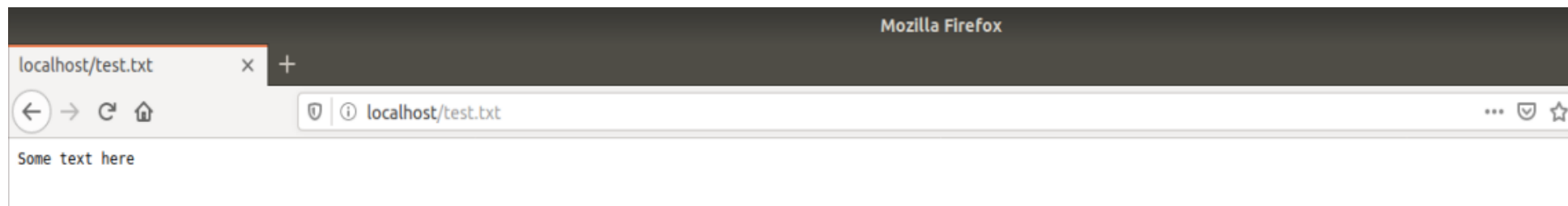


1. Создан файл test.txt, получен через браузер



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

```
flash@flash-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
flash@flash-VirtualBox:~$ sudo apt-get install curl  
Чтение списков пакетов... Готово  
Построение дерева зависимостей  
Чтение информации о состоянии... Готово  
Следующие пакеты устанавливались автоматически и больше не требуются:  
  fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3  
  libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1 libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5  
  libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libdataserverui-1.2-2 libeot0 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreedp-client2-2 libfreedp2-2  
  libgc1c2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmsspub-0.1-1  
  libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxapian30 libxmlsec1 libxmlsec1-nss lp-solve  
  media-player-info python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy usb-creator-common  
Для их удаления используйте «sudo apt autoremove».  
Будут установлены следующие дополнительные пакеты:  
  libcurl4  
Следующие НОВЫЕ пакеты будут установлены:  
  curl libcurl4  
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 48 пакетов не обновлено.  
Необходимо скачать 373 kB архивов.  
После данной операции объём занятого дискового пространства возрастёт на 1 038 kB.  
Хотите продолжить? [д/н] у  
Пол:1 http://ru.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libcurl4 amd64 7.58.0-2ubuntu3.8 [214 kB]  
Пол:2 http://ru.archive.ubuntu.com/ubuntu bionic-updates/main amd64 curl amd64 7.58.0-2ubuntu3.8 [159 kB]  
Получено 373 kB за 0с (2 952 kB/s)  
Выбор ранее не выбранного пакета libcurl4:amd64.  
(Чтение базы данных ... на данный момент установлено 154182 файла и каталога.)  
Подготовка к распаковке .../libcurl4_7.58.0-2ubuntu3.8_amd64.deb ...  
Распаковывается libcurl4:amd64 (7.58.0-2ubuntu3.8) ...  
Выбор ранее не выбранного пакета curl.  
Подготовка к распаковке .../curl_7.58.0-2ubuntu3.8_amd64.deb ...  
Распаковывается curl (7.58.0-2ubuntu3.8) ...  
Настраивается пакет libcurl4:amd64 (7.58.0-2ubuntu3.8) ...  
Настраивается пакет curl (7.58.0-2ubuntu3.8) ...  
Обрабатываются триггеры для man-db (2.8.3-2ubuntu0.1) ...  
Обрабатываются триггеры для libc-bin (2.27-3ubuntu1) ...  
flash@flash-VirtualBox:~$
```

flash@flash-VirtualBox: ~

Файл Правка Вид Поиск Терминал Справка

```
flash@flash-VirtualBox:~$ sudo apt-get install telnet
```

Чтение списков пакетов... Готово

Построение дерева зависимостей

Чтение информации о состоянии... Готово

Уже установлен пакет telnet самой новой версии (0.17-41).

telnet помечен как установленный вручную.

Следующие пакеты устанавливались автоматически и больше не требуются:

```
fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3
libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1 libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5
libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2
libgc1c2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmspub-0.1-1
libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxapian30 libxmlsec1 libxmlsec1-nss lp-solve
media-player-info python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy usb-creator-common
```

Для их удаления используйте «sudo apt autoremove».

Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 48 пакетов не обновлено.

```
flash@flash-VirtualBox:~$
```

```
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 '^J'.

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

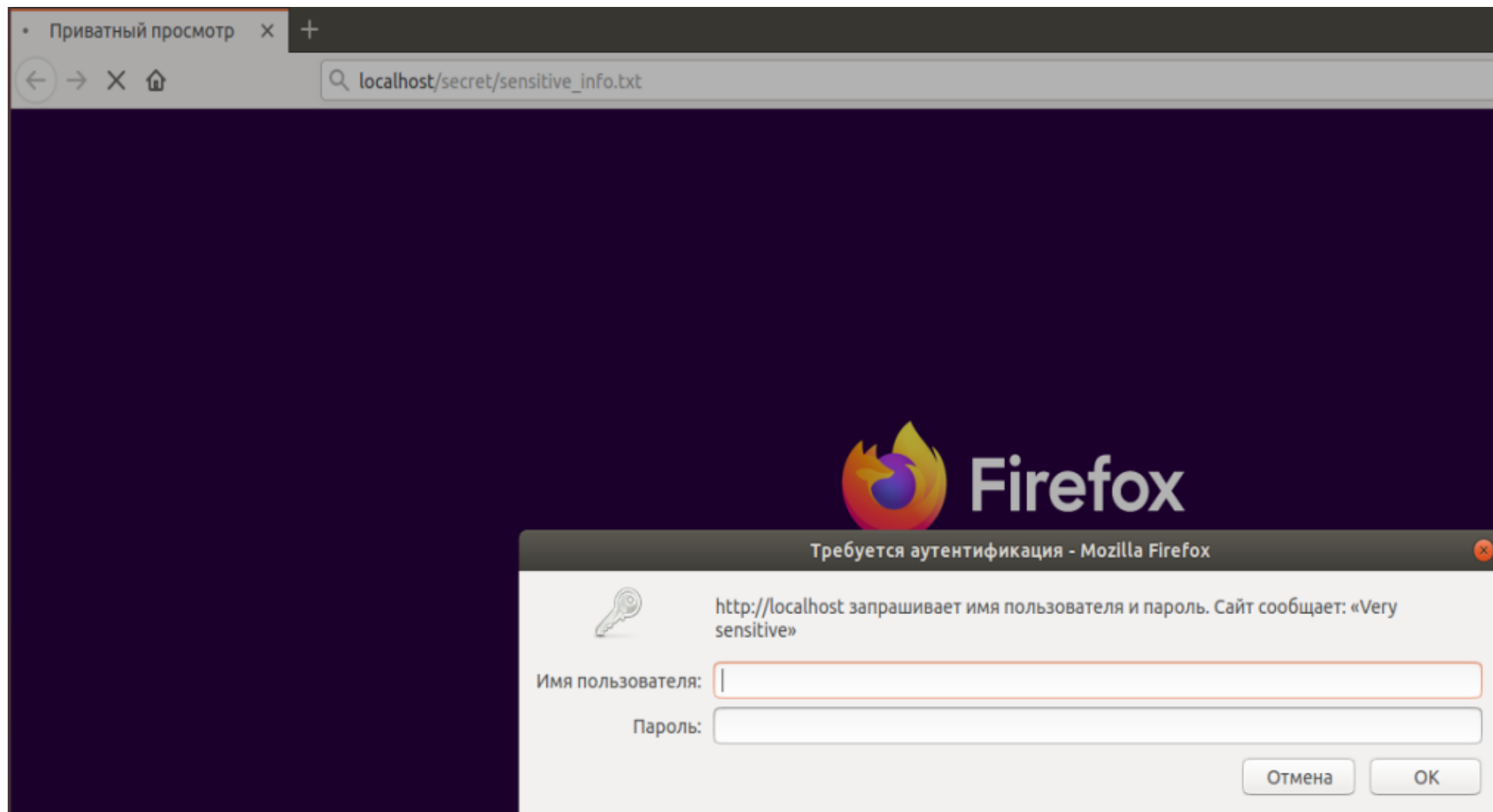
```
flash@flash-VirtualBox:/var/www/html/secret$ ls  
sensitive_info.txt
```

Добавлена базовая авторизация для директории /secret

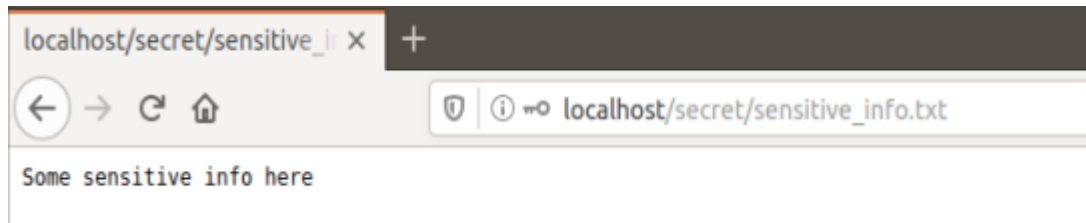
```
flash@flash-VirtualBox:/var/www/html/secret$ sudo htpasswd -c /var/www/pass flosch  
New password:  
Re-type new password:  
Adding password for user flosch
```

```
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 "flosch:12345"
Some sensitive info here
```

И через telnet

```
flash@flash-VirtualBox:/var/www/html/secret$ telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /secret/sensitive_info.txt HTTP/1.1
Host: localhost

HTTP/1.1 401 Unauthorized
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 27 Mar 2020 16:45:34 GMT
Content-Type: text/html
Content-Length: 204
Connection: keep-alive
WWW-Authenticate: Basic realm="Very sensitive"

<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$ telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /secret/sensitive_info.txt HTTP/1.1
Host: localhost
Authorization: Basic Zmxvc2g6MTIzNDU=

HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 27 Mar 2020 16:54:21 GMT
Content-Type: text/plain
Content-Length: 25
Last-Modified: Fri, 27 Mar 2020 15:46:36 GMT
Connection: keep-alive
ETag: "5e7e1fdc-19"
Accept-Ranges: bytes

Some sensitive info here
```

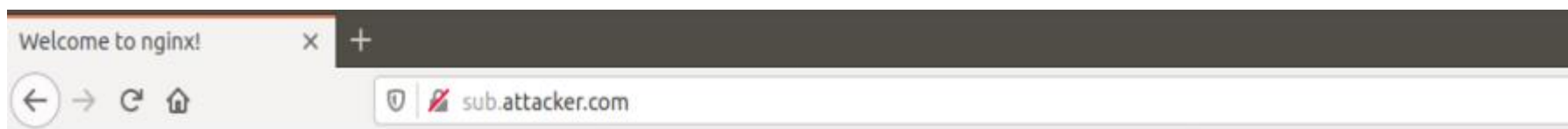
3. Запросы к HTML как правило уходят с куками, так как генерация страницы зависит от информации о пользователе (авторизован ли, какие курсы он проходит и т.д.), а статичные картинки как правило уходят без кук, т.к. они подтягиваются на основе HTML. Если картинка генерируется каким-то скриптом, то она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

```
flash@flash-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
127.0.0.1      victim.com attacker.com sub.attacker.com sub.sub.attacker.com  
127.0.0.1      localhost  
127.0.1.1      flash-VirtualBox  
  
# The following lines are desirable for IPv6 capable hosts  
::1          ip6-localhost ip6-loopback  
fe00::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters
```

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



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

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

60	http://attacker.com	GET	/	304	451
61	http://victim.com	GET	/	304	182
62	http://sub.attacker.com	GET	/	304	252
63	http://sub.sub.attacker.com	GET	/	304	256

RequestResponse

RawParamsHeadersHex

1GET / HTTP/1.1

2Host: attacker.com

3User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:74.0) Gecko/20100101 Firefox/74.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

5Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3

6Accept-Encoding: gzip, deflate

7Connection: close

8Cookie: test3=sub-attacker-com\_attacker-com; test4=sub-sub-attacker-com\_attacker-com; test5=attacker-com\_attacker-com; test6=attacker-com

9Upgrade-Insecure-Requests: 1

10If-Modified-Since: Sat, 28 Mar 2020 17:11:03 GMT

11If-None-Match: "5e7f8527-5"

12Cache-Control: max-age=0

test2: Кука с домена на другой домен не устанавливается

61	http://victim.com	GET	/
62	http://sub.attacker.com	GET	/
63	http://sub.sub.attacker.com	GET	/

RequestResponse

RawHeadersHex

1 GET / HTTP/1.1

2 Host: victim.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 Upgrade-Insecure-Requests: 1

9 If-Modified-Since: Sat, 28 Mar 2020 17:11:03 GMT

10 If-None-Match: "5e7f8527-5"

11 Cache-Control: max-age=0

--

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

13

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

13

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;

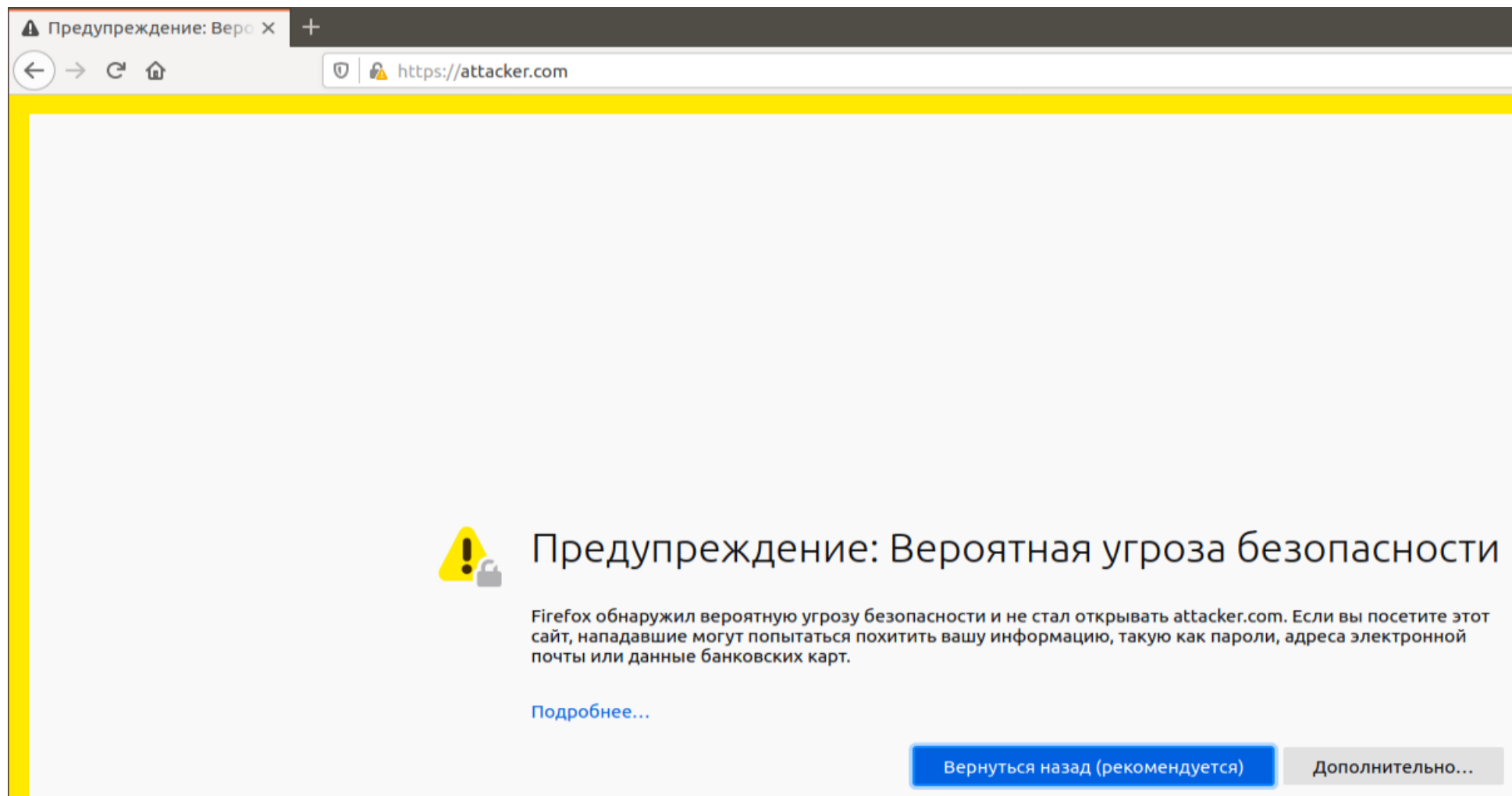
    location / {
        try_files $uri $uri/ =404;
    }
}

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

test.localhost

Субъект	_____
Страна	ru
Область/Край/Республика	spb
Местонахождение	spb
Организация	none
Подразделение	none
Общее имя	test.localhost
Адрес электронной почты	none

Издатель	_____
Страна	ru
Область/Край/Республика	spb
Местонахождение	spb
Организация	none
Подразделение	none
Общее имя	test.localhost
Адрес электронной почты	none

Срок действия	_____
Действителен с	30.03.2020, 18:42:29 (Europe/Moscow)
Действителен по	30.03.2021, 18:42:29 (Europe/Moscow)

Информация об открытом ключе	_____
Алгоритм	RSA
Размер ключа	2048
Экспонента	65537
Модуль	F0:FC:2C:F3:84:0B:A6:AA:EF:9E:7C:25:E8:47:86:D3:37:58:39:24:0A:66:74:11:3A:37:DB:D6:57:F8:7F:53:4B:FE:FC...
Разное	_____
Серийный номер	66:0C:6F:3B:33:42:29:FC:97:F1:EE:72:10:91:69:FC:F2:DF:82:2A