# WEB

...

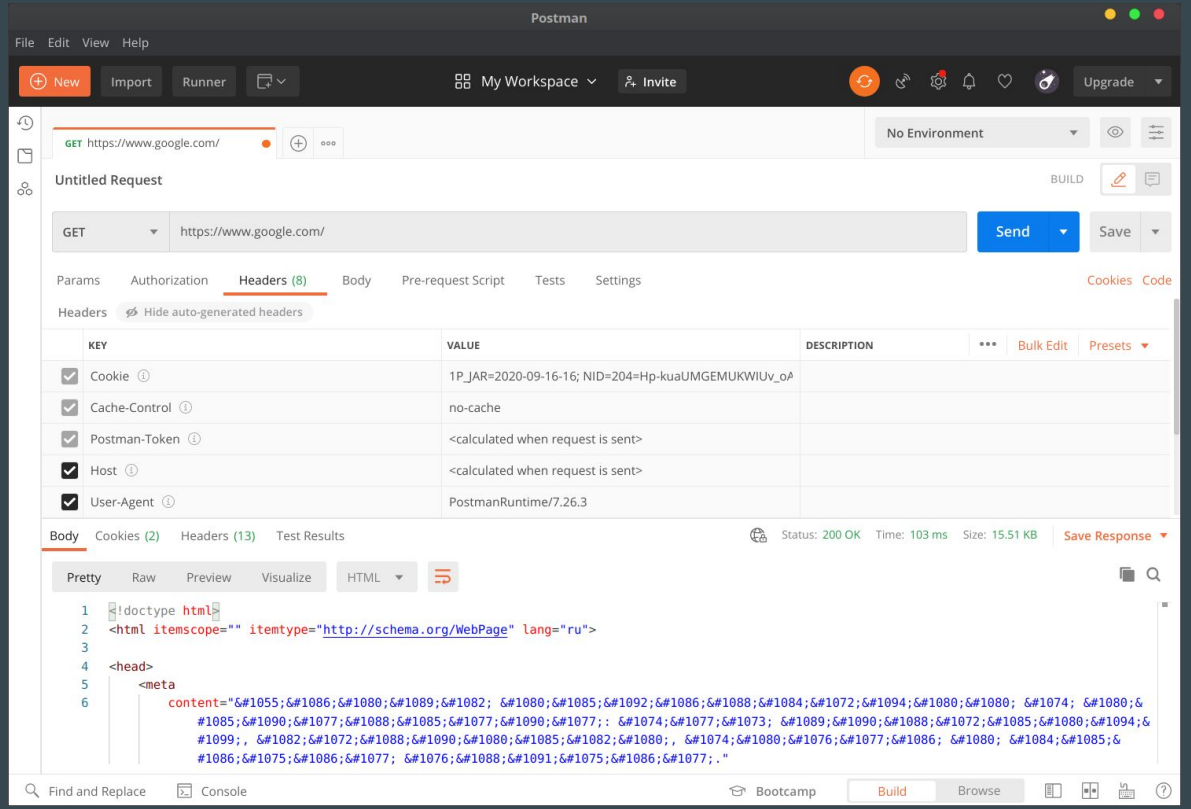
# Web

Tools:

- Postman
- Burp Suite
- Python
- Nmap, nikto, etc..
- Ручки, гугл, голова

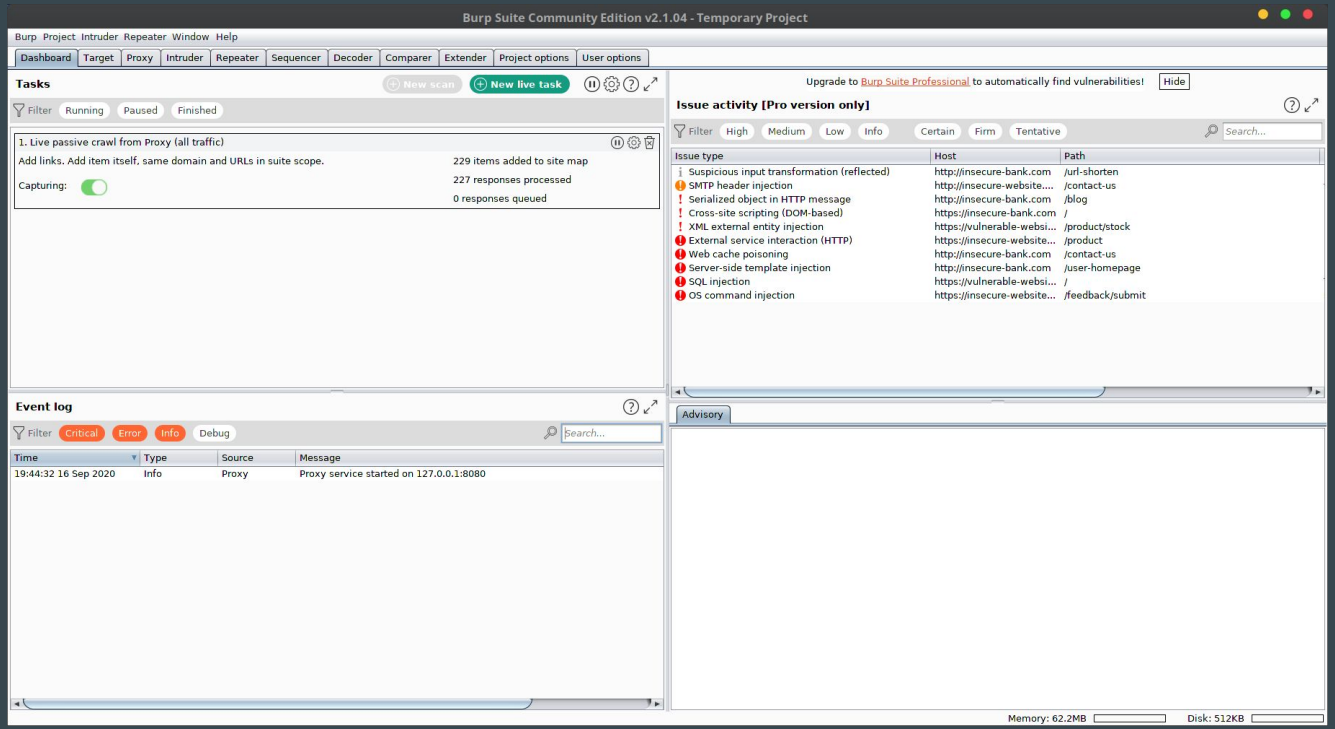
# Postman

В нём максимально простой и интуитивно понятный интерфейс. Любой запрос, любого типа, с любыми параметрами он отправит. Стоит просто потыкать, посмотреть мб тутор, попробовать и всё станет понятно.



# Burp Suite

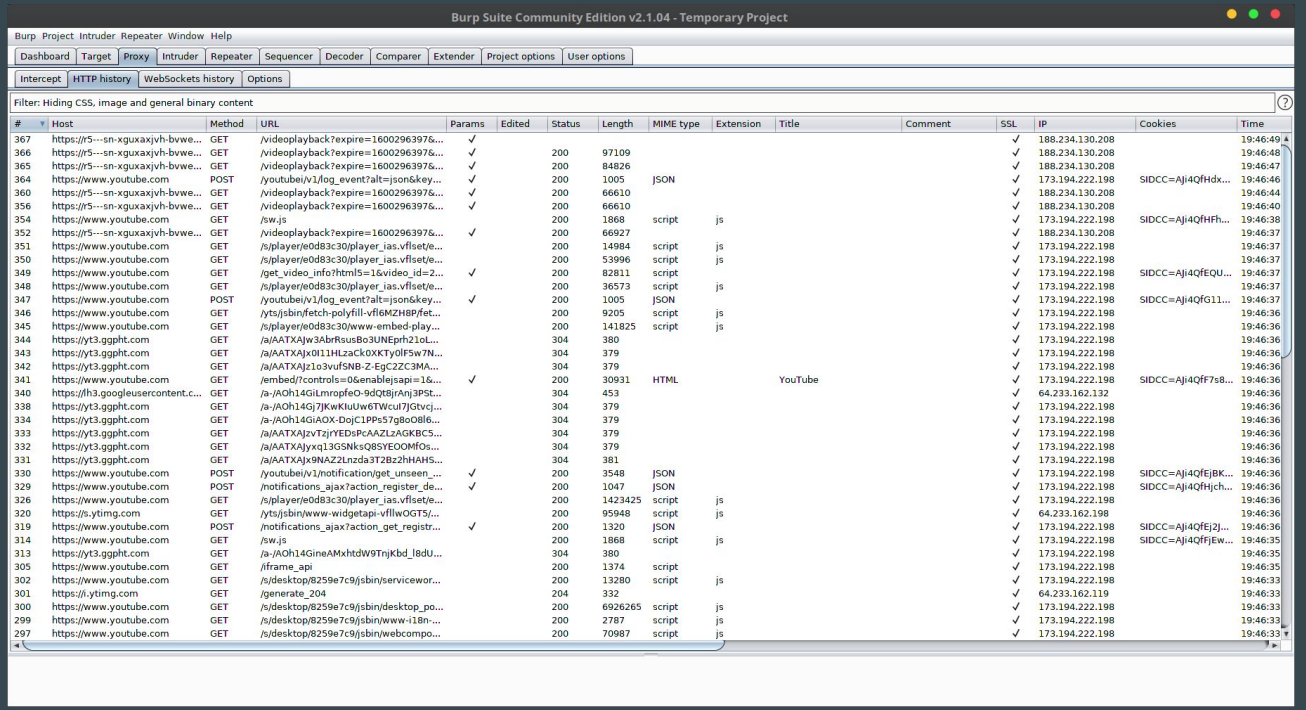
Это уже тяжелее и не так-то просто его поставить и настроить, но и его возможности совсем другие.



# Что в Burp’е есть?

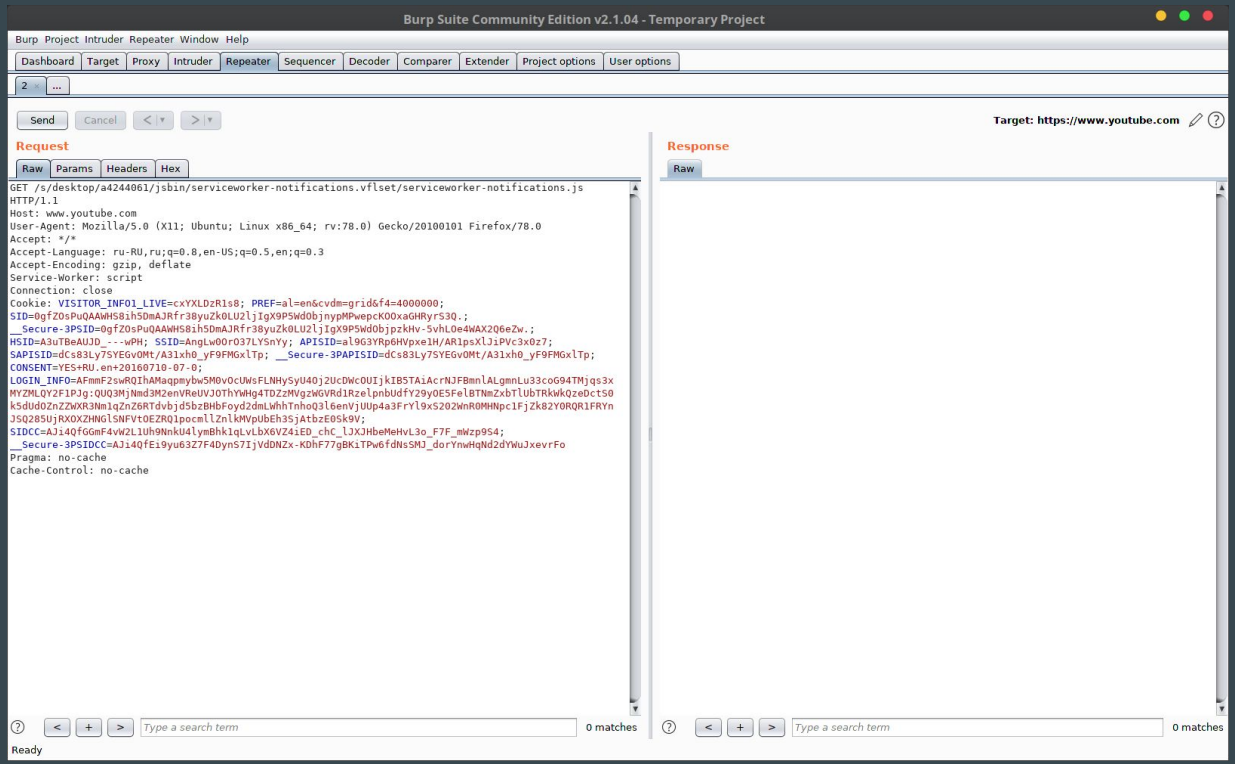
- Возможность посмотреть каждый выходящий и входящий пакет. (HTTP history)
- Breakpoint на вход и выход пакетов, иногда очень удобно, когда сервер выкидывает сразу кучу всего, таким образом можно выбирать что пропускать дальше, а что откинуть.
- Repeater. Вы поймали пакет и теперь хочется изменить, как раз для этого репитер и есть в этой программе. В следующих слайдах я покажу как это происходит.
- Простенький декодер хекса, бейса и тп
- Функций в нём куда больше, я сейчас буду показывать и говорить об основных.

300 пакетиков пролетело, стоило просто зайти на ютуб. Отправим первый попавшийся в repeater и получше посмотрим. Выбираем пакет - пкм - Send to repeater.



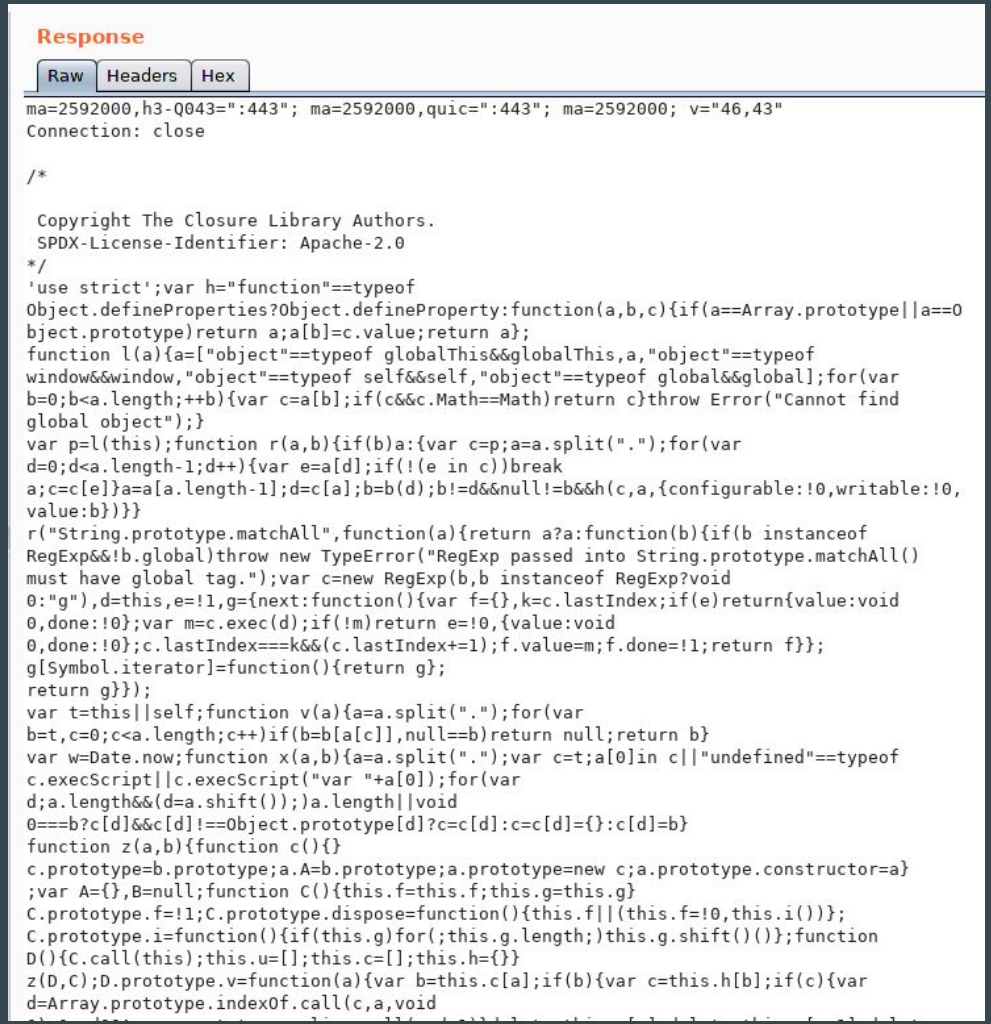

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title | Comment | SSL | IP | Cookies | Time |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 367 | https://r5---sn-xguxaxjvh-bvwe... | GET | /videoplayback?expire=1600296397&... | ✓ | | | | | | | | ✓ | 188.234.130.208 | | 19:46:49 |
| 366 | https://r5---sn-xguxaxjvh-bvwe... | GET | /videoplayback?expire=1600296397&... | ✓ | | 200 | 97109 | | | | | ✓ | 188.234.130.208 | | 19:46:48 |
| 365 | https://r5---sn-xguxaxjvh-bvwe... | GET | /videoplayback?expire=1600296397&... | ✓ | | 200 | 84826 | | | | | ✓ | 188.234.130.208 | | 19:46:47 |
| 364 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json&key... | ✓ | | 200 | 1005 | JSON | | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfHdx... | 19:46:46 |
| 360 | https://r5---sn-xguxaxjvh-bvwe... | GET | /videoplayback?expire=1600296397&... | ✓ | | 200 | 66610 | | | | | ✓ | 188.234.130.208 | | 19:46:44 |
| 356 | https://r5---sn-xguxaxjvh-bvwe... | GET | /videoplayback?expire=1600296397&... | ✓ | | 200 | 66610 | | | | | ✓ | 188.234.130.208 | | 19:46:40 |
| 354 | https://www.youtube.com | GET | /sw.js | | | 200 | 1868 | script | js | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfHFh... | 19:46:38 |
| 352 | https://r5---sn-xguxaxjvh-bvwe... | GET | /videoplayback?expire=1600296397&... | ✓ | | 200 | 66927 | | | | | ✓ | 188.234.130.208 | | 19:46:37 |
| 351 | https://www.youtube.com | GET | /s/player/e0d83c30/player_ias.vflset/e... | | | 200 | 14984 | script | js | | | ✓ | 173.194.222.198 | | 19:46:37 |
| 350 | https://www.youtube.com | GET | /s/player/e0d83c30/player_ias.vflset/e... | | | 200 | 53996 | script | js | | | ✓ | 173.194.222.198 | | 19:46:37 |
| 349 | https://www.youtube.com | GET | /get_video_info?html5=1&video_id=2... | ✓ | | 200 | 82811 | script | | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfEQU... | 19:46:37 |
| 348 | https://www.youtube.com | GET | /s/player/e0d83c30/player_ias.vflset/e... | | | 200 | 36573 | script | js | | | ✓ | 173.194.222.198 | | 19:46:37 |
| 347 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json&key... | ✓ | | 200 | 1005 | JSON | | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfG11... | 19:46:37 |
| 346 | https://www.youtube.com | GET | /yts/jsbin/fetch-polyfill-vfl6MZH8P/fet... | | | 200 | 9205 | script | js | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 345 | https://www.youtube.com | GET | /s/player/e0d83c30/www-embed-play... | | | 200 | 141825 | script | js | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 344 | https://yt3.ggpht.com | GET | /a/AATXAJw3AbrRsusBo3UNEprh21oL... | | | 304 | 380 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 343 | https://yt3.ggpht.com | GET | /a/AATXAJx0l11HLzaCk0XKTy0lF5w7N... | | | 304 | 379 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 342 | https://yt3.ggpht.com | GET | /a/AATXAJz1o3vufSNB-Z-EgC2ZC3MA... | | | 304 | 379 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 341 | https://www.youtube.com | GET | /embed/?controls=0&enablejsapi=1&... | ✓ | | 200 | 30931 | HTML | | YouTube | | ✓ | 173.194.222.198 | SIDCC=AJi4QfF7s8... | 19:46:36 |
| 340 | https://lh3.googleusercontent.c... | GET | /a-/AOh14GiLmropfeO-9dQt8jrAnj3PSt... | | | 304 | 453 | | | | | ✓ | 64.233.162.132 | | 19:46:36 |
| 338 | https://yt3.ggpht.com | GET | /a-/AOh14Gj7JKwKIuUw6TWcul7JGtvcj... | | | 304 | 379 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 334 | https://yt3.ggpht.com | GET | /a-/AOh14GiAOX-DojC1PPs57g8oO8l6... | | | 304 | 379 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 333 | https://yt3.ggpht.com | GET | /a/AATXAJzvTzjrYEDsPcAAZLzAGKBC5... | | | 304 | 379 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 332 | https://yt3.ggpht.com | GET | /a/AATXAJyxq13GSNksQ8SYEOOMfOs... | | | 304 | 379 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 331 | https://yt3.ggpht.com | GET | /a/AATXAJx9NAZ2Lnzda3T2Bz2hHAHS... | | | 304 | 381 | | | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 330 | https://www.youtube.com | POST | /youtubei/v1/notification/get_unseen_... | ✓ | | 200 | 3548 | JSON | | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfEjBK... | 19:46:36 |
| 329 | https://www.youtube.com | POST | /notifications_ajax?action_register_de... | ✓ | | 200 | 1047 | JSON | | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfHjch... | 19:46:36 |
| 326 | https://www.youtube.com | GET | /s/player/e0d83c30/player_ias.vflset/e... | | | 200 | 1423425 | script | js | | | ✓ | 173.194.222.198 | | 19:46:36 |
| 320 | https://s.ytimg.com | GET | /yts/jsbin/www-widgetapi-vfllwOGT5/... | | | 200 | 95948 | script | js | | | ✓ | 64.233.162.198 | | 19:46:36 |
| 319 | https://www.youtube.com | POST | /notifications_ajax?action_get_registr... | ✓ | | 200 | 1320 | JSON | | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfEj2j... | 19:46:36 |
| 314 | https://www.youtube.com | GET | /sw.js | | | 200 | 1868 | script | js | | | ✓ | 173.194.222.198 | SIDCC=AJi4QfFjEw... | 19:46:35 |
| 313 | https://yt3.ggpht.com | GET | /a-/AOh14GineAMxhtdW9TnjKbd_l8dU... | | | 304 | 380 | | | | | ✓ | 173.194.222.198 | | 19:46:35 |
| 305 | https://www.youtube.com | GET | /jframe_api | | | 200 | 1374 | script | | | | ✓ | 173.194.222.198 | | 19:46:35 |
| 302 | https://www.youtube.com | GET | /s/desktop/8259e7c9/jsbin/servicewor... | | | 200 | 13280 | script | js | | | ✓ | 173.194.222.198 | | 19:46:33 |
| 301 | https://i.ytimg.com | GET | /generate_204 | | | 204 | 332 | | | | | ✓ | 64.233.162.119 | | 19:46:33 |
| 300 | https://www.youtube.com | GET | /s/desktop/8259e7c9/jsbin/desktop_po... | | | 200 | 6926265 | script | js | | | ✓ | 173.194.222.198 | | 19:46:33 |
| 299 | https://www.youtube.com | GET | /s/desktop/8259e7c9/jsbin/www-i18n-... | | | 200 | 2787 | script | js | | | ✓ | 173.194.222.198 | | 19:46:33 |
| 297 | https://www.youtube.com | GET | /s/desktop/8259e7c9/jsbin/webcompo... | | | 200 | 70987 | script | js | | | ✓ | 173.194.222.198 | | 19:46:33 |

Тут полностью тело запроса, которое можно изменять и отправить заново, нажав на Send



Я не изменял тело запроса, просто нажал Send и получил такой ответ от yt.

(Можно ломать, дада, быстрее)



# Python

Основная либа:

- Requests

  С ней можно тоже посылать запросы в любом виде и смотреть ответы от сервера.

  Хорошая статья о ней с примерами

- Также питон позволяет все это автоматизировать, что на некоторых задачах крайне необходимо.

# Ручки, гугл, голова

Да именно они, ведь практически все вещи можно найти в интернете, разобрать и изменить под конкретную задачу.

Всегда читайте и гуглите врайтапы, к примеру “writeups web ctf” и вы найдете кучу новой инфы каждый раз. Если знаете какая уязвимость, но никак не можете разобраться как ее эксплуатировать, то, к примеру, запрос о SQLi “sqli bypass” выдаст вам примеры и возможно объяснения почему так происходит, что крайне необходимо.

Сам по себе веб безумно большой и крайне разносторонний, поэтому “ручки, гугл, голова” - это ваша основная тулза!