

Lazily Finding Holes Without Breaking The Law

Nick von Dadelszen – Technical Director

Event – OWASP Day 2015

Date – 27th February 2015

Company Overview



The Catalyst



The Catalyst

- When scoping jobs I use browse through Burp to get a site map and to log my activities
- Potential client rings up asking for quote
- I browse site to assess functionality
- After scoped, I casually check Burp and notice a passive scan alert
- Turns out the site has some creds in JavaScript which turns into a fairly big deal
- Have to responsibly disclosure a serious security issue during the sales process

The Bright Idea



The Bright Idea

- What if I could be looking for vulnerabilities all the time when I browse the internet
- What if I could find them without even trying
- I could pump all of my browsing traffic through a proxy that searches for vulnerabilities passively
- Must not break the law and perform active attacks

The Law



The NZ Law



The Law

Crimes Act 1961.pdf - SumatraPDF

File View Go To Zoom Favorites Settings Help

Page: 187 / 279 Find: 252

Reprinted as at
19 August 2013

Crimes Act 1961

Part 10 s 255

252 Accessing computer system without authorisation

(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

The Implementation



The Implementation



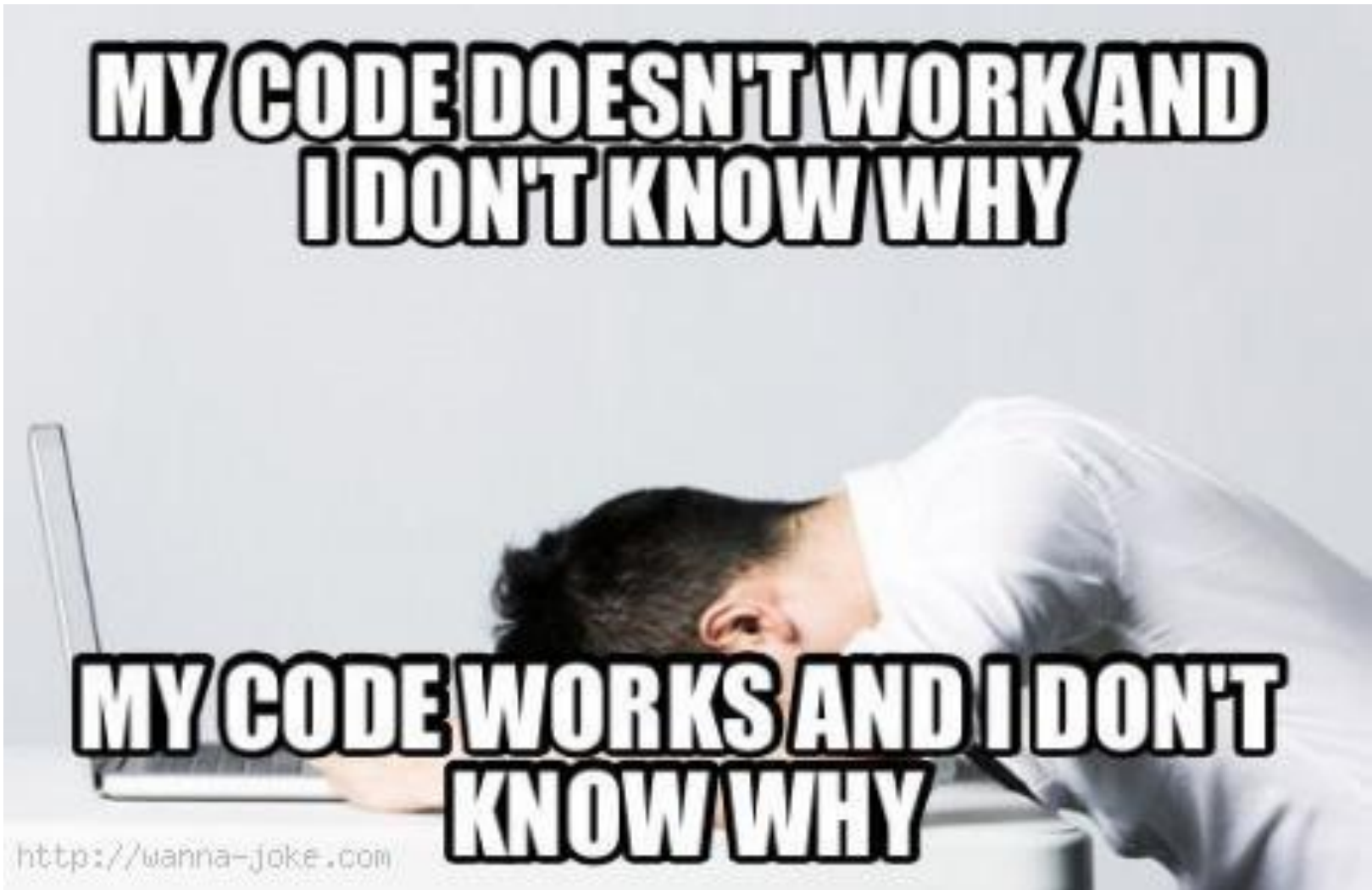
The Implementation

- I am lazy
- Burp suite already has a passive scan engine so lets just use that
- Want to run it in headless mode on a remote server so I can use it wherever I am without having to load Burp etc
- Should log all passive scan results to console and a file
- Should capture full packets for any high severity issue identified

The Implementation

```
root@ip-172-31-42-193: ~
20150224-2122-119,Medium,HTML5 cross-origin resource sharing,http://ping.crowdscience.com:80/max_log.js
20150224-2122-120,Medium,HTML5 cross-origin resource sharing,http://www.reddit.com:80/api/info.json
20150224-2122-121,Medium,HTML5 cross-origin resource sharing,http://widget.perfectmarket.com:80/nbcnews/get/
20150224-2122-122,Medium,HTML5 cross-origin resource sharing,http://maxcdn.bootstrapcdn.com:80/font-awesome/4.3.0/fonts/fontawesome-webfont.woff
20150224-2122-123,Medium,HTML5 cross-origin resource sharing,http://canwestglobal.112.2o7.net:80/b/ss/canwestglobal,cannfinancialpost/1/H.25.4/s79740713997690
20150224-2122-124,Medium,HTML5 cross-origin resource sharing,http://cdnapi.kaltura.com:80/html5/html5lib/v2.18.2.2/mwEmbedFrame.php
20150224-2122-125,Medium,HTML5 cross-origin resource sharing,http://ip-api.com:80/json
20150224-2122-126,Medium,HTML5 cross-origin resource sharing,http://cs.specificclick.net:80/sync/
20150224-2122-127,Medium,HTML5 cross-origin resource sharing,http://beta.images.theglobeandmail.com:80/media/www/fonts/pratt-web-heavy-webfont.woff
20150224-2122-128,Medium,HTML5 cross-origin resource sharing,http://beta.images.theglobeandmail.com:80/media/www/fonts/pratt-webfont.woff
20150224-2122-129,Medium,HTML5 cross-origin resource sharing,http://rtd.tubemogul.com:80/upi/pid/NC4WTmcy
20150224-2122-130,Medium,HTML5 cross-origin resource sharing,http://media1.s-nbcnews.com:80/i/uxassets/nbcnews/2015-02-19-180838/build_ux/fonts/ProximaNova-Reg-webfont.woff
20150224-2122-131,Medium,HTML5 cross-origin resource sharing,http://media1.s-nbcnews.com:80/i/uxassets/nbcnews/2015-02-19-180838/build_ux/fonts/ProximaNova-Sbold-webfont.woff
20150224-2122-132,Medium,HTML5 cross-origin resource sharing,http://media1.s-nbcnews.com:80/i/uxassets/nbcnews/2015-02-19-180838/build_ux/fonts/icon.woff
20150224-2122-133,Medium,HTML5 cross-origin resource sharing,http://omniture.theglobeandmail.com:80/b/ss/bellgmpnewprod/1/H.24.4/s78751281988061
20150224-2122-134,Medium,HTML5 cross-origin resource sharing,http://a.disquscdn.com:80/next/assets/font/1cons.dba73c09e46bcbe2e83906259dcdf4f2.woff
20150224-2122-135,Low,Cookie without HttpOnly flag set,http://trc.taboola.com:80/nbcnews/trc/3/json
20150224-2122-136,High,HTML5 cross-origin resource sharing,http://trc.taboola.com:80/nbcnews/trc/3/json
20150224-2122-137,Low,Source code disclosure,http://a.disquscdn.com:80/next/discovery.c23f8ac34bc2524beaa53b95dedc73c5.js
20150224-2122-138,Medium,HTML5 cross-origin resource sharing,http://media2.s-nbcnews.com:80/i/MSNBC/Components/Video/_Player/configurations/No%20Modify/HTML5/font/CC-Close.gif
20150224-2122-139,Medium,HTML5 cross-origin resource sharing,http://media2.s-nbcnews.com:80/j/MSNBC/Components/Video/_NEW/x_lon_school_141217.nbcnews-video-reststate-800.jpg
20150224-2122-140,Medium,HTML5 cross-origin resource sharing,http://media3.s-nbcnews.com:80/i/uxassets/nbcnews/2014-09-18-230313/build_ux/fonts/ProximaNova-Reg-webfont.woff
20150224-2122-141,Medium,HTML5 cross-origin resource sharing,http://media3.s-nbcnews.com:80/i/uxassets/nbcnews/2014-09-18-230313/build_ux/fonts/ProximaNova-Sbold-webfont.woff
20150224-2122-142,High,HTML5 cross-origin resource sharing,http://trc.taboola.com:80/nbcnews/log/3/visible
20150224-2122-143,High,HTML5 cross-origin resource sharing,http://trc.taboola.com:80/nbcnews/log/2/debug
20150224-2122-144,High,Flash cross-domain policy,http://static.chartbeat.com:80/crossdomain.xml
20150224-2122-145,Medium,HTML5 cross-origin resource sharing,http://www.nbcnews.com:80/id/52493270
20150224-2122-146,Medium,HTML5 cross-origin resource sharing,http://media1.s-nbcnews.com:80/i/uxassets/nbcnews/2015-02-19-180838/build_ux/img/loading-spinner-yellow-lg.png
20150224-2122-147,High,HTML5 cross-origin resource sharing,http://trc.taboola.com:80/nbcnews/log/3/available
20150224-2122-148,Low,Source code disclosure,http://cdnapi.kaltura.com:80/html5/html5lib/v2.18.2.2/load.php
20150224-2122-149,Medium,HTML5 cross-origin resource sharing,http://images.taboola.com:80/taboola/image/fetch/f_jpg%2Cq_80%2Ch_150%2Cw_300%2Cc_fill%2Cg_faces%2Ce_sharpen/http%3A//cdn.taboolasyndication.com/1ibtrc/static/thumbnails/bac44f7e9bda5ff7860f30cecad1d9ee.jpg
20150224-2122-150,Medium,HTML5 cross-origin resource sharing,http://images.taboola.com:80/taboola/image/fetch/f_jpg%2Cq_80%2Ch_150%2Cw_300%2Cc_fill%2Cg_faces%2Ce_sharpen/http%3A//cdn.taboolasyndication.com/1ibtrc/static/thumbnails/f36205fd2facd564c7cfe8bac92ac735.jpg
20150224-2122-151,Medium,HTML5 cross-origin resource sharing,http://images.taboola.com:80/taboola/image/fetch/f_jpg%2Cq_80%2Ch_150%2Cw_300%2Cc_fill%2Cg_faces%2Ce_sharpen/http%3A//media2.s-nbcnews.com/i/MSNBC/Components/Video/_NEW/News%2520Channel/nc_mssing_mssionry_150224.jpg
20150224-2122-152,Medium,HTML5 cross-origin resource sharing,http://images.taboola.com:80/taboola/image/fetch/f_jpg%2Cq_80%2Ch_150%2Cw_300%2Cc_fill%2Cg_faces%2Ce_sharpen/http%3A//media1.s-nbcnews.com/i/MSNBC/Components/Video/_NEW/2015-02-14T01-38-12-92--1280x720.jpg
20150224-2122-153,High,Flash cross-domain policy,http://adm.fwmrm.net:80/crossdomain.xml
20150224-2122-154,High,Flash cross-domain policy,http://link.theplatform.com:80/crossdomain.xml
20150224-2122-155,Medium,HTML5 cross-origin resource sharing,http://rtd.tubemogul.com:80/upi/pid/YT1ZQXKA
20150224-2122-156,Medium,HTML5 cross-origin resource sharing,http://px.dynamicsield.com:80/imp
20150224-2122-157,Low,Cookie without HttpOnly flag set,http://snas.nbcuni.com:80/snas/api/getRemoteDomainCookies
20150224-2122-158,Medium,HTML5 cross-origin resource sharing,http://link.theplatform.com:80/s/2E2eJc/9mLJyPbisyaq
20150224-2122-159,Medium,HTML5 cross-origin resource sharing,http://link.theplatform.com:80/s/ngc/9mLJyPbisyaq
20150224-2122-160,Medium,HTML5 cross-origin resource sharing,http://media2.s-nbcnews.com:80/crossdomain.xml
20150224-2122-161,Low,Flash cross-domain policy,http://media2.s-nbcnews.com:80/crossdomain.xml
20150224-2122-162,Medium,HTML5 cross-origin resource sharing,http://media2.s-nbcnews.com:80/i/MSNBC/Components/Video/_Player/configurations/thePlatform/skins/helveticaNeue.swf
20150224-2122-163,Medium,HTML5 cross-origin resource sharing,http://cdnapi.kaltura.com:80/html5/html5lib/v2.18.2.2/skins/kdark/fonts/icomoon.woff
20150224-2122-164,Medium,HTML5 cross-origin resource sharing,http://cdnbakmi.kaltura.com:80/p/1698541/sp/169854100/thumbnail/entry_id/0_wo5shdz8/version/100000/acv/142/width/300/height/168
20150224-2122-165,Medium,Session token in URL,http://stats.kaltura.com:80/api_v3/index.php
20150224-2122-166,Medium,HTML5 cross-origin resource sharing,http://stats.kaltura.com:80/api_v3/index.php
20150224-2122-167,Medium,HTML5 cross-origin resource sharing,http://msnbc.112.2o7.net:80/b/ss/msnbcnbcnewscomprod/1/H.26.1-D52A/s73702814919202
20150224-2122-168,High,Flash cross-domain policy,http://ping.chartbeat.net:80/crossdomain.xml
20150224-2122-169,Medium,HTML5 cross-origin resource sharing,http://cdnbakmi.kaltura.com:80/p/1698541/sp/169854100/thumbnail/entry_id/0_wo5shdz8/version/100000/acv/142/width/100/vid_slices/100
20150224-2122-170,Medium,HTML5 cross-origin resource sharing,http://msnbc.112.2o7.net:80/b/ss/msnbcnbcnewscomprod/1/H.26.1-D52A/s77686800913776
20150224-2122-171,High,Cleartext submission of password,http://publisher.cpmgo.com:80/login.php
20150224-2122-172,Low,Password field with autocomplete enabled,http://publisher.cpmgo.com:80/login.php
20150224-2122-173,Low,Cookie without HttpOnly flag set,http://www.likesasap.com:80/
20150224-2122-174,Low,Cookie without HttpOnly flag set,http://cpmgo.com:80/
root@ip-172-31-42-193: ~# Burp/20150224-2122#
```

The Problems



The Problems

- Adding Burp extensions in headless mode is hard
 - Had to call on the skills of Feabell to solve this one
 - Used a bootstrap extender to load a saved config then load our main extension
- Java is crap and keeps crashing
 - Needed to restart every 1000 issues

Adding Custom Scan Items

PYTHON

THIS IS PLAGIARISM.
YOU CAN'T JUST "IMPORT ESSAY."



JAVA

I'M TWO PAGES IN AND I STILL
HAVE NO IDEA WHAT YOU'RE SAYING.



Adding Custom Scan Items

- Its easy to add custom scans to Burp
- It is easier to add custom scan items to Burp using Python than Java
- Have I ever told anyone that I have Java?
- Have to work out how to load Python extensions in headless mode

Adding Custom Scan Items

```
def doPassiveScan(self, baseRequestResponse):
    #print "Starting doPassiveScan..."
    analyzedResponse = self.helpers.analyzeResponse(baseRequestResponse.getResponse()) # R
    analyzedRequest = self.helpers.analyzeRequest(baseRequestResponse)

    #print 'test'
    url = analyzedRequest.getUrl()
    params = analyzedRequest.getParameters()

    issues = list()

    # url checks
    #print url.getPath()

    # Padding Oracle
    if 'WebResource.axd' in url.getPath() or 'ScriptResource.axd' in url.getPath():
        if PaddingOracleCheck(params):
            print "Found Padding Oracle issue"
            issues.append(PaddingOracleIssue(baseRequestResponse.getHttpService(),
                                             analyzedRequest.getUrl()))

    #DependencyHandler
    if 'DependencyHandler.axd' in url.getPath():
        if DependencyHandlerCheck(params):
            print "Found DependencyHandler issue"
            issues.append(DependencyHandlerIssue(baseRequestResponse.getHttpService(),
                                                  analyzedRequest.getUrl()))

    if len(issues) > 0:
        return issues
    else:
        return None
```

Padding Oracle



Padding Oracle For Dummies

- Crypto is hard!!
- Sometimes the end-user is used as a mechanism to transfer encrypted data
- This allows the end user to perform crypto attacks against the mechanism
- Padding Oracle occurs when a user can modify the encrypted text to obtain at least three different results:
 - Cipher text gets decrypted, resulting data is correct.
 - Cipher text gets decrypted, resulting data is garbled and causes some exception or error handling in the application logic.
 - Cipher text decryption fails due to padding errors.

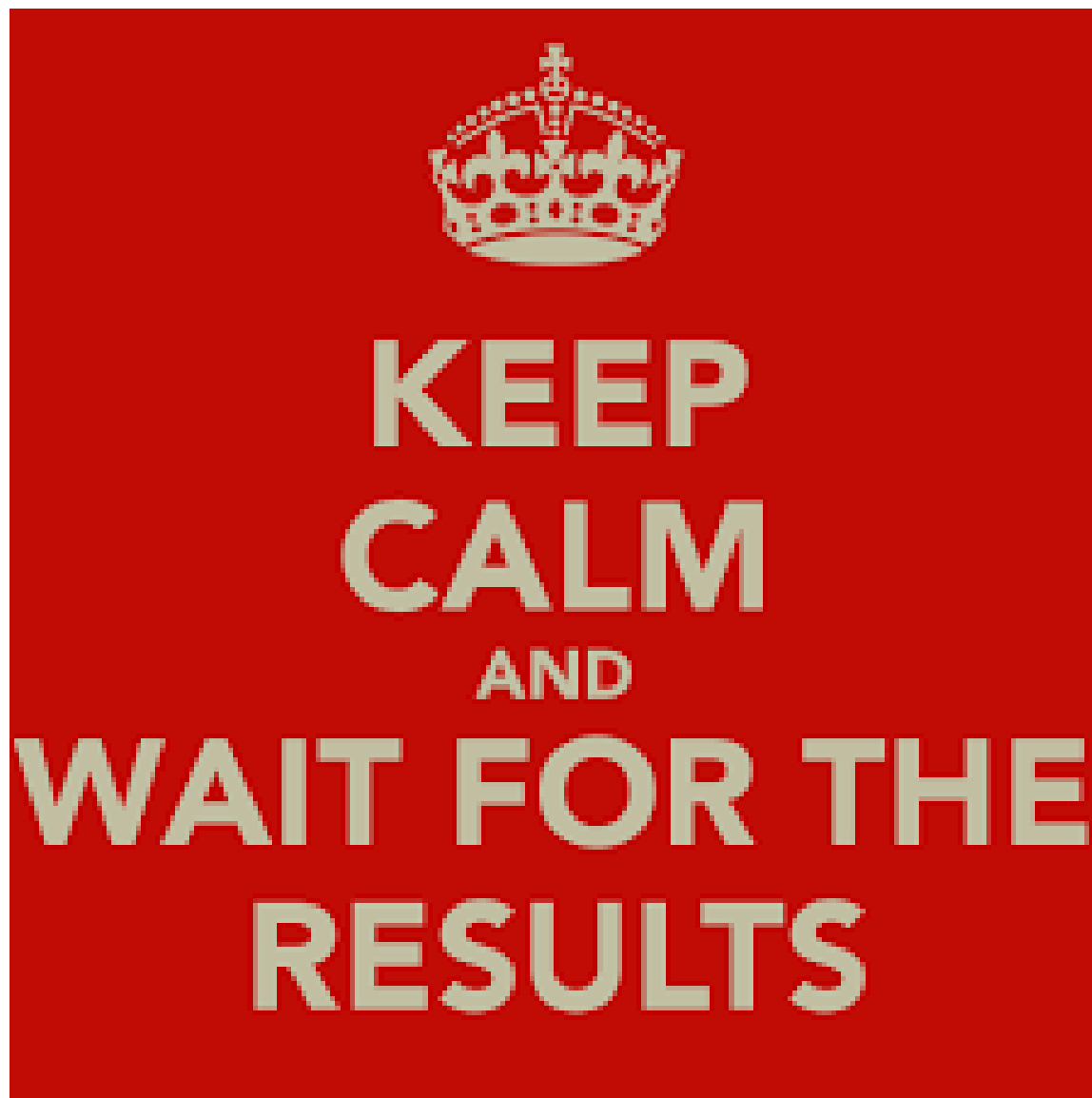
Padding Oracle For Dummies

- Padding Oracles found in multiple frameworks and applications:
 - ASP.Net
 - JavaServer Faces
 - Ruby on Rails
 - SAML
 - SSL
 - Lucky Thirteen
 - POODLE
- Can allow both decryption and encryption of messages
- The fix is to append a HMAC to the encrypted message to prevent message tampering

Testing For Padding Oracle Passively

- The ASP.Net patch (MS10-070) appended an HMAC to encrypted payloads
- This can be checked easily by reviewing requests to WebResource.axd and ScriptResource.axd
- A previously released tool (ms10-070_check.py) already does this
- I re-implemented this check as a passive vulnerability check in Burp
- Can now detect ASP.Net Padding Oracle just by browsing sites

The Results



The Results

- Ran on and off for a couple of months
 - Over 24,000 issues logged
- Majority were boring:
 - Cleartext passwords
 - Cookie issues
 - Session token in URL
- Several more interesting:
 - Padding Oracle
 - SQL statement in request parameter
- Had to responsibly disclosure one issue during the exercise

What Is With .mil?

demotivationalposterZ.com



MILITARY INTELLIGENCE

It sounds way better on paper.

What Now?



What Now?

- So, where to from here?
- Should I publish my proxy publicly?
- Set up a TOR exit node?
- Want to re-implement standalone rather than relying on Burp

Questions and Contacts



Presentation Download
[www.lateralsecurity.com/
resources.html](http://www.lateralsecurity.com/resources.html)

Lateral Security (IT) Services Limited

Wellington

38-42 Waring Taylor Street (level 7, Petherick Tower)
PO Box 8093, Wellington 6143, New Zealand
Phone: +64 4 4999 756
Email: sas@lateralsecurity.com

Auckland

187 Queen Street (level 8, Landmark House)
PO Box 7706, Auckland, New Zealand
Phone: +64 9 3770 700
Email: sas@lateralsecurity.com

Melbourne

200 Queen Street (level 13)
Melbourne, VIC 3000, Australia
Phone: +61 1300 554745
Email: sas@lateralsecurity.com