Mining Security Requirements from Common Vulnerabilities and Exposures for Agile Projects

Wentao Wang, Arush Gupta, Nan Niu

QuaRAP'18 Banff, Canada

University of CINCINNATI

Mining Security Requirements from Common Vulnerabilities and Exposures

Wentao Wang,

QuaRAP

CVE-2017-15974 Detail

Current Description

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

Source: MITRE

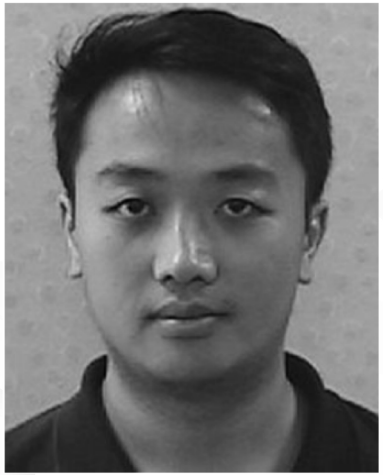
Description Last Modified: 10/29/2017

Hyperlink
https://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
https://www.exploit-db.com/exploits/43085/

Technical Details

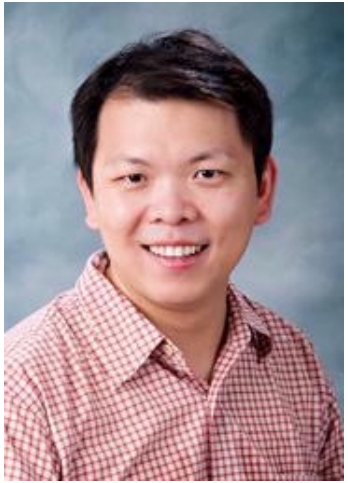
Vulnerability Type (View All)

- SQL Injection (CWE-89)



Wentao Wang
Ph.D. Candidate
University of Cincinnati

Arush Gupta
Master Student
University of Cincinnati



Dr. Nan Niu
Advisor
University of Cincinnati

University of CINCINNATI

Outline

- Motivation
- Approach Details and Research Questions
  - ❖ Retrive Vulnerabilities as Candidates
  - ❖ Derive Security Acceptance Criterias
  - ❖ Design Test Cases
- Summary

University of CINCINNATI

Butterfly Effect

CVE-2016-4449

University of CINCINNATI

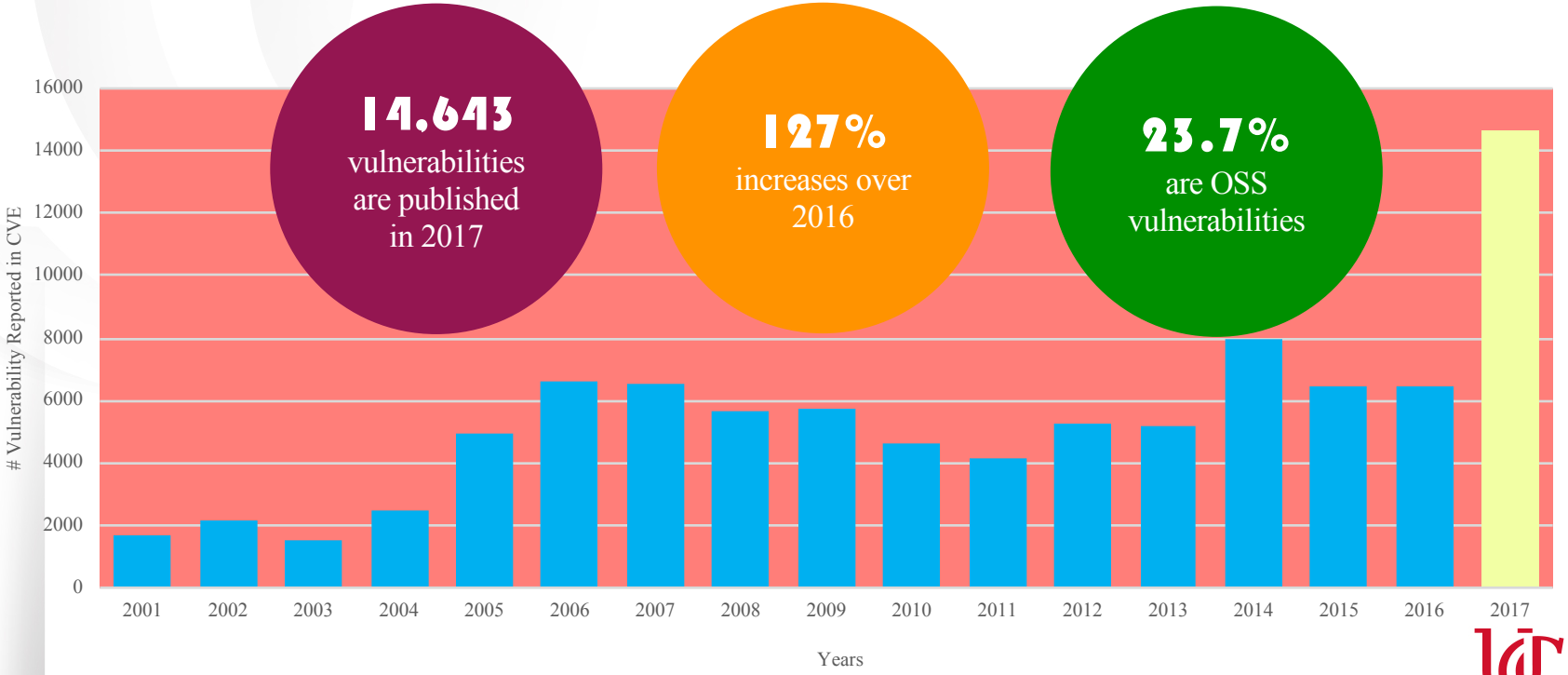
Butterfly Effect

More than **10** companies were affected

Involves more than **29** software products

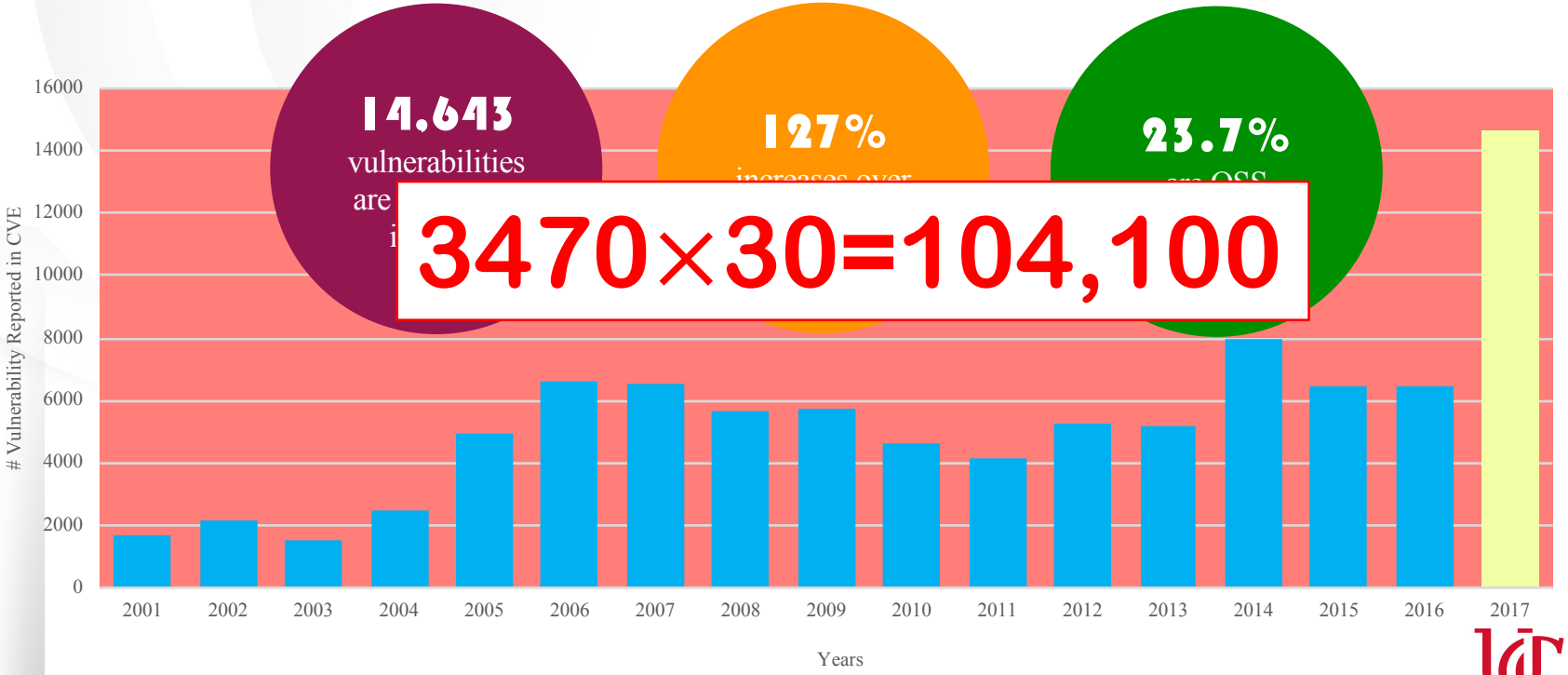
University of CINCINNATI

Vulnerabilities in CVE



University of CINCINNATI

Vulnerabilities in CVE



University of CINCINNATI

Subject Project

iTrust

Home Logout Change Password **Welcome, Kelly Doctor**

- Patient Info
- Appointments
- Office Visit
- Messaging
- Telemedicine
- Add
- Personal Info
- Other

Notifications

Message Notification

5 Appointment requests.

12 Unread messages.

Today's Appointments

Telemedicine Reports

0 physiological status reports

0 weight/pedometer status reports

University of CINCINNATI

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 can not be modified or log into the system, and can only be reactivated by the administrator.
- [S3] The HCP uploads a comma-seperated 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.

University of CINCINNATI

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 pa

1.3 Sub-flows:

- [S1] The HCP enters a patient as a new user of iTrust Medical Records system. Only the assigned MID and a secret key (the initial password) are personally provided to the user The HCP can edit the patient according to data format 6.4 [E1] with all initial values (exc appropriate. Patient MID should be the number assigned when the patient is added to th 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 it is the patient they intend to deactivate [E2]. A deactivated patient can not be modified by the administrator.
- [S3] The HCP uploads a comma-seperated value file containing one patient per row. The name, last name, and e-mail address, with additional columns available for the other der tables are populated, and the MIDS and temporary passwords are displayed to the HCP

1.4 Alternative Flows:

- [E1] The system prompts the enterer/editor to correct the format of a required data field 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 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.

Version	Date (mm/dd/yy)	# of Java Methods		# of Req.s Units	
		total	new	total	new
v4	12/12/07	1106	–	92	–
v6	08/23/08	1496	522	128	37
v7	01/15/09	1548	180	140	19
v8	08/17/09	1500	86	153	14
v9	01/11/10	1636	153	181	20
v10	08/17/10	1737	103	198	23
v11	01/17/11	1856	123	287	140
v12	08/14/11	2135	344	194	48
v13	01/17/12	2342	202	199	6
v14	08/16/12	2336	133	203	7
v15	01/06/13	2378	73	208	5
v16	08/19/13	2421	72	205	11
v17	01/09/14	2665	256	211	10
v18	08/20/14	2849	181	227	16
v19	01/08/15	2946	97	242	15

W. Wang, A. Gupta, Y. Wu, "Continuously Delivered? Periodically Updated? Never Changed? Studying an Open Source Project's Releases of Code, Requirements, and Trace Matrix", JITRE, 2015.

University of CINCINNATI

Security requirements in iTrust

4. Non-Functional Requirements

4.1 HIPAA

Implementation must not violate HIPAA guidelines.

4.2 Exlusive 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.

University of CINCINNATI

Security requirements in iTrust

4. Non-Functional Requirements

4.1 HIPAA

Implementation must not violate HIPAA guidelines.

4.2 Exlusive 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

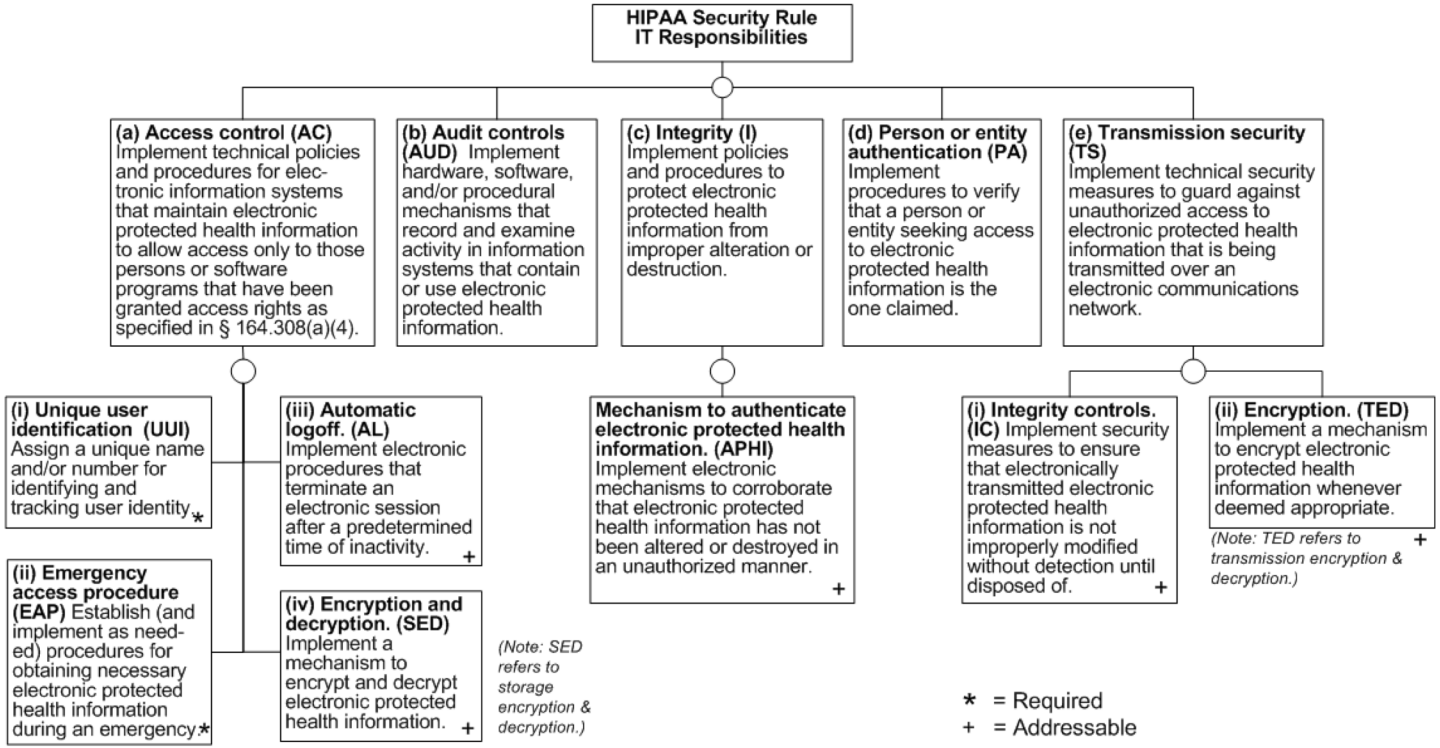
The system shall have a privacy policy linked off of the home page. The privacy policy should follow the template provided here.

4.6 Security of MID

Remove MID from being displayed on all pages and URLs. MIDs should be considered private, sensitive information.

University of CINCINNATI

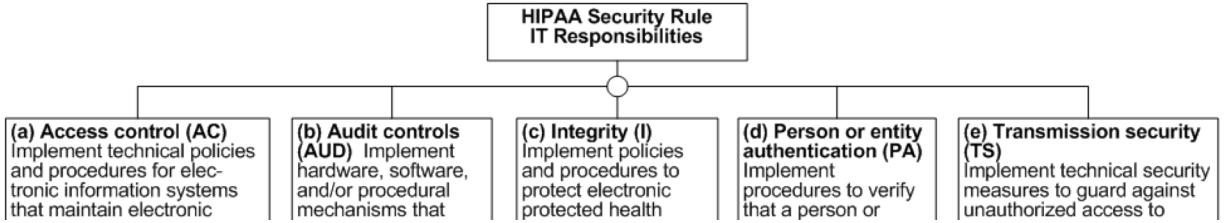
Health Insurance Portability & Accountability Act



J. Cleland-Huang, A. Czauderna, M. Gibiec, J. Emenecker, "A Machine Learning Approach for Tracing Regulatory Codes to Product Specific Requirements", ICSE, 2010

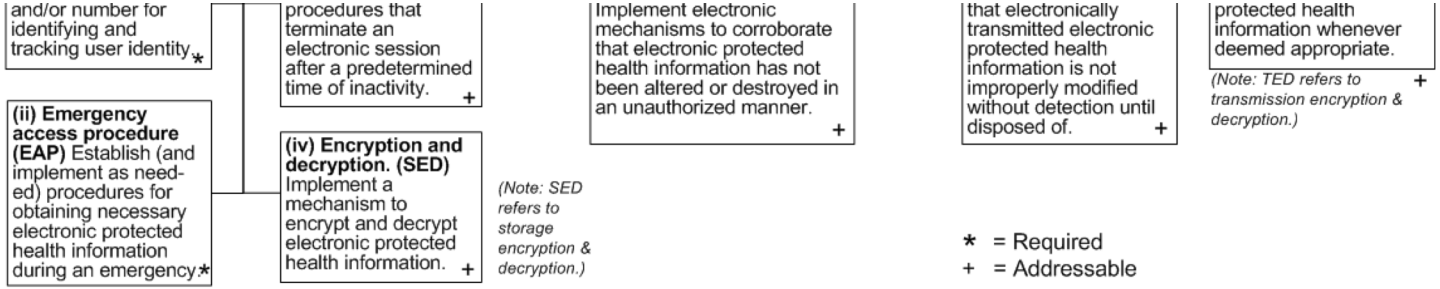
University of CINCINNATI

Health Insurance Portability & Accountability Act



No documentation or ignore low-level security requirements

W. Behutiye, P. Karhap¨a¨a, D. Costal, M. Oivo, and X. Franch, "Nonfunctional requirements documentation in agile software development: challenges and solution proposal," in PROFES, 2017



J. Cleland-Huang, A. Czauderna, M. Gibiec, J. Emenecker, "A Machine Learning Approach for Tracing Regulatory Codes to Product Specific Requirements", ICSE, 2010

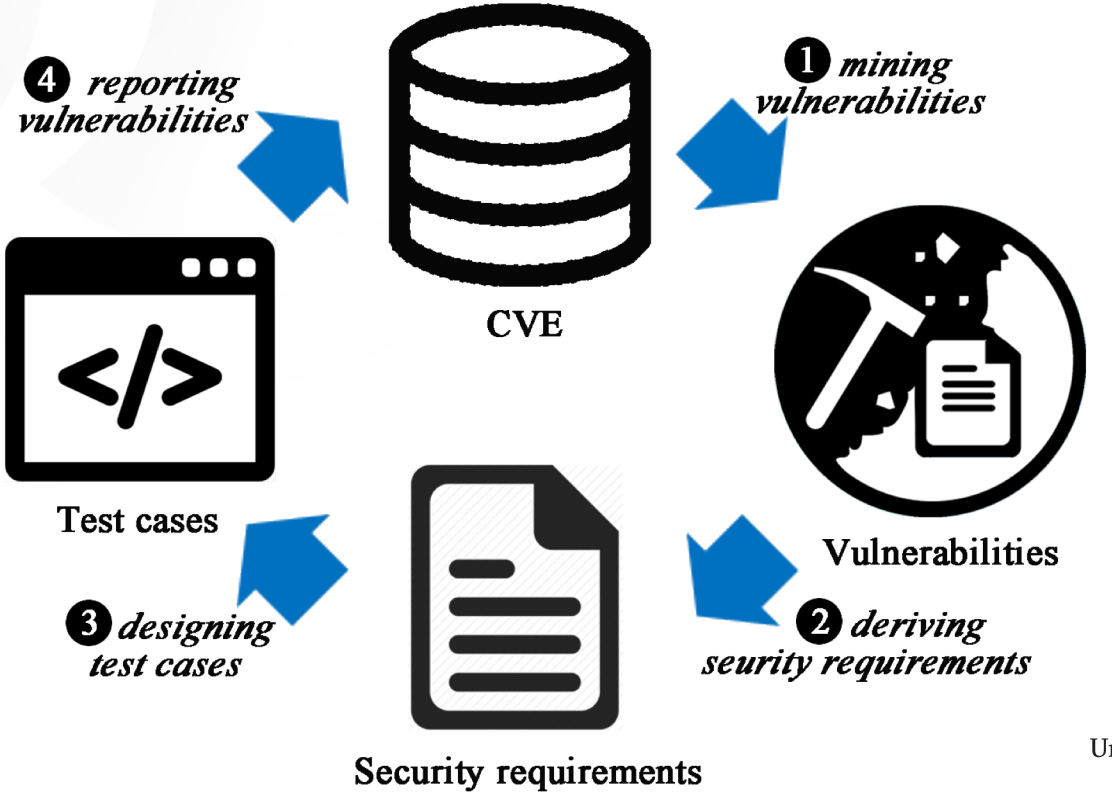
University of CINCINNATI

Outline

- Motivation
- Approach Details and Research Questions
  - ❖ Retrive Vulnerabilities as Candidates
  - ❖ Derive Security Acceptance Criterias
  - ❖ Design Test Cases
- Summary

University of CINCINNATI

Overview



University of CINCINNATI

Retrieval Vulnerabilities

- Query: UC1 (iTrust)

Patient Information

First name:

Last Name:

Email:

University of CINCINNATI

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://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
https://www.exploit-db.com/exploits/43085/

Technical Details

Vulnerability Type (View All)

- SQL Injection (CWE-89)

- Query: UC1 (iTrust)

Patient Information

First name:

Last Name:

Email:

University of CINCINNATI

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://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
https://www.exploit-db.com/exploits/43085/

Technical Details

Vulnerability Type (View All)

- SQL Injection (CWE-89)

- Query: UC1 (iTrust)
- Latent semantic

  Database : MySQL, SQLI
- LSI

[1] J. H. Hayes, A. Dekhtyar, and J. Osborne, “Improving Requirements Tracing via Information Retrieval,” in RE, 2003.

University of CINCINNATI

Derive Security Requirements

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://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
https://www.exploit-db.com/exploits/43085/

Technical Details

Vulnerability Type (View All)

- SQL Injection (CWE-89)

- Acceptance criteria
  - Given-When-Then
  - Awareness

University of CINCINNATI

Derive Security Requirements

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://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
https://www.exploit-db.com/exploits/43085/

Technical Details

Vulnerability Type (View All)

- SQL Injection (CWE-89)

- Acceptance criteria
  - Given-When-Then
  - Awareness

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).

University of CINCINNATI

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://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
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).

University of CINCINNATI

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://packetstormsecurity.com/files/144444/tPanel-2009-SQL-Injection.html
https://www.exploit-db.com/exploits/43085/

Technical Details

Vulnerability Type (View All)

- SQL Injection (CWE-89)

PatientBean.firstName=“ or 1=1”

Patient Information

First name:	or 1=1
Last Name:	Smith
Email:	a@b.com

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).

University of CINCINNATI

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?

University of CINCINNATI

Outline

- Motivation
- Approach Details and Research Questions
  - ❖ Retrive Vulnerabilities as Candidates
  - ❖ Derive Security Acceptance Criterias
  - ❖ Design Test Cases
- Summary

University of CINCINNATI

Summary

- Mining security requirements from CVE

  Less security related experience is needed when using our approache

- Complemenatary with existing approaches

  Elicitation of security requirements is based on brainstorming, checklists, and analyzing reports of previous failures [1].

  [1] J. Cleland-Huang, “Safety stories in agile development,” in IEEE Software, 2017

- Next steps

  Research questions

  Automation

  Evaluations (effectiveness, genieralizability)

University of CINCINNATI

Thanks!

University of CINCINNATI