

<https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html>

**Proof of Concept (Response):**

