Protection and security of information systems

Security check

prof. Ph.D. Krešimir Fertalj

University of Zagreb

Faculty of Electrical Engineering and Computing

Zaštita i sigurnost informacijskih sustava

Provjera sigurnosti

prof. dr. sc. Krešimir Fertalj

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Creative Commons

- **you are free to:**
  - **share**—reproduce, distribute and communicate the work to the public
  - **remix**—rework the work
- **under the following conditions:**
  - **appointment**. You must acknowledge and attribute the authorship of the work in a manner specified by the author or licensor (but not in a manner that suggests that you or your use of their work has their direct endorsement).
  - **non-commercial**. You may not use this work for commercial purposes.
  - **shares under the same conditions**. If you modify, transform, or create using this work, you may distribute the adaptation only under a license that is the same or similar to this one.

In the case of further use or distribution, you must make clear to others the license terms of this work. The best way to do this is to link to this website.

Any of the above conditions may be waived with the permission of the copyright holder.

Nothing in this license infringes or limits the author's moral rights.

The text of the license was taken from http://creativecommons.org/.

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.

Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

Security check

Security Testing

Provjera sigurnosti

Security Testing

Software correctness check (general)

- Program testing, program verification, program testing
  - detection of errors or defects within the program
  - the success of the test is proportional to the number of errors found
- According to the purpose of testing
  - Verification - verification of correctness (good implementation)
  - Validation - confirmation of validity (real, acceptable product)
- According to the check object
  - Structural (white-box testing) - source code
  - Functional (black-box) - compilation
- According to the verification method
  - static analysis - no startup, source code or .NET MSIL, Java Bytecode
  - dynamic analysis - by running, which does not exclude the source code

Provjera ispravnosti softvera (općenito)

- Testiranje programa, provjeravanje programa, ispitivanje programa
  - otkrivanje pogrešaka odnosno nedostataka unutar programa
  - uspješnost testa razmjerna je broju pronađenih pogrešaka
- Prema svrsi testiranja
  - Verifikacija - ovjera ispravnosti (dobra provedba)
  - Validacija - potvrda valjanosti (pravi, prihvatljiv proizvod)
- Prema objektu provjere
  - Strukturalno (white-box testing) - izvorni kod
  - Funkcionalno (black-box) - kompilat
- Prema načinu provjere
  - statička analiza - bez pokretanja, izvorni kod ili .NET MSIL, Java Bytecode
  - dinamička analiza - pokretanjem, što ne isključuje izvorni kod

Key terms

- **["normal"] Test**-verifies that some aspect of the software is correct

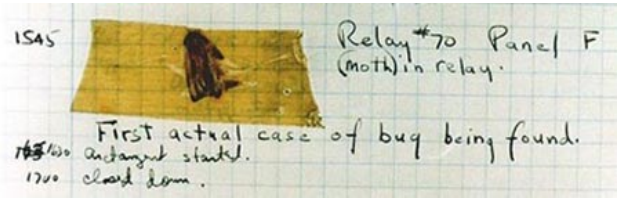
- **Security test**-tries to prove that some part is not working properly

-**Error**(error) - an omission by the programmer, eg due to misunderstanding
  - -leads to one or more failures
  - -we distinguish in relation to "error" which means an unwanted state, i.e. a malfunction

-**Failure**(fault), defect, informally bug - defective part of the code
  - -eg wrongly assuming that an array is indexed by 1 instead of 0 causes an array element access failure

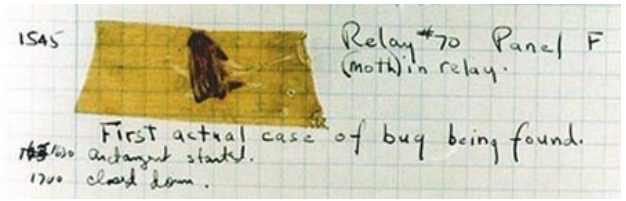
-**A standstill**in operation (failure) - condition caused by one or more malfunctions
  - -eg system shutdown due to "buffer overrun" error

-**Correction**(Fix) **-** state of repair



Ključni pojmovi

- **[„normalan”] Test** - provjerava je li neki aspekt softvera ispravan
- **Test sigurnosti** - nastoji dokazati da neki dio ne radi kako treba
- **Pogreška** (error) - propust programera, npr. radi nerazumijevanja
  - dovodi do jednog ili više kvarova
  - razlikujemo u odnosu na "pogrešku" koja znači neželjeno stanje, tj. kvar
- **Kvar** (fault), defekt (defect), neformalno bug - neispravan dio koda
  - npr. pogrešna pretpostavka da se polje indeksira od 1 umjesto 0 izaziva kvar pristupa elementu polja
- **Zastoj** u radu (failure) - stanje izazvano jednim ili više kvarova
  - npr. prestanak rada sustava zbog kvara "buffer overrun"
- **Ispravak** (Fix) - stanje popravka



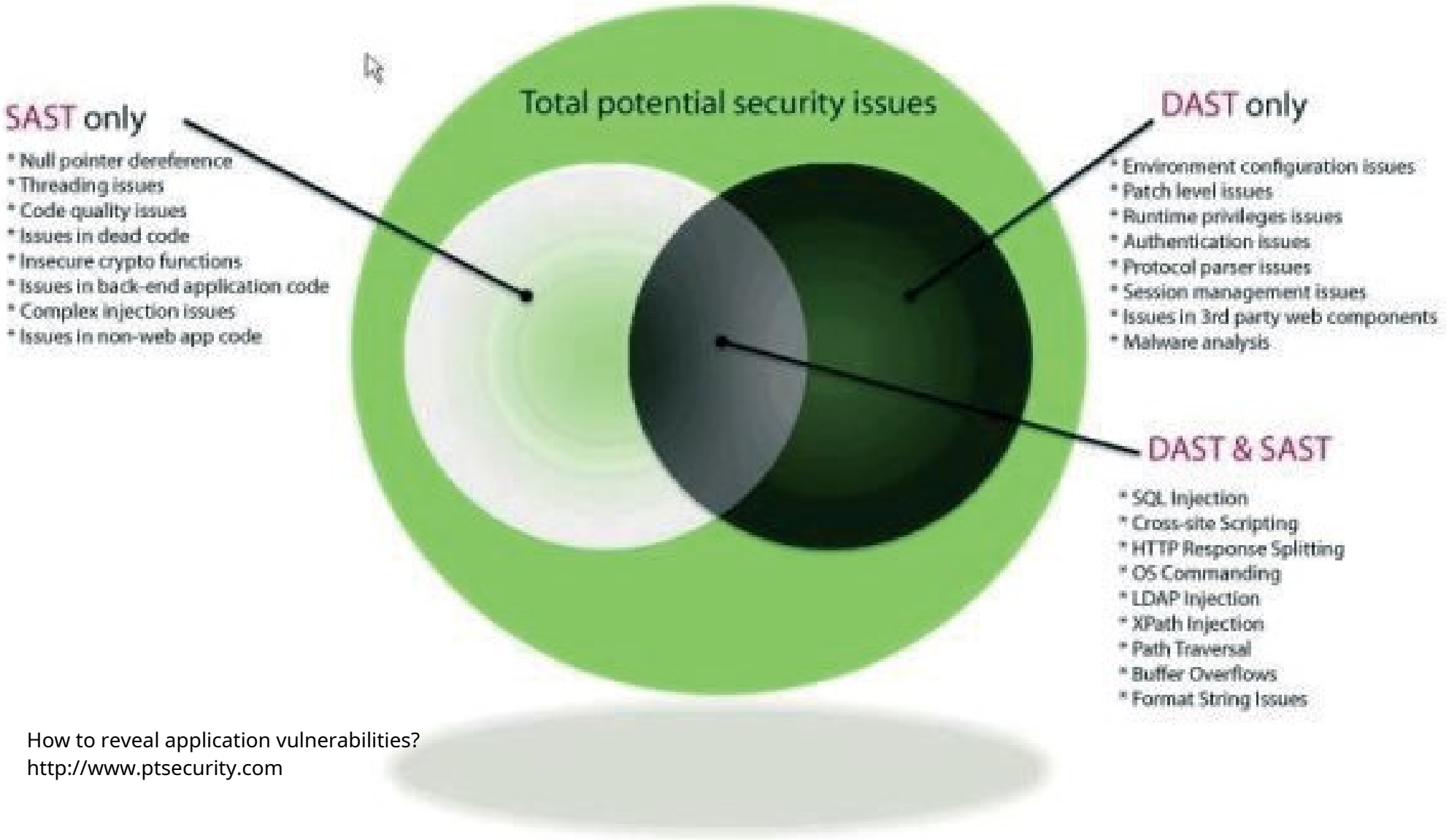
Application security verification procedures

- Supervision ("Technical Reviews", "Code Reviews", "Inspections", ...)
  - testing tends to cause deadlock, monitoring looks for malfunction
- Static Application Security Testing (**SAST**) # white-box static
  - which does not require execution
  - access to the source code on the client and on the server
- Dynamic Application Security Testing (**DAST**) # black-box dynamic
  - requires execution
  - does not have access to the source code and operating environment on the server
- Interactive Application Security Testing (**IAST**) # white-box dynamic
  - dynamic with access to the source code and operating environment on the server
- Source code analysis - static or dynamic with access to the entire code

Postupci provjere sigurnosti aplikacija

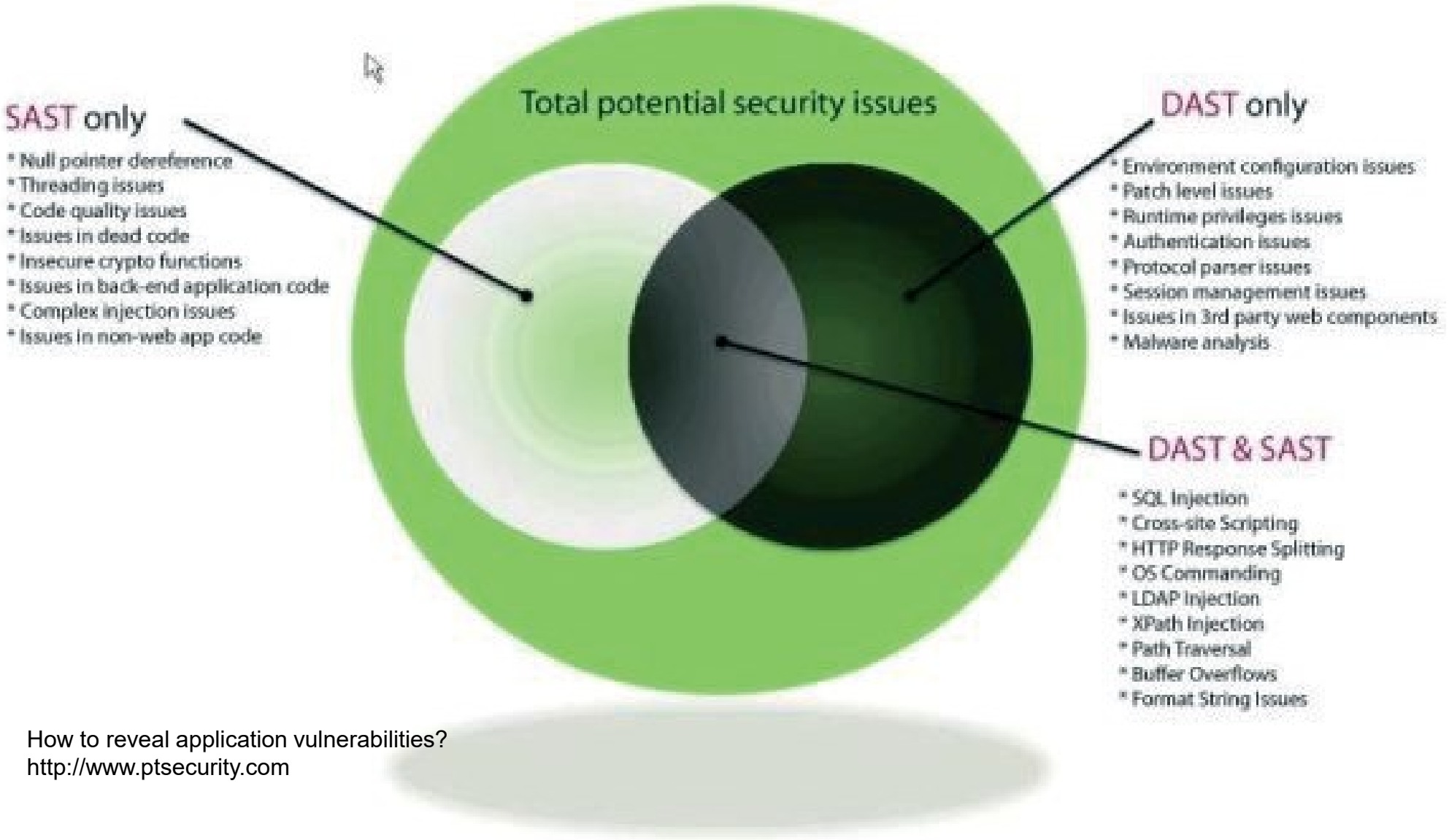
- Nadzor (“Technical Reviews”, “Code Reviews”, "Inspections", ...)
  - testiranje nastoji izazvati zastoj, nadzor traži neispravnost
- Static Application Security Testing (**SAST**) # white-box statička
  - koja ne zahtijeva izvršenje
  - pristup izvornom kodu na klijentu i na serveru
- Dynamic Application Security Testing (**DAST**) # black-box dinamička
  - zahtijeva izvršenje
  - nema pristup izvornom kodu i pogonskoj okolini na serveru
- Interactive Application Security Testing (**IAST**) # white-box dinamička
  - dinamička s pristupom izvornom kodu i pogonskoj okolini na serveru
- Analiza izvornog koda - statička ili dinamička s pristupom čitavom kodu

How to reveal application vulnerabilities?



How to reveal application vulnerabilities?
http://www.ptsecurity.com

How to reveal application vulnerabilities?



How to reveal application vulnerabilities?
http://www.ptsecurity.com

Supervision

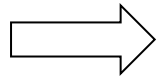
Security Review, Code Reviews, Inspection

Nadzor

Security Review, Code Reviews, Inspection

Revision, review (peer review)

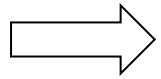
- Variants



  - inspection
  - Team review
  - Walkthrough

- Use it
  - finding defects earlier in the life cycle - up to 80% before testing
  - finding defects with less effort than testing
    - IBM - review 3.5 h/defect, test 15-25 h/defect
  - finding different defects than by testing - design and requirements problems
  - teaching developers - not to repeat the same mistakes

Revizija, recenzija (peer review)



- Varijante
  - Inspekcija (inspection)
  - Timski pregled (team review)
  - Prohod (walkthrough)

- Koristi
  - nalaženje defekata ranije u životnom ciklusu - do 80% prije testiranja
  - nalaženje defekata s manje napora nego testiranjem
    - IBM - pregled 3.5 h/defekt, test 15-25 h/defekt
  - nalaženje drugačijih defekata nego testiranjem - problemi dizajna i zahtjeva
  - poduka razvojnika - da ne ponavljaju iste pogreške

Inspection

- Formal process
  - Thorough coverage of separate roles
    - Moderator - leads the meeting, monitors problems
    - The reader - paraphrases (retells) the code, not the author
    - Recorder - records defects
    - Author - provides code context, explains, fixes after review
  - Checklists for specific objectives
  - Data collection for error tracking
  - Determining the need for subsequent inspections

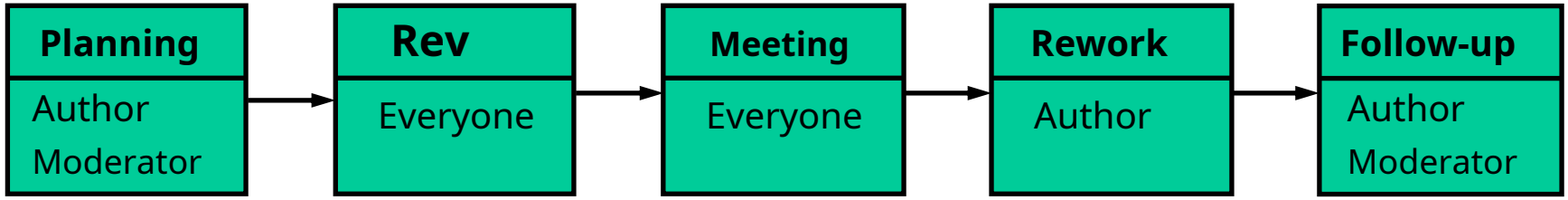
- Extensive documentation of effectiveness
  - 16-20 defects/kLOC inspections vs. 3 defects/kLOC passes

Inspekcija

- Formalni proces
  - Temeljita pokrivenost odvojenim ulogama
    - Moderator - vodi sastanak, prati probleme
    - Čitalac - parafrazira (prepričava) kod, nije autor
    - Zapisničar - evidentira defekte
    - Autor - osigurava kontekst koda, objašnjava, popravlja nakon pregleda
  - Kontrolne liste za specifične ciljeve
  - Prikupljanje podataka za praćenje pogrešaka
  - Određivanje potrebe za narednim inspekcijama

- Opsežna dokumentacija učinkovitosti
  - 16-20 defekt/kLOC inspekcije naspram 3 defekt/kLOC prohoda

Inspection process



- Planning
  - the author initiates, the moderator equips, the meeting prepares the inspection package
- Preparation
  - reviewers review, use checklists and analytical tools, mark defects
- Meeting
  - the reader recounts, the reviewers comment and question, the recorder records
  - the team concludes the code evaluation
- Processing
  - the author fixes
- Control (follow-up)
  - the moderator verifies the correctness of the changes, the author reports the code (check-in)

Proces inspekcije

- Planiranje
  - autor inicira, moderator ekipira, skupa pripreme inspekcijski paket
- Priprema
  - recenzenti pregledavaju, koriste kontrolne liste i analitičke alate, označavaju defekte
- Sastanak
  - čitalac prepričava, recenzenti komentiraju i zapitkuju, zapisničar evidentira
  - tim zaključuje procjenu koda
- Prerada
  - autor popravlja
- Kontrola (follow-up)
  - moderator verificira korektnost promjena, autor prijavljuje kod (chek-in)

Variants

- Team review
  - Team inspection ("light" inspection)
  - Persons: moderator, reviewers (who are not code authors)
  - Modules or smaller sets of classes
  - 1-2 hours, < 1 kLOC

- Walkthrough
  - The author leads the meeting and explains the code
  - A less formal process
  - Undefined process
  - No checklists or metrics

Varijante

- Timski pregled
  - Timski pregled ("lagana" inspekcija)
  - Osobe: moderator, recenzenti (koji nisu autori koda)
  - Moduli ili manji skupovi klasa
  - 1-2 sata, < 1 kLOC
- Prohod (walkthrough)
  - Autor vodi sastanak i objašnjava kod
  - Manje formalan proces
  - Nedefiniran proces
  - Nema kontrolnih lista ili metrike

Other procedures

- Pair programming
  - Guide (driver) and observer (observer, navigator)
  - Change of roles and partners

- *Peer deskcheck*
  - Only one reviewer with the author
  - informal review
  - may include checklists and other procedures

- *Pass around* (circular addition?)
  - multiple, simultaneous *Peer deskcheck*
  - multiple reviewers (same code)

Drugi postupci

- Programiranje u paru
  - Vodič (driver) i promatrač (observer, navigator)
  - Zamjena uloga ali i partnera
- *Peer deskcheck*
  - Samo jedan recenzent uz autora
  - neformalna recenzija
  - može uključiti kontrolne liste i druge postupke
- *Pass around* (kružno dodavanje?)
  - višestruki, istodobni *Peer deskcheck*
  - više recenzenata (istog koda)

Static check

Static Analysis

Statička provjera

Static Analysis

Static analysis

- SAST (Quick and Dirty)
  - Code analysis without execution
  - It covers everything but testing
  - Using the code analyzer
  - It can be part of a code review

- Limitations: false detection and false non-recognition
  - **False Positives**-non-existent bugs, powerlessness with complex code or external
  - **False Negatives**-failure to recognize bugs, complexity of code, weakness of rules

Statička analiza

- SAST (Quick and Dirty)
  - Analiza koda bez izvršavanja
  - Obuhvaća sve osim testiranja
  - Korištenje analizatora koda
  - Može biti dio revizije koda

- Ograničenja: pogrešno otkrivanje i pogrešno neprepoznavanje
  - **False Positives** - nepostojeći bugovi, nemoć pri složenom kodu ili vanjskom
  - **False Negatives** - neprepoznavanje bugova, složenost koda, slabost pravila

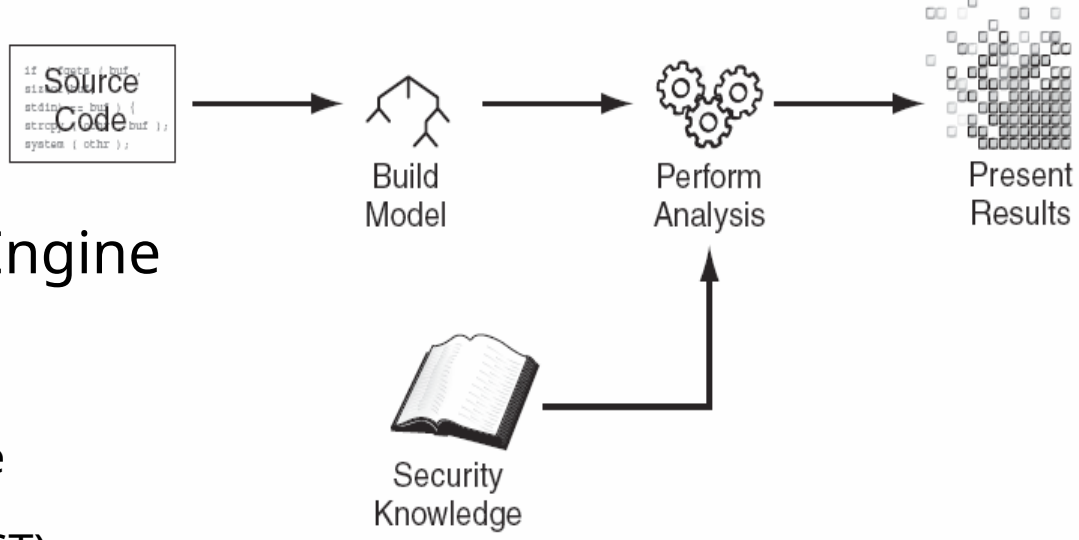
Types of static analysis

- Type checking - part of the programming language
  - ex. int i = "abc";
- Style checking - good practices
  - Rules - spaces/spaces, nomenclature, comments, ...
- Program understanding - inferring meaning
  - All method usage, global variable declaration finding, ...
- Property checking - ensuring that there is no bad behavior
  - For example memory leak : if (malloc() == NULL)
- Program verification (Program verification) - ensuring correct behavior
  - For example free(mem);
- Bug finding - detection of possible errors
  - Bug patterns

Vrste statičke analize

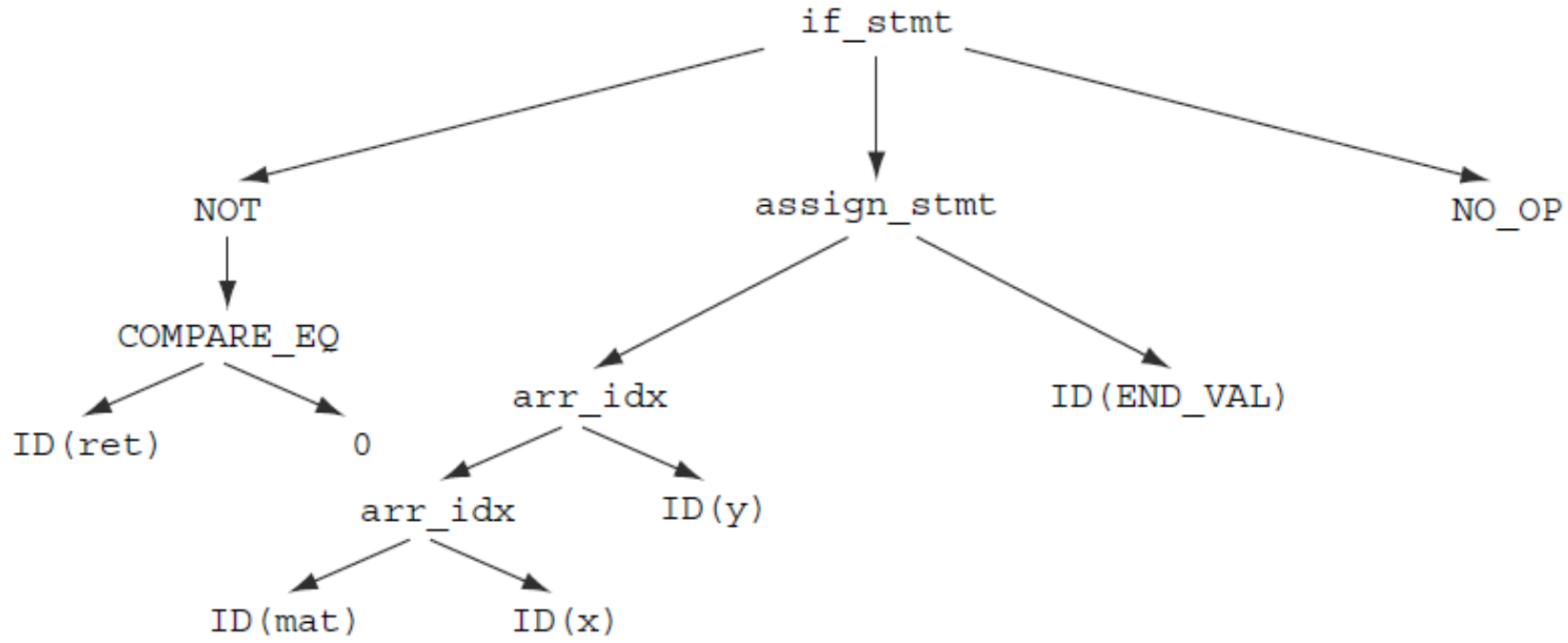
- Provjera tipova (Type checking) - dio programskog jezika
  - pr. int i = ”abc”;
- Provjera stila (Style checking) - dobre prakse
  - Pravila - praznine/proredi, nazivlje, komentari, …
- Razumijevanje programa (Program understanding) - zaključivanje značenja
  - Sva korištenja metode, nalaz deklaracije globalnih varijabli, …
- Provjera svojstava (Property checking) - osiguranje da nema lošeg ponašanja
  - Npr. curenje memorije : if (malloc() == NULL)
- Verifikacija programa (Program verification) - osiguranje ispravnog ponašanja
  - Npr. free(mem);
- Traženje pogrešaka (Bug finding) - otkrivanje mogućih pogrešaka
  - Obrasci bugova

Mechanisms of static analysis

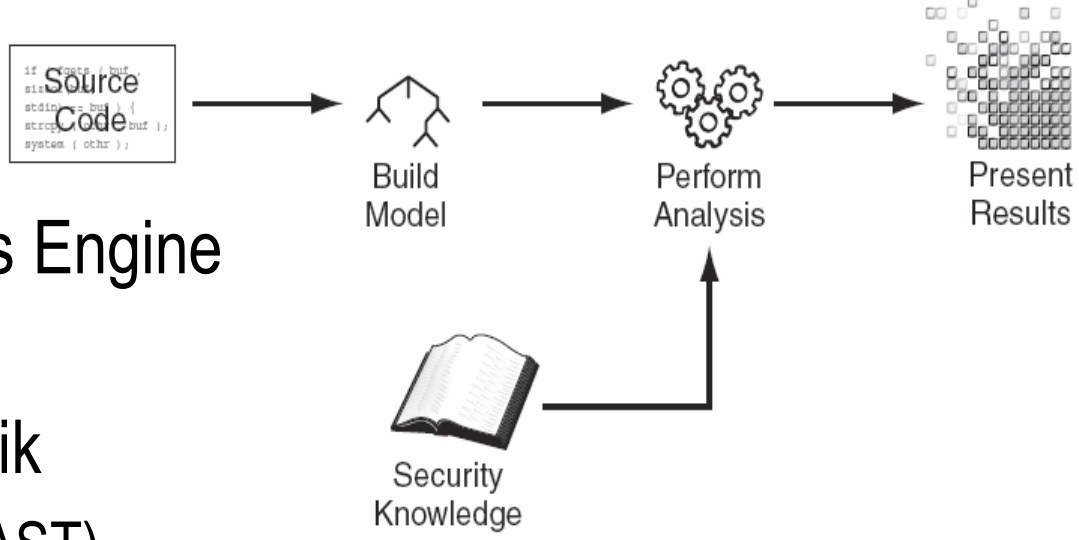


- Parser, Model Builder, Analysis Engine

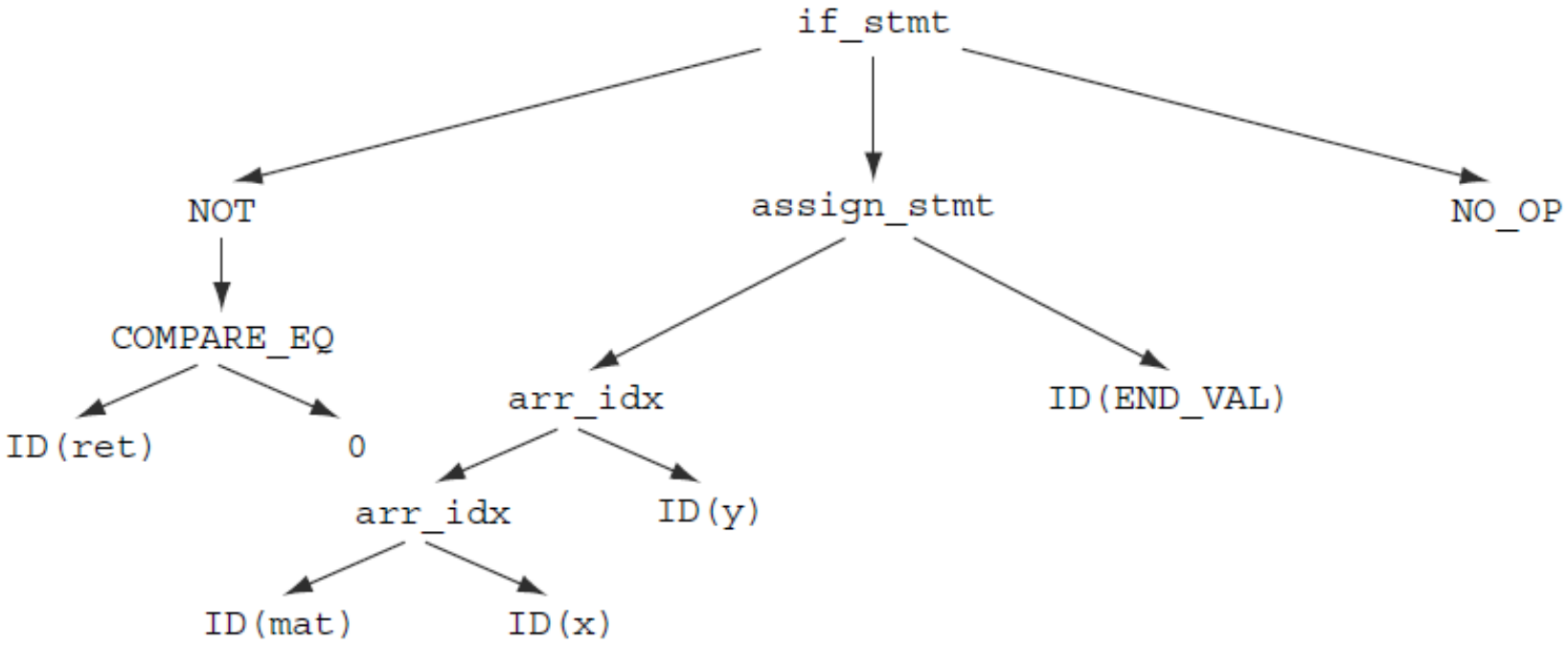
- A parser for every programming language
  - generates an Abstract Syntax Tree (AST)



Mehanizmi statičke analize



- Parser, Model Builder, Analysis Engine
- Parser za svaki programski jezik
  - generira Abstract Syntax Tree (AST)



Lexical analysis and parsing

Example, program section

```
if (ret) // probably true
    mat[x][y] = END_VAL;
```

The corresponding sequence of symbols (tokens)

IF LPAREN ID(ret) RPAREN ID(mat) LBRACKET ID(x) RBRACKET LBRACKET ID(y) RBRACKET EQUAL ID(END_VAL) SEMI

Extracted by syntax rules, parsed according to grammar productions

```
if                          { return IF; }
(                           { return LPAREN; }
)                           { return RPAREN; }
[                           { return LBRACKET; }
]                           { return LBRACKET; }
=                           { return EQUAL; }
;                           { return SEMI; }
/[ \t\n]+/                  { /* ignore whitespace */ }
/\/\/.*/                    { /* ignore comments */ }
/[a-zA-Z][a-zA-Z0-9]*"/     { return ID; }
```

```
stmt := if_stmt | assign_stmt
if_stmt := IF LPAREN expr RPAREN stmt
expr := lval
assign_stmt := lval EQUAL expr SEMI
lval = ID | arr_access
arr_access := ID arr_index+
arr_idx := LBRACKET expr RBRACKET
```

Tehnike analize

- Leksička analiza (Lexical Analysis) i parsiranje
  - Primjer, programski odsječak
  - Pripadni slijed simbola (tokena)

```
if (ret) // probably true
  mat[x][y] = END_VAL;
```

```
IF LPAREN ID(ret) RPAREN ID(mat) LBRACKET ID(x) RBRACKET
LBRACKET ID(y) RBRACKET EQUAL ID(END_VAL) SEMI
```

  - Izdvojen sintaksnim pravilima, parsiran prema produkcijama gramatike

```
if                          { return IF; }
(                           { return LPAREN; }
)                           { return RPAREN; }
[                           { return LBRACKET; }
]                           { return LBRACKET; }
=                           { return EQUAL; }
;                           { return SEMI; }
/[ \t\n]+/                  { /* ignore whitespace */ }
/\/\/.*/                    { /* ignore comments */ }
/[a-zA-Z][a-zA-Z0-9]*"/     { return ID; }
```

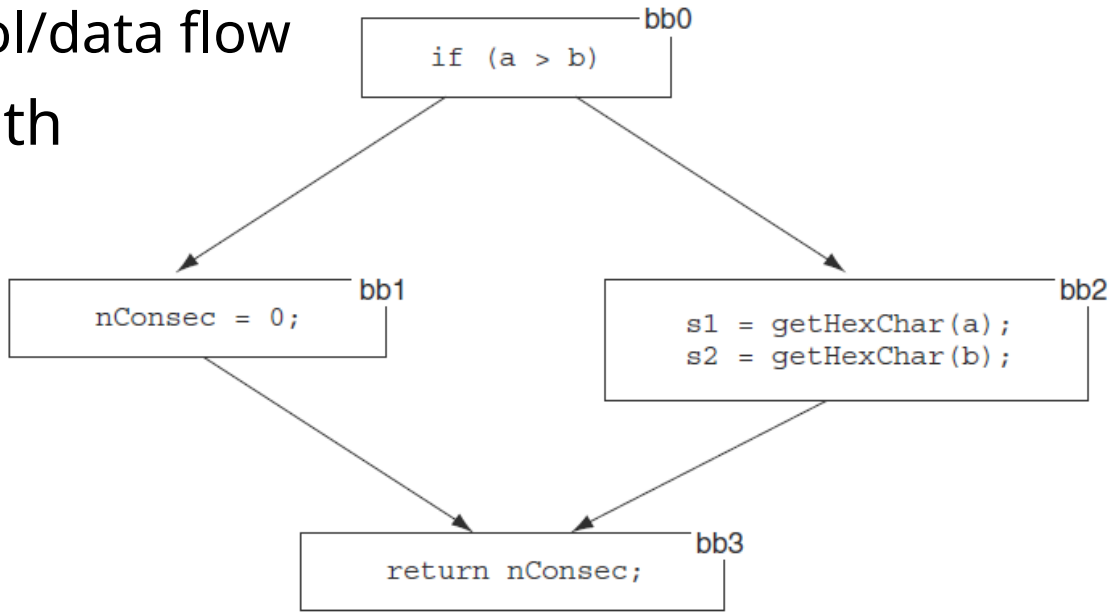
```
stmt := if_stmt | assign_stmt
if_stmt := IF LPAREN expr RPAREN stmt
expr := lval
assign_stmt := lval EQUAL expr SEMI
lval = ID | arr_access
arr_access := ID arr_index+
arr_idx := LBRACKET expr RBRACKET
```

Data Flow Analysis

- Collecting information about the data stream when the program is executed while it is stopped
- Semantic analysis - based on AST and symbol table

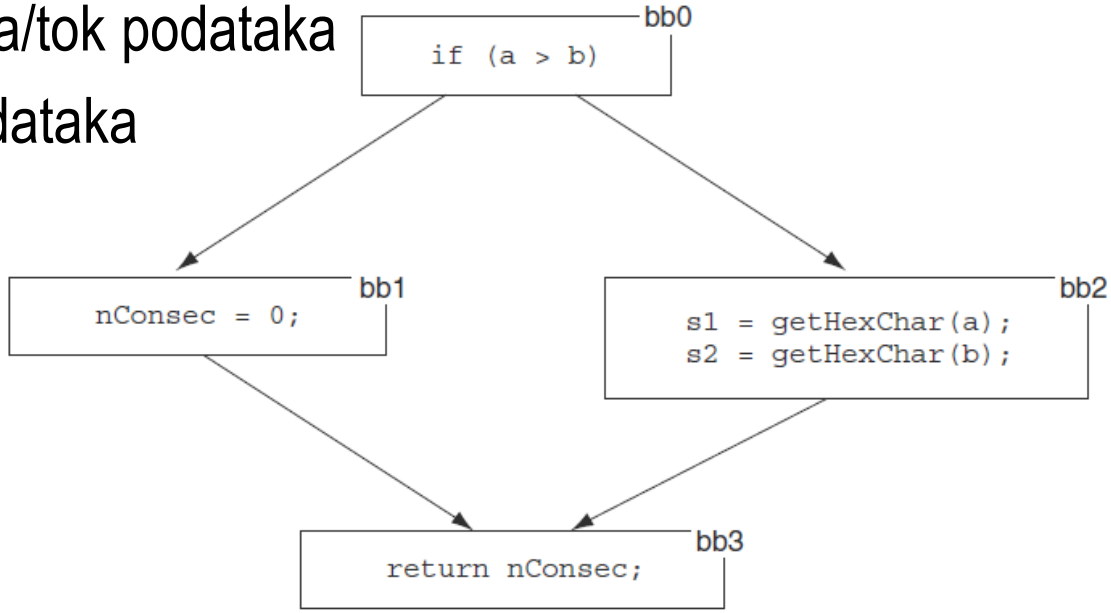
- Basic block - a sequence of statements that does not stop or branch except at the end
- Control Flow Analysis – control/data flow
- Control Flow Path - data path

- Flow control chart
  - Control Flow Graph (CFG)
  - Example: graph with 4 basic blocks



Tehnike analize (2)

- Analiza toka podataka (Data Flow Analysis)
  - Prikupljanje informacija o kolanju podataka pri izvršenju programa dok je zaustavljen
  - Semantička analiza - na temelju AST i tablice simbola
  - Osnovni blok - slijed naredbi koji se ne zaustavlja ili grana osim na kraju
  - Control Flow Analysis – kontrola/tok podataka
  - Control Flow Path - putanja podataka
- Graf kontrole toka
  - Control Flow Graph (CFG)
  - Primjer: graf s 4 osnovna bloka



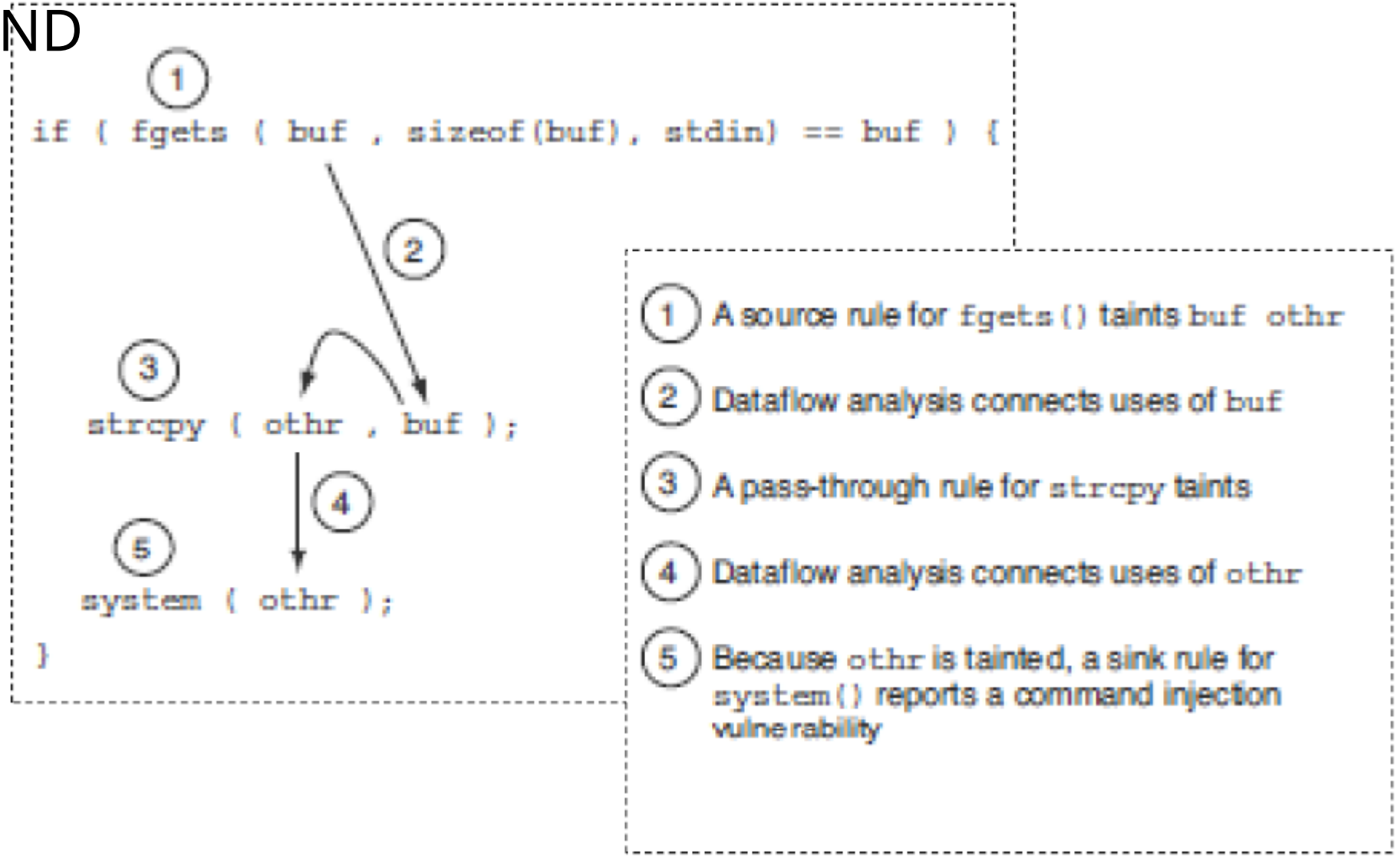
- Taint Analysis
  - Identification of variables *soiled* by user input
  - Monitoring their propagation according to possibly vulnerable functions (*son*)
  - If they are not disinfected before the drain - vulnerability
- The rules of blob propagation
  - Source rules - data entry
    - Orders *read(), getenv(), getpass(), gets().*
  - Sink rules - locations that should not receive dirty data
    - Example, Java *Statement.executeQuery()*, C *strcpy()*
  - Pass-through rules
    - If it is *string* soiled and *trim(string)* will be dirty
  - Cleanse rules - input validation
  - Entry-point rule - similar to the source, e.g. *main(...)*

Tehnike analize (3)

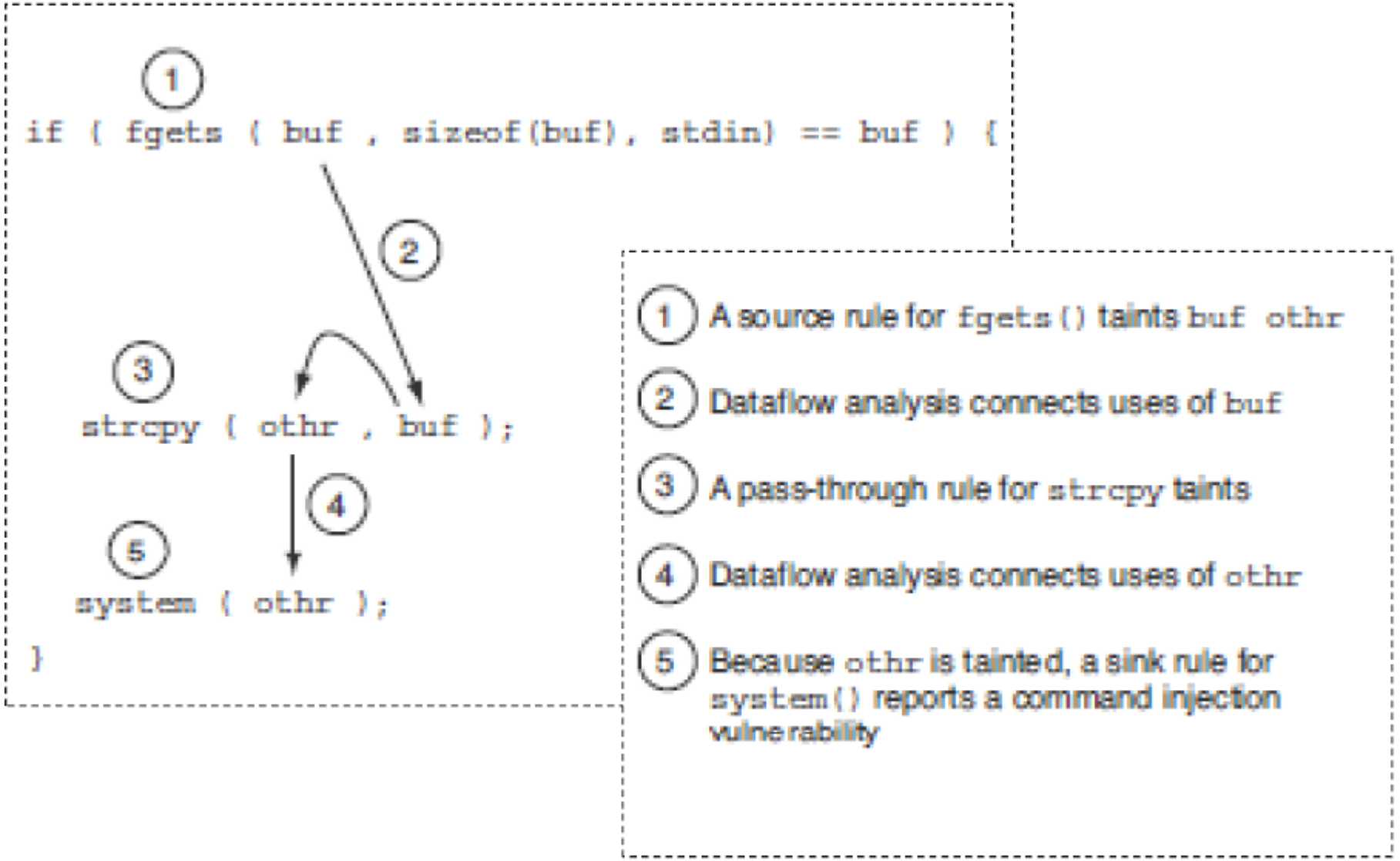
- Analiza „mrlja” (Taint Analysis)
  - Identifikacija varijabli *uprljanih* korisničkim unosom
  - Praćenje njihove propagacije prema moguće ranjivim funkcijama (*sink*)
  - Ako nisu dezinficirane prije odvoda - ranjivost
- Pravila propagacije mrlja
  - Pravila izvora (source rules) - unos podataka
    - Naredbe *read(), getenv(), getpass(), gets().*
  - Pravila slivnika (sink rules) - lokacije koje ne bi smjele primiti prljave podatke
    - Primjer, Java *Statement.executeQuery()*, C *strcpy()*
  - Pravila propuštanja (pass-through)
    - Ako je *string* zaprljan i *trim(string)* će biti zaprljan
  - Pravila čišćenja (cleanse rules) - validacija unosa
  - Pravila početka (entry-point rule) - slično izvoru, npr. *main(…)*

Example of static analysis

- AND



Primjer statičke analize



Advantages and disadvantages of static analysis

- Advantages
  - Full code coverage (code coverage) - in theory
  - The potential to confirm the absence of entire classes of bugs
  - It catches *bugs* different compared to dynamic analysis

- Weaknesses
  - High false detection rate
  - Difficult test shaping
  - Complexity of construction (tool) - "parser for every language"
    - not enough when using additional frameworks or libraries
  - Not having the entire source code in practice (OS, shared libraries, DLLs, ...)

Prednosti i nedostaci statičke analize

- Prednosti
  - Potpuna pokrivenost koda (code coverage) - u teoriji
  - Potencijal potvrde izostanka čitavih klasa bugova
  - Hvata *bugove* različite u odnosu na dinamičku analizu

- Slabosti
  - Visok postotak pogrešnog otkrivanja
  - Teško oblikovanje testa
  - Složenost izgradnje (alata) - „parser za svaki jezik"
    - nedovoljno kada se koriste dodatni okviri ili biblioteke
  - Neimanje cjelokupnog izvornog koda u praksi (OS, shared libraries, DLLs, …)

Tools for static analysis

- https://www.owasp.org/index.php/Source_Code_Analysis_Tools

- StyleCophttps://github.com/StyleCop/StyleCop - C#
- CodeSmarthttp://www.axtools.com/ - C#, C++, VB.NET
- NDependhttp://www.ndepend.com/ - C#, jDepend for Java

- VS Code Analysis (FxCop, Roslyn analyzers) - C#, C/C++, ...
- PMD - Java, C, C++, C#, Groovy, PHP, Ruby, Fortran, JavaScript, PLSQL, ...
- Fortify Source Code Analyzer - 25 languages
- Checkstyle - Java
- Klocwork K7 Suite - Java
- FindBugs, Find Security Bugs - Java
- Coverity Prevent - C#, clang, gcc

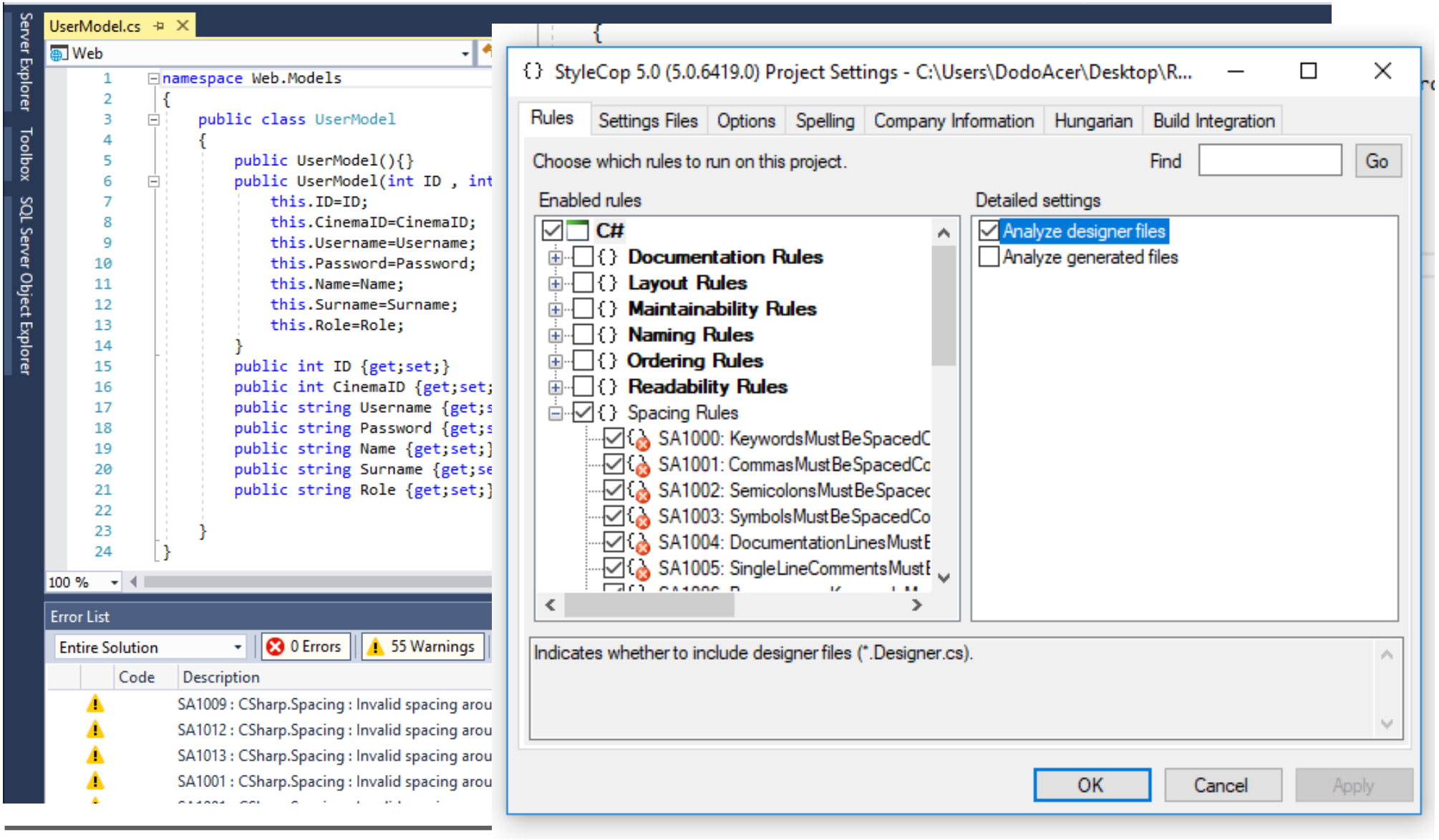
Alati za statičku analizu

- https://www.owasp.org/index.php/Source_Code_Analysis_Tools

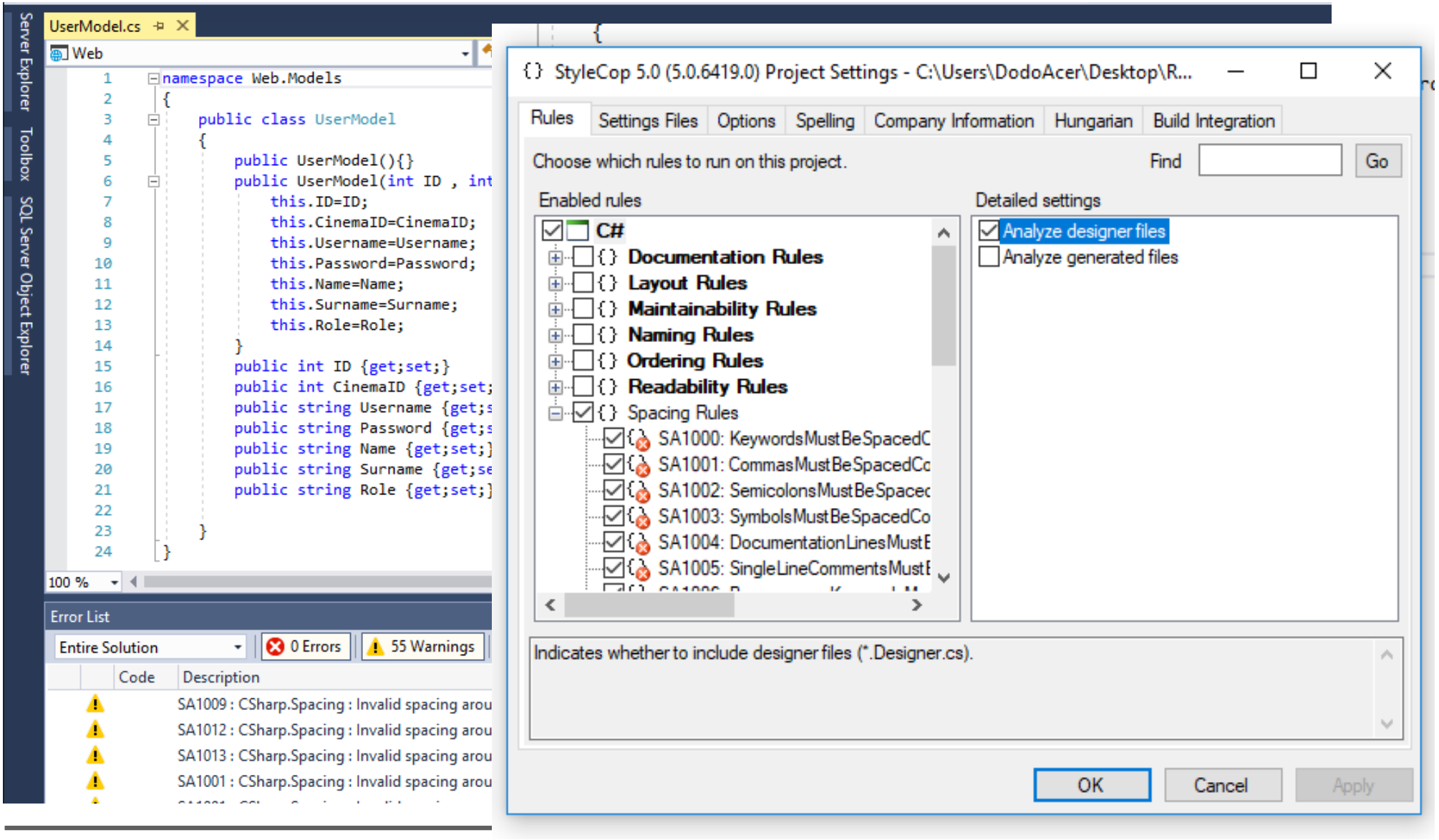
- StyleCop https://github.com/StyleCop/StyleCop - C#
- CodeSmart http://www.axtools.com/ - C#, C++, VB.NET
- NDepend http://www.ndepend.com/ - C#, jDepend za Javu

- VS Code Analysis (FxCop, Roslyn analyzers) - C#, C/C++, …
- PMD - Java, C, C++, C#, Groovy, PHP, Ruby, Fortran, JavaScript, PLSQL, ...
- Fortify Source Code Analyzer - 25 jezika
- Checkstyle - Java
- Klocwork K7 Suite - Java
- FindBugs, Find Security Bugs - Java
- Coverity Prevent - C#, clang, gcc

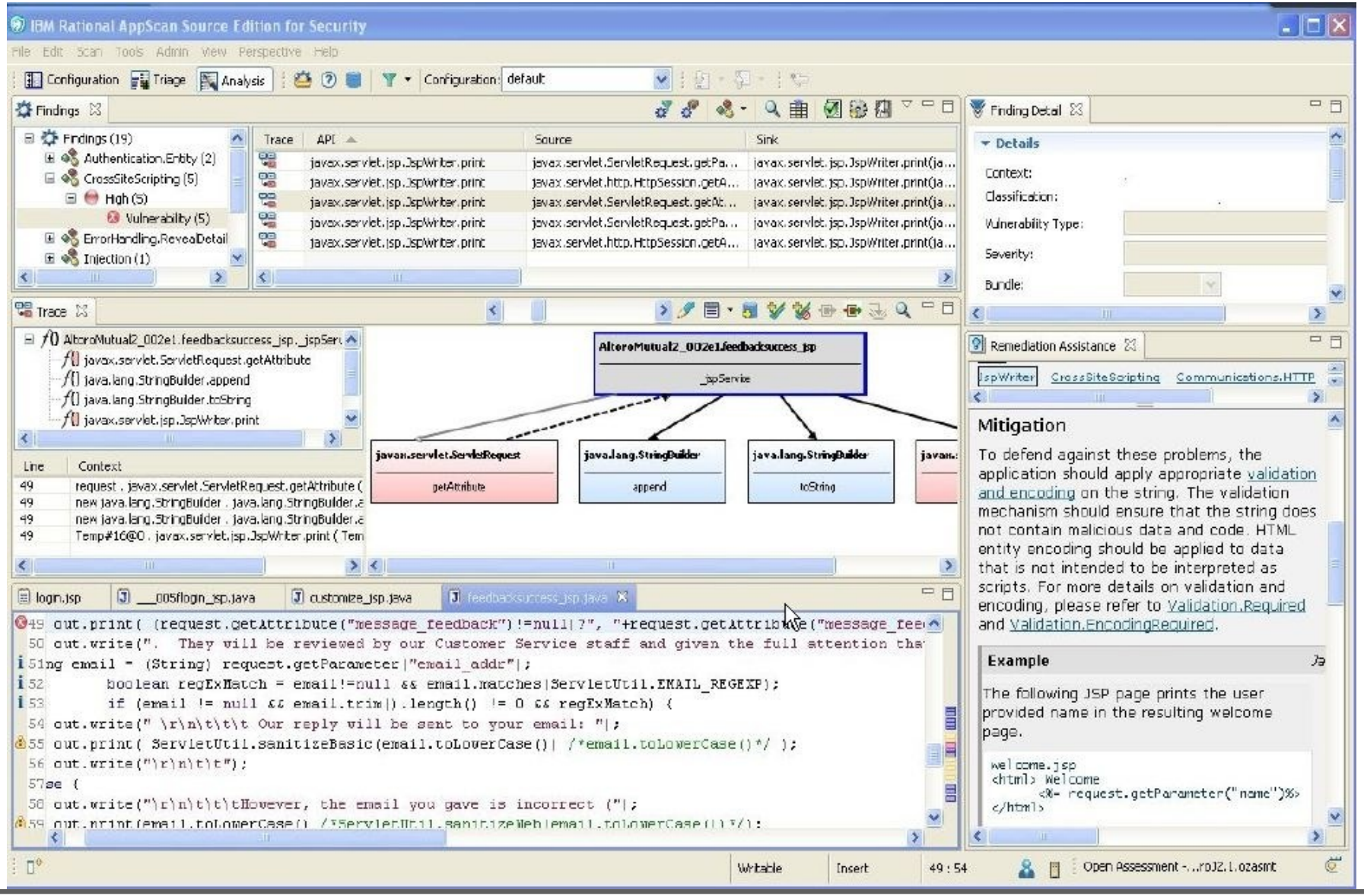
Example: StyleCop



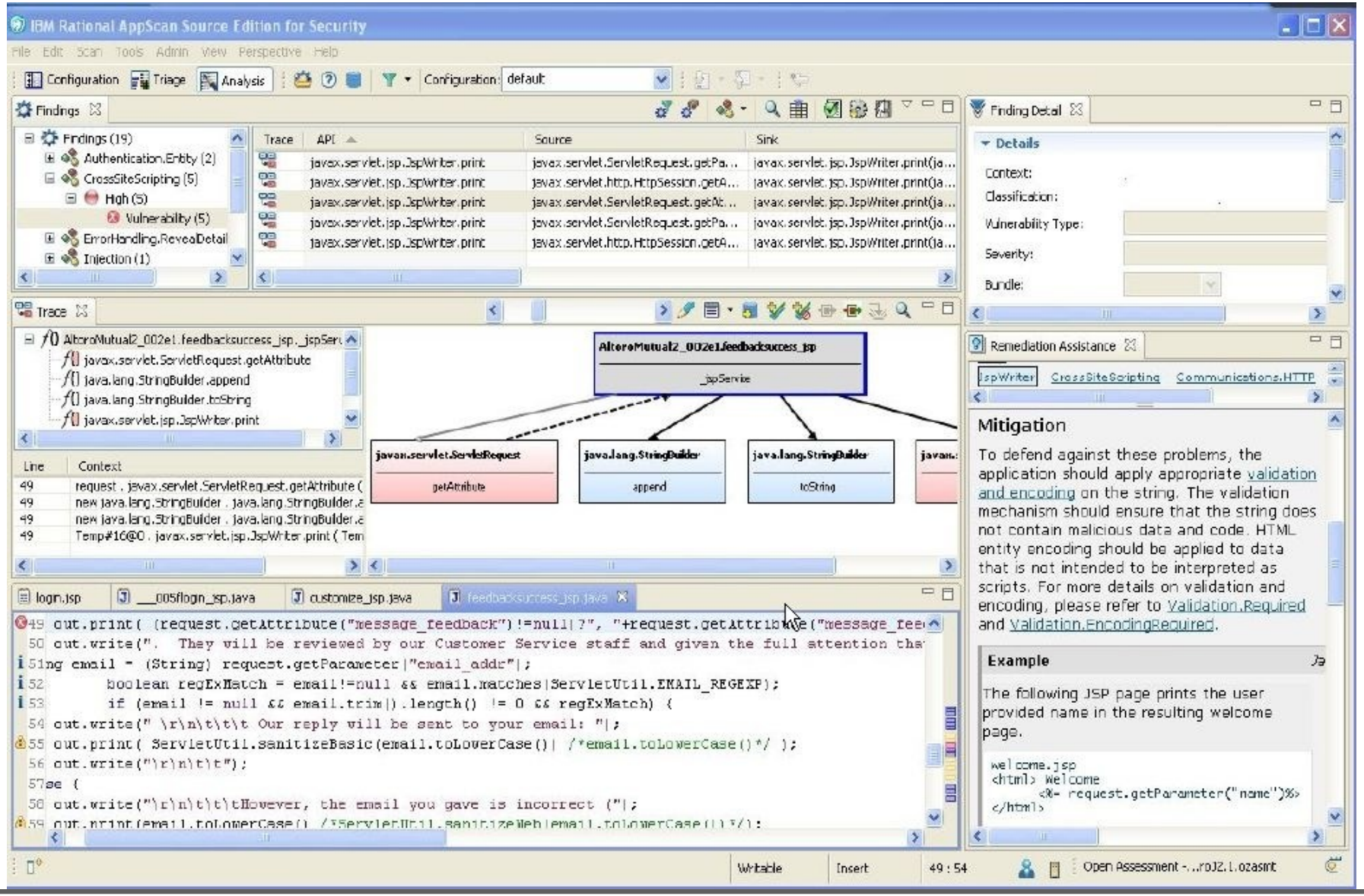
Primjer: StyleCop



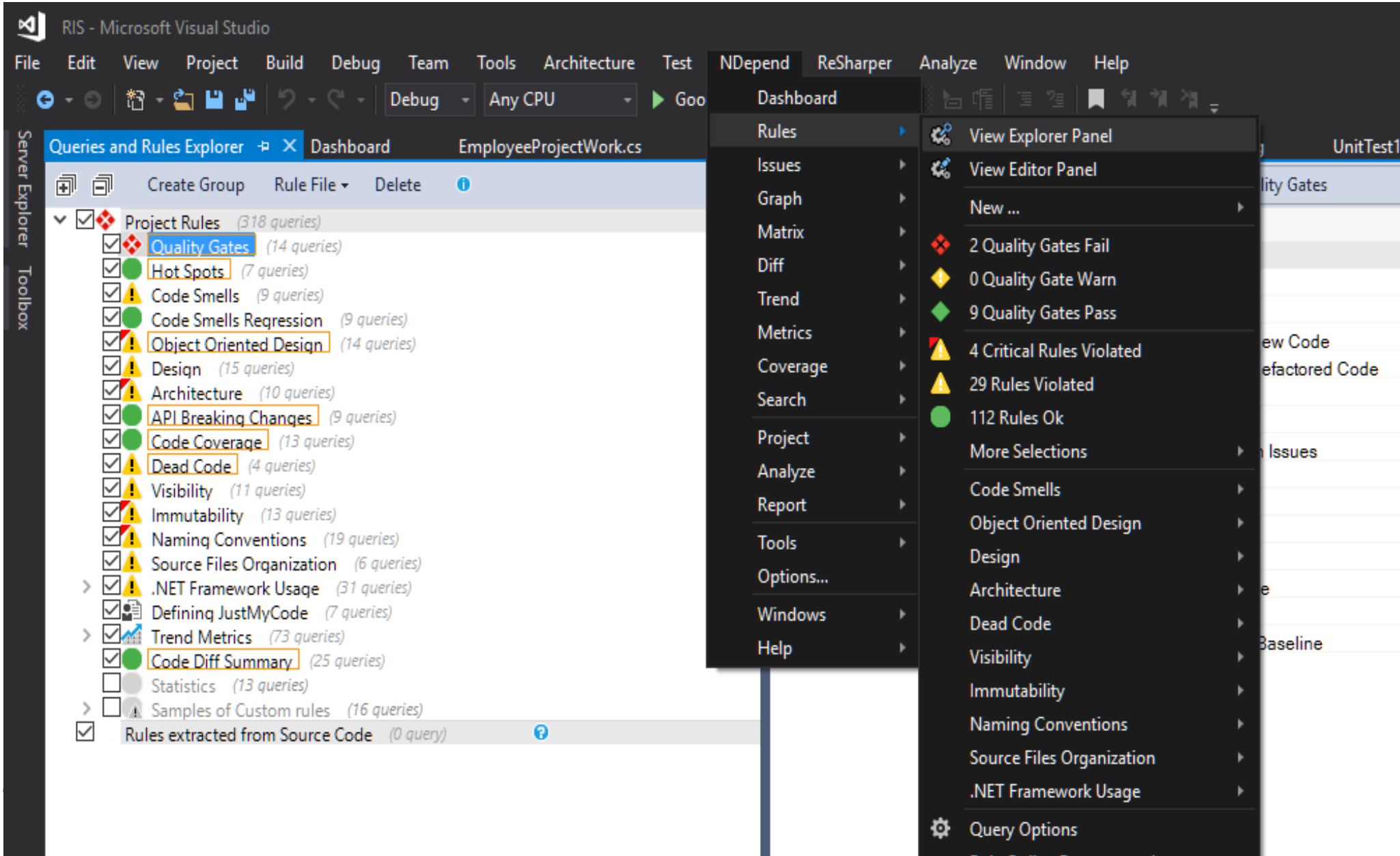
Example: IBM Rational Appscan Source Edition for Security



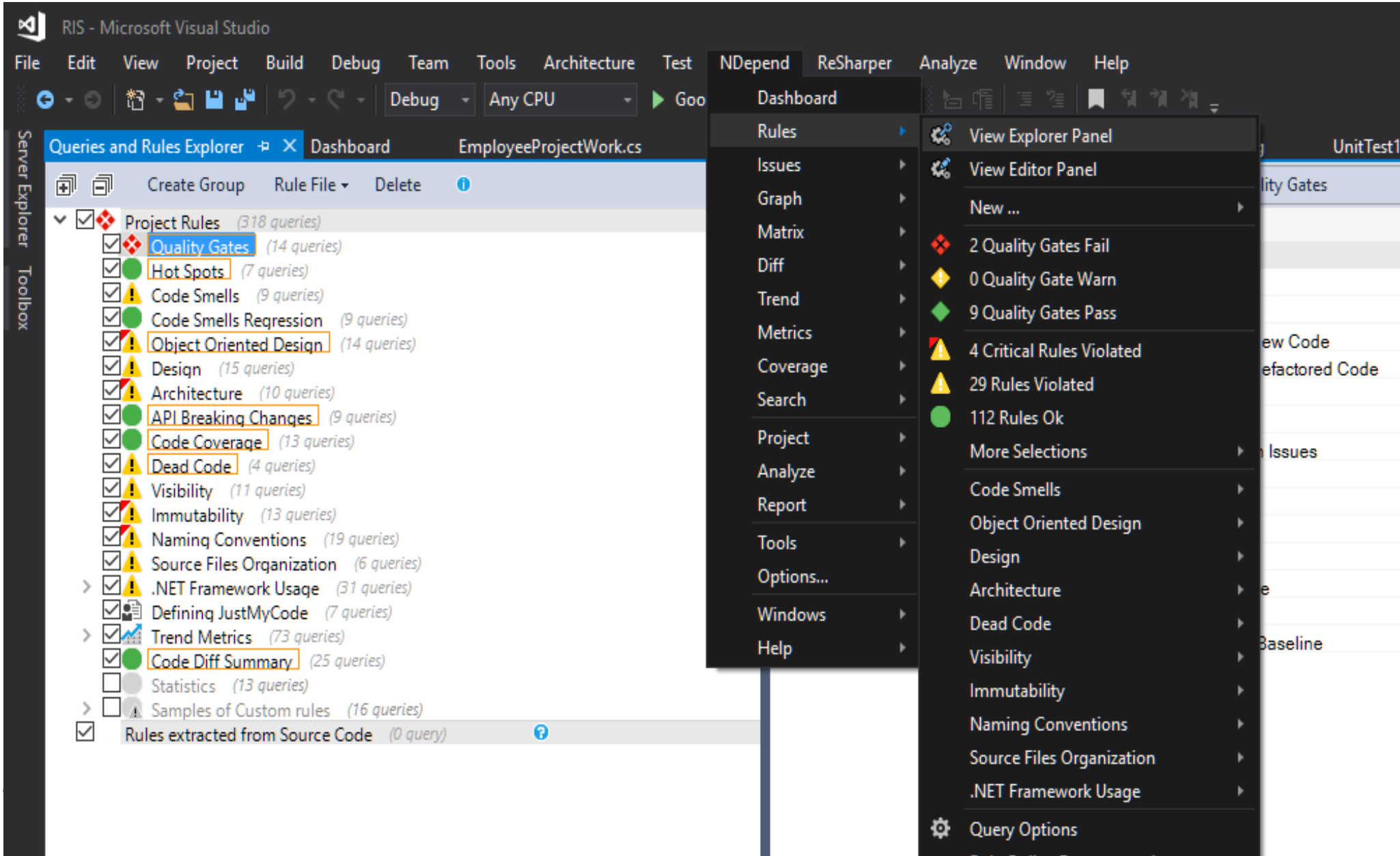
Primjer: IBM Rational Appscan Source Edition for Security



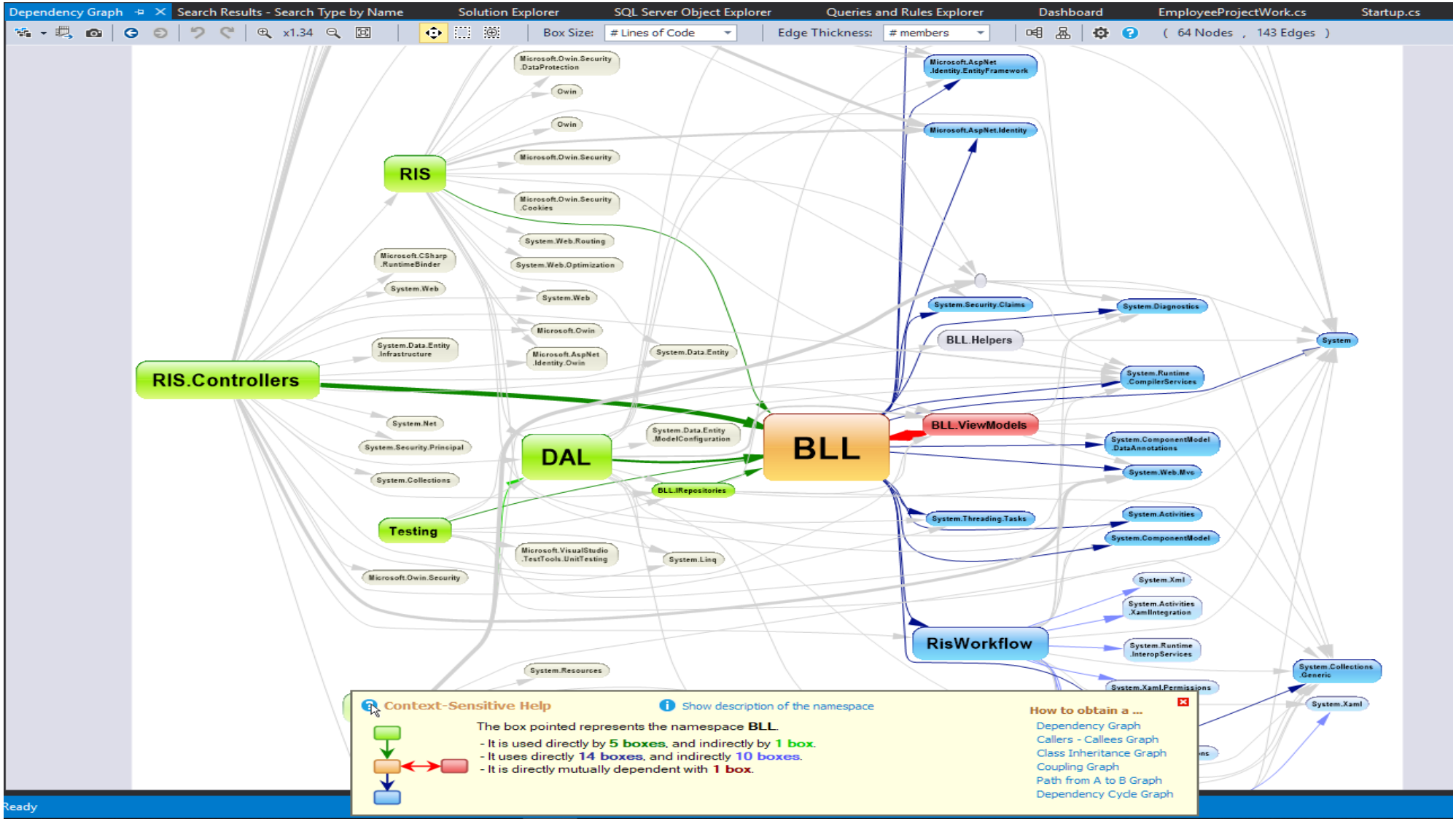
Example: NDepend



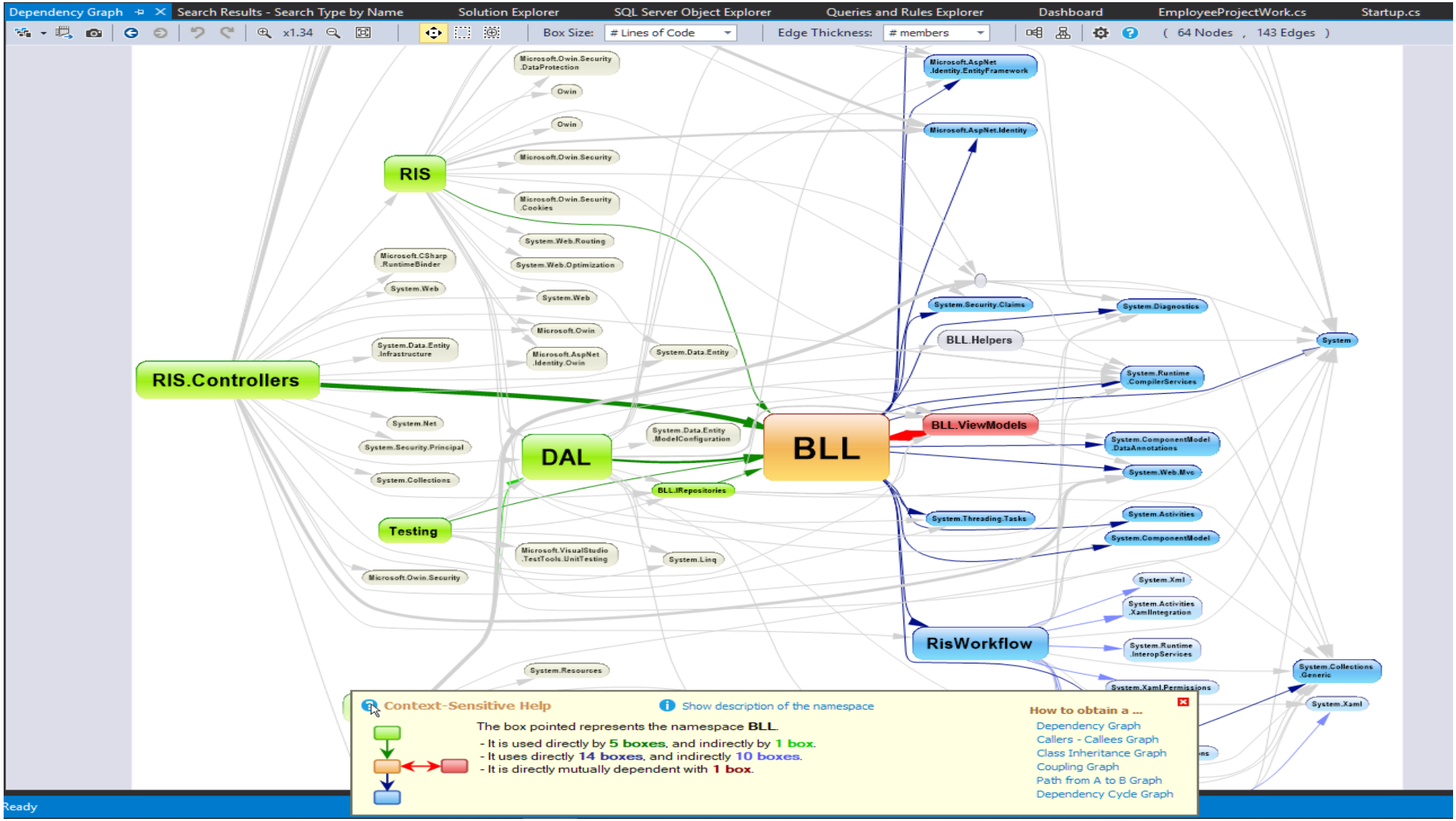
Primjer: NDepend



Example: application component dependency



Primjer: zavisnost komponenti aplikacije



Dynamic check

Dynamic Analysis

Fuzzing

Penetration Testing

Dinamička provjera

Dynamic Analysis

Fuzzing

Penetration Testing

Fuzzing - "combing" (eng. fuzz = hair)

- DAST (The Good, the Bad and the Ugly)
  - fault injection into the application (fuzzing, fuzz testing)
  - sending incorrect, unexpected or random data to the program input
  - similar to regression, only with bad data
  - "combing" applications, protocols, files
- Advantages:
  - simplicity, platform, language independence
- Disadvantages:
  - application to a narrow set of vulnerabilities, eg. *Buffer overflows, Integer overflows,...*
  - complex application to technologies (Web 2.0, JSON, Flash, HTML 5.0, Jscript)
  - relatively long duration (permutations of incorrect data samples)

Fuzzing - "pročešljavanje" (eng. fuzz = dlačica)

- DAST (The Good, the Bad and the Ugly)
  - ubrizgavanje kvara u aplikaciju (fuzzing, fuzz testing)
  - slanje neispravnih, neočekivanih ili nasumičnih podataka ulazu programa
  - slično regresiji, samo s lošim podacima
  - „češljanje” aplikacija, protokola, datoteka
- Prednosti:
  - jednostavnost, nezavisnost o platformi, jeziku
- Nedostaci:
  - primjena na uzak skup povredivosti, pr. *Buffer overflows, Integer overflows,...*
  - složena primjena na tehnologije (Web 2.0, JSON, Flash, HTML 5.0, Jscript)
  - relativno dugo trajanje (permutiranja uzoraka neispravnih podataka)

- Glupo = Dumb (mutational) fuzzing
  - enough less knowledge about the goal and the tools
  - pseudorandom anomalies of correct data
  - repercussions
    - more analysis needed
    - redundancy of findings

Standard HTTP GET request

GET /index.html HTTP/1.1

Anomalous requests

AAAAAA...AAAA /index.html HTTP/1.1

GET ///////index.html HTTP/1.1

GET %n%n%n%n%n%n.html HTTP/1.1

GET /AAAAAAAAAAAA.html HTTP/1.1

GET /index.html HTTTTTTTTTTTTP/1.1

GET /index.html HTTP/1.1.1.1.1.1.1.1

- Smart (generational) fuzzing
  - data generated based on the model
  - requires in-depth knowledge of the target and specialized tools
  - purposeful anomalies by knowledge of formats, standards, ... (PDF, RFC)
  - repercussions
    - less need for analysis
    - less duplication of findings

Postupci

- Glupo = Dumb (mutational) fuzzing
  - dovoljno manje znanja o cilju i alatima
  - pseudoslučajne anomalije ispravnih podataka
  - posljedica
    - potrebno više analize
    - redundancija nalaza

```
Standard HTTP GET request
   GET /index.html HTTP/1.1
Anomalous requests
   AAAAAA...AAAA /index.html
        HTTP/1.1
   GET ///////index.html HTTP/1.1
   GET %n%n%n%n%n%n.html HTTP/1.1
   GET /AAAAAAAAAAAAA.html HTTP/1.1
   GET /index.html
        HTTTTTTTTTTTTTP/1.1
   GET /index.html
        HTTP/1.1.1.1.1.1.1.1.1
```

- Pametno = Smart (generational) fuzzing
  - podaci generirani na temelju modela
  - zahtijeva dubinsko poznavanje cilja i specijaliziranih alata
  - smišljene anomalije poznavanjem formata, standarda, ... (PDF, RFC)
  - posljedica
    - manja potreba za analizom
    - manje dupliciranje nalaza

Tools for dynamic analysis

- https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

- CERT Basic Fuzzing Framework (BFF) and Failure Observation Engine (FOE)
  - Open source https://github.com/CERTCC/certfuzz

- Peach Fuzzer - *automated security testing platform*
- WebScarab - analysis of applications that use HTTP/HTTPS, *intercepting proxy*
- Burp - web applications, buffer overflow, CSS, SQL injection, …
- Fuddly - *fuzzing and data manipulation framework (for GNU/Linux)*
- Hongfuzz - *general fuzzer*

- *Profilers, …*

Alati za dinamičku analizu

- https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

- CERT Basic Fuzzing Framework (BFF) i Failure Observation Engine (FOE)
  - Otvoreni kod https://github.com/CERTCC/certfuzz

- Peach Fuzzer - *automated security testing platform*
- WebScarab - analiza aplikacija koje koriste HTTP/HTTPS, *intercepting proxy*
- Burp - web aplikacije, buffer overflow, CSS, SQL injection, …
- Fuddly - *fuzzing and data manipulation framework (for GNU/Linux)*
- Hongfuzz - *general fuzzer*

- *Profileri, …*

Penetration testing (Pen Test), ethical hacking

- assessment of system or network security by simulating a malicious attack
- person, team, preferably external consultants
- written permission of the owner (implementation of illegal activities)

- Purpose
  - Confirmation of the functionality of security controls
  - Timely detection of security flaws
  - Prevention of security incidents
  - Investment justification
  - Compliance with regulatory requirements

Penetracijsko testiranje (Pen Test), etičko hakiranje

- procjena sigurnosti sustava ili mreže simuliranjem zlonamjernog napada
- osoba, ekipa, poželjno vanjski konzultanti
- pismena dozvola vlasnika (provedbe nezakonitih aktivnosti)

- Svrha
  - Potvrda funkcionalnosti sigurnosnih kontrola
  - Pravovremeno uočavanje sigurnosnih propusta
  - Prevencija sigurnosnih incidenata
  - Opravdavanje investicije
  - Ispunjavanje regulatornih zahtjeva

Approach to penetration testing

- Types of verification according to the availability of information
  - without available information (eng. *black-box test*) - as a real attack
  - with all information (eng. *white-box test*) - the worst case, when the attacker knows everything, or the simulation of an attack by an internal attacker
  - with partially available information (eng. *gray-box test*) - hybrid

- Test starting point criterion
  - External - from a remote location (Internet) to publicly available systems
  - Internal - from the intranet, simulation of an incident of unauthorized access to the internal network infrastructure

- Other criteria
  - Range, stealth, techniques, aggressiveness

Pristup penetracijskom testiranju

- Vrste provjere prema raspoloživosti informacija
  - bez dostupnih informacija (eng. *black-box test*) - kao pravi napad
  - sa svim informacijama (eng. *white-box test*) - najgori slučaj, kad napadač sve zna, ili simulacija napada od strane unutrašnjeg napadača
  - s djelomično dostupnim informacijama (eng. *gray-box test*) - hibrid
- Kriterij početne točke testa
  - Vanjski - s udaljene lokacije (Interneta) prema javno dostupnim sustavima
  - Unutrašnji - s intraneta, simulacija incidenta neovlaštenog pristupa unutrašnjoj mrežnoj infrastrukturi
- Ostali kriteriji
  - Opseg, prikrivenost, tehnike, agresivnost

Performing a penetration test

- **Research**(Eng.*reconnaissance*), scouting
  - the examiner tries to collect as much information as possible.
  - passive - publicly available information (eg data from social networks, Google)
  - active - research tools (e.g.*nslookup*), to determine certain parameters
- **Scanning**(Eng.*scanning*)
  - the tester scans open ports (*port scanning*) using tools (e.g. Nmap)
  - goal - enumeration of services, versions of enumerated services and OS (*OS and service fingerprinting*).
  - vulnerability scan (*vulnerability scanning*), automated tools (e.g. OpenVAS)
- **Gaining access**(Eng.*obtaining access*)
  - exploitation of vulnerabilities, either manually or with a tool (e.g. Metasploit),
  - depending on the agreement with the owner, some vulnerabilities will not be exploited (eg server crash)
- **Access retention**(Eng.*maintaining access*)
  - examiner installs malicious*backdoor*and*rootkit*programs for further access to the system
  - this and the next phase are not usually carried out in practice, but represent a scenario of a real attack
- **Erasing traces**(Eng.*erasing records*)
  - the examiner attempts to delete log entries that would indicate their unauthorized access

Izvođenje penetracijskog testa

- **Istraživanje** (eng. *reconnaissance*), izviđanje
  - ispitivač pokušava prikupiti što više informacija.
  - pasivno - javno dostupne informacije (npr. podaci s društvenih mreža, Google)
  - aktivno - istraživački alati (npr. *nslookup*), da bi se odredili određeni parametri
- **Skeniranje** (eng. *scanning*)
  - ispitivač skenira otvorene portove (*port scanning*) korištenjem alata (npr. Nmap)
  - cilj - enumeracija servisa, verzije enumeriranih servisa i OS (*OS and service fingerprinting*).
  - skeniranje ranjivosti (*vulnerability scanning*), automatiziranim alatima (npr. OpenVAS)
- **Dobivanje pristupa** (eng. *obtaining access*)
  - iskorištavanje ranjivosti, ručno ili alatom (npr. Metasploit),
  - ovisno o dogovoru s vlasnikom, neke ranjivosti se neće iskorištavati (npr. rušenje poslužitelja)
- **Zadržavanje pristupa** (eng. *maintaining access*)
  - ispitivač instalira zloćudne *backdoor* i *rootkit* programe za daljnji pristup sustavu
  - ova i naredna faza se u praksi najčešće ne provode ali predstavljaju scenarij realnog napada
- **Brisanje tragova** (eng. *erasing evidence*)
  - ispitivač pokušava izbrisati dnevničke zapise koji bi ukazivali na njihov neovlašteni pristup

Tools	Basic functionality	Phase
Harvester	Researching publicly available information using search engines, social networks, etc.	Research
Nmap	Network research and port scanning.	Scanning
QualysGuard (Network)	Network scan for known vulnerabilities.	Scanning
QualysGuard (WAS)	Vulnerability scanning of web applications.	Scanning
ASPauditor	Identification of vulnerable and poorly configured ASP.NET servers.	Scanning
Nobody	Scanning web servers for various vulnerabilities, such as dangerous ones files etc.	Scanning
REC	A multifunctional tool for penetration testing of web applications.	Scanning
Sqlmap	SQL injection vulnerability detection and exploitation.	Conducting an attack
Metasploit	A multifunctional platform for exploiting vulnerabilities.	Conducting an attack
HTTP DoS	Denial of service at the application layer.	Conducting an attack
Hydra	Remote password cracking.	Conducting an attack
Wireshark	Recording and analysis of network traffic.	Conducting an attack

Alat	Osnovna funkcionalnost	Faza
Harvester	Istraživanje javno dostupnih informacija korištenjem tražilica, društvenih mreža itd.	Istraživanje
Nmap	Istraživanje mreže i skeniranje portova.	Skeniranje
QualysGuard (Network)	Mrežno skeniranje poznatih ranjivosti.	Skeniranje
QualysGuard (WAS)	Skeniranje ranjivosti web aplikacija.	Skeniranje
ASPauditor	Identifikacija ranjivih i loše konfiguriranih ASP.NET poslužitelja.	Skeniranje
Nikto	Skeniranje web poslužitelja na razne propuste, kao što opasne datoteke itd.	Skeniranje
ZAP	Multifunkcionalni alat za penetracijsko testiranje web aplikacija.	Skeniranje
Sqlmap	Otkrivanje i iskorištavanje ranjivosti SQL umetanja.	Provođenje napada
Metasploit	Multifunkcionalna platforma za iskorištavanje ranjivosti.	Provođenje napada
HTTP DoS	Uskraćivanje usluge na aplikacijskom sloju.	Provođenje napada
Hydra	Udaljeno probijanje lozinki.	Provođenje napada
Wireshark	Snimanje i analiza mrežnog prometa.	Provođenje napada

Example: Nmap and QualysGuard

```
root@bt :~# nmap -sS -sV 22.22.22.22 Host is up
(0.0027s latency).
Not shown: 992 filtered ports PORT
                STATE    SERVICE          VERSION
21/tcp          open     ftp              Microsoft      ftp
25/tcp          open     smtp?
80/tcp          open     http             Microsoft IIS httpd 6.0
110/tcp         open     pop3             Microsoft Windows 2003 POP3 Service1.0 Microsoft
443/tcp         open     ssl/http         IIS httpd 6.0
3389/tcp open            microsoft-rdp Microsoft Terminal Service
```

Summary of Vulnerabilities

Vulnerabilities Total	24	Security Risk (Avg)	5.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	1	0		
4	0	0		
3	0	0		
2	1	0		
1	0	0		
Total	2	0		

5 Biggest Categories

Category	Confirmed	Potential
Information gathering	0	0
TCP/IP	0	0
Windows	2	0
Web server	0	0
CGI	0	0
Total	2	0

5 Microsoft Windows Remote Desktop Protocol Remote Code Execution

QID:	90783
Category:	Windows
CVE ID:	CVE-2012-0002, CVE-2012-0152
Vendor Reference:	MS12-020
Bugtraq ID:	-
Service Modified:	03/29/2012
User Modified:	-

Primjer: Nmap i QualysGuard

```
root@bt:~# nmap -sS -sV 22.22.22.22
Host is up (0.0027s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE       VERSION
21/tcp   open   ftp           Microsoft ftpd
25/tcp   open   smtp?
80/tcp   open   http          Microsoft IIS httpd 6.0
110/tcp  open   pop3          Microsoft Windows 2003 POP3 Service1.0
443/tcp  open   ssl/http      Microsoft IIS httpd 6.0
3389/tcp open   microsoft-rdp Microsoft Terminal Service
```

Summary of Vulnerabilities

Vulnerabilities Total	24	Security Risk (Avg)	5.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	1	0		
4	0	0		
3	0	0		
2	1	0		
1	0	0		
Total	2	0		

5 Biggest Categories

Category	Confirmed	Potential
Information gathering	0	0
TCP/IP	0	0
Windows	2	0
Web server	0	0
CGI	0	0
Total	2	0

5 Microsoft Windows Remote Desktop Protocol Remote Code Execution

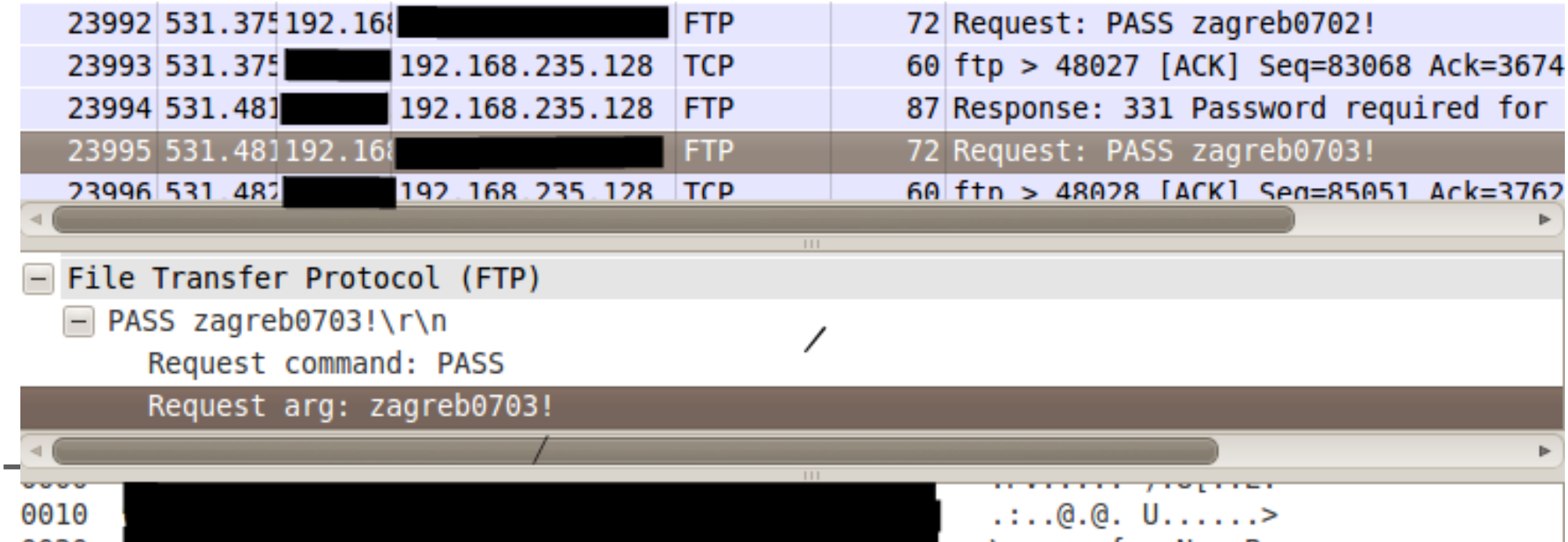
QID:	90783
Category:	Windows
CVE ID:	CVE-2012-0002, CVE-2012-0152
Vendor Reference:	MS12-020
Bugtraq ID:	-
Service Modified:	03/29/2012
User Modified:	-

Example: Hydra, Wireshark

- Dictionary attack with the Hydra tool

```
[STATUS] 446.66 tries/min, 187152 tries in 06:59h, 0 todo in 00:01h [STATUS] attack finished for
22.22.22.22 (waiting for children to finish) 1 of 1 target successfully completed, 0 valid passwords
found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-06-10 17:20:30
```

- Authentication data during the attack captured by the Wireshark tool

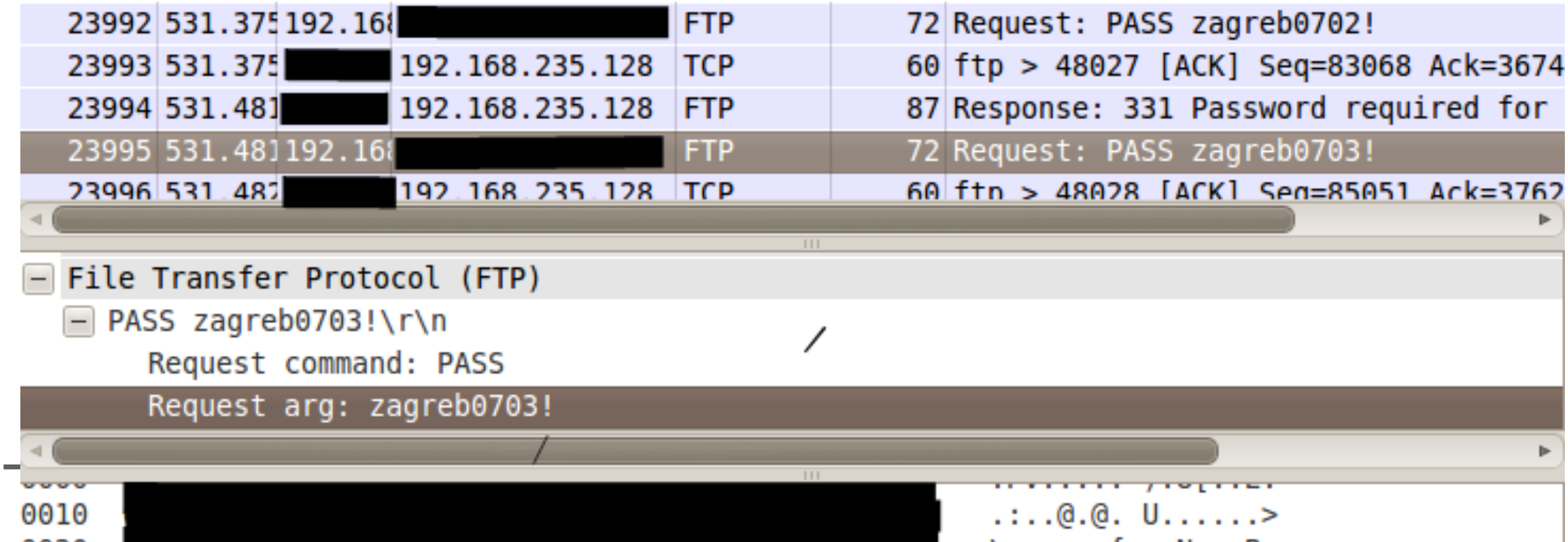


Primjer: Hydra, Wireshark

- Napad rječnikom alatom Hydra

```
[STATUS] 446.66 tries/min, 187152 tries in 06:59h, 0 todo in 00:01h
[STATUS] attack finished for 22.22.22.22 (waiting for children to finish)
1 of 1 target successfuly completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-06-10 17:20:30
```

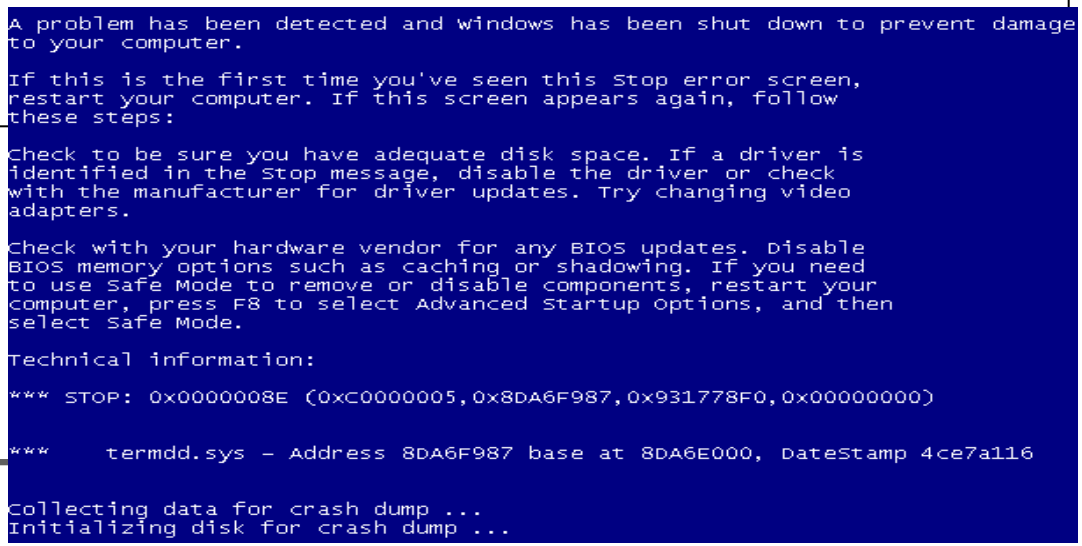
- Autentifikacijski podaci tijekom napada snimljeni alatom Wireshark



Example: Metasploit

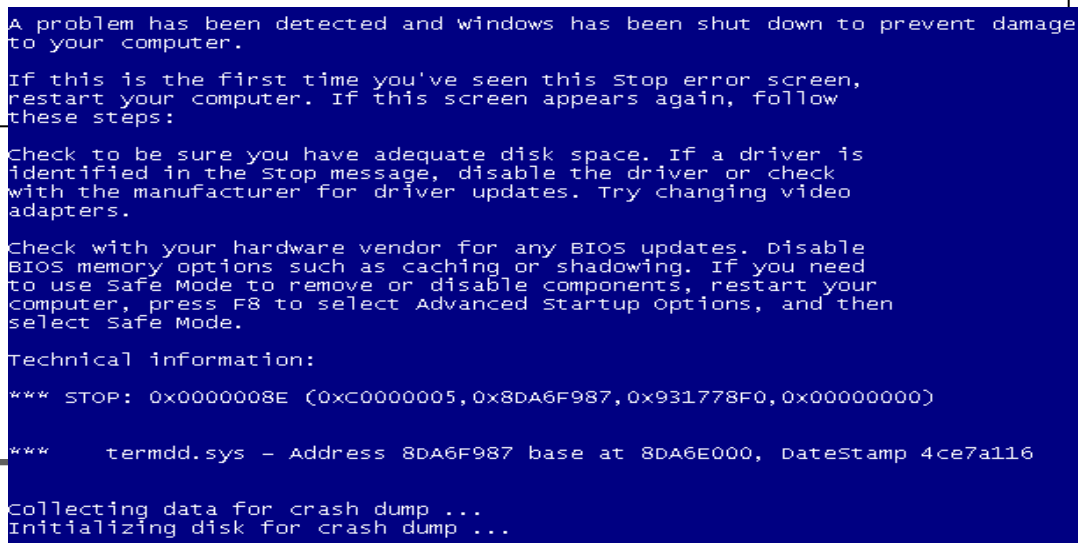
```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids msf
auxiliary(ms12_020_maxchannelids) > show options Module
        options    (auxiliary/dos/windows/rdp/ms12_020_maxchannelids): Current
   To us            Setting            Required     Description
   - - - -      - - - - - - - - - - - - - -     - - - - - - - -     - - - - - - - - - - -
   RHOST                                yes          The  target    address
   REPORT       3389                    yes          The  target    port
msf auxiliary(ms12_020_maxchannelids) > set RHOST 11.11.11.11 RHOST =>
11.11.11.11
msf auxiliary(ms12_020_maxchannelids) > exploit
[*] 11.11.11.11:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS

[*] 11.11.11.11:3389 - 210 bytes sent [*]
11.11.11.11:3389 - Checking RDP with [+]
11.11.11.11:3389 seems down
```



Primjer: Metasploit

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > show options
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   3389             yes       The target port
msf auxiliary(ms12_020_maxchannelids) > set RHOST 11.11.11.11
RHOST => 11.11.11.11
msf auxiliary(ms12_020_maxchannelids) > exploit
[*] 11.11.11.11:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-
Free DoS
[*] 11.11.11.11:3389 - 210 bytes sent
[*] 11.11.11.11:3389 - Checking RDP
[+] 11.11.11.11:3389 seems down
```



Tools for penetration testing and intrusion detection

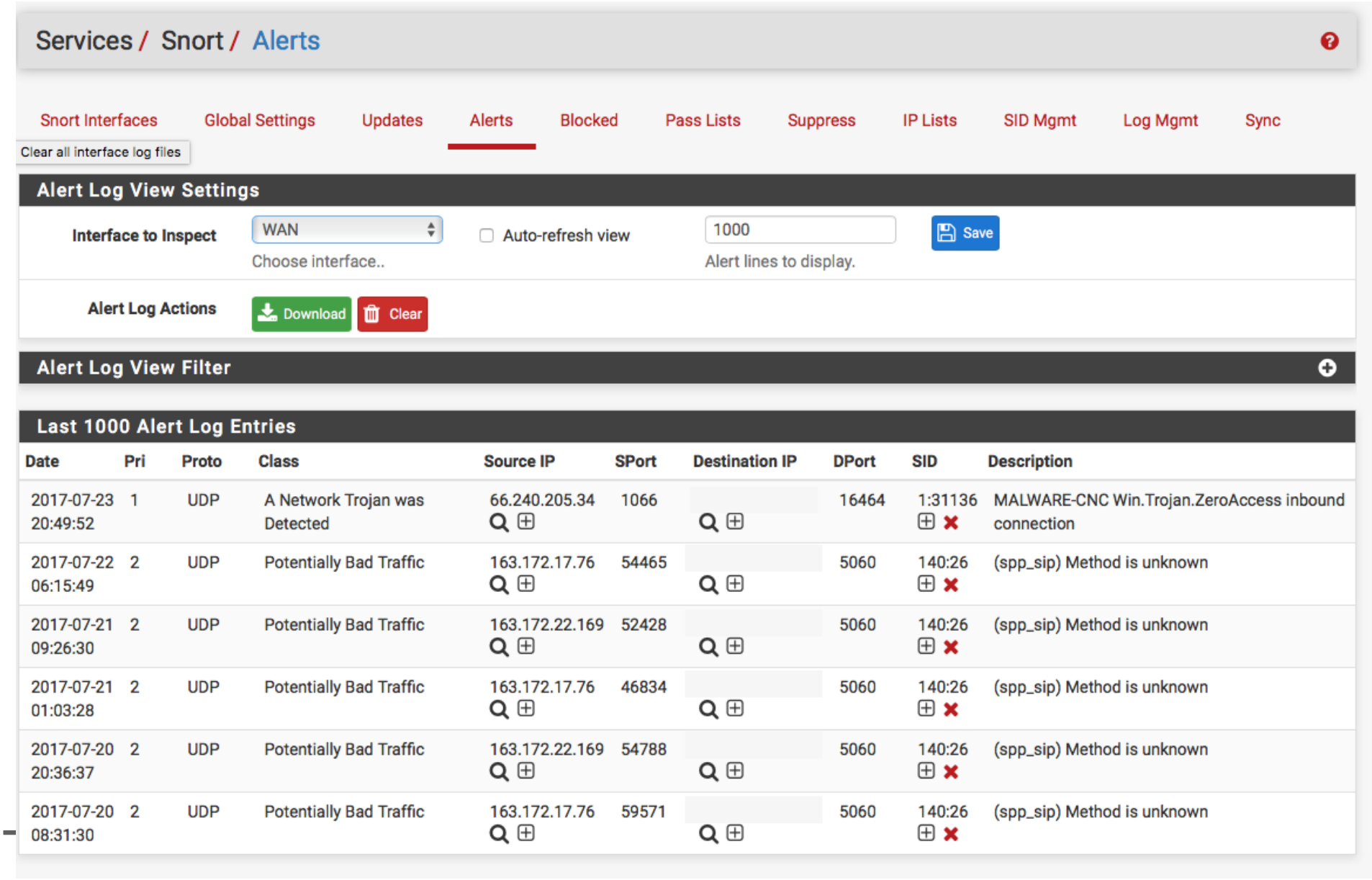
- Pentest
  - https://www.owasp.org/index.php/Category:Penetration_Testing_Tools
  - Aircrack-ng - WIFI scanner - open source
  - Burp Suite - web vulnerability scanner
  - Cain & Abel - "password recovery tool" - packet sniffer, password cracker, ...
  - Ettercap - suite for man in the middle attacks - open source
  - John The Ripper - password cracker
  - Nessus - vulnerability scanner - free trial
  - Kismet - network detector, packet sniffer, IDS - freeware
  - Zed Attack Proxy (**REC**) - web application security scanner - Apache 2 License
- ID/PS
  - https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
  - **Snort**, OSSEC, ..., Solarwinds Log and Event Manager, ...

Alati za penetracijsko testiranje i detekciju upada

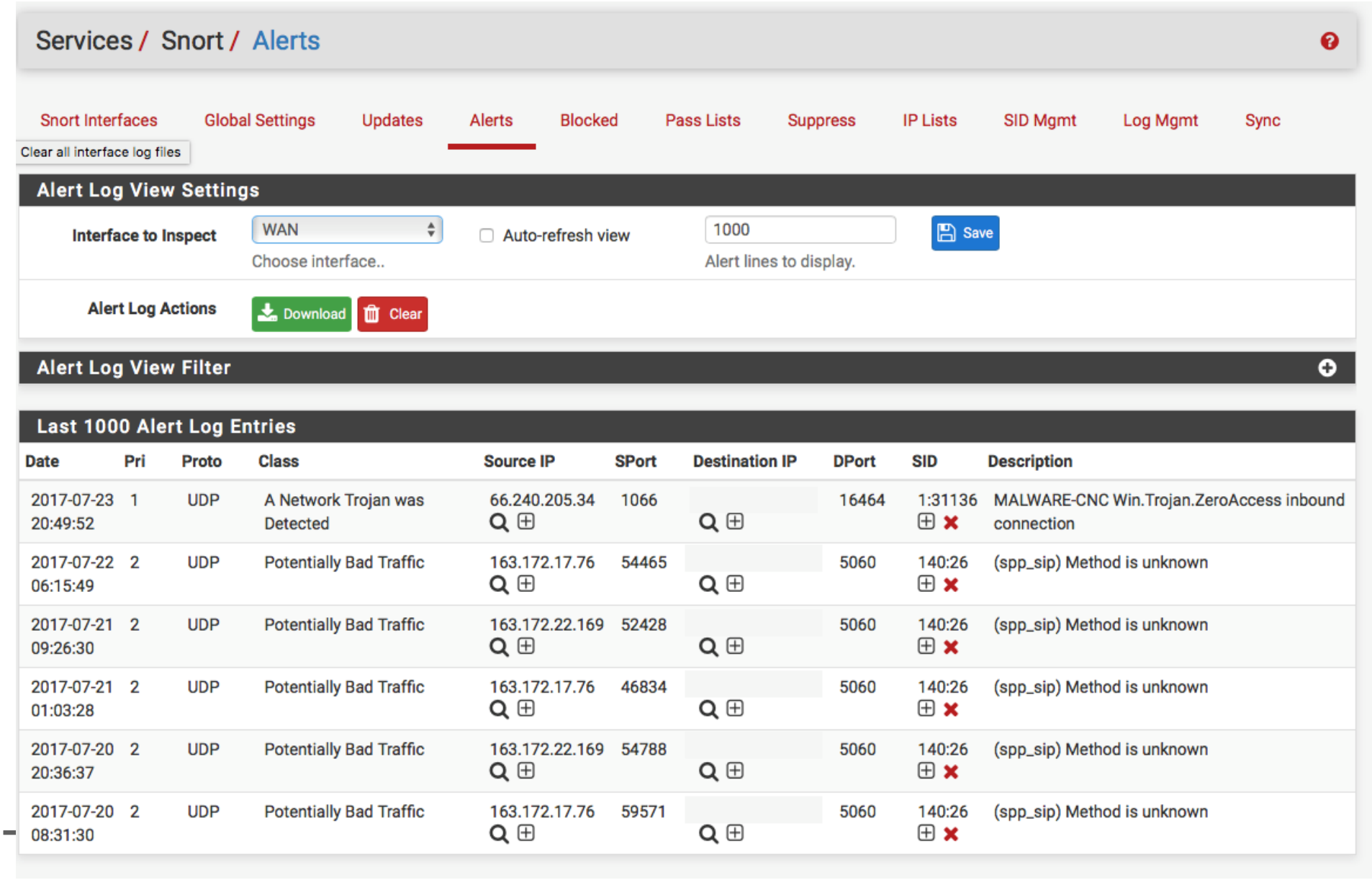
- Pentest
  - https://www.owasp.org/index.php/Category:Penetration_Testing_Tools

  - Aircrack-ng - WIFI skaner - otvoreni kod
  - Burp Suite - skaner web ranjivosti
  - Cain & Abel - „password recovery tool" - packet sniffer, password cracker, …
  - Ettercap - suite for man in the middle attacks - otvoreni kod
  - John The Ripper - password cracker
  - Nessus - skener ranjivosti - free trial
  - Kismet - mrežni detektor, packet sniffer, IDS - freeware
  - Zed Attack Proxy (**ZAP**) - web application security scanner - Apache 2 License
- ID/PS
  - https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
  - **Snort**, OSSEC, …, Solarwinds Log and Event Manager, …

Example: Snort



Primjer: Snort



Services / Snort / Alerts

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Clear all interface log files

Alert Log View Settings

Interface to Inspect: WAN — Choose interface..

Auto-refresh view

1000 — Alert lines to display.

Save

Alert Log Actions: Download | Clear

Alert Log View Filter

Last 1000 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-07-23 20:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066		16464	1:31136	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown
2017-07-20 08:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571		5060	140:26	(spp_sip) Method is unknown

References

- OWASP Category: Vulnerability Scanning Tools
- OWASP Code Review Guide
- OWASP Testing Guide

- More tools…
  - http://sectools.org/
  - https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
  - Software Security Assessment Tools Review, 2009

Reference

- OWASP Category: Vulnerability Scanning Tools
- OWASP Code Review Guide
- OWASP Testing Guide

- Još alata …
  - http://sectools.org/
  - https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
  - Software Security Assessment Tools Review, 2009