How i was able to bypass strong xss protection in well known website. (imgur.com)

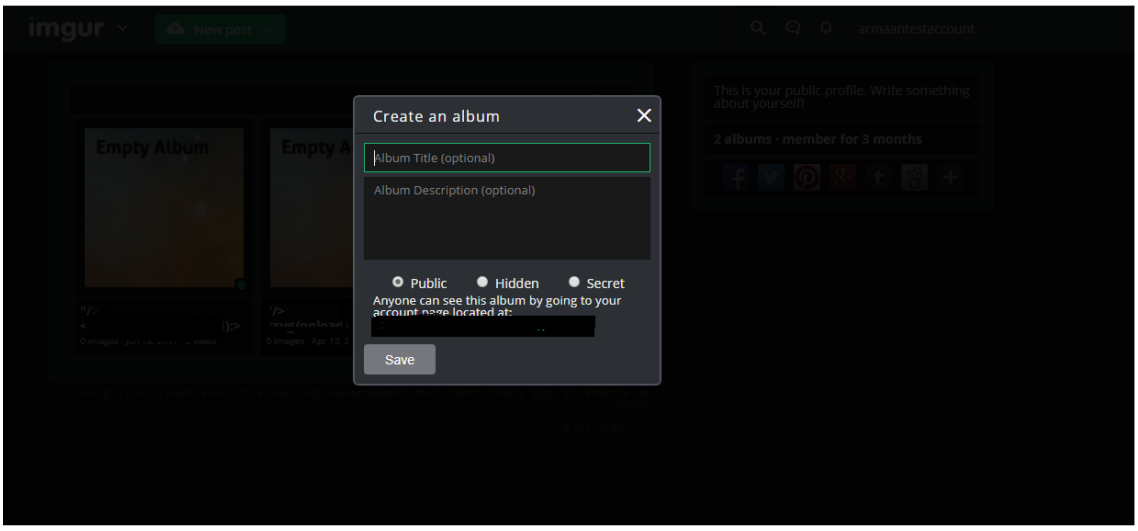
Armaan Pathan Follow
Jul 21, 2017 · 2 min read

after finishing my final exams i have decided to give a dedicated time to bug bounty, not to EARN but to LEARN, so i had selected my target.

so i selected my domain which was imgur.com.

as soon as i selected the target i started browsing the website & at there i found that there is a option

ALBUM DESCRIPTION



i decide to find that album description is vulnerable to Cross site scripting vulnerability or not.

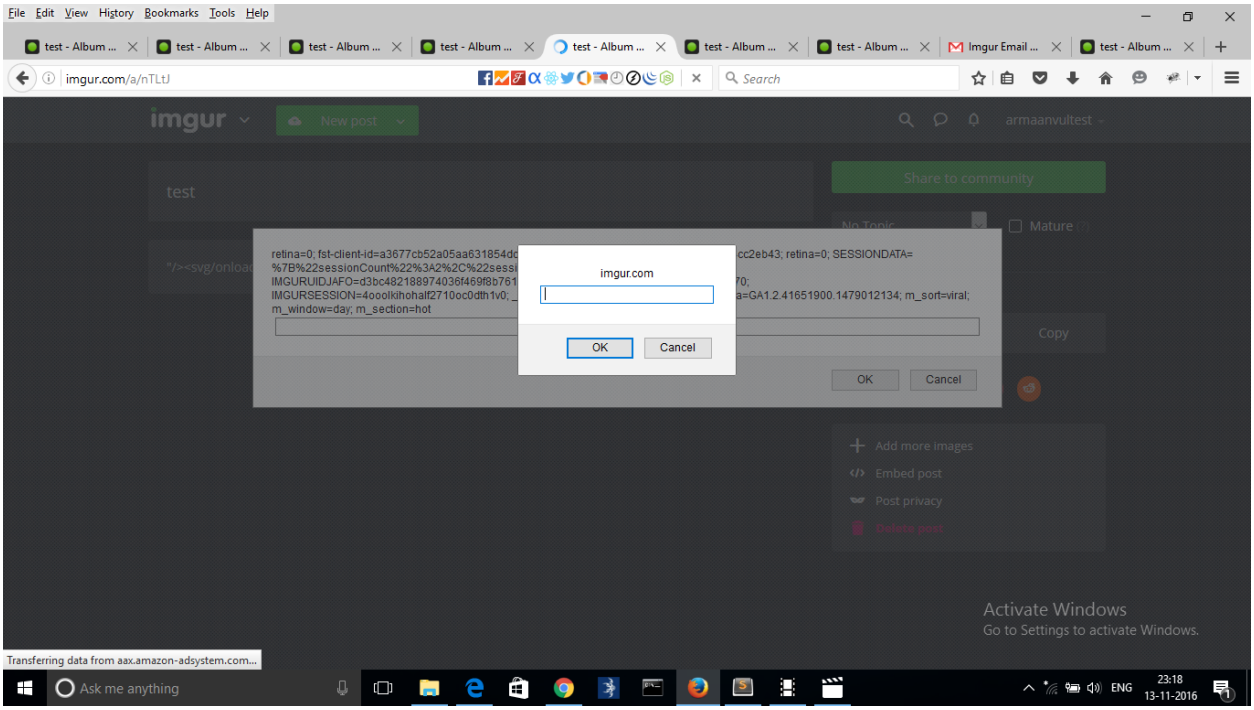
so first i entered “/><script>alert(1);</script> and i noticed that it had removed the <script> tags from the album description at it was displaying alert(1); without any pop-up.

Then I decided to use event handler payload to check that i am getting the pop-up or not. so i tried “/><svg/onload=prompt(1);> & and now i had noticed that it has removed the onload tag from album description and it was only displaying <svg/prompt(1);> tag.

So here i had noticed the behavior of the application that it is stripping out the <script> tags and also stripping out the event handlers.

Then after I finally decided to use both <script> tag and event handlers to bypass the xss protection so i used ”/><svg /on<script>load=prompt(document.domain);>”/><svg /on<script>load=prompt(document.cookie);>

AND



i had bypassed the XSS protection over there and was able to store the malicious scripts.

and after reported it was patched & rewarded with sweet bounty :)