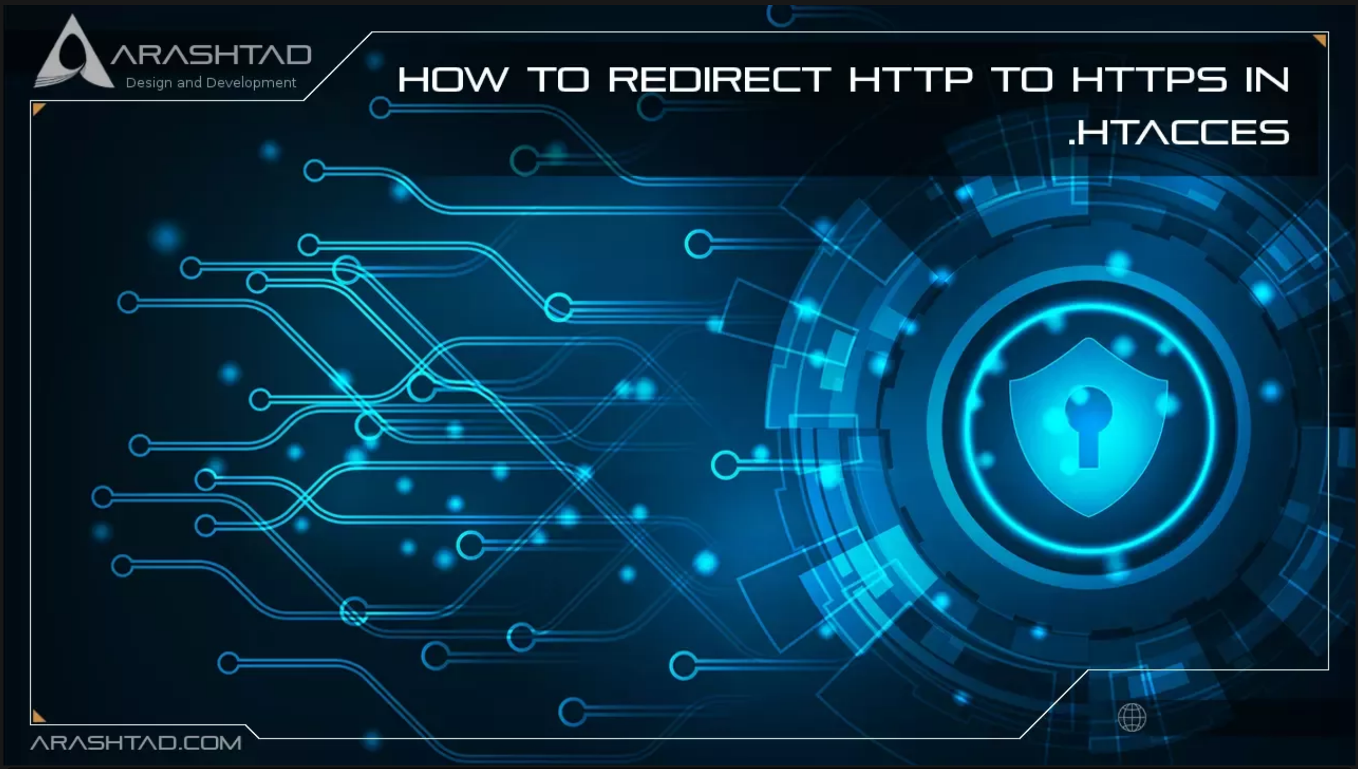
How to Redirect HTTP to HTTPS in .htacces

No comments



For sites without SSL certificates, Chrome and Firefox now display insecure warnings. Without SSL, your website will appear insecure to your visitors. Therefore, encrypting the connection with SSL is necessary for safety, accessibility, or PCI compliance. Redirection from HTTP to HTTPS becomes very important.

What is HTTP?

It is through the Hypertext Transfer Protocol (HTTP) that web browsers and servers can exchange data in order to communicate. This network protocol standard is called the Transmission Control Protocol (TCP). As a stateless system, HTTP enables connections on demand and does not require constant connections. Whenever a user clicks a link on their system, it requests a connection to the server. After the server responds to the request, the user sees the data on their web browser.

The speed of this connection depends on how fast the server is connected to the system. It is also an "application layer protocol," which means that it strives to preserve the clarity of the information it transmits. While this allows a reliable connection to servers, it can also allow malicious actors to intercept the data during transmission, allowing them to read and modify it. Known as a "Man-in-the-Middle Attack," this requires a secure way of communicating over the Internet. That's where HTTPS comes in.

What is HTTPS?

HTTPS is the secure version of HTTP, which is commonly used to transfer data between web browsers and websites. HTTPS is encrypted in order to increase the security of data transfers. When users are logging into their bank accounts, email services, or health insurance providers, this is particularly important. A website that requires login credentials should use HTTPS. Chrome, for instance, marks websites that do not use HTTPS differently from websites that do. Look for the padlock in the URL bar to indicate the site is secure. HTTPS is taken seriously by web browsers. Google Chrome and other browsers flag non-HTTPS sites as unsafe.

The Importance of Redirecting HTTP to HTTPS

Using HTTPS, websites' information is not broadcast in a way that can be easily viewed by anyone snooping on the network. When information is sent over regular HTTP, it is broken into packets of data that can be easily sniffed using free software. This makes communication over an unsecure medium, like public Wi-Fi, highly vulnerable to interception. In fact, all communication over HTTP occurs in plain text, making them highly accessible to anyone with the right tools, and susceptible to on-path attacks.

The HTTPS protocol encrypts traffic so that even if the packets are sniffed or intercepted, they appear as nonsensical data. A website without HTTPS may be injected with content by Internet service providers (ISPs) or other intermediaries without the website owner's permission. It is common for ISPs to inject paid advertising into their customers' web pages in an attempt to increase revenue. Consequently, when this occurs, the website owner does not receive any profit from the advertisements or control over their quality. HTTPS prevents unmoderated third parties from injecting ads into web content.

What Is SSL?

In online communication, SSL (Secure Sockets Layer) establishes encrypted links between a web server and a browser. By using SSL technology, all data transmitted between the browser and the web server is encrypted. An SSL certificate is essential for creating an SSL connection. You will need to provide all the details regarding your website and company once you activate SSL on your web server. Once this is done, two cryptographic keys are created: a Public Key and a Private Key. In order to force HTTPS on your website, edit the .htaccess file. Let's go over how to edit the .htaccess file before redirecting HTTP to HTTPS.

Image not found or type unknown

How to Redirect HTTP to HTTPS in .htacces

.htaccess File Editing

The .htaccess file contains instructions/directives that tell the server how to act in certain situations and directly impact how your website functions. The most common directives are as follows:

- Redirects
- Rewriting URLs

Editing a .htaccess file involves the following steps:

1. Transmit the file via FTP to the server after editing it on your computer.

2. Edit files remotely using the "Edit" mode in the FTP program.

3. Edit the file using a text editor and SSH.

4. cPanel's File Manager can be used to make changes to the file.

Using the cPanel File Manager to Edit .htaccess

Ensure that you backup your website in case anything goes wrong.

1. Enter Your cPanel account

2. Files > File Manager > Document Root

3. The next step is to choose the domain name that you want to access

4. Now you should check “Show Hidden Files (dotfiles)”

5. Click on the “Go”

6. You can find the .htaccess file after opening a new tab or window.

7. You can edit the .htaccess file by right-clicking and selecting “Code Edit ”.

8. Click "Edit" after you see a dialogue box asking about encoding.

9. Edit the file

10. Next, “Save Changes” when completed.

11.You should test your website to make sure it is working properly. Try again if there is an error. revert to the previous version in case of an error. You can close the window by clicking "Close" once you are finished.

How to Redirect HTTP to HTTPS in .htaccess?

1.You should redirect all web traffic

If any code exists in .htaccess, add the lines below:

```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.yourdomain.com/$1 [R,L]
```

2. Next, you should redirect only a specific domain

You can redirect a specific domain to use HTTPS by adding the following code:

```
RewriteEngine On
RewriteCond %{HTTP_HOST} ^yourdomain\.com [NC]
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.yourdomain.com/$1 [R,L]
```

3. Redirect only a specific folder On a certain folder, redirect to HTTPS as follows:

```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteCond %{REQUEST_URI} folder
RewriteRule ^(.*)$ https://www.yourdomain.com/folder/$1 [R,L]
```

Note: You should Replace “yourdomain” with your actual domain name wherever it is necessary. Moreover, about the folder, replace /folder with the actual folder name.

Conclusion

Most sensitive websites switched to HTTPS years ago and all other sites are evolving over time. Eventually, browser pressures will force all sites to switch HTTP to HTTPS, and they will strongly resist even showing non-HTTPS sites. HTTPS may not be the ultimate data transfer protocol. Currently, HTTPS stands above HTTP, but one day it might be enhanced or replaced by another protocol. Cybersecurity continues to evolve and advance as new data security issues and limitations arise.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.

Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP NEWSLETTER RSS FEED