Implementing Security HTTP Headers to Prevent Vulnerabilities

"HTTP Public-Key Pinning"

This document provides an insight about the above security header and illustrates how it could be successfully and easily implemented into the application during the development phase to get rid of most of the general Web application vulnerabilities arising due to server misconfigurations.

It is easy to implement and covers various types of Web Servers including Apache, Microsoft IIS, Nginx and others.

HTTP Public Key Pinning:

- Minimize the man-in-the-middle (**MITM**) attacks risk by pinning certificate.
- **This is possible with HPKP (HTTP Public Key Pinning) header.**
- You can pin the root certificate public key or immediate certificate.
- HPKP currently works in Firefox and Chrome and support SHA-256 hash algorithm.

There are four possible parameter configurations.

Parameter Value	**Meaning**
report-uri="url"	Report to the specified URL if pin validation fails. This is optional.
pin-sha256="sha256key"	Specify the pins here
max-age=	Browser to remember the time in seconds that site is accessible only using one of the pinned keys.
IncludeSubDomains	This is applicable on a subdomain as well.

Configuration Required:

Example: Let's see HPKP header example from facebook.com

public-key-pins-report-only:max-age=500;
pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=";
pin-sha256="r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E=";
pin-sha256="q4PO2G2cbkZhZ82+JgmRUyGMoAeozA+BSXVXQWB8XWQ=";
report-uri=http://reports.fb.com/hpkp/