SECON'2017

#SECONRU

IX МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ РАЗРАБОТЧИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Антипаттерны безопасного программирования

Евстифеев Петр

Разработчик компании «Код безопасности»

ПЕНЗА

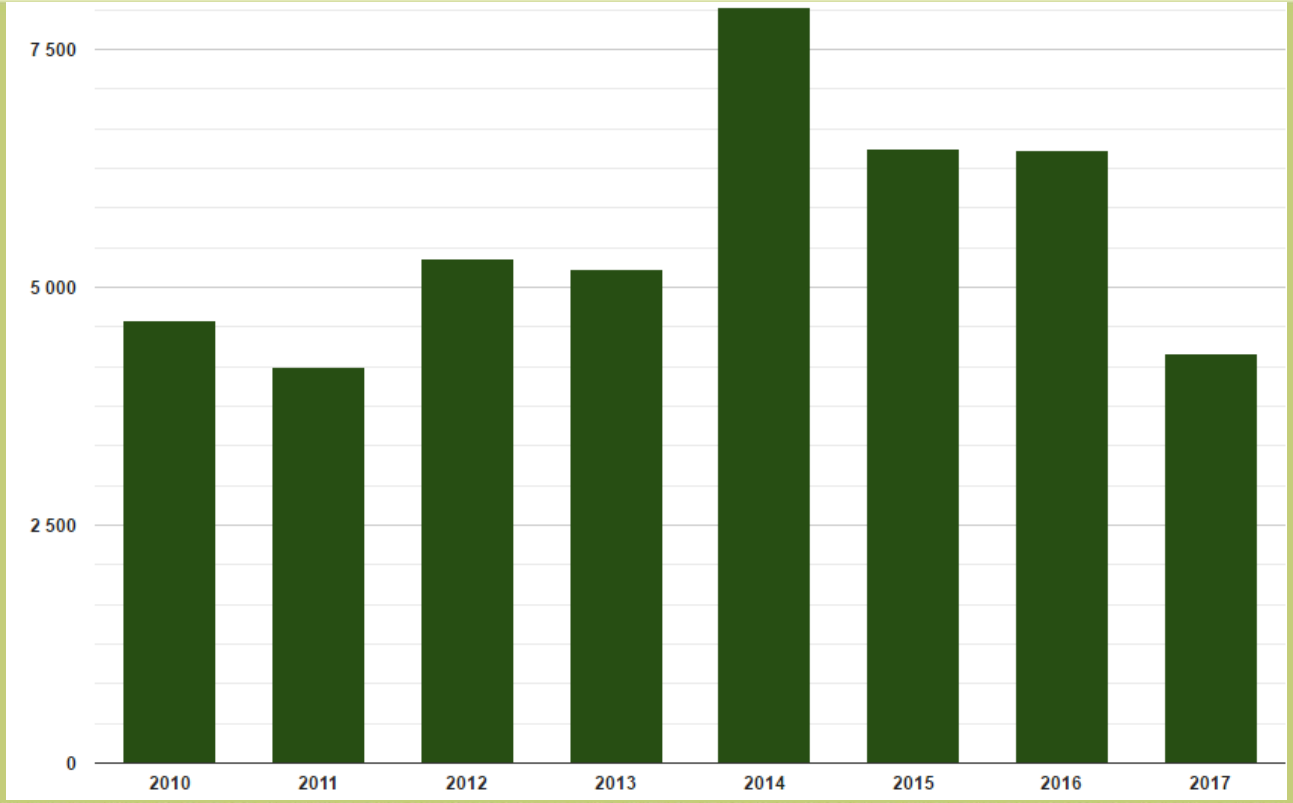
whoami

- Developer in ltd "Security Code"
- Security Researcher
- Experienced in:
  - C/C++/Python
  - Reverse Engineering
  - Digital Forensic
  - Penetration Testing

Agenda

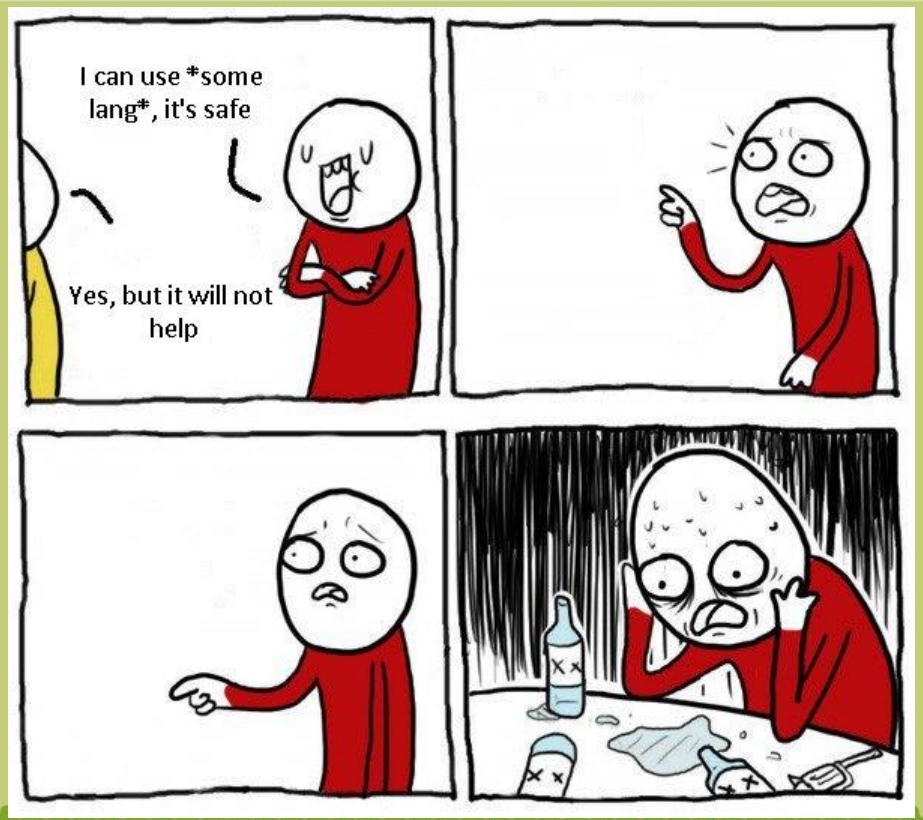
- What is a secure code
- Some language-independent examples of unsafe code
- Recommendations for writing secure code
- Nothing about:
  - Buffer overflow
  - XSS/CSRF/XSRF
  - Weak cryptography

Vulnerability Statistics



Why software is unsafe?

Java, Haskell, Erlang, Rust, GoLang, etc.



What is secure code

- Secure code is the code without weakness
- Software weakness - flaw, fault, bug, vulnerability or other error in software implementation, code, design, or architecture that if left unaddressed could result in systems and networks being vulnerable to attack
- Vulnerability - weakness of an asset or control that can be exploited by one or more threats

CVE vs CWE

- CVE - Common Vulnerabilities and Exposures
- CWE - Common Weakness Enumeration

CWE TOP 25

http://cwe.mitre.org/top25/

3 sections:

- Insecure Interaction Between Components (6)
- Risky Resource Management (11)
- Porous Defenses (8)

Injections

- 1st place in OWASP TOP 10
- 1st,2nd place in CWE TOP 25
- Easily exploitable
- Databases: SQL/NoSQL, Client-server/Embedded
- LDAP
- XPath
- OS commands (popen, exec, system)

SQL Injection Example – Код курильщика

```
username = request.get("username");
password = request.get("password");
query = "SELECT * FROM Users WHERE Uname = ' " + username + " '  AND
Password = MD5('" + password + "')";
result = sql_exec(query);
if(result.count() == 1 && result.get_first()["ID"] == 13) {
        //This is the administrator
        ...
}
```

SQL Injection Example

- Expected query:

SELECT * FROM Users WHERE Uname = 'Admin' AND Password = MD5('qwerty')

- Attacker's query:

SELECT * FROM Users WHERE Uname = ' Vasya_Pupkin' AND Password = MD5('')
OR 1 LIMIT x,1 #

where x = 1,2,3…rowcount

Код здорового человека

```
username = escaping(request.get("username"));
password = escaping(request.get("password"));
query = "SELECT * FROM Users WHERE Uname = '?'  AND Password = MD5('?')";
statement = sql_prepare(query);
result = sql_bind(statement, username, password);
…
```

SQL Injection - Protection

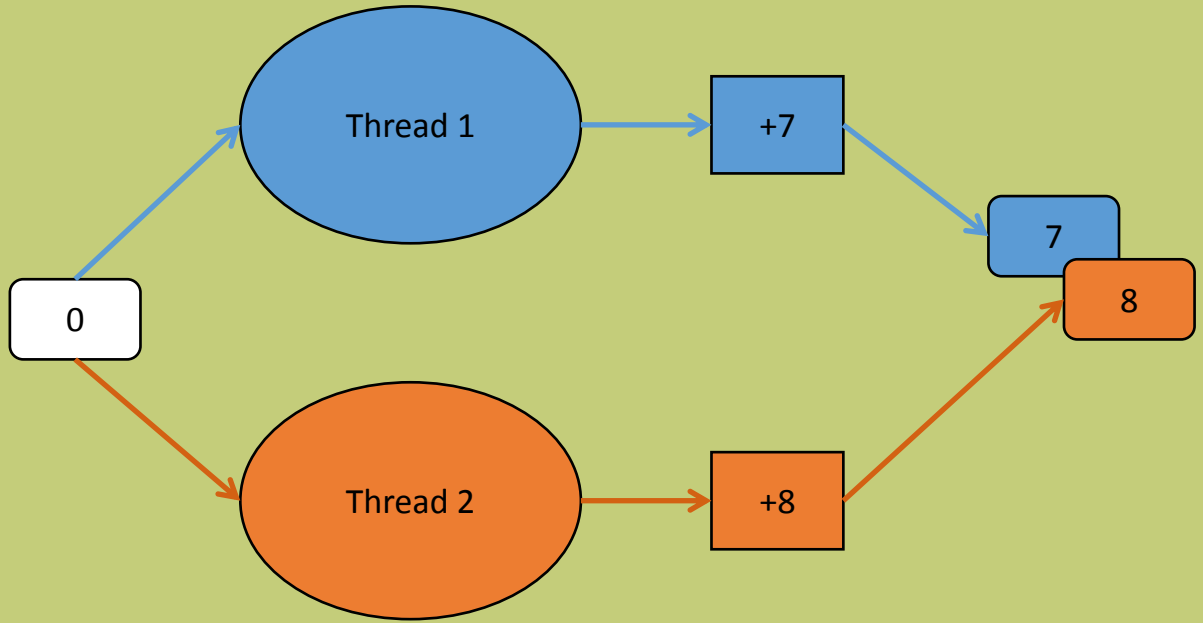
- Verify user data
- Use prepared statement/Stored procedures
- Use ORM
- Read the documentation
- Use the database user with low privileges

Race conditions/Data race

Race condition - Example

```
balance = 0;
IncreaseBalance(int number) {
        balance = balance + number;
}
SomeFunction() {
        thread1 = Thread(IncreaseBalance, 7);
        thread2 = Thread(IncreaseBalance, 8);
        thread1.join();
        thread2.join();
        print(balance);   //May be 7,8,15
}
```

Hot it works?



Race condition - Real-life example

```
# SingleThread App
DoTransfer(string wallet_from,  string wallet_to,  int number) {
        statement = sql_prepare ("SELECT * FROM Cash WHERE Waller_ID = ' ? '");
        balance_1 = sql_bind(statement, wallet_from) .get_first()["Balance"];
        balance_2 = sql_bind(statement, wallet_to) .get_first()["Balance"];
        balance_1 = balance_1 - number;
        balance_2 = balance_2 + number;
#Begin Transaction
#Update balances
#Commit
}
```

Startbucks case

Race Condition - Protection

- Use synchronization objects © Ваш К.О.
- Use the task queue
- Check your software on multi-core systems
- Read the documentation

Missing Function Level Access Control

TRUST NOBODY

Example 1

```
GetUserInfoInternal(id){
        ...
}
GetUserInfo(id, user_token) {
        if(userValid(user_token)) {
                GetUserInfoInternal(id);
        } else {
                ...
        }
}
```

Example 2

```
# Never do that
if(isAdmin) {
        someUiWidgets.Visible = True;
}
```

True story: Cloud password manager

```
# Incomming JSON
{
        …
        "AccountName": @myMail@,
        "Experation date": "15.12.2016",   31.12.2099
        "Expired": True                    False
        …
}
```

True story: Secure messenger

```
# Outgoing XML
<Message from="1" to="2">      Replace “from id” - profit
        <Text>Hello, transfer money to me</Text>
</Message>
```

Path Traversal

Path traversal Example

```
dataPath = "/users/profiles";
username = request.get("user");
profilePath = dataPath + "/" + username;

open(profilePath);
```

Missing/Incorrect Error/Exception Handling

Missing Error Handling Example

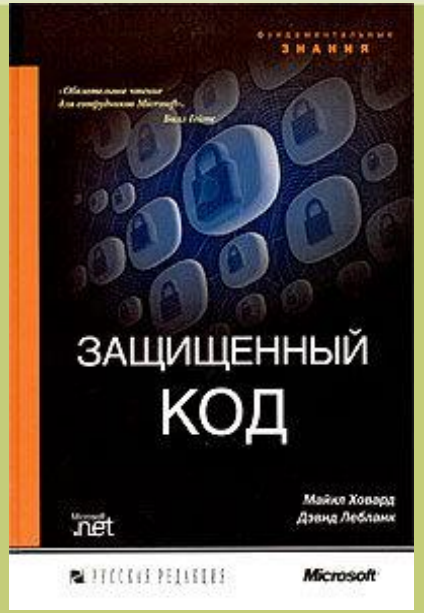
```
# Windows only
ImpersonateNamedPipeClient(hPipe);
DoSomething();
RevertToSelf();
```

Incorrect Exception Handling Example

```
Mutex mutex;
BuildLogsSync() {
        try {
                lock_mutex(mutex);
                BuildLogs();
                unlock_mutex(mutex);
        } catch {
        }
}
```

Integer Overflow or Wraparound

Homework



Secure Coding:

- http://cwe.mitre.org
- http://owasp.org
- http://bdu.fstec.ru
- https://www.cvedetails.com
- https://www.securecoding.cert.org

Thank you!

SECON'2017

IX МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ РАЗРАБОТЧИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Евстифеев Петр

разработчик компании «Код безопасности»

zofktulhu@gmail.com