# Static analysis with graudit

Eldar *"Wireghoul"* Marcussen

http://www.justanotherhacker.com

Ruxcon Meetup June 2010

# Agenda

- Introduction
- Comparison
- Signatures
- Usage
- Questions

# Introduction

OH HAI DER

# Static analysis

Static code analysis is the analysis of computer software that is performed without actually executing programs built from that software (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code and in the other cases some form of the object code. The term is usually applied to the analysis performed by an automated tool, with human analysis being called program understanding, program comprehension or code review.

– Wikipedia

# Alternatives

- RATS
- SWAAT
- Yasca
- Rips
- Others

# Reporting

- No formal reporting
- Code view
- Over rated?

http://www.pixelbeat.org/scripts/ansi2html.sh

Security Compass

SWAAT

# Vulnerability Report

## Section 1: Summary of Findings

During this scan, SWAAT examined 3 file(s), containing a total of 128 line(s).

| Risk Level | Number of findings |
|---|---|
| High | 3 |
| Medium | 20 |
| Low | 5 |

## Section 2: Detailed Findings

### High Risk Findings

| Finding Name | eval |
|---|---|
| Severity of Finding | High |
| Description | This function should never take unchecked user input as a parameter. Reasons for this vary, but it might be the case that, for instance, it is evaluated by the language environment or by an external program such as a shell. |
| | • In C:\swaat\swaat\swaat\tests\example.php, line 9 (context is *<?php eval("evil!") ?>*)<br>• In C:\swaat\swaat\swaat\tests\example.php, line 59 (context |

Entries in perl database: **33**
Entries in ruby database: **46**
Entries in python database: **62**
Entries in c database: **334**
Entries in php database: **55**

Analyzing **tests/example.php**

# RATS results.

**Severity: High**
Issue: mail
Arguments 1, 2, 4 and 5 of this function may be passed to an external program. (Usually sendmail).
server. If these values are derived from user input, make sure they are properly formatted and cont

File: **tests/example.php**
Lines: 47 62

**Severity: Medium**
Issue: stat
A potential TOCTOU (Time Of Check, Time Of Use) vulnerability exists. This is the first line where a
that may match up with this check: 12 (exec)

File: **tests/example.php**
Lines: 7

## Inputs detected at the following points

Total lines analyzed: **72**
Total time **0.000399** seconds
**180451** lines per second

```
dns-lookup.php-3-<?
dns-lookup.php:4:echo "<form method=\"POST\" action=\"" .$_SERVER['SCRIPT_NAME'] . "?" . $_SERVER['QUERY_STR
ING'] . "\">";
dns-lookup.php-5-?>
################################################
dns-lookup.php-16-echo "<pre>";
dns-lookup.php:17:echo shell_exec("nslookup  " . $targethost);
dns-lookup.php-18-echo "</pre>";
################################################
header.php-10-if ($username <> "" and $password <> "") {
header.php:11:  $query  = "SELECT * FROM accounts WHERE username='". $username ."' AND password='".stripslas
hes($password)."'";
header.php:12:  $result = mysql_query($query) or die('Did you <a href="setupreset.php">setup/reset the DB</a
>? <p><b>SQL Error:</b>' . mysql_error($conn) . '<p><b>SQL Statement:</b>' . $query);
header.php-13-  if (mysql_num_rows($result) > 0) {
################################################
header.php-54-          <?
header.php:55:          $query  = "SELECT * FROM accounts WHERE cid='".$_COOKIE["uid"]."'";
header.php:56:          $result = mysql_query($query) or die('Did you <a href="setupreset.php">setup/reset t
he DB</a>?');
header.php-57-          echo mysql_error($conn);
```

# Custom signatures

- Word list
- Regular expressions
- Adhoc
- Gotchas

# Word list

alter

insert

update

where

union

outer join

select * from

# Regular Expressions

```
create (database|table|trigger|view|sequence)

(inner|cross|((left|right)( outer)?) +join

(WHERE|where) .*=.*\$(_GET|_POST|
_REQUEST|_SESSION|_COOKIE)[^; ]+
```

# Adhoc signatures

Database - reads from STDIN

```
graudit -z -d php index.php | \
perl -ne 'if ($_ =~ m/\$(.*) ?= ?\$_(GET|POST|
REQUEST|COOKIE)\[.*?\]/) { print "\\\$$1"; }' | \
graudit -d - index.php
```

```
eldar@eldar-laptop:~/research/maiacms$ graudit -z -d php index.php | perl -ne 'i
f ($_ =~ m/\$(.*?) ?= ?\$_(GET|POST|REQUEST|COOKIE)\[.*?\]/) { print "\\\$$1"; }
' | graudit -c 10 -d - index.php
index.php-1-<?php
index.php-2-    require ("includes/connections.php");//Includes functions and da
tabase connection
index.php:3:    $page = $_GET['page'];
index.php-4-
index.php-5-    //SEF Get Page ID
index.php:6:    if (empty($page)) {
index.php-7-            $url = parse_url($_SERVER['REQUEST_URI']);
index.php-8-            $parts = split("/", $url['path']);
index.php-9-            $cat = $parts[1];
index.php:10:           $page = $parts[2];
index.php:11:           if (empty($page))
index.php:12:                   $page = "index";
index.php:13:           $result = $db->Execute("select p.id from pages p, catego
ries cat where p.category = cat.id and cat.short_name = '$cat' and p.short_name
= '$page'");
index.php-14-           if ($result->RowCount() > 0) {
index.php-15-                   $row = $result->FetchRow();
index.php:16:                   $page = $row[0];
index.php-17-           }
index.php:18:           else if ($cat == "chimera" && $page == "xml") {
```

# Signature gotchas

select * from

“select from”

select .* from

“select a,b as c from users union select * from”

eval ?\($_GET\[.*\])

Whitespace----------^

# Automated scan: SVN

```
#!/bin/sh
REPOS="$1"
REV="$2"
/usr/local/bin/svnlook diff -r $REV $REPOS | \
graudit -d php - | \
ansi2html.sh | \
mail -e -s "Graudit - $REPOS($REV)" "root@domain.com"
```

# Automated scan: RSS

```
#!/bin/sh
#Scrape and graudit by Wireghoul

GET http://freshmeat.net/tags/php | \
grep -E 'href="/urls/.*" class="floatright welcome padleft5
download' | \
sed -e's/<a href="\/urls/http:\/\/freshmeat.net\/urls/g' \
-e's/" class=/ /g' | \
awk '{print $1}' | xargs -n1 wget -nc
unzip *.zip
tar zxvf *.tgz
tar zxvf *.tar.gz
graudit -x *.js -d fruit .
```

# 0day & Questions

```
eldar@eldar-laptop:~/research/maiacms$ ../../graudit/graudit -d fruit . |more
./admin/index.php-8-                    $file_link = "index.php?com=".$_GET['com']."&file=".$_GET['file'];
./admin/index.php:9:                    require('components/'.$_GET['com'].'/'.$_GET['file'].'.php');
./admin/index.php-10-           }
./admin/index.php-11-           else
./admin/index.php:12:                   require('components/'.$_GET['com'].'/'.$_GET['com'].'.php');
./admin/index.php-13-           exit;
```