Operationalizing Web Application Security – QSC 2018

Frank Catucci – Director, Application Security and DevSecOps
Welcome to QSC 2018 and a Quick Introduction

Who am I?: Some of you may know me already from my past life with Qualys. If not, I am currently the Director of Application Security and DevSecOps for ImagineX Consulting.

Previously, I was the Director of Product Management for Application Security at Qualys for 4+ years.

I am also an appsec and infosec enthusiast, hacker and consultant during the day but also security researcher by night and by life.

I bring to you decades of experience spanning Fortune 500 enterprise, financial services, university/higher education, government, and a fair share of start-ups and businesses, both public and private, which I feel grants me the ability to see and lead information security consulting and advisory with a unique, complete, and widely encompassing approach in all aspects of cybersecurity.
Quick Profile

Frank Catucci, CISSP

Professional Profile
Frank previously served as the Director of Web Application Security, Product Management and Subject Matter Expert for Qualys. Before that he held a variety of roles and consulting engagements across many industries.

Frank has over 20 years of experience in the Information Technology and Information Security field that spans Fortune 500 enterprise, financial services, university / higher education, government, health care, legal, start-up, public and private industries.

Frank is a contributor to, and current chapter president, of his local Open Web Application Security Project (OWASP) chapter. Frank also conducts security research, bug hunting, and often speaks at information security conferences and events.

Personal Mantra
“If opportunity doesn’t knock, build a door,”
-Milton Berle
Objective and what I am here to discuss with you today: Repeatedly now, ImagineX Consulting has been engaged to transform existing application security programs and one in particular for a very large financial tech company, from a competitive product, to Qualys WAS.

Today I will illustrate how Qualys WAS' scale, automation and coverage enabled this client to overcome traditional application scanning constraints and transition to a successful new appsec program that leveraged manual testing services and reporting built around the Qualys Cloud Platform WAS Solution.

We will dive in and look at exactly how this combined approach can be used to increase coverage, scale and effectiveness, and to decrease application security risk.
This organization’s application security challenges were not unique. But, that does not make them any less important!

- Internal staff were already at their limits with time, skill, priority and focus.
- Apps are dynamic and ever changing; their coverage was not.
- Internal scanning is an imperative capability. This was difficult with other solutions.
- Automated scanning cannot, and never will be able to, find all vulnerabilities. Manual testing is required.
- Spending far too much money for questionable results.*
- Scale and automation.
- Reporting and visibility.*
- Actionable and accurate data relayed to development groups.
How We Address These Challenges

By delivering effective transformation from competing product with little real insight and control, to Qualys WAS with ImagineX Professional Services!

- A single report of all your Web Applications
- Aggregated findings across some or all of your applications to find areas of weakness
- Hover over findings, vulnerabilities or applications to get counts
- Highly Customizable via filters and tags
- List of most vulnerable Web Applications
- A one stop inventory of all your onboarded Web Applications
- Filter results to pinpoint desired applications
- Quick Actions to perform many tasks via drop down menu
- Monitor all your vulnerabilities in one place
- View, ignore, patch or retest via drop down menu
- Filter by severity, or age
- Utilize tagging for granular reporting
How ImagineX and Qualys Work Together

ImagineX Provides and Delivers

• Qualys expertise. Our Qualys consultants consist of former Qualys employees and customers. Together we have over three decades of Qualys expertise in all of the modules and diverse industries

• A comprehensive review of WAS program goals – what are you trying to achieve and how?

• Configuration review of Web Apps and Option Profiles

• Scan diagnostics

• Best Practices

• Review of any pain points or difficulties you may be having

• Future goals and plans and how to best achieve them

Qualys Provides and Delivers – Best in Breed DAST

• Robust API

• Scalable and automated solutions that provide accurate and actionable data and results

• High value-to-spend ratio solutions

• Low rate of false positives and false negatives

• Insight into dynamically changing applications AND perimeters

• Support of modern architecture, languages and app support including CMS systems

• DevSecOps capable out of the box, especially with plugins and extensions

• All in one comprehensive SaaS security solution with multifaceted visibility
What This Particular Case Study and Project Looked Like

The plan and understanding:

• Desire for the client’s security experts to demonstrate that Qualys can be used as the primary web app scanner, with the ability to cover all applications that are currently covered by the competitor;
• Internal Scanning appliances would be deployed on an internal network (for the first time) and scans against non-production test applications will be completed. Supplemented with expert validation of findings to eliminate false positives.
• Documentation delivered to support integrating the Qualys web application vulnerability scanning into client’s operations.
### The Approach

Our phased approach:

<table>
<thead>
<tr>
<th>Phase 1 Discovery &amp; Configuration</th>
<th>Phase 2 Manual Assessments</th>
<th>Phase 3 Internal Appliances</th>
<th>Phase 4 Coverage Monitoring</th>
<th>Phase 5 Roll Out Readiness</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Duration:</strong> 4.5 Weeks</td>
<td><strong>Duration:</strong> 2 Weeks</td>
<td><strong>Duration:</strong> By $date$</td>
<td><strong>Duration:</strong> 4 Weeks</td>
<td><strong>Duration:</strong> 3 Week</td>
</tr>
<tr>
<td><strong>Scope:</strong></td>
<td><strong>Scope:</strong></td>
<td><strong>Scope:</strong></td>
<td><strong>Scope:</strong></td>
<td><strong>Scope:</strong></td>
</tr>
</tbody>
</table>
| - Onboard 250 external applications into Qualys WAS | - Conduct 3 pentests to validate capabilities  
  - App1  
  - App2  
  - App3 | - Deploy Qualys virtual scanner appliances onto internal network.  
  - Review scanning architecture  
  - Configure Qualys WAS to newly deployed scanner appliances  
  Note: Virtual scanner appliances were deployed to DMZ and DEV VLANS | - Complete Internal scanning pilot  
  - Scan and compare the following internal applications;  
  - Portal  
  - App3  
  - App4  
  - App5 | - Produce operating procedures  
  - Documentation  
  - Run Books to allow for a repeatable and detailed deployment and continuous program |
The numbers:

• 210 web applications onboarded into the Qualys Web Application Scanning Product
• 37 separate authentication records created
• 5 option profiles created
• 2,374 total vulnerabilities detected
• 182 high-severity vulnerabilities detected
• 772 medium-severity vulnerabilities detected
• 1,420 low-severity vulnerabilities detected
## Comparison Metrics

### More numbers:

<table>
<thead>
<tr>
<th>Production App - Sample 1</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>Critical / Level 5</td>
<td>High / Level 4</td>
<td>Medium / Level 3</td>
<td>Low / Level 2</td>
</tr>
<tr>
<td>Competitor</td>
<td>17</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Qualys WAS</td>
<td>25</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Production App - Sample 2</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>Critical / Level 5</td>
<td>High / Level 4</td>
<td>Medium / Level 3</td>
<td>Low / Level 2</td>
</tr>
<tr>
<td>Competitor</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Qualys WAS</td>
<td>68</td>
<td>1</td>
<td>0</td>
<td>17</td>
<td>15</td>
</tr>
</tbody>
</table>
Web Application Scanning Maturity Model

Maturity Model:

- **Lvl 1 - Reactive**
  - PEOPLE: NOVICE
  - PROCESSES: AD HOC
  - PROGRAM: MANUAL
  - OPERATIONS: EXPERIMENTAL
  - Level: Reactive

- **Lvl 2 - Repeatable**
  - PEOPLE: BEGINNER
  - PROCESSES: MANAGED
  - PROGRAM: MOBILIZED
  - OPERATIONS: SECURE
  - Level: Repeatable

- **Lvl 3 - Automated**
  - PEOPLE: INTERMEDIATE
  - PROCESSES: DEFINED
  - PROGRAM: AUTOMATED
  - OPERATIONS: ENABLED
  - Level: Automated

- **Lvl 4 - Integrated**
  - PEOPLE: ADVANCED
  - PROCESSES: QUANTITATIVE
  - PROGRAM: INTEGRATED
  - OPERATIONS: INTEROPERABLE
  - Level: Integrated

- **Lvl 5 - Intelligent**
  - PEOPLE: EXPERT
  - PROCESSES: OPTIMIZED
  - PROGRAM: PREDICTIVE
  - OPERATIONS: OPTIMIZED
  - Level: Intelligent

- **Uninformed**
  - Secure & Automated Deployment
  - Predictive Intelligence Through Analytics
Recommendations for next steps?

Shift Left:

- Breaches average cost is $4 million
- Good Security Hygiene – Preventative

Reduce Unplanned Work

- Unplanned work affects the entire organization
- Avoid business-related project delays
- Audit Fees are Costly
We will leverage modern automation tooling and DevSecOps processes to deliver value efficiently.
ImagineX Helps With AppSec Health Checks

Application Security Health Checks description:

- Web application security assessment focused on discovery and identification of web assets and their associated highest risk vulnerabilities, including the OWASP Top Ten.
- Effective way to identify high-risk web application vulnerabilities that would be easily identified by attackers.
- Provide clients a cost-effective way to quickly check security posture of applications.

**Key Strengths**

- Quick. High risk focus. Ideal for tight schedules or budgets. Easily incorporates with Qualys WAS to expanded upon Application Security capabilities.
Comprehensive Application Security Assessments description:

- Service also commonly known as Application Pentesting.
- A complete web application security assessment identifying vulnerabilities such as the OWASP Top Ten, business logic flaws and other web application security weaknesses that may not or cannot be detected with an automated scanner.
- A combination of automated discovery and vulnerability scanning with experienced professionals manually testing to provide the highest level of security assurance and advanced vulnerability identification.

Key Strengths

- Eliminate the need to hire AppSec specialists, or subsidize the resources you do have. Leverage expert technical knowledge and expertise.
Managed AppSec Qualys WAS Scanning Services

Managed Application Security Scanning description:

- Continuously discover and monitor web applications for security vulnerabilities utilizing Qualys WAS.
- Recurring automated web application vulnerability scanning and confirmation of findings.
- Supplemented with expert validation of findings to eliminate false positives.

Key Strengths

- Agile, Quick, Expert verification lowers remediation efforts. Ensure resources are spending time addressing vulnerabilities instead of managing a testing platform.
ImagineX Consulting is a business and technology consulting firm whose goal is to help our clients transform their businesses by embracing lean delivery techniques and emerging technologies such as cloud, information security, and mobile. Through the use of our experimentation techniques and modern delivery methods, we assist our clients in driving higher quality solutions to market earlier. Our execution success is rooted in our unique local model that is supported by our industry and subject matter specialists. Our ImagineX culture thrives on entrepreneurship, risk taking, mutual trust, teamwork, encouraging change, and letting our consultants own their way of working.

ImagineX Consulting is headquartered in Denver with offices in Atlanta, Raleigh, Washington, DC, Tel Aviv, Israel and Toronto. Our ImagineX Labs are located in Toronto, Canada and Sofia, Bulgaria.