

# Урок 1. Введение в веб

## Оглавление

1. Установите VirtualBox и виртуальную машину с Ubuntu. Все дальнейшие задания рекомендуется делать на Ubuntu. ....	2
2. Установите и запустите nginx. Введите в адресной строке браузера <code>http://localhost</code> и убедитесь, что nginx показывает приветственную страницу. Найдите ваш запрос к домашней странице в логах nginx. ....	2
3(*). Установите Burp Suite в качестве прокси. Попробовать основные функции: history, interception, sitemap, repeater. ....	5

1. Установите VirtualBox и виртуальную машину с Ubuntu. Все дальнейшие задания рекомендуется делать на Ubuntu.

Выполнена установка OS Ubuntu 20.04.1-desktop в системе виртуализации VirtualBox.

2. Установите и запустите nginx. Введите в адресной строке браузера `http://localhost` и убедитесь, что nginx показывает приветственную страницу. Найдите ваш запрос к домашней странице в логах nginx.

1.1. Подключим арт-репозиторий для стабильной версии nginx

```
echo "deb http://nginx.org/packages/ubuntu `lsb_release -cs` nginx" | sudo tee /etc/apt/sources.list.d/nginx.list
```

убеждаемся, что репозиторий подключен

```
cat /etc/apt/sources.list.d/nginx.list
```

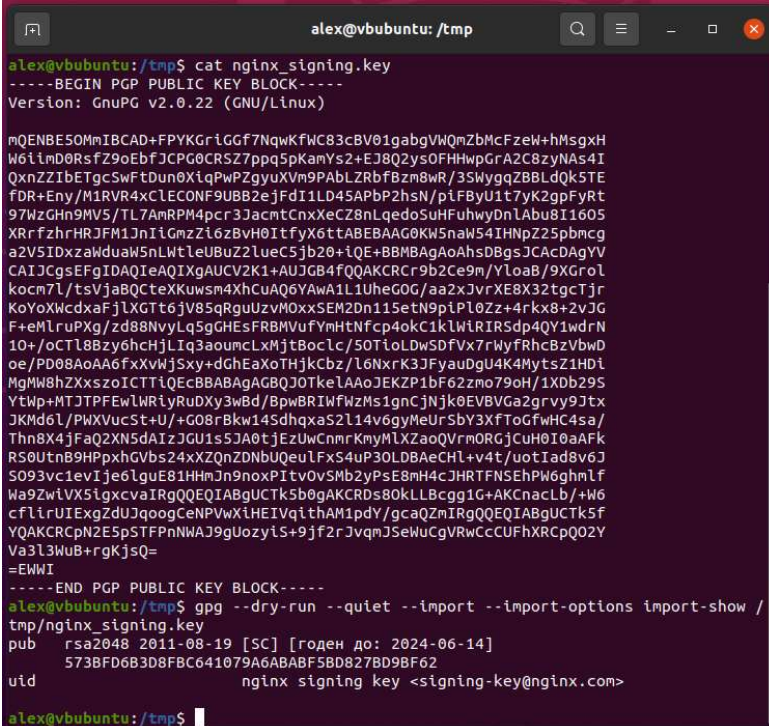
```
deb http://nginx.org/packages/ubuntu focal nginx
```

1.2. Копируем ключ для проверки подлинности пакетов

```
wget /tmp/nginx_signing.key https://nginx.org/keys/nginx_signing.key
```

Убеждаемся в подлинности ключа

```
gpg --dry-run --quiet --import --import-options import-show /tmp/nginx_signing.key
```



```
alex@vbubuntu: /tmp
alex@vbubuntu:/tmp$ cat nginx_signing.key
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQENBE50MnIBCAD+FPYKGrIGGf7NqWKFwC83cBV01gabgVWQmZbMcFzew+hMgqXH
W6ilmD0RsFZ9oEbfJCPG0CRS7Zppq5pKamYs2+EJ8Q2ysOFHHwpGrA2C8zyNAS4I
QxnZ21bETgcSwFtdun0XiQpWPZgyuXVm9PAbLZRbfBzm8wR/35WygqZBBLdQk5TE
fDR+Eny/M1RVR4xCLECONF9UBB2ejFdI1LD45APbP2hsN/piFByUit7yK2gpFyRt
97WzGHn9MV5/TL7AmRPM4pcr3JacmtCnXxeCZ8nLqedoSuHFUhwYDnLAbu8I1605
XRrfzhrHRJFM1JnIlgmZLi6zBVH0ItfyX6ttABEBAAG0Kw5naw54IHNPZ25pbmcg
a2R5IDxzawduaW5nLWtleUBuZ21ueC5jb20+IQE+BBMBAGAAhSDBgsJCAcDagYV
CAIJGgsEFgIDAQIeAQIXgAUCV2K1+AUJGB4fQQAkRCr9b2Ce9m/YloaB/9XGrol
kocm7L/tsVjaBQCteXKuwsml4XhCuAQ6YAWA1L1UheG0G/aa2xJvrXE8X32tgcTjr
KoYoXwcdaFjLXGtt6jV85qRguUzvM0xxSEM2Dn115etN9piPL0Zz+4rkx8+2vJG
F+eMLruPXg/zd8BNvyLq5GgHESFRBMVufYmHtnfcp4okC1kLwIRISdp4QY1wdrN
10+/oCTL8Bzy6hcHjLIQ3aoumCLxMjtBocLc/50TioLDwSDfVx7rWyfRhcbZVbwD
oe/PD08AoAA6fxXvWjSxy+dGhEaXoThjKcbz/L6NxrK3JFyauDgU4K4MytsZ1HDl
MgMM8hZXszoICTTlQEcBBABAgAGBQJOTkeLAAoJEKZP1bF62zmo79oH/1XDb29S
YtWp+MTJTPFEwLWRIyRuDXy3wBd/BpWBRIWfWzMs1gnCjNjk0EVBVGa2grvy9Jtx
JKMd6l/PWxVucSt+U/+G08rBkw145dhqxaS2L14v6gyMeUrSbY3XfToGfWHC4sa/
Thn8X4jFaQ2XN5dAIzJGU1s5JA0tjEzUwCnmrKmyMLXZaoQVrmORGjCuH0I0aAFK
RS0utnB9HPpxhGVbs24xXZQnZDNbUQeulFXS4uP30LDBAeCHL+v4t/uotIad8v6J
S093vc1evIje6lguE81HHmJn9noxPitvOv5Mb2yPsE8mMH4cJHRTFNSEhPW6ghmLf
W9Zw1VX5lgxcvaIRgQQEQIABGUCTK5b0gAKCRDs80kLLBcgg1G+AKCnaclb/+W6
cfliRUExgZdUJqoogCeNPVwXiHEIVqithAM1pdY/gcaQZnIRgQQEQIABGUCTK5f
YQAKCRCPnE5pSTFPnNWAJ9gUoziys+9jf2rJvqmJSeWuCGVRwCCCUfHXRcpQ02Y
Va3l3WuB+rgKjsQ=
=EWWI
-----END PGP PUBLIC KEY BLOCK-----
alex@vbubuntu:/tmp$ gpg --dry-run --quiet --import --import-options import-show /
tmp/nginx_signing.key
pub   rsa2048 2011-08-19 [SC] [роден до: 2024-06-14]
      573BFD6B3D8FBC64107A6ABABF5BD827BD9BF62
uid           nginx signing key <signing-key@nginx.com>

alex@vbubuntu:/tmp$
```

### 1.3. Перемещаем ключ в каталог доверенных ключей apt

```
sudo mv /tmp/nginx_signing.key /etc/apt/trusted.gpg.d/nginx_signing.asc
```

### 1.4. Обновляем кэш репозиторий, и устанавливаем nginx

```
sudo apt update
```

```
sudo apt install nginx
```

### 1.5. Проверяем конфигурацию nginx

```
cd /etc/nginx/conf.d/
```

```
sudo cp default.conf test.conf
```

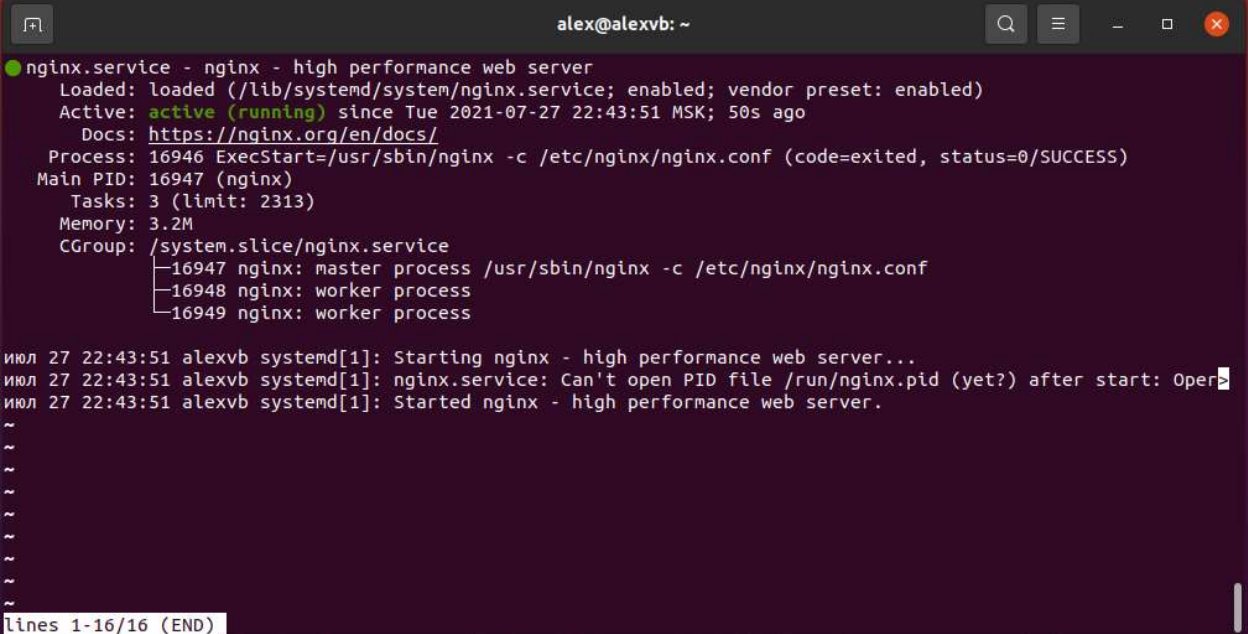
```
sudo vim test.conf
```

Убеждаемся, что nginx слушает 80 порт и убираем комментирование кода с блока php

### 1.6. Проверяем статус процесса и доступность nginx

```
systemctl start nginx
```

```
systemctl status nginx
```

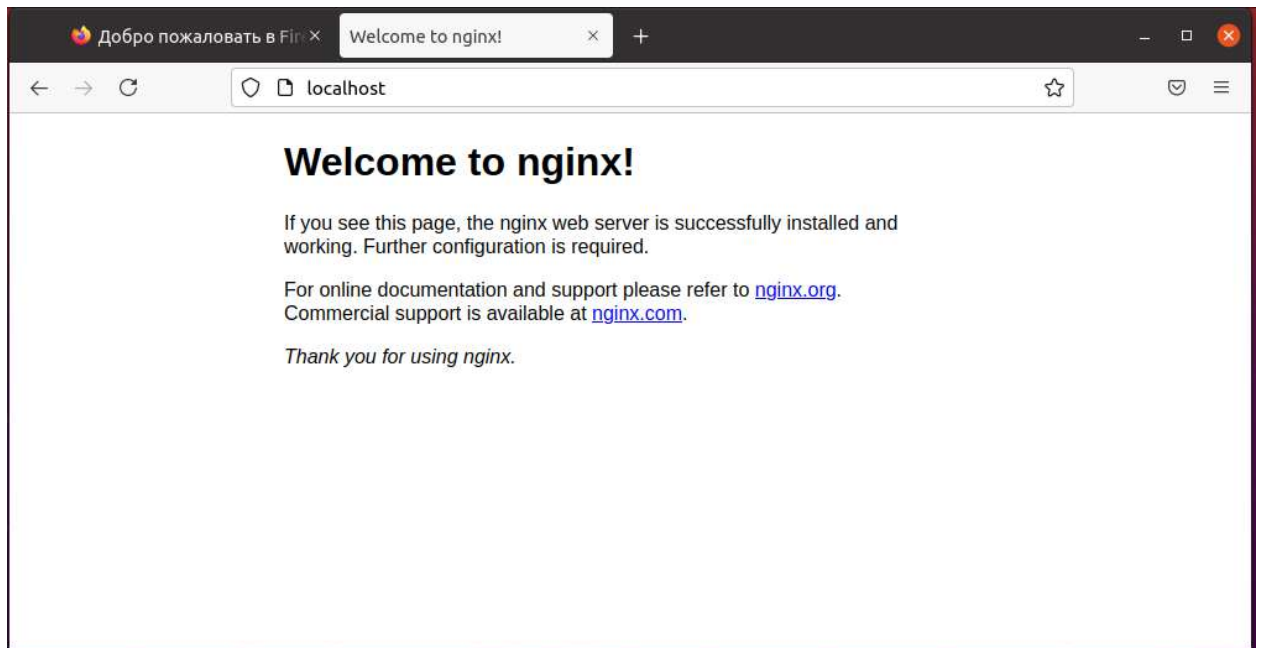
A terminal window titled 'alex@alexvb: ~' showing the output of 'systemctl status nginx'. The output includes details about the nginx.service, its active state, and the processes it runs. At the bottom, there are log messages from systemd indicating the start of the service.

```
alex@alexvb: ~
● nginx.service - nginx - high performance web server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-07-27 22:43:51 MSK; 50s ago
     Docs: https://nginx.org/en/docs/
   Process: 16946 ExecStart=/usr/sbin/nginx -c /etc/nginx/nginx.conf (code=exited, status=0/SUCCESS)
  Main PID: 16947 (nginx)
    Tasks: 3 (limit: 2313)
   Memory: 3.2M
   CGroup: /system.slice/nginx.service
           └─16947 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
             └─16948 nginx: worker process
               └─16949 nginx: worker process

июл 27 22:43:51 alexvb systemd[1]: Starting nginx - high performance web server...
июл 27 22:43:51 alexvb systemd[1]: nginx.service: Can't open PID file /run/nginx.pid (yet?) after start: Oper
июл 27 22:43:51 alexvb systemd[1]: Started nginx - high performance web server.

~
~
~
~
~
~
~
lines 1-16/16 (END)
```

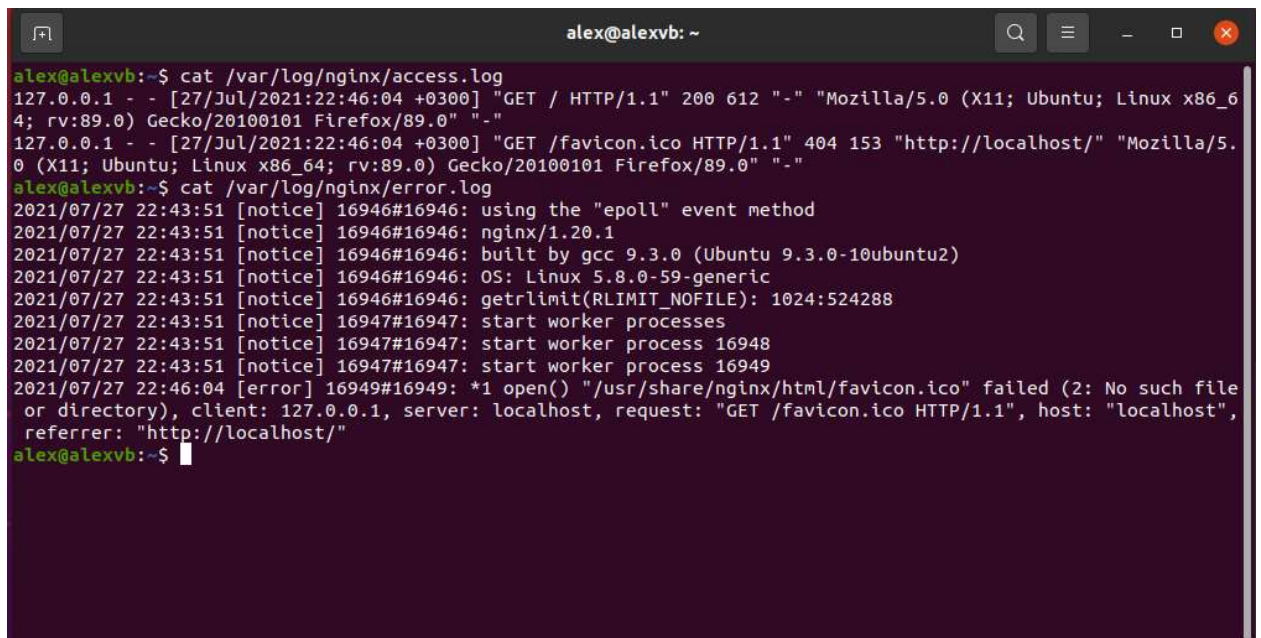
1.7. Открываем браузер в адресной строке браузера вводим `http://localhost`



1.8. Проверяем логи:

`/var/log/nginx/access.log`

`/var/log/nginx/error.log`



3(\*). Установите Burp Suite в качестве прокси. Попробовать основные функции: history, interception, sitemap, repeater.

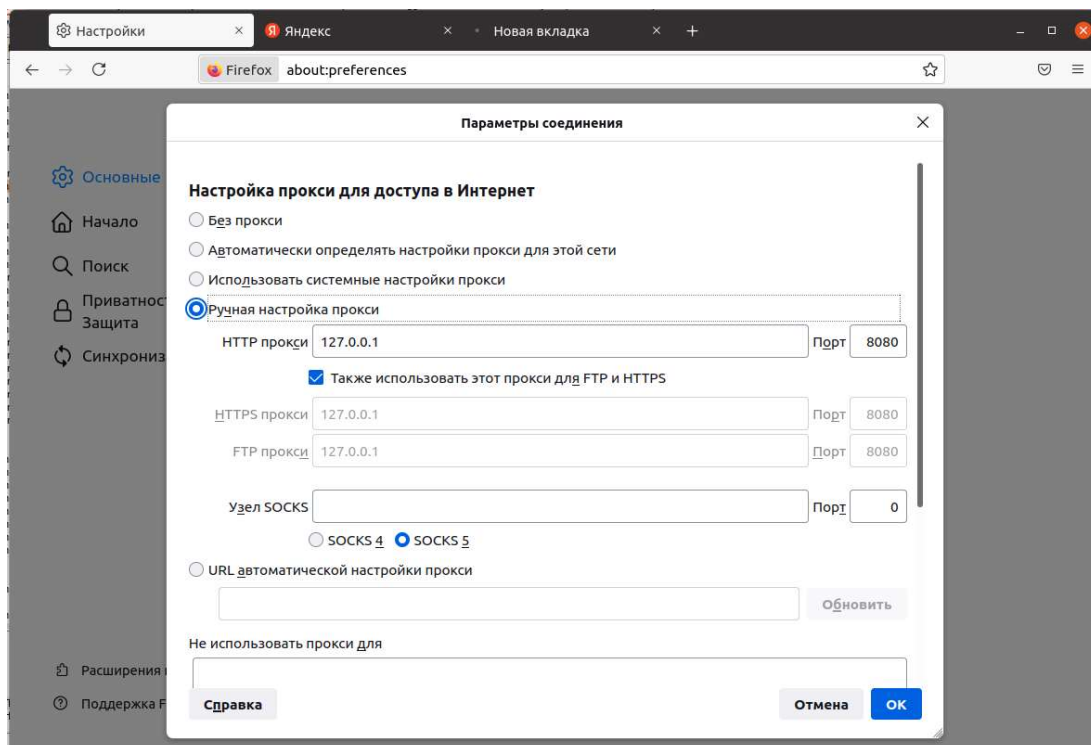
3.1. Скачиваем Burp Suite Community <https://portswigger.net/burp/communitydownload>

3.2. Выполняем команду `sudo bash burpsuite_community_linux_v2021_6_2.sh`

устанавливаем программу по дефолту, не меняя в процессе установки никакие параметры

3.3. Запускаем Burp Suite, в процессе запуска тоже выбираем дефолтные настройки

3.4. Выполняем настройку прокси HTTP 127.0.0.1:8080 в браузере Mozilla Firefox



### 3.5. Проверяем что Burp Suite слушает порт 8080

The screenshot shows the Burp Suite Community Edition v2021.6.2 interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar has tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, and User options. The 'HTTP history' tab is active, displaying a list of intercepted requests. The table below shows the details of the intercepted requests:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
412	http://example.com	GET	/			200	1626	HTML		Example Domain			93.184.216.34
413	http://detectportal.firefox.com	GET	/canonical.html			200	321	XML	html				34.107.221.82
414	http://detectportal.firefox.com	GET	/success.txt?pv4		✓	200	239	text	txt				34.107.221.82
415	http://detectportal.firefox.com	GET	/success.txt?pv6		✓	200	239	text	txt				34.107.221.82
416	http://detectportal.firefox.com	GET	/canonical.html		✓	200	321	XML	html				34.107.221.82
417	http://detectportal.firefox.com	GET	/success.txt?pv4		✓	200	239	text	txt				34.107.221.82
418	http://detectportal.firefox.com	GET	/success.txt?pv6		✓	200	239	text	txt				34.107.221.82
419	http://detectportal.firefox.com	GET	/success.txt?pv4		✓	200	239	text	txt				34.107.221.82
420	http://detectportal.firefox.com	GET	/success.txt?pv6		✓	200	239	text	txt				34.107.221.82
421	http://detectportal.firefox.com	GET	/success.txt?pv6		✓	200	238	text	txt				34.107.221.82
422	http://detectportal.firefox.com	GET	/success.txt?pv4		✓	200	239	text	txt				34.107.221.82
423	http://detectportal.firefox.com	GET	/canonical.html		✓	200	321	XML	html				34.107.221.82
424	http://detectportal.firefox.com	GET	/success.txt?pv4		✓	200	239	text	txt				34.107.221.82
425	http://detectportal.firefox.com	GET	/success.txt?pv6		✓	200	239	text	txt				34.107.221.82
426	http://detectportal.firefox.com	GET	/canonical.html		✓	200	321	XML	html				34.107.221.82
427	http://detectportal.firefox.com	GET	/success.txt?pv4		✓	200	239	text	txt				34.107.221.82

The 'Request' tab is selected, showing the details of the first request (GET / HTTP/1.1). The 'Response' tab is also selected, showing the details of the first response (200 OK). The 'Inspector' tab is active, showing the 'Request Headers (7)' and 'Response Headers (13)'. The 'Response Headers' section shows the following headers:

- padding: 2em;
- background-color: #fdfdff;
- border-radius: 0.5em;
- box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);

The 'Request' tab shows the following request details:

```
1 GET / HTTP/1.1
2 Host: example.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
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
```

### 3.6. Пробуем Intercept

The screenshot shows the Burp Suite Community Edition v2021.6.2 interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar has tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, and User options. The 'Intercept' tab is active, displaying the details of the intercepted request. The 'Request' tab is selected, showing the details of the first request (GET / HTTP/1.1). The 'Response' tab is also selected, showing the details of the first response (200 OK). The 'Inspector' tab is active, showing the 'Request Headers (7)' and 'Response Headers (13)'. The 'Request Headers' section shows the following headers:

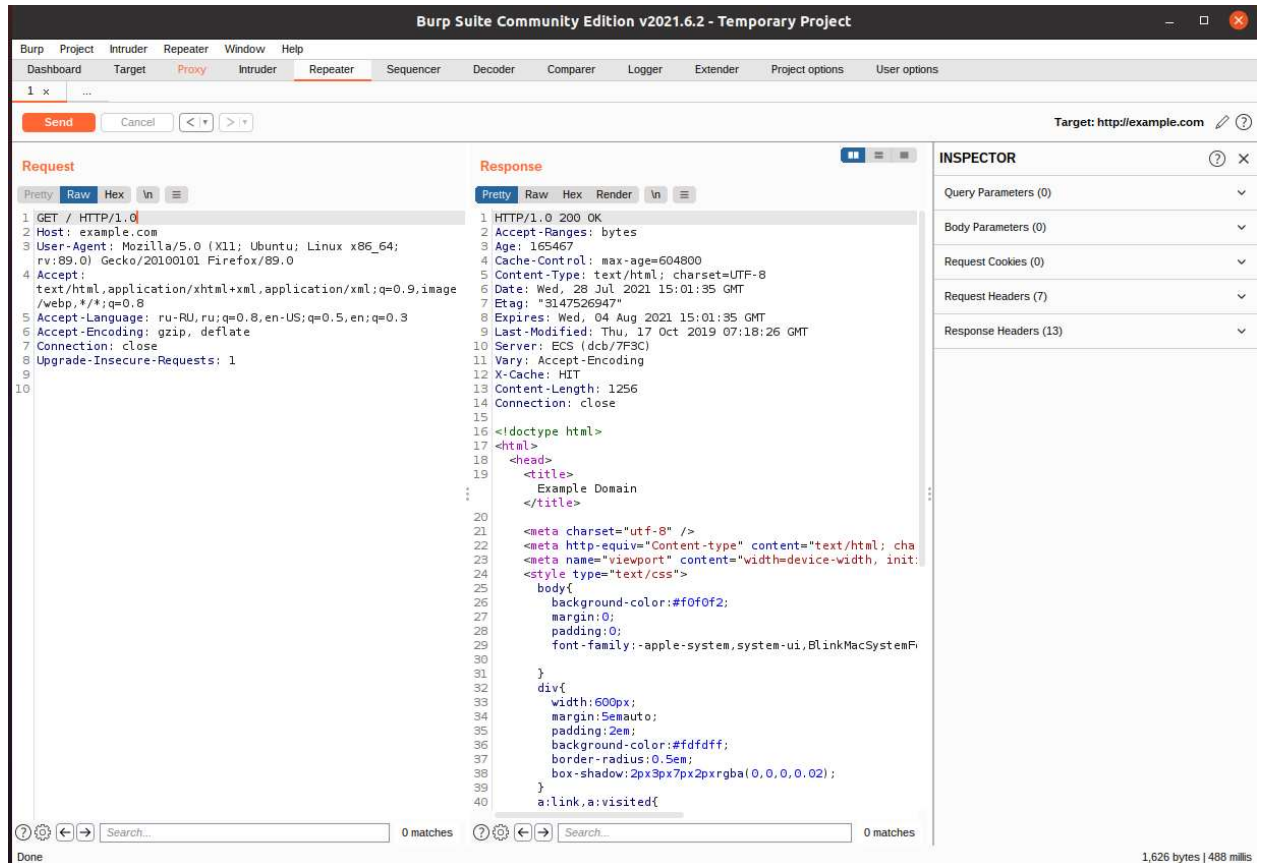
- padding: 2em;
- background-color: #fdfdff;
- border-radius: 0.5em;
- box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);

The 'Request' tab shows the following request details:

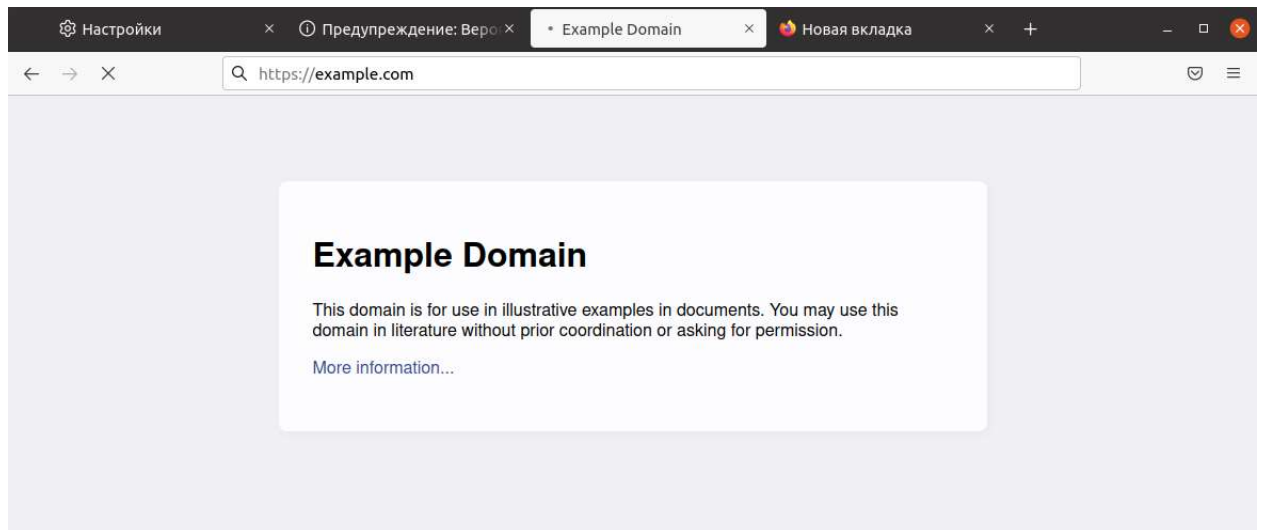
```
1 GET / HTTP/1.1
2 Host: example.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
```



### 3.7. Пробьем Repeater



### 3.8. Подкидываем в Firefox сертификат Burp Suite, пробуем работать с https



### 3.9. Смотрим Logger

Burp Suite Community Edition v2021.6.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer **Logger** Extender Project options User options

Capture filter: Logger memory limit set to 50MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length	Start response timer	Comment
10	17:26:19 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	321	115	
11	17:26:19 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	321	151	
12	17:26:19 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	321	219	
13	17:26:19 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/success.txt	ipv4	1	200	239	103	
14	17:26:20 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	239	104	
15	17:26:20 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	321	114	
16	17:26:20 28 Jul 2021	Proxy	GET	example.com	/		0	200	1609	268	
17	17:26:30 28 Jul 2021	Proxy	GET	stroi-otdelka.ru	/wp-content/uploads/201...		15	200	56563	245	
18	17:28:34 28 Jul 2021	Proxy	GET	stroi-otdelka.ru	/wp-content/uploads/201...		0	200	56563	8510	
19	17:37:02 28 Jul 2021	Proxy	GET	example.com	/		0	200	1626	268	
20	17:37:05 28 Jul 2021	Proxy	GET	example.com	/		0	200	1626	229	
21	17:37:06 28 Jul 2021	Proxy	POST	yandex.ocsp-responder....	/		21	200	1717	131	
22	17:37:08 28 Jul 2021	Proxy	POST	yandex.ocsp-responder....	/		21	200	1717	460	
23	17:37:11 28 Jul 2021	Proxy	POST	yandex.ocsp-responder....	/		21	200	1717	149	
24	17:37:11 28 Jul 2021	Proxy	POST	yandex.ocsp-responder....	/		21	200	1717	277	
25	17:37:12 28 Jul 2021	Proxy	GET	example.com	/		0	200	1626	728	
26	17:37:14 28 Jul 2021	Proxy	POST	ocsp.digicert.com	/		23	200	818	138	
27	17:37:15 28 Jul 2021	Proxy	POST	ocsp.pki.goog	/gts1olcore		29	200	720	117	
28	17:37:16 28 Jul 2021	Proxy	POST	ocsp.digicert.com	/		23	200	818	146	
29	17:44:38 28 Jul 2021	Proxy	GET	example.com	/		0	200	1626	30354	
30	17:44:38 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/success.txt	ipv6	1	200	239	2836	
31	17:44:38 28 Jul 2021	Proxy	GET	example.com	/		0	200	1631	22963	
32	17:44:38 28 Jul 2021	Proxy	GET	detectportal.firefox.com	/canonical.html		0	200	321	23872	

**Request**

1 GET /wp-content/uploads/2017/05/linkerbar.png HTTP/1.1

2 Host: stroi-otdelka.ru

3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:89.0) Gecko/20100101 Firefox/89.0

4 Accept: image/webp, \*/\*

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: przvonline=0; przvidistance=0; przvdome=da3a3d2eaa09c5c5d5f5ebcf5926353c7570f4a51052082555f87c70945e; przvlng=ru; przvg=9c95d24631f8c8df49cb85d29fd96e8b4ff03d3c320a8b25a9114e5ef64f2911; przvusr=277043c5b24d13d885d6af259a4830f192cbd5bd11fd0f42834ad264888424; \_ym\_uid=1627481659112356086; \_ym\_d=1627481659; WhiteCallback\_visitorId=8092905803; WhiteCallback\_visit=14197456514; WhiteSaas\_uniqueLead=no; \_ga=

**Response**

1 HTTP/1.1 200 OK

2 Server: nginx-reuseport/1.20.1

3 Date: Wed, 28 Jul 2021 14:26:30 GMT

4 Content-Type: image/png

5 Content-Length: 56245

6 Last-Modified: Sun, 01 Sep 2019 18:53:21 GMT

7 Connection: close

8 ETag: "5d6c13a1-dbb5"

9 Expires: Fri, 27 Aug 2021 14:26:30 GMT

10 Cache-Control: max-age=2592000

11 Accept-Ranges: bytes

12

13

14

15

16

17

**INSPECTOR**

Query Parameters (1)

Request Headers (8)

Response Headers (8)

### 3.10. Пробуем Sitemap

Burp Suite Community Edition v2021.6.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer **Logger** Extender Project options User options

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time
https://example.com	GET	/		200	1605	HTML	Example Domain		18:10

**Request**

1 GET / HTTP/2

2 Host: example.com

3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:89.0) Gecko/20100101 Firefox/89.0

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 Upgrade-Insecure-Requests: 1

8 Te: trailers

9 Connection: close

**INSPECTOR**

Request Headers (8)

Response Headers (12)