FROSTY LABS

BE THE CHANGE THAT YOU WANT TO SEE IN THE WORLD

CVE-2020-10107

by Frosty 05/03/2020

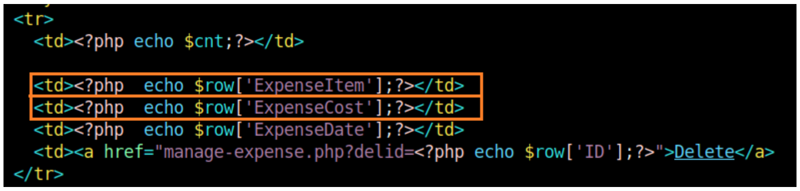
Daily Expense Tracker System (DETS) is vulnerable to stored cross site scripting (XSS). This post will be a brief write up about discovery and exploitation of CVE-2020-10107. This vulnerability exists in the Daily Expense Tracker System project version 1, which you can download from phpgurukul, here.

According to phpgurukul's website, this application has been downloaded at least 499 times – time of vulnerability discovery.

Discovering the Vulnerability

After a static code review, I noticed that SQL output is directly rendered to the user. I decoded to test whether there is input sanitation when storing values in the MySQL database. A simple payload as described below could be used when storing values in the MySQL database, to exploit the vulnerability when viewing `manage-expense.php`.

The php code below shows that values are grabbed directly from the MySQL database and are rendered to the user, without any output escaping.



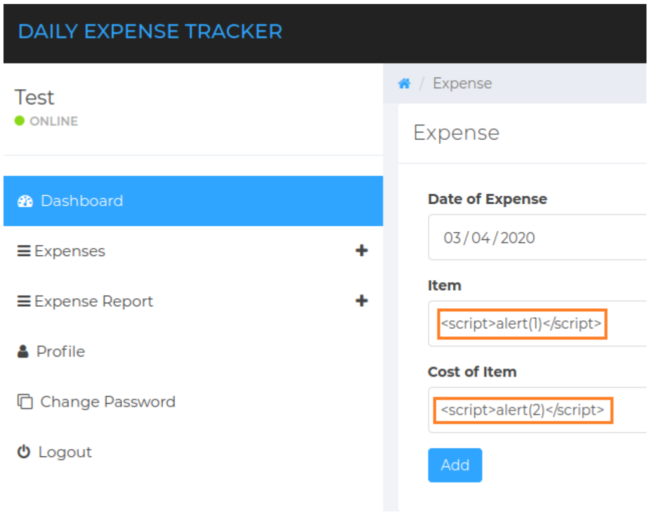
```
<tr>
  <td><?php echo $cnt;?></td>

  <td><?php  echo $row['ExpenseItem'];?></td>
  <td><?php  echo $row['ExpenseCost'];?></td>
  <td><?php  echo $row['ExpenseDate'];?></td>
  <td><a href="manage-expense.php?delid=<?php echo $row['ID'];?>">Delete</a>
</tr>
```

Source code of manage-expense.php

Verifying the Vulnerability

In the image below, it is seen that `alert(1)` and `alert(2)` are used. This is a habit which I have gotten myself into when testing for such a vulnerability. The numbers allow me to identify specifically which field is vulnerable. This is useful in cases where one field is vulnerable, but the other may not be.

```
<script>alert(1)</script>
```



Expense

Date of Expense

03/04/2020

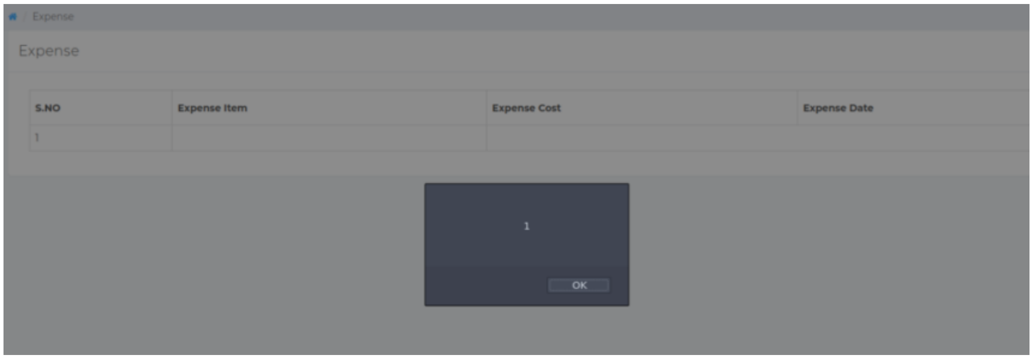
Item

<script>alert(1)</script>

Cost of Item

<script>alert(2)</script>

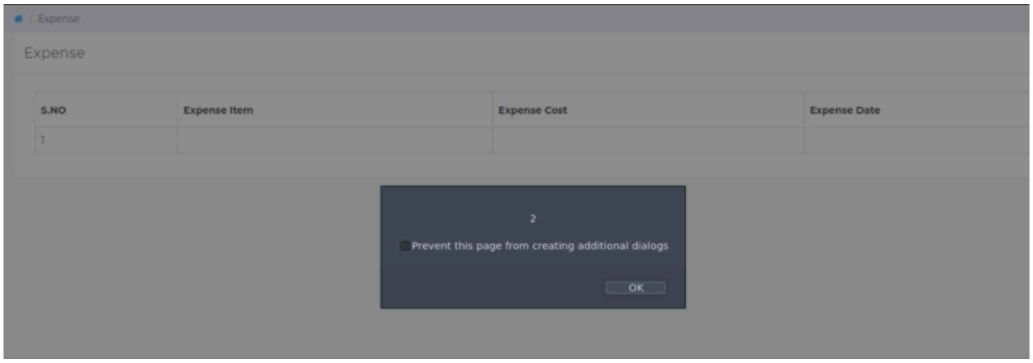
Testing XSS parameters



S.NO	Expense Item	Expense Cost	Expense Date
1			

1

alert 1



S.NO	Expense Item	Expense Cost	Expense Date
1			

2

□ Prevent this page from creating additional dialogs

alert 2

Posted in Writeups • Tagged CVE

Published by Frosty

View all posts by Frosty

PREV

CVE-2020-10106

NEXT

HackTheBox: Postman

3 Replies to "CVE-2020-10107"

Briandar
25/03/2020 at 11:52 AM

Thanks very useful. Will certainly share website with my good friends.

REPLY

Frosty
26/03/2020 at 10:02 PM

Super, happy to hear you found this useful 🙂

REPLY

Briandar
05/04/2020 at 3:38 AM

Good webpage you possess in here.

REPLY

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

TOPICS

Blog

Projects

Writeups

RECENT POSTS

Debian Configure IP Address and VLANs
29/09/2022

HackTheBox: BountyHunter
20/11/2021

Published Paper!
23/04/2021

HackTheBox: Passage
06/03/2021

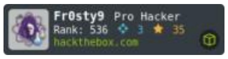
Configure GitHub SSH Keys
07/02/2021

HackTheBox: Tabby
07/11/2020

VulnHub: Zico 2
20/09/2020

BADGES

Hack the Box



Fr0sty9 Pro Hacker
Rank: 536 3 ★ 35
hackthebox.com

TryHackMe