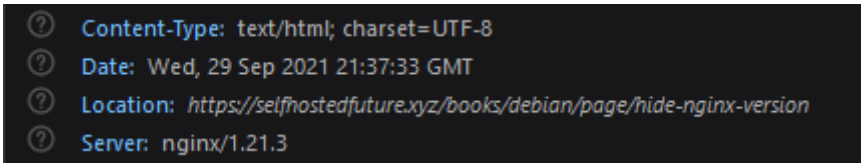
Hide Nginx version

Test if your website sends `Server` header

When you make a request to a Nginx-powered website, by default, every response will contain Nginx's server version in a `Server` header. You can test this by opening *developer options* in your browser (`F12` in Firefox) and looking at the requests in the *Network* tab.



Other method is to use `curl`:

```
$ curl -IL https://selfhostedfuture.xyz
```

The output shows a similar result:

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
...
```

Hide Nginx version from `Server` header

Even though exposing the server's Nginx version isn't a huge security threat, it makes it easier for attackers to find exploits and vulnerabilities specifically for the given version. This is especially important if you forget updating your server for a while.

> Hiding Nginx's version is *Security Through Obscurity*, since more advanced attackers are able to find what they want anyway

Edit Nginx configuration

Open the Nginx configuration file in `/etc/nginx/nginx.conf`:

```
$ sudo vi /etc/nginx/nginx.conf
```

By default, your config will look something like this (settings here can be overwritten by configuration in `/etc/nginx/conf.d`):

```
user  nginx;
worker_processes  auto;

error_log  /var/log/nginx/error.log notice;
pid        /var/run/nginx.pid;


events {
    worker_connections  1024;
}


http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    #gzip  on;

    include /etc/nginx/conf.d/*.conf;
}
```

Focus on the `http` server block and add the `server_tokens` directive and set it to `off`:

```
server_tokens off;
```

Like this:

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    server_tokens off;
    ....
```

Test configuration

Before restarting, check that you haven't made a mistake in the configuration:

```
$ sudo nginx -t
```

Proceed if the output looks like this:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

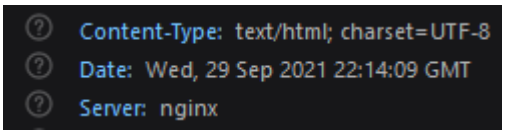
Restart Nginx

Restart Nginx for the changes to take effect:

```
$ sudo systemctl restart nginx
```

Confirm the change

Look into the *Network* tab again, or use `curl` to see whether Nginx still reports the version. It is also possible to completely hide the fact that the website is Nginx powered, but that is for another post.




```
$ curl -IL https://selfhostedfuture.xyz
```

```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
```

Revision #4
Created 29 September 2021 23:36:48 by Marek
Updated 30 September 2021 00:33:56 by Marek