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

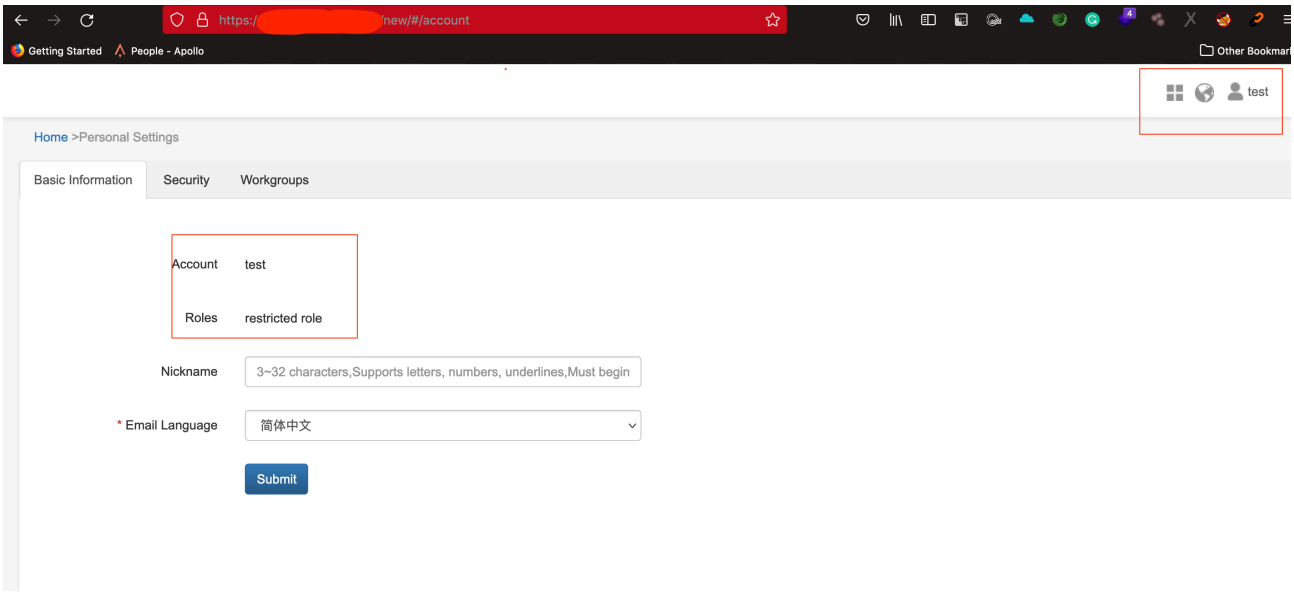
Vulnerability Description: The application iCare(Novaicare) developed by Xi'an NovaStar Tech Co.,Ltd on their VNNOX cloud platform v7.16.0 which is used to centrally monitor display status of LED screens suffers from multiple Privilege Escalation Bugs.The bug lies in the poor access control management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

Severity: HIGH

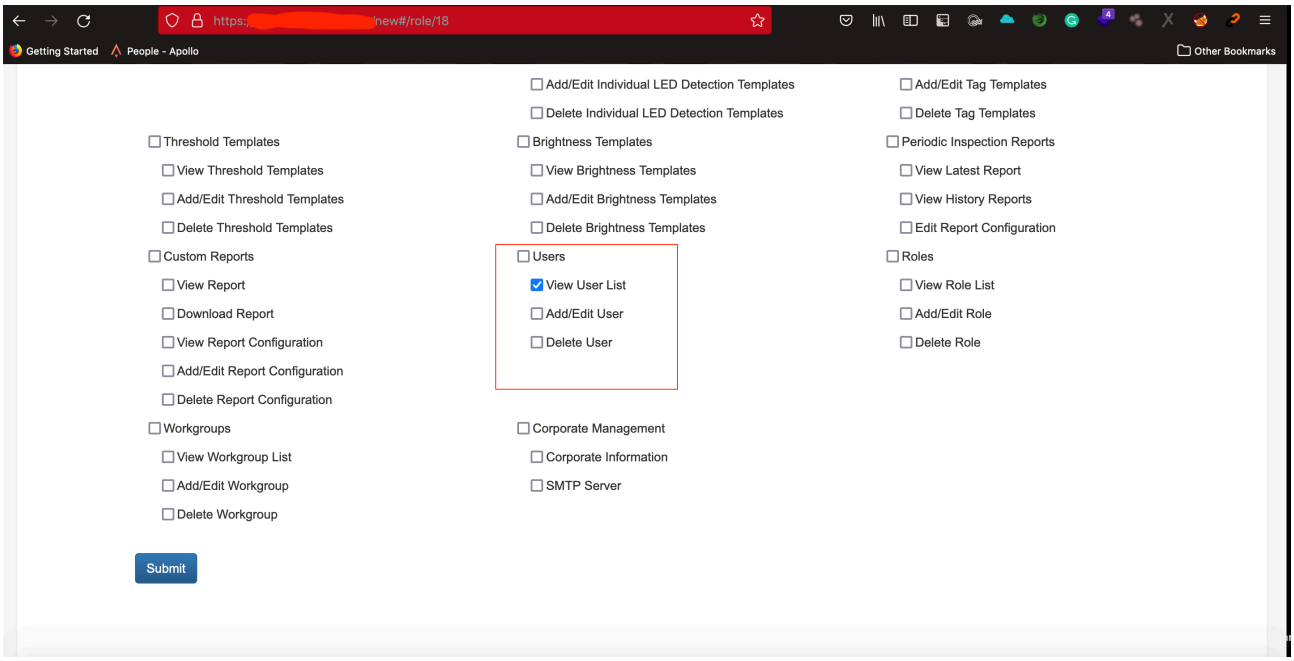
Observation: When a new user is created on the Novaicare platform and added to a restricted role(a role with only User view privileges) , that user can escalate the privileges and perform multiple privileged actions including : 1. View Corporate Information and SMTP Server Details 2. Ability to delete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

1. View Enterprise and SMTP Info

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



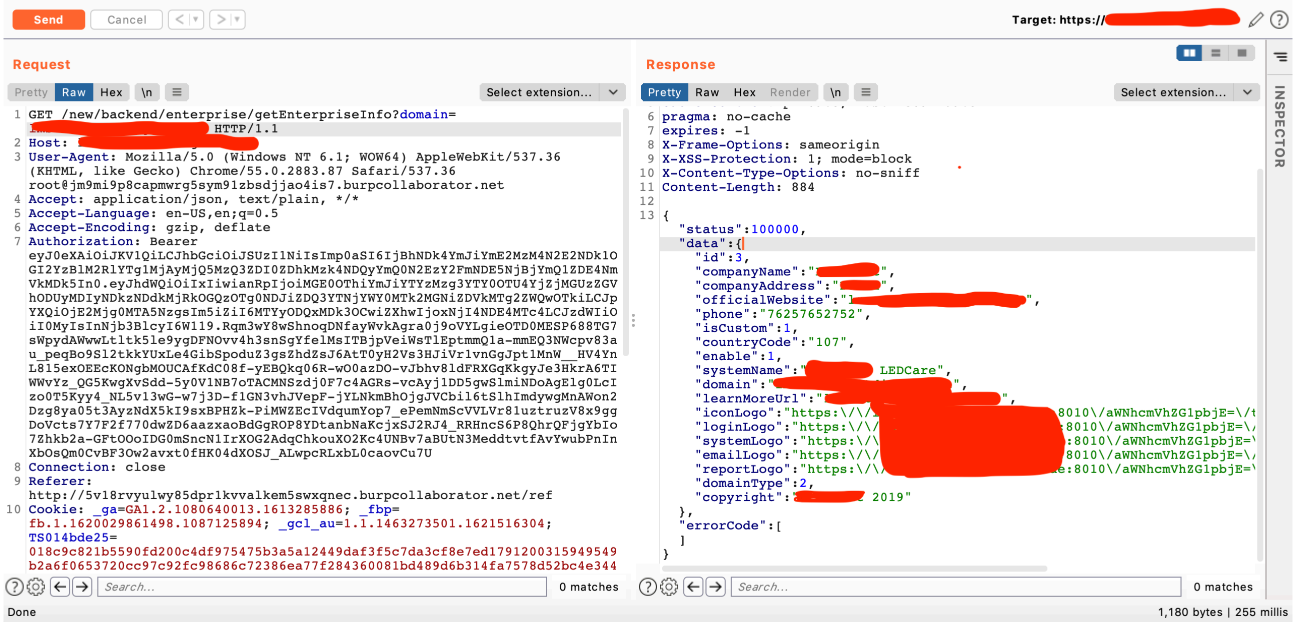
Restricted Role Privileges have been shown below:



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:

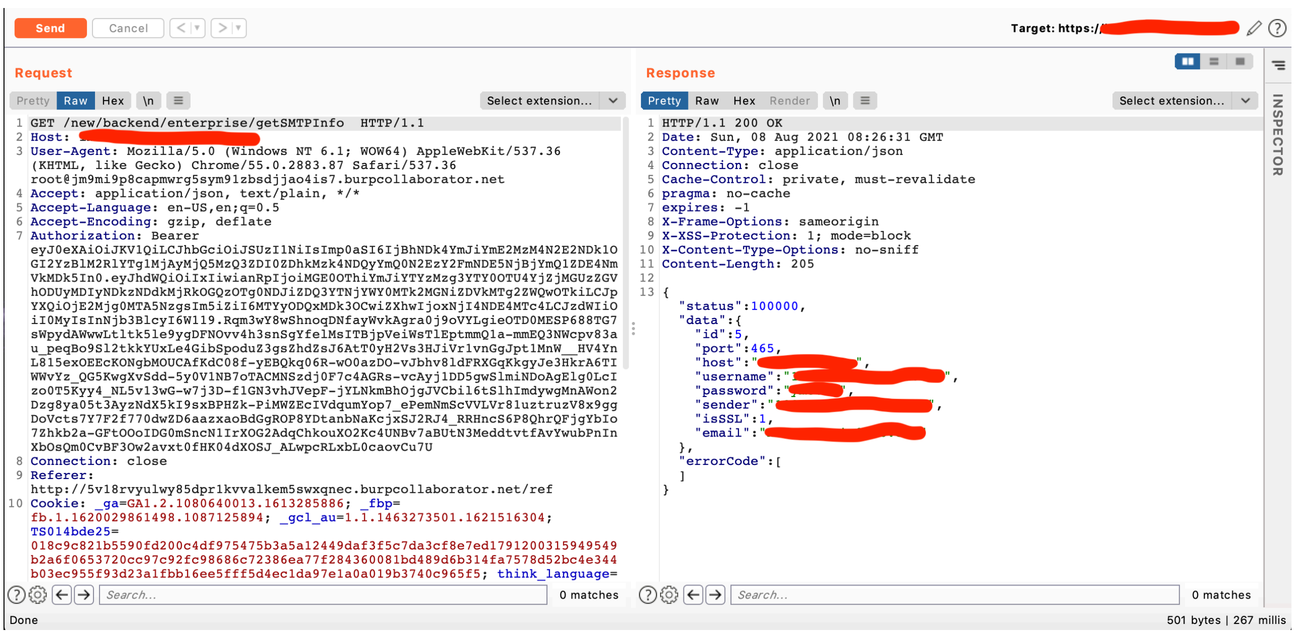
::Corporate Information::

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)



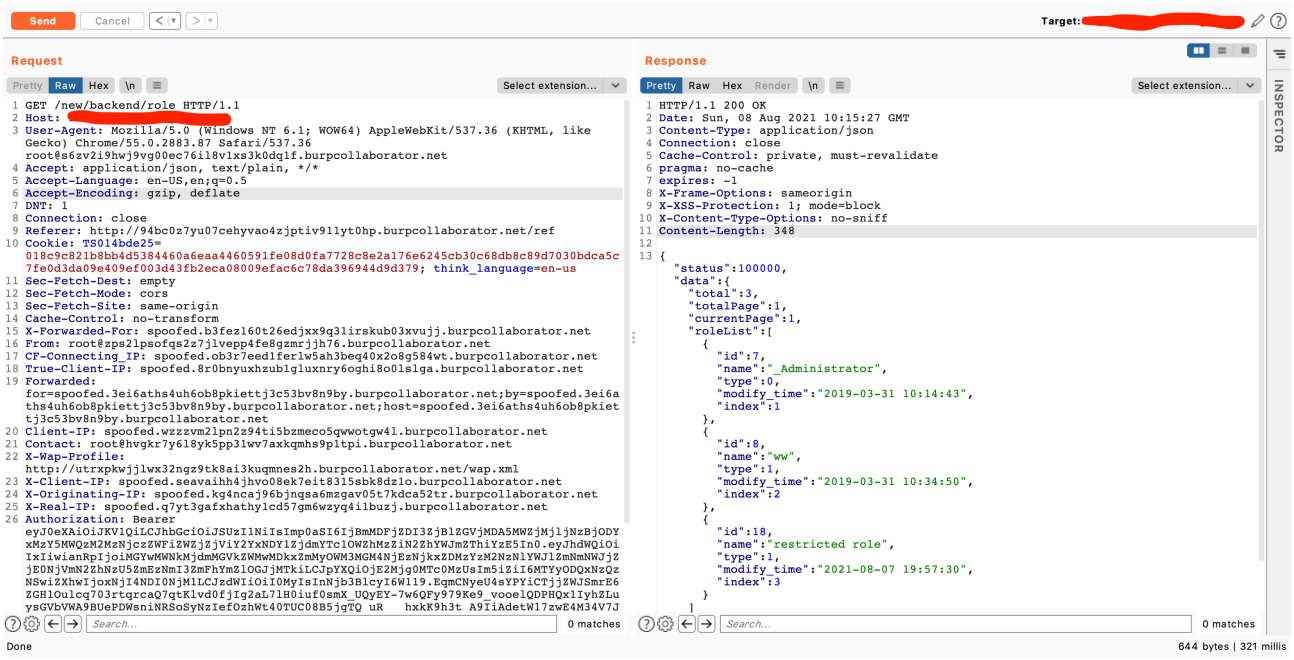
::SMTP Server Details::

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



::View Roles::

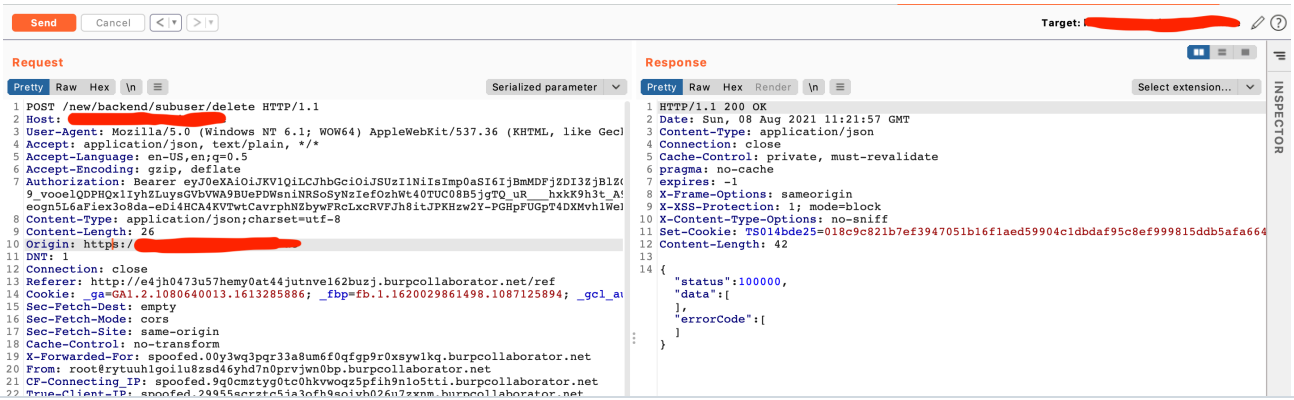
Visit Endpoint given in POC with a restricted role(a role with only User view privileges) User account : (GET /new/backend/role)



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)



Releases

No releases published

Packages

No packages published

Contributors 1

viperbluff Sahil Tikoo