1. **Remove Unnecessary http headers from response**

**Problem:**

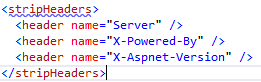
An adversary can fingerprint the web server from HTTP responses.

**Solution:**

* 1: Download iis\_stripheaders\_module\_1.0.5.msi and install it in APP server.

Download link: <https://github.com/Dionach/StripHeaders/releases>

* Add strip headers tag in, system.webserver tag in PL web.config file.



1. **Hide Sensitive data from error message**

**Problem:**

An adversary might be able to use sensitive information revealed by error messages to launch further attacks.

**Solution:**

* Add appsetting key, ‘SensitiveErrorDisplay’ in PL web.config. Possible values for ‘SensitiveErrorDisplay’ are ‘N’ or ‘Y’.



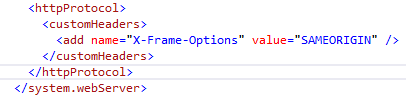
1. **Click Jacking**

**Problem:**

An adversary can trick a user into performing a sensitive operation by Clickjacking.

* **Solution:**

Add http protocol tag in system.webserver tag in web.config file:



1. **Setting and Clearing Cookies**

**Problem:**

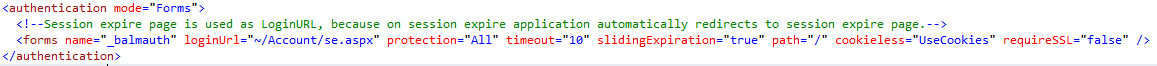
1. Session cookie attributes are not set properly.
2. A local adversary can hijack sessions as the session is not invalidated on logout.

* **Solution:**

Form authentication cookies and AspNet session cookies must set properly on login and must clear on logout or session expiration.

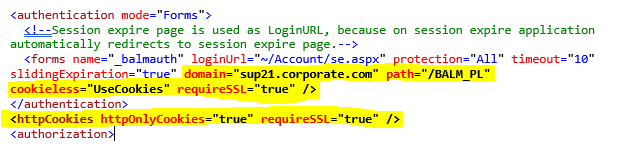
**Set cookies:**

Authentication tag in web.config:



1. **Setting up domain, Temp path and SSL connection.**

* **Solution:** Add domain and temp path of application name in web.config file



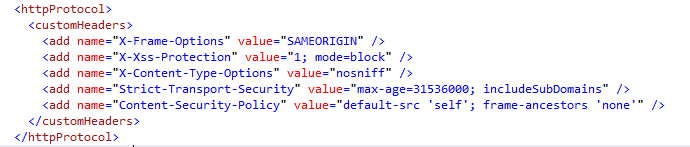
1. **Preventing Cross-Site Scripting Attacks**

**Problem:** An attacker can use XSS to send a malicious script to an unsuspecting user.

* **Solution:**

Add all below http custom headers in web.config file

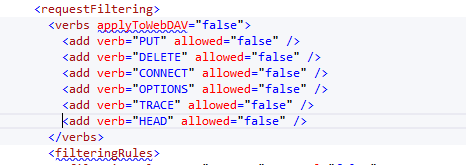
* X-Frame-Options
* X-Xss-Protection
* X-Content-Type-Options
* Strict-Transport-Security
* Content-Security-Policy



1. **Disable HTTP methods like OPTIONS, TRACE and HEAD.**

**Problem:** An attacker can manipulate these verbs to bypass the security controls.

* **Solution:**  Add below http methods to requestfiltering tag in web.config file
* OPTIONS
* TRACE
* HEAD



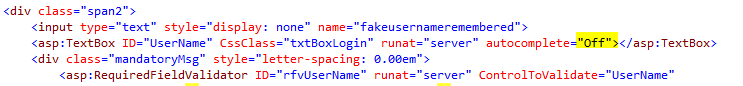
1. **Remove Autocomplete feature on login page for user name**

**Problem:**

A local advisory can steal sensitive information from the autocomplete feature of web browser

* **Solution:**  Edit Login.aspx page and put **Autocomple=“Off”** in place of **Autocomple=** **“none”** for UserName TextBox.

**Eg:**



1. **Enable CustomErrors for local users**

* **Solution:**  Keep **Remote Only** in CustomErrors tag in web.config file.

**Eg:**

