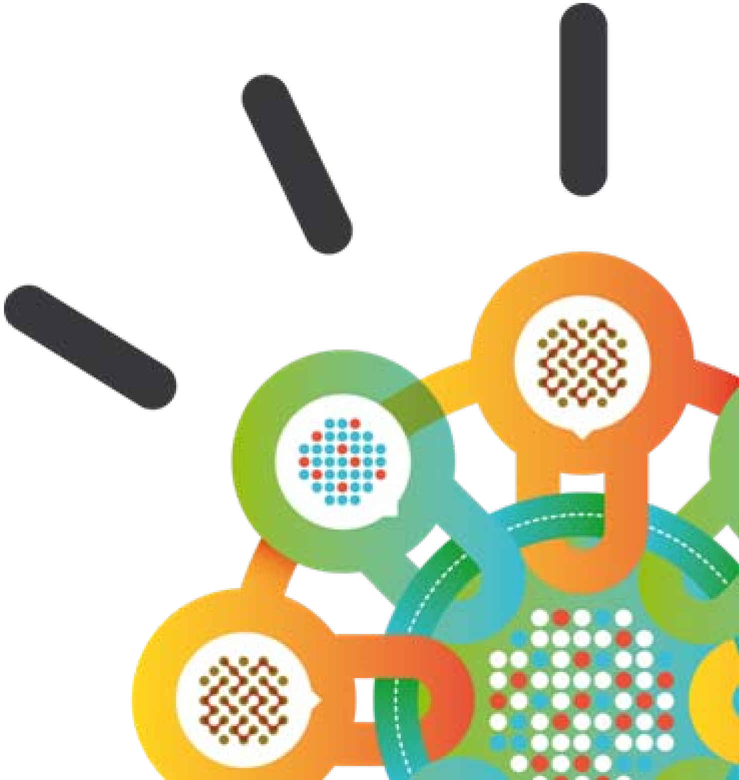
Security Intelligence.
Think Integrated.

Application Security from IBM

Karl Snider, Market Segment Manager

March 2012



Helping Solve Customer Challenges

Application Security

amdocs

Finding Application Vulnerabilities

"GlassBox scanning allowed us to improve results accuracy as well as test for new class of vulnerabilities undetected by conventional web application security scanning technologies"

Boris Gorin, Amdocs

SAP

Reducing the Cost of Being Secure

"AppScan not only helps us to avoid costs related to hacking attacks, but also reduces the manual effort needed for analysis and the costs for testing"

Michael Neumaier,Senior Quality Specialist, SAP AG

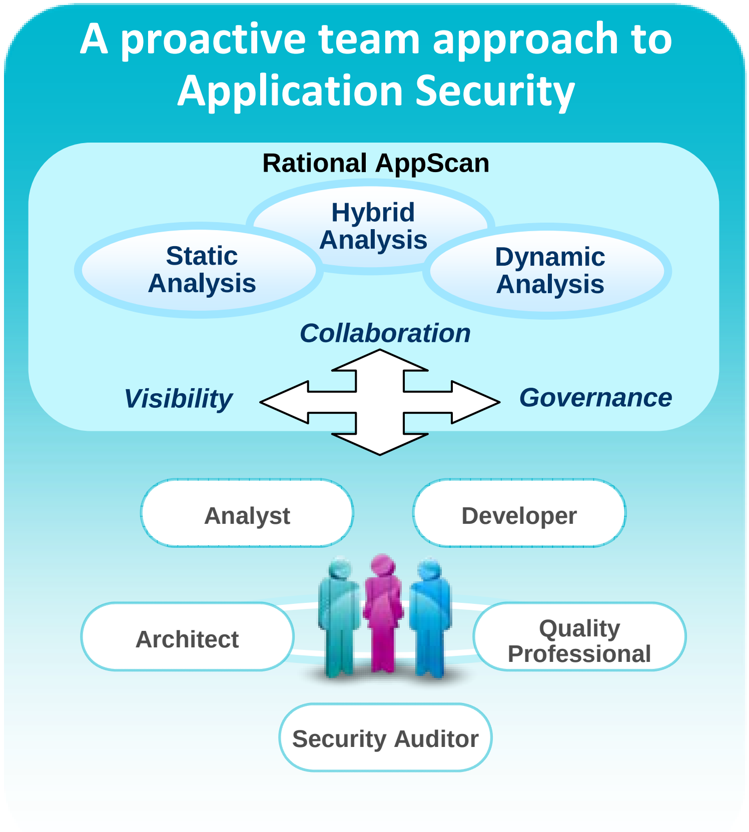
Providing Oversight and Governance

"We were able to increase the participation of the IT community in web application scanning"

Alex Jalso, Assistant Director, Office of Information Security, WVU

Organizations need to take a ***proactive approach*** to Application Security

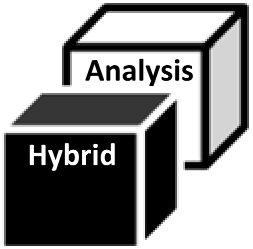
- **Embed security testing early** in the development lifecycle to support agile delivery demands
- Bridge the gap between "Security" and "Development" through **joint collaboration and visibility**, enabling regulatory compliance
- Integrate security testing **into the development lifecycle**, through interfaces to development tools



One specific AppScan feature: Javascript Analyzer

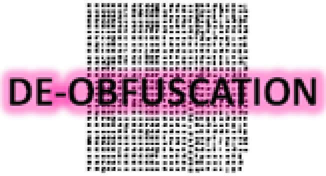
In AppScan Standard 8.0, we shipped JSA – a unique hybrid scan engine to auto-detect client-side issues such as:

- DOM-based XSS
- HTML5 Notification API Poisoning
- HTML5 Client-side Stored XSS
- Phishing through Open Redirect
- HTML5 Web Storage API Poisoning
- HTML5 Web Worker URL Manipulation
- HTML5 Client-side SQL Injection
- Email Attribute Spoofing



STRING

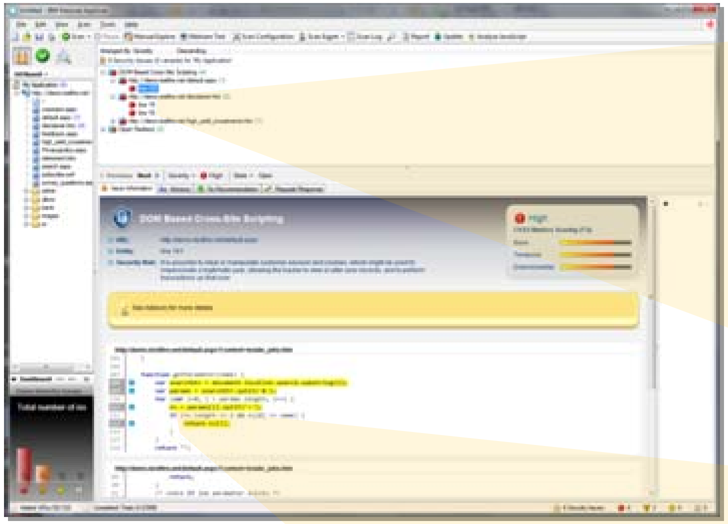
/* analysis */



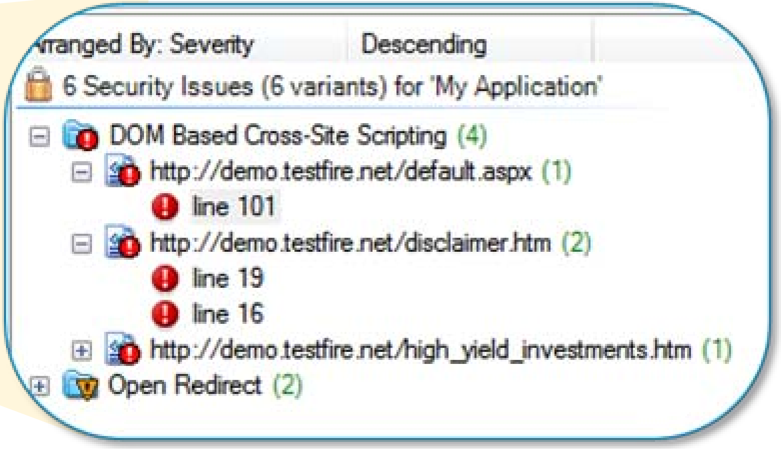
HTML5

Viewing JSA Results in AppScan

AppScan Standard – Scan Results



Vulnerable URL and line of code

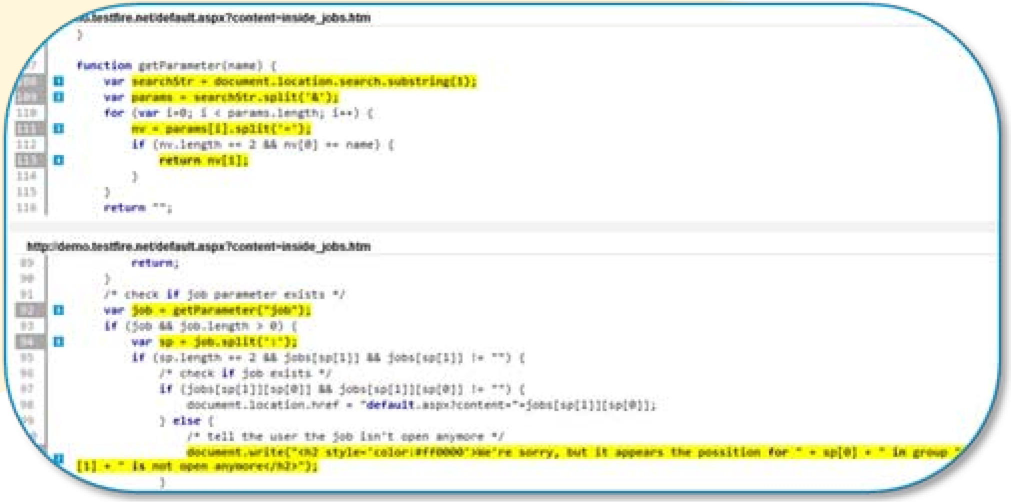


Arranged By: Severity | Descending

6 Security Issues (6 variants) for 'My Application'

- DOM Based Cross-Site Scripting (4)
  - http://demo.testfire.net/default.aspx (1)
    - line 101
  - http://demo.testfire.net/disclaimer.htm (2)
    - line 19
    - line 16
  - http://demo.testfire.net/high_yield_investments.htm (1)
- Open Redirect (2)

Tainted data flow information



...o.testfire.net/default.aspx?content=inside_jobs.htm

```
}

function getParameter(name) {
    var searchStr = document.location.search.substring(1);
    var params = searchStr.split('&');
    for (var i=0; i < params.length; i++) {
        nv = params[i].split('=');
        if (nv.length == 2 && nv[0] == name) {
            return nv[1];
        }
    }
    return "";
```

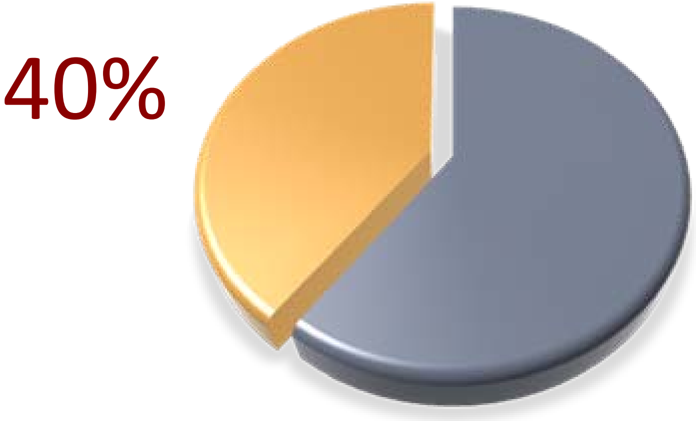
http://demo.testfire.net/default.aspx?content=inside_jobs.htm

```
            return;
        }
        /* check if job parameter exists */
        var job = getParameter("job");
        if (job && job.length > 0) {
            var sp = job.split(':');
            if (sp.length == 2 && jobs[sp[1]] && jobs[sp[1]] != "") {
                /* check if job exists */
                if (jobs[sp[1]][sp[0]] && jobs[sp[1]][sp[0]] != "") {
                    document.location.href = "default.aspx?content="+jobs[sp[1]][sp[0]];
                } else {
                    /* tell the user the job isn't open anymore */
                    document.write("<h2 style='color:#FF0000'>We're sorry, but it appears the possition for " + sp[0] + " in group "
[1] + " is not open anymore</h2>");
                }
```

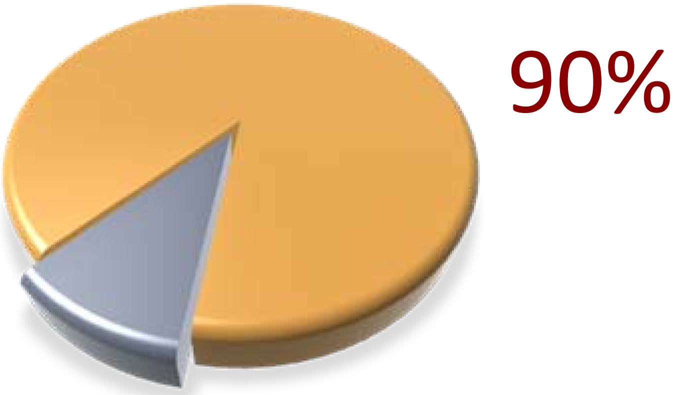
JSA Analysis Algorithms Enhanced

- Our original JSA research whitepaper, showed that out of the Fortune500 + 178 most popular internet sites, 14.5% were found to be riddled with client-side JavaScript vulnerabilities
- We spent some time improving our analysis algorithms….

Apps vulnerable To Client-side JavaScript vulnerabilities



Applications with issues in 3rd Party JavaScript code



Why IBM Security: Breadth, deep expertise, integration

Leadership

- "After doing our research, we determined that IBM was a leader in the field of dynamic application scanning." *Alex Jalso, Assistant Director, Office of Information Security, WVU*
- Identified as a Leader in Gartner SAST Magic Quadrant, December 2010
- Identified as a Leader in Gartner DAST Magic Quadrant, December 2011
- Pioneer of new hybrid analysis techniques, including Correlation, JavaScript Analyzer and GlassBox
- Pioneer of developer-friendly solutions

Integration

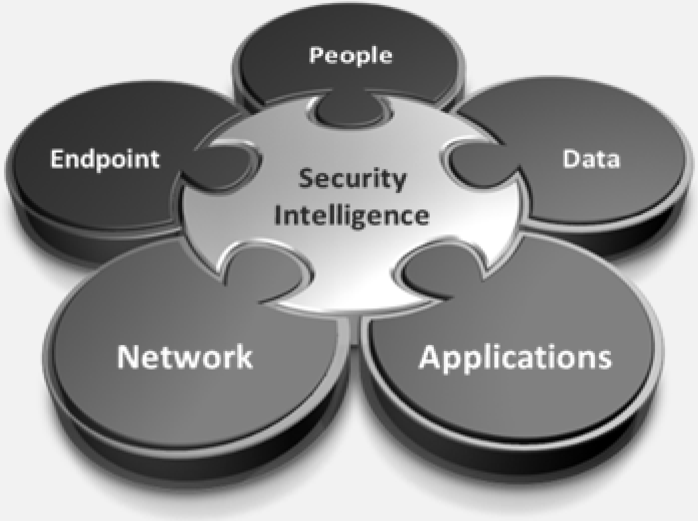
- Integration with IBM AppScan and SiteProtector to enhance web application security through IPS policy modification from application vulnerability data
- Integrates with IBM Rational development lifecycle solutions to enable collaboration between security and development teams

Expertise

- "We turned to IBM because they offered both the technology leadership and the deep security expertise…"

  Marek Hlávka, Chief Security Officer, Skoda Auto

Think Integrated.



ibm.com/security

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.