storebrand

What We've Learned from Exposing Atlassian on the Internet: In-Depth Analysis from an Offensive Perspective

Oleksandr Kazymyrov

BSides Munich 2023

storebrand

Oleksandr Kazymyrov

Information Security Expert

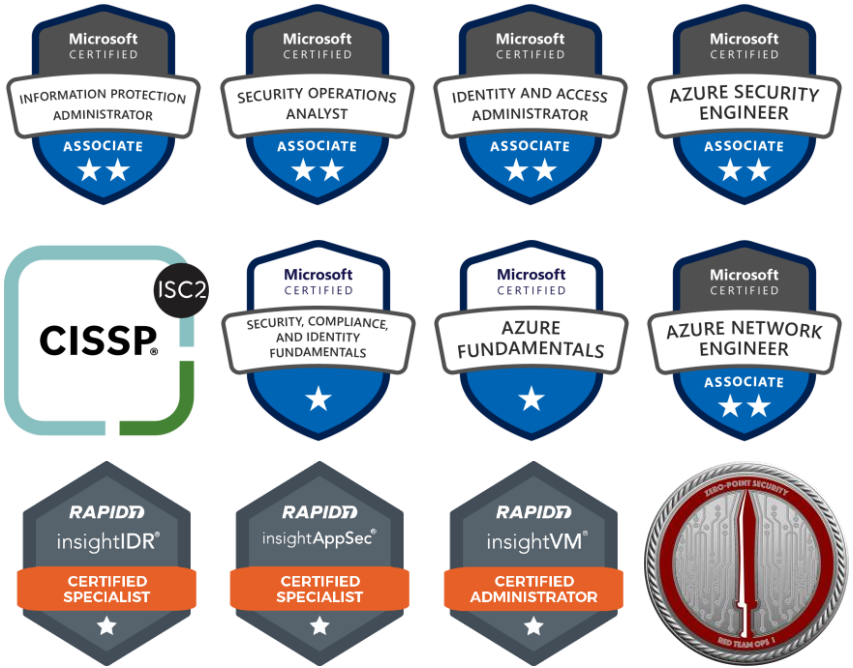
Bergen, Vestland, Norge

512 følgere · Over 500 forbindelser

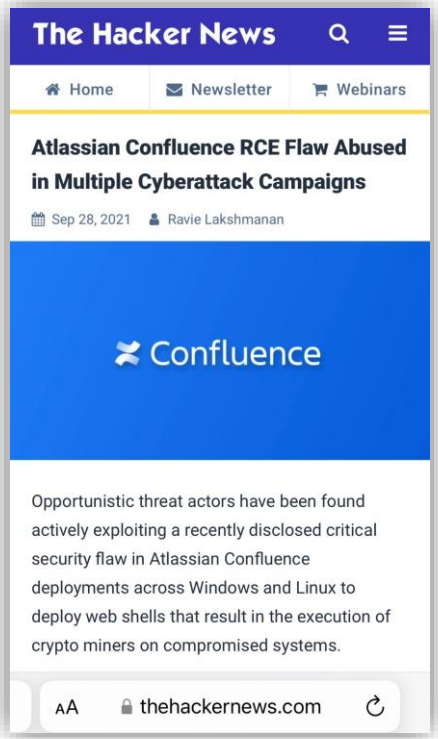
Se felles forbindelser

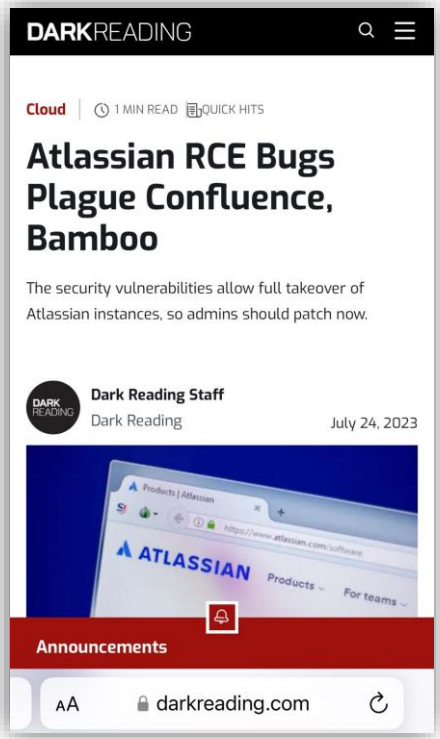
Bli med for å se profilen

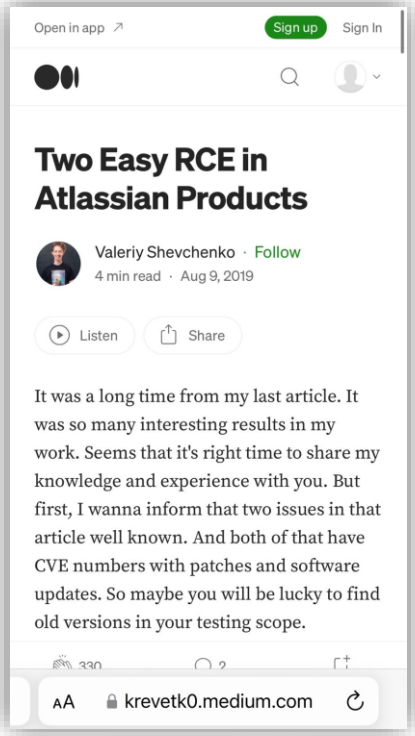
Who am I?

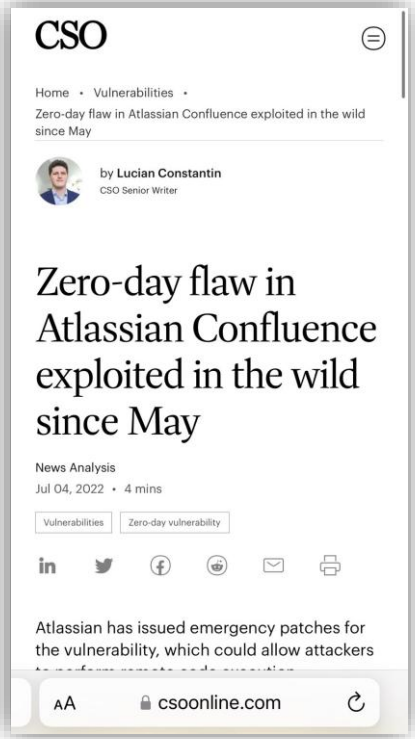


Atlassian in security news









Atlassian in security news

BLEEPINGCOMPUTER

Search Site

NEWS DOWNLOADS VPNS VIRUS REMOVAL GUIDES TUTORIALS DEA

Home > News > Security > Atlassian patches critical Confluence zero-day exploited in attacks

Atlassian patches critical Confluence zero-day exploited in attacks

By Sergiu Gatlan — October 4, 2023 — 01:41 PM — 0

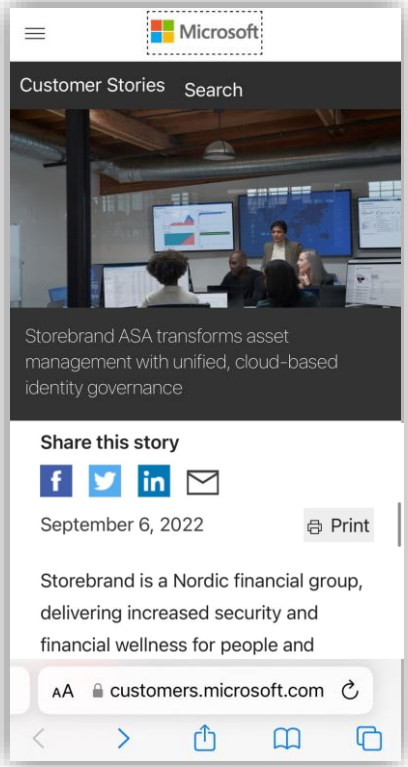
Australian software company Atlassian released emergency security updates to fix a maximum severity zero-day vulnerability in its Confluence Data Center and Server software, which has been exploited in attacks.

Versions prior to 8.0.0 are not affected by this vulnerability.

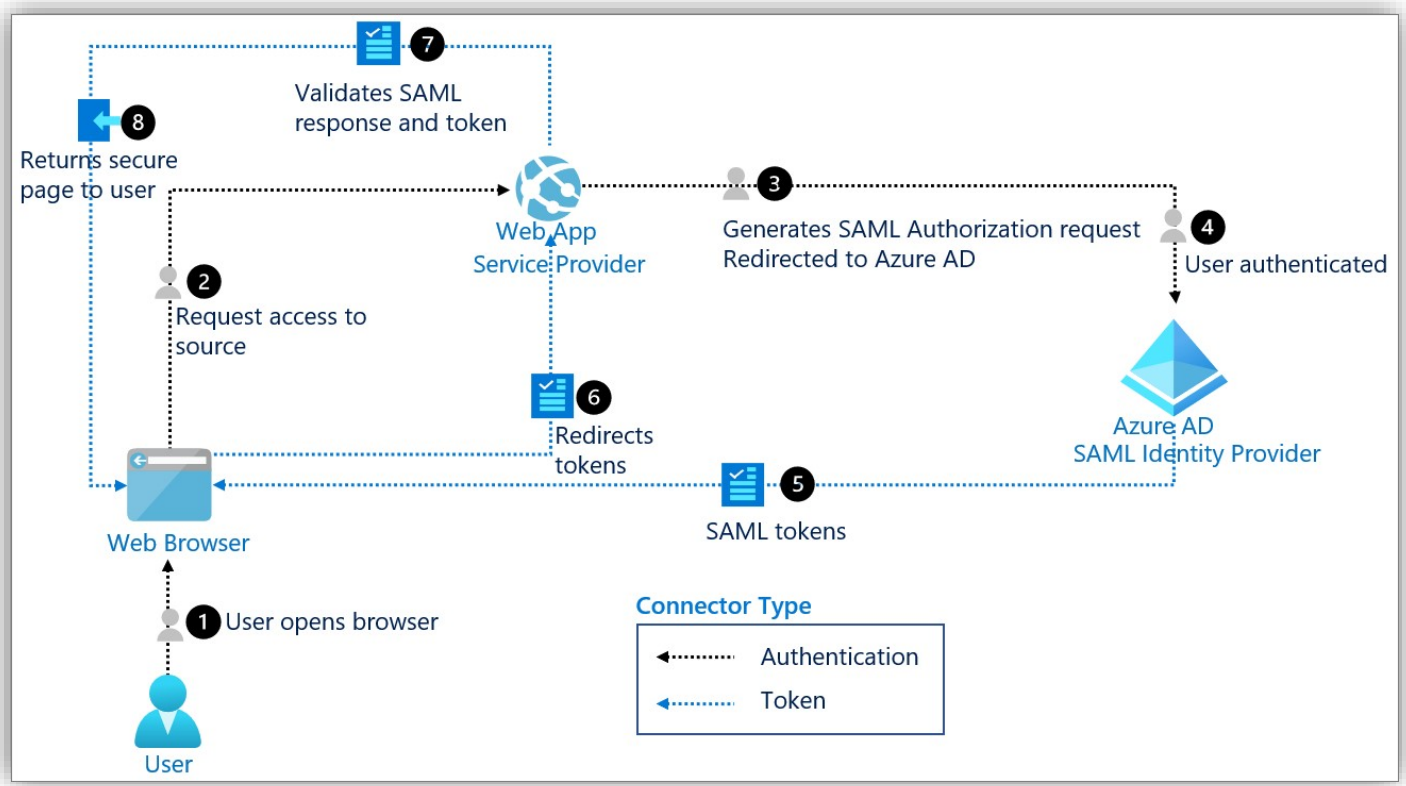
Product	Affected Versions
Confluence Data Center and Confluence Server	• 8.0.0 • 8.0.1 • 8.0.2 • 8.0.3 • 8.0.4 • 8.1.0 • 8.1.1 • 8.1.3 • 8.1.4 • 8.2.0 • 8.2.1 • 8.2.2 • 8.2.3 • 8.3.0 • 8.3.1 • 8.3.2 • 8.4.0 • 8.4.1 • 8.4.2 • 8.5.0 • 8.5.1

Instances on the public internet are particularly at risk, as this vulnerability is exploitable anonymously.

Storebrand in the cloud

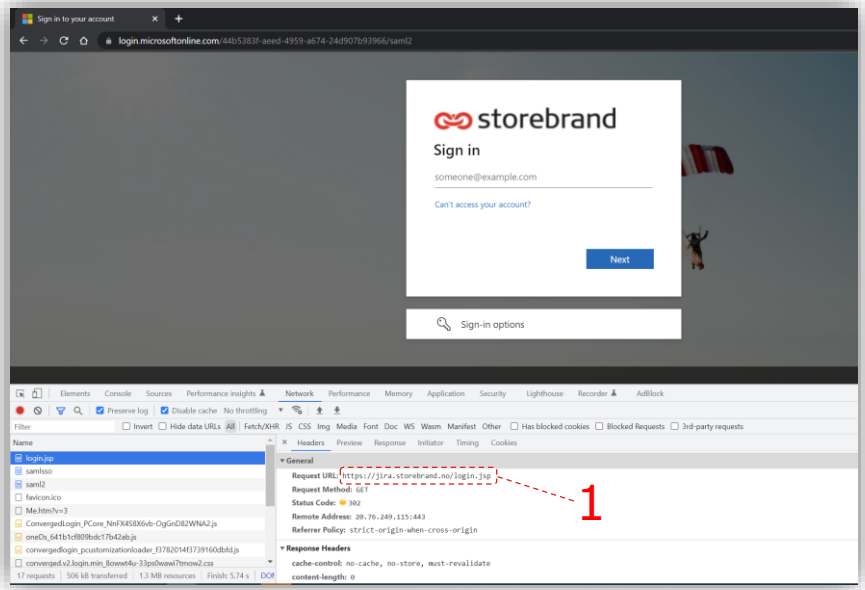


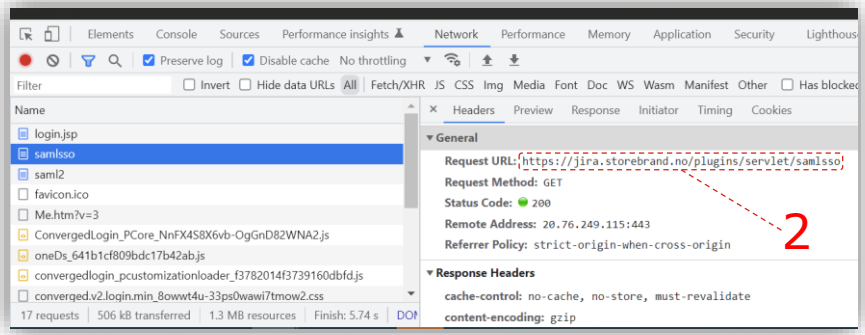
SAML authentication with Microsoft Entra ID

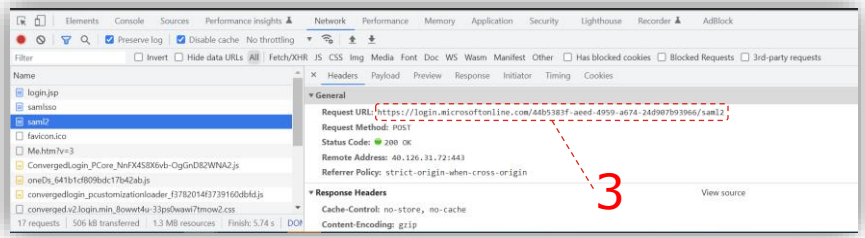


Source: SAML authentication with Microsoft Entra ID

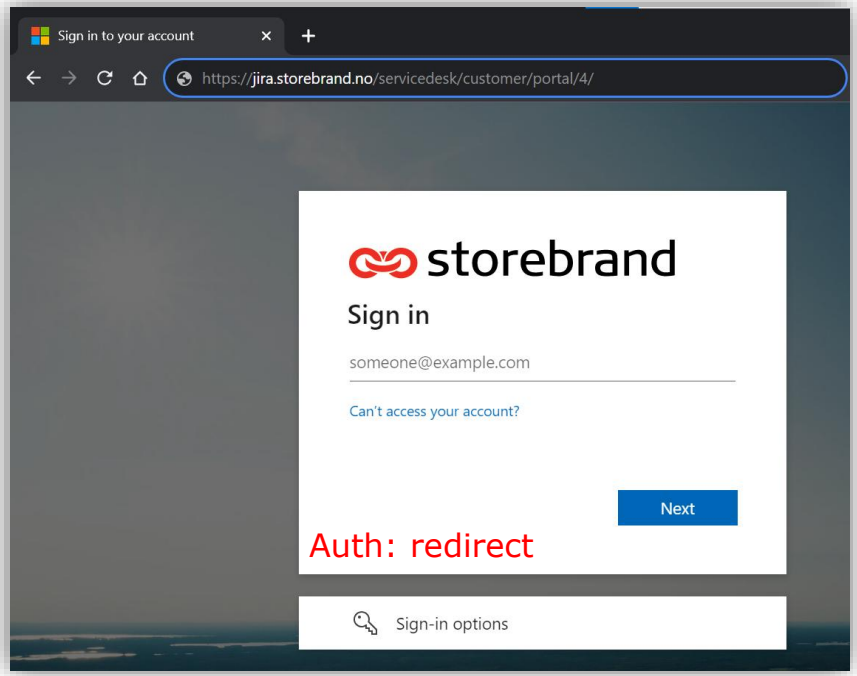
Azure AD: first steps in the authentication flow

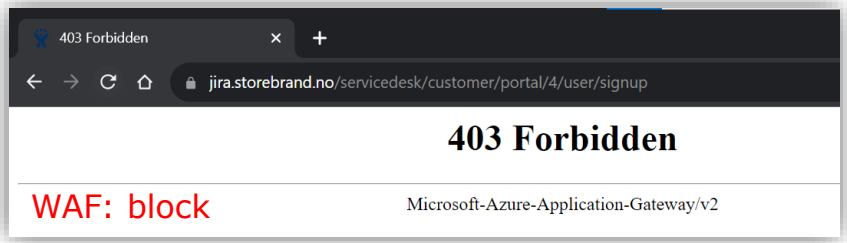


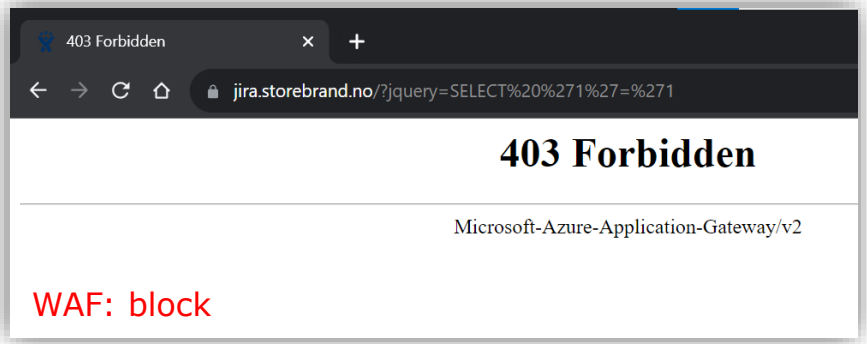




SSO and WAF: expected behavior



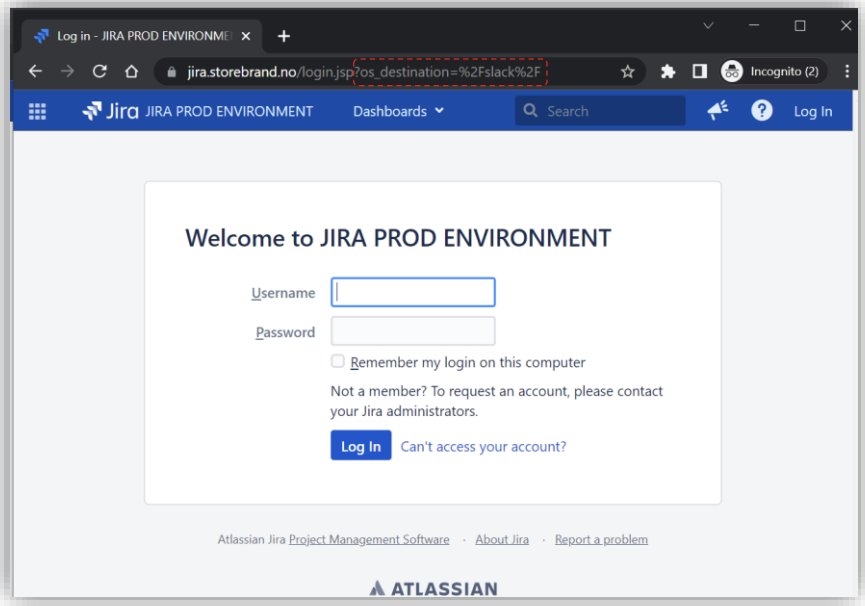


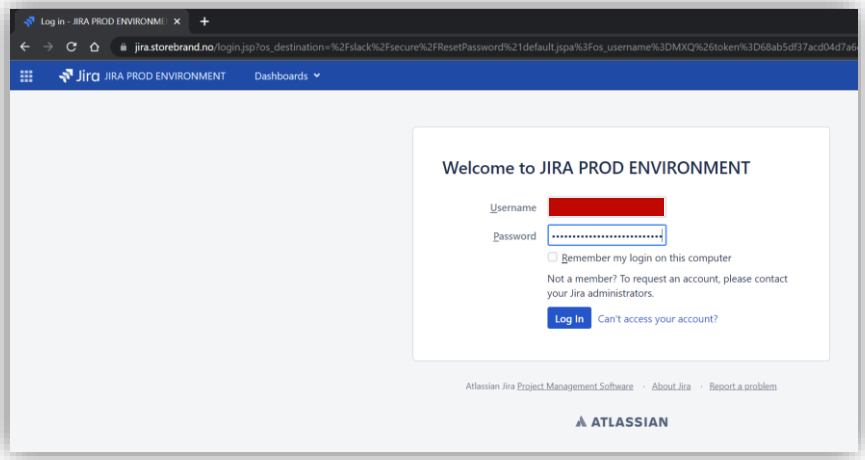


Bypass SSO

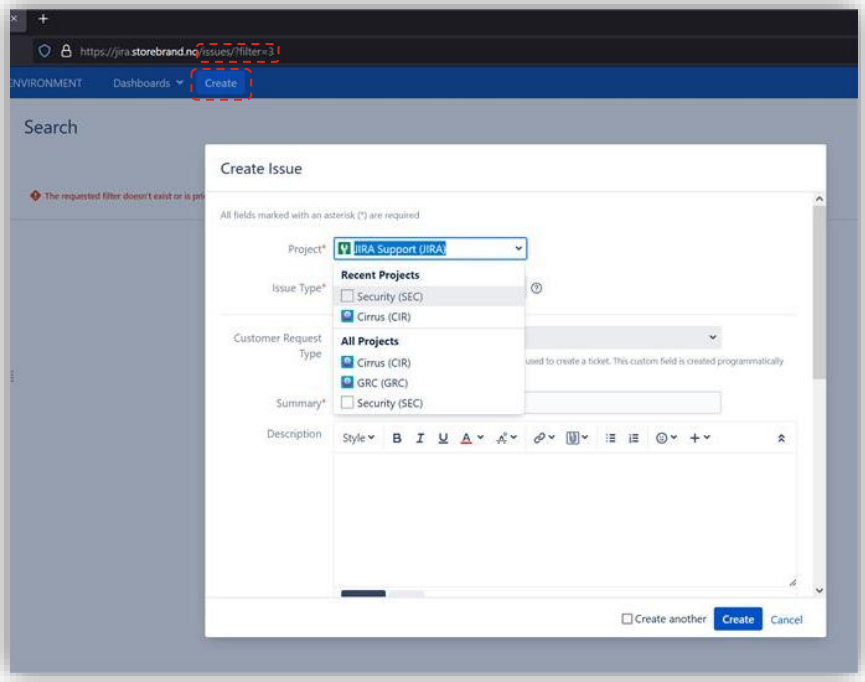
This is URL to bypass SSO: https://jira-t.storebrand.no/login.jsp?os_destination=%2Fslack%2F

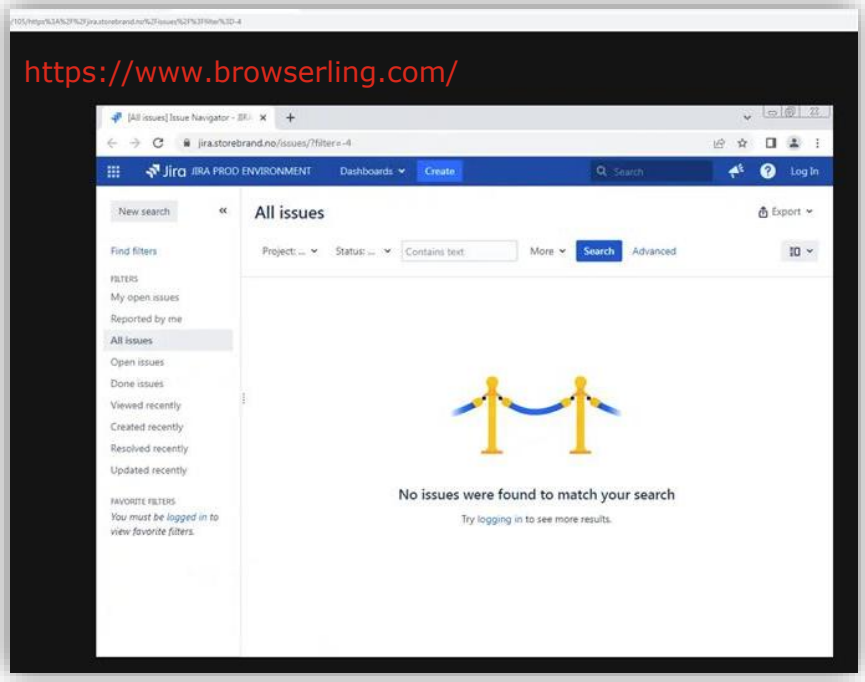
The most important part is **?os_destination=%2Fslack%2F**, which triggers Non SSO URLs



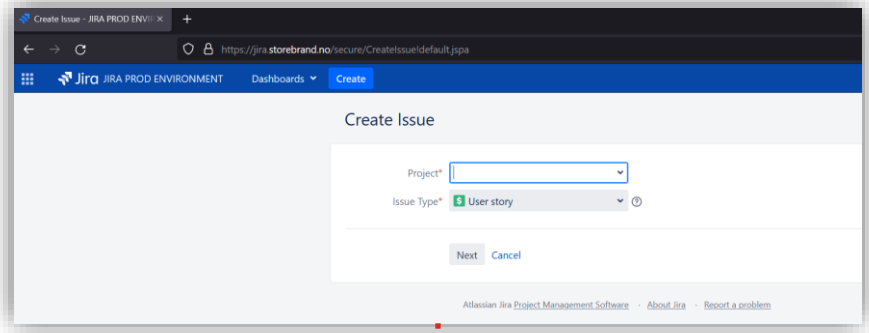


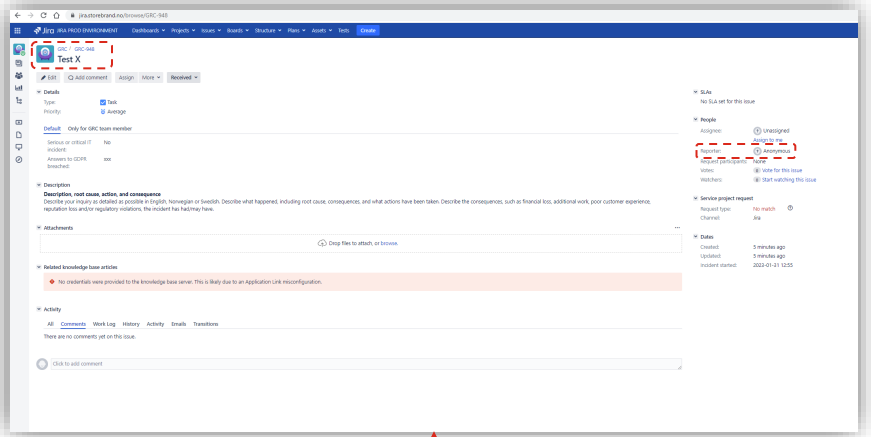
Anonymous access: information gathering over the Internet

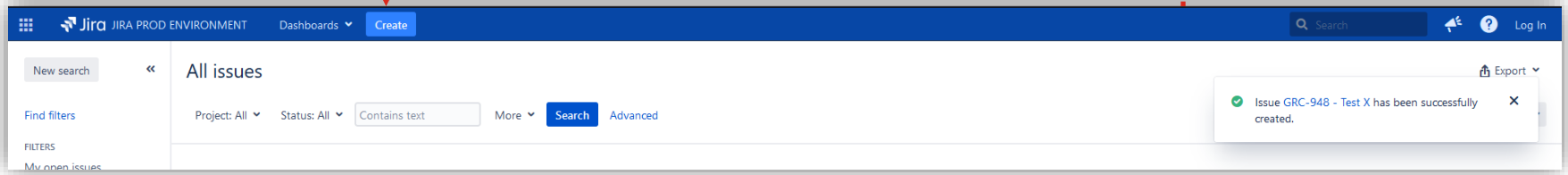




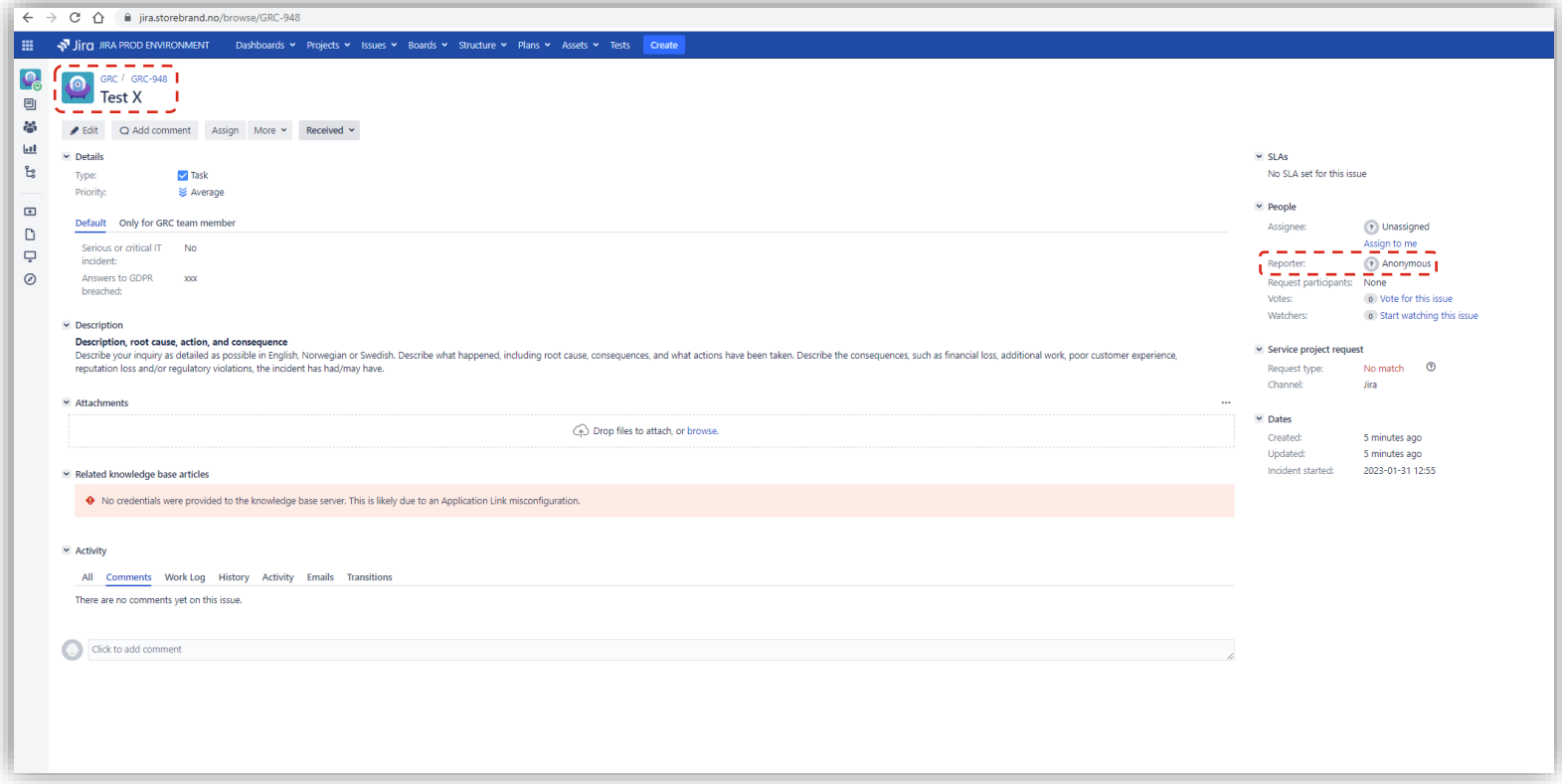
Anonymous access: create an issue



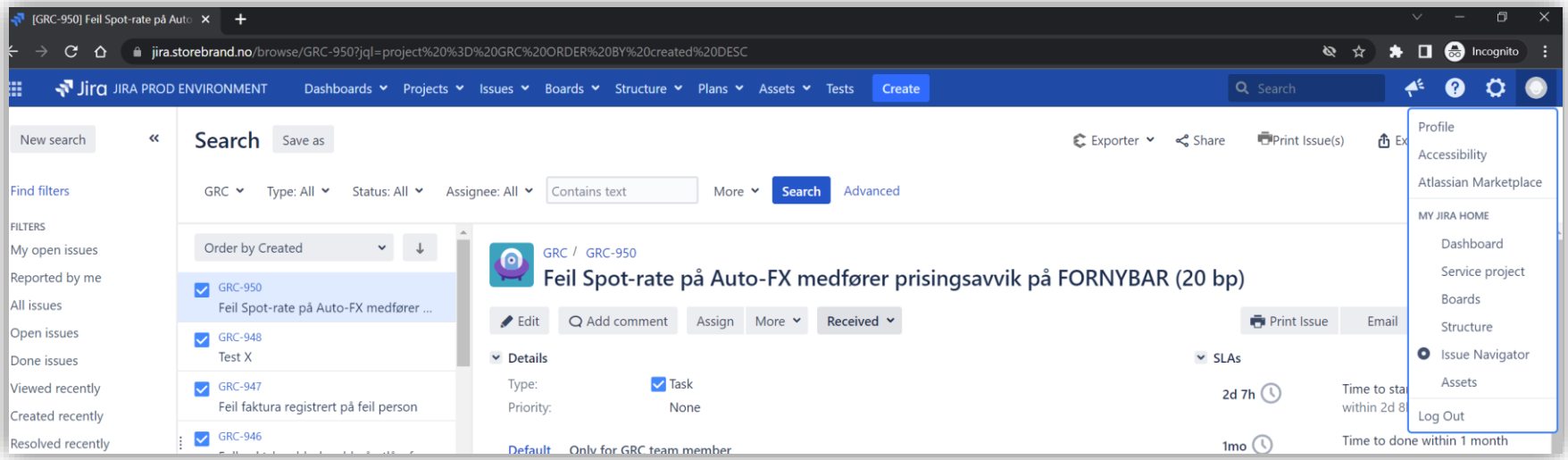




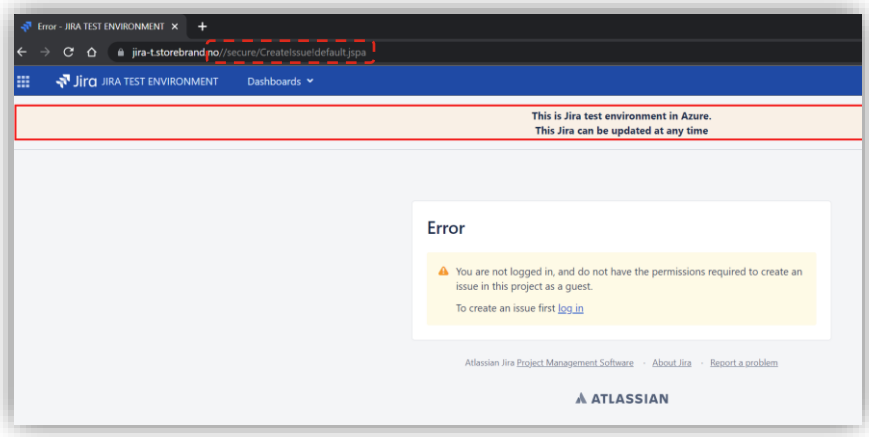
Anonymous access: create an issue

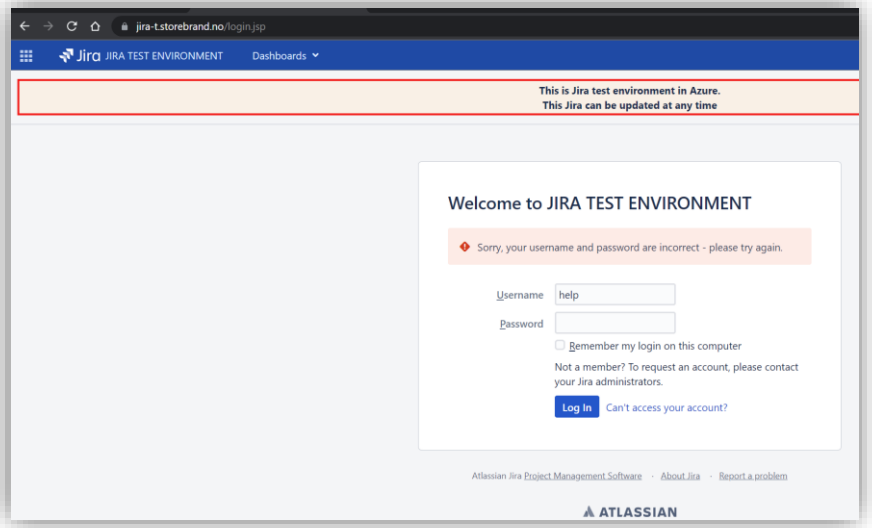


Anonymous access: search for low-hanging fruits

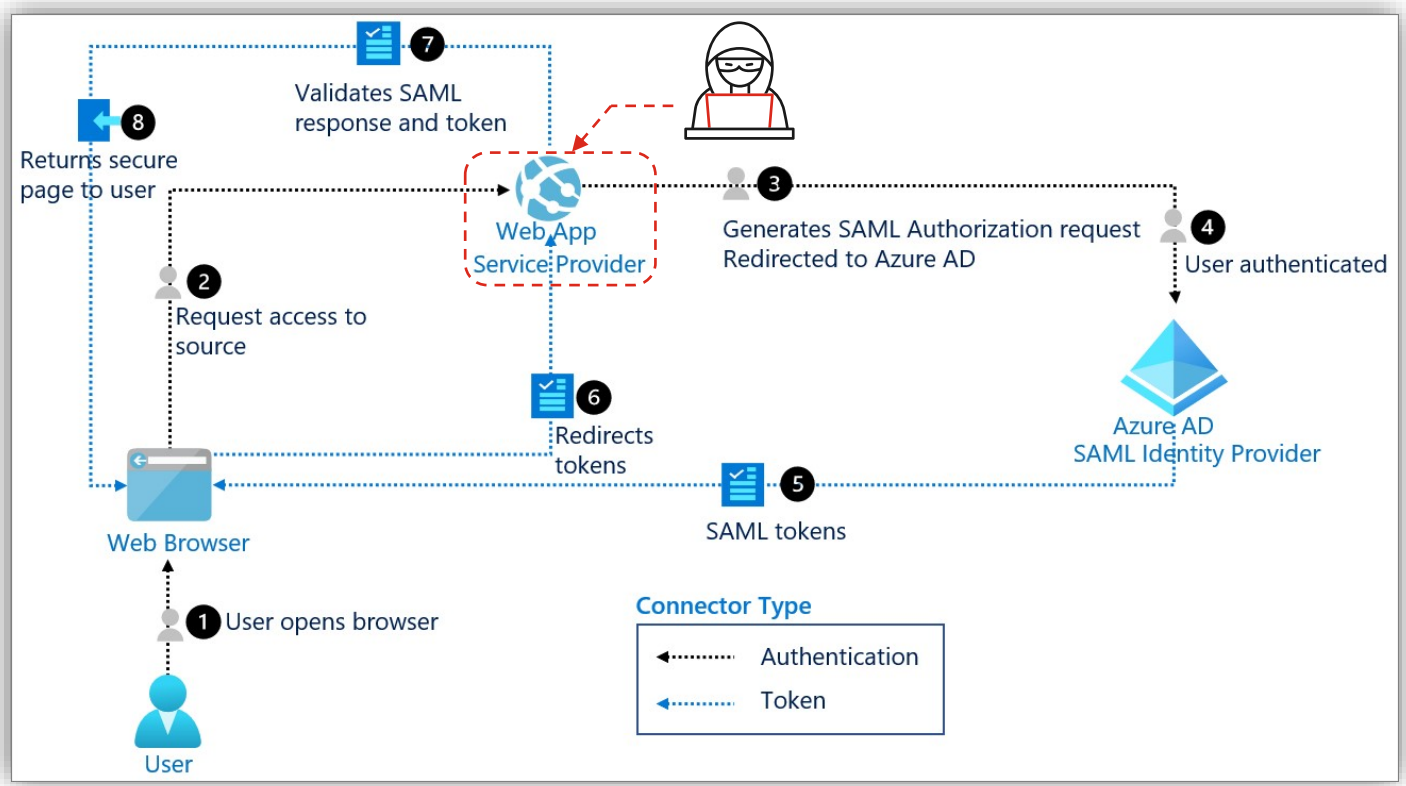


Impact: brute force

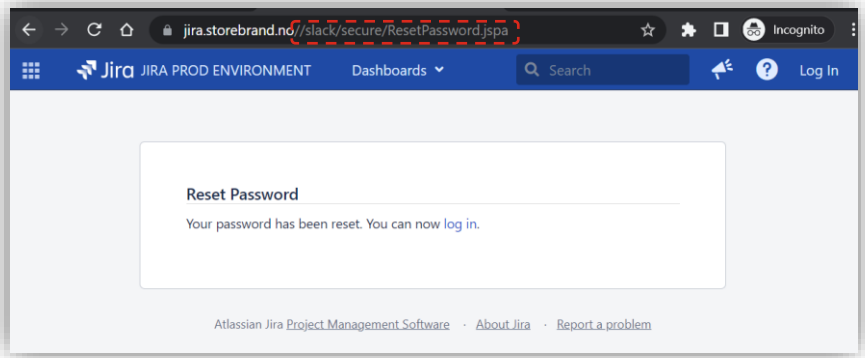




SAML authentication with Microsoft Entra ID



Impact: password reset (via Jira)



Password reset request

A request has been received to reset your password.

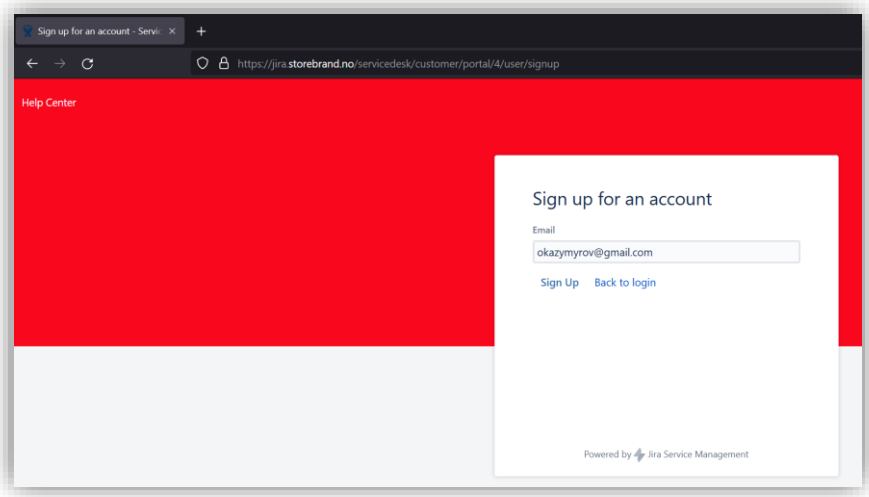
If you follow the link below you will be able to personally reset your password.
https://jira.storebrand.no/secure/ResetPassword!default.jspa?
os_username=[redacted]

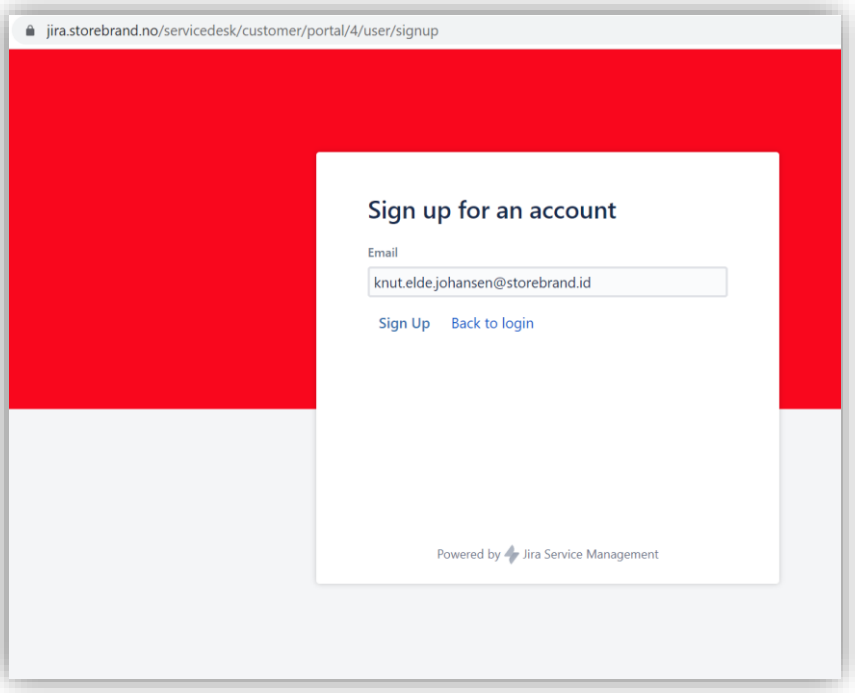
This password reset request is valid for the **next 24 hours**.
Don't worry you can always ask for a new password using the following link:
https://jira.storebrand.no/secure/ForgotLoginDetails.jspa?username=[redacted]

Here are the details of your account:

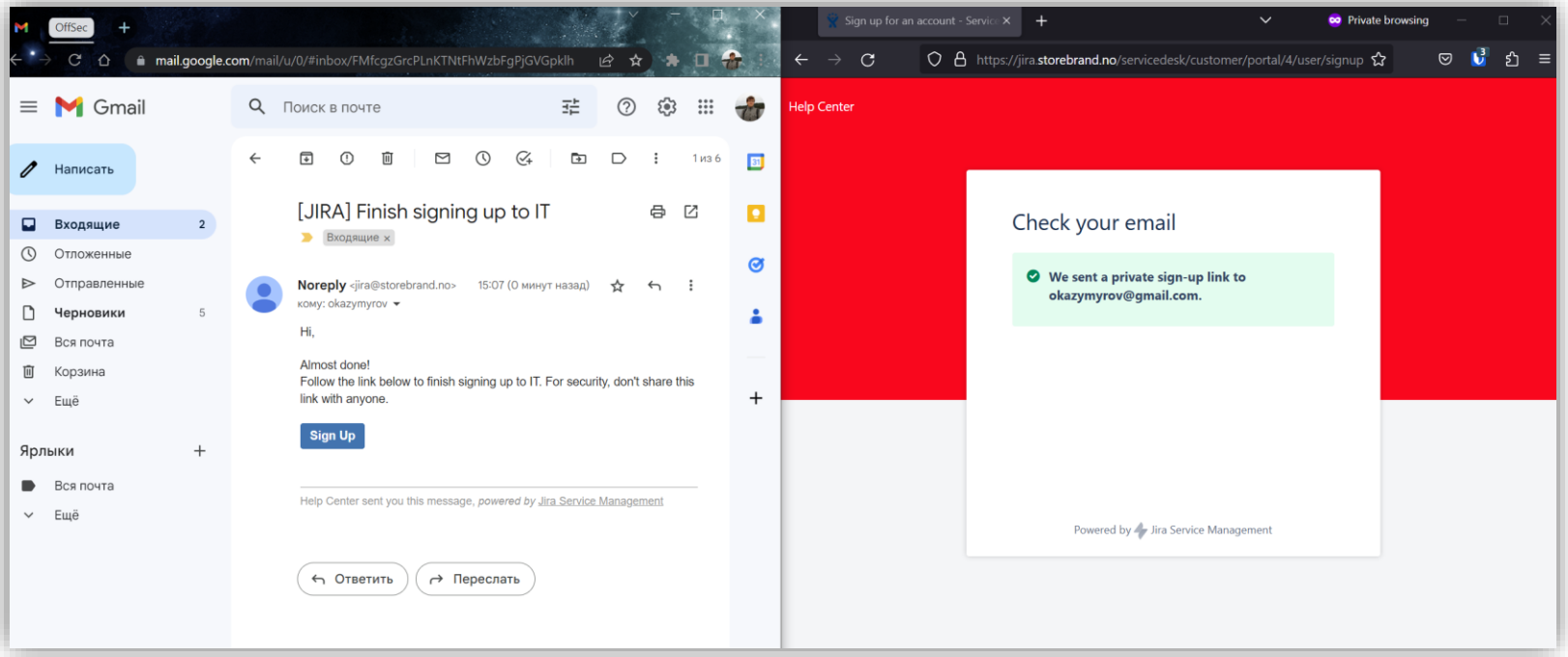
Username: [redacted]
Email: oleksandr.kazymyrov@storebrand.no
Full Name: Kazymyrov, Oleksandr

Impact: sign up for an account

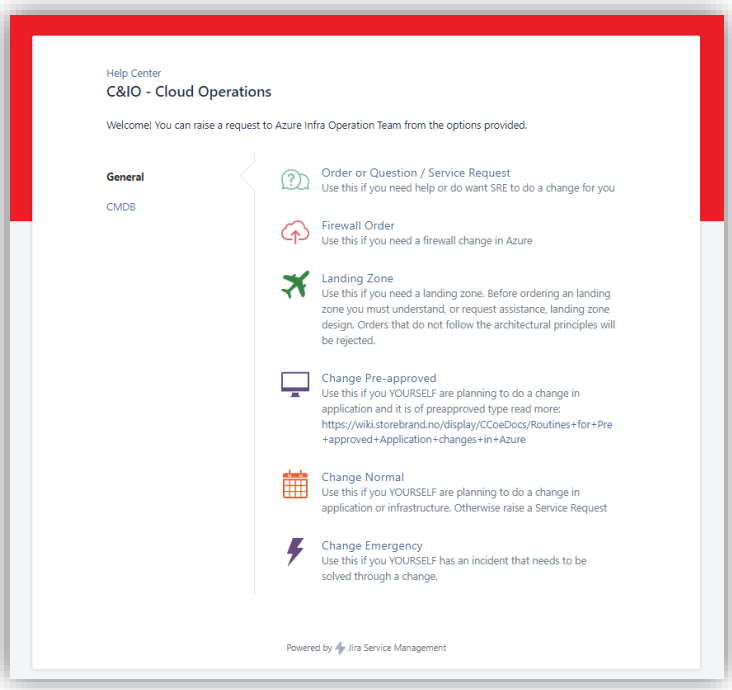


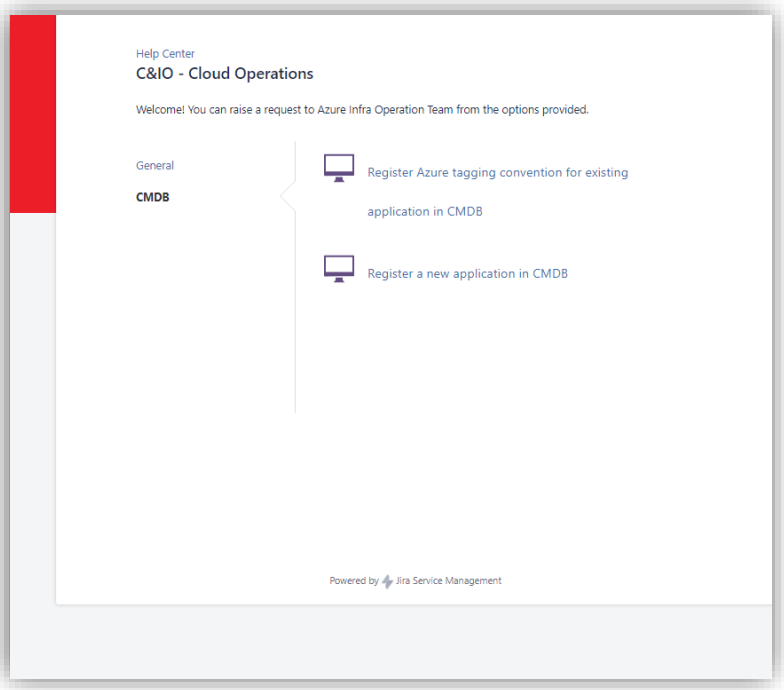


Impact: sign up for an account

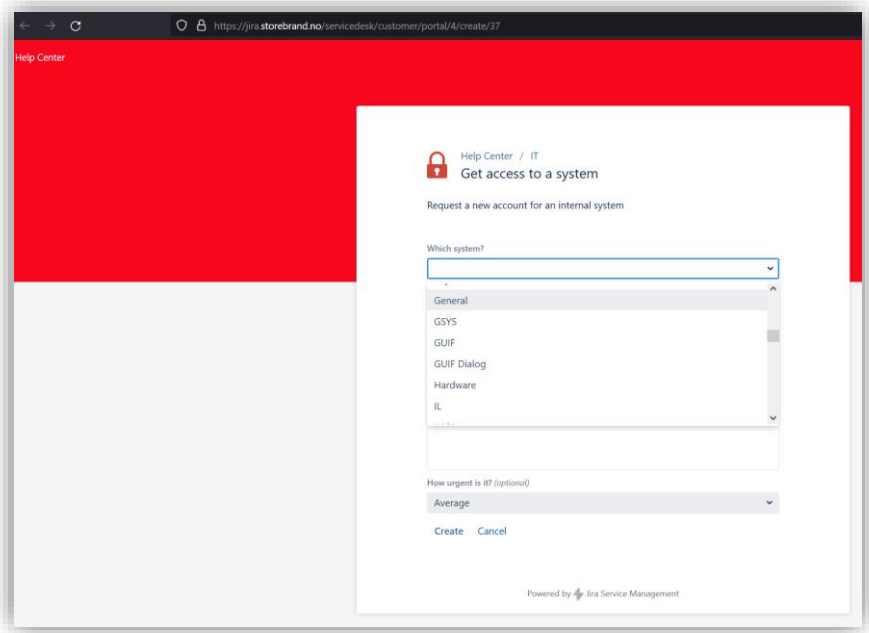


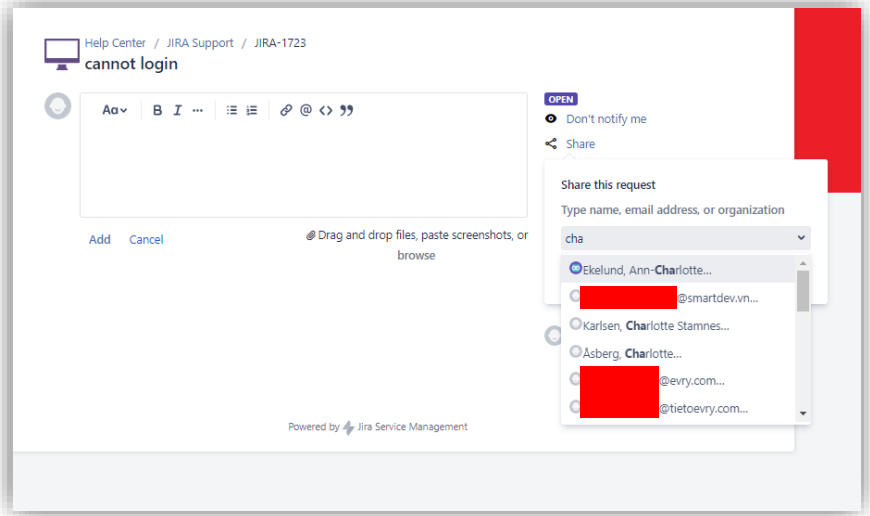
Impact: enumeration / reconnaissance



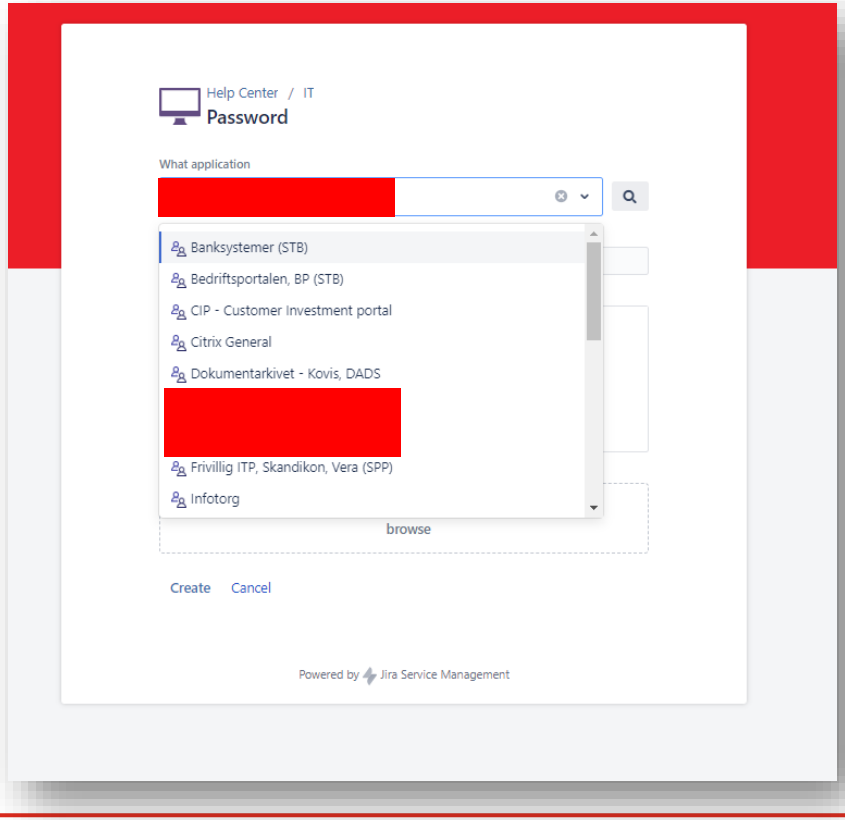


Impact: enumeration / reconnaissance

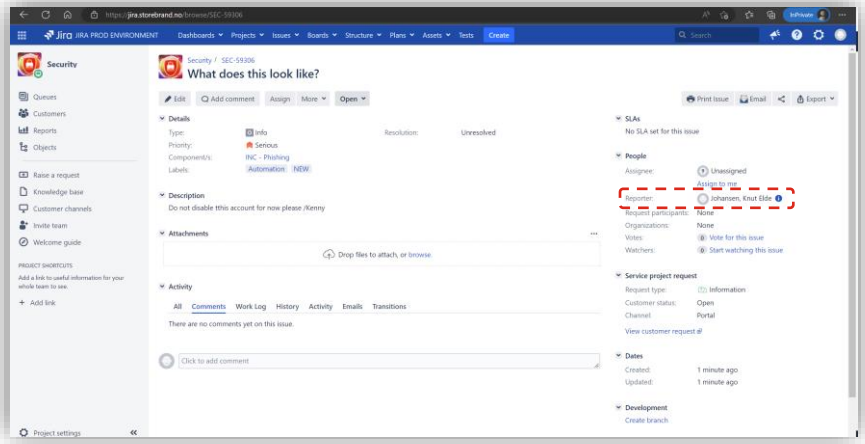


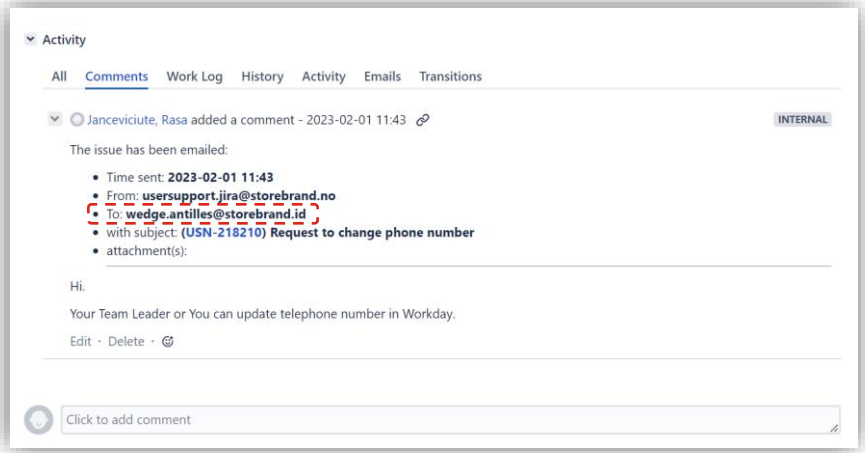


Impact: social engineering via IT support

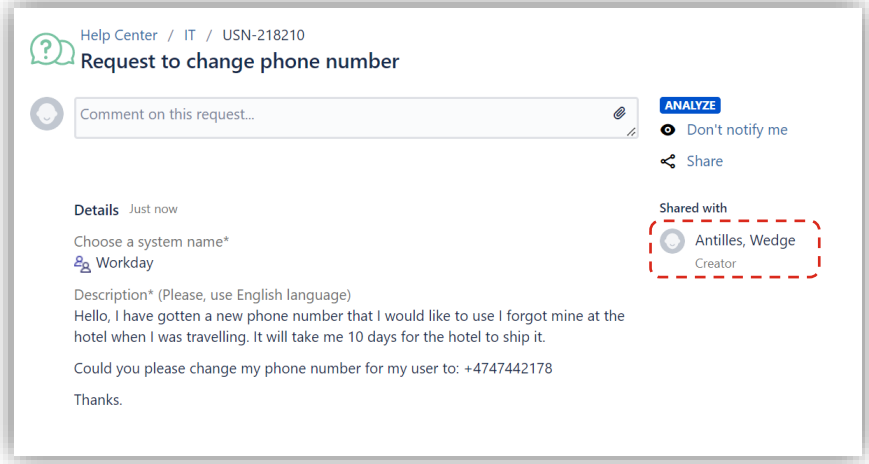


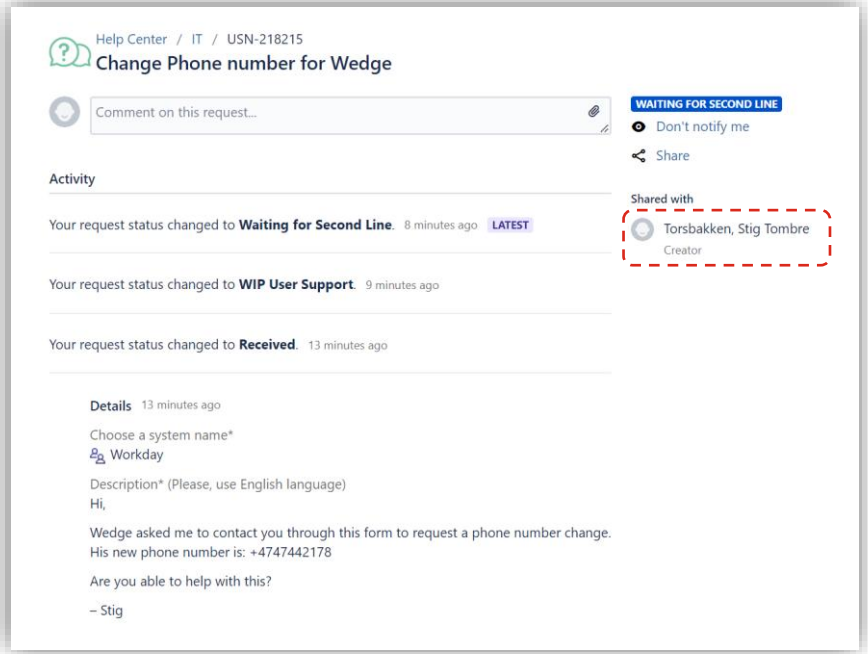
Impact: social engineering via IT support



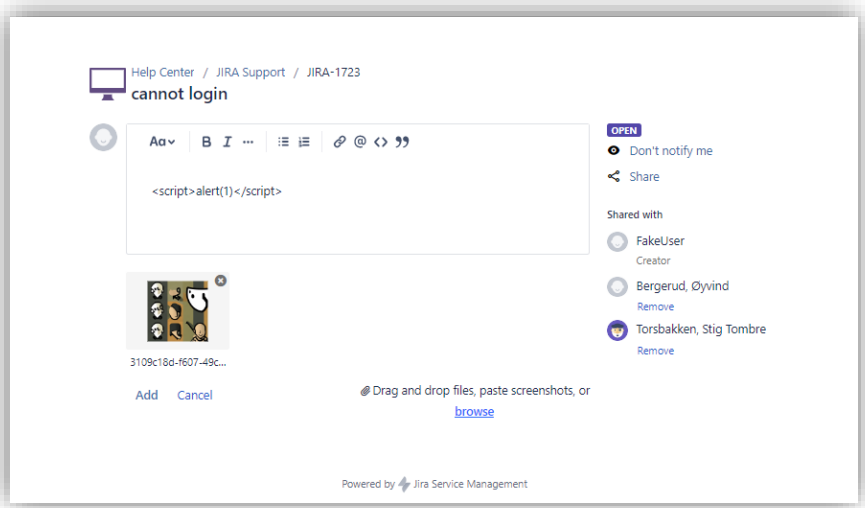


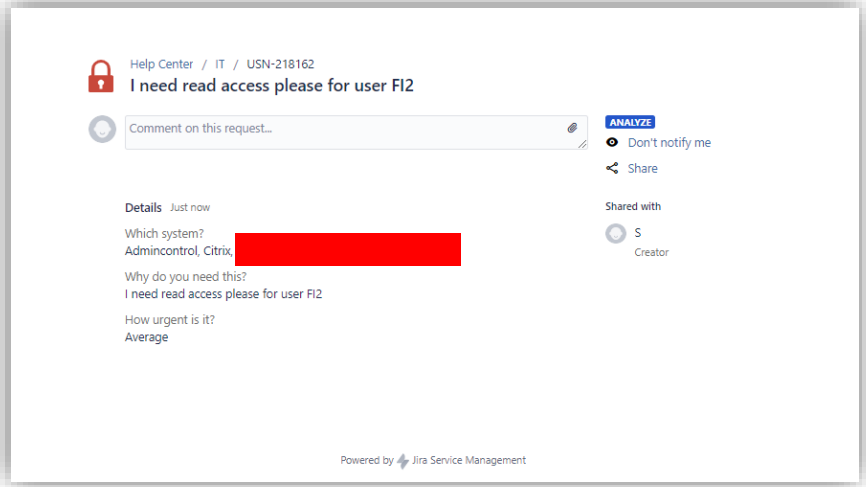
Impact: social engineering via IT support



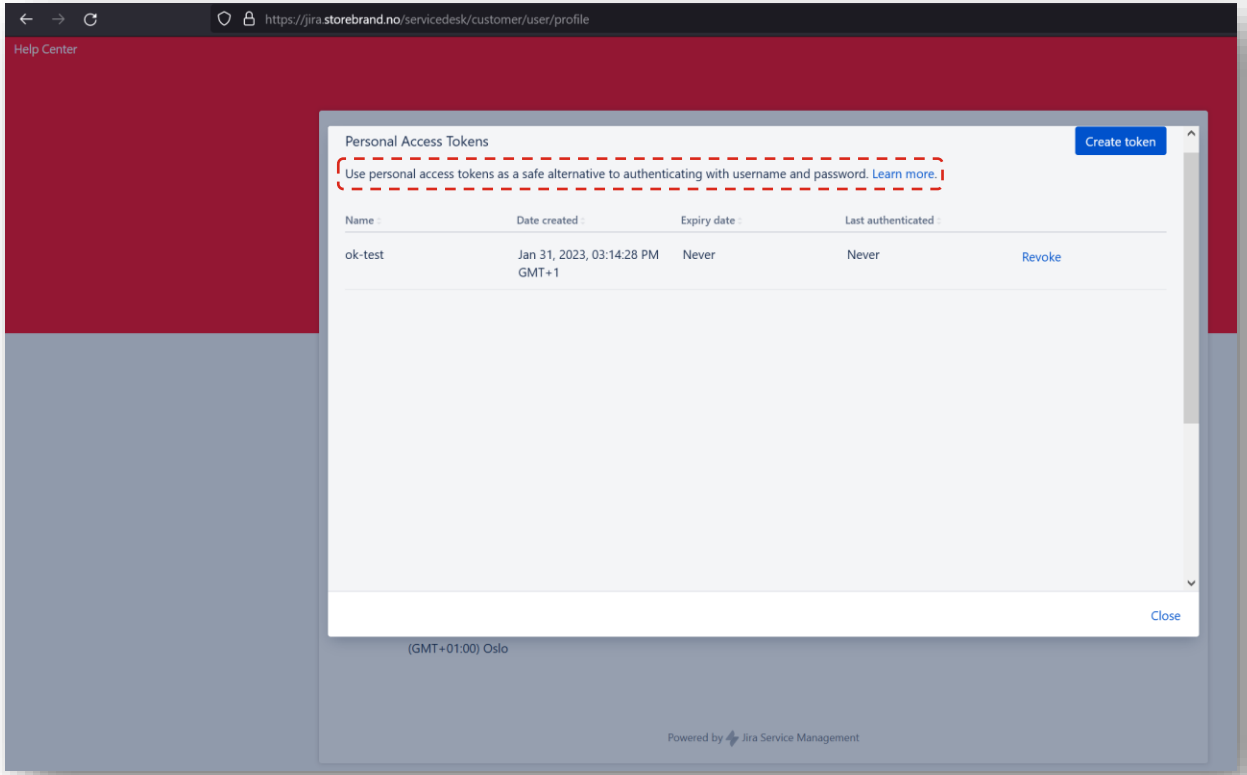


Impact: social engineering via IT support

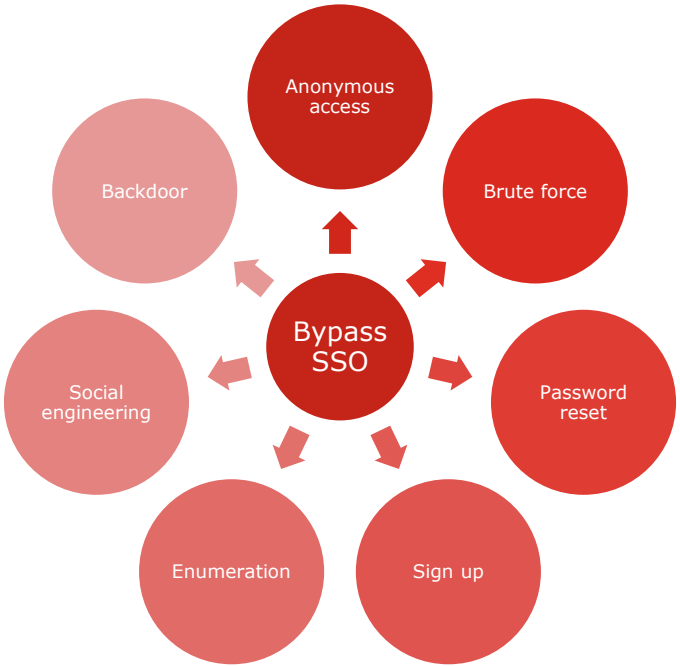




Impact: backdoor



Summary of impact



”

Our greatest glory is not in never falling, but in rising every time we fall.

Confucius