Security Assessment of
Waratek AppSecurity for Java

Executive Summary
Executive Summary

Security Assessment of Waratek AppSecurity for Java

Introduction
Between September and November 2014 BCC Risk Advisory (www.bccriskadvisory.com) performed a security assessment of Waratek AppSecurity for Java, which is designed to prevent SQL Injection attacks on legacy applications built on insecure code due to weak secure coding practices. The assessment consisted of simulating attacks from malicious hackers with an aim to gaining a foothold in the target application and extracting or manipulating the data stored in the back-end Oracle relational database.

Waratek AppSecurity for Java - Securing Java from the Inside Out

Java is used for the majority of production Enterprise applications deployed today. However, these applications lack the ability to defend themselves from today's targeted, dynamic attacks. Existing attempts to protect applications rely on static code analysis, application best practices, or network devices such as web application firewalls (WAF), none of which are completely effective.

Waratek introduces a completely new and much more powerful and operationally realistic approach. Known as Run-time Application Self-Protection, or RASP, this class of solution provides runtime application self-protection, securing Java applications and preventing attacks with no code changes, agents or network devices. Gartner has identified RASP as “A must-have, emerging security technology”.

Waratek supports several key use cases to monitor and defend data-centre or cloud deployed enterprise applications:

- SQL Injection Attack Mitigation: Waratek is focused on preventing SQL Injection attacks, as these are the most damaging with respect to bulk loss of sensitive data.
- Zero Day Attack Mitigation:
- Compliance

And because Waratek operates at the JVM layer, all three use cases are supported for both internally-developed code as well as third-party library software.
Executive Summary

Why BCC Risk Advisory?

BCC is a company formed by OWASP Global board member, Eoin Keary. We have experience in assessing thousands of websites for many organisations across the globe using both our edgescan™ service and traditional consultancy model. We specialise in software security from secure development to penetration testing and threat modelling.

We work for some of the world’s largest pharmaceutical, media, software development and financial services organisations and have trained thousands of developers in secure application development across the globe in the last 4 years.

We provide a cloud based Software-as-a-Service (SaaS) solution, edgescan™ which continuously tests public internet facing assets (servers, web applications) for the latest vulnerabilities and weaknesses, providing our clients with easily actionable data and management information in order to help mitigate risk.

SQL injection:

SQL Injection is used to attack data applications by inserting malicious SQL statements into an entry field for execution. A successful SQL injection exploit can read and modify sensitive data in the database, execute administration operations on the database and more. According to some estimates, SQL Injection is responsible for more than 80 percent of the total records stolen in hacking incidents. It is considered the number 1 application security threat by both OWASP and SANS.

Objective:

Waratek AppSecurity for Java is claimed to be a new approach to the problem of preventing SQL Injection in legacy applications where the source code may not be available, namely, Runtime Application Security Protection (RASP). BCC Risk Advisory was asked to verify its effectiveness at preventing SQL Injection attacks against an Oracle database.

Put simply: Could the testing verify that Waratek AppSecurity can detect (and prevent) if any tainted data (data from an external source) contained additional ANSI SQL Syntactical elements and hence a SQL Injection attempt.

Approach

The application was a purposely-built insecure application running on a Java 7 supported Java Virtual Machine utilising a relational database from Oracle 11g.

The assessment was performed by utilising a combination of common open source, commercial tools and manual techniques, in order to exploit the SQL Injection vulnerabilities contained within the application. The approach was in 2 phases:

1. Verify the application had indeed SQL Injection vulnerabilities and to what extent these could be exploited.

2. Verify once Waratek AppSecurity was enabled that the vulnerabilities were protected by Waratek AppSecurity and could not be exploited using both the initial successful exploitation techniques and in addition attempting to use more advanced techniques.

_Initially the application was verified to be insecure and vulnerable to SQL Injection attacks._

All of the requests in scope to the server and subsequently to the backend database could be manipulated by injecting ANSI SQL into the requests. The result of the successful attacks was to give the attacker the ability to Add, Update, Delete and extract data from the application regardless of the intentions, functionality of the application or how the application was intended to be used. In effect the application was vulnerable to SQL Injection and exploitable.

_The vulnerabilities discovered were very easy to find, verify and exploit and would result in a devastating attack against any business with such security weaknesses._


Upon enabling Waratek AppSecurity the testing methodology was re-run using the same attack methods and tools initially to substantiate if the previous techniques were still effective as before or if the Waratek AppSecurity actually detected and blocked the attack vectors.

Upon testing the vulnerable application with Waratek AppSecurity enabled it was clear the application was responding in a different manner. Upon further investigation the HTTP responses returned from the application indicated the application was not vulnerable to the same SQL Injection vectors as previously used. The application returned Oracle Syntax errors and also Waratek AppSecurity return/error codes indicating the attacks were no longer successful.

In order to further verify the robustness of the solution we executed further testing, but to no avail, by leveraging additional attack techniques such as encoding and WAF (Web Application Firewall) bypass & escaping attacks – _Listed in technical appendix_

Conclusion:

Waratek AppSecurity for Java appears to prevent SQL Injection attacks in the case of legacy Java based applications with an Oracle Relational database as a backend, without changes to the application source code required. It also appears to prevent/mitigate advanced SQL Injection techniques that are used to bypass certain Web Application Firewalls (WAF). It is our understanding that Waratek AppSecurity for Java does indeed dramatically improve the security of vulnerable legacy Java based applications.

In conclusion, our testing of Waratek AppSecurity for Java demonstrated that zero false positives were detected for the range of attack vectors used during testing.
Types of attacks and schemas used when assessing Waratek AppSecurity for Java

- Common SQL Injection attack vectors totalling in the thousands
- Changing encoding schemes (UTF-7, URL, Hex, Unicode)
- Null byte obfuscation
- Invalid Unicode and HEX attacks
- WAF (Web Application Firewall) bypass & escaping attacks.
- Capitalisation
- Whitespace placement
- Comment placement

Assessment Tools Used:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burp Professional</td>
<td>See Portswigger.net</td>
</tr>
<tr>
<td>ZAP (Zed Attack Proxy)</td>
<td>See owasp.org</td>
</tr>
<tr>
<td>SQLMap</td>
<td>See sqlmap.org</td>
</tr>
<tr>
<td>SQLIX</td>
<td>See owasp.org</td>
</tr>
<tr>
<td>SQL Power Injector</td>
<td>See sqlpowerinjector.com</td>
</tr>
<tr>
<td>Custom/bespoke scripts</td>
<td>BCC Risk Advisory</td>
</tr>
<tr>
<td>edgescan correlation engine</td>
<td>For internal tracking</td>
</tr>
</tbody>
</table>

Reference Material

Definitions

- [https://www.owasp.org/index.php/SQL_Injection](https://www.owasp.org/index.php/SQL_Injection)
- [https://www.owasp.org/index.php/Blind_SQL_Injection](https://www.owasp.org/index.php/Blind_SQL_Injection)

Prevention


WAF evasion

- [http://www.blackhatlibrary.net/SQL_injection/evasion](http://www.blackhatlibrary.net/SQL_injection/evasion)
Executive Summary

BCC Testing Team:

Eoin Keary

Summary

Eoin is a member of the Global Board and was president of OWASP (2011-2013). The role of the Executive Board is to set the direction of OWASP and to drive its strategic goals. He has over 20 years of experience in software security, and has worked for a number of companies, including a large company in the financial services sector. He has also been involved in a number of large-scale security projects, including Web Application Penetration Testing (WAPT) and PCI DSS. He is currently the principal consultant at edgescan.

Experience

- Member of the OWASP SAAM (Software Assurance Methodology) team.
- E&L-Auditor for national and international projects.
- Application Security Group and lead for the OWASP Europe and OWASP Europe.
- Lead for the OWASP Ireland application security event and OWASP Europe.
- Security application development manager and lead for hundreds of developers for private and public sector organizations.
- OWASP board member for the Irish chapter, involved with the OWASP community since 2007.
- Application security and mobile application security.
- 9 years of application development code development experience.
- 15 years of information security experience.
- Application development and security development toolset.
- OWASP Ireland international security conference 2009-2010.
- OWASP Ireland international security conference 2009-2010.
- OWASP Ireland international security conference 2009-2010.

Rahim Jina

Summary

Rahim graduated in 2002 from Trinity College Dublin, with a degree in Information & Communications Technology, specializing in Computer Security & Mobile Communication. He has over 20 years of experience in software security, having worked for a number of companies, including a large company in the financial services sector. He has also been involved in a number of large-scale security projects, including Web Application Penetration Testing (WAPT) and PCI DSS. He is currently the principal consultant at edgescan.

Experience

- Application security and mobile application security.
- 9 years of application development code development experience.
- 15 years of information security experience.
- Application development and security development toolset.
- OWASP Ireland international security conference 2009-2010.
- OWASP Ireland international security conference 2009-2010.
- OWASP Ireland international security conference 2009-2010.
Executive Summary

Owen Pendlebury

Summary

Owen graduated in 2009 from Dundalk Institute of Technology, with a degree in Computer Applications and Support and an honours degree in IT Management, specialising in web application development and networking. In 2009, Owen completed an MSc in Security & Forensic Computing from Dublin City University.

He has over 4 years experience in penetration testing working as part of a global attack & penetration team for a “Big 4” professional services company. He has in-depth experience of application and network penetration testing and has worked in this area with many local and global institutions.

Owen is a member of the Irish Board of OWASP. He also lectures at the National College of Ireland in web application and network security and secure application development.

Expertise

- Web application security
- Security source code review
- Network Security
- Global penetration testing
- Risk assessment
- Unix & Windows operating system security
- Firewall & web application firewall security
- VoIP Security
- Mobile Security
- Physical Penetration testing

Experience

- Member of the OWASP board

Owen has participated in numerous infrastructure and application penetration testing assignments, including:

- Internal and external infrastructure and policy based penetration tests for various global companies across a whole range of industry sectors.
- Penetration testing in specialist technologies such as wireless networking and Android application security.
- Web application and network penetration tests for major organisations in the financial services sector, consisting of ‘black-box’, ‘white-box’ and ‘grey-box’ testing.
- Reviewed all new web applications deployed throughout a financial services organisation to ensure they conformed with security standards.
- Performed a successful physical penetration test at a large investment bank’s premises in London City.
- Provided IT audit and control reviews in the following areas for financial services clients:
  - Change Management
  - Application Control Testing
  - IT Application and Network Security
  - IT Operations

Contact Information:

+353 876805277
owen.d@corporateadvisory.com
http://www.linkedin.com/pub/owen-pendlebury/18/142/552/