Vulnerability Disclosure Document

Date: 01/23/2024

Introduction

Bryce “Raindayzz” Harty has identified a security vulnerability existing in FileMage Gateway. FileMage does not properly manage the lifecycle of a user's session. This vulnerability is present and identified on all most up to date versions of FileMage Gateway

Product Description

FileMage Gateway is an FTP/SFTP server backed by a cloud object storage API. Deployable from your cloud provider marketplace and billed hourly.

Vulnerability Information

1. Account Logout Session Cookie

Description	FileMage does not properly handle the session cookie when a user logs out of the application or changes their password therefore leaving it vulnerable to replaying/hijacking attacks.
Impact	An attacker can leverage the outdated session cookies to access administrator capabilities.
Recommendation	Implement session refreshes when a user account logs out of the application.

Additional Information https://cwe.mitre.org/data/definitions/613.html

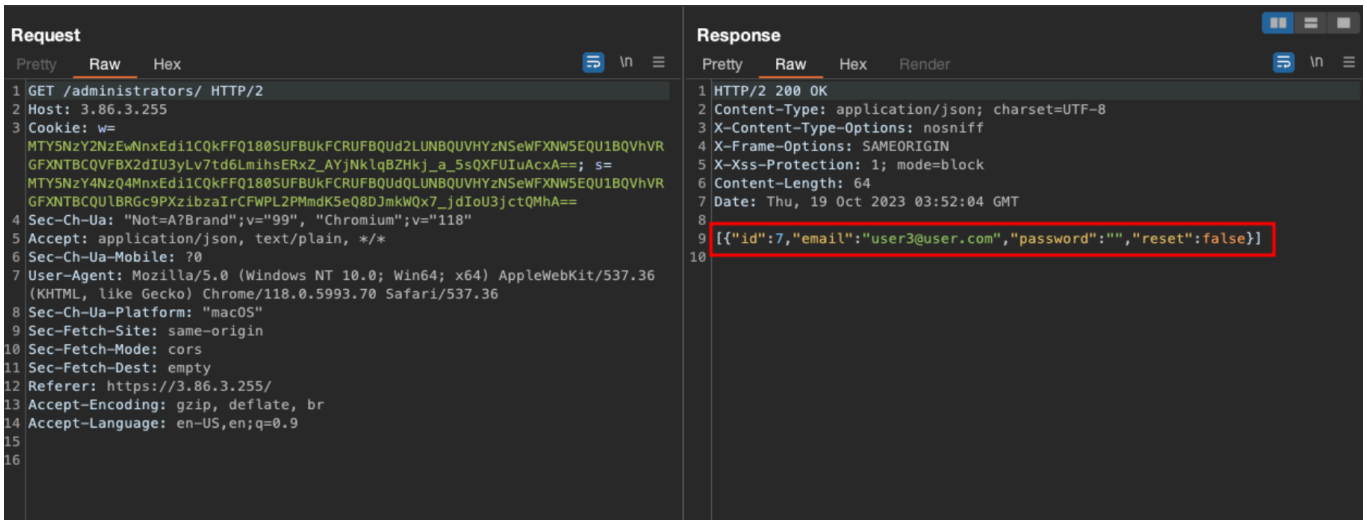
There are two ways to perform the attack. Both attack vectors are mentioned below

Technical Details

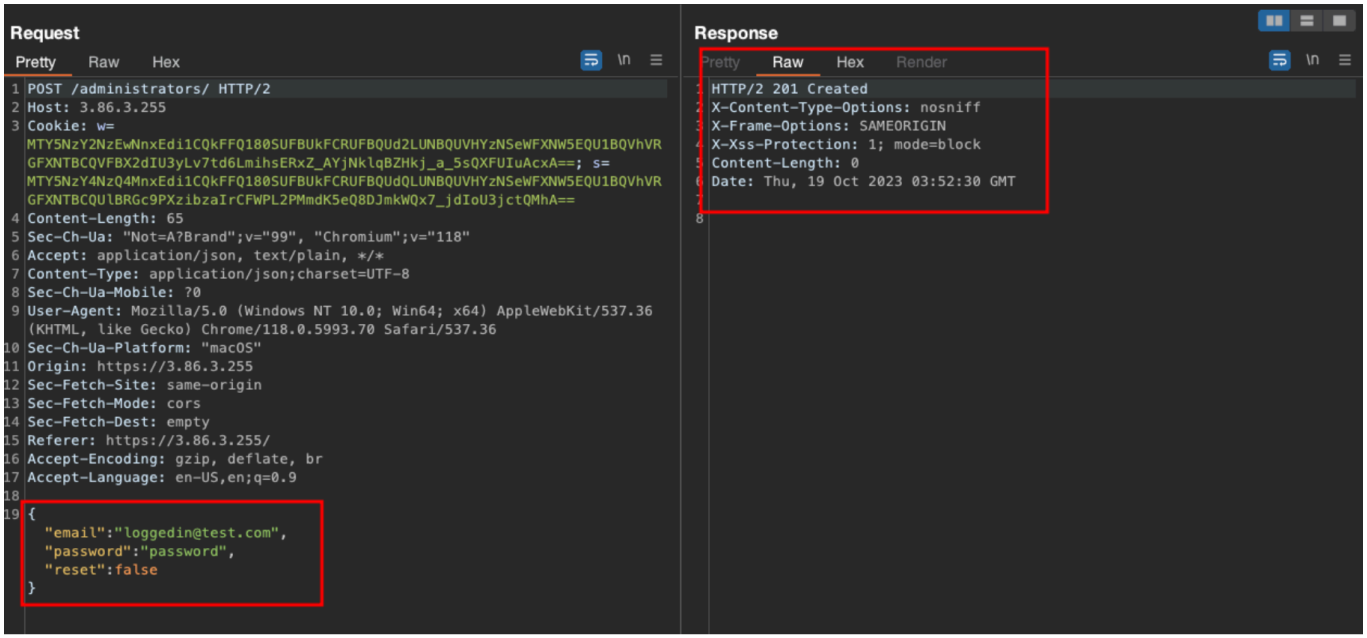
Attack #1 - Account Logout Session Cookie

With an administrative account we were able to view the current list of administrators and add a new admin using GET/POST requests as demonstrated below:

GET /administrators

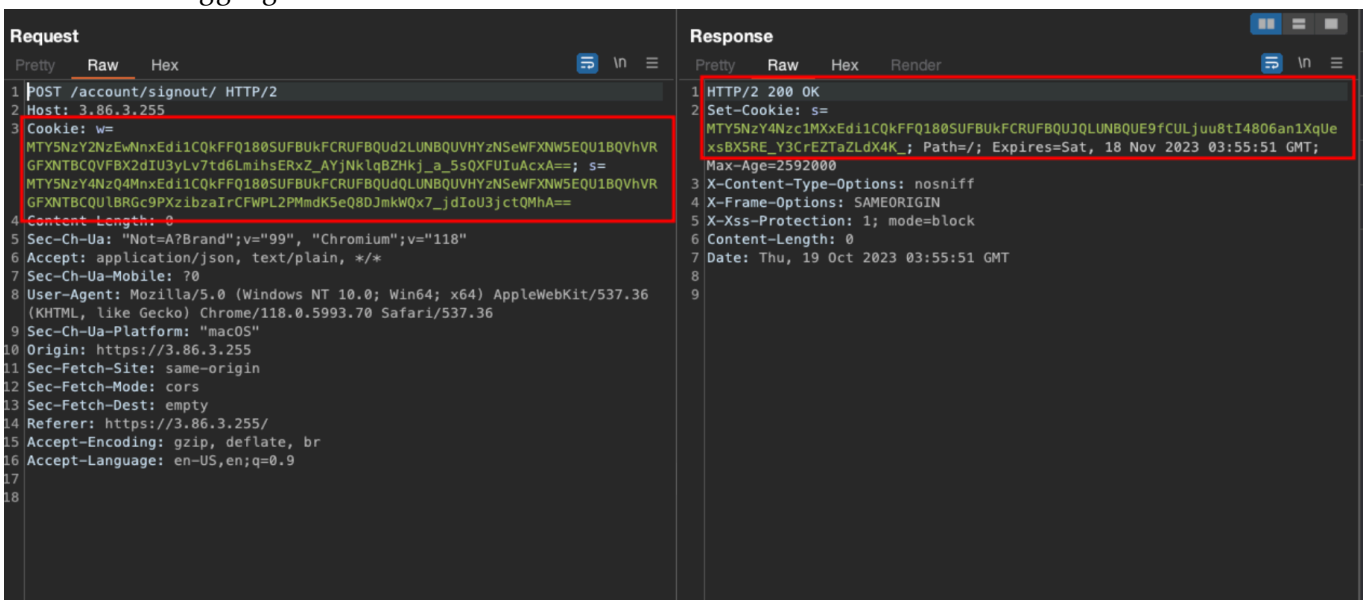


POST /administrators - adding a new user called "LOGGEDIN@TEST.COM"



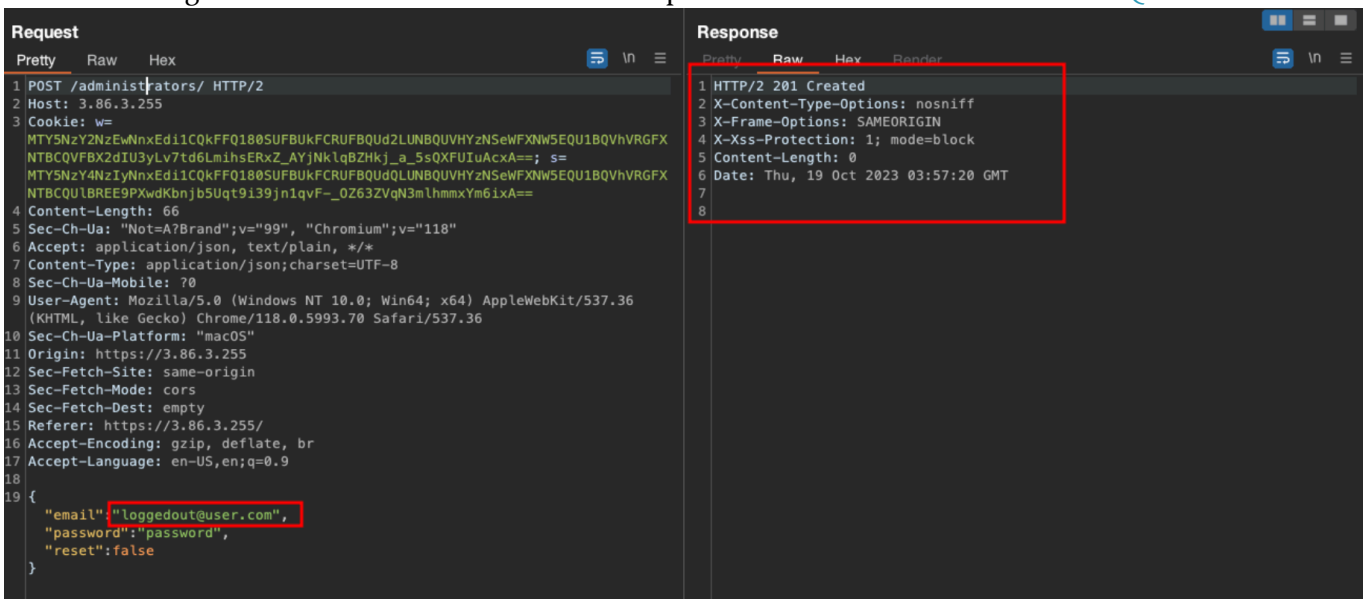
The vulnerability is identified when a user logs out, it does not invalidate the session cookie.

User logging out of the session.

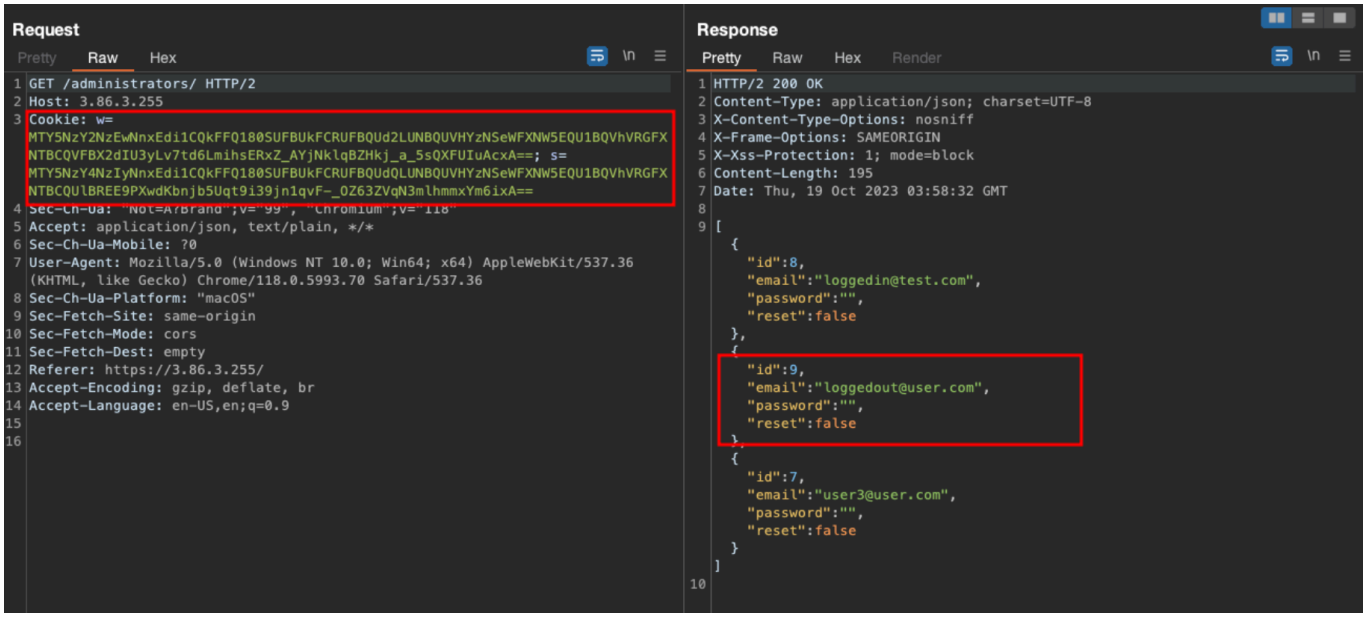


Now when using the same session cookie, we are still able to view and add additional administrator users as seen below:

Adding an additional user called with expired session cookie "LOGGEDOUT@TEST.COM"



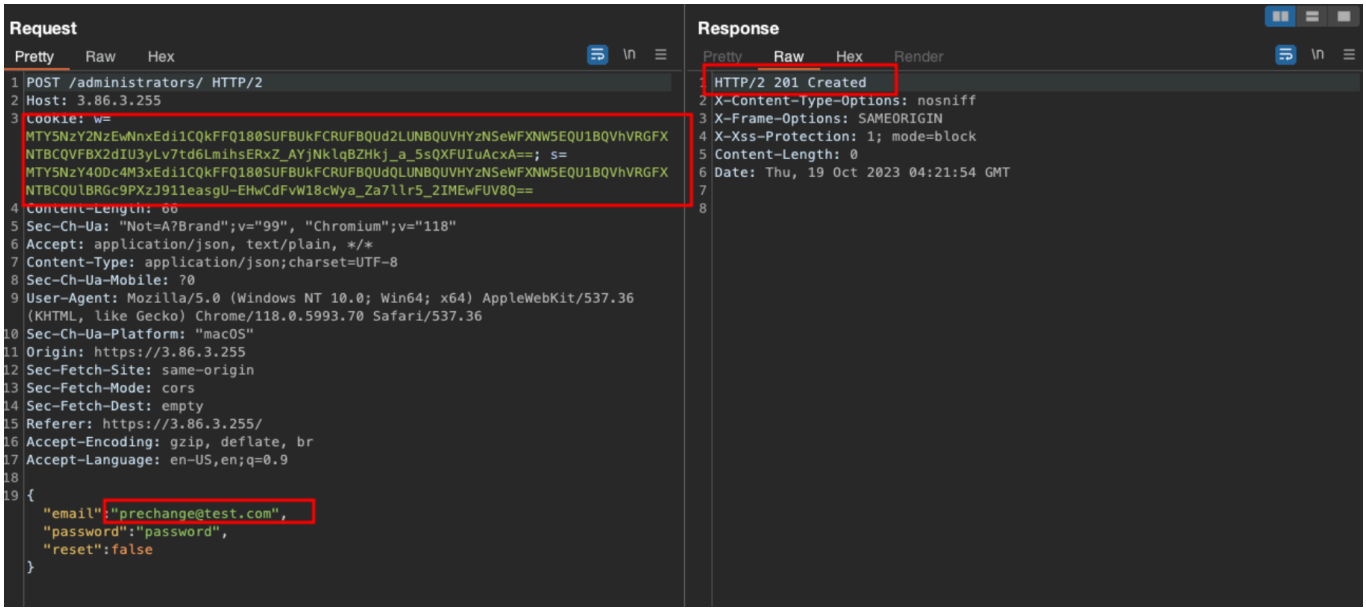
GET /administrators with expired session cookie



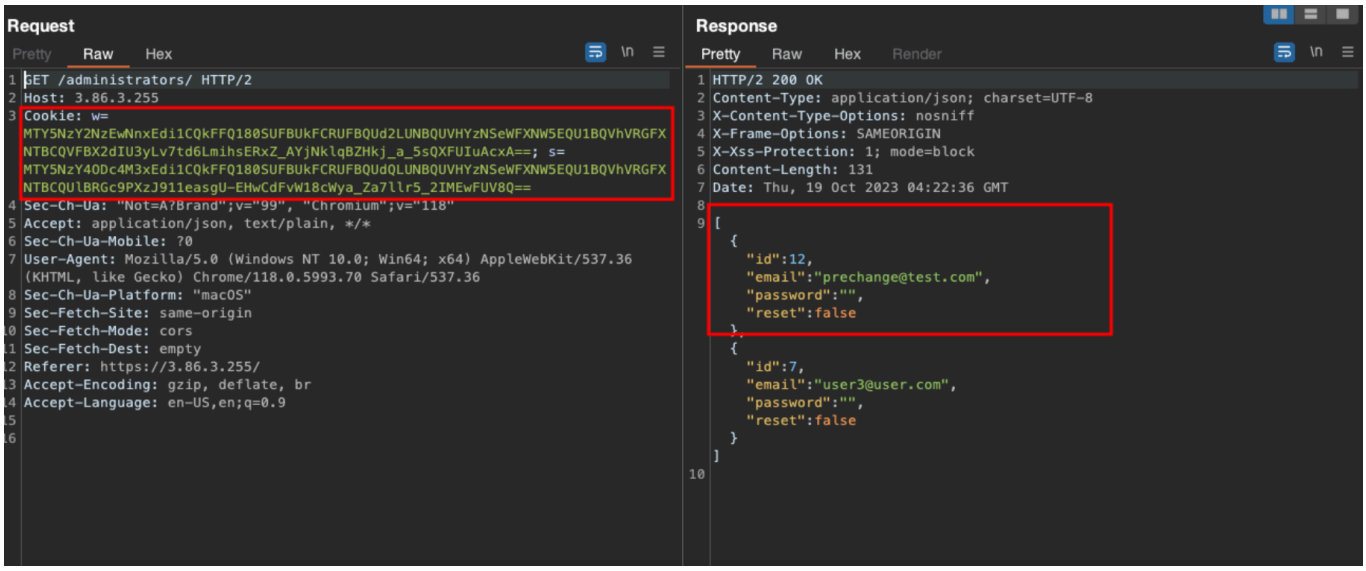
Attack #2 - Account Password Session Cookie

With an administrative account we are able to view the current list of administrators and add a new admin using GET/POST requests demonstrated below:

POST /administrators - adding a new user called "PRECHANGE@TEST.COM"

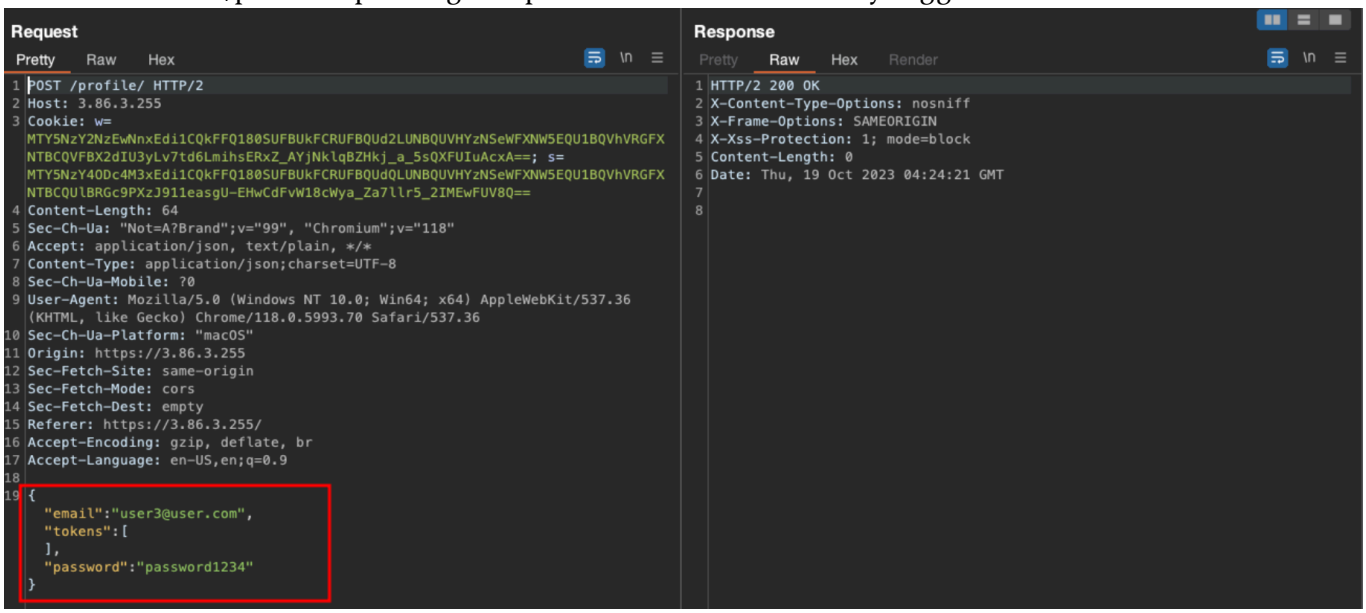


GET /administrators



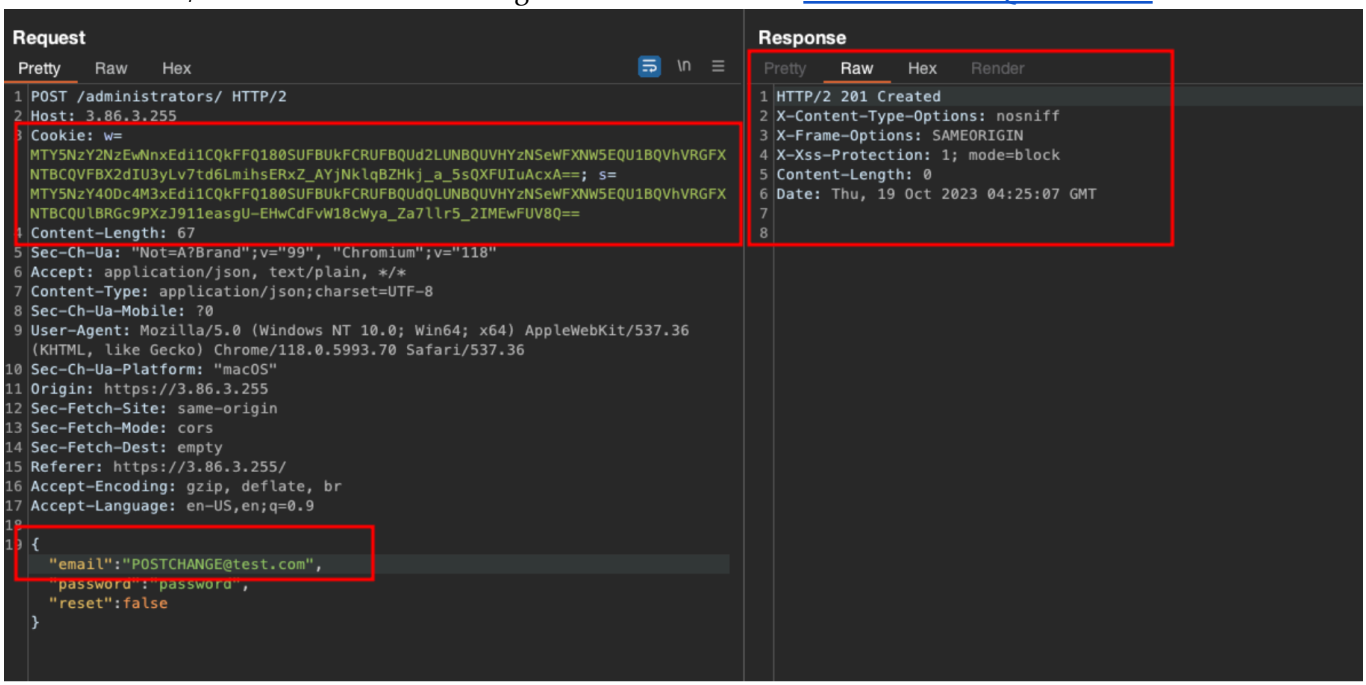
The user is able to change their existing password and still use the old session cookie to perform admin functionality.

POST to /profile updating the password of the currently logged in account.

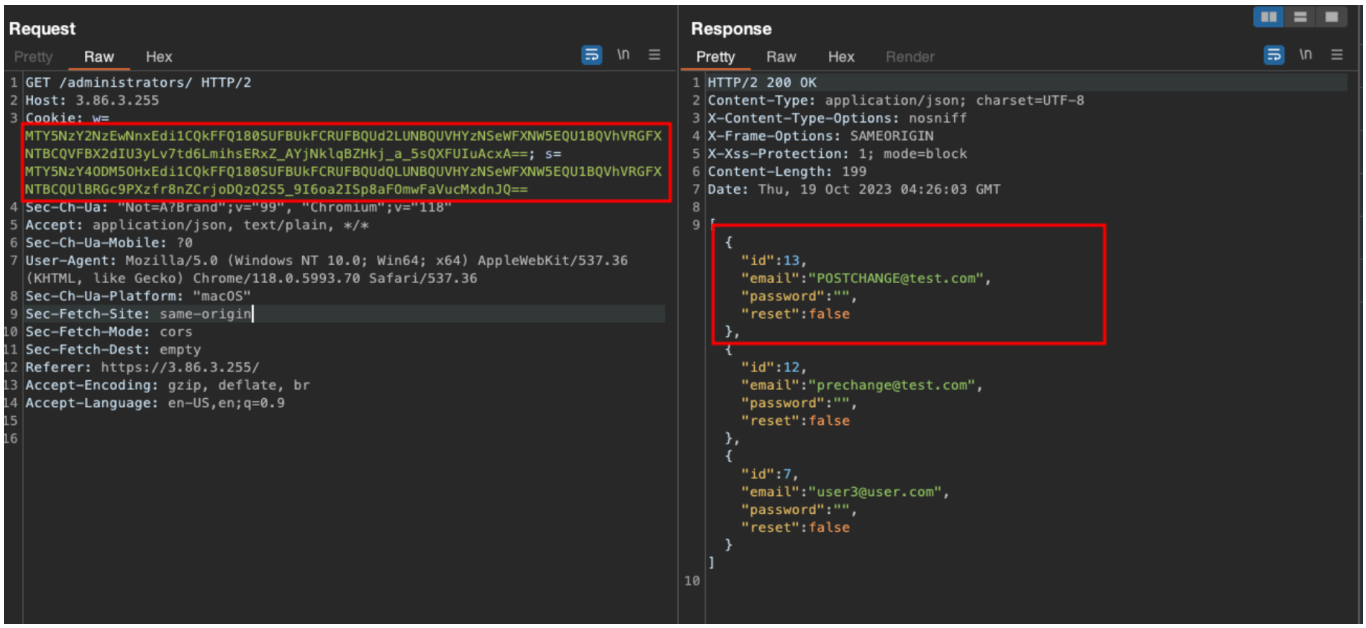


We are still able to add and view old accounts simulating admin functionality.

POST /administrators - adding a new user called "POSTCHANGE@TEST.COM"



GET /administrators



Impact

Filemage contains a vulnerability that could allow an attacker to maintain unauthorized access over a hijacked session after the legitimate user has signed out or changed the password of their account.

Heirloom Security has assigned the following personnel to facilitate and coordinate responsible disclosure efforts.

Name	**Role**	**Email**
Bryce “Raindayzz” Harty	Researcher	bryce@heirloomsecurity.com