RAPID7

WEB SECURITY AND ASSESSMENT

Michael Lai

Senior Security Sales Engineer

CISSP, CISA, MBA, MSc, BEng(hons)

NASDAQ: RPD

Delivering Security Data & Analytics

that revolutionize the practice of cyber security

5,100+	37%	99	800+
Customers	Fortune 1000	Countries	Employees

We'd Love to Partner with You

Customer Focused

RAPID7 COMMUNITY

RAPID7 VOICE

2016 UNITED RAPID7 SECURITY SUMMIT

Highly Commended

tsia STAR AWARD 2015

SANS BEST OF 2014 WINNER IN Vulnerability Assessment

AUSCERT AWARDS 2014 WINNER Best Security Initiative

BEST PLACES TO WORK BOSTON BUSINESS JOURNAL 2015

2014 SILVER STEVIE WINNER FOR SALES & CUSTOMER SERVICE

SC MAGAZINE

SC MAGAZINE AWARDS 2015 Europe HIGHLY COMMENDED

SC MAGAZINE AWARDS 2015 WINNER Honored in the U.S.

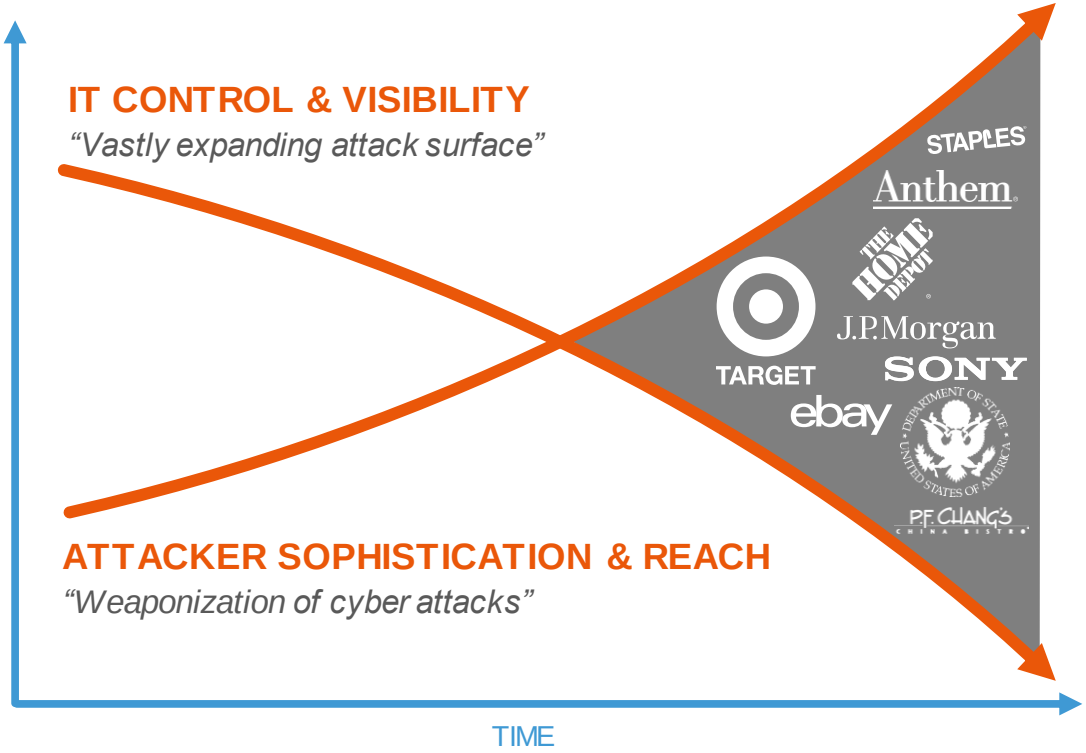
Trusted By 5,100 Organizations

DBS aetna amazon HUAWEI Johnson & Johnson ORACLE Nasdaq

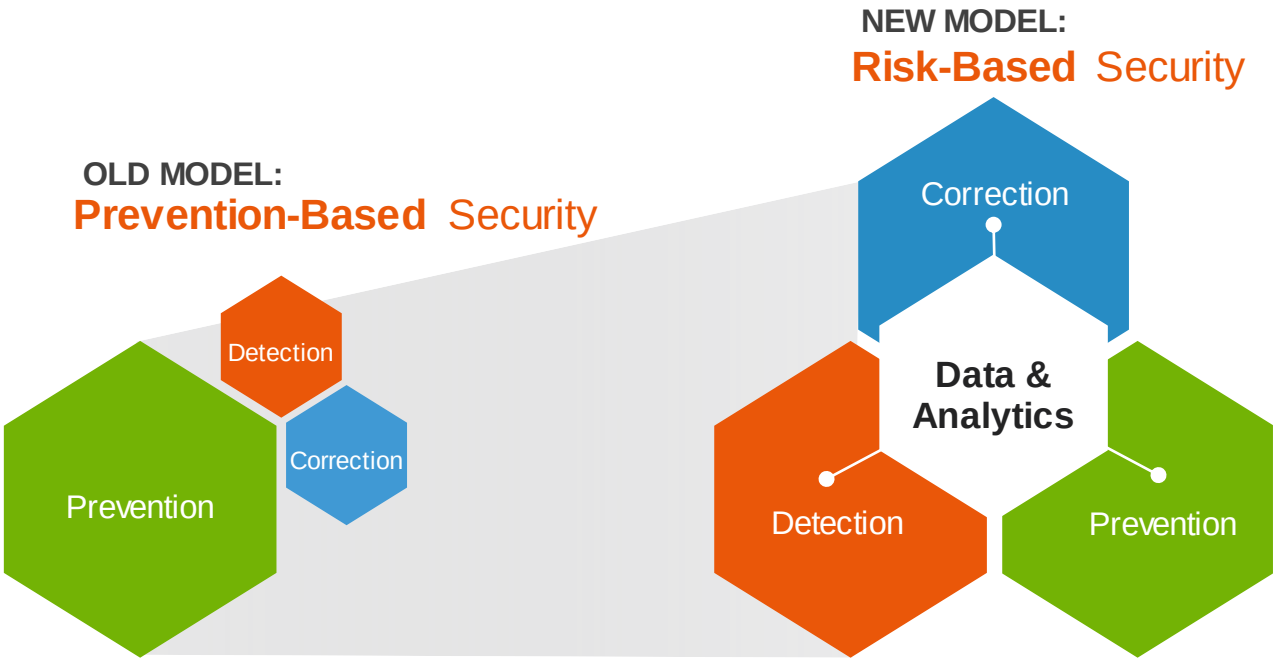
hp Microsoft IBM Sands LAS VEGAS SANDS CORP. virgin atlantic Walt Disney SAP

RAPID7

New Explosion Of High-Impact Cyber Attacks



Massive Shift to Risk-Based Approach to Security



By 2020,

60%

of enterprise information security budgets will be allocated for

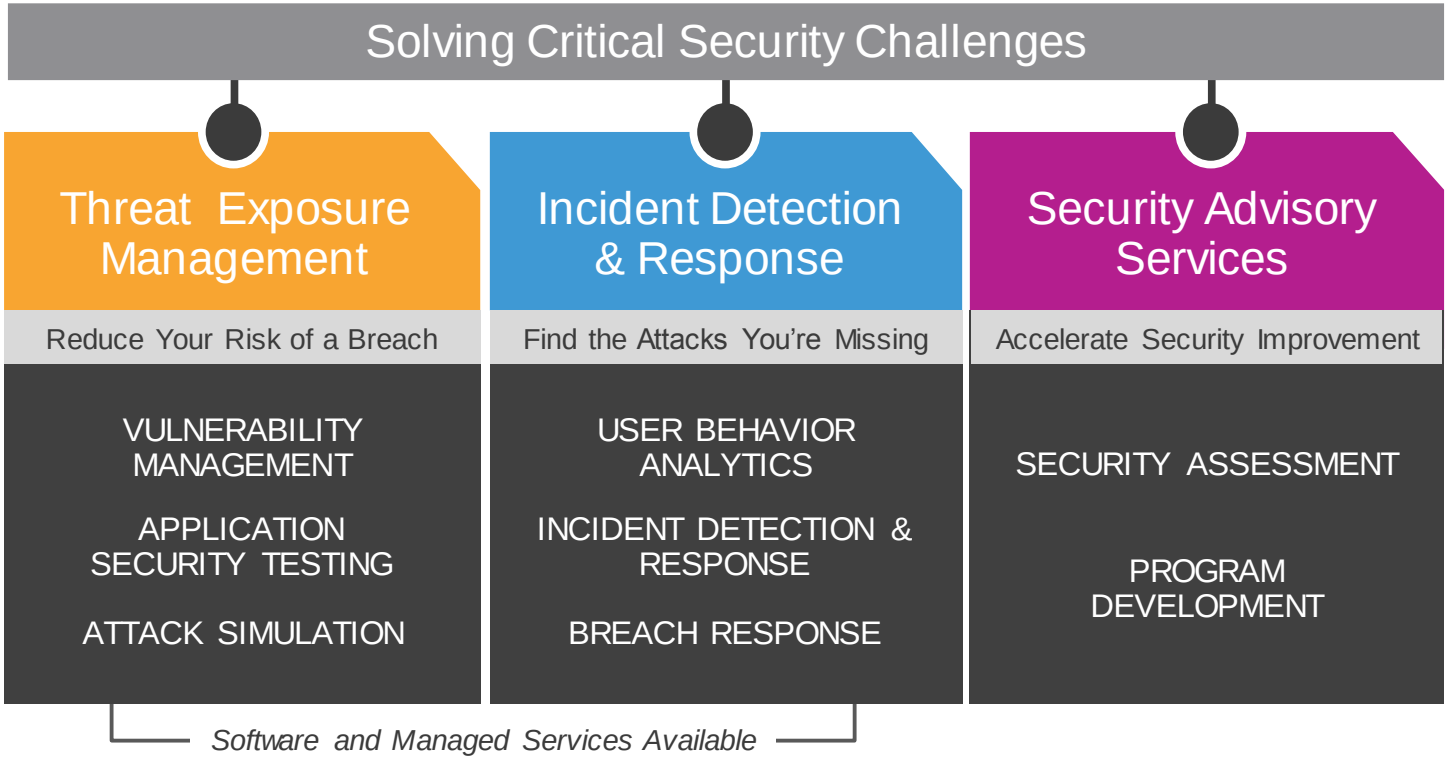
rapid detection and response approaches

up from less than 20% in 2015.

– Gartner: "Shift Cybersecurity Investment to Detection," dated 7 January 2016

RAPID7

Rapid7's Innovative Solutions



OWASP TOP 10 EXAMPLE

OWASP Top 10 2013

- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross Site Scripting
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Known Vulnerable Components
- A10 – Unvalidated Redirects and Forwards

Web application attacks are the most common attack pattern, representing **40% of all breaches.**

- 2016 Verizon Data Breach Investigations Report

RAPID7

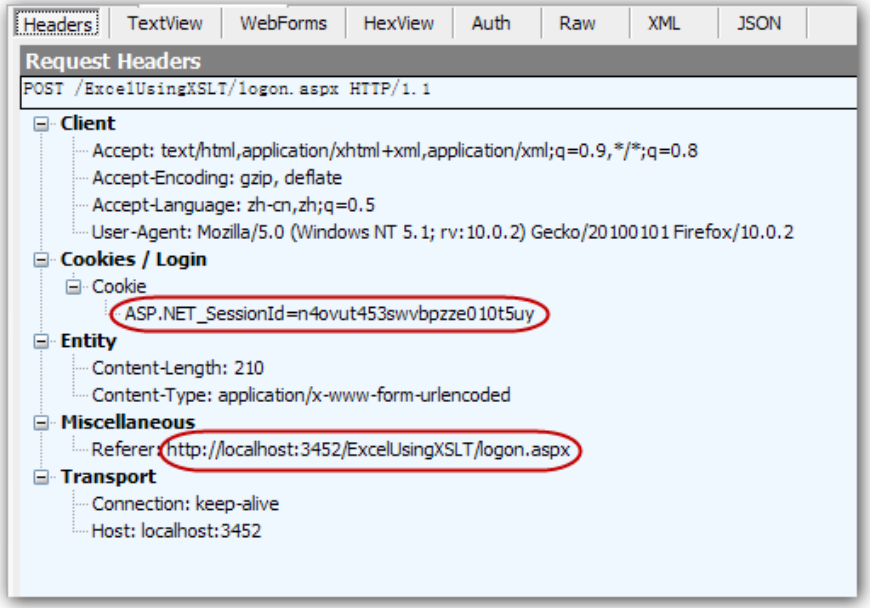
A1 - Injection

- Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- One approach, according to the SQL error message, rewrite the input to bypass the control logic.
- If input is ***'or'1*** , the statement becomes ***Select * From Table where username='admin' AND password='or'1'***

RAPID7

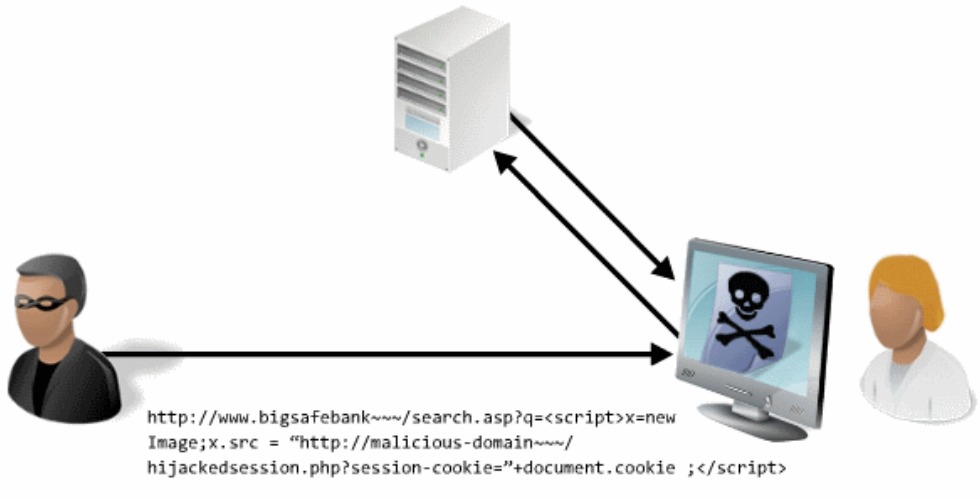
A2 – Broken Authentication and Session Management

- General speaking, the vulnerability allows bypassing the authentication control.
- There are many approaches such as brute force and stolen cookie.



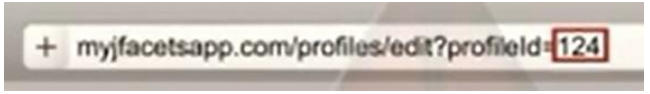
A3, A8 – XSS and CSRF

- XSS enables attackers to inject client-side scripts into web pages viewed by other users. Usually the script is hidden in the request from the victim (E.g. Phishing email with a link to a trustable site but with XSS vulnerability).
- Protection can be done not only at the web site, but also exist at the browser.
- CSRF needs the script run with a valid credential (usually due to cookie reuse). One case is the script would transfer money to another account if the victim has already logged in the bank.



A4 – Insecure Direct Object References

- Through simple and easy way to bypass the control to access some object.
- You only need a browser and know how to count.
- Other example is some discussion portal site has VIP zone which can be accessed after login. But the login can be avoided if you put any VIP URL directly.



A5 – Security Misconfiguration
A9 – Using Known Vulnerable Components

- Security Misconfiguration is usually due to the default is “Allow All” but not “Deny All”.
- Using Known Vulnerable Components is due to component has vulnerability identified (e.g. OpenSSL Heartbleed).
- A5 and A9 sometime are overlapped such as using default ID and PW of Apache.

Revoke permissions on vulnerable packages to mitigate impact

Execute permissions for specific packages may be revoked from untrusted users by running the following command on the Oracle server as a DBA. `REVOKE EXECUTE ON <SCHEMA>.<PACKAGENAME> FROM <USER|GROUP> FORCE;`
Where PACKAGENAME is the name of a vulnerable package, SCHEMA is the schema which the package resides in, and
…

This will address the following 18 issues:

- Oracle DBMS_AQADM_SYS SQL Injection (oracle-dbms_aqadm_sys-sql-injection)
- Oracle DBMS_CAPTURE_ADM_INTERNAL Buffer Overflow (oracle-dbms_capture_adm_internal-bof)
- Oracle DBMS_CDC_IPUBLISH Buffer Overflow (oracle-dbms_cdc_ipublish-sql-injection-bof)

…

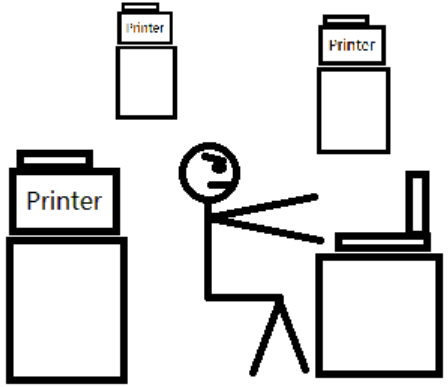
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A10 – Unvalidated Redirects and Forwards

- A6: The attacker can get the sensitive data such as ID card number, credit card number through different methods such as sniffer a non-encrypted connection or other Top 10 vulnerabilities.
- A7: The hacker can bypass the access level control. The problem is usually due to the request is not validated. An example is some discussion portal site has VIP zone can be accessed after login as a normal user and then input the VIP URL directly.
- A10: Vulnerability is due to unsecure redirect to avoid the security control or

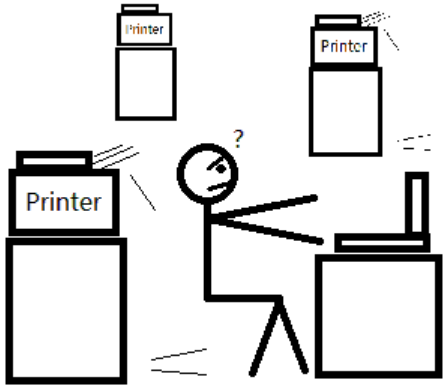
  e.g. Redirect to a phishing site http://www.goodsite.com/redirect.jsp?url=badsite.com
  e.g. Avoid internal control http://www.example.com/boring.jsp?fwd=admin.jsp

WEB ASSESSMENT

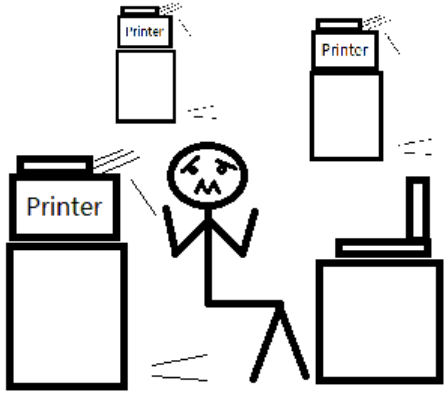
A Real Ghost Story In Hong Kong



9pm, Michael worked alone at the office where most of the light was turned off.



12am, 1st network printer started to print test page, and then the 2nd printer. Michael started to be scare.



12:10am, all printers kept printing out the test page. Michael was very scare and kept saying “god saves me, I am too young to die”.

The Truth Of The Ghost – Web Robot Scan The Web

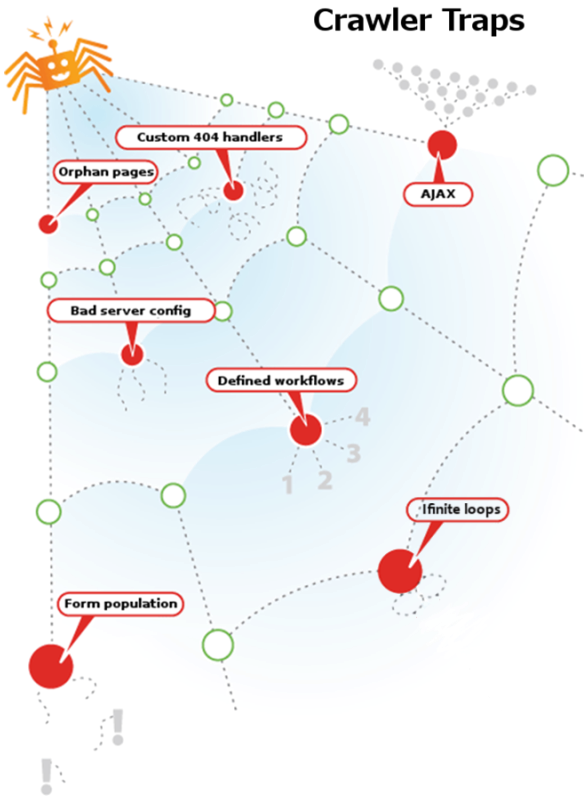
- IT setup to run vulnerability scan to the office network at the mid-night.
- The web scan is performed by the robot which will crawl the pages, do some operations such as sending different characters to the server.
- Once the robot crawl the network printer management page and find the “Test Page” button, he will keep pressing it.
- The robot found and click the “Factory Default” button hence no one could scan until configured the printer again.
- **Key Message: More scan time, more test will be run by the robot and more vulnerability can be found.**

Case: A Well Known Online Game Was Hacked

- First attack in Apr 11 and 100m users' info e.g. credit card was exposed.
- A consultant team from US was employed to study the problem and the final solution was deploying a WAF.
- The hacker had no time limitation to scan the web app and discover new vulnerability that not found by the consultant team.
- Second attack in Oct 11, another 100k employees' info disclosed. No one knew how many user info was stolen.
- Once the company found and fixed the SQL injection at the Apache server, there was no more incident.

3 Basic Steps Of Web Assessment

- Crawl – Spider the site and look for forms and active content. Other approach is understanding the request format that the server is looking for.
- Test – Based on the crawl finding, input unexpected content to the server. Vulnerability is identified according to the server response.
- Validation – If extra proof is needed, validation (usually manual work) will follow, such as sending a request with command to change the database.



ASSESSMENT SOLUTION

Choosing The Best Web App Security Scanner

by Chirita Ionel, OWASP Chapter Broad Member

What Scanner Should be

- Wide Coverage
- Fast scans
- Low number of false positives
- Low number of false negatives
- Scalability
- Easy to use
- Permanent vulnerability DB updates
- To be Cheap !?

Evaluation Criteria

- Protocol support
- Authentication
- Session management
- Crawling
- Data Parsing
- Testing
- Command and control
- Reporting
- Hardware Requirements & support

RAPID7

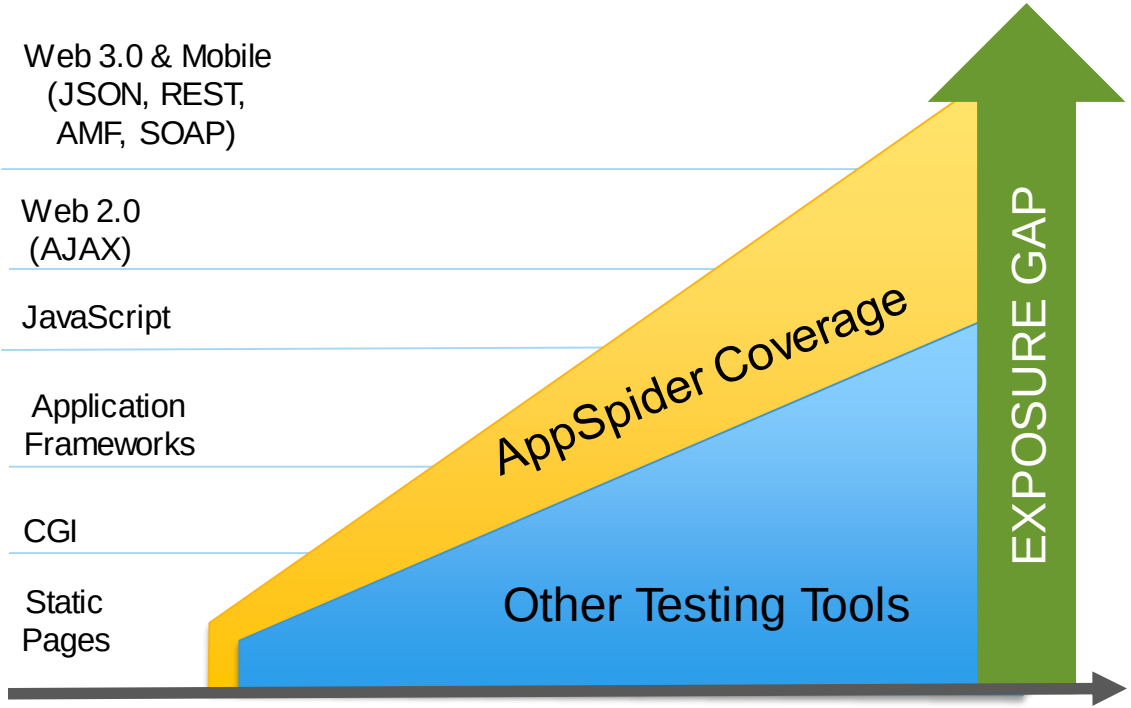
Complete Web Vulnerability Management Solution

Layer	Example	Solution Highlight
User Interface	Web page, form, e.g. query page	Customer needs to define the solution such as a policy at the WAF or recoding.
Code	Self developed code, e.g. Java	
Middle Layer	Deliver web service, e.g. Apache	Vulnerability from the common software, usually have well known solution, e.g. patch.
OS	OS platform, e.g. Linux	

- From the Online Game case, if there is a vulnerability at the middle layer, it may appear at different parameters on multiple web pages.
- Complete Solution
  - 1. Add the policy to the WAF/IPS as temporary solution.
  - 2. Test the Web Server upgrade impact to the web and upgrade it.
  - 3. Remove the added WAF policy.

Assessment Consideration

- Coverage for modern applications
- Authentication & maintaining session
- Crashing, incomplete scans, needs training
- Accuracy: false +ve/-ve
- Cumbersome reports
- Support



Today to Future

- Understand the application technologies and their security requirements, e.g. AJAX, JSON, REST, AMF, SOAP, SPA - Dynamic content and cannot be crawled, these APIs are used by both mobile and web application.
- Test the scanner capabilities. Ask the vendor to see how the solution to scan the modern APPs such as AJAX, JSON, SPAs and how the scanner to handle the parameters.
- Verify how the scanner works with the modern APPs. It includes importing proxy logs and testing Swaggers APIs automatically. Don't forget to verify the ability in authentication and session management.
- Future Proof: Ensure your security investments are future-proofed by talking to your vendor about how their solutions will be able to handle new technologies as they arrive.
- *APPs assessment should be integrated in the development cycle in order to fix the vulnerability before the launch.*

THANK YOU

michael_lai@rapid7.com