Case Study

Application Security Testing of a Global Ticket Booking eCommerce Application

BUSINESS SITUATION

Client developed a smart ticketing platform, designed in collaboration with over 700 venues across Australia, New Zealand, Asia, Canada, and the United States. As an industry first, it gives customers total customization, flexibility and control.

Packed with sophisticated intelligence including custom built CRM, full business API integration, the ability to build venues and seat maps in real time, along with visual and usable dashboard reports driven by Tableau – Ticket Search is a SAAS product with allow client and their customer to buy tickets over the internet and box office.

This product was configurable to be used to four different payment gateways including Stripe, SecurePay, Paypal, CyberSource.
Client was looking at vulnerability assessment and penetration testing for the entire SaaS solution including testing integrations with the payment gateways

SNAPSHOT

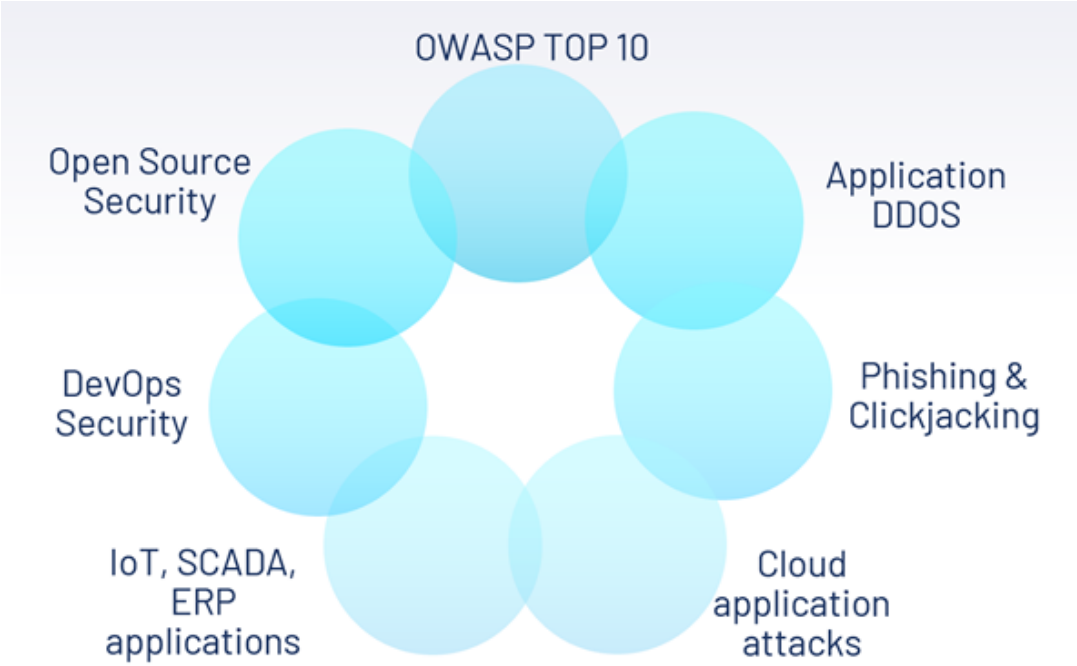
Industry:	Event Management and eCommerce
Business Unit:	Cyber Security
Services:	Web Application Security Testing

SOLUTION

Our testing methodology was adapted from the following security frameworks and vulnerability categories:

1. Open Web Application Security Project Framework **(OWASP)**
2. Web Application Security Consortium **(WASC)**
3. National Institute of Standards and Technology **(NIST)**

Our testing methodology was adapted from the following security frameworks and vulnerability categories:

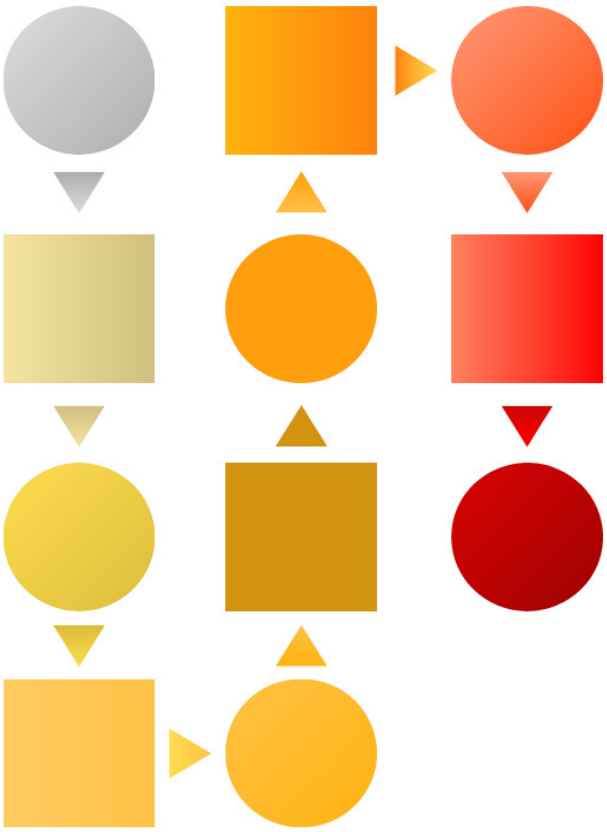


The assessment was limited to the following categories:

1. Grey Box Assessment
2. Vulnerability Assessment
3. Penetration Testing

WHAT WAS DEVELOPED:

Penetration testing approach



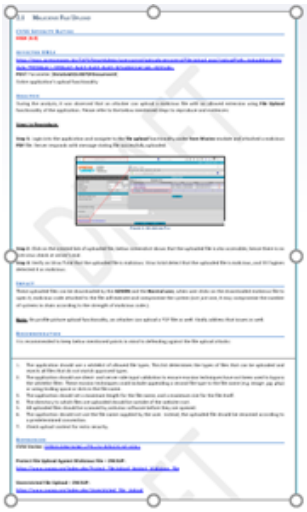
KEY TOOLS USED

- Nessus
- Netsparker
- BurpSuite Pro
- PortSecure
- KALI Linux
- Metasploit
- Cain and Abel
- Wireshark
- Pwdump
- Firewalk
- Ike-Scan, Ike-Probe, Ike-Crack
- Fport
- NTP Enumerator

TECHNOLOGY STACK

- ASP.Net
- AWS
- WebAPIs
- Tableau
- SQL Server
- AWS Lamba
- Dockers
- Node.js
- GitLab

REPORT FORMAT



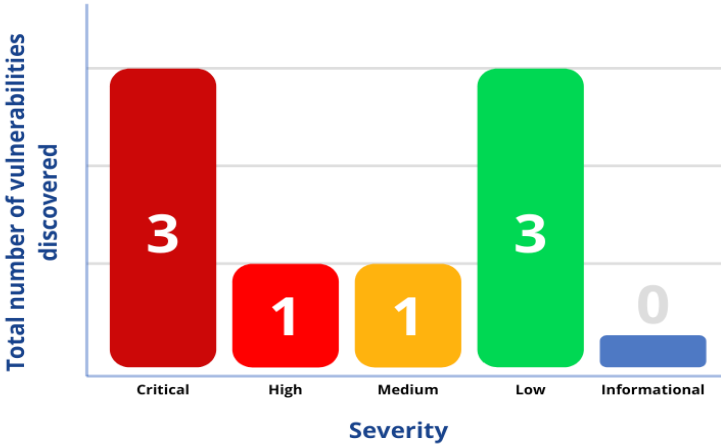
Sections (Technical Report)

- Issue Title
- Severity Level (as per CVSS Scoring)
- Affected URL & Parameters or IP address & Port
- Analysis (Including steps to reproduce with evidences)
- Impact (in business terms)
- Recommendation (including code snippets if need)
- References

BENEFITS

Number of Vulnerabilities found as per below:

- 8 key vulnerabilities found during penetration testing
- Timely fixes saved against any financial implications
- Provided secure development training to the client development team
- Reviewed and provided recommendation on client application design



Adactin is a premium Australian software consulting company dedicated to excellent software development and testing with a comprehensive service suite encompassing quality assurance, design and development services, data analytics products and other digital transformation enterprise solutions including quality ICT training programs. The company has a core competency and thought leadership position built around the science of IT development and testing application development.
For more information, please visit https://www.adactin.com

Sydney
Address: 14, Level 3, Civic Arcade 48-50 George Street
Parramatta NSW 2150 | Phone: (02) 9057 8016
Fax: +61 2 8824 9522 | Email: info@adactin.com

Canberra
Address: Unit 7A/1 Geils Court, Deakin ACT 2601
Phone: +61 429446670 | Email: info@adactin.com

Melbourne
Address: 416-420, Level 2, Collins Street, VIC 3000
Phone: (03) 9115 7477 | Email: info@adactin.com