

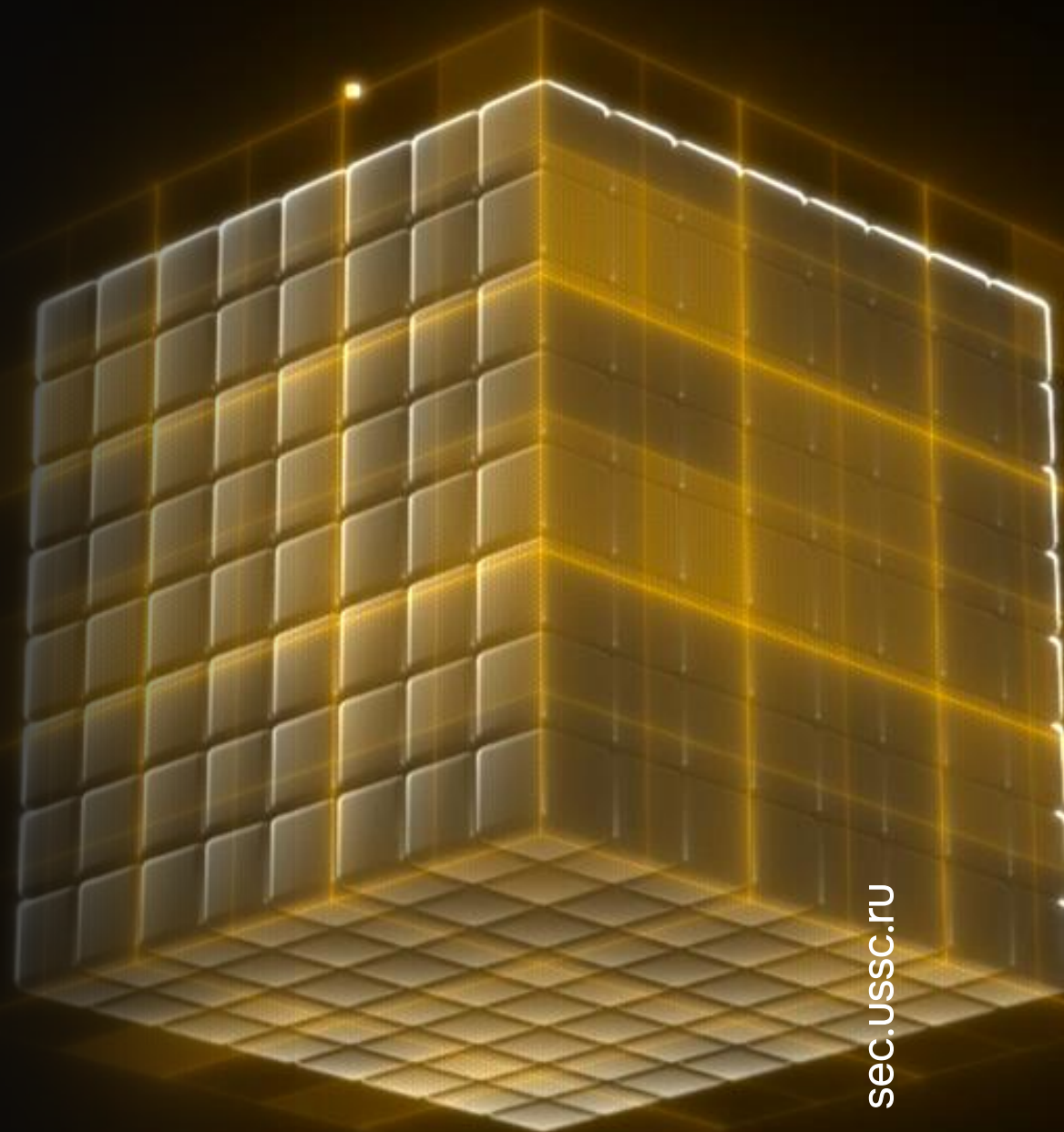


**ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ**

Fast recon — быстрая разведка при пентесте веб-приложения

Никита Распопов

Специалист по анализу защищенности УЦСБ



sec.uscc.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

```
File Actions Edit View Help
1 x 2 x .. x
(kali@kali)-[~]
└─$ subfinder -silent -d [REDACTED]

(kali@kali)-[~]
└─$ ./xurlfind3r -d [REDACTED]

[otx] [REDACTED]
[otx] [REDACTED]
[otx] [REDACTED]
[otx] [REDACTED]
[otx] [REDACTED]

(kali@kali)-[~]
└─$ dirsearch -u [REDACTED] -w ~/SecLists/Discovery/Web-Content
/dirsearch.txt -t 10 -r 1

dirsearch v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 10 | Word
list size: 29378
Output File: /home/kali/.dirsearch/reports/[REDACTED]_-24-03-05_02-24-2
8.txt
Error Log: /home/kali/.dirsearch/logs/errors-24-03-05_02-24-28.log
Target: [REDACTED]

(kali@kali)-[~]
└─$ echo [REDACTED] | hakrawler
```



- ! Долго
- ! Неудобно
- ! Тяжело отслеживать результаты



5/20 Критерии качественной разведки

Фильтровать
недоступные доменные
имена

Эффективно парсить
веб-кеш приложений

Составить sitemap
приложения
для dirsearch

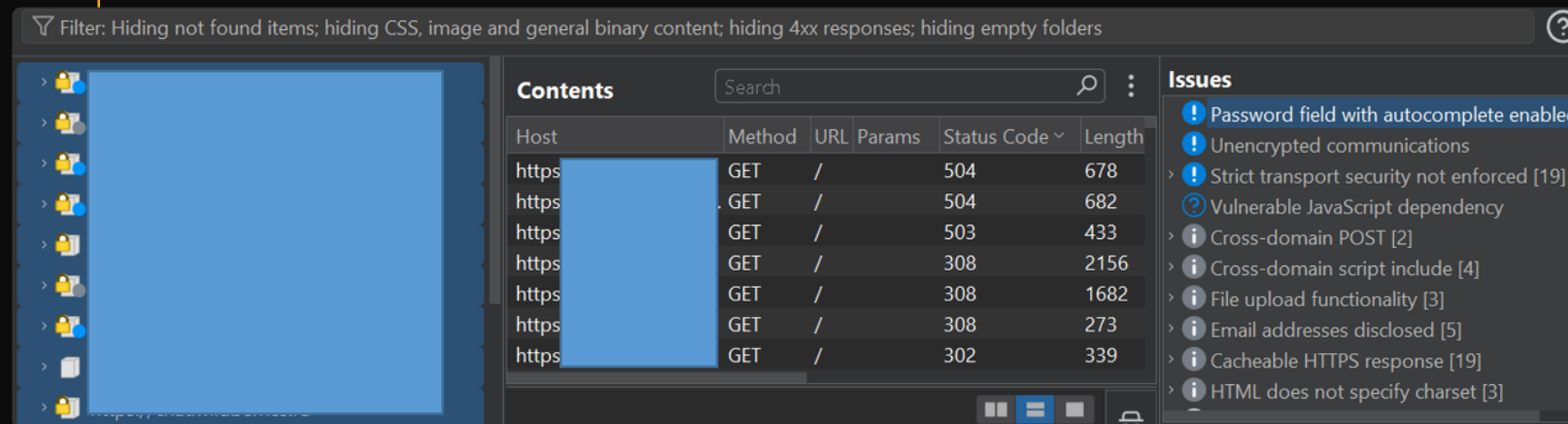
Конечные точки
и параметры
из JS-файлов



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
```

```
(kali@kali)-[~]
└─$ ./xurlfind3r -d [REDACTED] | awk '{ print $2}' | waybtools -tr
WayBack Toolkit 0.1.0
```

```
WayBack Toolkit v0.3.0
```

```
[*] Start Job
```

```
[*] [REDACTED]
```

```
> training → [REDACTED]
```

```
> instructions → [REDACTED]
```

```
> dictionary → [REDACTED]
```

```
> faqs → [REDACTED]
```

```
> main → [REDACTED]
```

```
> uploading → https://[REDACTED]
```

```
> service → https://[REDACTED]
```

```
> suppliers → https://[REDACTED]
```

```
> discount → https://[REDACTED]
```

```
> setDiscounts → [REDACTED]
```

```
> supplementary → http://[REDACTED]
```

```
(kali@kali)-[~]
└─$ ./xurlfind3r -d [REDACTED] | awk '{ print $2}' | waybtools -g brute
```

```
WayBack Toolkit v0.3.0
```

```
WayBack Toolkit 0.1.0
```

```
[*] Start Job
```

```
[*] End Job
```

```
(kali@kali)-[~]
```

```
└─$ cat brute
```

```
https://[REDACTED]/
https://[REDACTED]/training/
https://[REDACTED]/training/instructions/
https://[REDACTED]/training/instructions/dictionary/
https://[REDACTED]/discount/
https://[REDACTED]/analytics/
https://[REDACTED]/login/
https://[REDACTED]/cmp/
https://[REDACTED]/cmp/campaigns/
https://[REDACTED]/cmp/campaigns/list/
https://[REDACTED]/cmp/statistics/
```




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		GET	/			301	369
2426		GET	/			301	369
2425		GET				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

```
endpoints.txt — Блокнот
Файл Правка Формат Вид Справка
https://...es.ru/runtime.b87b2b86ae90f7e7.js
https://...es.ru/polyfills.2a59d29e36746caf.js
https://...es.ru/main.676df7087737df69.js
https://...u/
https://...u/services/trudoustroystvo
https://...u/profile/balance
https://...u/
https://...u/runtime.js?69e367661ede6756d822
https://...u/vendors.js?dd6ffb7c0f5a973240a6
https://...u/localization.js?b36966e8638a7204fe28
https://...u/main.js?16754511019e87a5f774
https://...ru/rainloop/v/1.17.0/static/js/min/polyfills.min.js?legacy
https://...ru/rainloop/v/1.17.0/static/js/min/boot.min.js?legacy
https://...clips
https://...videos
```

```
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)

Potential params found - 201 filtered: Show origin Words found - 54 filtered: Show or

uiv	Guru
url	Gurus
userId	JavaScript
userName	JavaScripts
user_id	Mail
username	Mails
utm_campaign	PRO
utm_medium	PROES
utm_source	Stream
vn-	Streams
	Telegram

Show "sus" Show query string with value XNLV Stop words: a,aboard,about,above,across

Potential links found - 8224 unique: Show origin endpoint In scope only

```
/account/manager/subordinates/tree
/account/manager/subordinates/requ
/account/manager/subordinates/requ
/account/manager/teams [https://tea
/account/manager/teams [https://tea
/account/manager/teams/[slug] [http
/account/manager/teams/[slug] [http
/account/manager/teams/add [https:
/account/manager/teams/add [https:
/account/manager/teams/edit/[slug]
/account/manager/teams/edit/[slug]
```

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

The screenshot shows the Burp Suite interface with the HTTP history tab selected. The history table lists several requests, with the last one selected. The filter settings panel is open, showing the 'Show only parameterized requests' option checked. The 'Request' tab is also visible at the bottom.

#	Host	Method	URL	Params
4669	https://firefox.settin...	GET	/v1/buckets/security-...	✓
4668	https://firefox.settin...	GET	/v1/buckets/monitor/...	✓
4666	https://content-sig...	GET	/chains/normandy.co...	✓
4663	https://incoming.tel...	POST	/submit/telemetry/de...	✓
4659	https://shavar.servi...	POST	/downloads?client=n...	✓
4656	http://detectportal.f...	GET	/success.txt?ipv6	✓
4653	http://detectportal.f...	GET	/success.txt?ipv4	✓
4652	http://detectportal.f...	GET	/success.txt?ipv6	✓
4650	http://detectportal.f...	GET	/success.txt?ipv4	✓
4638	http://detectportal.f...	GET	/success.txt?ipv6	✓
4637	http://detectportal.f...	GET	/success.txt?ipv4	✓

Filter settings: Hiding non-parameterized items; hiding CSS, image and general binary content

Configure filter

Settings mode Bambda mode

Filter by request type

- Show only in-scope items
- Hide items without responses
- Show only parameterized requests

Filter by search term

Regex Case sensitive Negative search

Show all Hide all Revert changes

Request

Pretty Raw Hex

1 GET /success.txt?ipv6 HTTP/1.1

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



16/20 BurpSuite 2 шаг

Items to Scan

- https://firefox.settings.services.mozilla.com/v1/buckets/security-state/collections/cert-revocations/changeset
- https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset
- https://content-signature-2.cdn.mozilla.net/chains/normandy.content-signature.mozilla.org-2024-04-09-14-36-37.chain
- https://incoming.telemetry.mozilla.org/submit/telemetry/dea06d46-5ceb-4767-99db-1c18b2f3e001/third-party-modules/Firefox/123.0/release/202402132...
- https://shavar.services.mozilla.com/downloads
- http://detectportal.firefox.com/success.txt
- http://detectportal.firefox.com/success.txt
- http://detectportal.firefox.com/success.txt
- http://detectportal.firefox.com/success.txt
- http://detectportal.firefox.com/success.txt

Consolidate items

You have selected 739 items to scan. Before continuing, you can use the filters below to remove certain categories of items, to make your scanning more targeted and efficient.

- Remove duplicate items (same URL and parameters) [332 items]
- Remove out-of-scope items (based on current suite scope) [all 739 items]
- Remove items with no parameters [0 items]
- Remove items with the following extensions [25 items]

Cancel Next

scan-> consolidate items -> выбор типа сканирования



17/20 Nuclei

Filter settings: Hiding non-parameterized items; hiding CSS, image and general binary content

Configure filter

Settings mode Bambda mode

Filter by request type

- Show only in-scope items
- Hide items without responses
- Show only parameterized requests

Filter by MIME type

- HTML
- Script
- XML
- CSS

Filter by search term

Regex Case sensitive Negative search

Filter by file extension

Show only: asp,aspx,jsp,p

Hide: js,gif,jpg,png,

Show all Hide all Revert changes Convert to Bambda

#	Host	Method	URL
168		GET	/logi
177		GET	/cmp
180		GET	/cmp
184		GET	/logi
188		GET	/new
189		GET	/train
193		GET	/train
194		GET	/proc
198		GET	/train
200		GET	/repc
206		GET	/logi

Request

Pretty Raw Hex

1 GET /lk/receipts/get?count=10 HTTP/2 1 HTTP/2 200 OK

```
(kali@kali)-[~]  
└─$ ./nuclei/nuclei -l params.txt -rl 30
```

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

