



Namaste, I'm Saraunsh Shewale from India <3. I love to hack !. Going to blog about my research in infosec, writups of CTF challenges & HTB machines and occasional life lessons !!

CVE-2021-28293

cve-2021-28293
 account-takeover
 vulnerability
 seceon
 siem-tool

Published on 07 Jun 2021

➤ My First CVE ID | Proof of Concept (PoC) !_

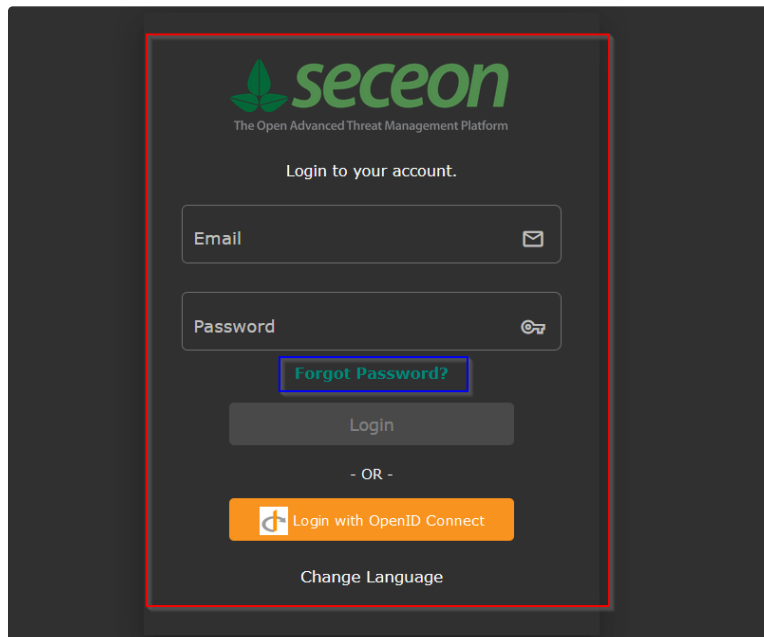
I always wonder how it feels to have a CVE ID assigned to our name & the day finally came to experience the true happiness towards my first CVE ID assignment. Let's get started with the actual PoC !!

Product Information

Vendor: Seceon Inc.
 Product Name: Seceon aiSIEM
 Version: 6.3.2
 Build: 585
 Vulnerability Type: Unauthenticated Account Takeover
 Severity: CRITICAL

PoC | Proof of Concept

#1. Go to login page of Seceon aiSIEM and click on "Forgot Password" button. URL - <https://192.168.x.x/nextgen/v1/#/login/forgot-password>.

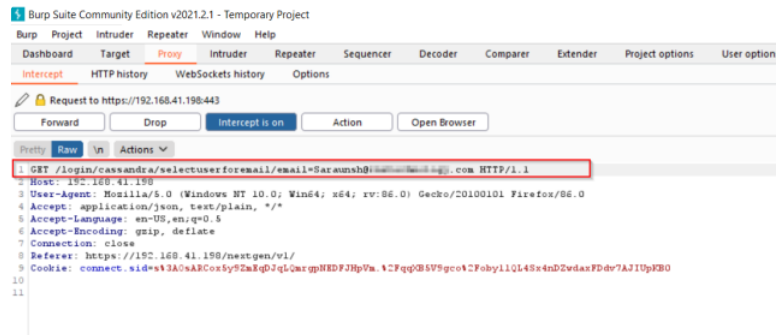


#2. Configure any browser with burp suite localhost IP & port to intercept requests/responses.

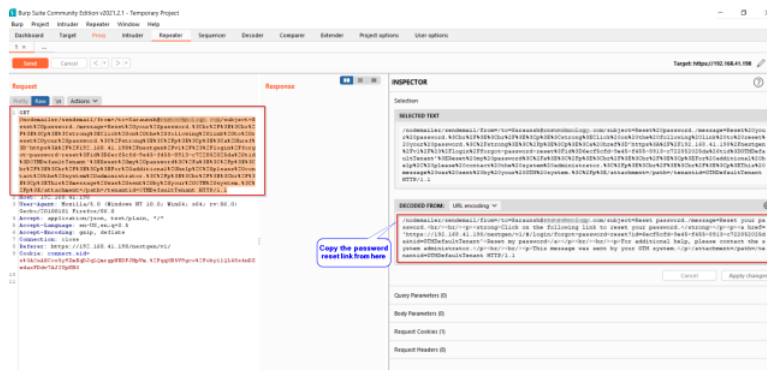
#3. Open burp suite proxy interceptor, go to "Proxy" tab and ensure Intercept is on.

#4. Now, enter the email address of the victim and click on "Send Reset Link" button.

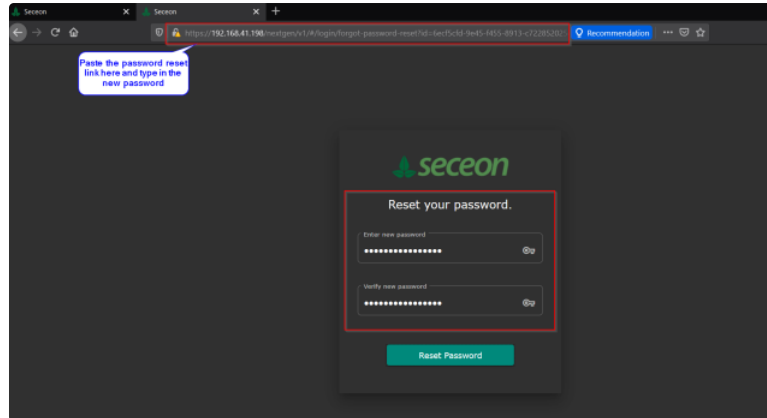
#5. You will observe the following request in burp suite, click on forward to proceed with the request.



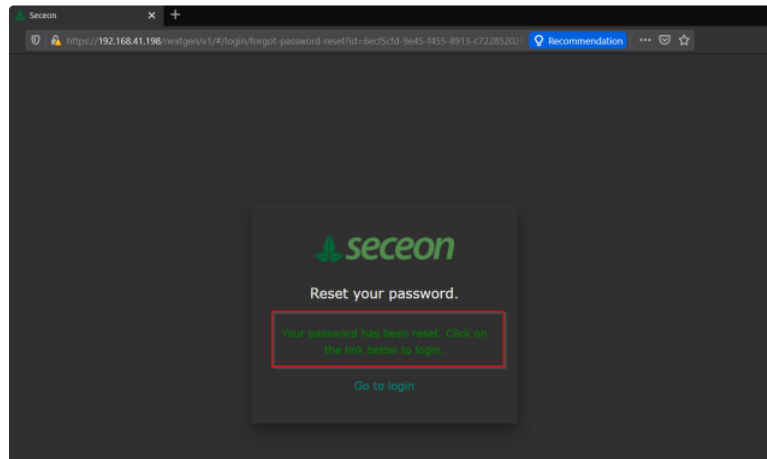
#6. Observe the next request very carefully, here the GET request call is being made to "sendemail" API endpoint along with the password reset (token) link !!



#7. Paste the copied link into the browser and enter the new password for the victim's SIEM account.



#8. Password is successfully changed and now an attacker can login with a victim's email address & new password that has been just changed.



Impact

Any malicious user/attacker can change the credentials of any user/victim with only email address of victim's account and that results in complete account takeover of the user. Only prerequisite to successful account takeover is email address of the victim.

Cheers !

The vulnerability got fixed in newer build versions & can not be exploitable further.

MITRE CVE: [Check Here](#)

Happy Learning <3








Gracias ❤️ !!

related posts

🔧 How Mere Words Transformed Me ? | Ft. My College Journey !

🔧 TCS HackQuest Season 5 | Round - 2 & 3

all tags

-  account-takeover
-  contest-based-hiring
-  ctf
-  cve-2021-28293
-  engineering-life
-  ethicalhacking
-  goodold-days
-  grandfinalist
-  hackquest5
-  happy-transformation
-  journey
-  life-changing-movements
-  saitama
-  seceon
-  siem-tool
-  tcs
-  tcshackquest
-  top10
-  vulnerability

