

Are You a PenTexter?

Peter Mosmans



August 18, 2016

peter.mosmans@radical.sexy

When hackers grow up...



CONSULTING

IF YOU'RE NOT A PART OF THE SOLUTION,
THERE'S GOOD MONEY TO BE MADE IN PROLONGING THE PROBLEM.



RADICALLY OPEN SECURITY

August 18, 2016

What is ChatOps?

Radically Open Security Chat

https://chat.radicallyopensecurity.com/group/ros-offtopic


ros-offtopic

Ms.Abstract_007 11:15
lolz

melanie 11:15

johnsinteur 11:15
rosbot pug me

rosbot 11:15
http://28.media.tumblr.com/tumblr_lk82r5fJzw1qebvsbo1_500.jpg



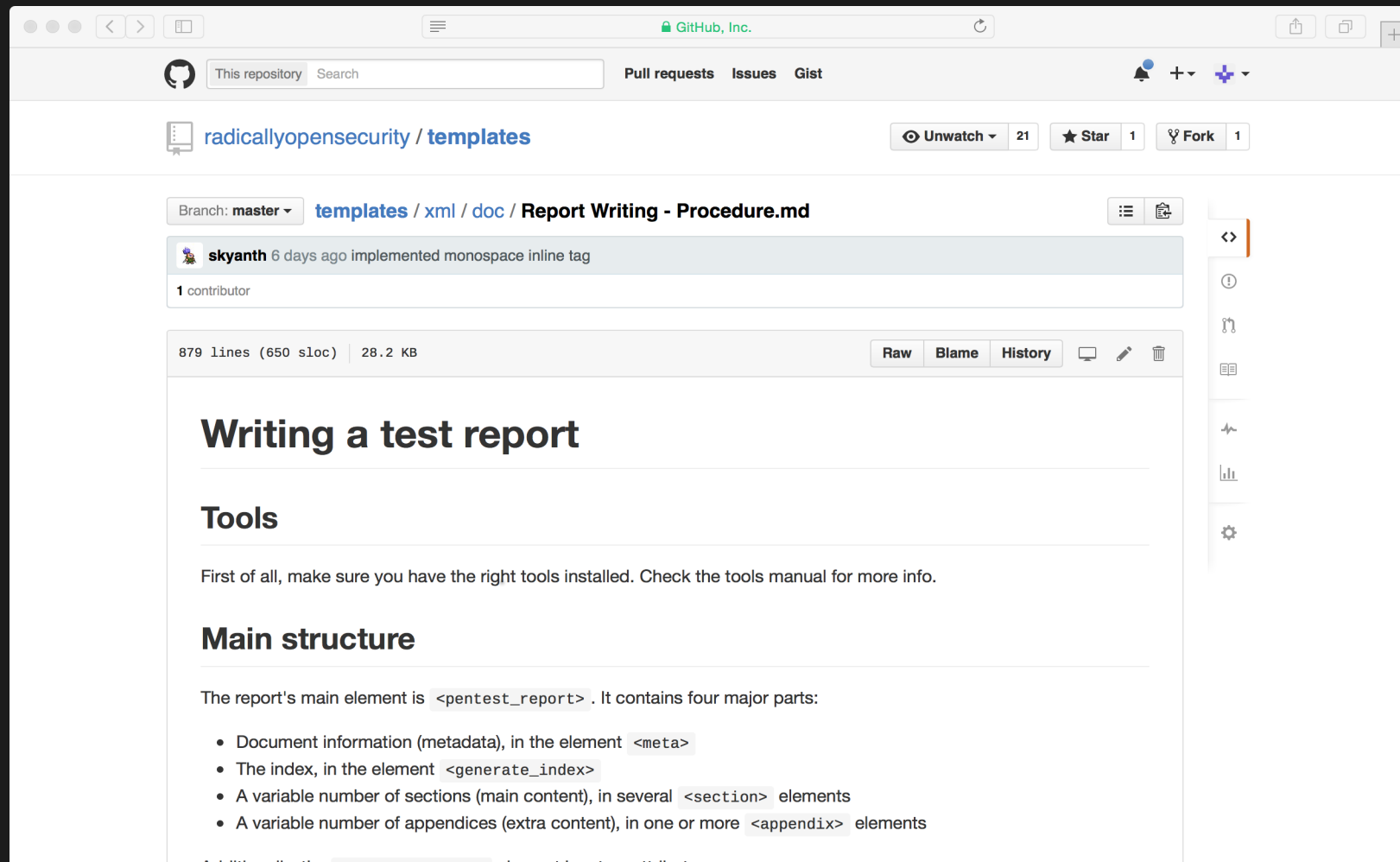
melanie 11:15
@Ms.Abstract_007: try it again! 😊

Message

bold _italics_ ~strike~ `inline_code` `multi` `line` >quote



What is PenText?



The screenshot shows a GitHub repository page for 'radicallyopensecurity / templates'. The file 'Report Writing - Procedure.md' is displayed, showing its main structure and content. The file is 879 lines (650 sloc) and 28.2 KB. It was last updated 6 days ago by user 'skyanth'. The content includes sections for 'Writing a test report', 'Tools', and 'Main structure'. The 'Main structure' section describes the report's main element, `<pentest_report>`, and lists its four major parts: document information (metadata), the index, a variable number of sections, and a variable number of appendices.

Branch: master templates / xml / doc / Report Writing - Procedure.md

skyanth 6 days ago implemented monospace inline tag

1 contributor

879 lines (650 sloc) | 28.2 KB

Raw Blame History

Writing a test report

Tools

First of all, make sure you have the right tools installed. Check the tools manual for more info.

Main structure

The report's main element is `<pentest_report>`. It contains four major parts:

- Document information (metadata), in the element `<meta>`
- The index, in the element `<generate_index>`
- A variable number of sections (main content), in several `<section>` elements
- A variable number of appendices (extra content), in one or more `<appendix>` elements

Additionally, the `<pentest_report>` element has two attributes:



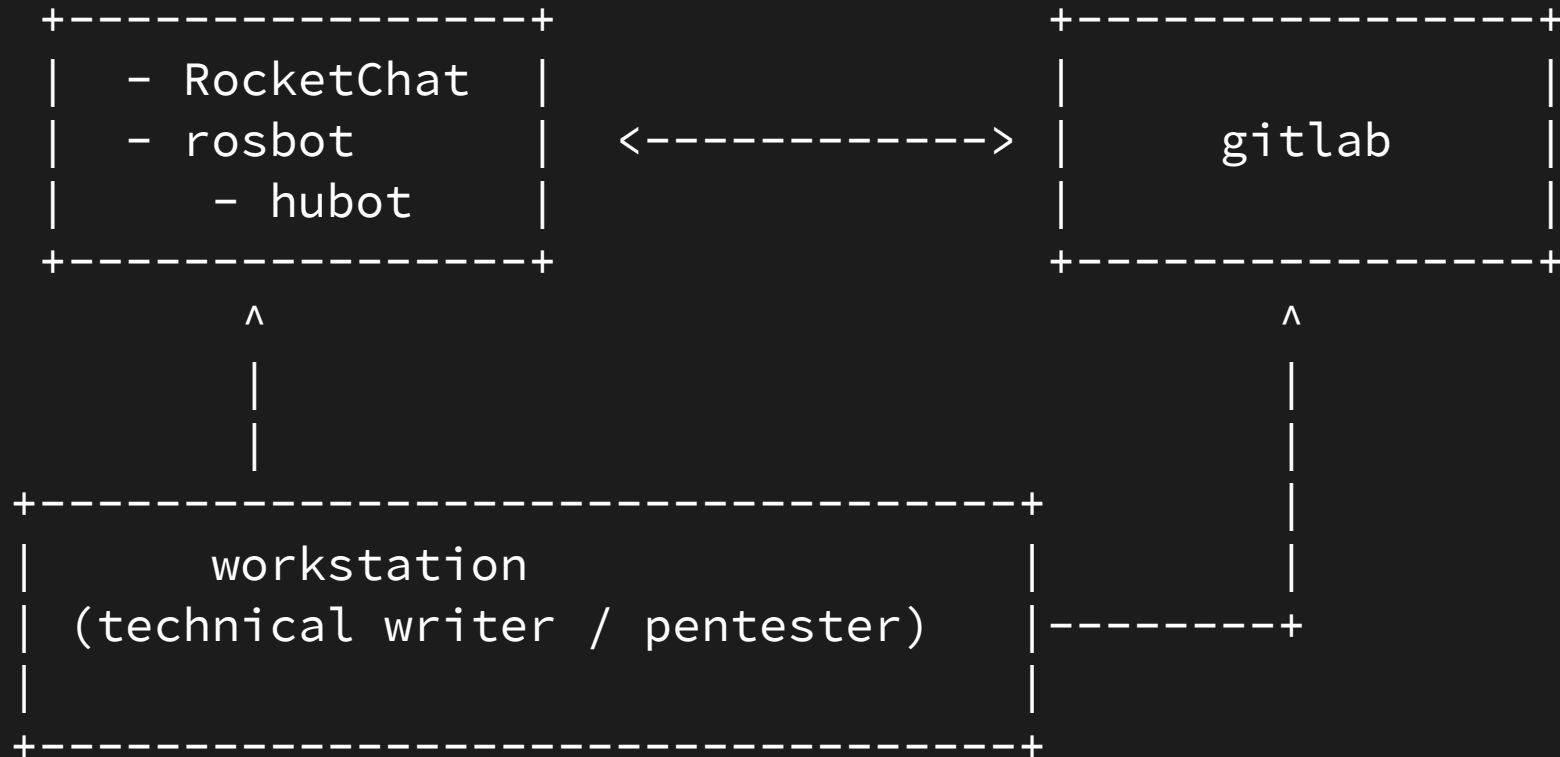
Demo Prologue: Getting Started

1. A clone of the PenText repository
2. PenText toolchain (Saxon, Apache FOP)
3. Content (plaintext)



August 18, 2016

Demo Setup



Content - Pentest

- * Main source: source/report.xml
- * Can re-use details from quote (e.g. client_info.xml)
- * Plus findings, non-findings and scan outputs (all XML)

```
<finding id="finding" threatLevel="Low" type="Information  
Leak">  
  <title>Title</title>  
  <description>Description.</description>  
  <technicaldescription>Techical  
description.</technicaldescription>  
  <impact>Consequences of exploitation</impact>  
  <recommendation>Steps to resolve the issue</recommendation>  
</finding>
```



More Demo Time!

The screenshot shows the Rocket.Chat web interface in a Mozilla Firefox browser window. The address bar displays `https://rocketchat.local/channel/chatops`. The interface is split into three main sections:

- Left Sidebar:** Contains a user profile for 'peter', a 'CHANNELS' list with '# chatops' selected, and 'DIRECT MESSAGES'.
- Main Chat Area:** Shows a conversation in the '# chatops' channel. It starts with a 'Start of conversation' header and a date separator for 'July 29, 2016'. Messages include:
 - A message from 'peter' (Admin, Owner) at 11:28 PM: 'rosbot startquote mypentest'.
 - A message from 'rosbot' at 11:28 PM: '[+] new channel created - Added peter to the new room off-mypentest startquote v0.6 - Humbly setting up your quote framework... [+] successfully created gitlab project off-mypentest with id 16 [+] listo!'.
 - A message from 'peter' (Admin, Owner) at 11:32 PM: 'rosbot startpentest mypentest'.
 - A message from 'rosbot' at 11:32 PM: '[+] new channel created - Added peter to the new room pen-mypentest startpentest v0.7 - Ready for some ACTION? [+] successfully created gitlab project pen-mypentest with id 17 [+] listo!'.
- Bottom:** A message input field with a rich text editor toolbar containing options for bold, italic, strikethrough, inline code, multi-line, and KaTeX.



RADICALLY OPEN SECURITY

August 18, 2016

What Else Can We Integrate?

- Scanning + Exploitation:
 - Nmap, w3af, sqlmap, hydra, etc..
- Reconnaissance:
 - Whois, Google, PassiveScan, etc..
- Cryptography
 - Hash cracking, etc..
- Other:
 - Email/SMS integration, spearphishing, CVEsearch



Red/Blue Pentesting

Radically Open Security Chat

https://chat.radicallyopensource.com/group/pen-██████████

Most Visited Getting Started ROS SugarCRM ROS Mediawiki ROS IRC Archive ROS Redmine

melanie

MORE UNREADS ↑

- @ Thice
- @ adam
- @ bob.goudriaan
- @ boi
- @ daan
- @ debbie
- @ dylan
- @ ecole
- @ ellie
- @ else.lenselink
- @ erik
- @ evan_camomile
- @ frouke
- @ ganesh
- @ giray
- @ ianc

MORE UNREADS ↓

pen-██████████

a point for Blue for finding missing input validation
(and adding that yesterday after 5, so I almost missed that)

melanie 17:02
goodjob Blue

rosbot 17:02
incremented Blue (24 pt)

<http://teachinginkoreanuniversity.com/wp-content/uploads/2015/10/awesome-interview-questions-for-candidates-600x320.jpg>

melanie 17:02
^
I like this one! 😊

muse 17:03
and finally, both teams get an additional point. not for findings

Message

bold _italics_ ~strike~ `inline_code` >quote

3438



Now an OWASP Project!

<PEN *Text* **>**

<https://pentext.org>

<https://github.com/radicallyopensecurity/pentext>



RADICALLY OPEN SECURITY

August 18, 2016

Questions?



RADICALLY
OPEN
SECURITY