Mining Security Requirements from Common Vulnerabilities and Exposures for Agile Projects

Wentao Wang, Arush Gupta, Nan Niu

QuaRAP’18 Banff, Canada
Mining Security Requirements from Common Vulnerabilities and Exposures for Agile Projects

Wentao Wang, Arush Gupta, Nan Niu
QuaRAP'18 Banff, Canada

CVE-2017-15974 Detail

Current Description

tPanel 2009 allows SQL injection for Authentication Bypass via 'or 1=1 or "=" to login.php.

Source: MITRE
Description Last Modified: 10/29/2017

Hyperlink

https://www.exploit-db.com/exploits/43085/

Technical Details
Vulnerability Type (View All)
- SQL Injection (CWE-89)
Outline

• Motivation
• Approach Details and Research Questions
  ❖ Retrieve Vulnerabilities as Candidates
  ❖ Derive Security Acceptance Criterias
  ❖ Design Test Cases
• Summary
Butterfly Effect

CVE-2016-4449
Butterfly Effect

More than 10 companies were affected

Involves more than 29 software products
Vulnerabilities in CVE

14,643 vulnerabilities are published in 2017

127% increases over 2016

23.7% are OSS vulnerabilities

127% increases over 2016
Vulnerabilities in CVE

14,643 vulnerabilities are published in 2017, a 127% increase over 2016. 23.7% are OSS.

3470 × 30 = 104,100
Subject Project
Requirements Evolution

UC1 Create and Deactivate Patients Use Case

1.1 Preconditions:
The iTrust HCP has authenticated himself or herself in the iTrust Medical Records system (UC3).

1.2 Main Flow:
An HCP is able to create a patient [S1] or disable a selected patient [S2]. The create/disable patients and HCP transaction is logged (UC5).

1.3 Sub-flows:
- [S1] The HCP enters a patient as a new user of iTrust Medical Records system. Only the name and email are provided. The patient’s assigned MID and a secret key (the initial password) are personally provided to the user, with which the user can reset his/her password. The HCP can edit the patient according to data format 6.4 [E1] with all initial values (except patient MID) defaulting to null and/or 0 as appropriate. Patient MID should be the number assigned when the patient is added to the system and cannot be edited. The HCP does not have the ability to enter/edit/view the patient’s security question/password.
- [S2] The HCP selects a patient to deactivate. The HCP is presented with a confirmation containing the name of the patient and determines if it is the patient they intend to deactivate [E2]. A deactivated patient cannot be modified or log into the system, and can only be reactivated by the administrator.
- [S3] The HCP uploads a comma-separated value file containing one patient per row. The fields of the CSV file must include at least the first name, last name, and e-mail address, with additional columns available for the other demographic values. The patients are created, the tables are populated, and the MIDS and temporary passwords are displayed to the HCP in a table. The event is logged.

1.4 Alternative Flows:
- [E1] The system prompts the enterer/editor to correct the format of a required data field because the input of that data field does not match that specified in data format 6.4 for patients.
- [E2] If the confirmation screen does not show the name of the intended patient, the HCP is then prompted to input the correct patient identification information again.
- [E3] If the file is malformed, then no data is added, and an error message explaining the correct file structure is presented.
Security requirements in iTrust

4. Non-Functional Requirements

4.1 HIPAA
Implementation must not violate HIPAA guidelines.

4.2 Exclusive Authentication
The system shall enable multiple simultaneous users, each with his/her own exclusive authentication.

4.3 Form Validation
The form validation of the system shall show the errors of all the fields in a form at the same time.

4.4 Reports
A report is a page which opens in a separate window and contains minimal decoration. The format is printer-friendly in that the background is white and the information does not exceed the width of 750 pixels so that upon printing, no information is lost due to the information being too wide.

4.5 Privacy Policy
The system shall have a privacy policy linked off of the home page. The privacy policy should follow the template provided here.

4.6 Security of MID
Remove MID from being displayed on all pages and URLs. MIDs should be considered private, sensitive information.
Security requirements in iTrust

4. Non-Functional Requirements

4.1 HIPAA
Implementation must not violate HIPAA guidelines.

4.2 Exclusive Authentication
The system shall enable multiple simultaneous users, each with his/her own exclusive authentication.

4.3 Form Validation
The form validation of the system shall show the errors of all the fields in a form at the same time.

4.4 Reports
A report is a page which opens in a separate window and contains minimal decoration. The format is printer-friendly in that the background is white and the information does not exceed the width of 750 pixels so that upon printing, no information is lost due to the information being too wide.

4.5 Privacy Policy
The system shall have a privacy policy linked off of the home page. The privacy policy should follow the template provided [here].

4.6 Security of MID
Remove MID from being displayed on all pages and URLs. MIDs should be considered private, sensitive information.
Health Insurance Portability & Accountability Act

Health Insurance Portability & Accountability Act

No documentation or ignore low-level security requirements

W. Behutiye, P. Karhapää, D. Costal, M. Oivo, and X. Franch, “Nonfunctional requirements documentation in agile software development: challenges and solution proposal,” in PROFES, 2017

Outline

• Motivation
• Approach Details and Research Questions
  - Retrieve Vulnerabilities as Candidates
  - Derive Security Acceptance Criteria
  - Design Test Cases
• Summary
Overview

1. Mining vulnerabilities
2. Deriving security requirements
3. Designing test cases
4. Reporting vulnerabilities

Test cases → CVE → Vulnerabilities → Security requirements → Test cases
Retrieval Vulnerabilities

• Query: UC1 (iTrust)
Retrieval Vulnerabilities

**CVE-2017-15974 Detail**

**Current Description**
tPanel 2009 allows SQL injection for Authentication Bypass via 'or 1=1 or ''='' to login.php.

**Source:** MITRE  
**Description Last Modified:** 10/29/2017

**Hyperlink**
- https://www.exploit-db.com/exploits/43085/

**Technical Details**

**Vulnerability Type** (View All)
- SQL Injection (CWE-89)

• Query: UC1 (iTrust)
Retrieval Vulnerabilities

- Query: UC1 (iTrust)
- Latent semantic
- Database: MySQL, SQLI
- LSI

Derive Security Requirements

- Acceptance criteria

**Given-When-Then**

**Awareness**

---

**CVE-2017-15974 Detail**

**Current Description**

tPanel 2009 allows SQL injection for Authentication Bypass via 'or 1=1 or '=' to login.php.

**Source:** MITRE  
**Description Last Modified:** 10/29/2017

**Hyperlink**

- [https://www.exploit-db.com/exploits/43085/](https://www.exploit-db.com/exploits/43085/)

**Technical Details**

- **Vulnerability Type** (View All)
  - SQL Injection (CWE-89)
AC1: Given an eligible user, when create patient or upload patients, then all input values shall be properly sanitized to prevent tautology (e.g., 1=1).

• Acceptance criteria Given-When-Then Awareness

CVE-2017-15974 Detail

Current Description
tPanel 2009 allows SQL injection for Authentication Bypass via 'or 1=1 or '=' to login.php.

Source: MITRE
Description Last Modified: 10/29/2017

Hyperlink
https://www.exploit-db.com/exploits/43085/

Technical Details
Vulnerability Type (View All)
• SQL Injection (CWE-89)
Design Test Cases

CVE-2017-15974 Detail

Current Description
tPanel 2009 allows SQL injection for Authentication Bypass via 'or 1=1 or '='' to login.php.

Source: MITRE
Description Last Modified: 10/29/2017

Hyperlink
https://www.exploit-db.com/exploits/43085/

Technical Details
Vulnerability Type (View All)
- SQL Injection (CWE-89)

ACI: Given an eligible user, when create patient or upload patients, then all input values shall be properly sanitized to prevent tautology (e.g., 1=1).
Design Test Cases

CVE-2017-15974 Detail

Current Description

tPanel 2009 allows SQL injection for Authentication Bypass via 'or 1=1 or "=" to login.php.

Source: MITRE
Description Last Modified: 10/29/2017

Hyperlink
https://www.exploit-db.com/exploits/43085/

Technical Details

Vulnerability Type (View All)
- SQL Injection (CWE-89)

ACI: Given an eligible user, when create patient or upload patients, then all input values shall be properly sanitized to prevent tautology (e.g., 1=1).
Potential Improvement

- **Step 1:**
  \[ RQ1: \] How to improve information retrieval method to achieve the goal of removing irrelevant candidates without filtering our relevant ones?

- **Step 2:**
  \[ RQ2: \] Which methods can better classify vulnerabilities to achieve the goal of easily selecting all representative vulnerabilities?

- **Step 3:**
  \[ RQ3: \] How to modify attacks in CVE to generate more security test cases which can achieve the goal of increasing testing coverage?
Outline

• Motivation
• Approach Details and Research Questions
  ❖ Retrieve Vulnerabilities as Candidates
  ❖ Derive Security Acceptance Criteria
  ❖ Design Test Cases
• Summary
Summary

• Mining security requirements from CVE
  Less security related experience is needed when using our approach.

• Complementary with existing approaches
  Elicitation of security requirements is based on brainstorming, checklists, and analyzing reports of previous failures [1].


• Next steps
  Research questions
  Automation
  Evaluations (effectiveness, generalizability)
Thanks!