Security Http Header Settings

Hide Server Name in Http Header

> This is Required to hide the http header for ex.(Apache) from http header that would actually hide the Server Used in your Production

```
//Install the lib apache modsecurity settings for ubuntu apache2 server
apt-get install libapache2-modsecurity

//Enable the security2 module
sudo a2enmod security2

//Add The Below Code in the Configuration File of apache which is enabled for
serviing
// Note: Dont add it in VirtualHost Context

<IfModule security2_module>
    SecRuleEngine on
    ServerTokens Full
    SecServerSignature "None"
</IfModule>
```

Hide Web server Version From Http header

> This is required toi hide the version used of the web server in the http header for security from any emtity who fing the information useful to Trespass the web server

```
// Add these Lines in the apache Conf file to hide the version of web server used
ServerTokens Prod
ServerSignature Off
```

Add X-XSS Protection for Server to securing form XSS Attacks By adding the Lines

> By default / or By requirement the X-XSS Protection can be or be set to 0. Setting this Flag to 0 disable the protection to XSS Attacks. WE have to set the flag to 1.

```
// Add below Line in the Apache  conf file to do so
// Note: Please Add these Lines Outside the VirtualHost scope
Header set X-XSS-Protection 1;mode=block
```

X-Content-Type-Options Header

The X-Content-Type-Options header is used to protect against MIME sniffing vulnerabilities. These vulnerabilities can occur when a website allows users to upload content to a website however the user disguises a particular file type as something else. This can give them the opportunity to perform cross-site scripting and compromise the website.

Unfortunately, the X-Content-Type-Options: nosniff header does not protect against all sniffing-related vulnerabilities.

```
// Add the Below Line the Configuration File of Apache
Header set X-Content-Type-Options nosniff
```

Content-Security-Policy Header

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft, to site defacement, to malware distribution.

```
// Add the below Line in you apache Configuration File
Header set Content-Security-Policy "frame-ancestors 'none';"
```

X-Frame-Options Header

The X-Frame-Options in used as HTTP response header. This prevents your site content embedded into other sites. Based on this value a browser allowed other sites to open web page in iframe. It also secure your Apache web server from clickjacking attack.

```
There are three options available to set with X-Frame-Options:

‘SAMEORIGIN’ – With this setting, you can embed pages on same origin. For example,
add iframe of a page to site itself.

‘ALLOW-FROM uri – Use this setting to allow specific origin (website/domain) to
embed pages of your site in iframe.

‘DENY – This will not allow any website to embed your site pages in an iframe.



// Add the Below Line the Configuration File of Apache
Header set X-Frame-Options SAMEORIGIN
```

RewriteEngine on

RewriteCond %{THE_REQUEST} !^(POST|GET)\ /.*\ HTTP/1.1$

RewriteRule .* - [F]

Header unset Server

Header always unset "X-Powered-By"

Header unset "X-Powered-By"

#BELOW HEADER ADDED FOR INTERNET EXPLORER SECURITY

Header set X-Download-Option "noopen"

RewriteEngine On

RewriteCond %{REQUEST_METHOD} !^(GET|POST)

RewriteRule .* - [R=405,L]

```
<Location />
        <LimitExcept GET POST>
        order deny,allow
        deny from all
        </LimitExcept>
</Location>
```

Lucky 13 Attack

For Django Based Application

https://www.djangoproject.com/weblog/2013/aug/06/breach-and-django/

https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/

Breach Attack

```
SetOutputFilter DEFLATE
    BrowserMatch ^Mozilla/4 gzip-only-text/html
    BrowserMatch ^Mozilla/4\.0[678] no-gzip
    BrowserMatch \bMSIE !no-gzip !gzip-only-text/html
    SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png|zip|gz|tgz|htc)$ no-gzip dont-
vary
    # BREACH migitation
```

```
    SetEnvIfNoCase Referer .* self_referer=no
    SetEnvIfNoCase Referer ^https://www\.example\.org/ self_referer=yes
    SetEnvIf self_referer ^no$ no-gzip
    Header append Vary User-Agent env=!dont-vary
```

Http Only & Secure Flags

> Add These Files To apache.conf file

```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
#For secure flag and HTTP only
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure;SameSite=None
```