Introduction To Yasca

Presented at
NYPHP

24 February 2009

Michael V. Scovetta

Agenda

- Who Am I?
- What is Yasca?
- How does it work?
- Requirements
- How should I use it?
- The Future of Yasca
- Demonstration
- Questions?

Who Am I?

- Development
  - CA ~2002
  - Perl, Java, PHP
- Information Security
  - UBS ~2005
- Security Consulting
  - Cigital ~2008
- Architecture
  - CA ~2008

What is Yasca?

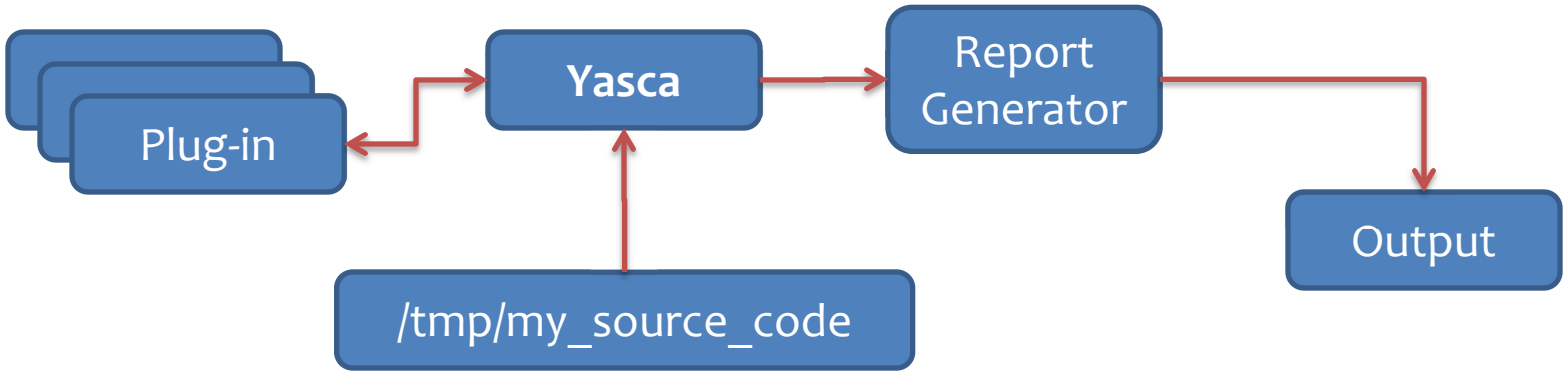
- Yasca started as a set of perl scripts that grepped through source code looking for XSS vulnerabilities.
  - `<%=request.getParameter("foo")%>`
  - `<?=$_REQUEST["foo"]?>`
- Then I needed to do multi-line searches:
  - ```
    String s = request.getParameter("foo");
    out.println(s);
    ```
- As I wrote more rules, I found other scanners that already had many of them.
- So I made calls out to them.
- Then everything got nasty and I wrote it all from scratch again in PHP.
    ```

What is Yasca?

- Yasca is an open-source tool that can help you analyze program source code.
- It leverages several static analysis tools.
  - PMD (http://pmd.sourceforge.net/)
  - J-Lint (http://artho.com/jlint/)
  - Pixy (http://pixybox.seclab.tuwien.ac.at/pixy/)
  - FindBugs (http://findbugs.sourceforge.net/)
- It can be used to scan virtually any file type, not only traditional source code.
- Yasca is written in command-line PHP and released under the BSD license.

How Does it Work?

- Architecture based on plug-ins.
  - "Major Plug-in" => calls another tool to do the scan
    - e.g. PMD, J-Lint, FindBugs, Pixy, Grep
  - "Minor Plug-in" => uses embedded logic
    - Relatively easy to write, extremely flexible



How Does it Work

- Yasca has plug-ins capable of scanning many file types, including Java, C/C++, PHP, COBOL, ASP, JavaScript, HTML, CSS, and Visual Basic.
- A special plugin (Grep) is designed to make new rules extremely easy to write.
  - Just define a regular expression, the file types it's applicable to, and a name for your rule and drop it in the "plugins" directory.
  - An example will follow.

Requirements

- Yasca has few base requirements:
  - PHP (Windows binaries included)
  - Java 1.5 (for PMD, FindBugs, and Pixy)
- Yasca has been tested on Windows XP, Vista, and a few flavors of Linux.
- If you find bugs or incompatibilities, please let me know!
  - scovetta@users.sourceforge.net

How Should I Use It?

- Yasca can be used in a number of different ways, including as a:
  - checkpoint within a formal SDLC
  - desktop tool for developers
  - tool integrated into a source code repository

- In its current form, Yasca is best suited for use as a developer tool.
  - i.e. run Yasca each week on your code base.

The Future of Yasca

- Future versions of Yasca may include the following features:
  - "diff" -- compare last week's results to this week's
  - data flow analysis / taint propagation
  - Program Query Language
    - http://pql.sourceforge.net/
  - Central results repository
- More information is available on the OWASP Project Page:
  - http://www.owasp.org/index.php/Category:OWASP_Yasca_Project_Roadmap

Demonstration

```
[root@ardonis yasca]# ./yasca
Yasca 1.2 - http://yasca.sourceforge.net - Designed & Developed by Michael V. Scovetta

Usage: yasca [options] directory
Perform analysis of program source code.

      --debug               additional debugging
  -h, --help                show this help
  -i, --ignore-ext EXT,EXT  ignore these file extensions
                              (default: exe,zip,jpg,gif,png,pdf,class)
      --ignore-file FILE    ignore findings from the specified xml file
      --source-required     only show findings that have source code available
  -f, --fixes FILE          include fixes, written to FILE (default: not included)
                              (EXPERIMENTAL)
  -s, --silent              do not show any output
  -v, --version             show version information

Examples:
  yasca c:\source_code
  yasca /opt/dev/source_code
  yasca -o c:\output.csv --report CSVReport "c:\foo bar\quux"

[root@ardonis yasca]#
```

Demonstration

```
[root@ardonis yasca]# ./yasca resources/test
Yasca 1.2 - http://yasca.sourceforge.net - Designed & Developed by Michael V.
   Scovetta

Initializing components...
Starting scan. This may take a few minutes to complete...
Forking external process (FindBugs)...
External process completed...
Forking external process (PMD) for ./plugins/default/pmd/yasca.xml...
External process completed...
Forking external process (PMD) for ./plugins/default/pmd/yasca-rules.xml...
External process completed...
Creating report...
Results have been written to /root/Desktop/Yasca/Yasca-Report-20090127013827.html

[root@ardonis yasca]#
```

Demonstration

Yasca

Attachments:

Version: 1.2 [check for updates]
Report Generated: 2009-01-27 13:39:54
Options: [change links | save ignore list | user guide | send feedback]

#	Location	Message / Source Line
SQL Injection		
001	test04.php:4	`mysql_query("select * from foo where t = '$a'");`
002	test40.php:8	`mysql_query($a);`
003	test31.php:6	`$result = mysql_query('S' . $category_id);`
004	test30.php:8	`mysql_query($x);`
005	test29.php:9	`mysql_query($x);`
006	test28.php:6	`mysql_query($x[0]);`
007	test27.php:20	`mysql_query($y);`
008	test23.php:17	`mysql_query("x $a y $b z");`
009	test23.php:10	`mysql_query("x $a y");`
010	test22.php:5	`mysql_query('a' . $x . 'b');`
011	test20.php:7	`mysql_query($x); // $x is either "a" or undefined`
012	test19.php:14	`$x = mysql_query($a);`

- Source Code Context (lines before/after finding)
- Problem description
- Proposed fix (where applicable)
- Add finding to the ignore list

Writing a Simple Rule Using the Grep Plug-in

- Problem: Management believes that developers have been embedding social security numbers directly in source code.

- Solution: Use Yasca and the 'Grep Plug-in' to scan all source code files for social security numbers.

Demonstration

```
[root@ardonis yasca]# less ./plugins/default/grep/SSN.grep

name = Social Security Number Found in Source Code
file_type = JAVA, php, NET, HTML
grep = /[^\d]\d{3}\-\d{2}\-\d{4}[^\d]/
category = Compliance: Sensitive Data
category_link = http://en.wikipedia.org/wiki/Social_security_number
severity = 1
description =
Social security numbers should never be embedded in program source
code.
END;
```

Questions?

Thank You!

- This presentation will be posted on www.yasca.org tonight.
- Please send comments, feedback, bug reports, feature requests, questions, etc. to:
  - scovetta@users.sourceforge.net

- **Thank you for listening!!**