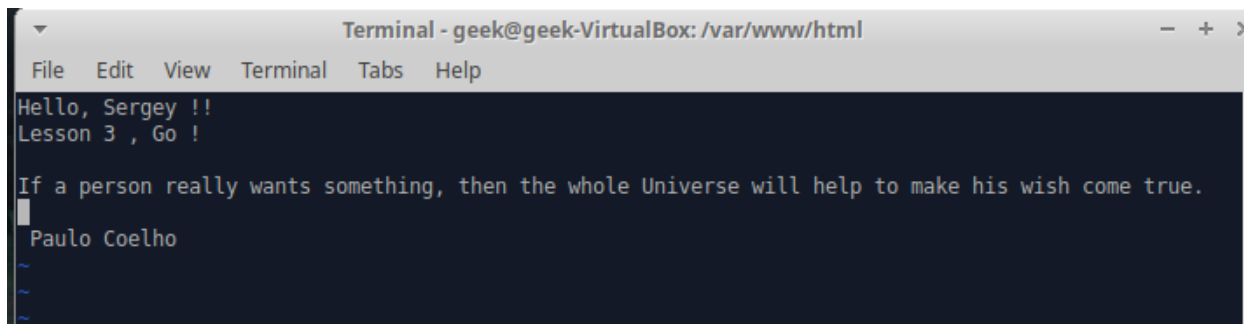


## Коротков Сергей

### Урок 3.

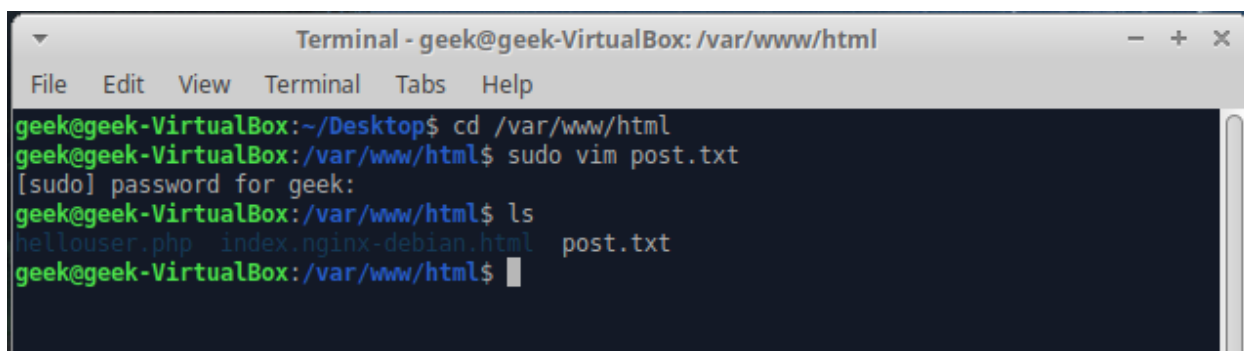
1. Создать файл test.txt в корневом каталоге сервера. Получить этот файл через браузер.

1) Создал файл test.txt



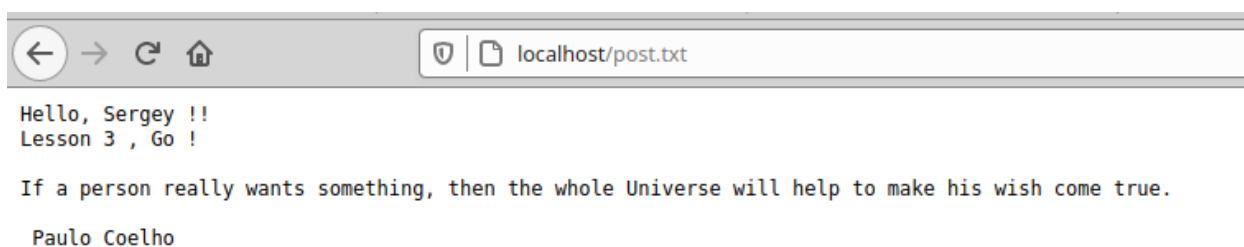
```
Terminal - geek@geek-VirtualBox: /var/www/html
File Edit View Terminal Tabs Help
Hello, Sergey !!
Lesson 3 , Go !

If a person really wants something, then the whole Universe will help to make his wish come true.
Paulo Coelho
~
~
~
```



```
Terminal - geek@geek-VirtualBox: /var/www/html
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ cd /var/www/html
geek@geek-VirtualBox:/var/www/html$ sudo vim post.txt
[sudo] password for geek:
geek@geek-VirtualBox:/var/www/html$ ls
hellouser.php  index.nginx-debian.html  post.txt
geek@geek-VirtualBox:/var/www/html$
```

2) Получил файл через браузер:



```
localhost/post.txt
Hello, Sergey !!
Lesson 3 , Go !

If a person really wants something, then the whole Universe will help to make his wish come true.

Paulo Coelho
```

Установить в терминале программу curl, получить тот же файл с помощью этой программы.

1)Получил файл при помощи программы curl:

```
geek@geek-VirtualBox:~/Desktop$ curl -v http://localhost/post.txt
* Trying 127.0.0.1:80...
* TCP_NODELAY set
* Connected to localhost (127.0.0.1) port 80 (#0)
> GET /post.txt HTTP/1.1
> Host: localhost
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< Date: Sat, 13 Feb 2021 15:17:38 GMT
< Content-Type: text/plain
< Content-Length: 147
< Last-Modified: Sat, 13 Feb 2021 12:55:03 GMT
< Connection: keep-alive
< ETag: "6027cc27-93"
< Accept-Ranges: bytes
<
Hello, Sergey !!
Lesson 3 , Go !

If a person really wants something, then the whole Universe will help to make his wish come true.

Paulo Coelho
* Connection #0 to host localhost left intact
geek@geek-VirtualBox:~/Desktop$
```

Установить telnet или netcat, получить тот же файл с помощью одной из этих программ.

1)Установил telnet, работает ошибок нет.

```
Terminal - geek@geek-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ sudo apt install telnet
[sudo] password for geek:
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnet is already the newest version (0.17-41.2build1).
telnet set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
geek@geek-VirtualBox:~/Desktop$ telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
^CConnection closed by foreign host.
```

2)Получил файл с помощью telnet:

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

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 13 Feb 2021 15:24:14 GMT
Content-Type: text/plain
Content-Length: 147
Last-Modified: Sat, 13 Feb 2021 12:55:03 GMT
Connection: keep-alive
ETag: "6027cc27-93"
Accept-Ranges: bytes

Hello, Sergey !!
Lesson 3 , Go !

If a person really wants something, then the whole Universe will help to make his wish come true.

Paulo Coelho
```

2. Создать на сервере файл `sensitive_info.txt`. Добавить базовую HTTP авторизацию для этого файла.

1) Создал на сервере файл `sensitive_info.txt`

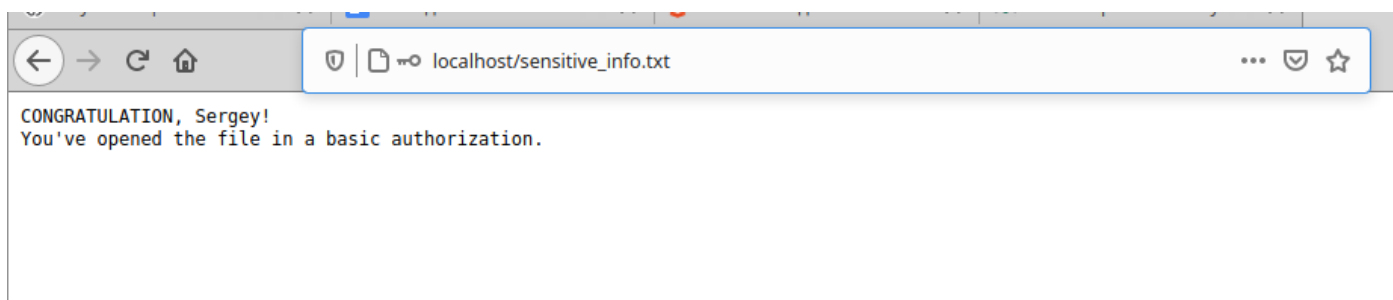
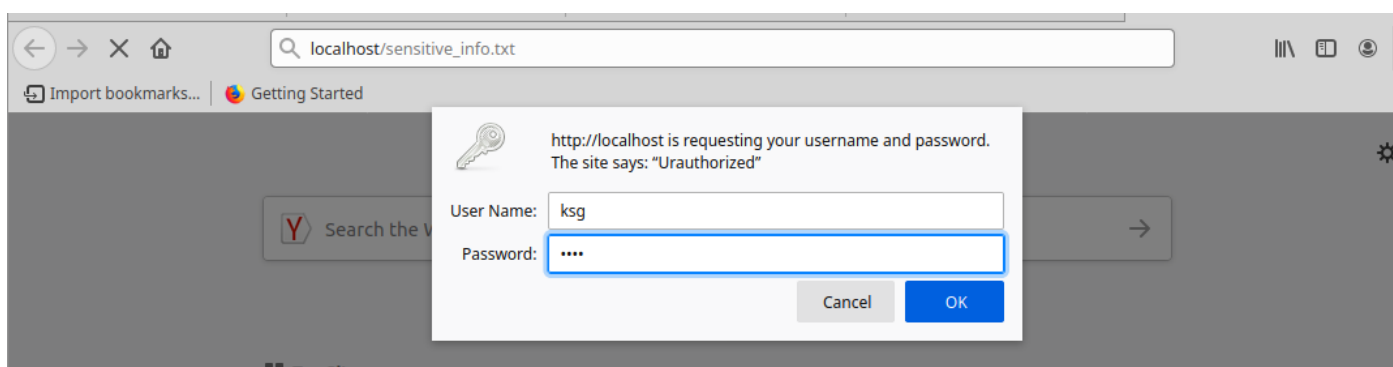
```
Terminal - geek@geek-VirtualBox: /var/www/html
File Edit View Terminal Tabs Help
CONGRATULATION, Sergey!
You've opened the file in a basic authorization.
```

```
Terminal - geek@geek-VirtualBox: /var/www/html
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ cd /var/www/html
geek@geek-VirtualBox:/var/www/html$ sudo vim sensitive_info.txt
[sudo] password for geek:
geek@geek-VirtualBox:/var/www/html$ ls
hellouser.php  index.nginx-debian.html  post.txt  sensitive_info.txt
geek@geek-VirtualBox:/var/www/html$
```

2) Добавил базовую HTTP авторизацию для этого файла.

```
location /sensitive_info.txt {
    auth_basic "Uauthorized";
    auth_basic_user_file /etc/nginx/htpasswd;
}
```

3) Получить этот файл через браузер:



4)Получил тот же файл с помощью telnet:

```
geek@geek-VirtualBox:~/Desktop$ telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /sensitive_info.txt HTTP/1.1
Host: localhost
Authorization: Basic a3Nn0jEyMzQ=

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 13 Feb 2021 19:54:28 GMT
Content-Type: text/plain
Content-Length: 73
Last-Modified: Sat, 13 Feb 2021 16:15:00 GMT
Connection: keep-alive
ETag: "6027fb04-49"
Accept-Ranges: bytes

CONGRATULATION, Sergey!
You've opened the file in a basic authorization.
Connection closed by foreign host.
geek@geek-VirtualBox:~/Desktop$
```

3. Открыть инструменты разработчика, вкладку Сеть (Network). Зайти на сайт <https://geekbrains.ru>. Проанализировать куки каждого запроса за HTML и картинками. Какие запросы уходят с куками, а какие без кук? Почему в каждом из случаев происходит именно такое поведение?

The screenshot shows a web browser window with the GeekBrains website open. The Network tab in the developer tools is active, displaying a list of requests. The requests include GET requests for images and CSS files, and POST requests for tracking and analytics. The right pane shows the details of a selected POST request, including headers, cookies, and response status.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	ib.adnxs.com	setuid?entity=385&code=ef9a0ff2360dc256224a	plgt.js:1 (img)	gif	82 B	43 B
200	GET	ib.adnxs.com	/partner=207&mapped=ef9a0ff2360dc256224a&noRedirect=1	plgt.js:1 (img)	gif	74 B	35 B
200	GET	ib.adnxs.com	bounce?setuid?entity=385&code=ef9a0ff2360dc256224a	plgt.js:1 (img)	gif	82 B	43 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=2&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	GET	dmg.digitaltarget.ru	lta=168&e=ef9a0ff2360dc256224a&l=86389501	plgt.js:1 (img)	gif	91 B	52 B
200	GET	ads.betweendigital...	matchbidder_id=10&external_user_id=ef9a0ff2360dc256224a	plgt.js:1 (img)	png	107 B	68 B
200	GET	ads.betweendigital...	matchbidder_id=10&external_user_id=ef9a0ff2360dc256224a&crf=1	plgt.js:1 (img)	png	107 B	68 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=3&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	GET	sync.1dmp.io	supersync?cid=7914e435-a562-48a5-aa01-6c28a47b11e9&pid=507302	plgt.js:1 (subdocument)	html	444 B	405 B
200	GET	sync.1dmp.io	supersync?t=7eb36db0-6ee0-11eb-ad67-f832e4719dd9	subdocument	html	444 B	405 B
200	GET	ad.mail.ru	cm.gif?w=28&id=ef9a0ff2360dc256224a	plgt.js:1 (img)	gif	cached	43 B
200	GET	sync.1dmp.io	pixel.gif?cid=e8610170-b6a0-4a0d-ab5f-68d104af7a7e&pid=w&uid=60e	supersync:6 (img)	gif	74 B	35 B
200	GET	ad.mail.ru	cm.gif?w=77&id=60ed8fb0-6a33-11eb-a6eb-901b0ea4a41b	supersync:7 (img)	gif	cached	43 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=4&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=4&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=4&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	POST	bam-cell.ru-data.net	753f6c5df67a-408172998v+1198.fe6ec20&to=IFBNFOYXKFQERSVUBB	bundle.min.js:2 (xhr)	gif	63 B	24 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=5&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=5&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B
200	POST	top-fwz1.mail.ru	tracker?ps13id=2794413u=https://geekbrains.ru/r=https://geekbr	code.js:4 (beacon)	gif	82 B	43 B
200	POST	mc.yandex.ru	40414440?wmode=0&wv-part=6&wv-hit=886587087&page-uri=https://	bundle.min.js:2 (xhr)	gif	82 B	43 B

При переходе пользователя на другую HTML страницу проставляется куки host: geekbrains, далее с домена geekbrains без куки запрос HTML host: px.abx.likebin.com возможно загрузка ссылки HTML страницы.

По картинкам Без кук запросы уходя по файлам которые формата jpg и jpeg это непосредственно сами фотографии, а картинки формата png запросы уходят с куками.

4. \* Для выполнения этого задания вам потребуется:

1) Настроить домены **attacker.com**, **sub.attacker.com**, **sub.sub.attacker.com**, **victim.com**. Каждый из этих доменов должен указывать на **127.0.0.1**

2) Настроить установку кук для доменов. Добавьте следующий конфигурационный файл nginx (изменив root сервера на свой):

```
#}
server {
    listen 80;
    server_name attacker.com;
    root /var/www/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";
        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;
    }
}

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

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

Проведите исследование механизма проставления кук, для этого попробуйте установить следующие куки:

The screenshot shows the Chrome DevTools Storage panel with the 'Cookies' tab selected. The left sidebar shows the site 'http://victim.com'. The main table lists cookies with columns: Name, Value, Domain, Path, Expires / Max-Age, Size, HttpOnly, Secure, SameSite, and Last Accessed. One cookie is visible: 'test2' with value 'attacker-com\_victim-com', domain 'victim.com', path '/', and expires 'Session'. The right sidebar shows the details for 'test2', including creation time, domain, expiration, and other attributes.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
test2	attacker-com_victim-com	victim.com	/	Session	28	false	false	None	Sun, 14 Feb 2021 12:43:04 GMT

**test2**: "attacker-com\_victim-com"  
Created: "Sun, 14 Feb 2021 12:43:04 GMT"  
Domain: ".victim.com"  
Expires / Max-Age: "Session"  
HostOnly: false  
HttpOnly: false  
Last Accessed: "Sun, 14 Feb 2021 12:43:04 GMT"  
Path: "/"  
SameSite: "None"  
Secure: false  
Size: 28

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
test3	sub-attacker-com_attacker-com	.attacker.com	/	Session	34	false	false	None	Sun, 14 Feb 2021 12:44:22 GMT
test4	sub-sub-attacker-com_attacker-com	.attacker.com	/	Session	38	false	false	None	Sun, 14 Feb 2021 12:44:22 GMT

**test3:** "sub-attacker-com\_attacker-com"  
 Created: "Sun, 14 Feb 2021 12:38:52 GMT"  
 Domain: ".attacker.com"  
 Expires / Max-Age: "Session"  
 HostOnly: false  
 HttpOnly: false  
 Last Accessed: "Sun, 14 Feb 2021 12:44:22 GMT"  
 Path: "/"  
 SameSite: "None"  
 Secure: false  
 Size: 34

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
test3	sub-attacker-com_attacker-com	.attacker.com	/	Session	34	false	false	None	Sun, 14 Feb 2021 12:44:22 GMT
test4	sub-sub-attacker-com_attacker-com	.attacker.com	/	Session	38	false	false	None	Sun, 14 Feb 2021 12:44:22 GMT

**test4:** "sub-sub-attacker-com\_attacker-com"  
 Created: "Sun, 14 Feb 2021 12:44:22 GMT"  
 Domain: ".attacker.com"  
 Expires / Max-Age: "Session"  
 HostOnly: false  
 HttpOnly: false  
 Last Accessed: "Sun, 14 Feb 2021 12:44:22 GMT"  
 Path: "/"  
 SameSite: "None"  
 Secure: false  
 Size: 38

По каждому пункту ответьте на вопросы:

1. Куда установились куки?
2. Если не установились, то почему?

Обобщите полученные знания и напишите вывод в формате:

1. С домена **attacker.com** на домен **sub.attacker.com** **куки не установлены**
2. С домена **attacker.com** на домен **victim.com** **куки установлены на victim.com**
3. С домена **sub.attacker.com** на домен **attacker.com** **куки установлены на attacker.com**
4. С домена **sub.sub.attacker.com** на домен **attacker.com** **куки установлены на attacker.com**

"Домен может проставлять куки для себя, может проставлять для нескольких поддоменов, но не может проставлять куки для другого домена". «Поддомены могут выставлять куки на родительский домен». Поддомен не может выставлять куки на другой поддомен.

5. (\*) Сгенерировать самоподписанный сертификат и разместить его на своем сервере.

```

Terminal - geek@geek-VirtualBox: /etc/nginx/sites-available
File Edit View Terminal Tabs Help

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

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;
    }
}

# SSL configuration
#
# listen 443 ssl default_server;
# listen [::]:443 ssl default_server;
#

```

```
geek@geek-VirtualBox:/etc/nginx/sites-available$ cd /etc/nginx/ssl
geek@geek-VirtualBox:/etc/nginx/ssl$ ls
nginx.crt  nginx.key
geek@geek-VirtualBox:/etc/nginx/ssl$
```

Page Info — https://your-ssl-site-here.com/

General

Permissions

Security

Website Identity

Website: your-ssl-site-here.com

Owner: This website does not supply ownership information.

Verified by: PortSwigger 

View Certificate

Expires on: February 1, 2022

Privacy & History

Have I visited this website prior to today? Yes, 2 times

Is this website storing information on my computer? No 

Clear Cookies and Site Data

Have I saved any passwords for this website? No 

View Saved Passwords

Technical Details

Connection Encrypted (TLS\_AES\_256\_GCM\_SHA384, 256 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Help

Welcome to nginx! — Mozilla Firefox

Welcome to nginx!

See this page, the nginx web server is successfully installed and configured. Further configuration is required.

Online documentation and support please refer to [nginx.org](https://nginx.org).

Commercial support is available at [nginx.com](https://nginx.com).

Thank you for using nginx.

← → ↺ 🏠

Firefox

about:certificate?cert=MIIQdTCCApgAwIBAgIEWQ28H0ANBgkqhkiG9w0BAQsFADCBijEUMBIGA1UEBhMLUG9ydFN3aWdnZXIxFDASBgNVBAgTC1BvcnRTd2lr

## Certificate

your-ssl-site-here.com

PortSwigger CA

### Subject Name

Country	PortSwigger
Organization	PortSwigger
Organizational Unit	PortSwigger CA
Common Name	your-ssl-site-here.com

### Issuer Name

Country	PortSwigger
State/Province	PortSwigger
Locality	PortSwigger
Organization	PortSwigger
Organizational Unit	PortSwigger CA
Common Name	PortSwigger CA

### Validity

Not Before	2/1/2021, 9:28:51 PM (Moscow Standard Time)
Not After	2/1/2022, 9:28:51 PM (Moscow Standard Time)

### Subject Alt Names

DNS Name	your-ssl-site-here.com
----------	------------------------