PALADION LETTER OF OPINION

Paladion’s Letter of Opinion

NOVAtime Technology, Inc. – Application Security Assessment

NOVAtime 5000 Workforce Management / Time Attendance Solution (NOVAtimeAnywhere®)

Paladion carried out an extensive audit of the <Application Name> application and its systems from the perspective of an external adversary between <Test Start Date> and <Test End Date>. This test reveals an external adversary's view of the application and will help understand security preparedness against evolving threats.

Our assessment results conclude that the <Application Name> application has been designed and implemented with sufficient security controls implemented to protect against adversaries. The controls implemented to protect against threats were found to be adequate.

Based on the results of the tests conducted between <Test Start Date> and <Test End Date>, Paladion can confirm that there were <no/number> open Critical Risk, <no/number> open High Risk, <no/number> open Medium Risk, and <no/number> open Low Risk vulnerabilities identified at this time.

Paladion's assessment methodology, tests performed and tools used are presented below. Our methodology is based on the applicable standards from OWASP, PCI DSS, NIST CSF and OSSTMM.

Methodology

Paladion's approach to application security assessment is a structured 5 step process that requires a high level of manual testing and application understanding. Each of the steps is discussed below.

Understanding the application

It is very important that the team understands all of the features and functions of the application. The team does this by browsing through the application, going through the user manuals or, if required, a walkthrough of the application along with the application owner or developers. We work with you to ensure we are fully aware of its aims, functions, etc.

Creating the Threat Profile

Our penetration test focuses on uncovering any vulnerability that an adversary may potentially exploit.

The Threat Profile comprises a list of potential threats against the application that we have identified. (For example, an online trading application Threat Profile might identify 20-40 threats). It becomes the starting point for our subsequent tests. We share this with you, and obtain your feedback to ensure that we have not overlooked anything, nor exaggerated a threat.

Creating the Test Plan

The final Threat Profile drives the Test Plan. We map each threat in the Threat Profile to specific pages on your site. For example, the threat of an adversary viewing the portfolios of other users might be mapped to the "View Portfolio" page.

The Test Plan then identifies all the attacks we need to carry out on those pages to assess that specific threat. For example, on the "View Portfolio" page, we might carry out a variable manipulation attack and a SQL Injection attack to see if we can view the portfolios of other users. The Test Plan is thus built up for all the threats in the Threat Profile. The list of the tests covered have been listed in the Tests Performed section.

Performing Manual and Automated tests

Once the Test Plan and Test Cases are prepared and approved by a project lead, the testing begins. This will comprise of a combination of manual and automated checks that adhere to the Test Plan. During the course of testing, the Test Engineer may identify additional tests or attacks to perform, in which case he updates the Test Plan and performs the subsequent new tests. The team takes up the threats one by one and starts performing the tests. If a test case is successful, it is marked as unsafe in the Test Plan. The sequence of screenshots demonstrating the attack is recorded and included in the final report.

Creating the Report

Once the team is through with the tests, the reporting process begins. The detailed report delineates each vulnerability discovered as well as the method of discovery. Potential solutions to each finding are also included. The report is made available to the client after it has been reviewed internally.

Tests Performed

Here's a list of all tests performed on the <Application Name> application and its systems.

1. Browser Refresh	2. Bypass Authentication
3. Command Injection	4. Cookie Tampering
5. Cross-Site Request Forgery	6. Cross Site Scripting
7. Cross-Site Tracing	8. Cryptographic Strength Validation
9. Custom Attacks On The Application	10. Default Passwords
11. Directory Traversal	12. DNS Records
13. Hard Coded Secrets	14. Hidden Variable Manipulation
15. HTML Source Code Analysis	16. OS Fingerprinting
17. Password Guessing	18. Port Scanning
19. Privilege Escalation	20. Sensitive Data In Cache
21. Sensitive Error Messages	22. Server/Service Fingerprinting
23. Session Hijacking	24. Session ID Prediction
25. SQL Injection	26. SSL Configuration
27. Variable Manipulation Attacks	28. Vulnerable Sample Applications On Server
29. Web Server Vulnerability Scan	30. WHOIS Records

Tool List

Here's the list of tools that we used for the Security Assessment of the <Application Name> application and its systems.

No.	Tool	Purpose
	Static Application Security Testing (SAST) Tools	
1.	Burp Professional	Automated Web Application Security Scanner
2.	Qualys	Automated Network Vulnerability Scanner
3.	Nessus	Automated Network Vulnerability Scanner
4.	Netsparker	Automated Web Application Security Scanner
5.	Nmap	Port scanner and Service Fingerprinting Tool
	Dynamic Application Security Testing (DAST) Tools	
6.	Burp Suite	Web Application Security Testing Framework
7.	Dnsscan	Finger printing tool for open recursive resolvers
8.	SSLScan	Scans for supported SSL ciphers
9.	SiteDigger	Google hacking
10.	Webscarab	Web Application Security Testing Framework
11.	WinHex	Memory Reading tool
12.	Wireshark	Network Sniffer and Packet Analyzer

Mapping to OWASP Top Ten - 2017

The Open Web Application Security Project (OWASP) is an industry initiative for web application security. OWASP has identified the 10 most common risks to web applications. These comprise the OWASP Top 10. The Application Penetration Test includes all the items in the OWASP Top 10 and more. The penetration tester tries to remotely compromise the OWASP Top 10 flaws. The flaws listed by OWASP in its most recent Top 10 and the status of the application against those are depicted in the table below.

#	The OWASP Top 10 - 2017	Status
A1	Injection	Safe/Unsafe
A2	Broken Authentication	Safe/Unsafe
A3	Sensitive Data Exposure	Safe/Unsafe
A4	XML External Entities (XXE)	Safe/Unsafe
A5	Broken Access Control	Safe/Unsafe
A6	Security Misconfiguration	Safe/Unsafe
A7	Cross-Site Scripting (XSS)	Safe/Unsafe
A8	Insecure Deserialization	Safe/Unsafe
A9	Using Components With Known Vulnerabilities	Safe/Unsafe
A10	Insufficient Logging and Monitoring	Safe/Unsafe

Note: For A3 "Sensitive Data Exposure", the penetration test verifies that no sensitive data stored on the client is weakly encrypted or transmitted in plaintext or using an insecure encryption scheme. The penetration test usually cannot verify whether the sensitive data stored at the server is weakly encrypted. This can be ideally detected in a code review.

Note: For A10 "Insufficient Logging and Monitoring", the penetration test checks whether logs and audit trails are accessible to the end-users. However, the penetration test cannot verify whether the application's event/incident logging, detection & response mechanisms/policies, deployed at the server, are adequate or sufficient. This can ideally be verified by performing a source code review along with an application architecture review, inclusive of Firewall and WAF configurations, if any. Since these are well-known attacks, we rate any weakness in the site that is vulnerable to these attacks as High, Medium or Low Risk depending on the data that the attacks compromise.

Mapping to NIST CSF

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across all sectors. Here's the list of sub-categories in the Framework Core that are covered in Paladion's Application Security Assessment methodology.

Function	**Category**	**Subcategory**
IDENTIFY (ID)	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
PROTECT (PR)	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-5: Protections against data leaks are implemented
DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-8: Vulnerability scans are performed

Note: The NIST CSF is an exhaustive framework with 98 sub-categories under 5 functions that covers all the required controls to be established in an organization from people, process and technology perspectives.

Disclaimer

This letter of opinion is valid for the period during which the assessment was carried out and it’s based on the hosted system, and software applications provided by Wolters Kluwer. Projection of any conclusions based on our findings for future periods and application versions is subject to the risk that the validity of such conclusions may be altered by the changes made to the application or systems or the failure to make the changes to the system when required.

Balaji Venkatasubramanian
Delivery Head – MDR VM
Paladion

PALADION
HIGH SPEED CYBER DEFENSE

Head Office: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, **Doha:** +97433559018, **Dubai:** +971-4-2595526, **Kuala Lumpur:** +60-3-7660-4988, **London:** +44(0)2071487475, **Mumbai:** +9102233655151, **Riyadh:** +966(0)114725163, **Virginia:** +1-844-507-7668

sales@paladion.net | www.paladion.net