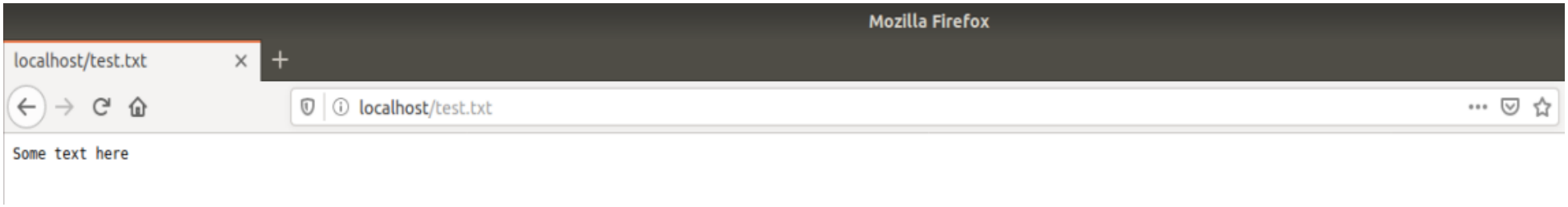
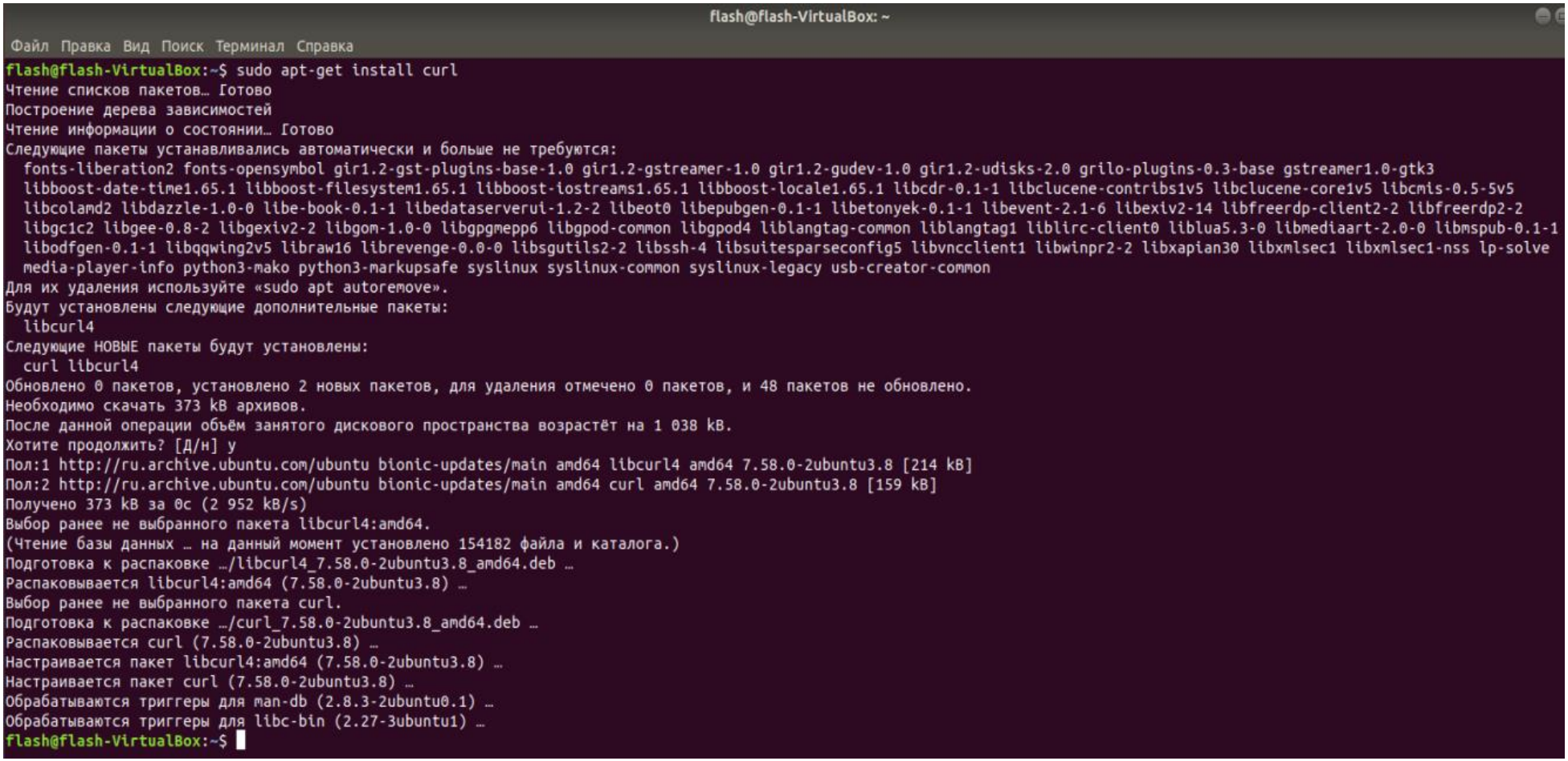
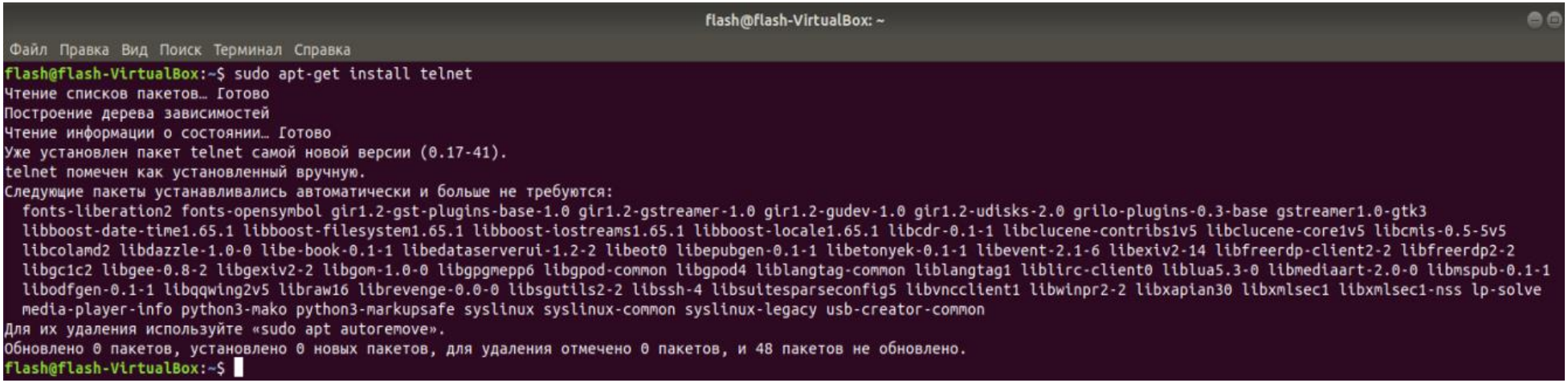
1. Создан файл test.txt, получен через браузер



Установлены программы curl и telnet и получен файл через эти программы в терминале






```
flash@flash-VirtualBox:~$ curl 127.0.0.1/test.txt
Some text here
```

```
flash@flash-VirtualBox:~$ telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /test.txt HTTP/1.1
Host: localhost

HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 27 Mar 2020 15:41:33 GMT
Content-Type: text/plain
Content-Length: 15
Last-Modified: Fri, 27 Mar 2020 15:30:02 GMT
Connection: keep-alive
ETag: "5e7e1bfa-f"
Accept-Ranges: bytes

Some text here
```

2. Создан файл sensitive_info.txt

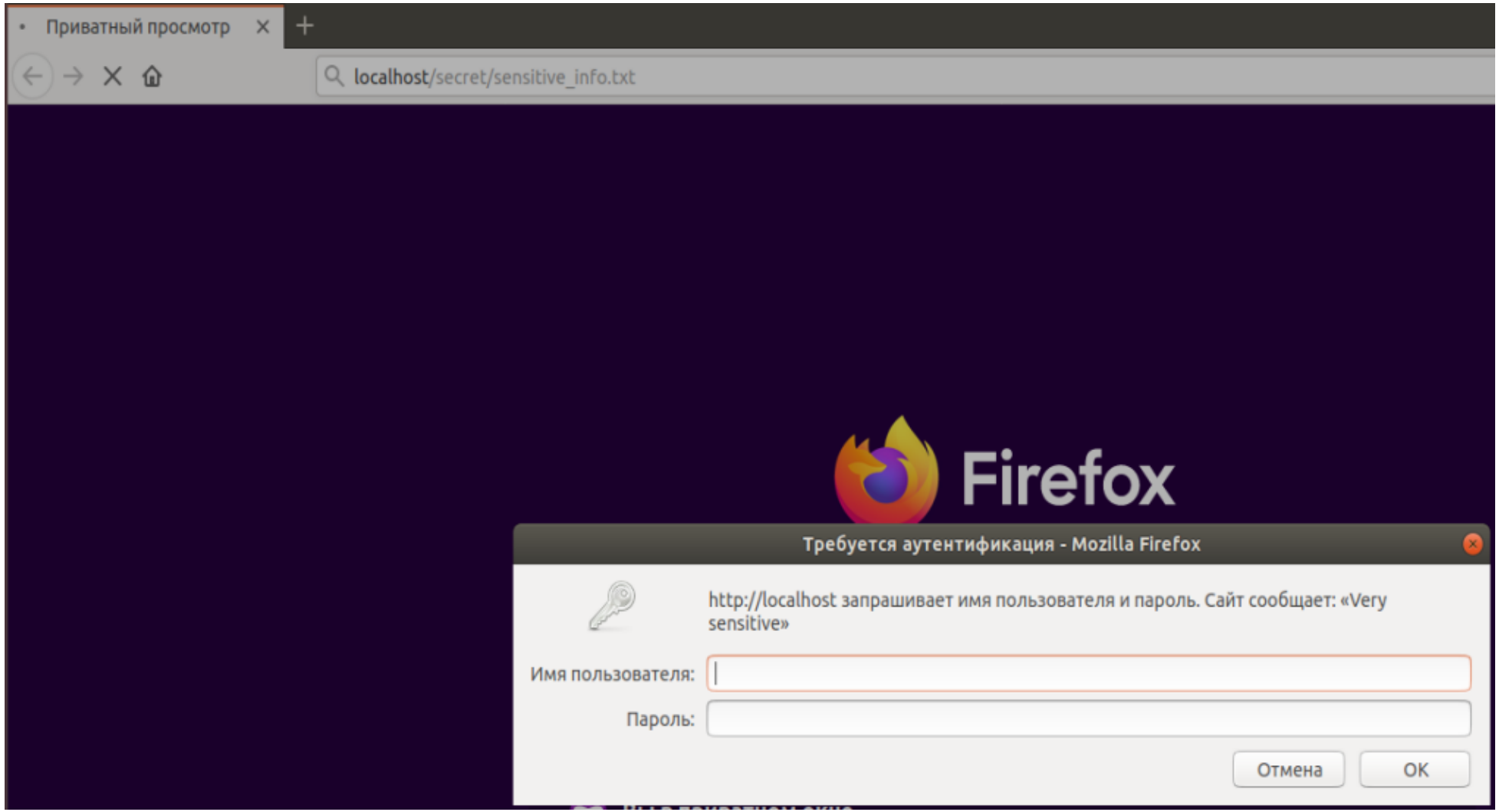
```
flash@flash-VirtualBox:/var/www/html/secret$ ls
sensitive_info.txt
```

Добавлена базовая авторизация для директории /secret

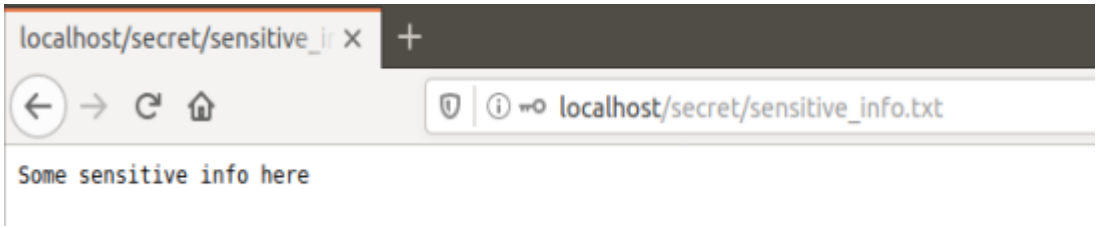
```
flash@flash-VirtualBox:/var/www/html/secret$ sudo htpasswd -c /var/www/pass flosh
New password:
Re-type new password:
Adding password for user flosh
```

```
server {
        listen 80;
        listen [::]:80;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name localhost;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }

        location /secret/ {
                auth_basic      "Very sensitive";
                auth_basic_user_file /var/www/pass;
        }
```

При обращении к файлу браузер просит авторизоваться



После ввода логина пароля получен доступ к файлу

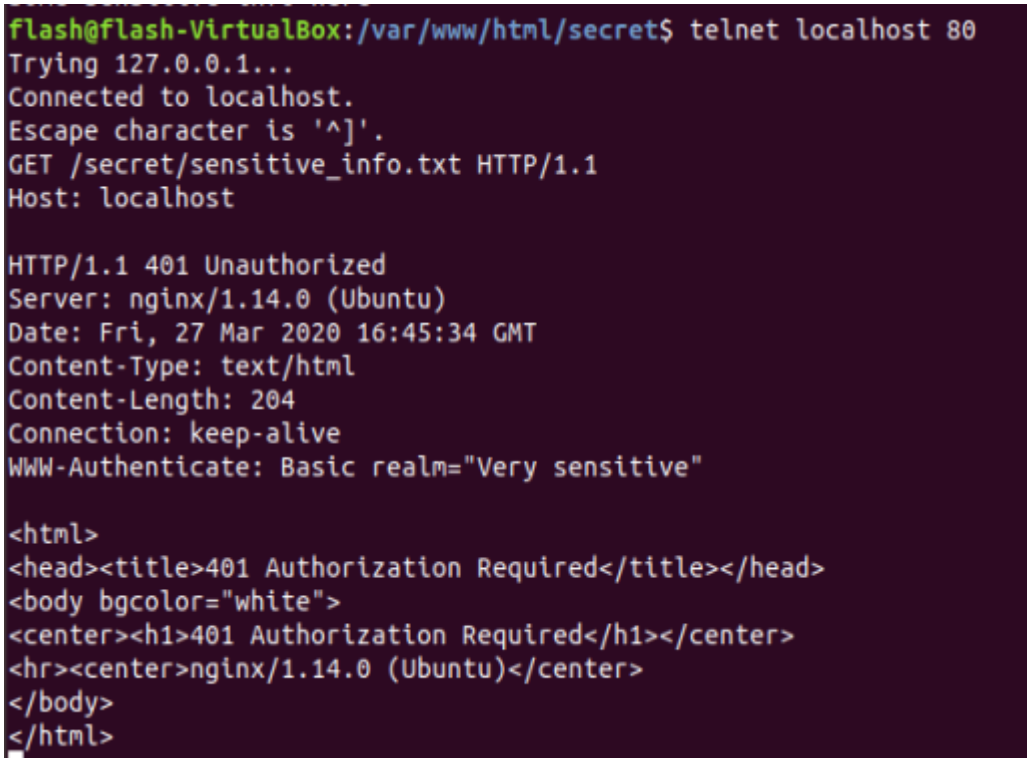


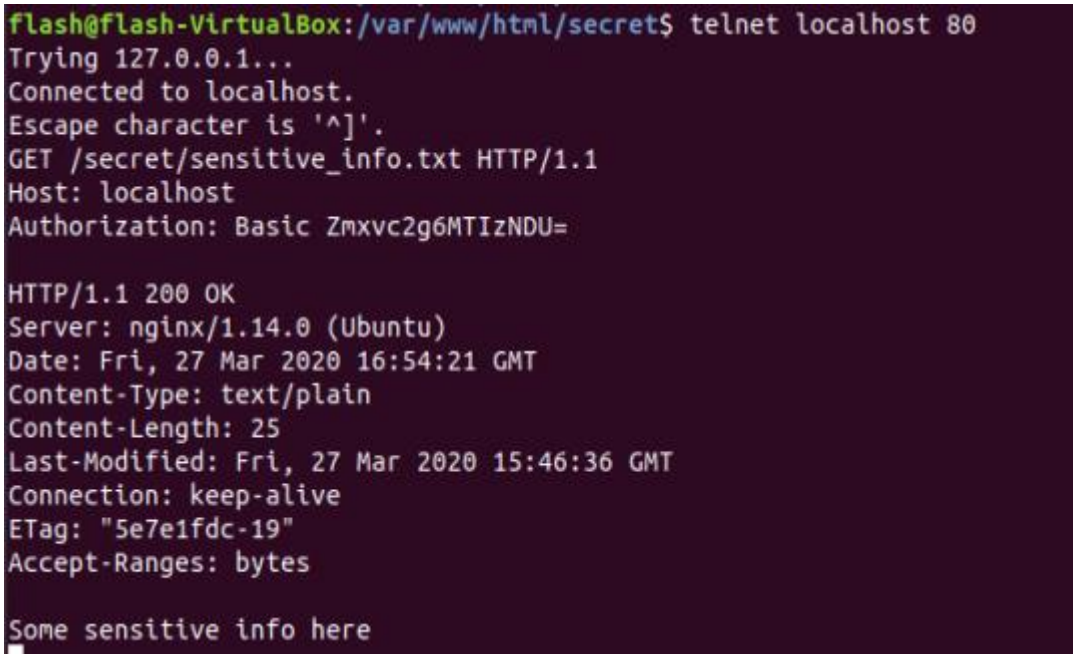
Файл получен через curl

```
flash@flash-VirtualBox:/var/www/html/secret$ curl localhost/secret/sensitive_info.txt
<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
```

```
flash@flash-VirtualBox:/var/www/html/secret$ curl localhost/secret/sensitive_info.txt -u "flosh:12345"
Some sensitive info here
```

И через telnet

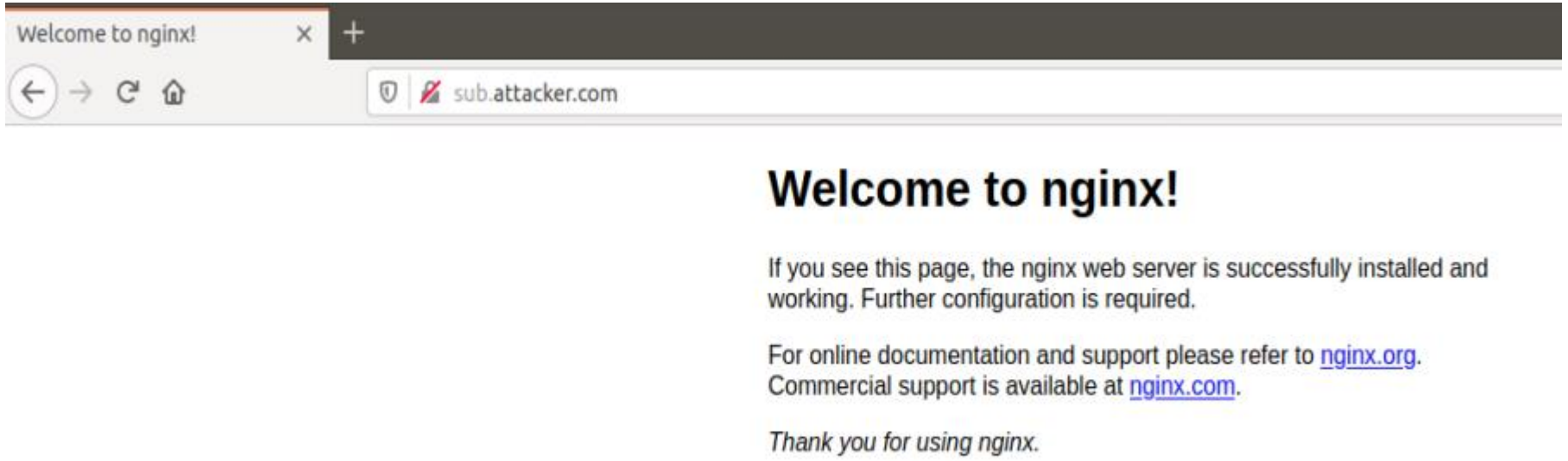




3. Запросы к HTML как правило уходят с куками, так как генерация страницы зависит от информации о пользователе (авторизован ли, какие курсы он проходит и т.д.), а статичные картинки как правило уходят без кук, т.к. они подтягиваются на основе HTML. Если картинка генерируется каким-то скриптом, то она тоже может сопровождаться куками.

4. В файл hosts внесены изменения, чтобы домены attacker.com, sub.attacker.com, sub.sub.attacker.com, victim.com указывали на 127.0.0.1

Например, при попытке перехода по адресу sub.attacker.com открывается наша приветственная страница



Добавлен конфигурационный файл /etc/nginx/sites-available/cookie-research.conf с парой дополнительных тестов

```
server {
    listen 80;
    server_name attacker.com;
    root /var/www/html;
    index index.test.html;
    location / {
        add_header "Set-Cookie" "test1=attacker-com_sub-attacker-com; Domain=sub.attacker.com";
        add_header "Set-Cookie" "test2=attacker-com_victim-com;       Domain=victim.com";
        add_header "Set-Cookie" "test5=attacker-com_attacker-com;     Domain=attacker.com";
        add_header "Set-Cookie" "test6=attacker-com";
        add_header Cache-Control no-cache;

        try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    server_name victim.com;
    root /var/www/html;
    index index.test.html;

    location / {
        try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    server_name sub.attacker.com;
    root /var/www/html;
    index index.test.html;

    location / {
        add_header "Set-Cookie" "test3=sub-attacker-com_attacker-com; Domain=attacker.com";
        try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    server_name sub.sub.attacker.com;
    root /var/www/html;
    index index.test.html;

    location / {
        add_header "Set-Cookie" "test4=sub-sub-attacker-com_attacker-com; Domain=attacker.com";
        try_files $uri $uri/ =404;
    }
}
```

Пришлось добавить строчку для каждого домена

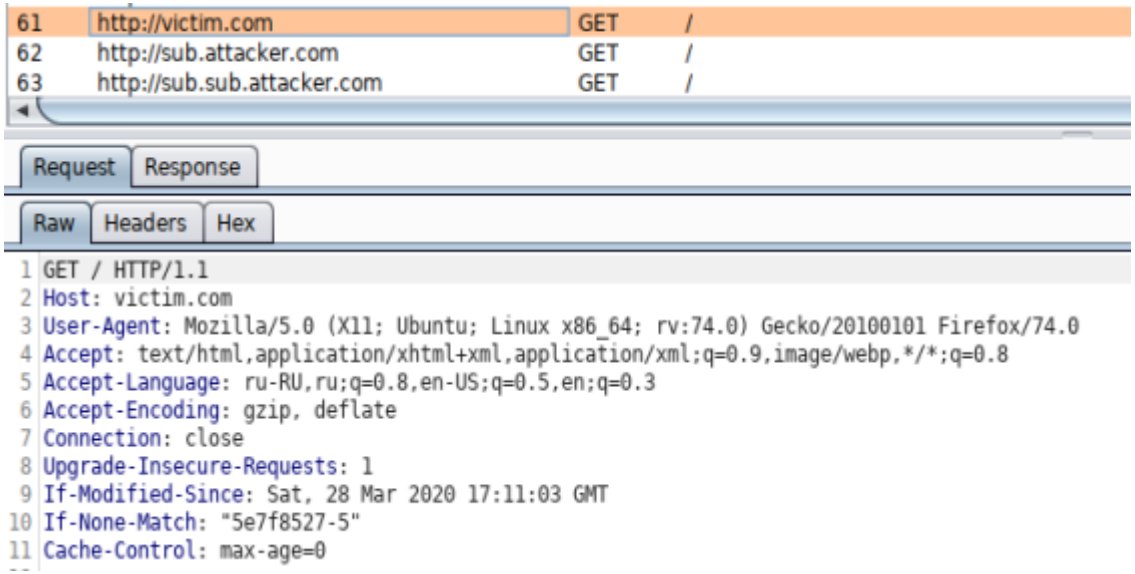
```
index index.test.html;
```

Иначе страница не открывалась, выдавая ошибку 403

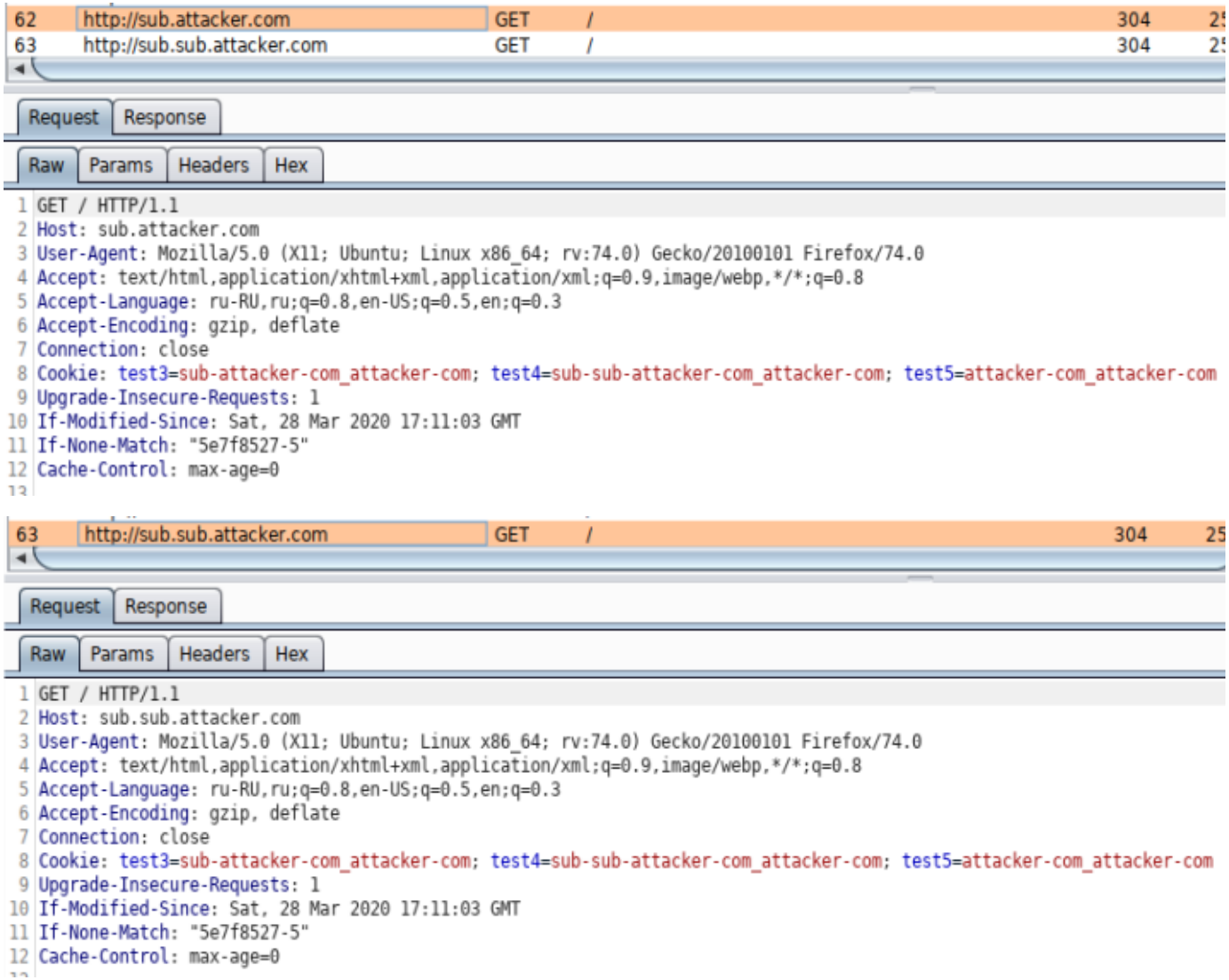
Исследование механизма проставления кук

test1: Кука с домена на поддомен не устанавливается

test2: Кука с домена на другой домен не устанавливается



test3, test4: Кука с поддоменов устанавливается на домен



62	http://sub.attacker.com	GET	/	304	25
63	http://sub.sub.attacker.com	GET	/	304	25

Request | Response

Raw | Params | Headers | Hex

```
1  GET / HTTP/1.1
2  Host: sub.attacker.com
3  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:74.0) Gecko/20100101 Firefox/74.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: test3=sub-attacker-com_attacker-com; test4=sub-sub-attacker-com_attacker-com; test5=attacker-com_attacker-com
9  Upgrade-Insecure-Requests: 1
10 If-Modified-Since: Sat, 28 Mar 2020 17:11:03 GMT
11 If-None-Match: "5e7f8527-5"
12 Cache-Control: max-age=0
```

63	http://sub.sub.attacker.com	GET	/	304	25

Request | Response

Raw | Params | Headers | Hex

```
1  GET / HTTP/1.1
2  Host: sub.sub.attacker.com
3  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:74.0) Gecko/20100101 Firefox/74.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: test3=sub-attacker-com_attacker-com; test4=sub-sub-attacker-com_attacker-com; test5=attacker-com_attacker-com
9  Upgrade-Insecure-Requests: 1
10 If-Modified-Since: Sat, 28 Mar 2020 17:11:03 GMT
11 If-None-Match: "5e7f8527-5"
12 Cache-Control: max-age=0
```

test5: Кука, установленная доменом на себя, устанавливается на себя и на поддомены, что видно из продемонстрированных скриншотов

test6: Кука, установленная без указания домена, устанавливается только на сам домен (на поддомены не устанавливается), см. выше

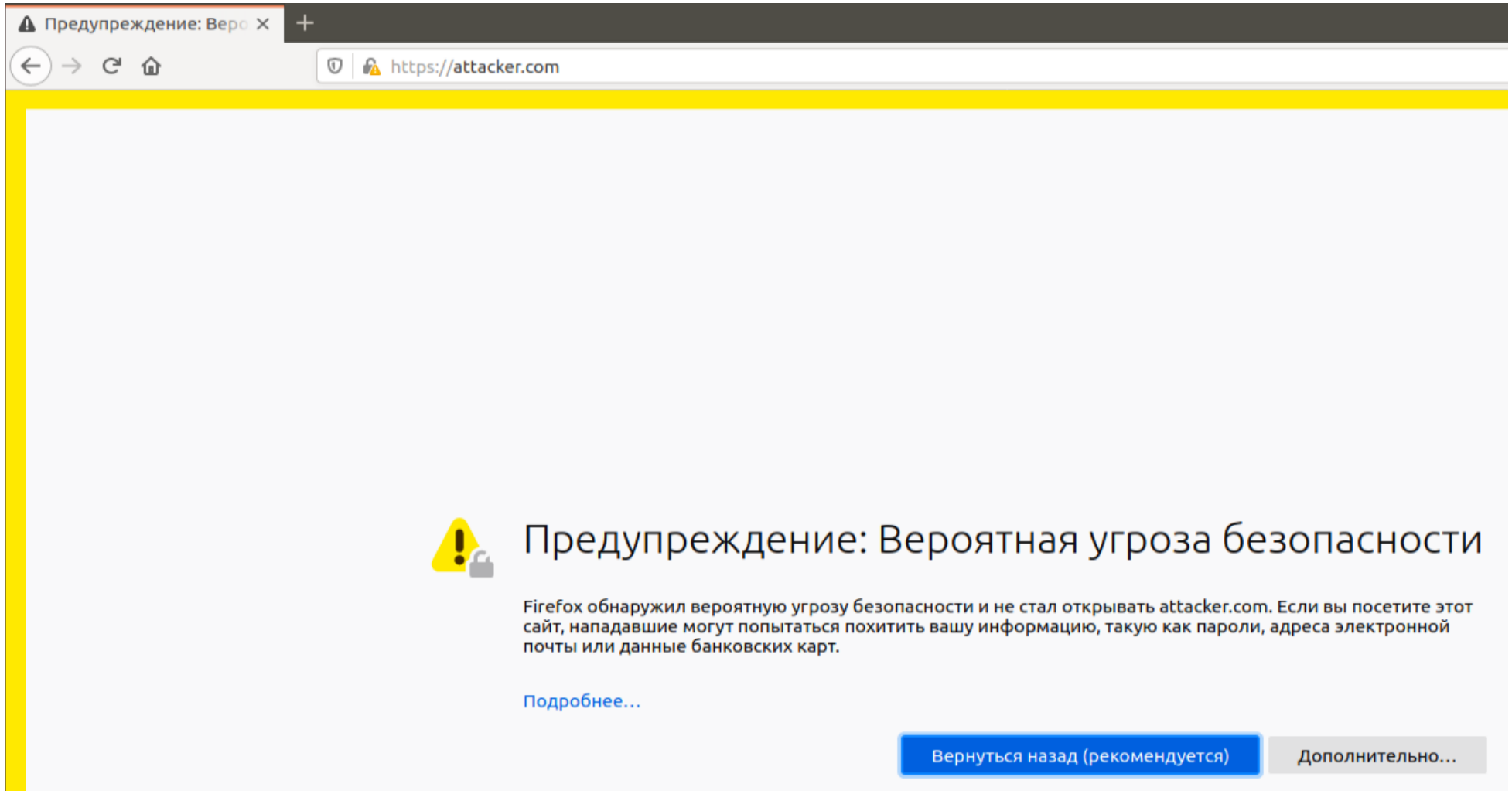
Вывод: Домен может проставлять куки для себя, для родительского домена и для директории при использовании параметра path (кука установится для директории и всех вложенных в нее), но не может проставлять куки для поддоменов и других сайтов.

5. Самоподписанный сертификат сгенерирован по инструкции https://abc-server.com/ru/blog/administration/creating-ssl-for-nginx-in-ubuntu-1604/

в конфигурационный файл nginx добавлены параметры для ssl-сертификатов

```
server {
    listen 80;
    server_name your-ssl-site-here.com;

    root /var/www/html;
    listen 443 ssl;
    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;

    location / {
     try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    listen 443 ssl;
    root /var/www/html;
    server_name attacker.com;
    index index.test.html;
    include snippets/self-signed.conf;
    include snippets/ssl-params.conf;
    location / {
        add_header "Set-Cookie" "test1=attacker-com_sub-attacker-com; Domain=sub.attacker.com";
        add_header "Set-Cookie" "test2=attacker-com_victim-com;       Domain=victim.com";
        add_header Cache-Control no-cache;

        try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    server_name victim.com;
    root /var/www/html;

    location / {
        try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    server_name sub.attacker.com;
    root /var/www/html;

    location / {
        add_header "Set-Cookie" "test3=sub-attacker-com_attacker-com; Domain=attacker.com";
        try_files $uri $uri/ =404;
    }
}
```

При обращении к сайту появляется предупреждение о несоответствии сертификата



Информация о сертификате