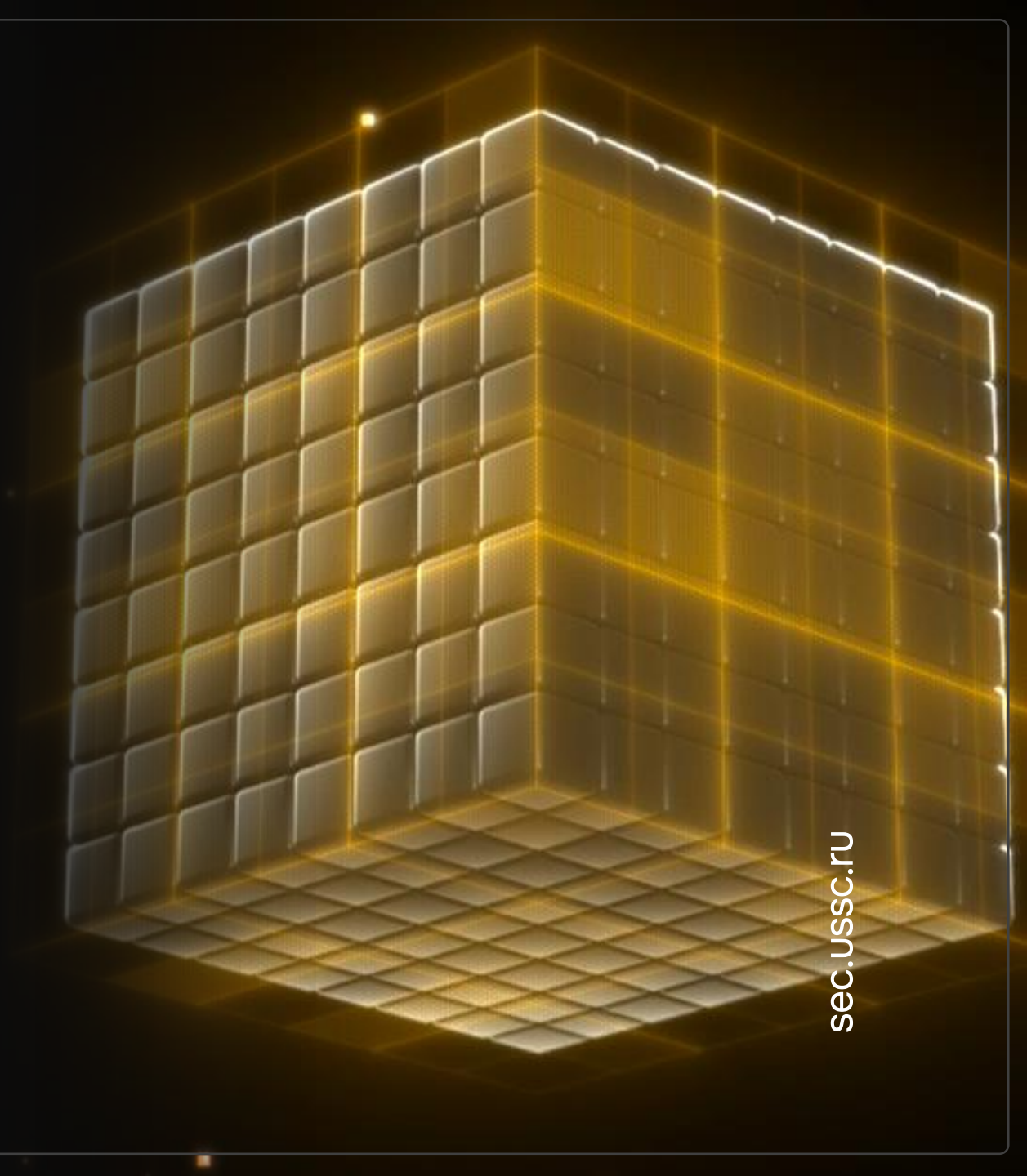
ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Fast recon — быстрая разведка при пентесте веб-приложения

Никита Распопов
Специалист по анализу защищенности УЦСБ



sec.ussc.ru

2/20 WHOAMI

Никита Распопов

- Специалист по анализу защищенности в УЦСБ
- Занимаюсь веб и мобильными приложениями
- Опыт в пентеста более 3 лет
- Спикер на конференциях
- В свободное время ищу баги
- Автор канала по пентесту @GigaHack

3/20 Этапы поиска уязвимостей

Ищем поддомены

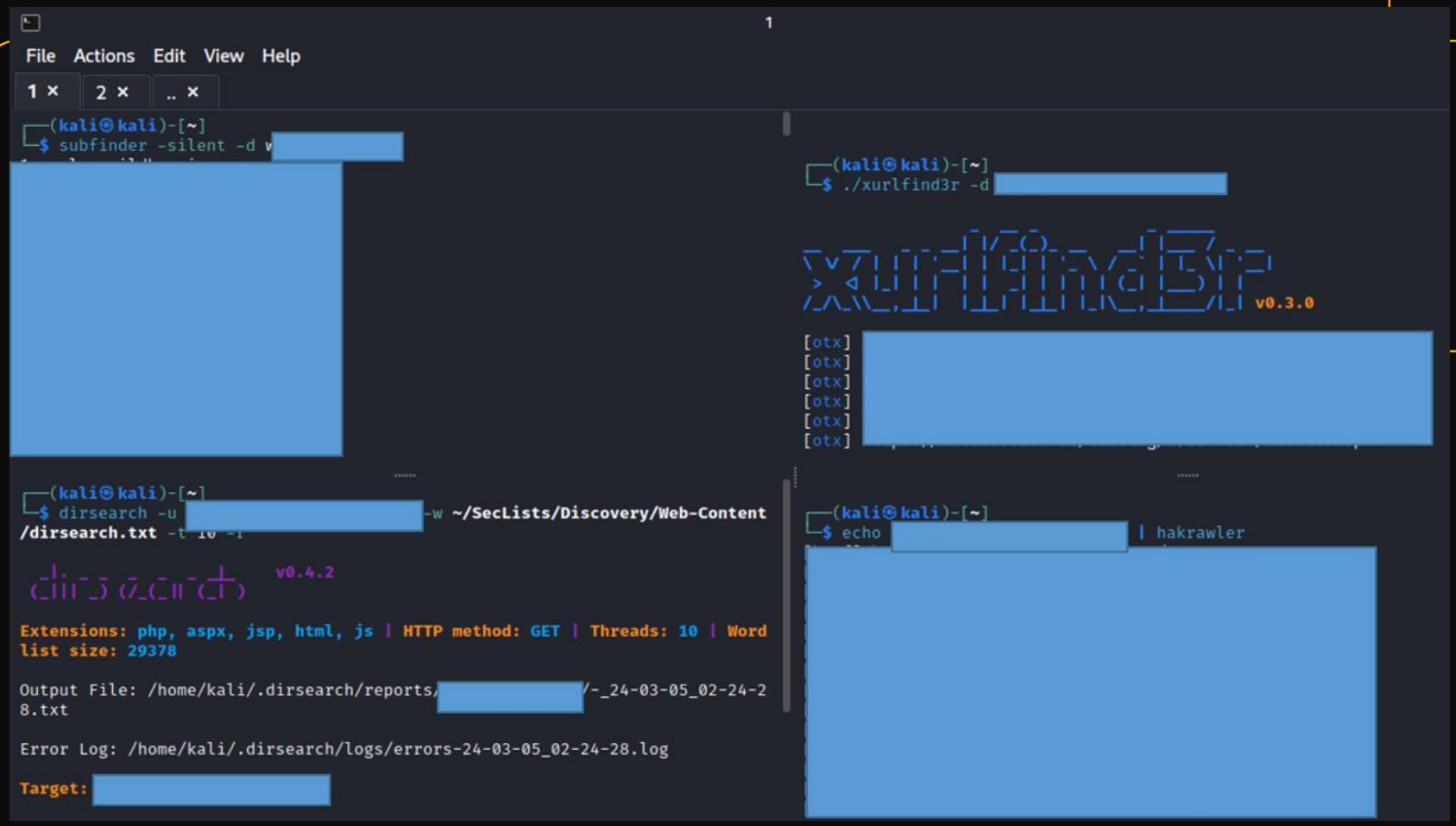
Краулим

Собираем кеш сайтов

Брутим директории

Фаззим параметры

4/20 Ручное проведение разведки



- ! Долго
- ! Неудобно
- ! Тяжело отслеживать результаты

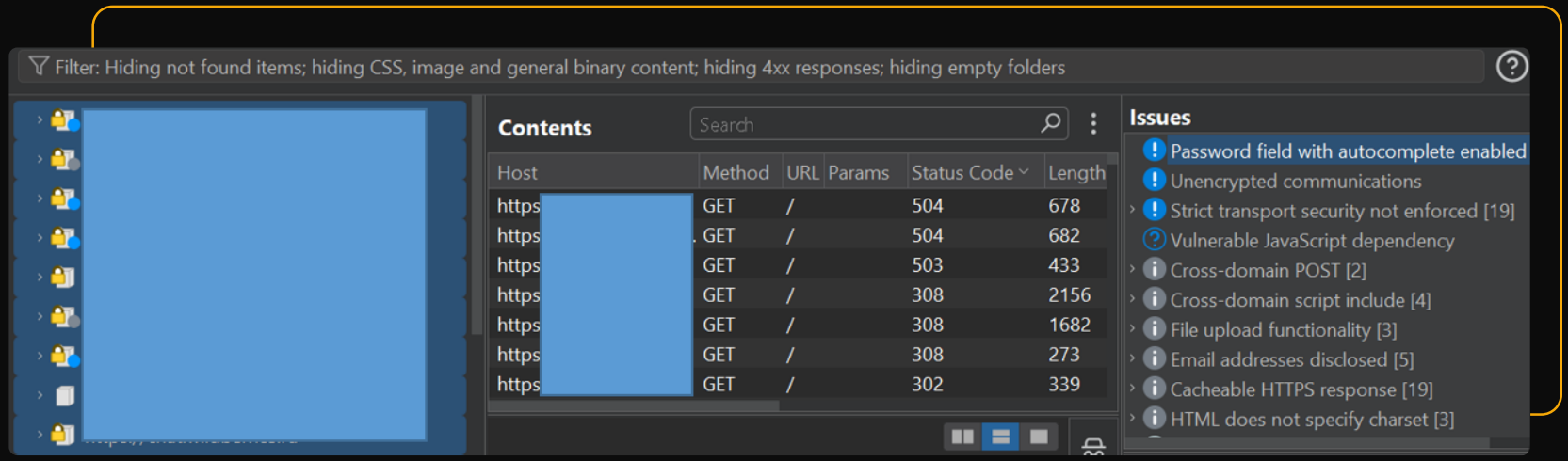
5/20 Критерии качественной разведки

- Фильтровать недоступные доменные имена
- Эффективно парсить веб-кеш приложений
- Составить sitemap приложения для dirsearch
- Конечные точки и параметры из JS-файлов

6/20 Фильтр недоступных доменных имен

Что нас интересует?

- 401/403 – bypass
- 500 – различные ошибки
- 200 – живые хосты




```
subfinder –silent –d domain | httpx --silent --proxy http://127.0.0.1:8081/ -o liveHost.txt
```

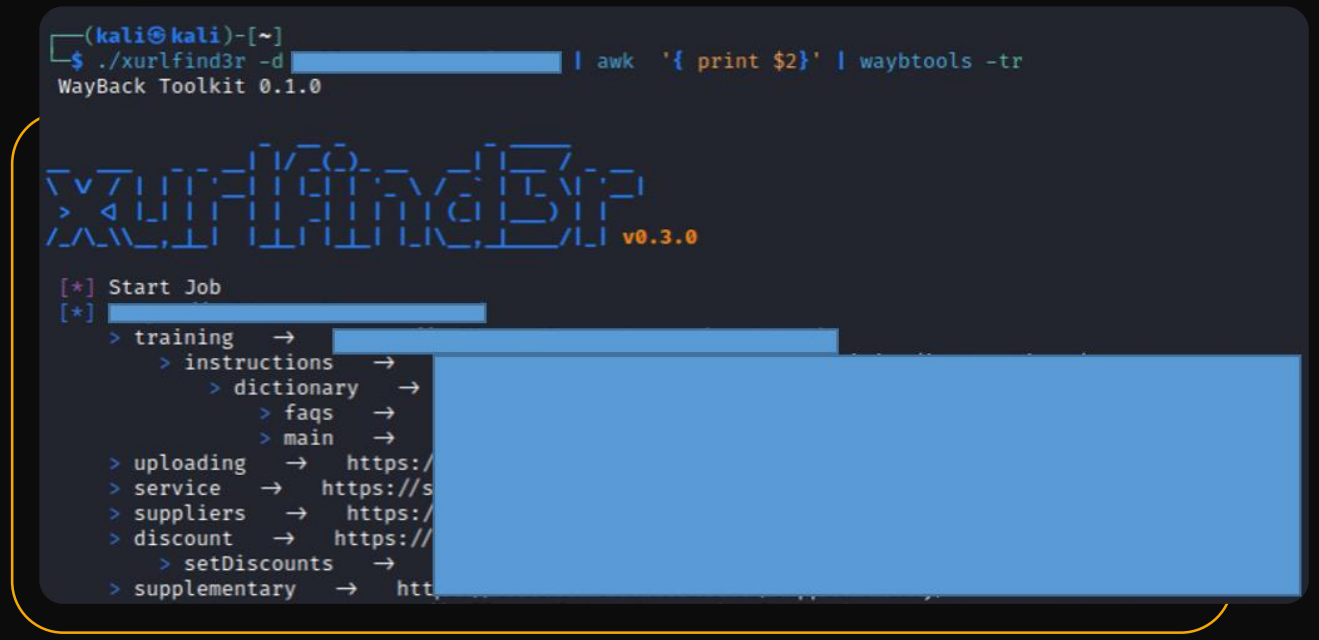
7/20 Что мы делаем с этими доменами

- 401/403 –обход утилитами: (laluka/bypass-url-parser, devploit/dontgo403)
- 500 – смотрим ответ сервера на предмет интересных данных
- File Upload – переходим к проверкам загрузки файлов
- Email disclosure – ищем почту в различных утечках
- Ищем сервисы AUTOPWN – Bitrix, Gitlab, Jira, Confluence, Owa

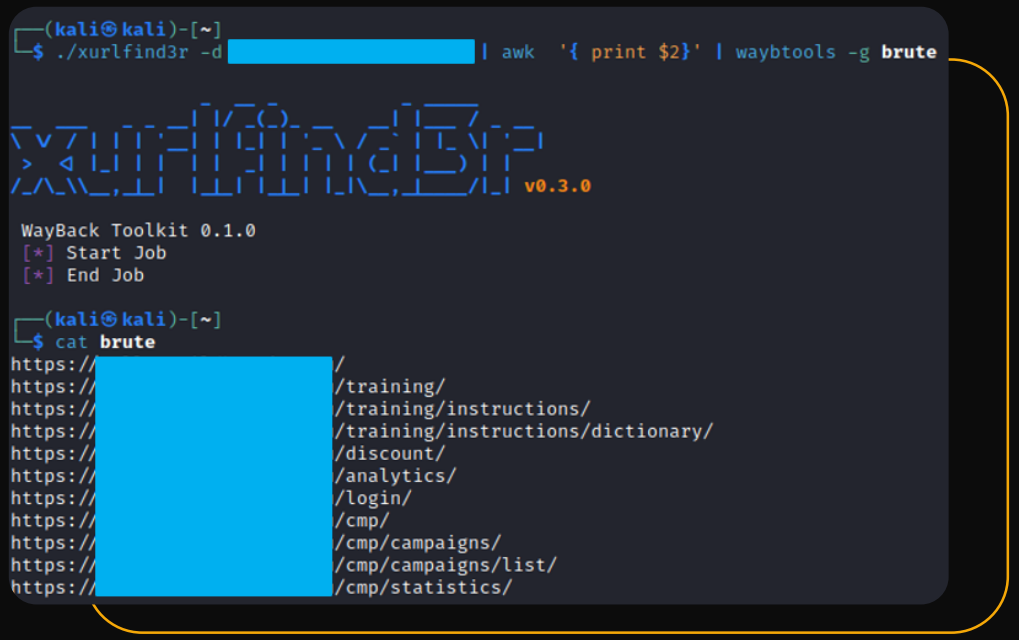
8/20 Эффективно парсим веб-кеш

xurlfind3r + waybtool

./xurlfind3r -d domain| awk '{ print $2}' | waybtools -tr



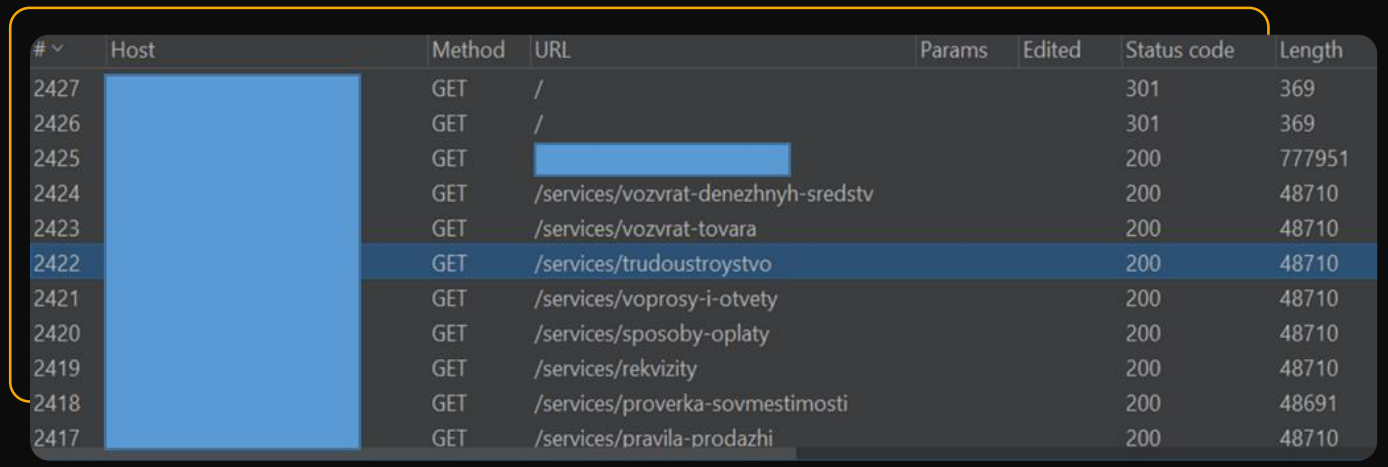
./xurlfind3r -d domain| awk '{ print $2}' | waybtools -g brute



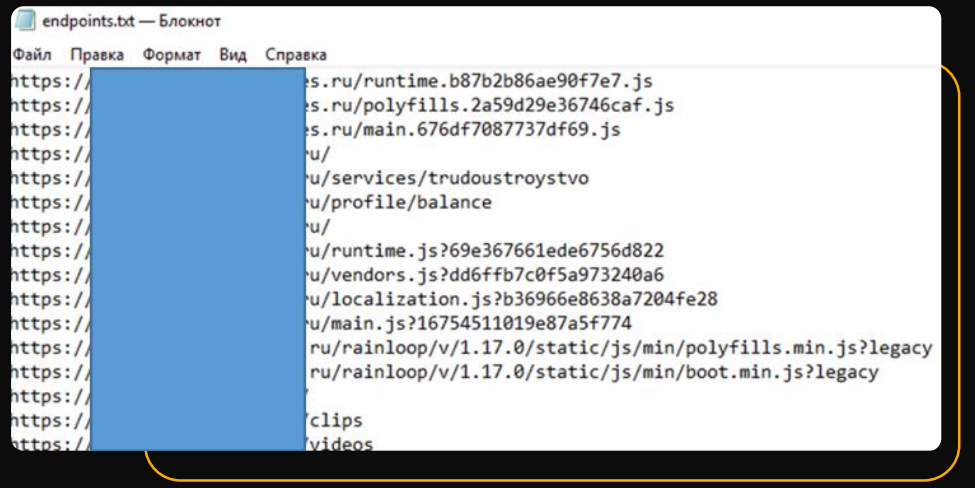
9/20 Результат работы с веб-кешем

- Дерево закешированных запросов
- Закешерованные файлы (бекапы, дампы, файлы конфигурации и т.д)
- Потенциальные конечные точки API
- Закешированные токены запросов
- Файлы с чувствительной информацией (документы, персональные данные и т.д.)

10/20 Составляем sitemap приложения



#	Host	Method	URL	Params	Edited	Status code	Length
2427	[redacted]	GET	/			301	369
2426		GET	/			301	369
2425		GET	[redacted]			200	777951
2424		GET	/services/vozvrat-denezhnyh-sredstv			200	48710
2423		GET	/services/vozvrat-tovara			200	48710
2422		GET	/services/trudoustroystvo			200	48710
2421		GET	/services/voprosy-i-otvety			200	48710
2420		GET	/services/sposoby-oplaty			200	48710
2419		GET	/services/rekvizity			200	48710
2418		GET	/services/proverka-sovmestimosti			200	48691
2417		GET	/services/pravila-prodazhi			200	48710



subfinder –silent –d domain | httpx --silent --proxy http://127.0.0.1:8081/ -o liveHost.txt | katana -list liveHost.txt -proxy http://127.0.0.1:8081/ -o endpoints.txt

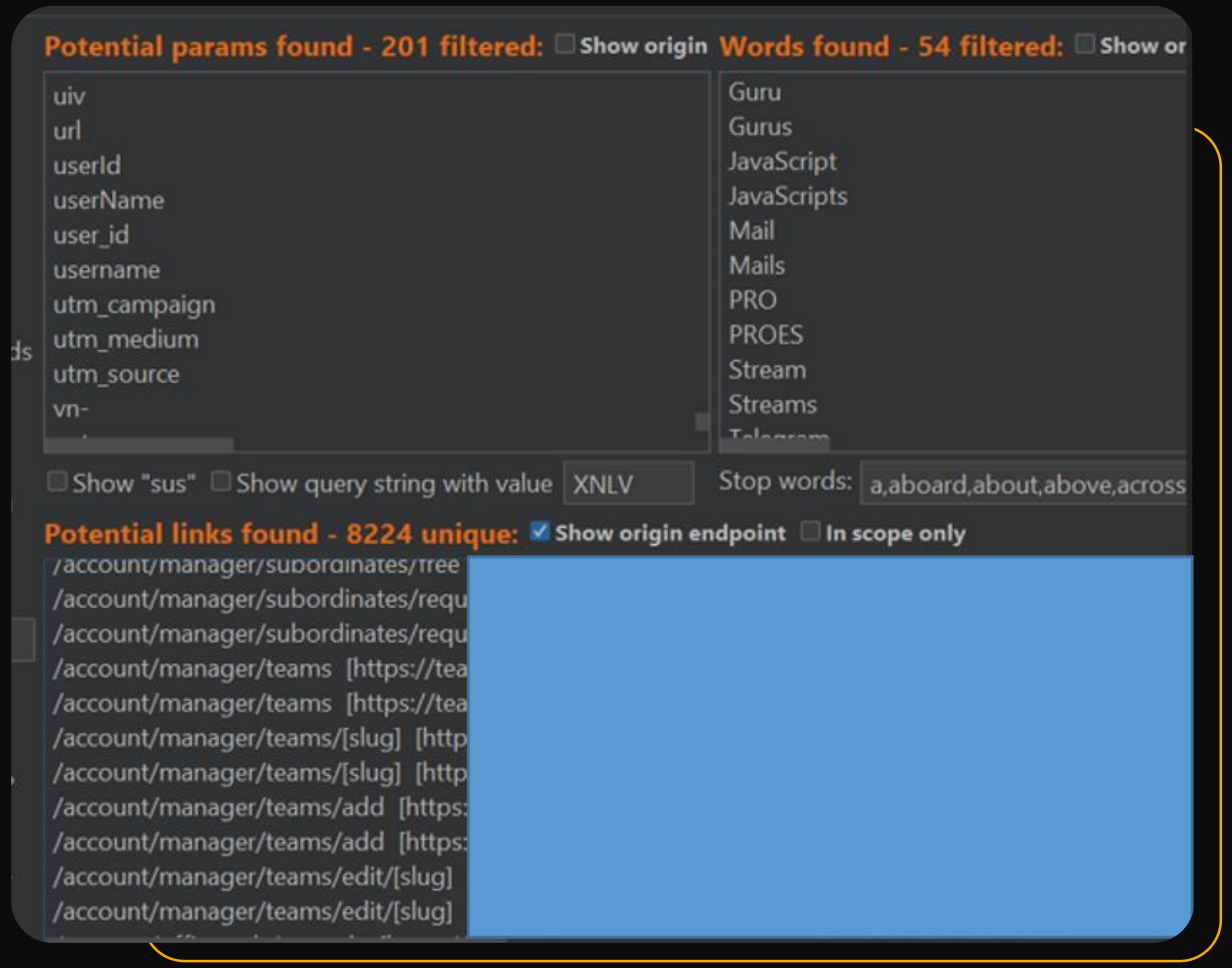
11/20 Дальнейшие действия

JS-файлы
(конечные точки, параметры, захардкоженные значения)

URL-адреса из верстки страниц

Комментарии в HTML

12/20 Анализируем JS с помощью GAP (Get All Parameters, Links, and Words)



Что мы получаем:

- Ссылки для брута директорий
- Параметры для фаззинга (x8,arjun)
- Конечные точки API

13/20 Итоговая команда для сбора данных о скоупе

```
subfinder -silent –d domain | ../httpx -silent –proxy http://127.0.0.1:8081/ -o 'liveHosts.txt' | ../katana -list 'liveHosts.txt' –proxy http://127.0.0.1:8081/ -o 'endpoints.txt'; ../xurlfind3r -l 'liveHosts.txt' | awk '{print $2}' > res.txt | grep '?' > params.txt | ../httpx –silent -proxy http://127.0.0.1:8081/
```

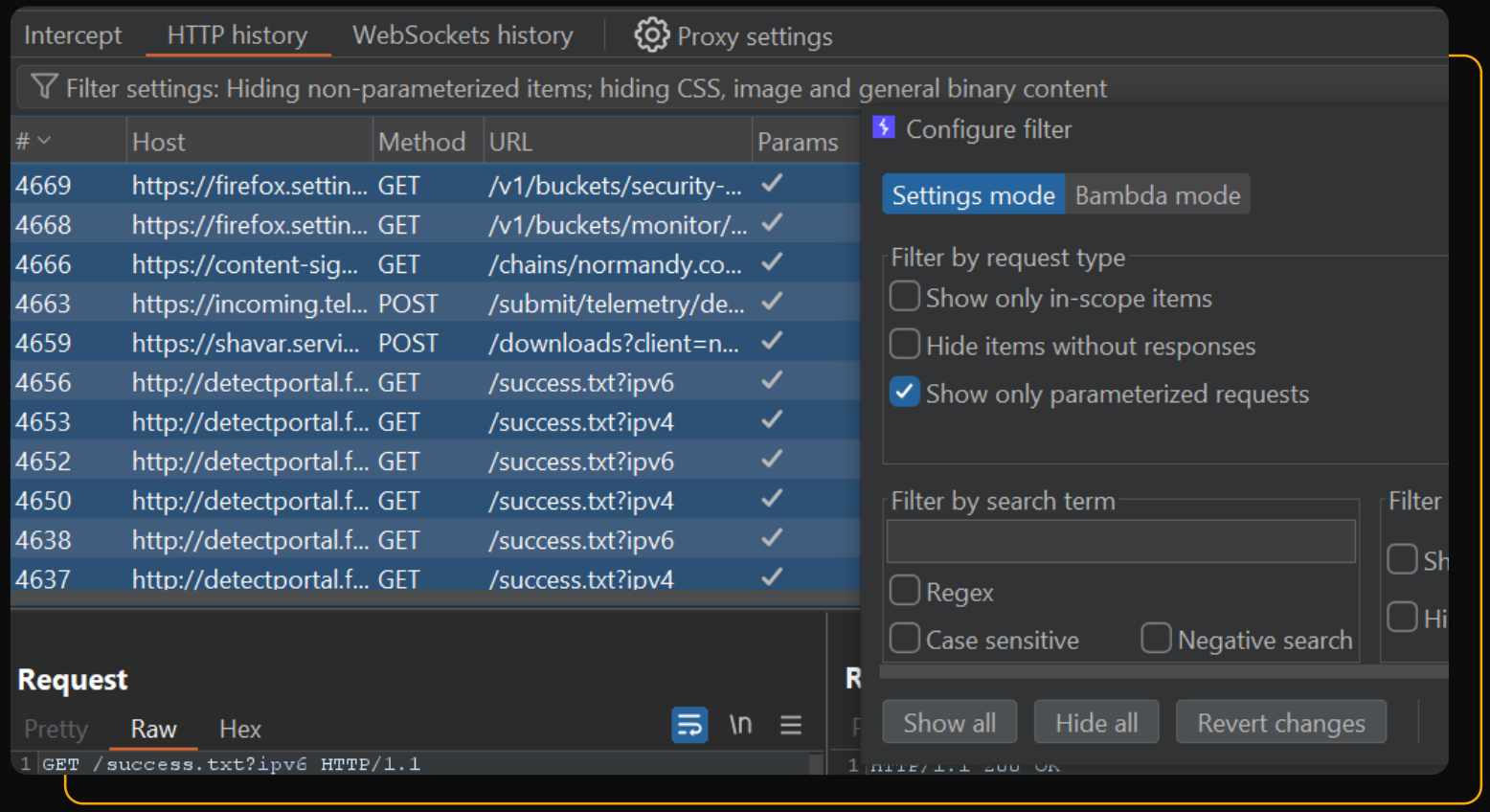
14/20 С помощью чего будем искать уязвимости?

BurpSuite

Nuclei

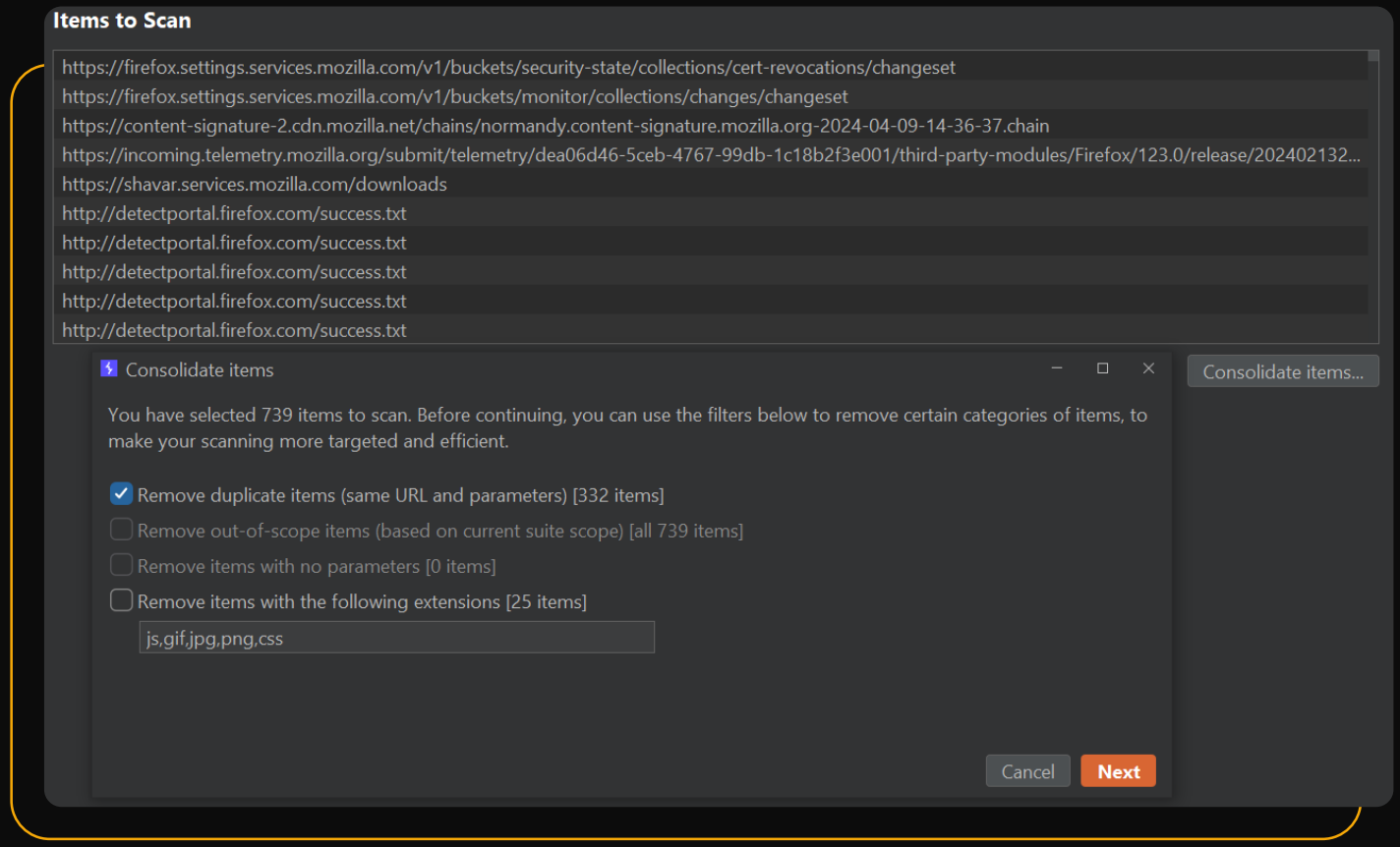
. . .

15/20 BurpSuite 1 шаг



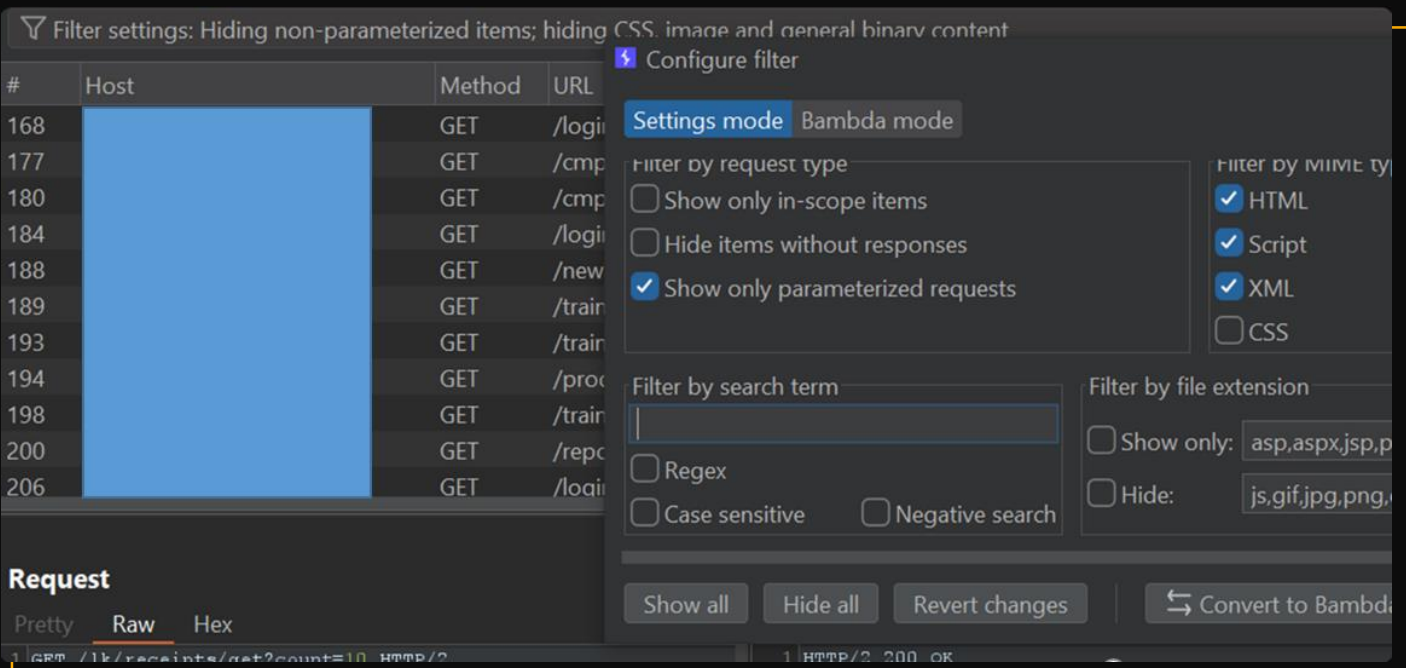
http history -> filter settings -> select params requests -> select all -> copy urls

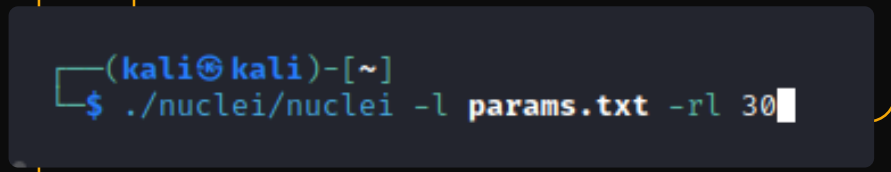
16/20 BurpSuite 2 шаг



scan-> consolidate items -> выбор типа сканирования

17/20 Nuclei

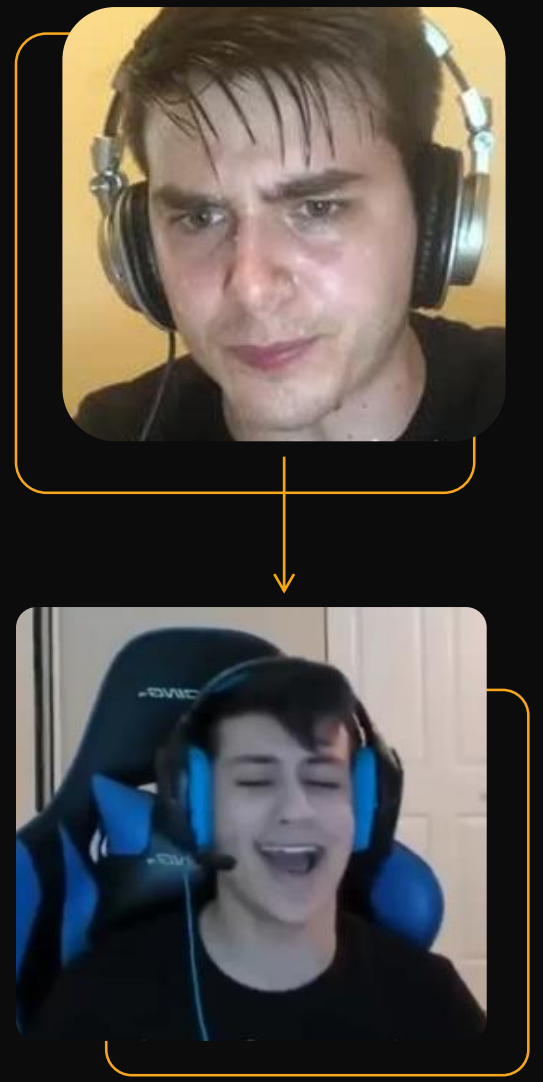




show params requests -> copy to params.txt -> ./nuclei –l params.txt –rl treads

18/20 Итоги

- Рассмотрели инструмент для эффективной работы с веб-кешем
- Получили первоначальные конечные точки для анализа
- Получили перечень URL-адресов для сканирования и дальнейших ручных проверок
- Сократили время необходимое для проведения первичной разведки периметра с 3-4 дней до 1-2 часов



19/20 Используемые утилиты

- https://github.com/n3170n/WayBackTools - парсинг веб кеша
- https://github.com/projectdiscovery/httpx - проверка доступа
- https://github.com/hueristiq/xurlfind3r - получение данных веб кеша
- https://portswigger.net/bappstore/815bb4ab64e240618dc673d65016e919(GAP) – параметры и ссылки из JS
- https://portswigger.net/burp/releases/professional-community-2024-1-1-4?requestededition=community&requestedplatform= - BurpSuite
- https://github.com/projectdiscovery/nuclei - сканер nuclei
- https://github.com/projectdiscovery/katana - краулинг

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Спасибо за внимание!
Вопросы?

Никита Распопов
Специалист по анализу защищенности УЦСБ

nraspopov@ussc.ru +7 (965) 520-59-06

cybersec@ussc.ru

sec.ussc.ru

Ссылка на презентацию