CSI 2008
SECURITY RECONSIDERED

Automated tools for security, the challenge 2.0?

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008

cigital
Software Confidence. Achieved.

CSI COMPUTER SECURITY INSTITUTE

about:me

- Security consultant at Cigital, Inc.

- Worked at NIST in the SAMATE project for the past 2.5 years, co-organized SATE 2008, tools spec.
- Web Apps Security Consortium officer, lead Script Mapping project,...
- Security blogging: http://rgaucher.info
- I do love tools!!

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008

outline

- Difficulties in security testing
- Type of tools:
  - Black-box: web apps scanners
  - White-box: source code analyzers
- How good are tools?
  - Pros & Cons: things you need to know

Romain Gaucher
rgaucher@cigital.com

CSI 2008
SECURITY RECONSIDERED

Difficulties in security testing

- Testing applications with many components
- Tools have to understand:
  - context, storage mechanisms, interaction...
- Many technologies, using different frontend, backend, etc.

cigital
Software Confidence. Achieved.

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008

CSI COMPUTER SECURITY INSTITUTE


abuse
array
attack
attribute
authentication
authorization
brute
buffer
command
content
credential
cross-
site
detour
disclosure
entity
expiration
external
file
forgery
http
improper
inclusion
indexing
information
injection
insecure
insufficient
layer
ldap
misconfiguration
overflow
permissions
protection
redirectors
request
resource
response
session
smuggling
soap
splitting
spoofing
sql
string
transport
url
validation
xml
xpath
xquery

Difficulties *[…]* cont'd

- But when they break into your websites, they also look at that:
  - Authentication mechanisms (OpenID anyone?)
  - Authorization/Permissions
  - Integration/Communications
  - etc.
- These are no longer purely technical issues, but logical layer flaws

Romain Gaucher
rgaucher@cigital.com

CSI2008
SECURITY RECONSIDERED

Web 2.0 Security :

"Security is lax on this side."

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008

cigital
Software Confidence. Achieved.

CSI COMPUTER SECURITY INSTITUTE

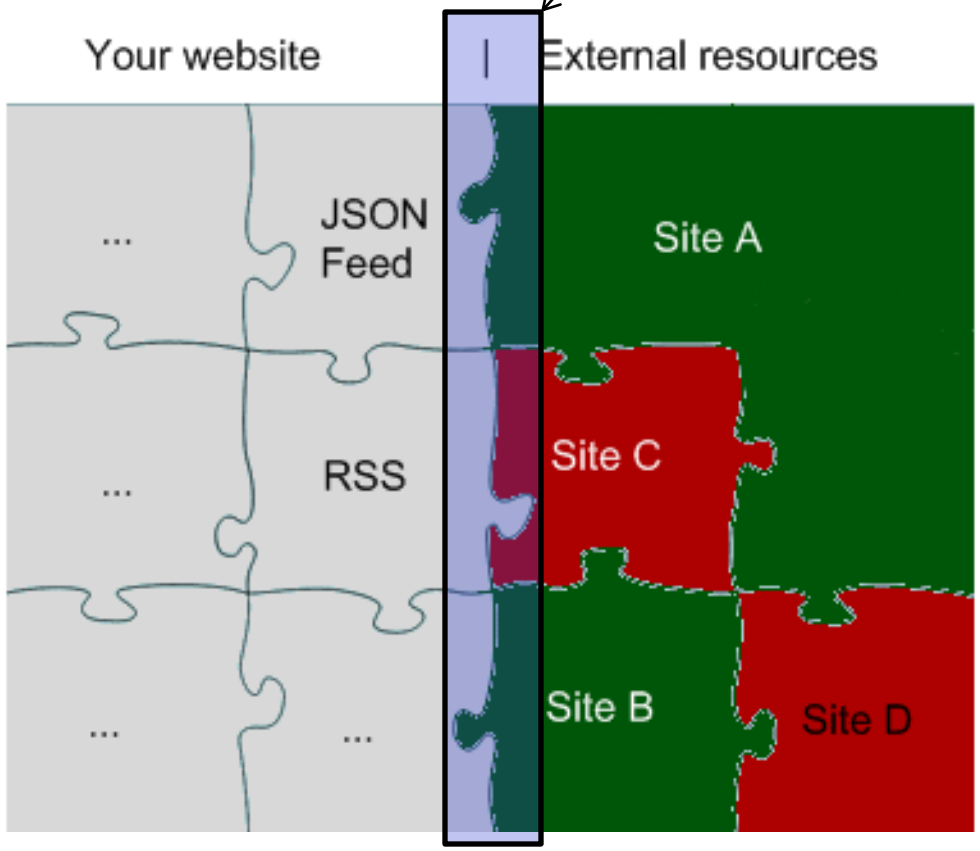
Some of the tools we use

- Dynamic analysis:
  - Access remotely like any user, cannot read the source code, etc.
  - Ex: Web apps scanner...
- Static analysis:
  - Access to the artifacts (source code, etc.)
  - ex: Source code analyzer, binary scanner...

Romain Gaucher
rgaucher@cigital.com

CSI2008
SECURITY RECONSIDERED

WEB APPLICATION SCANNER



SOURCE CODE SCANNER

YOU DON'T HAVE MUCH CLUE ABOUT WHAT'S GOING ON THERE…

cigital
Software Confidence. Achieved.

Romain Gaucher
rgaucher@cigital.com

Web 2.0, Nov. 18, 2008

CSI COMPUTER SECURITY INSTITUTE

Web apps scanners

- Remote tool: access the website like any user
- Find security problems by attacking the web apps

- Performs 3 operations:
  - Crawl/Extract Info/Understand the website
  - Attack/Probe
  - Report the successful attacks

Romain Gaucher
rgaucher@cigital.com

CSI 2008
SECURITY RECONSIDERED

Challenges for web apps scanners

- Handle client-side technologies
- Understand the application logic and cover all the interesting parts of the webapps (attack surface)
- Find interesting and well targeted attacks, probe and report them correctly

- We can tune them in many ways:
  - Custom attacks, Manual crawling…

cigital
Software Confidence. Achieved.

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008

CSI COMPUTER SECURITY INSTITUTE

Source code analyzers

- Local tool: read the source code/configuration/…
- Usually, 3 steps:
  - Compile the source code (using external tools)
  - Parse and build representations (many of them)
  - Find problems with different analysis: matching, behavioral, flow-based, mathematical, etc.
- Does not execute the code!

Romain Gaucher
rgaucher@cigital.com

Challenges for SCA

- Understand connections between components
- Handle API (SQL, GUI, etc.)
- Code complexities (pointers, references, exploding code complexities,…)
- Report the problem to the user/assessor!

- We *must* tune tools to enable checks, create custom rules for the given code base

Romain Gaucher
rgaucher@cigital.com

Increasing complexity

- Tool vendors have to constantly improve the capabilities:
  - New frameworks, technologies, formats, languages…
  - New attack techniques/weaknesses
  - New API/functions to understand
- Better ways of integrating the tools

Romain Gaucher
rgaucher@cigital.com

But tools worth it!

- They are fast and not biased, tools are important for efficiency
- Black-box:
  - **Virtually** no false-positive, they are good for finding low-hanging fruits (and more if tuned correctly)
- White-box:
  - **Full access** to the application, consistent checks, good path coverage of your code

Romain Gaucher
rgaucher@cigital.com

Know what you're doing with tools

• Tools *have to* be tested and calibrated by knowledgeable users
•You *must* integrate tools in your SDLC…
• Reported problems *must* be analyzed, grouped, prioritized, explained to developers…

• An important problem: false impression of security if the tool doesn't find anything
• "You cannot polish junk!"

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008

Using a tool

It’s not

cigital
Software Confidence. Achieved.

Romain Gaucher
rgaucher@cigital.com
Web 2.0, Nov. 18, 2008