

Alma Mater Studiorum – Università di Bologna

Scuola di Ingegneria e Architettura
Corso di Laurea in Ingegneria Informatica

Analisi del rischio e studio delle vulnerabilità in un sistema di home intelligence su piattaforma ad agenti: il caso Home Manager

Candidato
Caterina Caravaggio

Relatore
Prof. Enrico Denti

Correlatori
Dott. Ing. Ambra Molesini
Prof. Marco Prandini

Anno Accademico 2017/2018

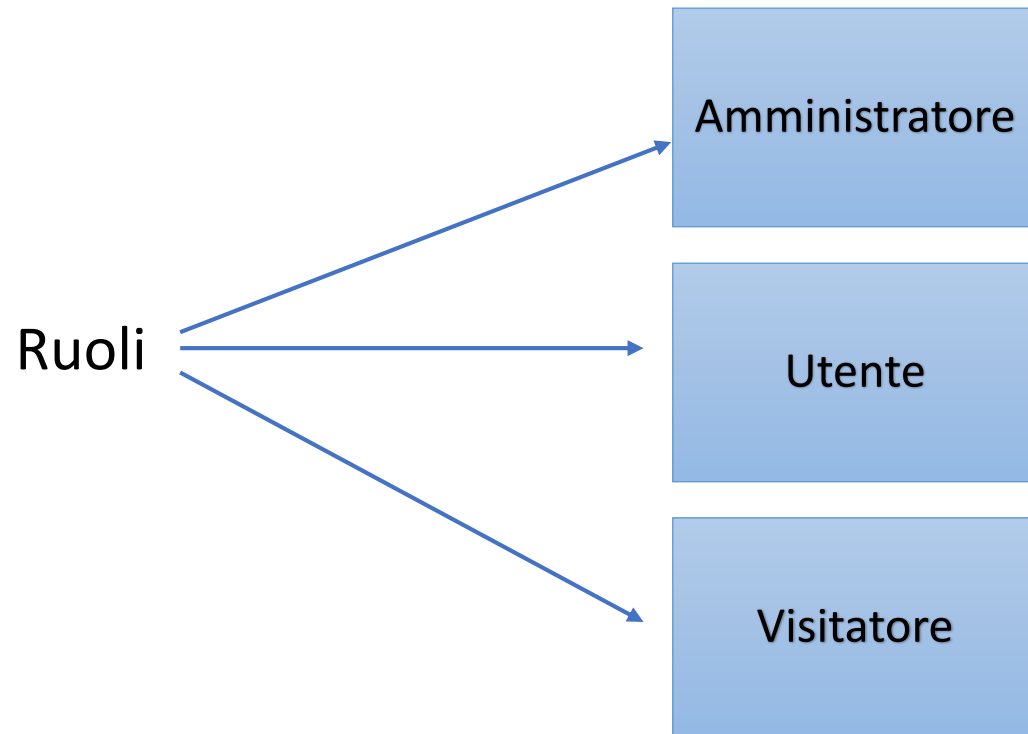
Contesto: Home Manager

- Sistema prototipale Smart Environment per l'automazione domestica ad agenti
- Ispirato a *Butlers*
- Sistema multi-agente sull'infrastruttura TuCsON
- Java-based



Prototipo attuale HM

- All'avvio vengono richiesti username e password



Scenario Smart Kitchen, quattro dispositivi intelligenti:

- Forno
- Frigo
- Dispensa
- Mixer

Le rispettive richieste vengono elaborate dal centro di tuple contenuto in TuCsON

Obiettivi

Trovare delle vulnerabilità nel prototipo allo stato attuale

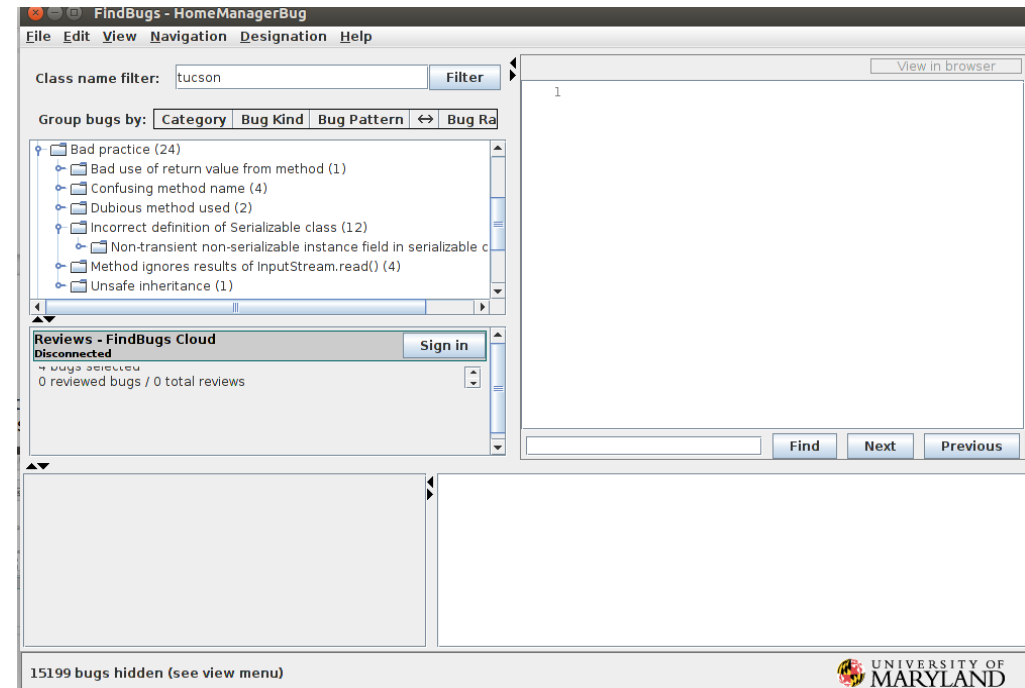
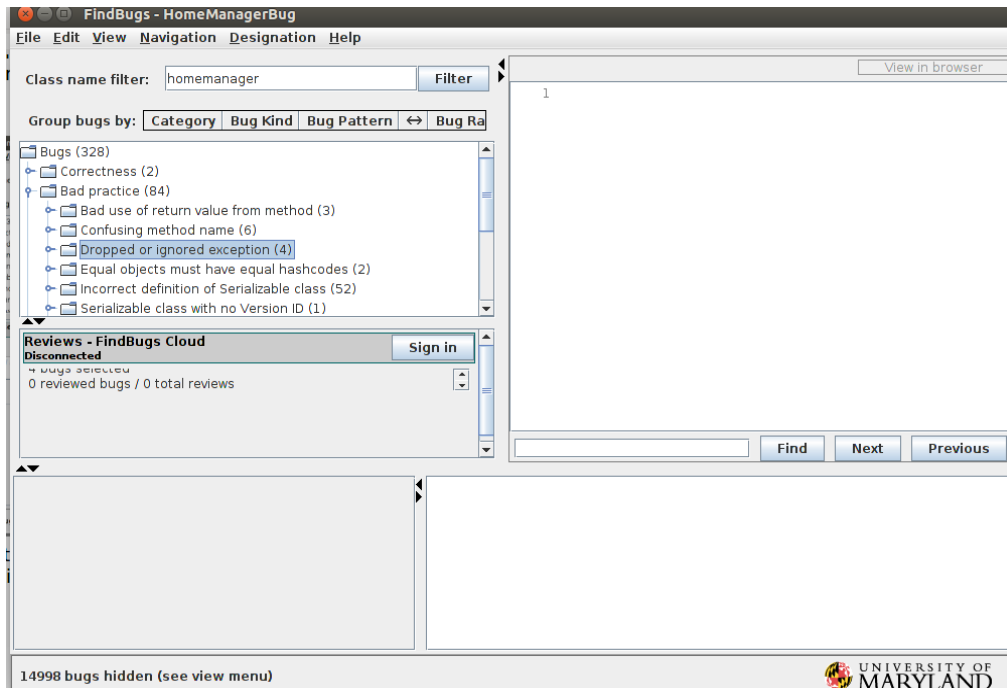
Stilare un'analisi del rischio per componenti che verranno aggiunti in seguito

Piano di collaudo

- Fronti su cui svolgere i test:
 - Persistenza dei dati
 - Comunicazione tra Home Manager e TuCsON
 - Errori di struttura del codice
- Uso di tool specifici quali findbugs, javasnoop e wireshark
- Linea di azione:
 - White box
 - Black box

White box: findbugs

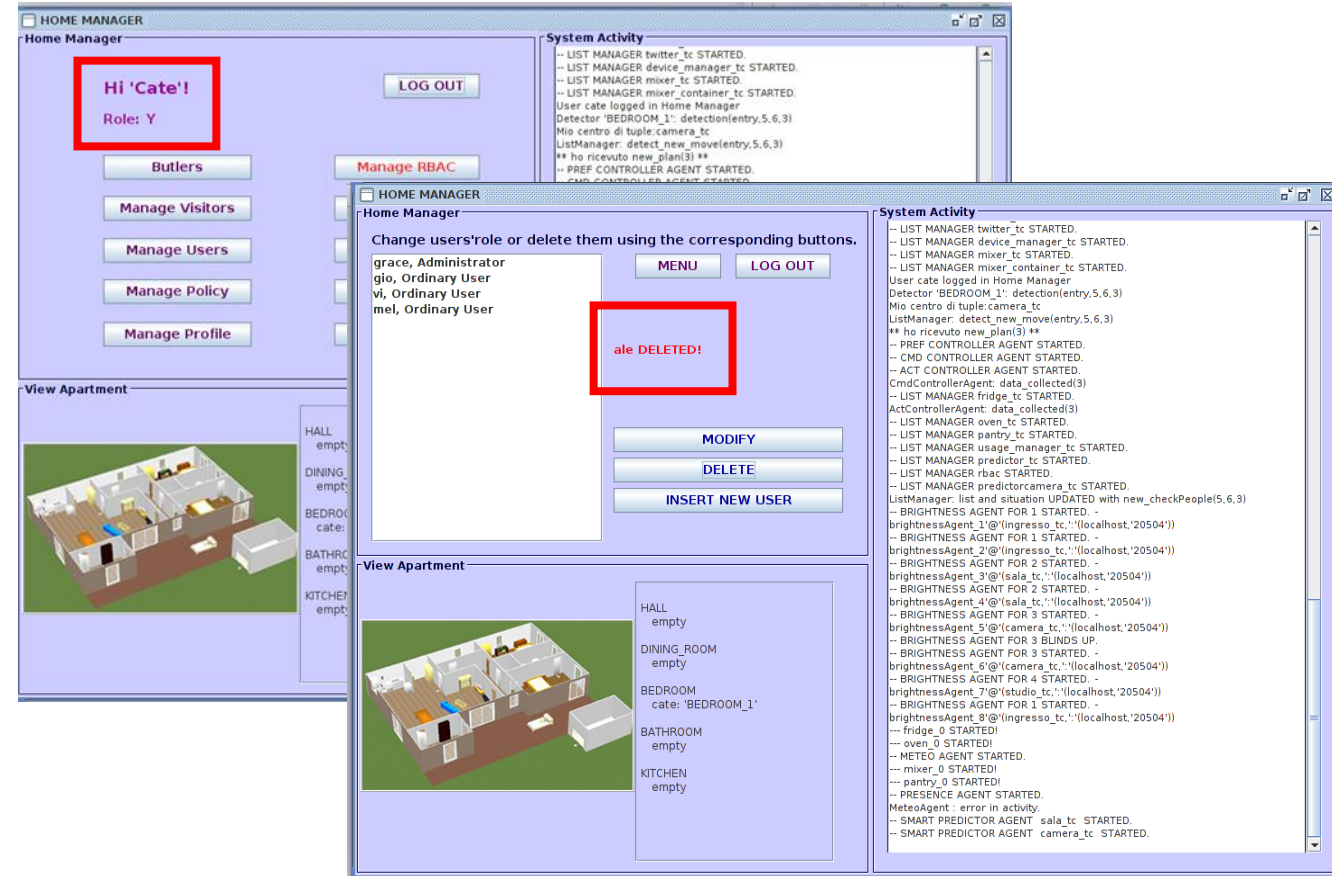
- Usato per trovare idiomi di codice che portano ad errori



White box: Database

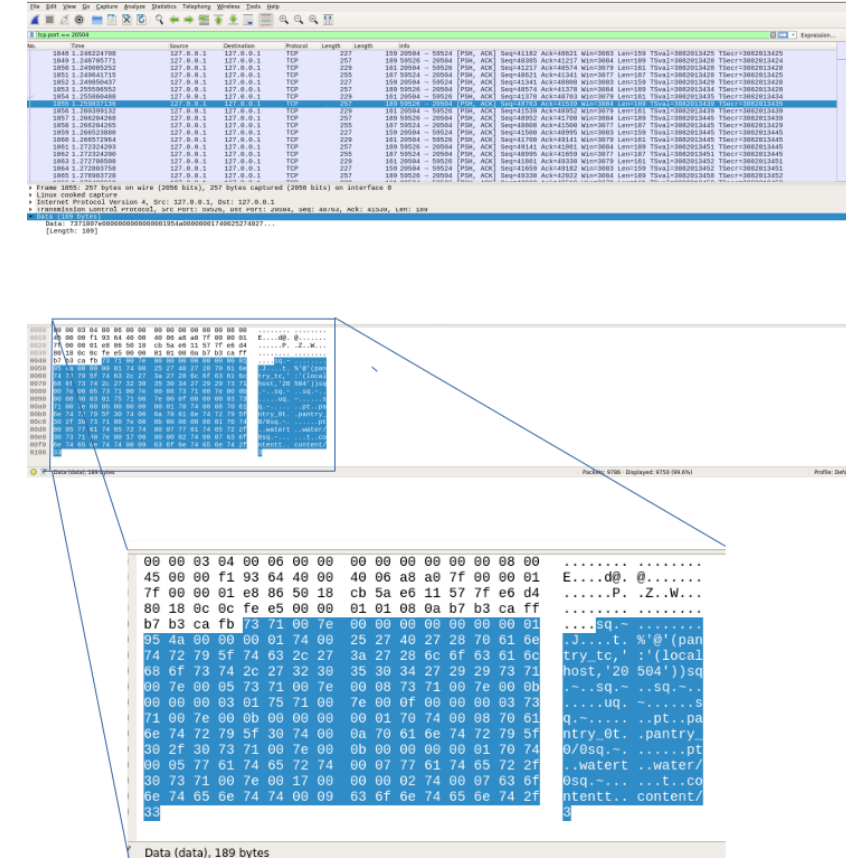
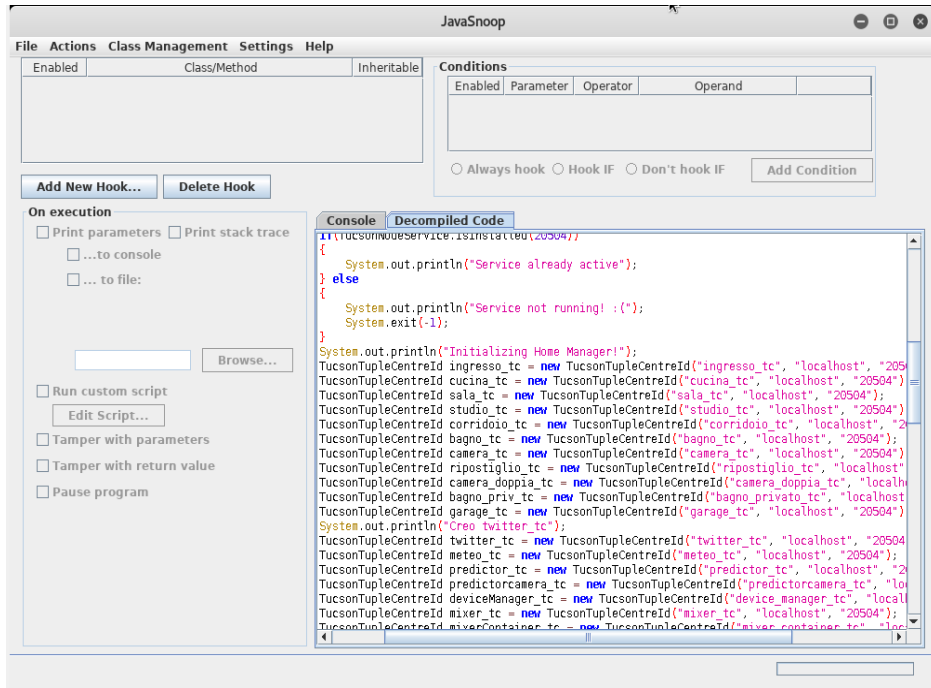
I file dove sono contenuti
tutti i dati sono in chiaro ma
soprattutto modificabili

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<persistence>
  <snapshot tc="'@(db,':'(localhost,'20504'))" time="2018-08-31_16.33.22">
    <tuples>
      <tuple>device(1,'Stereo Philips MCM 190/22',20,'on;off;cd;tuner','R',2)</tuple>
      <tuple>device(2,'TV Plasma Samsung PS 42C7H',20,'on;off','R',2)</tuple>
      <tuple>device(3,'TV Plasma Panasonic TX-32PS12D',20,'on;off','R',3)</tuple>
      <tuple>device(4,'Washer Hoover Vision VHD816PI-30',1.52,'prog_A;prog_B;prog_C;prog_D;prog_E;off','W',4)</tuple>
      <tuple>device(5,'Captain Oven',40,'on;off','E',5)</tuple>
      <tuple>device(6,'LivingRoom Conditionair',30,'on;off','E',2)</tuple>
      <tuple>device(7,'Riscaldamento hot',30,'on;off','E',2)</tuple>
      <tuple>device(8,'BedRoom Conditionair',30,'on;off','E',3)</tuple>
      <tuple>washer_programs(1,4,prog_A,1000)</tuple>
      <tuple>washer_programs(2,4,prog_B,1500)</tuple>
      <tuple>washer_programs(3,4,prog_C,2000)</tuple>
      <tuple>washer_programs(4,4,prog_D,1000)</tuple>
      <tuple>washer_programs(5,4,prog_E,1800)</tuple>
      <tuple>sensor(1,'HALL_1',1)</tuple>
      <tuple>sensor(2,'HALL_2',1)</tuple>
      <tuple>sensor(3,'DINING_ROOM_1',2)</tuple>
      <tuple>sensor(4,'DINING_ROOM_2',2)</tuple>
      <tuple>sensor(5,'BEDROOM_1',3)</tuple>
      <tuple>sensor(6,'BEDROOM_2',3)</tuple>
      <tuple>sensor(7,'BATHROOM',4)</tuple>
      <tuple>sensor(8,'CAMERA_hall_1',1)</tuple>
      <tuple>visitor(1,'Patrick','Jones')</tuple>
      <tuple>visitor(2,'Clare','Williams')</tuple>
      <tuple>visitor(3,'Julia','Jones')</tuple>
      <tuple>user([4,'Grace','Smith',grace,grace,'A',22,28,'3-3;2-2;2-1'])</tuple>
      <tuple>user([6,'Cate','Smith',cate,cate,'A',22,28,'3-3;2-2;2-1'])</tuple>
      <tuple>user([5,'Alex','Smith',ale,ale,'A',15,15,'3-3'])</tuple>
      <tuple>user([3,'George','Smith',glo,glo,'O',22,28,'2-1;3-3'])</tuple>
      <tuple>user([1,'Jack','Smith',vi,vi,'O',24,28,'3-3;2-1'])</tuple>
      <tuple>user([2,'Henry','Smith',mel,mel,'O',21,24,'2-2'])</tuple>
      <tuple>meteo_site('OpenWeatherMap','http://api.openweathermap.org/data/2.5/weather?q=', '/OpenWeatherMap_Logo.png')</tuple>
      <tuple>meteo_site('Google','http://api.wunderground.com/api/2cae48e983982ec4/conditions/Lang:it/q/', '/google-
iconBis.png')</tuple>
      <tuple>meteo_site('Yahoo','http://weather.yahooapis.com/forecastrss?w=', '/Yahoo.jpg')</tuple>
      <tuple>timer_prediction(900000)</tuple>
      <tuple>lamp(1,'HALL_FRONT_DOOR',1)</tuple>
      <tuple>lamp(2,'HALL_FRONT_BATHROOM',2)</tuple>
      <tuple>lamp(3,'KITCHEN_PART',3)</tuple>
      <tuple>lamp(4,'LIVROOM_PART',4)</tuple>
      <tuple>lamp(5,'BEDROOM_PC_DESK',5)</tuple>
      <tuple>lamp(6,'BEDROOM_MAIN_LIGHT',6)</tuple>
    </tuples>
  </snapshot>
</persistence>
```



Black box: Javasnnoop e Wireshark

Javasnnoop per trovare la porta di comunicazione



Wireshark per intercettare la comunicazione

Analisi del rischio per sviluppi futuri

Pensato per sviluppi nel distribuito.

Requisiti necessari per avere:

- Riservatezza
- Immunità
- Disponibilità
- Integrità
- Protezione della manutenzione
- Scoperta delle intrusioni

Minacce	Livello di rischio
Furto credenziali amministratore	Alto
Furto credenziali utente	Medio
Furto credenziali visitatore	Basso
Eliminazione credenziali amministratore	Alto
Eliminazione credenziali utente	Basso
Creazione di un amministratore non autorizzato	Alto
Cambio ruolo ad un livello superiore	Alto
Furto preferenze	Basso
Accensione di intelligent-device non autorizzato	Alto
Disattivazione di sensori di movimento	Medio
Attacco al database	Alto
Denial of Service	Alto
Sniffing	Medio
Rootkit	Alto

Conclusioni e Sviluppi futuri

- Trovate vulnerabilità da eliminare
- Stilata analisi del rischio

Sviluppi futuri:

- Cifrare i file del database e renderli non-modificabili dall'esterno
- Mettere in sicurezza la comunicazione con TuCsON
- Seguire le linee guida dell'analisi del rischio per nuovi componenti

GRAZIE PER L'ATTENZIONE