Secure Apache from Clickjacking with X-FRAME-OPTIONS

By **Chandan Kumar** / in **Apache HTTP (https://geekflare.com/category/web-infrastructure/apache/)**,**Security (https://geekflare.com/category/security/)** / Updated: February 7, 2018

17 SHARES

Implement X-FRAME-OPTIONS in HTTP headers to prevent Clickjacking attacks

Clickjacking (https://www.owasp.org/index.php/Clickjacking) is well-known web application vulnerabilities (https://geekflare.com/scan-security-vulnerabilities-to-secure-website/).

For example, it was used as an attack on Twitter.

To defense Clickjacking attack on your Apache web server, you can use **X-FRAME-OPTIONS** to avoid your website being hacked from Clickjacking.

The **X-Frame-Options** in HTTP response header can be used to indicate whether or not a browser should be allowed to open a page in frame or iframe.

This will prevent site content embedded into other sites.

Did you every try embed Google.com on your website as a frame? You can’t because it’s protected and you can protect it too (http://sucuri.7eer.net/c/245992/212721/3713).

There are three settings for X-Frame-Options:

1. **SAMEORIGIN**: This setting will allow a page to be displayed in a frame on the same origin as the page itself.
2. **DENY**: This setting will prevent a page displaying in a frame or iframe.
3. **ALLOW-FROM uri**: This setting will allow a page to be displayed only on the specified origin.

Implement in Apache, IBM HTTP Server

- Login to Apache or IHS server
- Take a backup of configuration file
- Add following line in `httpd.conf` file

```
Header always append X-Frame-Options SAMEORIGIN
```

- Restart respective web server to test the application

Implement in Shared Web Hosting

If your website is hosted on shared web hosting (https://www.siteground.com/index.htm?afcode=4f8d16df8f11e30b0e41557ee8ab1afc), then you won’t have permission to modify httpd.conf.

However, you can achieve this by adding following line in **.htaccess** file.

```
Header append X-FRAME-OPTIONS "SAMEORIGIN"
```

Change is reflected immediately without doing any restart.

Verification

You can use any web developer tool to view Response headers. You can also use an online tool – Header Checker (https://siterelic.com/tools/x-frame-options-test) to verify.

How did it go?

If you are running an online business, then you may consider using Cloud WAF (https://geekflare.com/web-application-firewall/) for all-in-one security protection and monitoring.

f | 🐦 | ◘ | in | 17 SHARES

About Chandan

Chandan Kumar is the founder and editor of Geek Flare. Learn more here (https://geekflare.com/about/) and connect with him on Twitter.

🐦 (https://twitter.com/ConnectCK)

You'll also like:

(https://geekflare.com/html5-changing-web-security/)

How HTML5 is Changing Web Security? (https://geekflare.com/html5-changing-web-security/)

(https://geekflare.com/tomcat-ssl-guide/)

How to Implement SSL in Apache Tomcat? (https://geekflare.com/tomcat-ssl-guide/)

Comments

Pavithra S *says*
DECEMBER 7, 2017 AT 8:53 PM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-46465)

Hi Chandan

added the below code in httpd.conf file but still could not see x-frame-options in response header in browser.
apache server used : httpserver_2.4.27

Header always append X-Frame-Options SAMEORIGIN

REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=46465#RESPOND)

> Pavithra S *says*
> **DECEMBER 7, 2017 AT 8:56 PM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-46466)**
>
> Header always append X-Frame-Options SAMEORIGIN
>
> **REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=46466#RESPOND)**

> **CHANDAN KUMAR (HTTPS://CHANDAN.IO/)** *says*
> **DECEMBER 9, 2017 AT 7:31 AM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-46554)**
>
> Hello Pavithra, Do you see any error? To me, it works.
>
> **REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=46554#RESPOND)**

Greg *says*
MAY 17, 2017 AT 6:09 PM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-39002)

Hi,
Thanks for the info! ☺
I have one question. Would it be possible to provide mor than one uri for the option 3:
"ALLOW-FROM uri: This setting will allow page to be displayed only on the specified origin."

I need at least 2 servers to make it work.

Kind regards,
Greg

REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=39002#RESPOND)

> **CHANDAN KUMAR (HTTP://CHANDAN.IO/)** *says*
> **MAY 18, 2017 AT 7:08 PM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-39028)**
>
> Hello Greg,
>
> I haven't tested multiple URI but looks like it's supported – https://tools.ietf.org/html/rfc7034#section-2.3.2.3 (https://tools.ietf.org/html/rfc7034#section-2.3.2.3)
>
> **REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=39028#RESPOND)**

Sreedhar Gajula *says*
NOVEMBER 3, 2016 AT 6:15 AM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-31350)

Hi Chandan – Thanks for the posting this article.
Do you know a way to implement X-FRAME-OPTIONS on Tomcat 7.0.59.0 running on Windows?
Thanks

REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=31350#RESPOND)

> **CHANDAN KUMAR (HTTPS://GEEKFLARE.COM)** *says*
> **NOVEMBER 5, 2016 AT 3:37 PM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-31411)**
>
> Hello Sreedhar,
>
> I haven't tried that yet in Tomcat so can't confirm. But I will see if I can and write about it. Thanks for visiting.
>
> **REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=31411#RESPOND)**

STEVE PRINGLE (HTTP://WWW.NYHTML.COM/) *says*
NOVEMBER 15, 2015 AT 5:35 PM (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/#COMMENT-1800)

We (found the 'Header Checker' tool very useful as it
(1) showed that three Apache servers was using DENY instead of SAMEORIGIN and
(2) that PHP versions were ranging from PHP/5.4.16 – PHP/5.4.28

REPLY (HTTPS://GEEKFLARE.COM/SECURE-APACHE-FROM-CLICKJACKING-WITH-X-FRAME-OPTIONS/?REPLYTOCOM=1800#RESPOND)