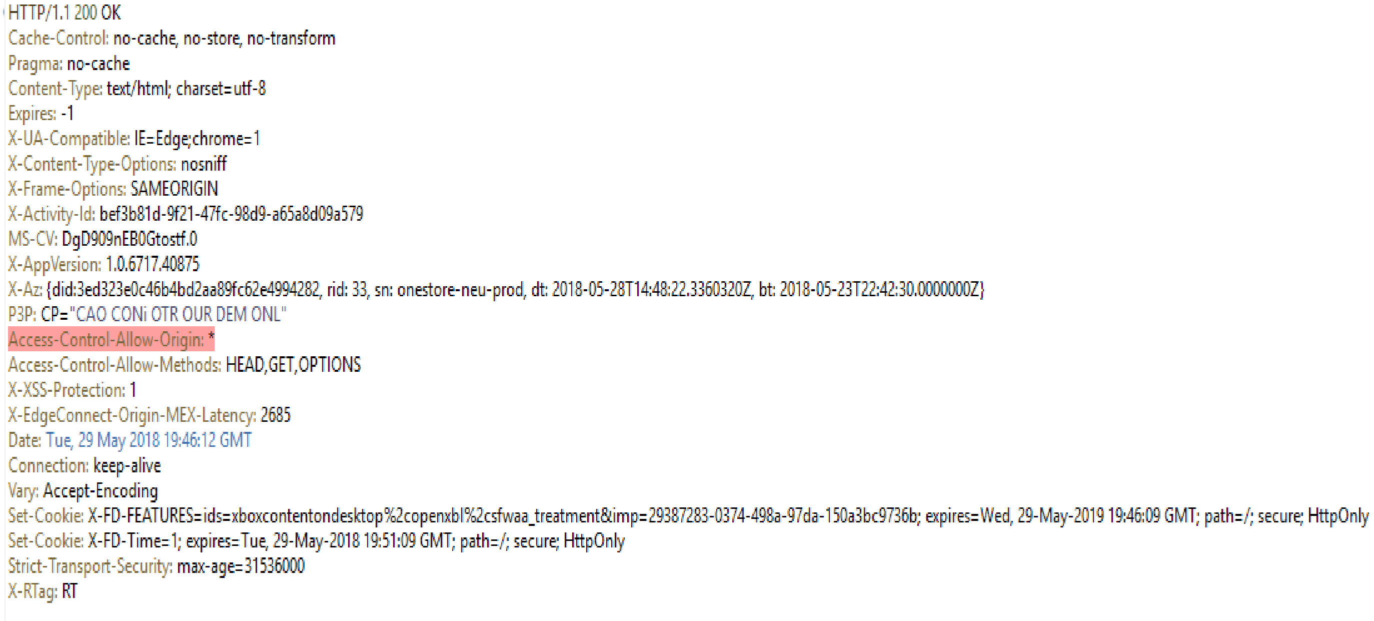
Security Summary

www.microsoft.com/en-in/

Submitted By :- Chaitanya Laxman

1. Insecure Cross-Origin Resource Access Control

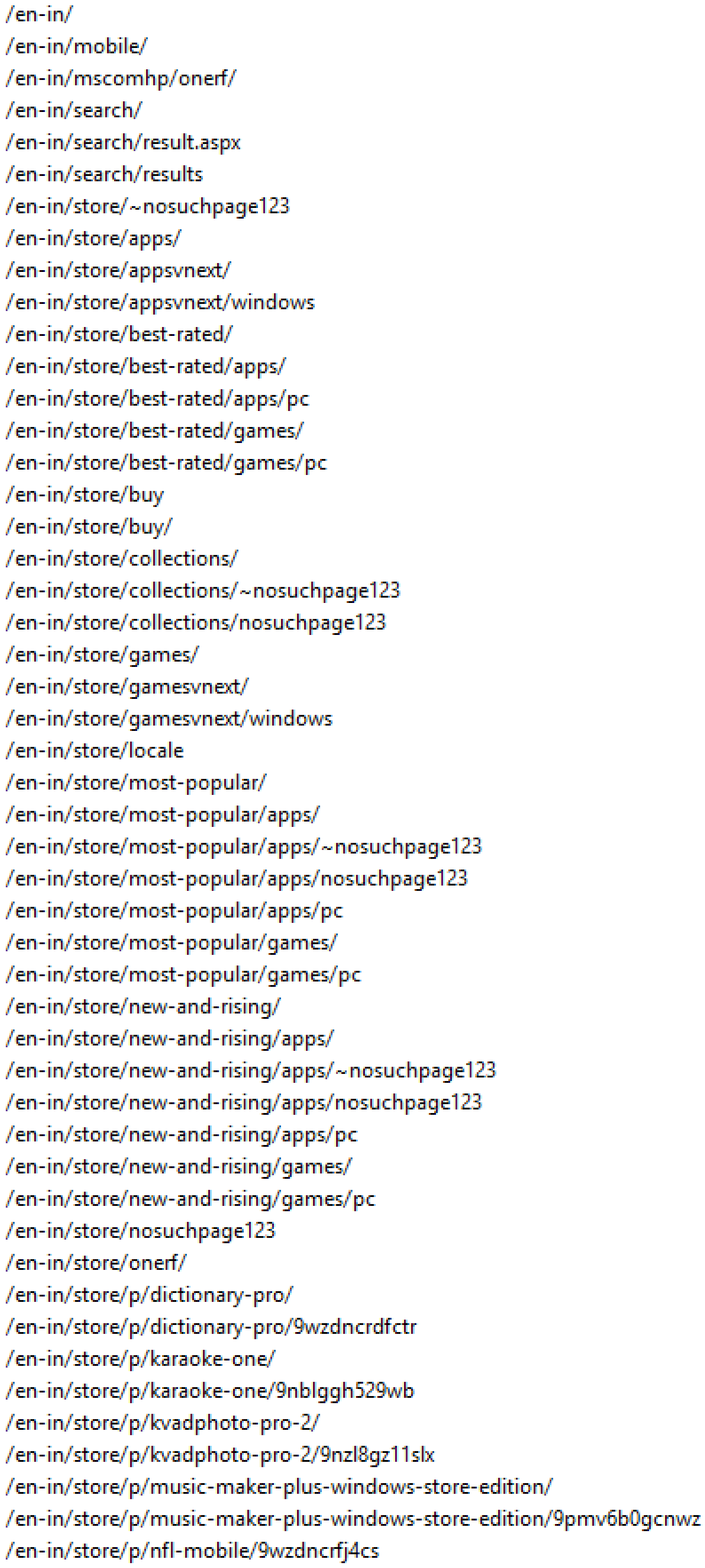
All these following resources have set an insecure **Cross-Origin Resource Sharing** (CORS) access control. CORS provides mechanisms that allow a server to restrict resource access for cross-site requests to certain trusted domains. The server in question has allowed resource from any origin by setting the value of **Access-Control-Allow-Origin** response header to a wildcard value.



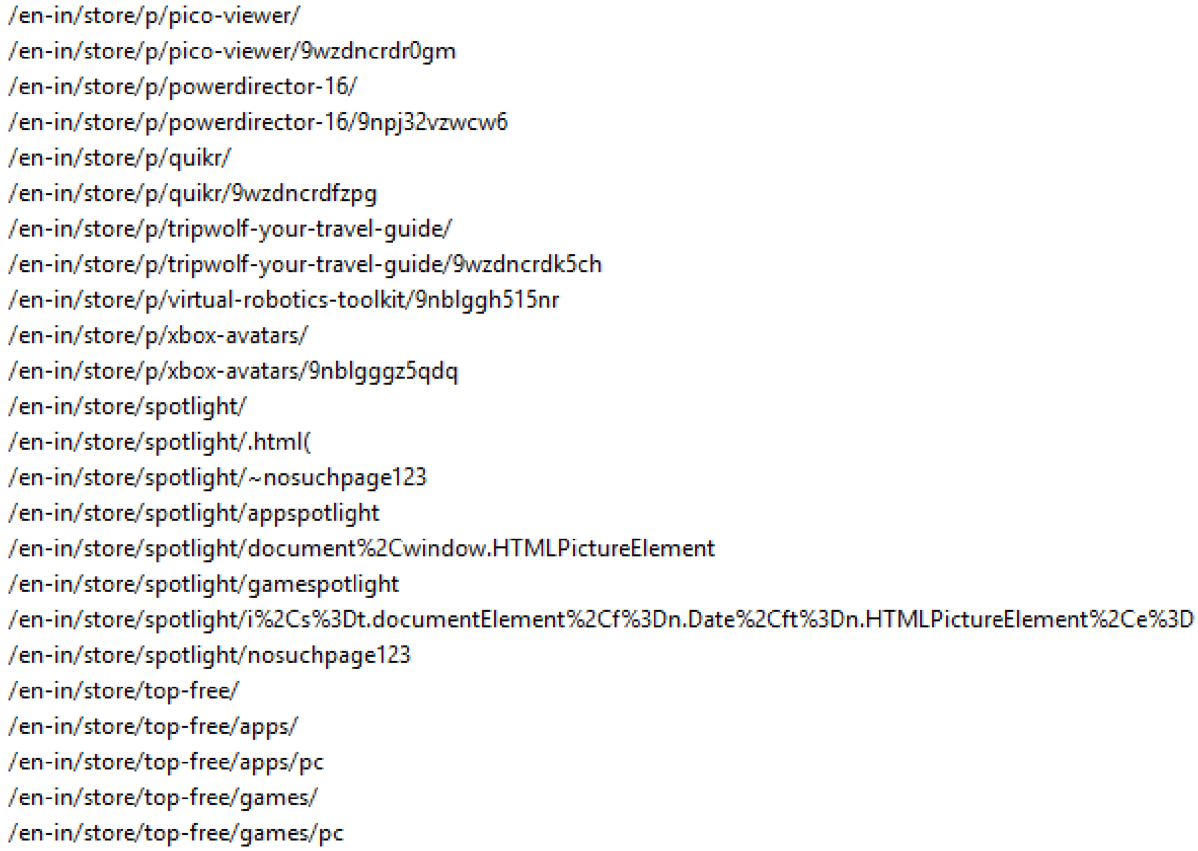
```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, no-transform
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
X-UA-Compatible: IE=Edge;chrome=1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Activity-Id: bef3b81d-9f21-47fc-98d9-a65a8d09a579
MS-CV: DgD909nEB0Gtostf.0
X-AppVersion: 1.0.6717.40875
X-Az: {did:3ed323e0c46b4bd2aa89fc62e4994282, rid: 33, sn: onestore-neu-prod, dt: 2018-05-28T14:48:22.3360320Z, bt: 2018-05-23T22:42:30.0000000Z}
P3P: CP="CAO CONi OTR OUR DEM ONL"
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: HEAD,GET,OPTIONS
X-XSS-Protection: 1
X-EdgeConnect-Origin-MEX-Latency: 2685
Date: Tue, 29 May 2018 19:46:12 GMT
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: X-FD-FEATURES=ids=xboxcontentondesktop%2copenxbl%2csfwaa_treatment&imp=29387283-0374-498a-97da-150a3bc9736b; expires=Wed, 29-May-2019 19:46:09 GMT; path=/; secure; HttpOnly
Set-Cookie: X-FD-Time=1; expires=Tue, 29-May-2018 19:51:09 GMT; path=/; secure; HttpOnly
Strict-Transport-Security: max-age=31536000
X-RTag: RT
```

So there is a security risk because any site can issue requests to access resources, regardless of origin.

RESOURCES :



```
/en-in/
/en-in/mobile/
/en-in/mscomhp/onerf/
/en-in/search/
/en-in/search/result.aspx
/en-in/search/results
/en-in/store/~nosuchpage123
/en-in/store/apps/
/en-in/store/appsvnext/
/en-in/store/appsvnext/windows
/en-in/store/best-rated/
/en-in/store/best-rated/apps/
/en-in/store/best-rated/apps/pc
/en-in/store/best-rated/games/
/en-in/store/best-rated/games/pc
/en-in/store/buy
/en-in/store/buy/
/en-in/store/collections/
/en-in/store/collections/~nosuchpage123
/en-in/store/collections/nosuchpage123
/en-in/store/games/
/en-in/store/gamesvnext/
/en-in/store/gamesvnext/windows
/en-in/store/locale
/en-in/store/most-popular/
/en-in/store/most-popular/apps/
/en-in/store/most-popular/apps/~nosuchpage123
/en-in/store/most-popular/apps/nosuchpage123
/en-in/store/most-popular/apps/pc
/en-in/store/most-popular/games/
/en-in/store/most-popular/games/pc
/en-in/store/new-and-rising/
/en-in/store/new-and-rising/apps/
/en-in/store/new-and-rising/apps/~nosuchpage123
/en-in/store/new-and-rising/apps/nosuchpage123
/en-in/store/new-and-rising/apps/pc
/en-in/store/new-and-rising/games/
/en-in/store/new-and-rising/games/pc
/en-in/store/nosuchpage123
/en-in/store/onerf/
/en-in/store/p/dictionary-pro/
/en-in/store/p/dictionary-pro/9wzdncrdfctr
/en-in/store/p/karaoke-one/
/en-in/store/p/karaoke-one/9nblggh529wb
/en-in/store/p/kvadphoto-pro-2/
/en-in/store/p/kvadphoto-pro-2/9nzl8gz11slx
/en-in/store/p/music-maker-plus-windows-store-edition/
/en-in/store/p/music-maker-plus-windows-store-edition/9pmv6b0gcnwz
/en-in/store/p/nfl-mobile/9wzdncrfj4cs
```

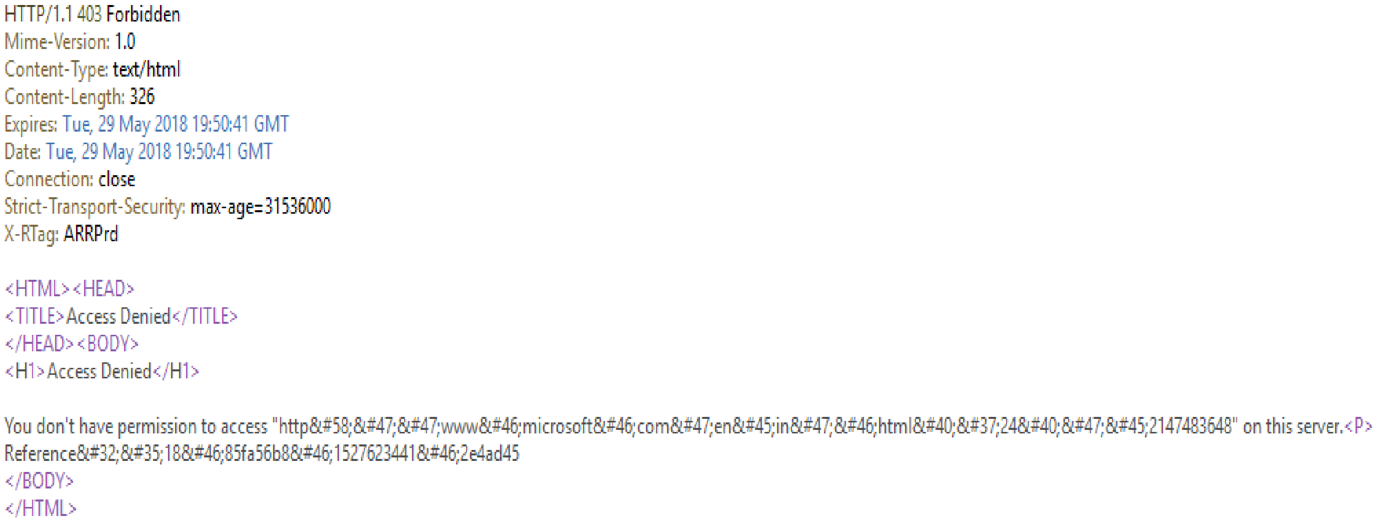


```
/en-in/store/p/pico-viewer/
/en-in/store/p/pico-viewer/9wzdncrdr0gm
/en-in/store/p/powerdirector-16/
/en-in/store/p/powerdirector-16/9npj32vzwcw6
/en-in/store/p/quikr/
/en-in/store/p/quikr/9wzdncrdfzpg
/en-in/store/p/tripwolf-your-travel-guide/
/en-in/store/p/tripwolf-your-travel-guide/9wzdncrdk5ch
/en-in/store/p/virtual-robotics-toolkit/9nblggh515nr
/en-in/store/p/xbox-avatars/
/en-in/store/p/xbox-avatars/9nblggz5qdq
/en-in/store/spotlight/
/en-in/store/spotlight/.html(
/en-in/store/spotlight/~nosuchpage123
/en-in/store/spotlight/appspotlight
/en-in/store/spotlight/document%2Cwindow.HTMLPictureElement
/en-in/store/spotlight/gamespotlight
/en-in/store/spotlight/i%2Cs%3Dt.documentElement%2Cf%3Dn.Date%2Cft%3Dn.HTMLPictureElement%2Ce%3D
/en-in/store/spotlight/nosuchpage123
/en-in/store/top-free/
/en-in/store/top-free/apps/
/en-in/store/top-free/apps/pc
/en-in/store/top-free/games/
/en-in/store/top-free/games/pc
```

Set the **Access-Control-Allow-Origin** response header to allow access from trusted domains only. Do not allow access from arbitrary domains.

2. Integer Overflow

Integers used to check the size of a data buffer, if reduced can incorrectly represent the total amount of data, resulting in a possible **buffer overflow**. The potential impact on security depends on how the integer value if used, If it is use as the size of a data buffer, forcing it to wrap to a lower value may result in bypassing of size checks, introducing possible buffer overflow conditions.

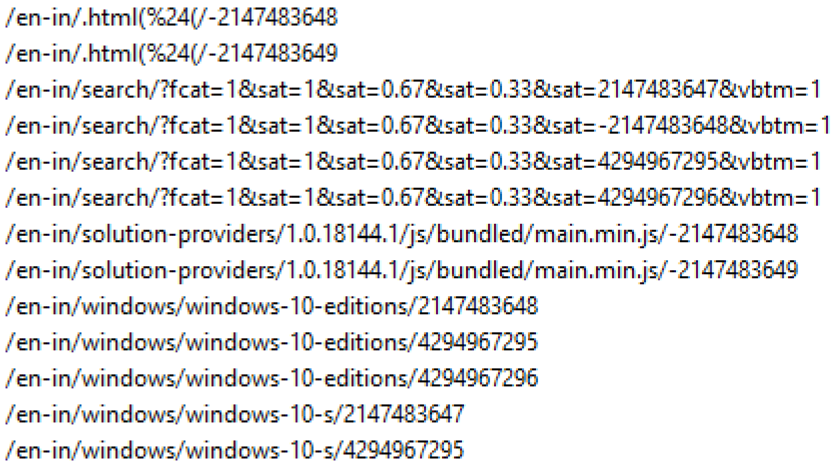


```
HTTP/1.1 403 Forbidden
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 326
Expires: Tue, 29 May 2018 19:50:41 GMT
Date: Tue, 29 May 2018 19:50:41 GMT
Connection: close
Strict-Transport-Security: max-age=31536000
X-RTag: ARRPrd

<HTML><HEAD>
<TITLE>Access Denied</TITLE>
</HEAD><BODY>
<H1>Access Denied</H1>

You don't have permission to access "http&#58;&#47;&#47;www&#46;microsoft&#46;com&#47;en&#45;in&#47;&#46;html&#40;&#37;24&#40;&#47;&#45;2147483648" on this server.<P>
Reference&#32;&#35;18&#46;85fa56b8&#46;1527623441&#46;2e4ad45
</BODY>
</HTML>
```

RESOURCES :



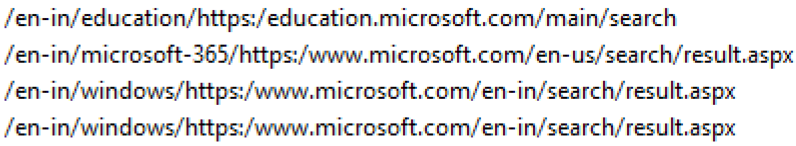
```
/en-in/.html(%24(/-2147483648
/en-in/.html(%24(/-2147483649
/en-in/search/?fcat=1&sat=1&sat=0.67&sat=0.33&sat=2147483647&vbtm=1
/en-in/search/?fcat=1&sat=1&sat=0.67&sat=0.33&sat=-2147483648&vbtm=1
/en-in/search/?fcat=1&sat=1&sat=0.67&sat=0.33&sat=4294967295&vbtm=1
/en-in/search/?fcat=1&sat=1&sat=0.67&sat=0.33&sat=4294967296&vbtm=1
/en-in/solution-providers/1.0.18144.1/js/bundled/main.min.js/-2147483648
/en-in/solution-providers/1.0.18144.1/js/bundled/main.min.js/-2147483649
/en-in/windows/windows-10-editions/2147483648
/en-in/windows/windows-10-editions/4294967295
/en-in/windows/windows-10-editions/4294967296
/en-in/windows/windows-10-s/2147483647
/en-in/windows/windows-10-s/4294967295
```

The developer should investigate the error and determine if a vulnerability is present.

3. Page Fingerprint Differential - Possible XPath / Xpath Blind Injection

There is a different response page fingerprint in relation to an Xpath injection request. This means that the response page content returned by the web application has a different signature from that returned by an ordinary request, which may indicate the existence of an **Xpath injection vulnerability,** though this isn’t confirmed. If this is due to an Xpath vulnerability, depending on the nature of the Xpath query, exploitation could allow attackers to bypass authentication or gain unauthorized access to sensitive **XML** data.

RESOURCES :



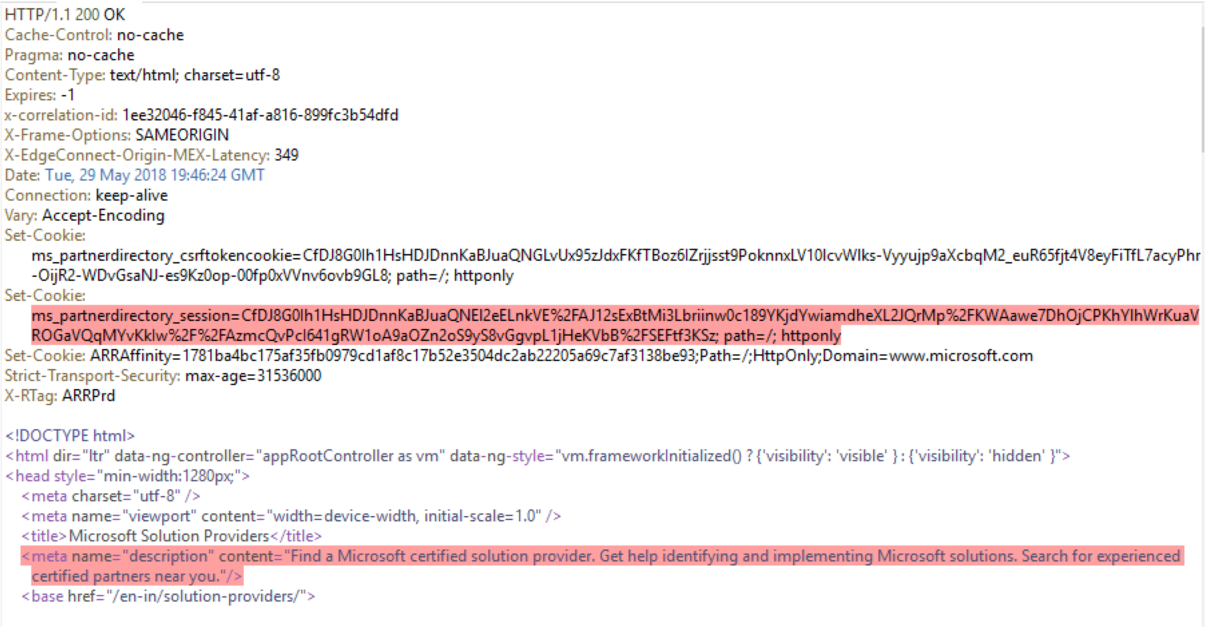
/en-in/education/https:/education.microsoft.com/main/search
/en-in/microsoft-365/https:/www.microsoft.com/en-us/search/result.aspx
/en-in/windows/https:/www.microsoft.com/en-in/search/result.aspx
/en-in/windows/https:/www.microsoft.com/en-in/search/result.aspx

This vulnerability if found, the developer should consider adopting the use of pre-compiled Xpath statements or query parameterized options.

4. Session Cookie Without Secure Flag

A known session cookie may have been set without the secure flag. Cookies can be exposed to network eavesdroppers. Session cookies are authentication credentials, attackers who obtain then can get unauthorized access to affected web applications.

I think when creating the cookie in the code, set the **secure flag** to **true**.



```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
x-correlation-id: 1ee32046-f845-41af-a816-899fc3b54dfd
X-Frame-Options: SAMEORIGIN
X-EdgeConnect-Origin-MEX-Latency: 349
Date: Tue, 29 May 2018 19:46:24 GMT
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie:
   ms_partnerdirectory_csrftokencookie=CfDJ8G0Ih1HsHDJDnnKaBJuaQNGLvUx95zJdxFKfTBoz6lZrjjsst9PoknnxLV10IcvWlks-Vyyujp9aXcbqM2_euR65fjt4V8eyFiTfL7acyPhr
   -OijR2-WDvGsaNJ-es9Kz0op-00fp0xVVnv6ovb9GL8; path=/; httponly
Set-Cookie:
   ms_partnerdirectory_session=CfDJ8G0Ih1HsHDJDnnKaBJuaQNEl2eELnkVE%2FAJ12sExBtMi3Lbriinw0c189YKjdYwiamdheXL2JQrMp%2FKWAawe7DhOjCPKhYlhWrKuaV
   ROGaVQqMYvKkIw%2F%2FAzmcQvPcl641gRW1oA9aOZn2oS9yS8vGgvpL1jHeKVbB%2FSEFtf3KSz; path=/; httponly
Set-Cookie: ARRAffinity=1781ba4bc175af35fb0979cd1af8c17b52e3504dc2ab22205a69c7af3138be93;Path=/;HttpOnly;Domain=www.microsoft.com
Strict-Transport-Security: max-age=31536000
X-RTag: ARRPrd

<!DOCTYPE html>
<html dir="ltr" data-ng-controller="appRootController as vm" data-ng-style="vm.frameworkInitialized() ? {'visibility': 'visible' } : {'visibility': 'hidden' }">
<head style="min-width:1280px;">
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>Microsoft Solution Providers</title>
  <meta name="description" content="Find a Microsoft certified solution provider. Get help identifying and implementing Microsoft solutions. Search for experienced
   certified partners near you."/>
  <base href="/en-in/solution-providers/">
```

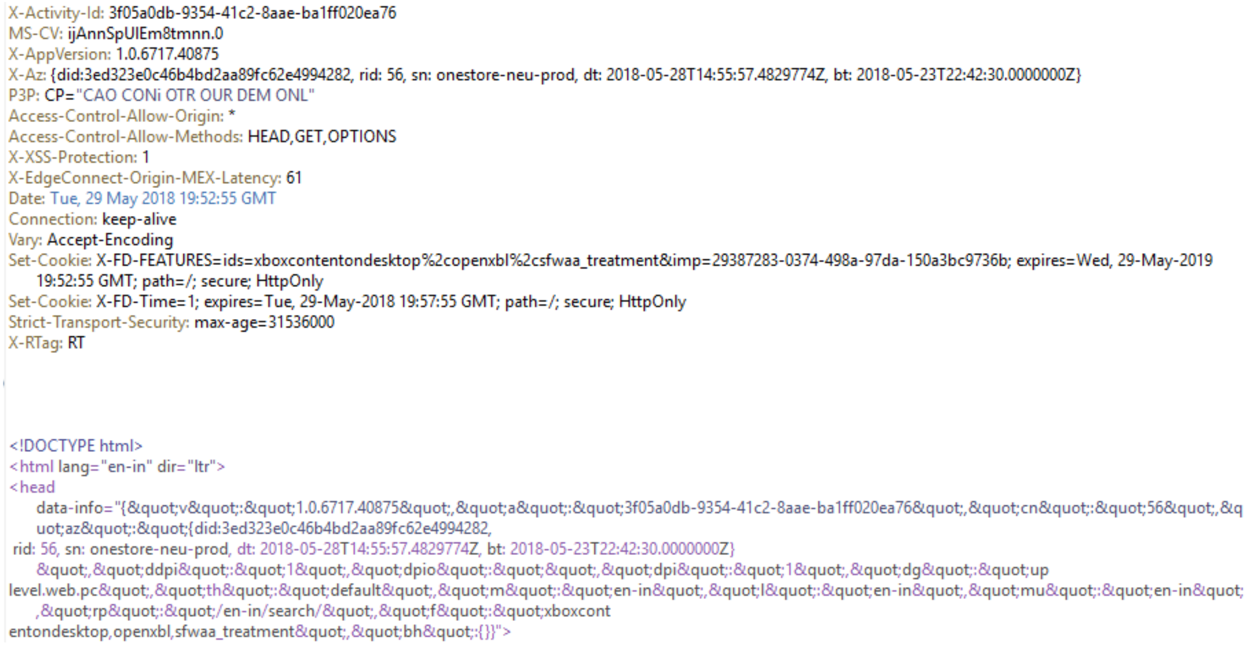
RESOURCE :

ms_partnerdirectory_session=CfDJ8G0Ih1HsHDJDnnKaBJuaQNEl2eELnkVE%2FAJ12sExBtMi3Lbriinw0c189YKjdYwiamdheXL2JQrMp%2FKWAawe7DhOjCPKhYlhWrKuaVROGaVQqMYvKkIw%2F%2FAzmcQvPcl641gRW1oA9aOZn2oS9yS8vGgvpL1jHeKVbB%2FSEFtf3KSz; path=/; httponly

5. SQL Injection - Blind Text Injection - Blind Arithmetic Evaluation

A possible SQL injection vulnerability is there. The developer should review the request and response against the code to manually verify whether or not a vulnerability is present. The best defence against SQL injection vulnerabilities is to use parameterized statements. Sanitizing input can prevent these vulnerabilities. Variables of string types should be filtered for escape characters, and numeric types should be checked to ensure that they are valid. Use of stored procedures can simplify complex queries and allow for tighter access control settings. Configuring database access controls can limit the impact of exploited vulnerabilities. This is a mitigating strategy that can be employed in environments where the code is not modifiable. Object-relational mapping eliminates the need for SQL.

Mysql_real_escape_string()



```
X-Activity-Id: 3f05a0db-9354-41c2-8aae-ba1ff020ea76
MS-CV: ijAnnSpUIEm8tmnn.0
X-AppVersion: 1.0.6717.40875
X-Az: {did:3ed323e0c46b4bd2aa89fc62e4994282, rid: 56, sn: onestore-neu-prod, dt: 2018-05-28T14:55:57.4829774Z, bt: 2018-05-23T22:42:30.0000000Z}
P3P: CP="CAO CONi OTR OUR DEM ONL"
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: HEAD,GET,OPTIONS
X-XSS-Protection: 1
X-EdgeConnect-Origin-MEX-Latency: 61
Date: Tue, 29 May 2018 19:52:55 GMT
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: X-FD-FEATURES=ids=xboxcontentondesktop%2copenxbl%2csfwaa_treatment&imp=29387283-0374-498a-97da-150a3bc9736b; expires=Wed, 29-May-2019
    19:52:55 GMT; path=/; secure; HttpOnly
Set-Cookie: X-FD-Time=1; expires=Tue, 29-May-2018 19:57:55 GMT; path=/; secure; HttpOnly
Strict-Transport-Security: max-age=31536000
X-RTag: RT



<!DOCTYPE html>
<html lang="en-in" dir="ltr">
<head
    data-info="{&quot;v&quot;:&quot;1.0.6717.40875&quot;,&quot;a&quot;:&quot;3f05a0db-9354-41c2-8aae-ba1ff020ea76&quot;,&quot;cn&quot;:&quot;56&quot;,&q
    uot;az&quot;:&quot;{did:3ed323e0c46b4bd2aa89fc62e4994282,
 rid: 56, sn: onestore-neu-prod, dt: 2018-05-28T14:55:57.4829774Z, bt: 2018-05-23T22:42:30.0000000Z}
    &quot;,&quot;ddpi&quot;:&quot;1&quot;,&quot;dpio&quot;:&quot;&quot;,&quot;dpi&quot;:&quot;1&quot;,&quot;dg&quot;:&quot;up
level.web.pc&quot;,&quot;th&quot;:&quot;default&quot;,&quot;m&quot;:&quot;en-in&quot;,&quot;l&quot;:&quot;en-in&quot;,&quot;mu&quot;:&quot;en-in&quot;
    ,&quot;rp&quot;:&quot;/en-in/search/&quot;,&quot;f&quot;:&quot;xboxcont
entondesktop,openxbl,sfwaa_treatment&quot;,&quot;bh&quot;:{}}">
```

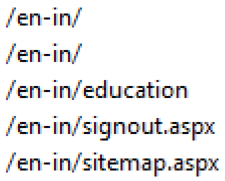
RESOURCES :

https://www.microsoft.com/en-in/microsoft-365/https:/www.microsoft.com/en-us/search/result.aspx
https://www.microsoft.com/en-in/search
https://www.microsoft.com/en-in/search/results
https://www.microsoft.com/en-in/store/most-popular/apps/pc
https://www.microsoft.com/en-in/store/most-popular/apps/pc
https://www.microsoft.com/en-in/windows/https:/www.microsoft.com/en-in/search/result.aspx

6. Cookie HttpOnly Flag Not Set

It is possible to access the cookie via client-side script code. The HttpOnly flag is a security measure that can help mitigate the risk of cross-site scripting attacks that target session cookies of the victim. I the HttpOnly flag is set and the browser supports this feature, attacker-supplied code will not be able to access the cookie.

RESOURCES :

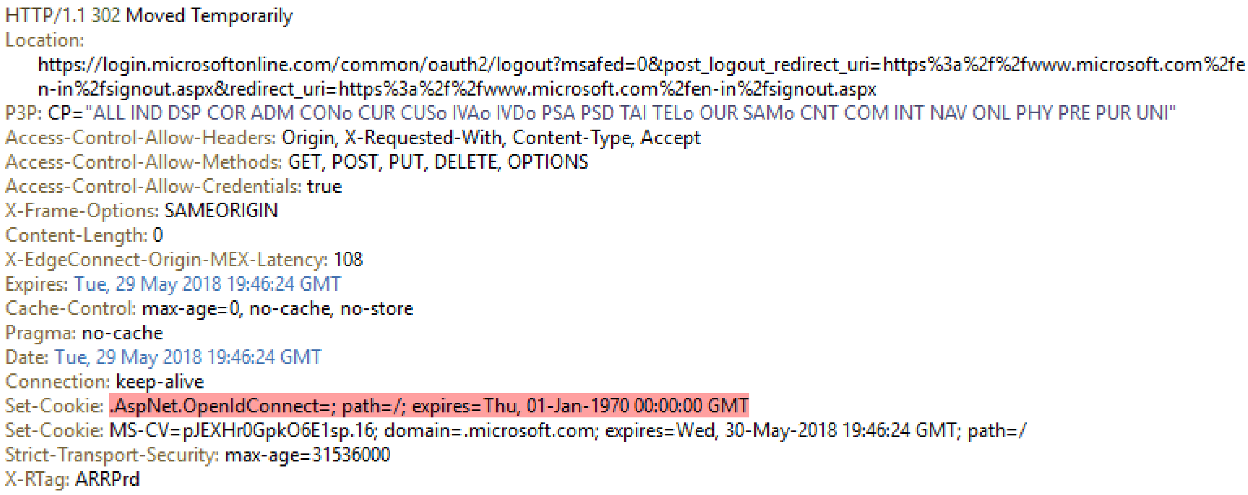


```
/en-in/
/en-in/
/en-in/education
/en-in/signout.aspx
/en-in/sitemap.aspx
```

7. Cookie Secure Flag Not Set

Cookie that was set without the secure flag was found. Therefore the cookie may be transmitted over unencrypted HTTP. This may allow the cookie to be observed in transit.

While creating cookies, the Secure flag is set should be ensured.



```
HTTP/1.1 302 Moved Temporarily
Location:
    https://login.microsoftonline.com/common/oauth2/logout?msafed=0&post_logout_redirect_uri=https%3a%2f%2fwww.microsoft.com%2fe
    n-in%2fsignout.aspx&redirect_uri=https%3a%2f%2fwww.microsoft.com%2fen-in%2fsignout.aspx
P3P: CP="ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR SAMo CNT COM INT NAV ONL PHY PRE PUR UNI"
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Credentials: true
X-Frame-Options: SAMEORIGIN
Content-Length: 0
X-EdgeConnect-Origin-MEX-Latency: 108
Expires: Tue, 29 May 2018 19:46:24 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Tue, 29 May 2018 19:46:24 GMT
Connection: keep-alive
Set-Cookie: .AspNet.OpenIdConnect=; path=/; expires=Thu, 01-Jan-1970 00:00:00 GMT
Set-Cookie: MS-CV=pJEXHr0GpkO6E1sp.16; domain=.microsoft.com; expires=Wed, 30-May-2018 19:46:24 GMT; path=/
Strict-Transport-Security: max-age=31536000
X-RTag: ARRPrd
```

RESOURCES :

```
/en-in/
/en-in/education
/en-in/evalcenter/
/en-in/evalcenter/
/en-in/signout.aspx
/en-in/sitemap.aspx
/en-in/solution-providers
/en-in/solution-providers
```