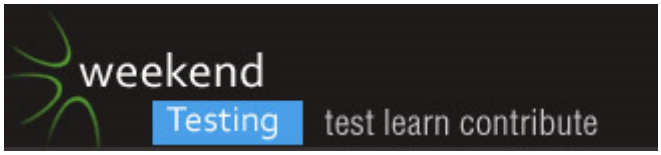
Test Hats

Functional | Security | Performance

Weeknight Testing

Security Testing Session Overview

21st September 2011



Tel: 020 3239 8254 | **Email:** sales@testhats.com | **Web:** www.testhats.com

© Copyright Test Hats, 2007 – 2011.

Introduction

The Weekend Testers are a global group of test professionals, who meet both at the Weekend and Weeknights to learn about software testing together. The informal group has grown in strength and there are now many chapters around the world.

Visit the website at **http://weekendtesting.com/**

September Weeknight Testing Session

Test Hats are proud to have been asked to facilitate a web based Weeknight Testing session in September. The lead facilitator on the night will be Mark Crowther, Principle Test Architect at Test Hats.

When

- **Date:** Wednesday 21st September
- **Time:** 7.30pm to 9.30pm

Location

- **URL:** http://184.175.76.222
- **Skype:** WeekNightTesting

Outline Agenda

- **Testing Session:** 7.30pm to 8.30pm
- **Feedback:** 8.30pm to 9.30pm

All Skype comments and notes will be collated and sent to the moderators at Weeknight Testing. The notes will then be added to the groups' forum.

- **http://weekendtesting.com/discussions**

© Copyright Test Hats, 2007 – 2011.

Exploratory Security Session

The theme of the September session is on web application security.

The web application that is the target and subject for the session is currently hiding behind a link at the above URL. This will be made active at **7.30pm**, **21st September**.

Background

It's our contention that testers who practice exploratory testing techniques have learned a number of essential skills for testing in a security context.

Being guided by test conditions but driven by heuristics. Thinking, observing, questioning, reasoning and testing ideas and insights, applying knowledge, acting on new information as it arises. These are essential skills for a security tester and those who regularly practice exploratory techniques are well equipped, technique wise if not domain knowledge wise, to test in a security context.

However, we also contend that security testing is seen as an exotic and separate field to application testing, and as such many testers avoid testing related to security.

We believe this is both and unfortunate and concerning state of affairs. With the continual rise in Cybercrime and growing threat from Hacktivist groups such a Lulzsec and Anonymous, it's essential that competent testers skill-up in security related testing.

© Copyright Test Hats, 2007 – 2011.

Mission

With this background, the mission of the September Weeknight Testing Session is;

> *"Encourage testers to perform exploratory testing, in a security context. In so doing they will demonstrate to themselves and the group, that they are capable of performing a level of security related testing."*

This mission will be achieved in part by Test Hats providing a test target and guidance notes, but mainly by the participants applying their skills and looking to break the application!

Exploratory Security Session

The session requires participants to consider security functionality of the application and assess whether certain security issues exist. The nature of potential bugs are described below but should be considered a guide only. The application is extremely badly developed and there are many ways to make it break in terms of security.

Outcomes

Tested hard enough the application is likely to exhibit all issues given below but the participants need to *prove it*. That proof comes in the form of such things as:

- well documented steps
- clear and repeatable paths to show a bug
- an unambiguous description of the bug

Probably of most important thing however is the ability of the participants to describe their thinking, insights, actions and heuristics used, that led them to the interesting discovery. This will provide the most learning for other participants.

© Copyright Test Hats, 2007 – 2011.

Mini Missions

The support team say customers are calling and reporting strange behaviour with our application, you and your team need to investigate. You have **one hour** so you're not expected to research every support ticket!

Ticket No: WNT-001	**State:** Active
Description: It appears some Snippet text was altered and then put back again.	
Possible Issue: Privilege Escalation	
Comments: (AF) The only way user Snippet text can get altered is by Admins. We have some Admins for the site but I asked them and they said they didn't change anyone's text. (DG) Are any users being set as Admins by mistake? (AF) Is it possible to find out how the application knows we're a User or Admin and then become an Admin? Where is that information stored or transmitted?	

Ticket No: WNT-002	**State:** Active
Description: User noted their content was changing 'on the fly', they enter some and then it got changed after them. As if someone was also logged into their account.	
Possible Issue: Privilege Escalation, Cookie Manipulation	
Comments: (DG) Does anyone in support know how users (ID) get identified by the application?	

Ticket No: WNT-003	**State:** Active
Description: User asked if we do pop-up ads? Apparently they were viewing uploads and got a pop-up that seemed out of place.	
Possible Issue: File Upload Cross Site Scripting (XSS)	
Comments: (PT) Can users upload scripts (in files) and have them run / pop-up messages? Thought it was just simple files they could add?	

© Copyright Test Hats, 2007 – 2011.

Ticket No: WNT-004	**State:** Active
Description: User reporting pop-up boxes again, this time when on the home page	
Possible Issue: Stored Cross Site Scripting (XSS)	
Comments: (PP) We let users enter HTML in some places but its limited and there are no pop-ups on the home page or anywhere else. (DG) HTML input is sanitized, over to test for investigation.	

Ticket No: WNT-005	**State:** Active
Description: User said they logged into their account area and got a pop-up	
Possible Issue: Stored Cross Site Scripting (XSS) via HTML attribute	
Comments: (MZ) What's the 'account area'? (DG) Profile. They can't enter HTML there, just form values, so no pop-ups / XSS	

Ticket No: WNT-006	**State:** Active
Description: User said they were navigating around and it made one of their Snippets get deleted	
Possible Issue: Cross Site Request Forgery	
Comments: (AL) LOL, they must have clicked the 'X' button then, not a bug. (DG) How does the delete work? Can a user get another user to delete stuff by 'accident'?	

© Copyright Test Hats, 2007 – 2011.

Ticket No: WNT-007	**State:** Active
Description: (Support) We noticed URLs getting exposed but they should be hidden	
Possible Issue: Failure to Restrict URL Access	
Comments: (SP) Don't agree the issue classification is as above but if users can see URLs then that could be a problem I guess. (DG) How can they get to see URLs? (CG) They can't, we hide them when we send the HTTP request, it's not shown in the browser.	

Final Notes

Please…

- … don't click anything that looks like Reset or Quit, you'll know it if you find it!
- … remember others can see your posts and files, so be sure to mess with them and cause much merriment, you're a hacker for today!
- … have fun!

Tools

You shouldn't need any tools to find security related issues as the application is full of them. However, we've found some add-ons that are useful:

- **Fire Bug:** https://getfirebug.com/downloads/
- **Tamper Data:** https://addons.mozilla.org/en-US/firefox/addon/tamper-data/
- **Cookies Manager:** https://addons.mozilla.org/en-US/firefox/addon/cookies-manager-plus/

If you can use tools and share your learning with the group then that'd be great!

Thanks and good luck!

© Copyright Test Hats, 2007 – 2011.