Задания необходимо сдавать в формате скриншотов, которые сопровождаются комментариями. Отчет должен быть в pdf формате.

Пожалуйста, пишите в названии pdf файла домашнего задания своё имя.

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

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

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

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

Получить этот файл через браузер.

Получить тот же файл с помощью curl и telnet или netcat.

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?

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):

```
$ cat /etc/nginx/sites-available/cookie-research.conf
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:

1. С домена `attacker.com` на домен `sub.attacker.com`
2. С домена `attacker.com` на домен `victim.com`
3. С домена `sub.attacker.com` на домен `attacker.com`
4. С домена `sub.sub.attacker.com` на домен `attacker.com`

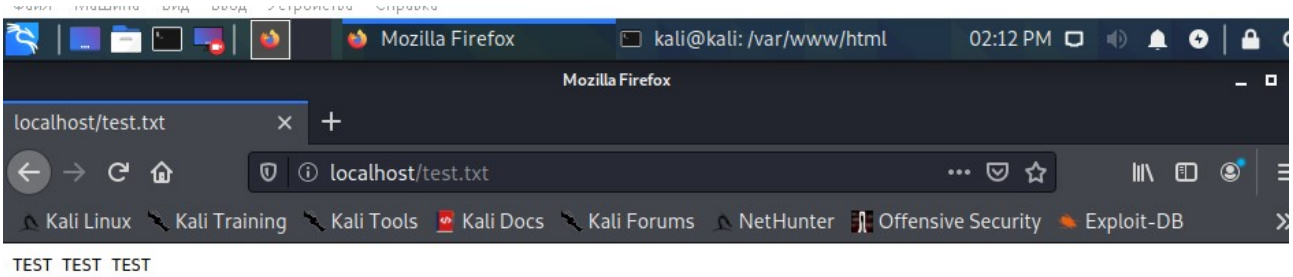
По каждому пункту ответьте на вопросы:

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

Обобщите полученные знания и напишите вывод в формате: "Домен может проставлять куки для себя, для ... и ..., но не может проставлять куки для ..., ... и ...".

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

1.

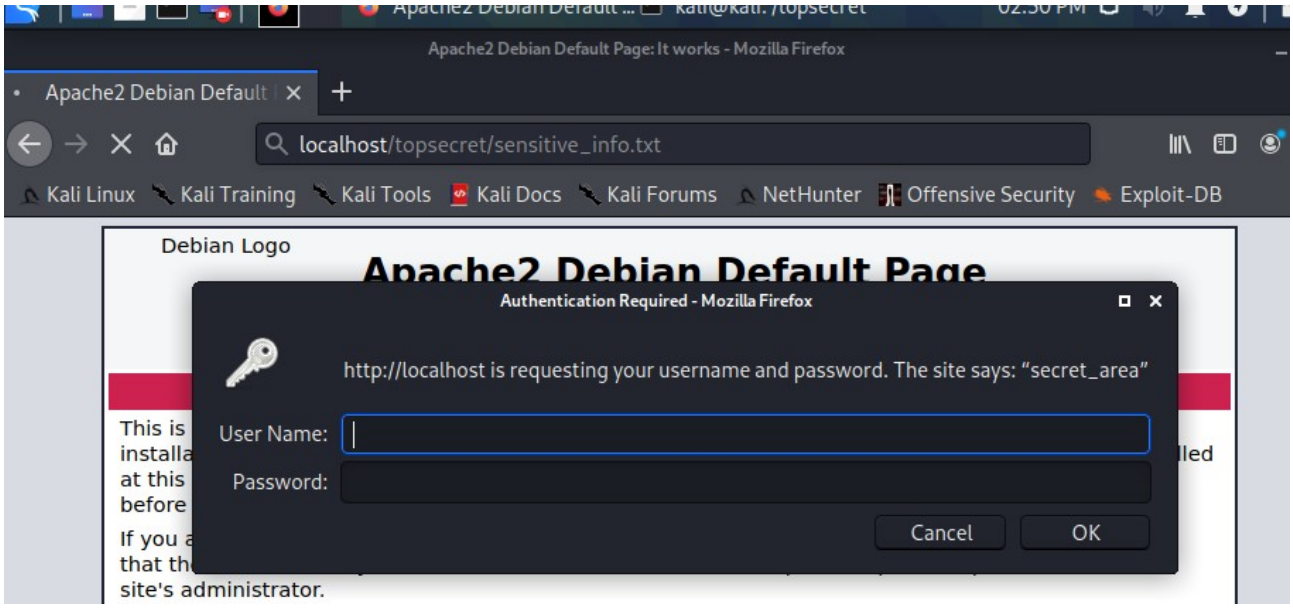


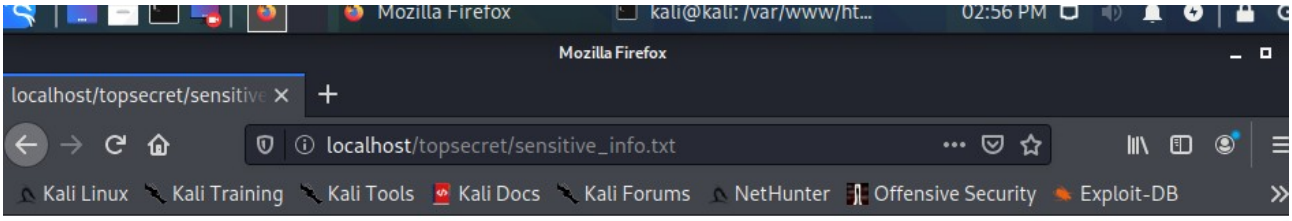
```
┌──(kali㉿kali)-[/var/www/html]
└─$ telnet localhost 80                                                    1 ×
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET /test.txt HTTP/1.1
Host:localhost

HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Sun, 28 Mar 2021 11:19:26 GMT
Content-Type: text/plain
Content-Length: 15
Last-Modified: Sun, 28 Mar 2021 11:10:27 GMT
Connection: keep-alive
ETag: "60606423-f"
Accept-Ranges: bytes

TEST TEST TEST
```

2.






```
┌──(kali㉿kali)-[/var/www/html/topsecret]
└─$ curl -u admin:77317020 localhost/topsecret/sensitive_info.txt
AUTH TEST AUTH TEST AUTH TEST
```

Через telnet можно обойти авторизацию не прописывая заголовки.

```
┌──(kali㉿kali)-[/var/www/html/topsecret]
└─$ telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET /topsecret/sensitive_info.txt
AUTH TEST AUTH TEST AUTH TEST
```

```
┌──(kali㉿kali)-[/var/www/html/topsecret]
└─$ telnet localhost 80                                                    1 ×
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET /topsecret/sensitive_info.txt HTTP/1.1
Host:localhost
Authorization:Basic YWRtaW46NzczMTcwMjA=

HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Sun, 28 Mar 2021 12:26:26 GMT
Content-Type: text/plain
Content-Length: 30
Last-Modified: Sun, 28 Mar 2021 11:56:06 GMT
Connection: keep-alive
ETag: "60606ed6-1e"
Accept-Ranges: bytes

AUTH TEST AUTH TEST AUTH TEST
```

```
┌──(kali㉿kali)-[/var/www/html/topsecret]
└─$ echo -n "admin:77317020" | openssl base64 -base64                      1 ×
YWRtaW46NzczMTcwMjA=
```

3. POST запрос /login

```
Cookie: utm_source=geekbrains.ru; utm_medium=referral;
_app_session=7e1bd730e1312c62bf43ce5eb0650230;
carrotquest_session=f6v16vcgtfy4qub9129stq415y532lfr; _gcl_au
=1.1.2021666444.1616935675; _gasessionid=20210328|05149691;
_gasessiondate=Sun, 28 Mar 2021 12:48:55 GMT; gbwsuid=
d2060476-94ca-4896-8c64-22a30d630c0a; _ga_D11RM3RGCC=
GS1.1.1616935675.1.0.1616935676.0; _ga=
GA1.2.1637674611.1616935676; tmr_reqNum=9; tmr_lvid=
6f023fa8a79ae9b3d76cc99b059a5185; tmr_lvidTS=1616935675662;
_gid=GA1.2.1280156310.1616935677; _ym_uid=1616935678617103110
; _ym_d=1616935678; _fbp=fb.1.1616935678899.1750648906;
_ym_isad=2; tmr_detect=0%7C1616935680943
```

GET запрос /login

```
Cookie: utm_source=geekbrains.ru; utm_medium=referral;
_app_session=7e1bd730e1312c62bf43ce5eb0650230
```

Все оставшиеся запросы к geekbrains

10	https://geekbrains.ru	GET	/	200	89642	HTML		ÐÐ»Ð°Ð²Ð½Ð°
11	https://geekbrains.ru	GET	/chat/rooms/unread_messages_...	200	572	JSON	json	
12	https://geekbrains.ru	GET	/api/v2/notices/count	200	466	text		
13	https://geekbrains.ru	GET	/api/v2/notices	206	6236	JSON		
14	https://geekbrains.ru	GET	/api/v2/dashboard/posts	200	5333	JSON		
15	https://geekbrains.ru	GET	/api/v2/dashboard/topics	200	3623	JSON		
16	https://geekbrains.ru	GET	/api/v2/dashboard/comments	200	4784	JSON		
17	https://geekbrains.ru	GET	/api/v2/dashboard/vacancies	200	3943	JSON		
18	https://geekbrains.ru	GET	/api/v2/dashboard/projects	200	2904	JSON		
19	https://geekbrains.ru	GET	/api/v2/dashboard/quizzes	200	3862	JSON		
20	https://geekbrains.ru	GET	/api/v2/cart/items_count	200	483	JSON		
21	https://geekbrains.ru	GET	/api/v2/cart/items_count	200	483	JSON		
22	https://geekbrains.ru	GET	/api/v2/schedule	200	1797	JSON		

Все оставшиеся содержат одинаковые cookie

```
Cookie: utm_source=geekbrains.ru; utm_medium=referral;
_app_session=f2b66ed74610c70b478983533b71ac46;
carrotquest_session=f6v16vcgtfy4qub9129stq415y532lfr; _gcl_au
=1.1.2021666444.1616935675; _gasessionid=20210328|05149691;
_gasessiondate=Sun, 28 Mar 2021 12:48:55 GMT; gbwsuid=
d2060476-94ca-4896-8c64-22a30d630c0a; _ga_D11RM3RGCC=
GS1.1.1616935675.1.1.1616935776.0; _ga=
GA1.2.1637674611.1616935676; tmr_reqNum=9; tmr_lvid=
6f023fa8a79ae9b3d76cc99b059a5185; tmr_lvidTS=1616935675662;
_gid=GA1.2.1280156310.1616935677; _ym_uid=1616935678617103110
; _ym_d=1616935678; _fbp=fb.1.1616935678899.1750648906;
_ym_isad=2; tmr_detect=0%7C1616935680943; user_id=
OTIwMjYy--8a1792de9d5d42de4a667866420f3277fd6a9569;
registered=1; jwt_token=
eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJnZWVrYnJhaW5zIiwiaWF0IjoxNjE2
OTM2NjgxLCJhdWQiOlsiYWNjZXNzIl0sInVzZXJfaWQiOjkyMDI2MiwidXBmI
joibGludXgiLCJleHAiOjE2MTcwMjMwODEsImF1dGhlbnRpY2F0YWJsZV9zYW
x0IjoiJDJhJDExJHFHVU5GUmpadmlEMDlpOHl0U1FmRk8iLCJyb2xlcyI6WyJ
1c2VyIl19.q0AII5i_1wqG8iH7coYIRv88RkFZceaF28H8ZSwEf2uBZ7hBJnE
k3jcFsyIJHpaChBYNWj2WknIR0XrvsVySiohv7Q2zV4sClxnyDSTLISjF77Sp
TA0Xm4kuaA4iFReH_Vz55leDJWDr91OqrDMZCwdlfvcdqi8m26z7b14stHZ3U
QiIQjerTRVYydtufkXUhLx3LR7uazTaLPB4IhvyCK7zjMs4-sGQQYtq-bEDK0
fMj3z_BHGkA5KpP7mrFhdTcH1xxbWTeelo963teINq2FbKFoWPHuPGdwavcR3
DqJ4Z0fC7ofd5MYUEgLszZNylqZn0LR3G9qeTUC9e2w02CQ; split=
%7B%22event_redesign_desktop_ab_test%3Afinished%22%3Atrue%7D;
 show_notifications=on; carrotquest_user_hash=
6dc619d1c42af0cc5c0f6a5e806ba615488a95db717af2d67bc40c7b9f926
```

Полный список cookie

_app_ses...	f2b66ed74610c...	geekbrains.ru	/	Session	44
_dc_gtm...	1	.geekbrains.ru	/	Sun, 28 Mar 2021 12...	22
_fbp	fb.1.161693567...	.geekbrains.ru	/	Sat, 26 Jun 2021 12:...	33
_ga_D11...	GS1.1.1616935...	.geekbrains.ru	/	Tue, 28 Mar 2023 1...	47
_gasessi...	Sun, 28 Mar 20...	.geekbrains.ru	/	Sun, 28 Mar 2021 1...	43
_gasessi...	20210328|0514...	.geekbrains.ru	/	Sun, 28 Mar 2021 1...	29
_gat_UA...	1	.geekbrains.ru	/	Sun, 28 Mar 2021 12...	19
_ga	GA1.2.1637674...	.geekbrains.ru	/	Tue, 28 Mar 2023 1...	30
_gcl_au	1.1.202166644...	.geekbrains.ru	/	Sat, 26 Jun 2021 12:...	32
_gid	GA1.2.1280156...	.geekbrains.ru	/	Mon, 29 Mar 2021 1...	31
_ym_d	1616935678	.geekbrains.ru	/	Mon, 28 Mar 2022 1...	15
_ym_isad	2	.geekbrains.ru	/	Mon, 29 Mar 2021 0...	9
_ym_uid	161693567861...	.geekbrains.ru	/	Mon, 28 Mar 2022 1...	26
carrotque...	f6v16vcgtfy4qu...	.geekbrains.ru	/	Sun, 28 Mar 2021 13...	51
carrotque...	6dc619d1c42af...	geekbrains.ru	/	Session	85
gbwsuid	d2060476-94c...	.geekbrains.ru	/	Wed, 23 Mar 2022 1...	43
jwt_token	eyJhbGciOiJSU...	geekbrains.ru	/	Mon, 29 Mar 2021 1...	605
registered	1	geekbrains.ru	/	Mon, 28 Mar 2022 1...	11
show_no...	on	geekbrains.ru	/	Session	20
split	%7B%22event...	geekbrains.ru	/	Sat, 26 Jun 2021 13:...	65
tmr_detect	0%7C1616935...	geekbrains.ru	/	Mon, 29 Mar 2021 1...	27
tmr_lvidTS	1616935675662	.geekbrains.ru	/	Thu, 24 Feb 2022 12...	23
tmr_lvid	6f023fa8a79ae...	.geekbrains.ru	/	Thu, 24 Feb 2022 12...	40
tmr_req...	15	.geekbrains.ru	/	Thu, 24 Feb 2022 12...	12
user_id	OTIwMjYy--8a...	.geekbrains.ru	/	Session	57
utm_med...	referral	geekbrains.ru	/	Mon, 28 Mar 2022 1...	18
utm_sour...	geekbrains.ru	geekbrains.ru	/	Mon, 28 Mar 2022 1...	23

Не содержит cookie запрос к титульной надписи geekbrains.

```
GET / HTTP/1.1
Host: geekbrains.ru
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Все остальные запросы содержат cookie ресурса utm_source, контекстной рекламы utm_medium, и cookie сессии.

Запросы на разделы, которые могут менятся у разных пользователей содержат соответственно куки для конкретного пользователя вроде user_id. Также судя по всему присутствуют куки для управления пользователями carrotquest, куки текущей даты, флаг регистрации, jwt токен для безопасной авторизации и тд и тп.

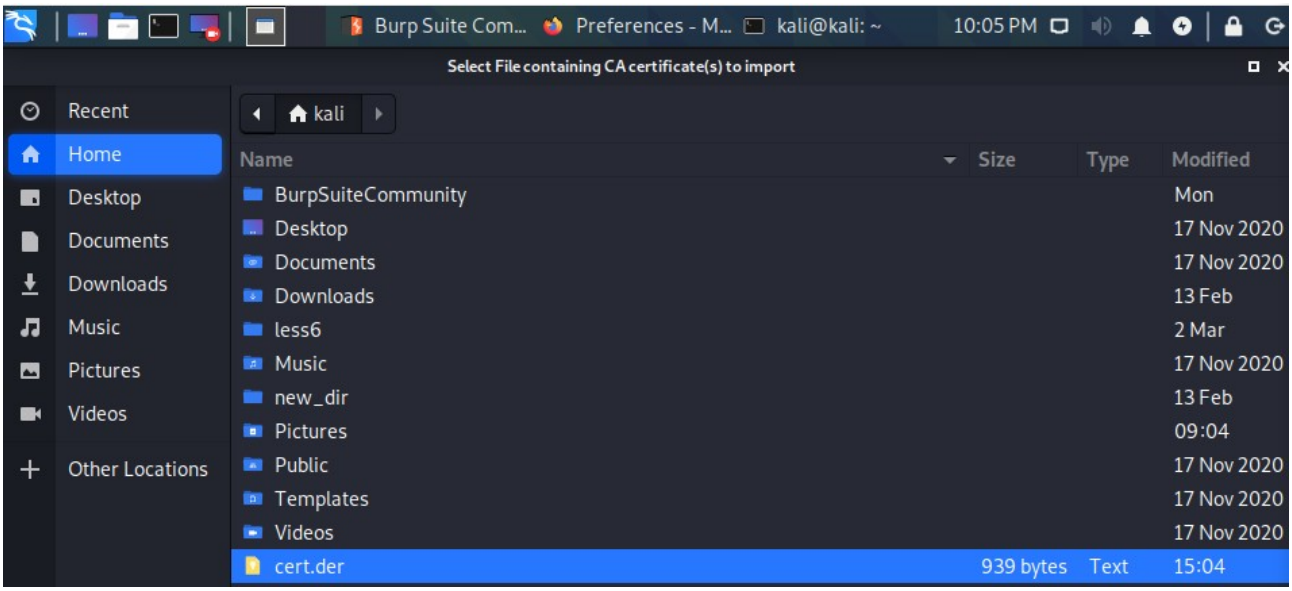
4. Куки на attacker.com

```
Connection: close
Referer: http://attacker.com/
Cookie: __opix_uid=1-vyvk8rti-kmtjcd2w; __zlcmid=
13KjukMAq3hhv4M
```

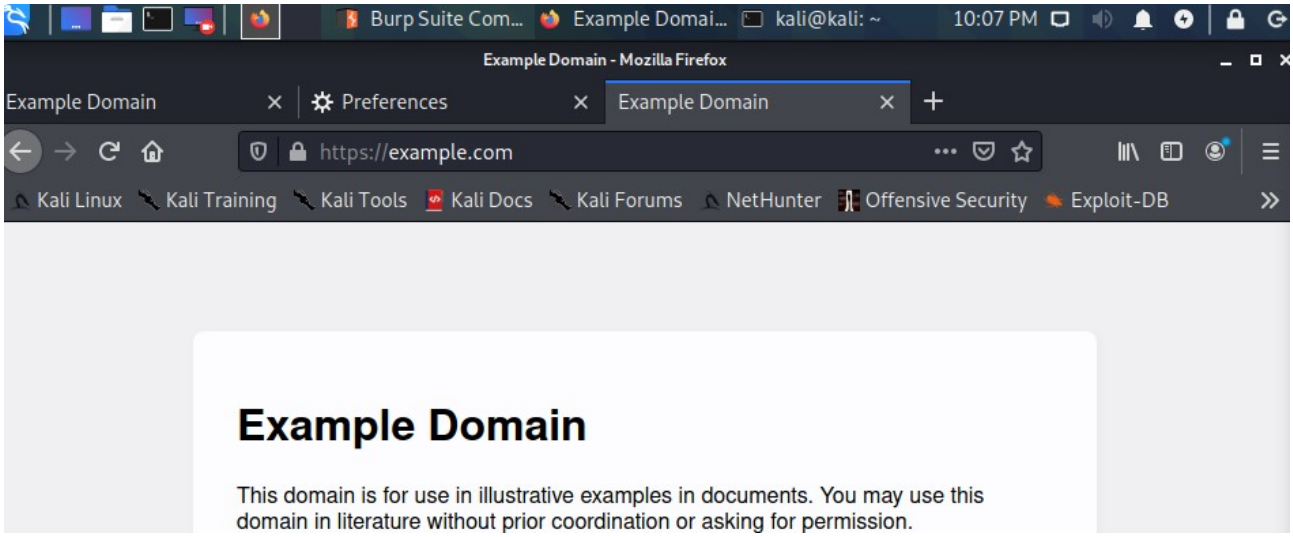
Куки на sub.attacker.com аналогично
На sub.sub.attacker.com

```
Connection: close
Cookie: __zlcmid=13KjukMAq3hhv4M
Upgrade-Insecure-Requests: 1
```

На victim.com не наблюдаю куков.
Домен может проставлять куки для себя и своих поддоменов.
5. Добавляем свой сертификат



Проверяем.


Burp Suite Com...
Example Domai...
kali@kali: ~
10:07 PM
Example Domain - Mozilla Firefox
Example Domain
Preferences
Example Domain
https://example.com
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Example Domain
This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.