PARASOFT®

Trust and Compliance - Start with Your Software!

Stanley Eu
Regional Director
Parasoft South East Asai

Parasoft Highlights

30 Years

No Debt or VCs

Highly Focused

8000+ Customers

32 Patents

Software Quality & Testing

Embedded

IoT

Enterprise

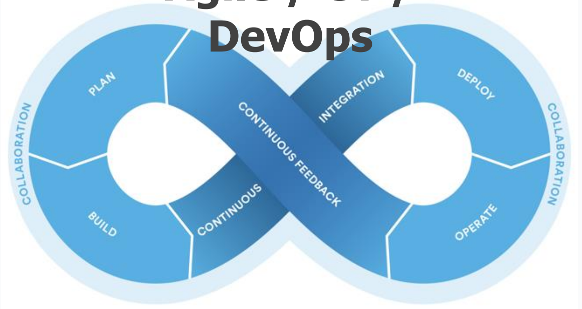
Software Development

- Analysis
- Unit Testing
- Functional
- API
- Service Virtualization
- Analytics

Compliance

- Coding Best Practices
- Security
- Safety
- Regulatory

Agile / CT / DevOps



PARASOFT

Do you focus on Security OR Quality?

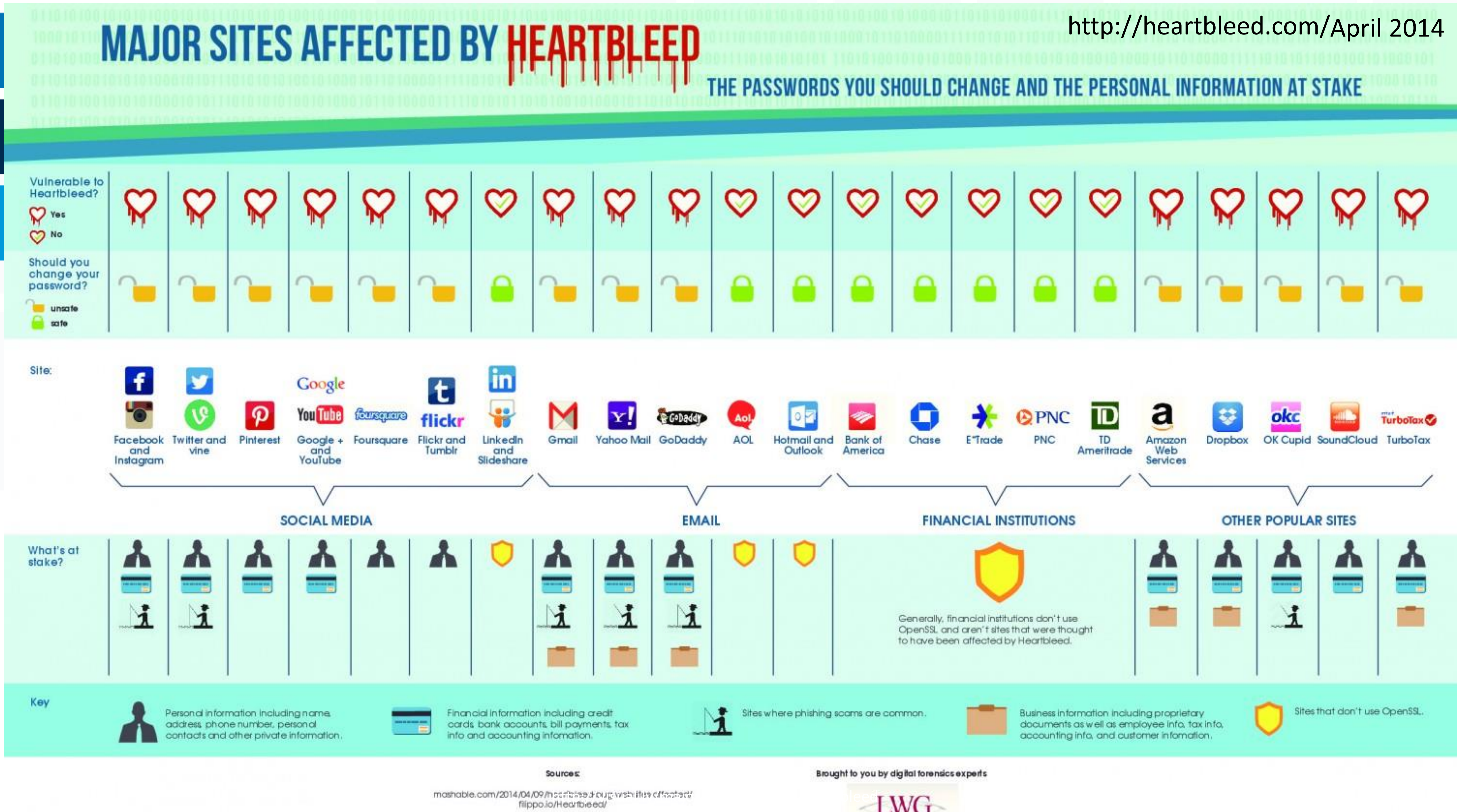
“We are left with the impression that security is somehow magically different than quality, which lowers our understanding of application security and makes us all a little less safe.”

Security has to be treated like quality, and quality has to be based On matured engineering practices…. Arthur Hicken, Parasoft

“The consensus of researchers is that at least half, and maybe as many as 70% of common software vulnerabilities are fundamental code quality problems that could be prevented by writing better software. Sloppy coding.”

- Jim Bird “Building Real Software”

http://heartbleed.com/April 2014



MAJOR SITES AFFECTED BY HEARTBLEED

THE PASSWORDS YOU SHOULD CHANGE AND THE PERSONAL INFORMATION AT STAKE

Vulnerable to Heartbleed? 💔 Yes ♡✓ No

Should you change your password? 🔓 unsafe 🔒 safe

SOCIAL MEDIA

Site:	Facebook and Instagram	Twitter and vine	Pinterest	Google + and YouTube	Foursquare	Flickr and Tumblr	LinkedIn and Slideshare
Vulnerable to Heartbleed?	💔	💔	💔	💔	💔	💔	♡✓
Should you change your password?	🔓	🔓	🔓	🔓	🔓	🔓	🔒
What's at stake?	👤 💳 🎣	👤 💳 🎣	👤 💳	👤 💳	👤	👤	🛡

EMAIL

Site:	Gmail	Yahoo Mail	GoDaddy	AOL	Hotmail and Outlook
Vulnerable to Heartbleed?	💔	💔	💔	♡✓	♡✓
Should you change your password?	🔓	🔓	🔓	🔒	🔒
What's at stake?	👤 💳 🎣 💼	👤 💳 🎣 💼	👤 💳 🎣 💼	🛡	🛡

FINANCIAL INSTITUTIONS

Site:	Bank of America	Chase	E*Trade	PNC	TD Ameritrade
Vulnerable to Heartbleed?	♡✓	♡✓	♡✓	♡✓	♡✓
Should you change your password?	🔒	🔒	🔒	🔒	🔒
What's at stake?	🛡 Generally, financial institutions don't use OpenSSL and aren't sites that were thought to have been affected by Heartbleed.				

OTHER POPULAR SITES

Site:	Amazon Web Services	Dropbox	OK Cupid	SoundCloud	TurboTax
Vulnerable to Heartbleed?	💔	💔	💔	💔	💔
Should you change your password?	🔓	🔓	🔓	🔓	🔓
What's at stake?	👤 💳 💼	👤 💳 💼	👤 💳 🎣	👤 💳	👤 💳 💼

Key

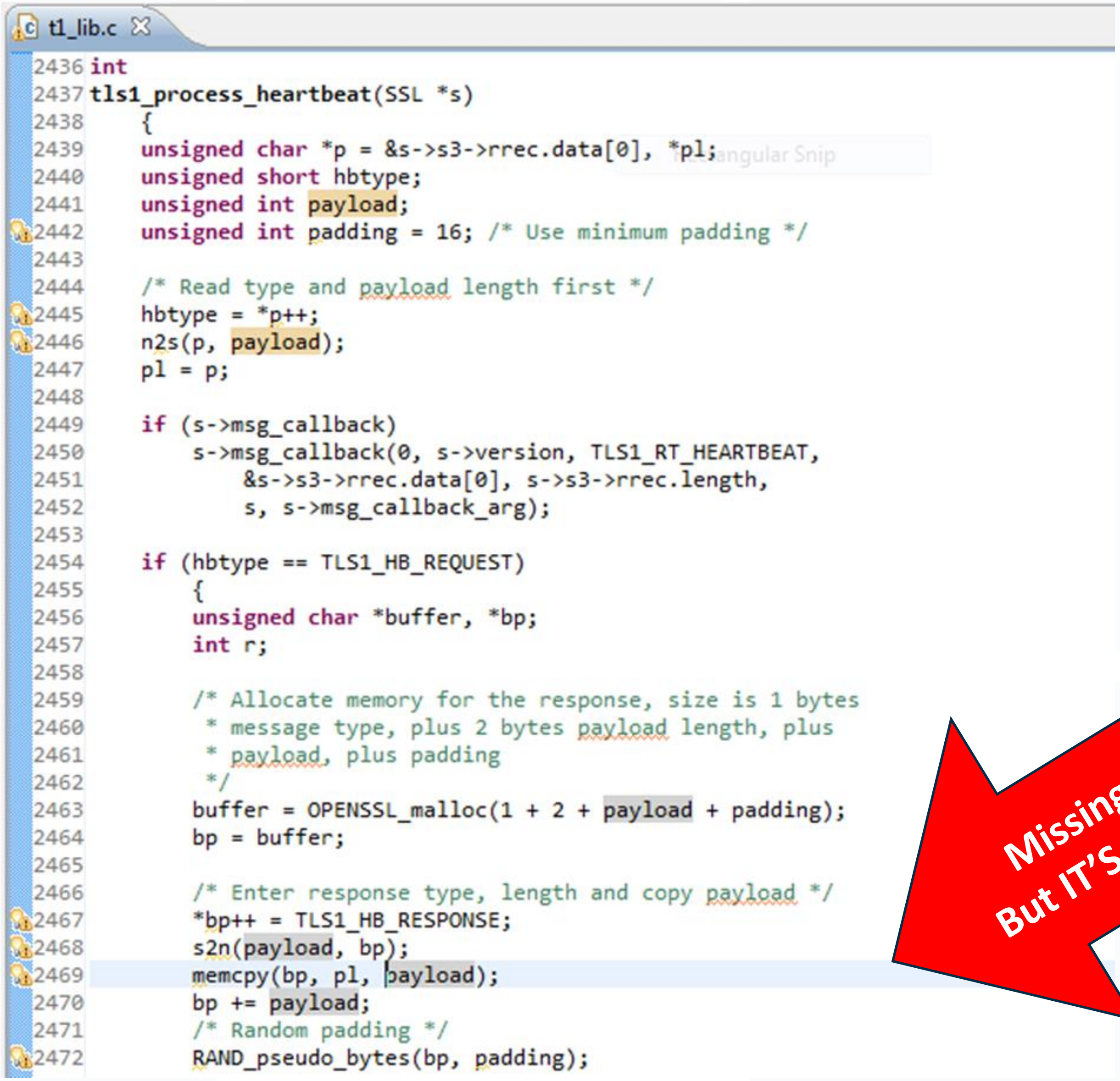
👤	Personal information including name, address, phone number, personal contacts and other private information.
💳	Financial information including credit cards, bank accounts, bill payments, tax info and accounting information.
🎣	Sites where phishing scams are common.
💼	Business information including proprietary documents as well as employee info, tax info, accounting info, and customer information.
🛡	Sites that don't use OpenSSL.

Sources:
mashable.com/2014/04/09/heartbleed-bug-websites-affected/
filippo.io/Heartbleed/

Brought to you by digital forensics experts

LWG

Just 1 Line of Code (LoC) in 2 files


t1_lib.c

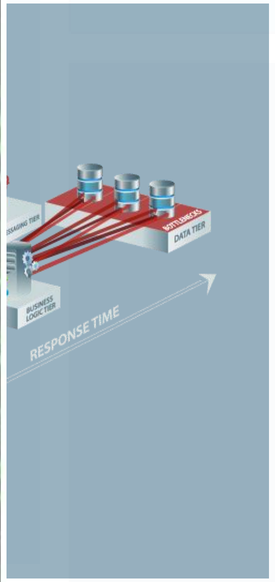
```
int
tls1_process_heartbeat(SSL *s)
    {
    unsigned char *p = &s->s3->rrec.data[0], *pl;
    unsigned short hbtype;
    unsigned int payload;
    unsigned int padding = 16; /* Use minimum padding */

    /* Read type and payload length first */
    hbtype = *p++;
    n2s(p, payload);
    pl = p;

    if (s->msg_callback)
        s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
            &s->s3->rrec.data[0], s->s3->rrec.length,
            s, s->msg_callback_arg);

    if (hbtype == TLS1_HB_REQUEST)
        {
        unsigned char *buffer, *bp;
        int r;

        /* Allocate memory for the response, size is 1 bytes
         * message type, plus 2 bytes payload length, plus
         * payload, plus padding
         */
        buffer = OPENSSL_malloc(1 + 2 + payload + padding);
        bp = buffer;

        /* Enter response type, length and copy payload */
        *bp++ = TLS1_HB_RESPONSE;
        s2n(payload, bp);
        memcpy(bp, pl, payload);
        bp += payload;
        /* Random padding */
        RAND_pseudo_bytes(bp, padding);
```

Missing Bounds Check!
But IT'S NOT EASY TO FIND!

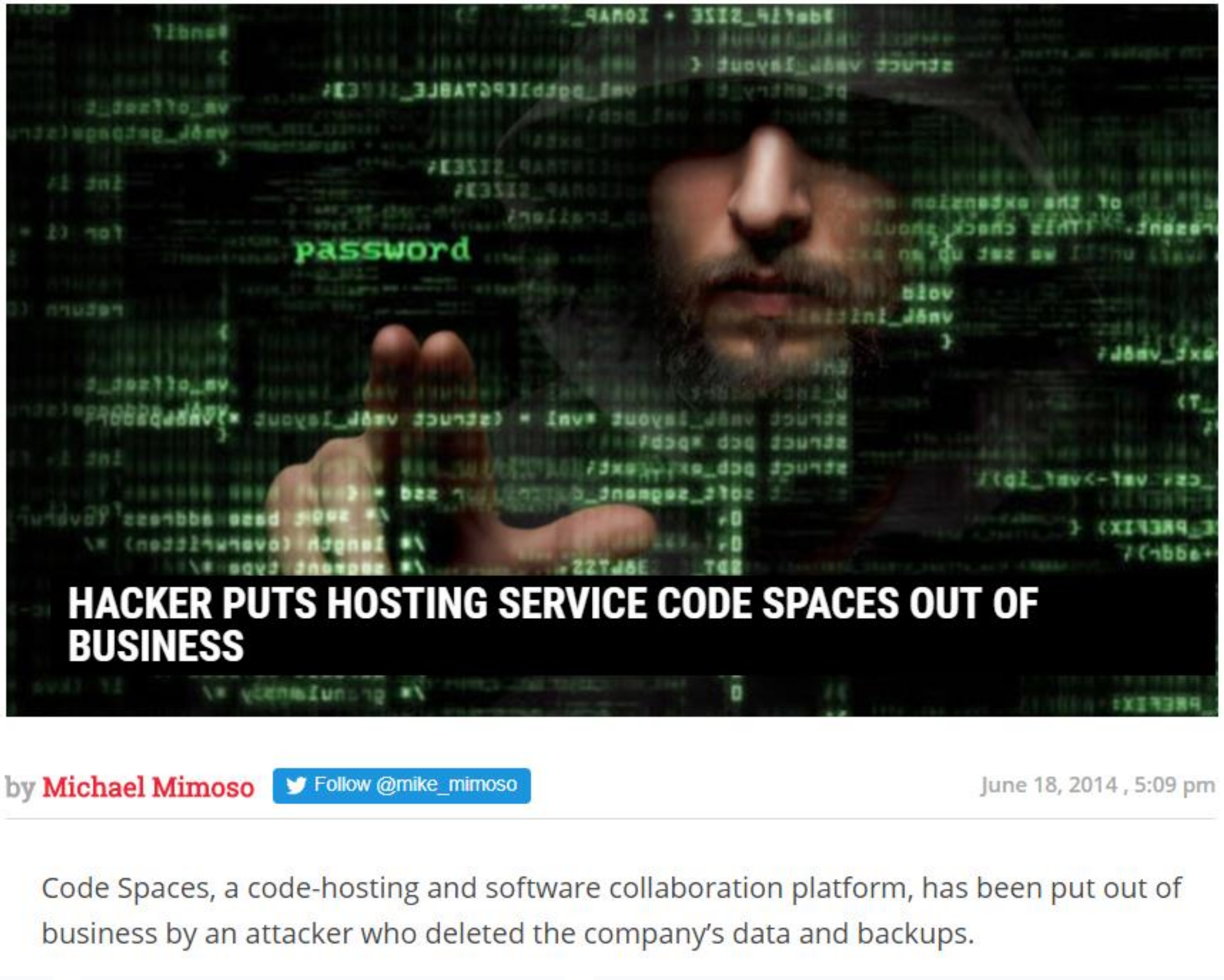
PARASOFT

Usage of Software is Everywhere

Cloud prc
accessibil
challenge
recent Co
attacked



drive
d security
ct every
anization



HACKER PUTS HOSTING SERVICE CODE SPACES OUT OF BUSINESS

by Michael Mimoso Follow @mike_mimoso June 18, 2014 , 5:09 pm

Code Spaces, a code-hosting and software collaboration platform, has been put out of business by an attacker who deleted the company's data and backups.

Danger lurks in connected devices!

IOT

Researcher Discloses 10 Zero
Wireless Routers

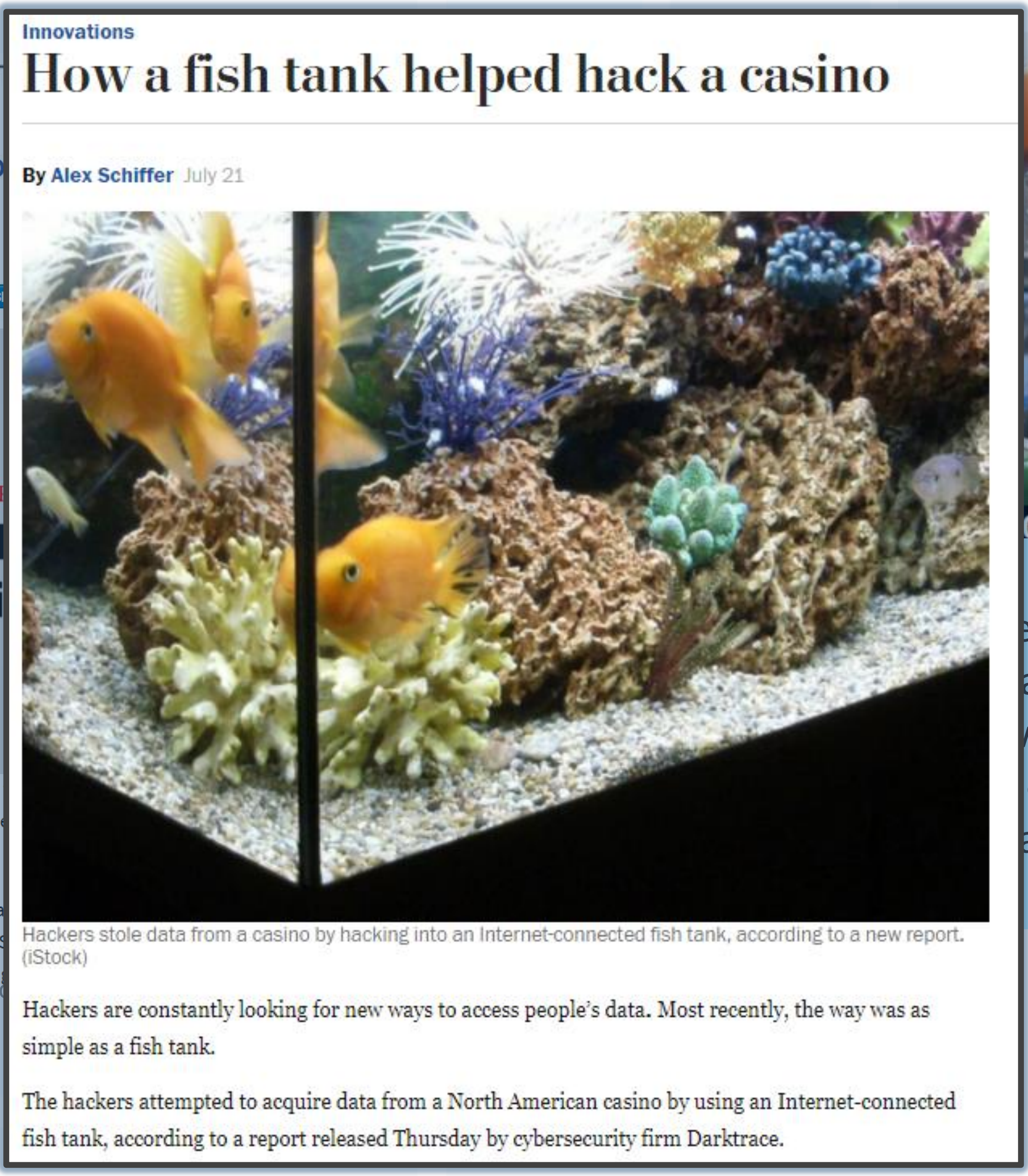
Monday, September 11, 2017 Swati Khandelwal

Tweet Share Share 19

10 ZE
D-
Wi

A security researcher has discovered not one or
routers from Taiwan-based networking equipm
attacks.

D-Link DIR 850L wireless AC1200 dual-band giga
including "several trivial" cross-site scripting (X
access, and command injection attacks resultin



Innovations

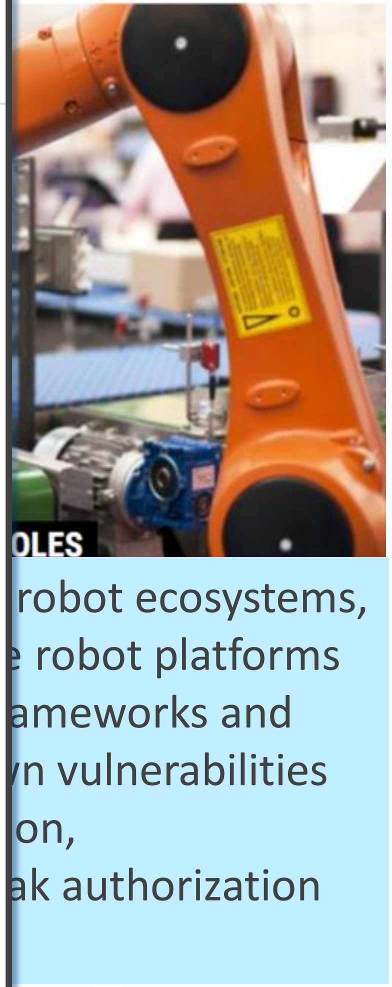
How a fish tank helped hack a casino

By Alex Schiffer July 21

Hackers stole data from a casino by hacking into an Internet-connected fish tank, according to a new report. (iStock)

Hackers are constantly looking for new ways to access people's data. Most recently, the way was as simple as a fish tank.

The hackers attempted to acquire data from a North American casino by using an Internet-connected fish tank, according to a report released Thursday by cybersecurity firm Darktrace.



OLES

robot ecosystems,
robot platforms
ameworks and
n vulnerabilities
on,
ak authorization

Strategy for Software Security starts with the Code

Test the Code, Test the Integration, Test the Function, Systems to Systems Test

- Static - Runtime Analysis
- Unit Testing
- API Testing
- Load Testing

Analysis & Testing

- Code Coverage
- Code Compliance
- Code Readiness

Reports & Dashboards

- Risk Analysis
- Change-based Testing

Intelligent Analytics

- Systems-of-Systems Testing
- Simulation

Service Virtualization

Do you focus on Security OR Quality?

"…We are left with the impression that security is somehow magically different than quality, which lowers our understanding of application security and makes us all a little less safe."

Security has to be treated like quality, and quality has to be based on matured engineering practices…. Arthur Hicken, Parasoft

SHIFT LEFT

"The consensus of researchers is that at least half, and maybe as many as 70% of common software vulnerabilities are fundamental code quality problems that could be prevented by writing better software. Sloppy coding."

- Jim Bird "Building Real Software"

PARASOFT

Strategy for CyberSecurity starts with the Code

Test the Code, Test the Integration, Test the Function, Systems to Systems Test

- Static - Runtime Analysis
- Unit Testing
- API Testing
- Load Testing

Analysis & Testing

- Code Coverage
- Code Compliance
- Code Readiness

Reports & Dashboards

- Risk Analysis
- Change-based Testing

Intelligent Analytics

- Systems-of-Systems Testing
- Simulation

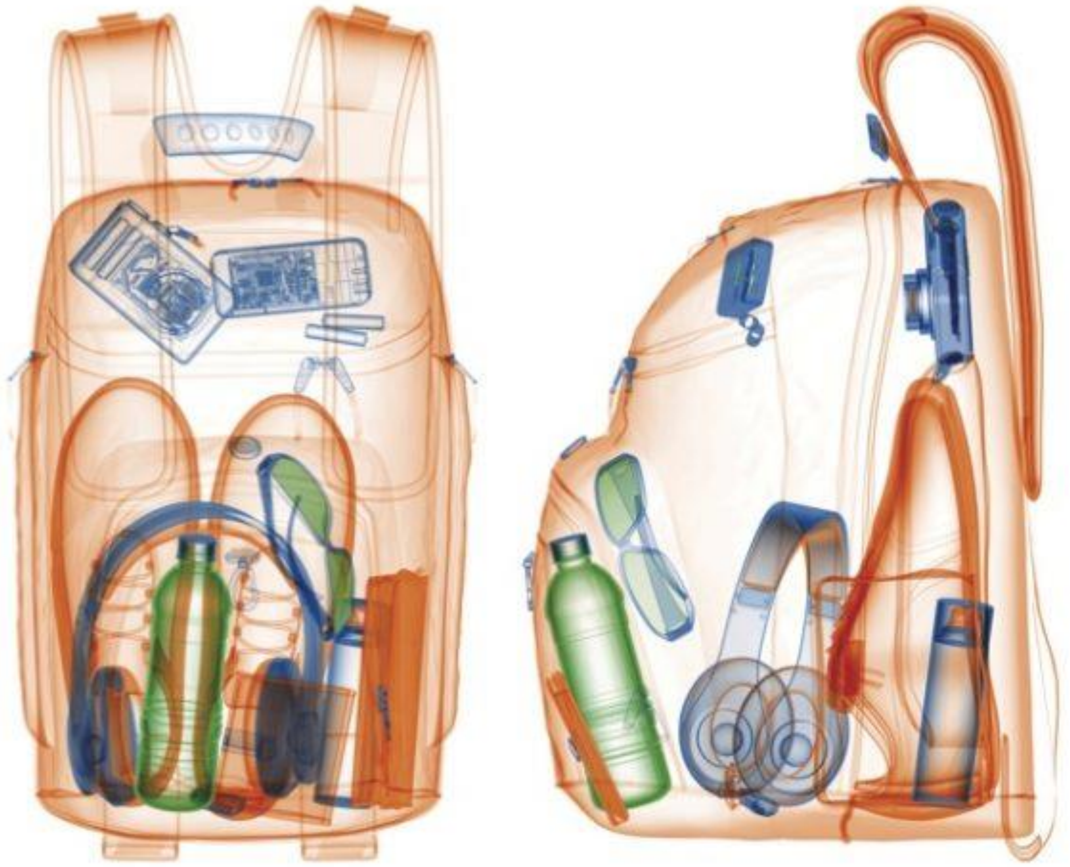
Service Virtualization

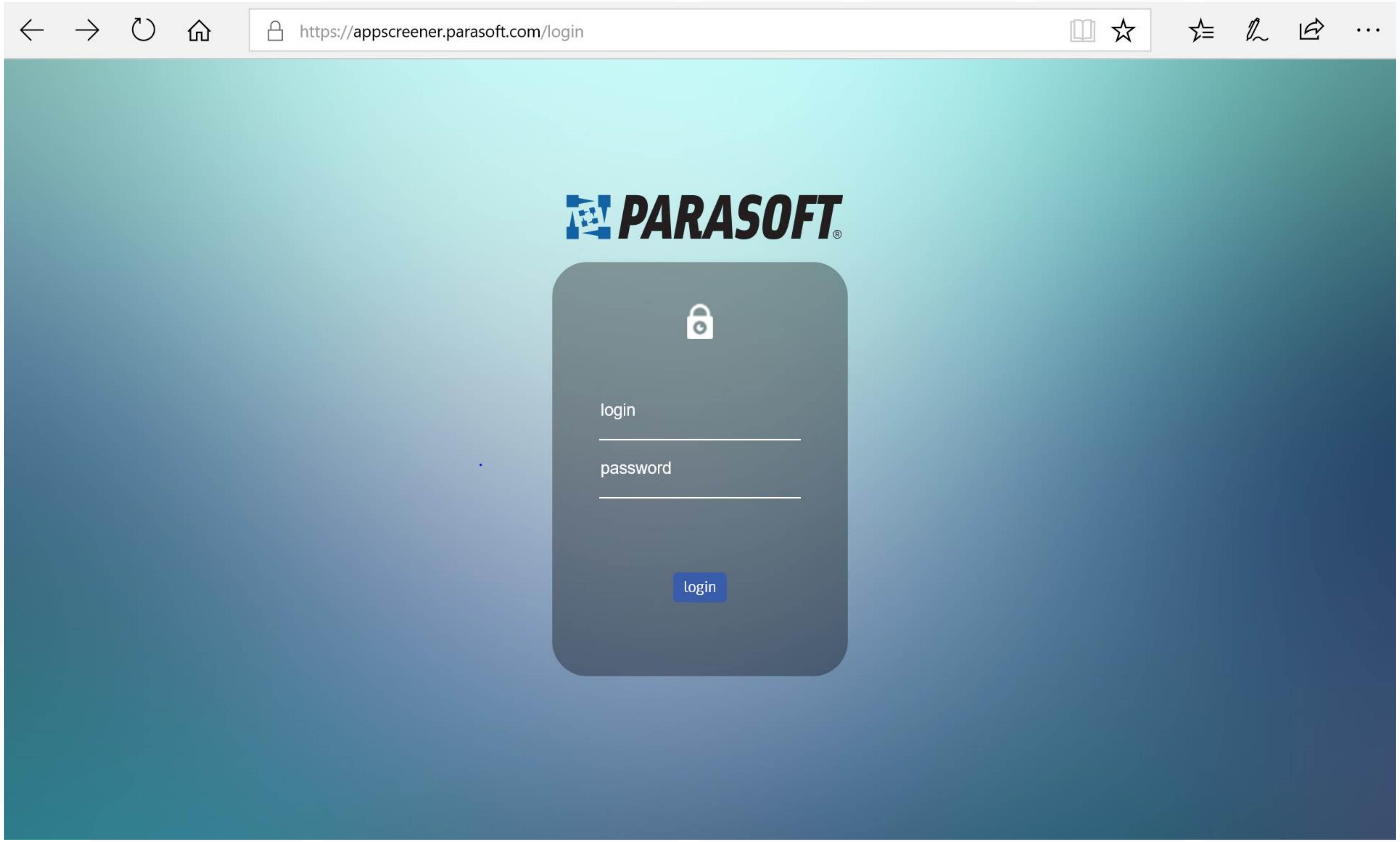
SHIFT LEFT

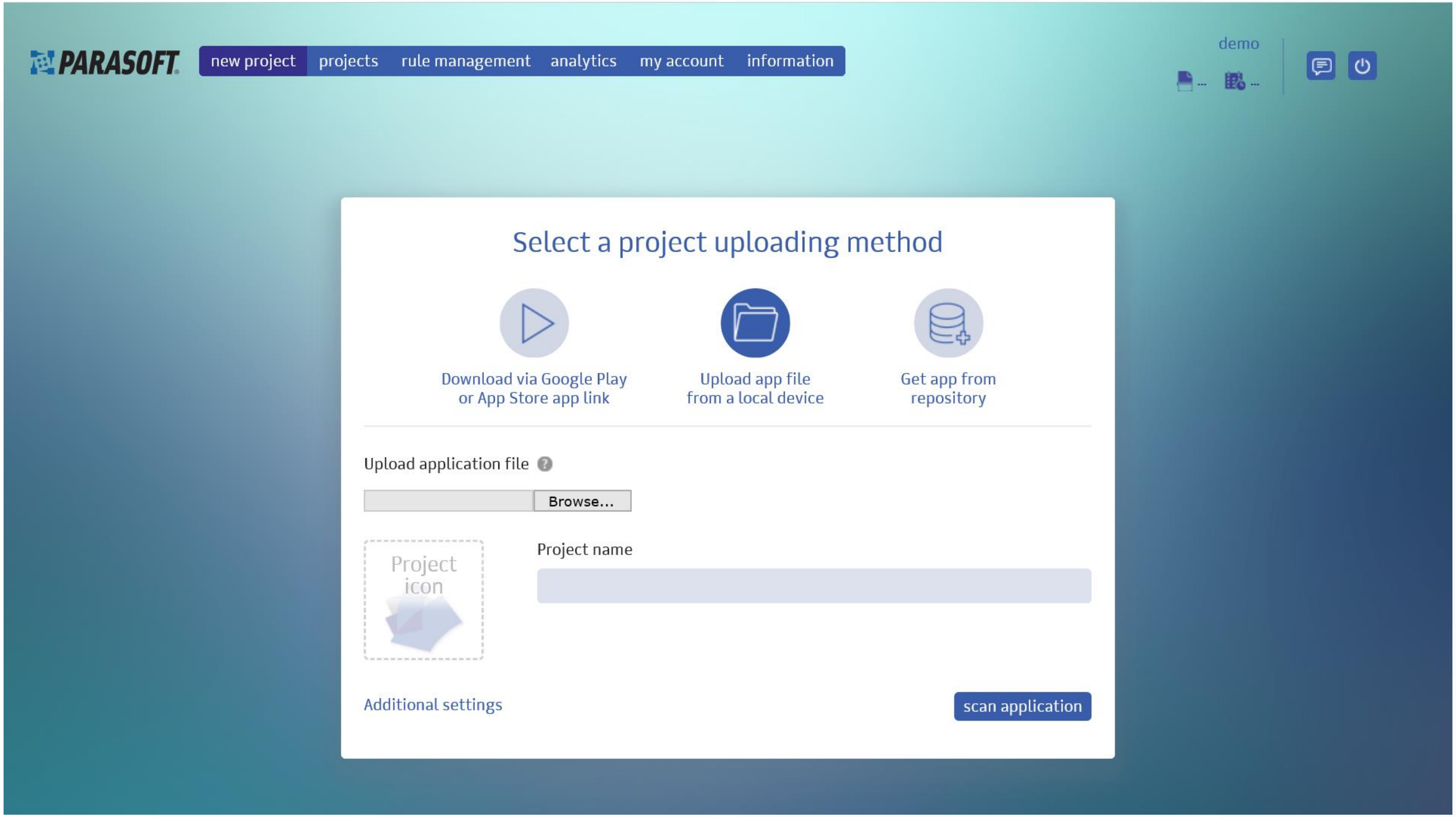
WAIT!

- We don't have the source code
- We don't own the source code
- We trust our vendors, They will fix the problem
- We cannot see mobile applications
- We only have the exe, dll, jar...binary files

You need an AppScanner!




https://appscreener.parasoft.com/login
PARASOFT
login
password
login

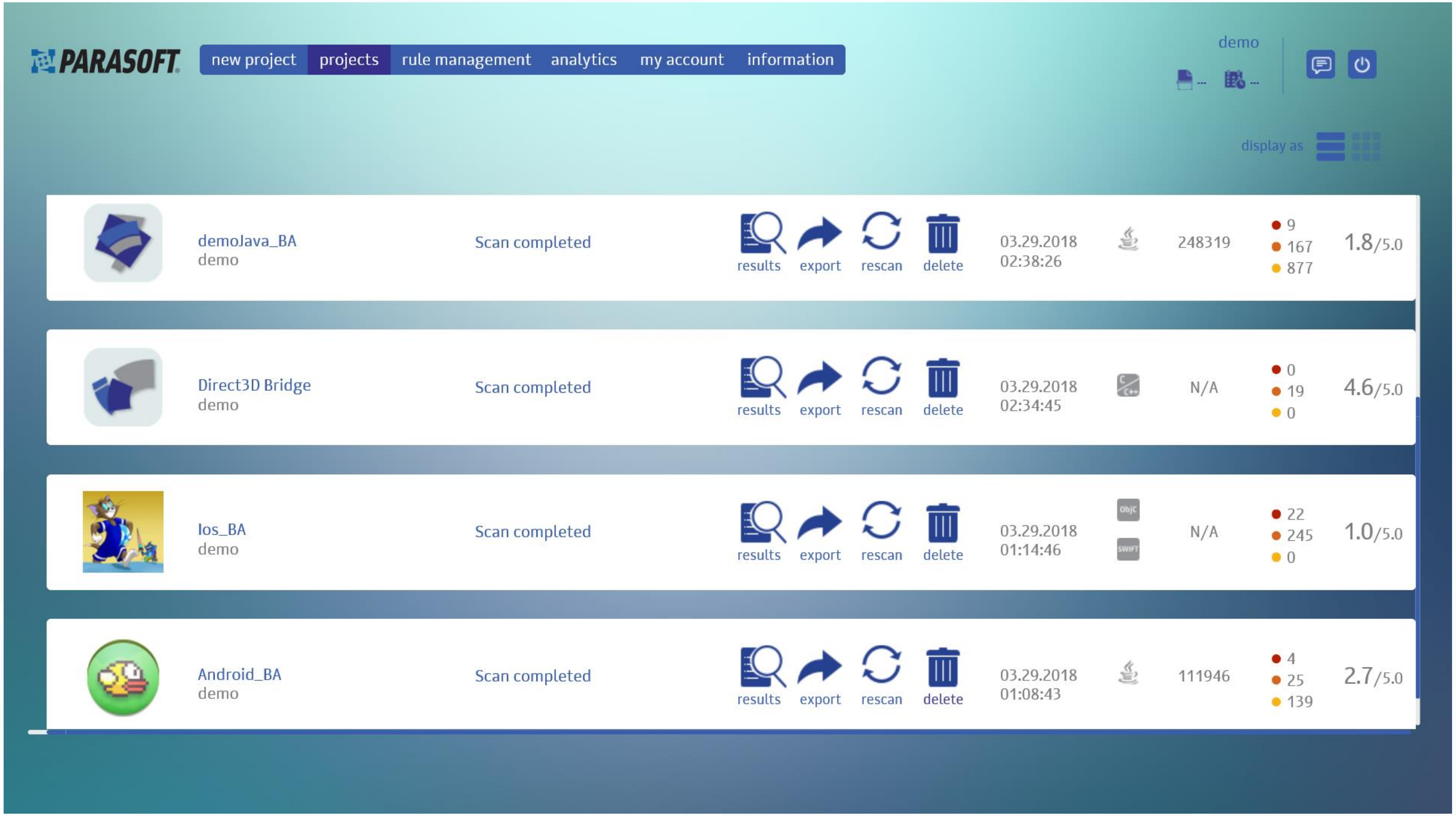


Select a project uploading method

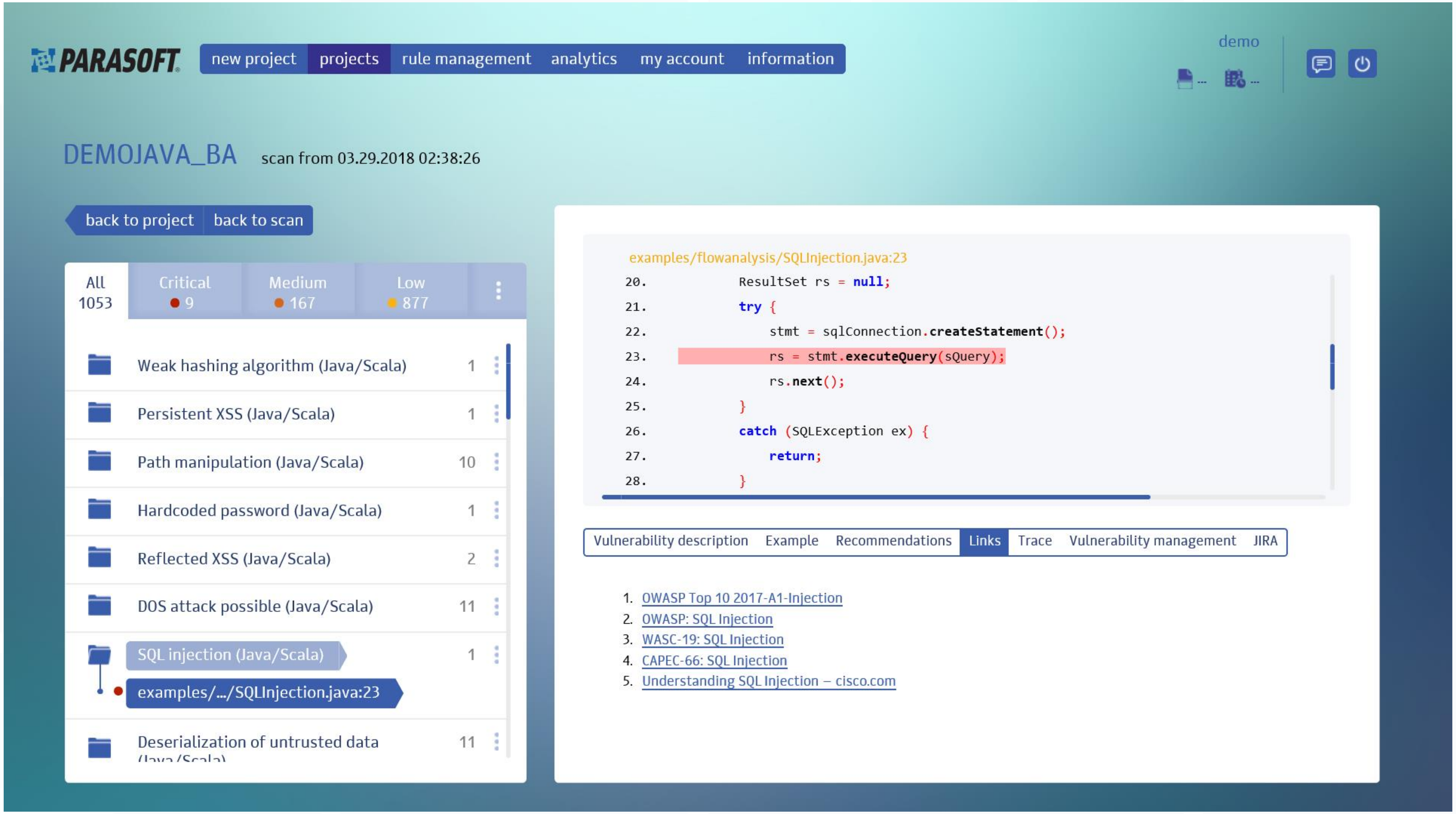
Download via Google Play or App Store app link
Upload app file from a local device
Get app from repository

Upload application file

Project name



demoJava_BA demo	Scan completed	results export rescan delete	03.29.2018 02:38:26		248319	● 9 ● 167 ● 877	1.8/5.0
Direct3D Bridge demo	Scan completed	results export rescan delete	03.29.2018 02:34:45	C C++	N/A	● 0 ● 19 ● 0	4.6/5.0
Ios_BA demo	Scan completed	results export rescan delete	03.29.2018 01:14:46	ObjC SWIFT	N/A	● 22 ● 245 ● 0	1.0/5.0
Android_BA demo	Scan completed	results export rescan delete	03.29.2018 01:08:43		111946	● 4 ● 25 ● 139	2.7/5.0



DEMOJAVA_BA scan from 03.29.2018 02:38:26

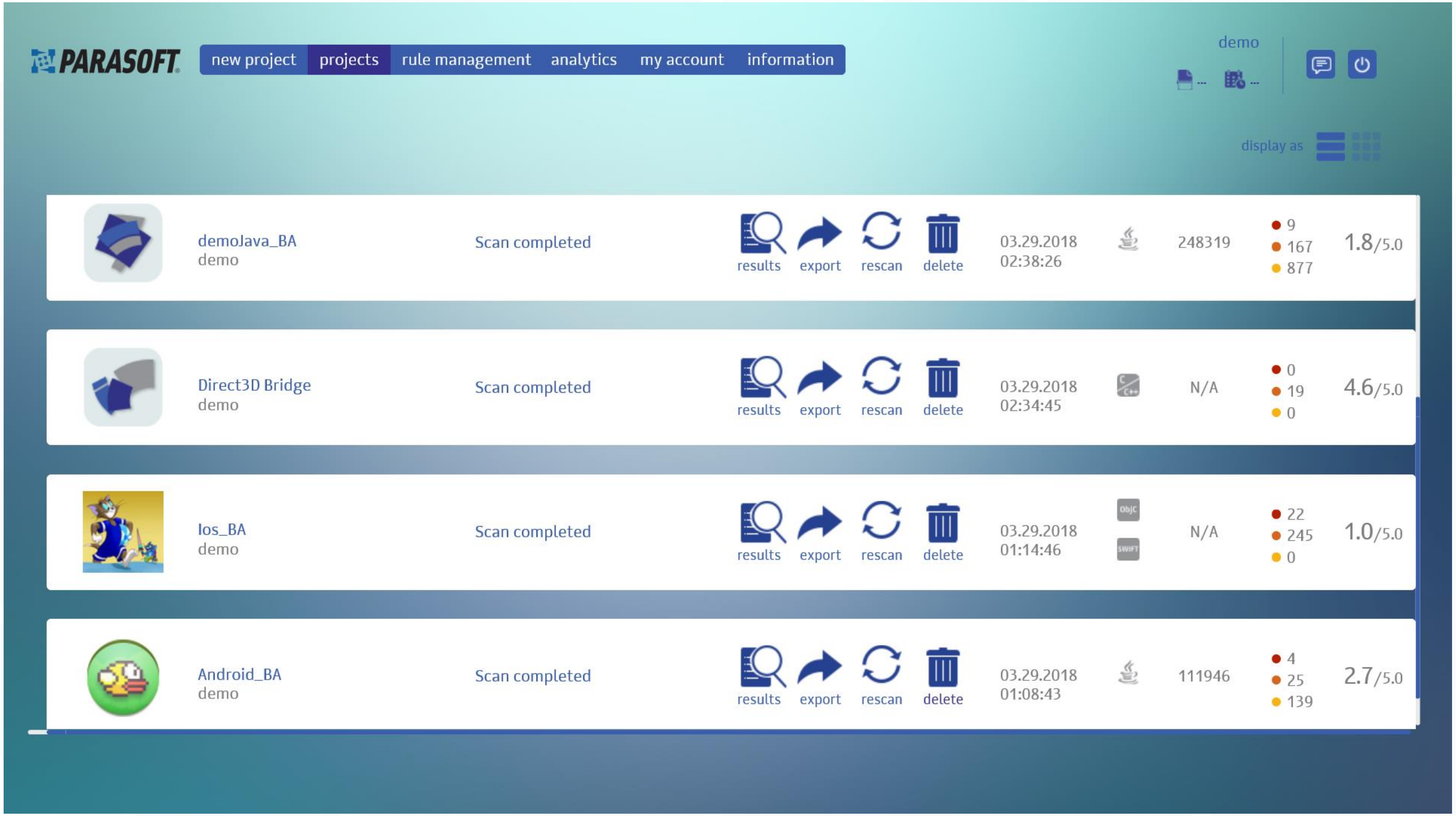
All	Critical	Medium	Low
1053	● 9	● 167	● 877

Weak hashing algorithm (Java/Scala)	1
Persistent XSS (Java/Scala)	1
Path manipulation (Java/Scala)	10
Hardcoded password (Java/Scala)	1
Reflected XSS (Java/Scala)	2
DOS attack possible (Java/Scala)	11
SQL injection (Java/Scala)	1
examples/.../SQLInjection.java:23	
Deserialization of untrusted data (Java/Scala)	11

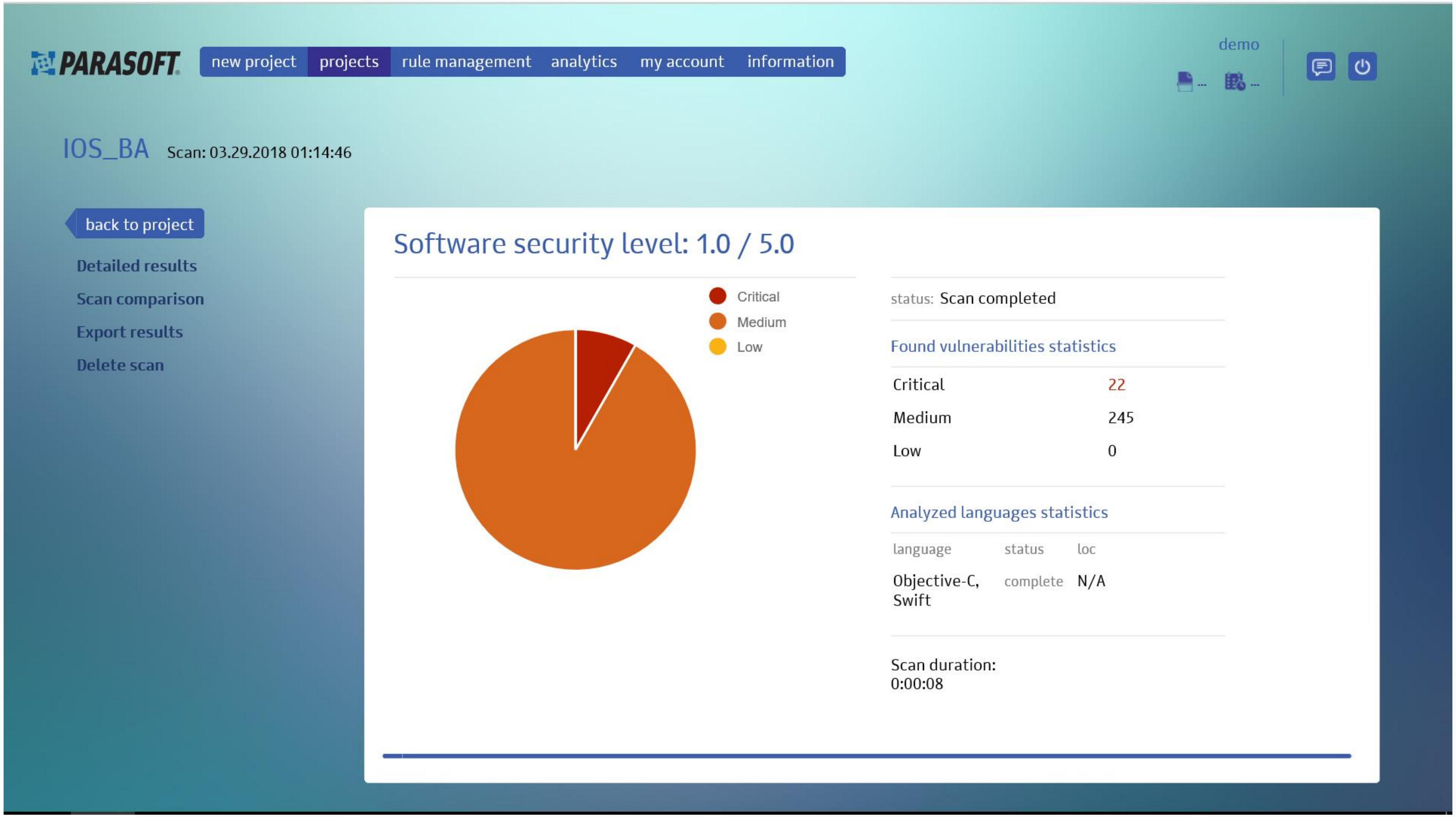
examples/flowanalysis/SQLInjection.java:23

```
        ResultSet rs = null;
        try {
            stmt = sqlConnection.createStatement();
            rs = stmt.executeQuery(sQuery);
            rs.next();
        }
        catch (SQLException ex) {
            return;
        }
```

1. OWASP Top 10 2017-A1-Injection
2. OWASP: SQL Injection
3. WASC-19: SQL Injection
4. CAPEC-66: SQL Injection
5. Understanding SQL Injection – cisco.com



demoJava_BA demo	Scan completed	results export rescan delete	03.29.2018 02:38:26		248319	● 9 ● 167 ● 877	1.8/5.0
Direct3D Bridge demo	Scan completed	results export rescan delete	03.29.2018 02:34:45	C C++	N/A	● 0 ● 19 ● 0	4.6/5.0
Ios_BA demo	Scan completed	results export rescan delete	03.29.2018 01:14:46	ObjC SWIFT	N/A	● 22 ● 245 ● 0	1.0/5.0
Android_BA demo	Scan completed	results export rescan delete	03.29.2018 01:08:43		111946	● 4 ● 25 ● 139	2.7/5.0



IOS_BA Scan: 03.29.2018 01:14:46

Software security level: 1.0 / 5.0

status: Scan completed

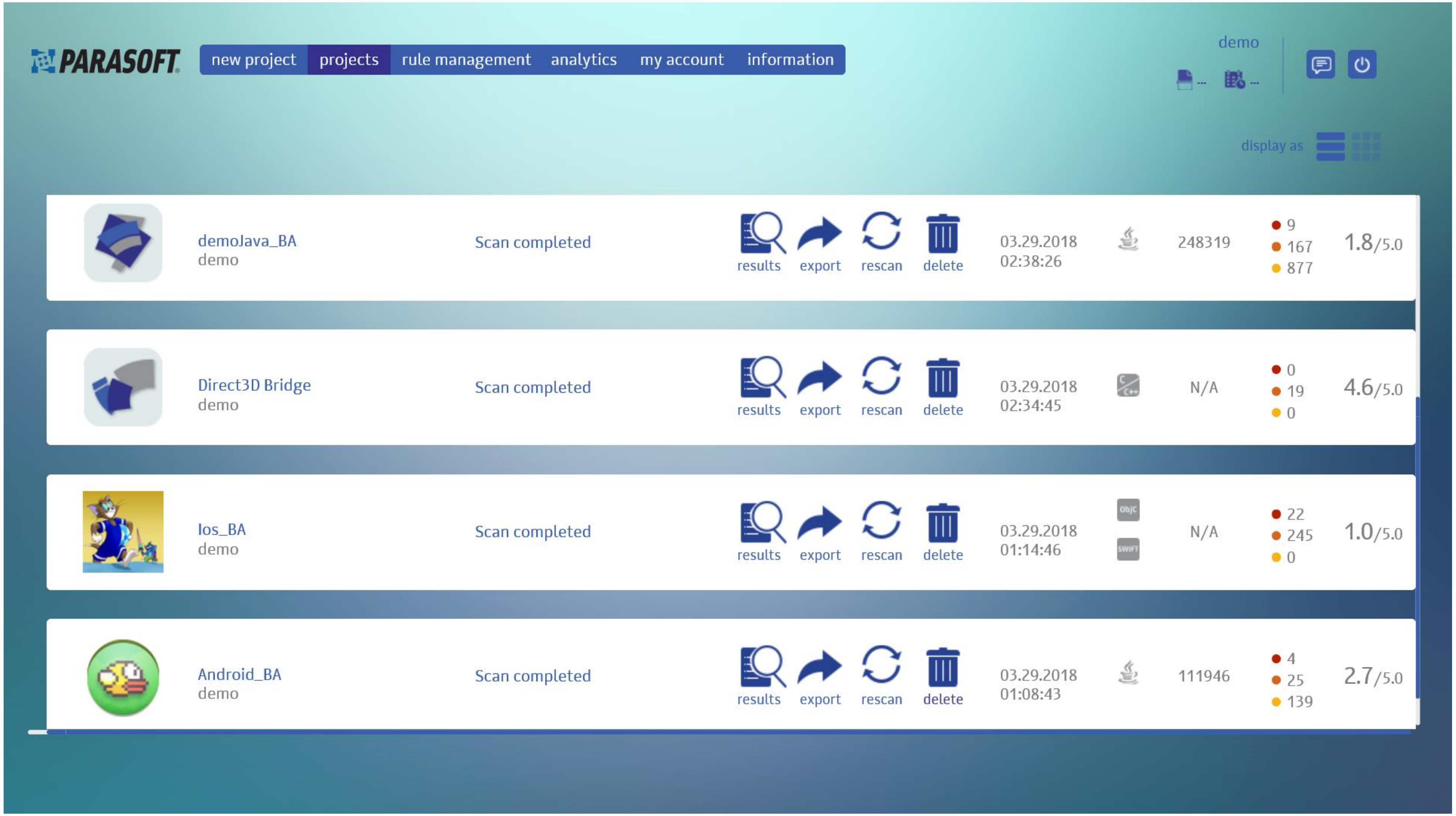
Found vulnerabilities statistics

Critical	22
Medium	245
Low	0

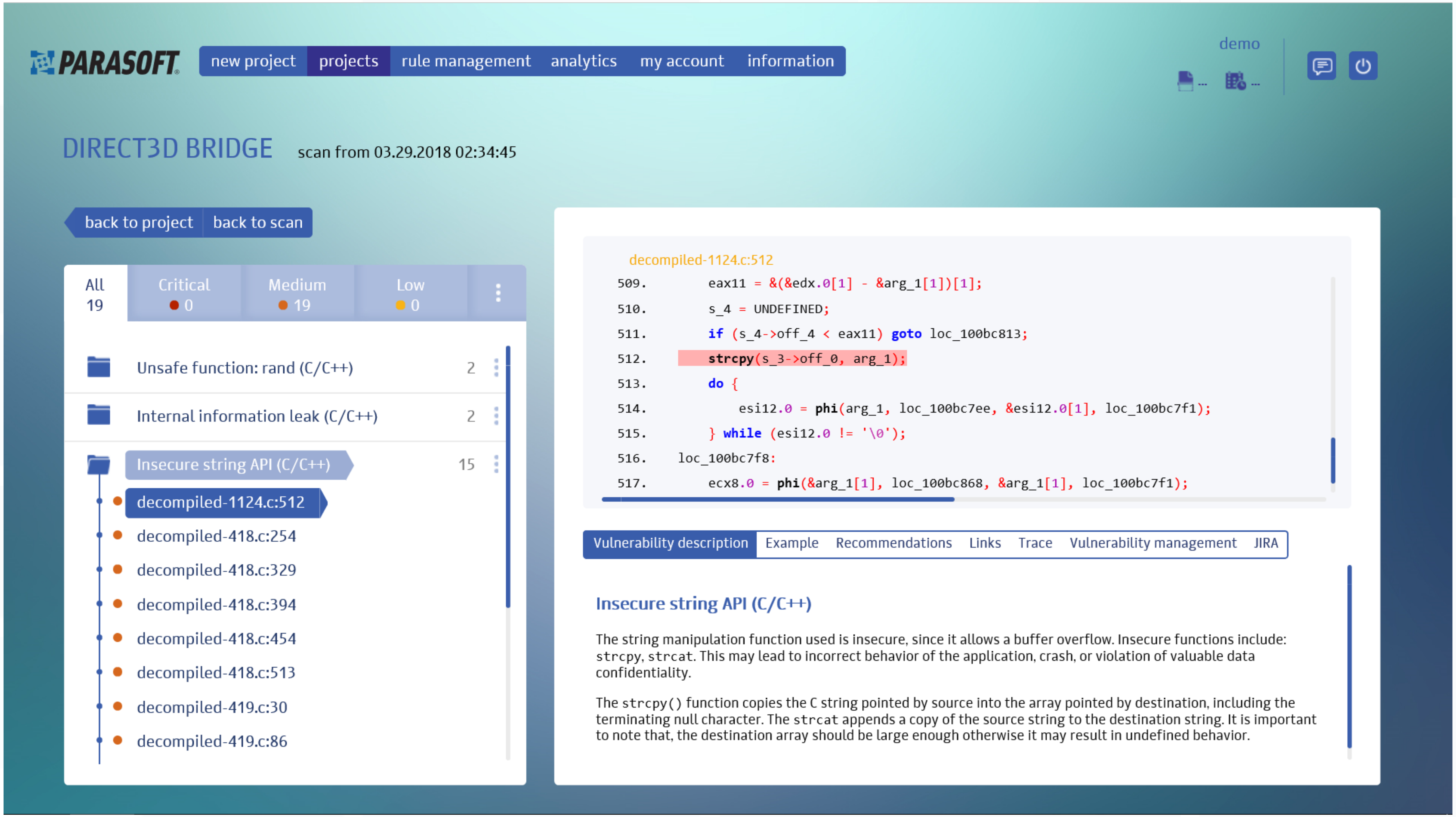
Analyzed languages statistics

language	status	loc
Objective-C, Swift	complete	N/A

Scan duration:
0:00:08



demoJava_BA demo	Scan completed	results export rescan delete	03.29.2018 02:38:26	248319	● 9 ● 167 ● 877	1.8/5.0
Direct3D Bridge demo	Scan completed	results export rescan delete	03.29.2018 02:34:45	N/A	● 0 ● 19 ● 0	4.6/5.0
Ios_BA demo	Scan completed	results export rescan delete	03.29.2018 01:14:46	N/A	● 22 ● 245 ● 0	1.0/5.0
Android_BA demo	Scan completed	results export rescan delete	03.29.2018 01:08:43	111946	● 4 ● 25 ● 139	2.7/5.0



DIRECT3D BRIDGE scan from 03.29.2018 02:34:45

All	Critical	Medium	Low
19	● 0	● 19	● 0

Unsafe function: rand (C/C++)	2
Internal information leak (C/C++)	2
Insecure string API (C/C++)	15

- decompiled-1124.c:512
- decompiled-418.c:254
- decompiled-418.c:329
- decompiled-418.c:394
- decompiled-418.c:454
- decompiled-418.c:513
- decompiled-419.c:30
- decompiled-419.c:86

decompiled-1124.c:512

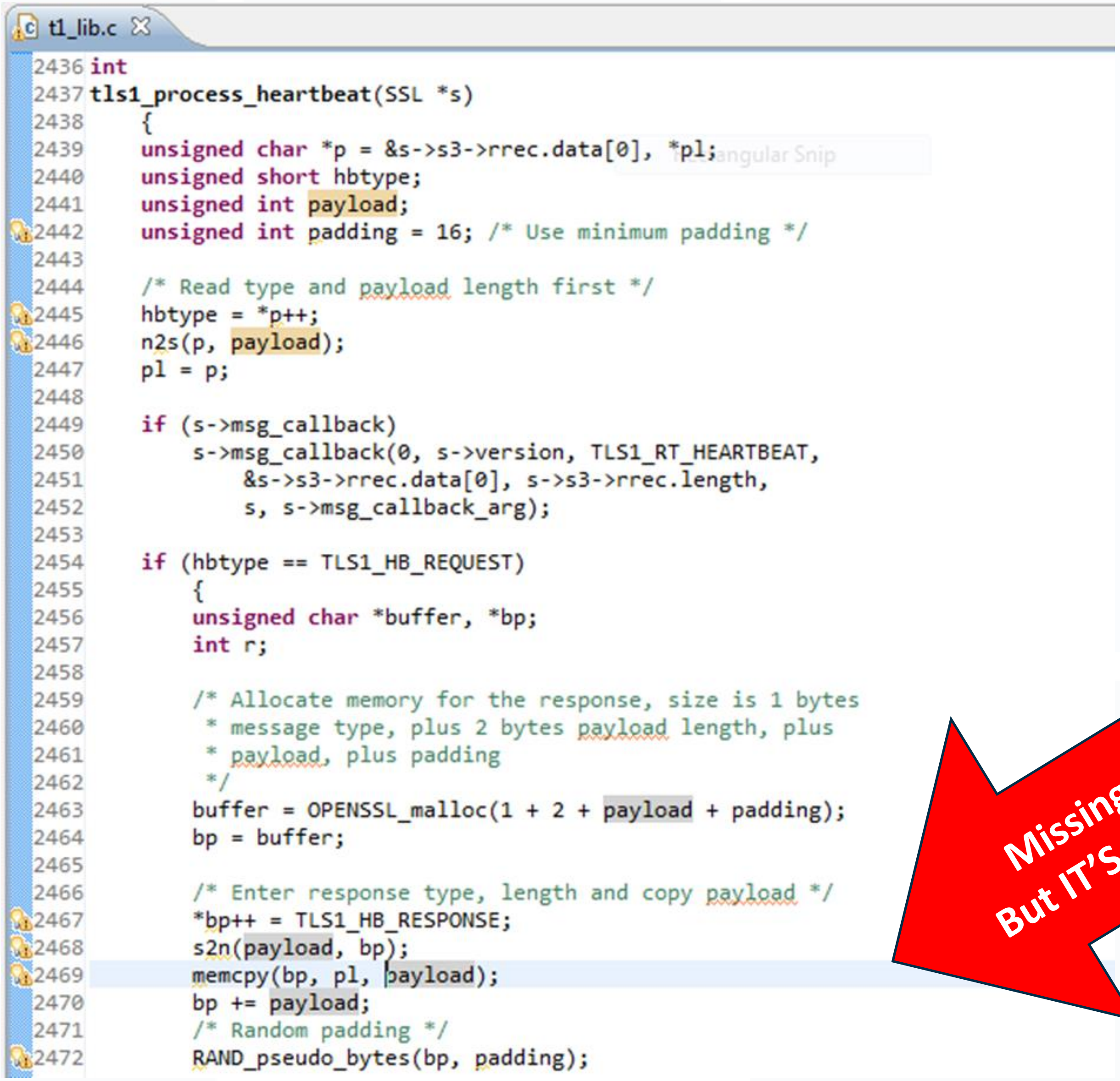
```
509.        eax11 = &(&edx.0[1] - &arg_1[1])[1];
510.        s_4 = UNDEFINED;
511.        if (s_4->off_4 < eax11) goto loc_100bc813;
512.        strcpy(s_3->off_0, arg_1);
513.        do {
514.            esi12.0 = phi(arg_1, loc_100bc7ee, &esi12.0[1], loc_100bc7f1);
515.        } while (esi12.0 != '\0');
516.    loc_100bc7f8:
517.        ecx8.0 = phi(&arg_1[1], loc_100bc868, &arg_1[1], loc_100bc7f1);
```

Insecure string API (C/C++)

The string manipulation function used is insecure, since it allows a buffer overflow. Insecure functions include: `strcpy`, `strcat`. This may lead to incorrect behavior of the application, crash, or violation of valuable data confidentiality.

The `strcpy()` function copies the C string pointed by source into the array pointed by destination, including the terminating null character. The `strcat` appends a copy of the source string to the destination string. It is important to note that, the destination array should be large enough otherwise it may result in undefined behavior.

Just 1 Line of Code (LoC) in 2 files


t1_lib.c

```c
int
tls1_process_heartbeat(SSL *s)
    {
    unsigned char *p = &s->s3->rrec.data[0], *pl;
    unsigned short hbtype;
    unsigned int payload;
    unsigned int padding = 16; /* Use minimum padding */

    /* Read type and payload length first */
    hbtype = *p++;
    n2s(p, payload);
    pl = p;

    if (s->msg_callback)
        s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
            &s->s3->rrec.data[0], s->s3->rrec.length,
            s, s->msg_callback_arg);

    if (hbtype == TLS1_HB_REQUEST)
        {
        unsigned char *buffer, *bp;
        int r;

        /* Allocate memory for the response, size is 1 bytes
         * message type, plus 2 bytes payload length, plus
         * payload, plus padding
         */
        buffer = OPENSSL_malloc(1 + 2 + payload + padding);
        bp = buffer;

        /* Enter response type, length and copy payload */
        *bp++ = TLS1_HB_RESPONSE;
        s2n(payload, bp);
        memcpy(bp, pl, payload);
        bp += payload;
        /* Random padding */
        RAND_pseudo_bytes(bp, padding);
```

Missing Bounds Check!
But IT'S NOT EASY TO FIND!

Benefits

- Improve Overall security and stability
- Avoid mistakes early in the source code (SHIFT LEFT)
- Detect and Prevent flow related issues
- Find the Problem Before it Become A Bug!
- Prevent and not Detect!

Remember –

Your CyberSecurity is only as good as the Weakest Link!

Thank you ‘Cảm ơn’

Parasoft | Perfecting Software