

# WEB

...

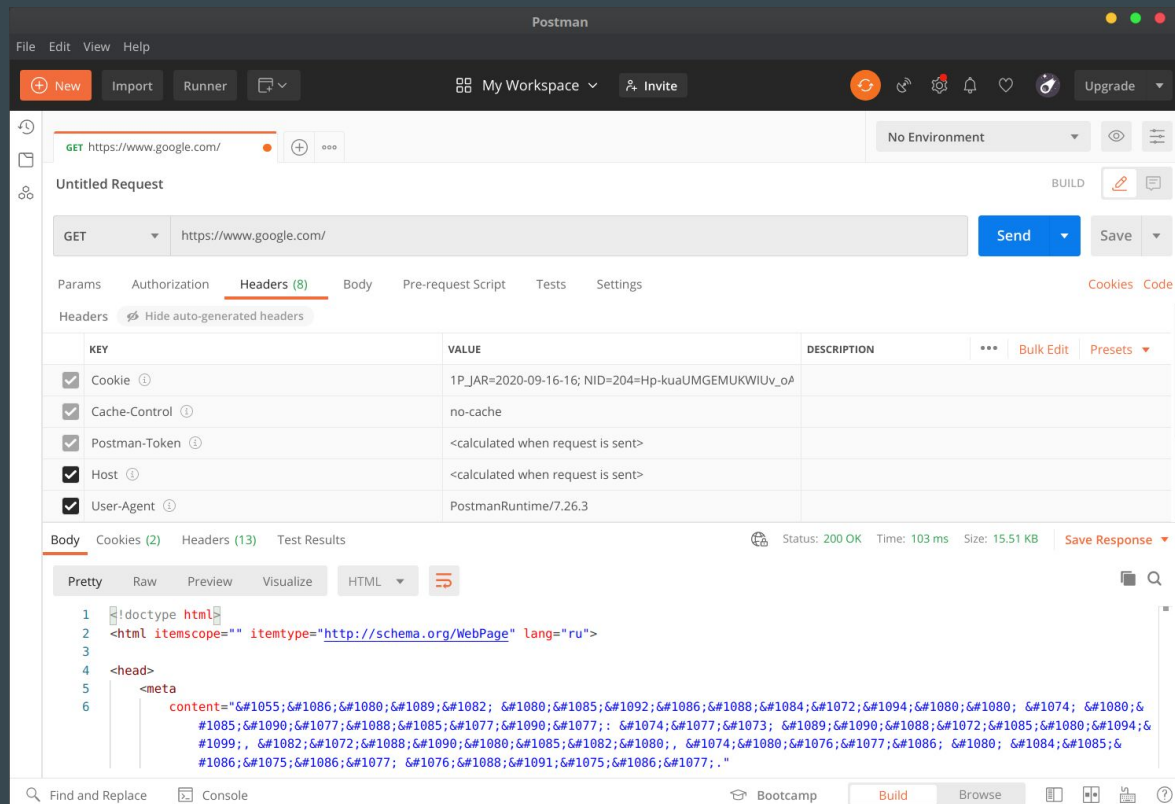
# Web

Tools:

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

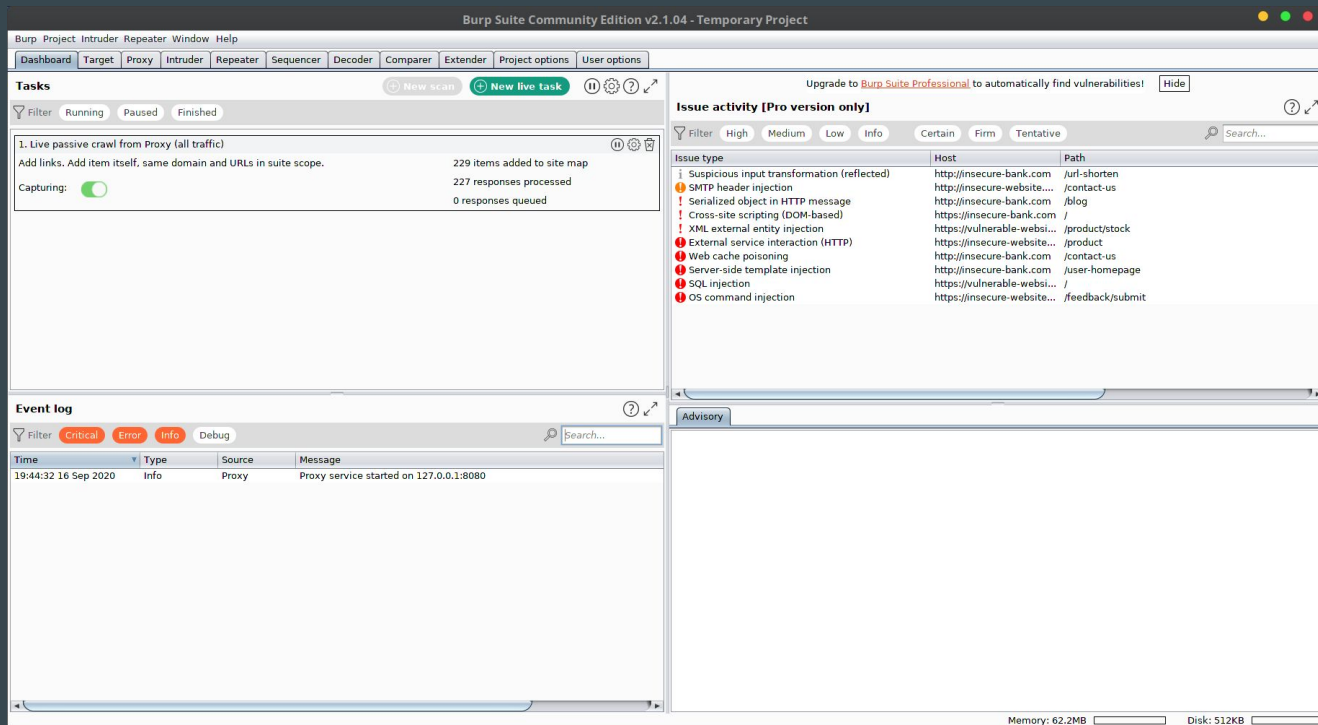
# Postman

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.



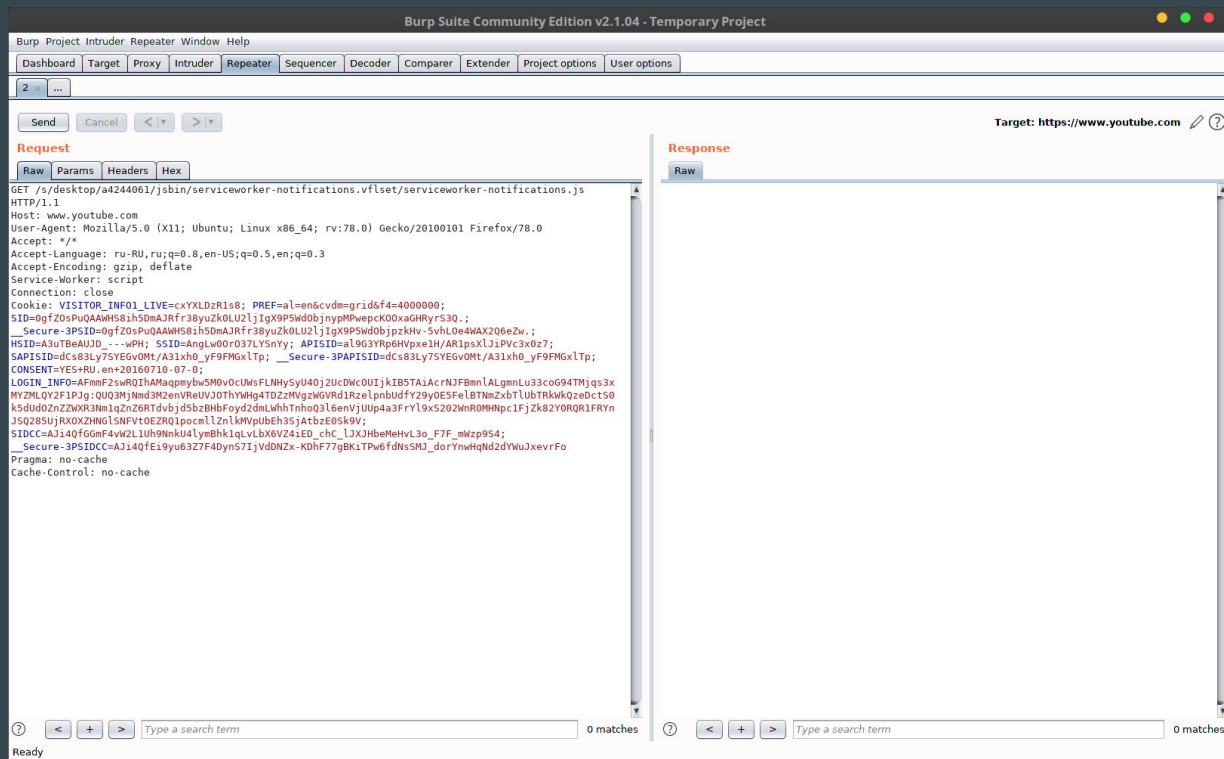
# Что в Burp'е есть?

- 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.

Burp Suite Community Edition v2.1.04 - Temporary Project																
Burp Project Intruder Repeater Window Help																
Dashboard   Target   Proxy   Intruder   Repeater   Sequencer   Decoder   Comparer   Extender   Project options   User options																
Intercept   HTTP history   WebSockets history   Options																
Filter: Hiding CSS, image and general binary content																
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	
367	https://rs---sn-xguxaxjh-bvwe...	GET	/videoplayback?expire=16002963976...	✓								✓	188.234.130.208		19:46:49	4
366	https://rs---sn-xguxaxjh-bvwe...	GET	/videoplayback?expire=16002963976...	✓		200	97109					✓	188.234.130.208		19:46:48	
365	https://rs---sn-xguxaxjh-bvwe...	GET	/videoplayback?expire=16002963976...	✓		200	84826					✓	188.234.130.208		19:46:47	
364	https://www.youtube.com	POST	/youtube/v1/log_event?alt=json&key=...	✓		200	1005	JSON				✓	173.194.222.198	SIDCC=Aji4QfHd...	19:46:46	
360	https://rs---sn-xguxaxjh-bvwe...	GET	/videoplayback?expire=16002963976...	✓		200	66610					✓	188.234.130.208		19:46:44	
356	https://rs---sn-xguxaxjh-bvwe...	GET	/videoplayback?expire=16002963976...	✓		200	66610					✓	188.234.130.208		19:46:40	
354	https://www.youtube.com	GET	/sw.js			200	1688	script	js			✓	173.194.222.198	SIDCC=Aji4QfHf...	19:46:38	
352	https://rs---sn-xguxaxjh-bvwe...	GET	/videoplayback?expire=16002963976...	✓		200	66927					✓	188.234.130.208		19:46:37	
351	https://www.youtube.com	GET	/i/player/0d83c30/player_ias.vflset/...			200	14984	script	js			✓	173.194.222.198		19:46:37	
350	https://www.youtube.com	GET	/i/player/0d83c30/player_ias.vflset/...			200	35996	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=Aji4QfEU...	19:46:37	
348	https://www.youtube.com	GET	/i/player/0d83c30/player_ias.vflset/...			200	36573	script	js			✓	173.194.222.198		19:46:37	
347	https://www.youtube.com	POST	/youtube/v1/log_event?alt=json&key=...	✓		200	1005	JSON				✓	173.194.222.198	SIDCC=Aji4QfG11...	19:46:37	
346	https://www.youtube.com	GET	/ytjs/bin/fetch-polyfill-vfl6M2H8P/fet...			200	9205	script	js			✓	173.194.222.198		19:46:36	
345	https://www.youtube.com	GET	/i/player/0d83c30/www-embed-play...			200	141825	script	js			✓	173.194.222.198		19:46:36	
344	https://yt3.ggpht.com	GET	/a/AATXAJw3AbrRusBo3UNPfh21oL...			304	380					✓	173.194.222.198		19:46:36	
343	https://yt3.ggpht.com	GET	/a/AATXAJx0i11HLzaCkOXkTyOlF5w7N...			304	379					✓	173.194.222.198		19:46:36	
342	https://yt3.ggpht.com	GET	/a/AATXAJz1o3vufSNB-2_EgC2ZC3MA...			304	379					✓	173.194.222.198		19:46:36	
341	https://www.youtube.com	GET	/embed/controls=0&enablejsapi=1&...	✓		200	30931			YouTube		✓	173.194.222.198	SIDCC=Aji4Qf7s8...	19:46:36	
340	https://h3.googleusercontent.c...	GET	/a-/AOH14GiUmropf6O-9dQ8jBjAnj3PSt...			304	453	HTML				✓	64.233.162.132		19:46:36	
338	https://yt3.ggpht.com	GET	/a-/AOH14Gi7JKwKluUw6TWcu7jGtvCj...			304	379					✓	173.194.222.198		19:46:36	
334	https://yt3.ggpht.com	GET	/a-/AOH14GiAOX-DojC1PPs57g8o08L6...			304	379					✓	173.194.222.198		19:46:36	
333	https://yt3.ggpht.com	GET	/a/AATXAJzTvTzjYEDsPCAAZLZAGKBCS...			304	379					✓	173.194.222.198		19:46:36	
332	https://yt3.ggpht.com	GET	/a/AATXAJxql3GSNksQ8SYEODMfOs...			304	379					✓	173.194.222.198		19:46:36	
331	https://yt3.ggpht.com	GET	/a/AATXAJx9NAZLZada3T2B2zh1AH5...			304	381					✓	173.194.222.198		19:46:36	
330	https://www.youtube.com	POST	/youtube/v1/notification/get_unseen...	✓		200	3548	JSON				✓	173.194.222.198	SIDCC=Aji4QfjBK...	19:46:36	
329	https://www.youtube.com	POST	/notifications_ajax?action_register_de...	✓		200	1047	JSON				✓	173.194.222.198	SIDCC=Aji4Qfjch...	19:46:36	
326	https://www.youtube.com	GET	/i/player/0d83c30/player_ias.vflset/...			200	1423425	script	js			✓	173.194.222.198		19:46:36	
320	https://s.ytimg.com	GET	/ytjs/bin/www-widgetapi-vflwOGTS/...			200	95948	script	js			✓	64.233.162.198		19:46:36	
319	https://www.youtube.com	POST	/notifications_ajax?action_get_regist...	✓		200	1320	JSON				✓	173.194.222.198	SIDCC=Aji4QfEj2...	19:46:36	
314	https://www.youtube.com	GET	/sw.js			200	1868	script	js			✓	173.194.222.198	SIDCC=Aji4QfjEw...	19:46:35	
313	https://yt3.ggpht.com	GET	/a-/AOH14GiAmeAMxhtdW9TnjkbJ_l8dU...			304	380					✓	173.194.222.198		19:46:35	
305	https://www.youtube.com	GET	/iframe_api			200	1374	script				✓	173.194.222.198		19:46:35	
302	https://www.youtube.com	GET	/i/desktop/8259e7c9jsbin/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	/i/desktop/8259e7c9jsbin/desktop_po...			200	6926265	script	js			✓	173.194.222.198		19:46:33	
299	https://www.youtube.com	GET	/i/desktop/8259e7c9jsbin/www-i18n...			200	2787	script	js			✓	173.194.222.198		19:46:33	
297	https://www.youtube.com	GET	/i/desktop/8259e7c9jsbin/webcomp...			200	70987	script	js			✓	173.194.222.198		19:46:33	

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



(Можно ломать, дада, быстрее)

Raw

## Headers

Hex

```
ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
Connection: close
```

1\*

Copyright The Closure Library Authors.  
SPDX-License-Identifier: Apache-2.0

```
'use strict';var h="function"==typeof
Object.defineProperty?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};
function l(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;+b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}
var p=l(this);function r(a,b){if(b){a:{var c=p;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break
a;c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&h(c,a,{configurable:!0,writable:!0,value:b})}}
r("String.prototype.matchAll",function(a){return a?a:function(b){if(b instanceof RegExp&&b.global)throw new TypeError("RegExp passed into String.prototype.matchAll() must have global tag.");var c=new RegExp(b,b instanceof RegExp?void 0:"g"),d=this,e=!1,g={next:function(){var f=c,k=c.lastIndex;if(e)return{value:void 0,done:!0};var m=c.exec(d);if(!m)return e=!0,{value:void 0,done:!0};c.lastIndex===k&&(c.lastIndex+=1);f.value=m;f.done=!1;return f}};g[Symbol.iterator]=function(){return g};
return g}});
var t=this||self;function v(a){a=a.split(".");for(var b=t,c=0;c<a.length;c++)if(b=b[a[c]],null==b)return null;return b}
var w=Date.now;function x(a,b){a=a.split(".");var c=t;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());a.length||void 0===b?c[d]&&c[d]!==Object.prototype[d]?c=c[d]:c[d]=b:
function z(a,b){function c(){}}
c.prototype=b.prototype;a.A=b.prototype;a.prototype=new c;a.prototype.constructor=a;
var A={},B=null;function C(){this.f=this.f;this.g=this.g}
C.prototype.f=1;C.prototype.dispose=function(){this.f||this.f=!0,this.i()};
C.prototype.i=function(){if(this.g)for(;this.g.length;)this.g.shift();function D(){C.call(this);this.u=[];this.c=[];this.h={}}
z(D,C);D.prototype.v=function(a){var b=this.c[a];if(b){var c=this.h[b];if(c){var d=Array.prototype.indexOf.call(c,a,void
```



# 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 вайтапы, 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!