



SOFTWARE SECURITY SERVICES: OFFERTA

Spett.le
PagoPA S.p.A.
Piazza Colonna 370
00187 Roma

[REDACTED]

Firenze, 17/02/2020

CODICE OFFERTA: 20/369/PPA/SCR v.1.2

Oggetto: Offerta per servizio specialistico di Software Security

Facendo riferimento agli accordi verbali intercorsi sottoponiamo, la ns. offerta relativa a quanto in oggetto.

Restando in attesa di Vs. cortese riscontro in merito, Vi porgiamo Cordiali Saluti.

Gianni Massa

[REDACTED]

SOMMARIO

1 INTRODUZIONE	2
1.1 Project scope	2
2 APPROCCIO AL PROGETTO E SERVIZI OFFERTI	5
2.1 Mobile Application Penetration Test	5
2.2 Secure Code Review	7
2.2.1 Elenco delle attività progettuali PER MOBILE TESTING	9
2.3 Web Application Penetration Test	10
2.3.1 Elenco delle attività progettuali PER WAPT	13
2.4 API Security Assessment	13
2.4.1 Elenco delle attività progettuali API ASSESSMENT	15
2.5 Deliverable	15
2.6 Team di progetto	16
3 OFFERTA ECONOMICA	18
3.1 Costi	18
3.2 Fatturazione	18
3.3 Pagamenti	18
3.4 Spese di Trasferta	18
3.5 Validità Offerta	19
3.6 Responsabilità di PagoPA	19
3.7 Autorizzazione All'esecuzione Delle Attività Ed Accesso Ai Sistemi Informativi	19
3.8 Conclusioni e referenze	20
OFFER ACCEPTANCE	21

1 INTRODUZIONE

1.1 PROJECT SCOPE

PagoPA SPA (in seguito PagoPA) ha la necessità di effettuare un'attività di verifica di sicurezza sul nuova applicazione mobile IO, che rappresenta un servizio innovativo verso il cittadino.

La proposta da parte di Minded Security prevede una attività iniziale di Mobile Assessment che sarà completata con una analisi dinamica manuale del Portale Sviluppatori (Web Application Penetration Testing) e una verifica di Sicurezza delle API coinvolte nei flussi applicativi.

Le informazioni ricevute riguardo lo schema di Funzionamento dell'App sono illustrate nella seguente figura:

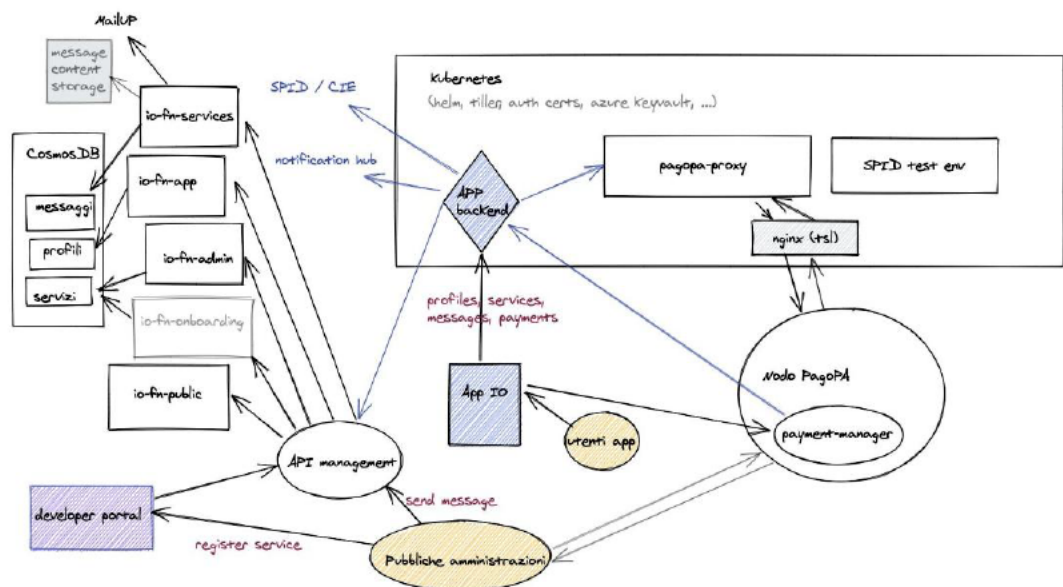


Figure 1: Schema Architettuale

Le altre informazioni fornite da Pago PA sono le seguenti.

App Mobile

Permette ai cittadini di visualizzare messaggi e servizi degli Enti che hanno fatto onboarding nella piattaforma IO.

L'autenticazione tra App e backend avviene in due fasi:

- 1) l'utente si autentica con SPID che verifica l'identità del cittadino
- 2) il backend che gestisce la risposta dell'IDP SPID genera un Bearer token e lo invia all'app mobile.

Tutte le richieste successive verso il backend sono effettuate attraverso il Bearer token ottenuto nel precedente step 2.

io-backend

Backend dell'app mobile. Interagisce con le Function ospitate nella piattaforma Azure per servire le richieste provenienti dall'app mobile. L'autenticazione tra backend e functions avviene tramite Bearer token.

Codice sorgente:

<https://github.com/pagopa/io-backend>

Specifiche Swagger:

https://github.com/pagopa/io-backend/blob/master/api_backend.yaml

https://github.com/pagopa/io-backend/blob/master/api_notifications.yaml

https://github.com/pagopa/io-backend/blob/master/api_pagopa.yaml

https://github.com/pagopa/io-backend/blob/master/api_public.yaml

io-functions-app

Functions ospitate su Azure interrogate dal backend dell'app per la consultazione di messaggi/servizi e per modificare il profilo utente (preferenze).

Codice sorgente:

<https://github.com/pagopa/io-functions-app>

Specifiche Swagger:

<https://github.com/pagopa/io-functions-app/blob/master/openapi/index.yaml>

API Management

Interrogato tramite Bearer token dagli Enti principalmente per inviare messaggi ai cittadini.

io-functions-service

Functions ospitate su Azure interrogate dall'api management per servire le richieste degli

enti

Codice sorgente:

<https://github.com/pagopa/io-functions-services>

Specifiche Swagger:

<https://github.com/pagopa/io-functions-services/blob/master/openapi/index.yaml>

```
io-app-master$ cloc .
  728 text files.
  699 unique files.
  118 files ignored. github.com/AlDanial/cloc v 1.74 T=1.24 s (493.5 files/s,
43587.5 lines/s)
```

Language	files	blank	comment	code
TypeScript	472	4626	4500	38068
YAML	5	125	99	2230
Markdown	82	442	0	932
JSON	15	0	0	630
JavaScript	7	87	20	561
Groovy	3	22	101	205
Bourne Shell	8	43	70	204
Java	2	21	26	195
Objective C	3	42	37	181
XML	9	23	6	158
Prolog	1	20	0	75
DOS Batch	1	24	2	74
Python	1	2	2	6
C/C++ Header	1	4	6	5
SUM:	610	5481	4869	43524

Di seguito le informazioni tecniche relative alle attività proposte e l'offerta economica relativa.

2 APPROCCIO AL PROGETTO E SERVIZI OFFERTI

Minded Security è un operatore globale di Information Security focalizzato sulle problematiche di Application Security. L'approccio alla valutazione della sicurezza delle applicazioni si basa sull'adozione di metodologie riconosciute a livello internazionale. Da diversi anni i consulenti Minded Security collaborano attivamente al progetto OWASP (The Open Web Application Security Project), con incarichi sempre più prestigiosi: dalla fondazione del capitolo italiano, alla leadership della linea guida per il testing delle web application (OWASP Testing Guide). Grazie all'esperienza acquisita e alle metodologie sviluppate, Minded Security rappresenta un centro di eccellenza per quanto riguarda la consulenza, i servizi professionali e la ricerca nel campo della Sicurezza del Software.

Il progetto prevede l'esecuzione delle seguenti attività:

- Mobile Application Penetration Test della piattaforma;
- Secure Code Review del codice sorgente dell'applicazione mobile;
- Web Application Penetration Testing Portale Sviluppatori;
- API Assessment.

Di seguito descriviamo il dettaglio tecnico delle attività.

2.1 MOBILE APPLICATION PENETRATION TEST

L'attività di Mobile Application Penetration Testing (MAPT) consiste nell'effettuare una simulazione reale di un attacco all'applicativo in oggetto al fine di valutarne l'effettivo livello di sicurezza. Minded Security adotta la metodologia descritta dagli standard OWASP Mobile Top 10 Risks 2016 e OWASP Mobile Testing Guide per effettuare il test dinamico.

La figura seguente mostra la metodologia esecutiva di alto livello:

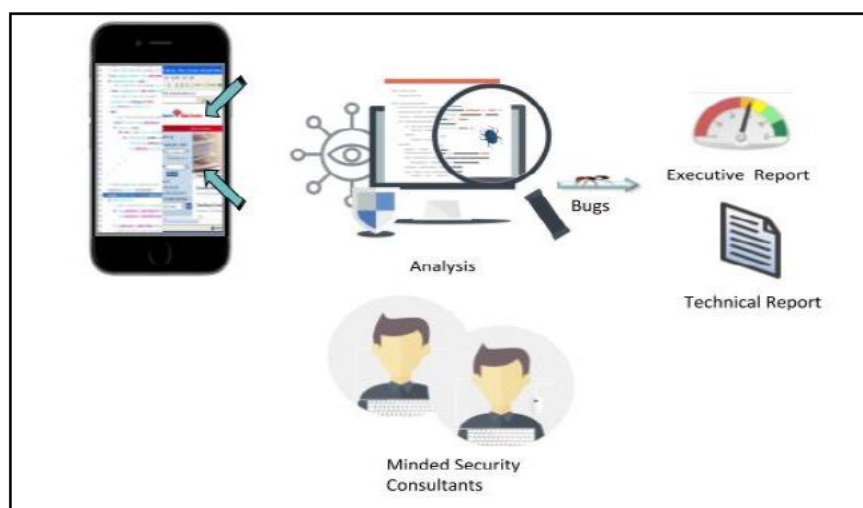


Figura 2: Metodologia di alto livello per MAPT

La metodologia include una serie di vettori di attacco per garantire un focus e un approccio coerente all'analisi complete del target. I vettori forniscono una struttura delle attività di analisi e reporting contenute nel documento. L'uso di azioni e test sFatturazione elettronicafici è dettato dalle caratteristiche osservate dai componenti dell'applicazione analizzati. Di seguito l'elenco dei test che verranno effettuati: Di seguito decriviamo il dettaglio delle tipologie di test previste.

<u>M1 - Improper Platform Usage</u>	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
<u>M2 - Insecure Data Storage</u>	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
<u>M3 - Insecure Communication</u>	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
<u>M4 - Insecure Authentication</u>	<p>This category captures notions of authenticating the end user or bad session management. This can include:</p> <ul style="list-style-type: none"> • Failing to identify the user at all when that should be required • Failure to maintain the user's identity when it is required • Weaknesses in session management
<u>M5 - Insufficient Cryptography</u>	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.
<u>M6 - Insecure Authorization</u>	<p>This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.).</p> <p>If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.</p>
<u>M7 - Client Code</u>	This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding

<u>Quality</u>	mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.
<u>M8 - Code Tampering</u>	<p>This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.</p> <p>Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.</p>
<u>M9 - Reverse Engineering</u>	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary instrumentation tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.
<u>M10 - Extraneous Functionality</u>	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

Tabella 1: Elenco vettori di test per MAPT

2.2 SECURE CODE REVIEW

L'attività di Secure Code Review consiste nell'analisi di sicurezza del codice sorgente dell'applicativo linea per linea: viene anche chiamato test di tipo white box, per sottolineare il fatto che chi esegue la verifica ha a disposizione la conoscenza completa dell'applicativo (insieme dei sorgenti).

Il processo di Secure Code Review prevede un approccio manuale all'analisi del codice: alcuni strumenti possono essere utilizzati per svolgere alcune attività di analisi ma questi non possono comprendere il contesto applicativo che è il capisaldo del code review.

L'attività comprende:

- l'analisi completa del codice

- il controllo manuale dei possibili falsi positivi tramite l'esecuzione sull'ambiente dinamico
- l'individuazione delle remediation da implementare date le problematiche riscontrate.

L'analisi di Code review sarà suddivisa secondo le seguenti fasi:

1. Discovery (Pre Transaction analysis).
2. Transactional analysis.
3. Post transaction analysis.
4. Procedure peer review.
5. Reporting & Presentation.

La figura seguente mostra la metodologia esecutiva di alto livello per un'attività di Secure Code Review:

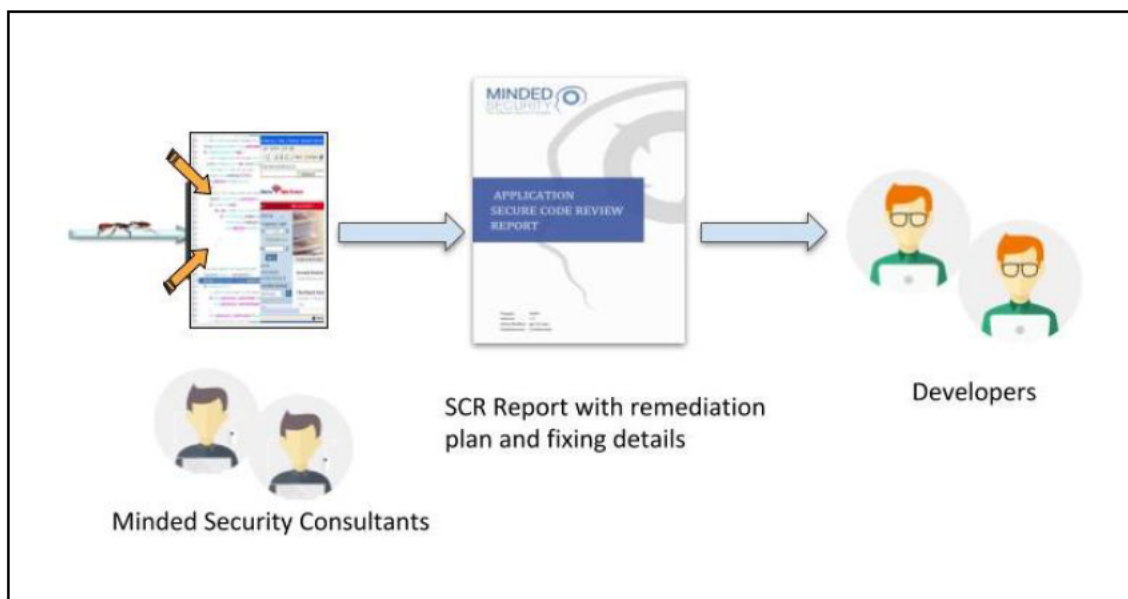


Figura 2: metodologia esecutiva ad alto livello per un Code Review

La metodologia comprende vettori di test per assicurarsi un focus consistente e un approccio di analisi completo. I vettori forniscono una struttura alle attività dell'analisi e riflettono la reportistica contenuta all'interno del documento. I seguenti vettori di test sono rappresentativi dell'approccio Minded Security per l'analisi del codice:

Categoria di test

Attività di analisi

Information Gathering	Attività di analisi del codice
Authentication	Review del meccanismo di autenticazione
Authorization	Review del meccanismo di controllo degli accessi
Data Validation	Review dei punti di ingresso dell'applicativo per controllare i meccanismi di Data Validation (XSS, SQL Injection, ecc.)
Session Management	Review del meccanismo di gestione delle sessioni e della loro robustezza
Errorhandling	Analisi di come l'applicativo gestisce gli errori applicativi
Cryptography	Review dei meccanismi crittografici
Logging	Review dei meccanismi di logging dell'applicativo e delle informazioni gestite
Communication	Review delle comunicazioni dell'applicativo con soggetti esterni (client, DB, LDAP, ecc.)

Tabella 2: Attività di analisi di Secure Code Review

Nel corso dell'attività saranno inoltre date le sFatturazione elettronicaifiche per verificare che i device siano Jailbroken e rooted nel caso in cui non siano già state realizzate.

2.2.1 ELENCO DELLE ATTIVITÀ PROGETTUALI PER MOBILE TESTING

L'attività in oggetto comprende:

Attività		Descrizione
1	Kick-off	Avviamento delle attività di progetto.
2	Mobile Application Penetration Testing (MAPT)	Attività di analisi delle vulnerabilità della parte pubblica dell'applicativo.
3	Secure Code Review	Analisi del codice sorgente dell'applicazione.
4	Report	Redazione Report tecnico ed executive summary per l'applicazione in oggetto.
5	Close-out	Revisione finale del progetto e presentazione dei risultati.
6	Recheck delle vulnerabilità	Verifica che le remediation implementate siano robuste

Tabella 3: Elenco delle attività progettuali

L'attività progettuale prevista verrà svolta da remoto presso gli uffici di Minded Security.

2.3 WEB APPLICATION PENETRATION TEST

L'attività di Web Application Penetration Testing (WAPT) consiste nell'effettuare una simulazione reale di un attacco informatico all'applicativo in oggetto al fine di valutarne l'effettivo livello di sicurezza. Minded Security adotta la metodologia OWASP Testing Guide V.4 e strumenti open source per valutare la sicurezza dell'applicazione da analizzare. La figura seguente mostra la metodologia esecutiva di alto livello:

Categoria	Finalità del controllo	Vulnerabilità da testare
Authentication Testing	L'applicazione fallisce a verificare l'autenticità di un utente	Verify HTTPS Endpoints Bypassing authentication schema Credential transport over an encrypted channel Default or guessable account Password quality Password reset Password lockout Password structure Blank password Brute Force Directory traversal/file include Vulnerable remember password and pwd reset Logout and Browser Cache Management Testing
AccessControl Testing	L'applicazione fallisce a forzare le appropriate restrizioni su dati o funzioni specifiche.	Parameter Analysis Authorization bypass Inconsistent use of access control Authorization Parameter Manipulation Authorized pages/functions
Data Validation	L'applicazione fallisce a testare la validità dei parametri forniti dall'utente: ad esempio la lunghezza, la sintassi, i caratteri accettati come valori dei parametri.	Cross site scripting HTTP Methods and XST SQL Injection Stored procedure injection ORM Injection LDAP Injection XML Injection SSI Injection XPath Injection

		IMAP/SMTP Injection Code Injection OS Commanding Buffer overflow Incubated vulnerability
Session Management	L'applicazione fallisce nell'utilizzo di un token di sessione (es. Cookie) che sia non predicibile per mantenere uno stato lato server che identifichi in maniera univoca l'utente autenticato.	Static session identifiers Easily predictable identifiers Token Insufficient length Session Management Schema Session Token Manipulation Exposed Session Variables CSRF
Cryptography	<p>L'applicazione fallisce nell'implementare correttamente la crittografia.</p> <p>Questo include il fatto di selezionare ed implementare correttamente algoritmi crittografici o scegliere un metodo sufficientemente randomico e non predicibile di generazione delle chiavi di cifratura.</p>	Sensitive Data in HTML SSL Version SSL Algorithms Digital Certificate Validity Proprietary or home-grown encryption algorithms Insecure cipher mode Poor key selection Insufficient key length Inappropriate key reuse Miscellaneous cryptography issues
Configuration Management	Verifica delle configurazioni dell'infrastruttura su cui è in esecuzione l'applicativo.	HTTP Methods Known vulnerabilities/Security Patches Web Server Configuration Web Server Components Common paths Application Admin Interfaces
Error Handling	L'applicazione mostra informazioni non pubbliche in caso di errore.	Application/User error messages
Client Side Testing	Viene testata l'esecuzione del codice nel client nativamente nel browser o nei suoi plugin.	DOM based Cross Site Scripting JavaScript Execution HTML Injection Client Side URL Redirect

CSS Injection
Client Side Resource Manipulation
Cross Origin Resource Sharing
Cross Site Flashing
Clickjacking
WebSockets
Web Messaging
Local Storage

Tabella 4: Vettori di attacco secondo la OWASP Testing Guide V.4

Di seguito una schematizzazione delle attività di verifica di sicurezza:

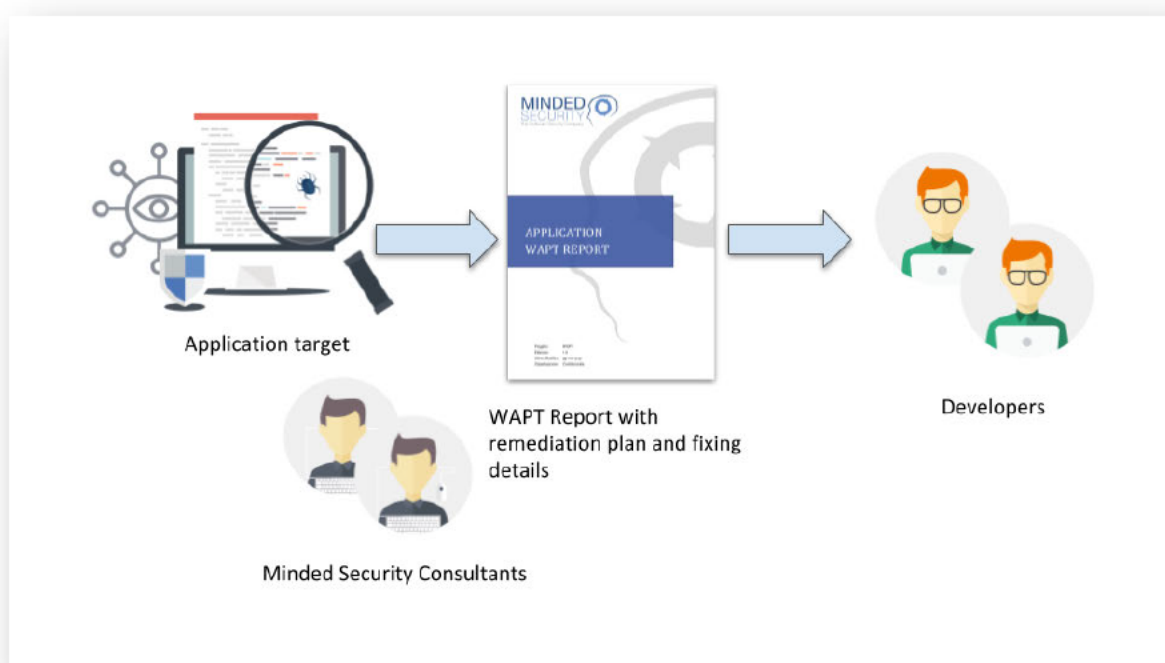


Figura 3: metodologia esecutiva ad alto livello per un WAPT

La metodologia comprende un insieme di vettori di attacco per assicurarsi un focus consistente e un approccio di analisi completo. I vettori forniscono una struttura alle attività dell'analisi e riflettono la reportistica contenuta all'interno del documento. L'utilizzo di azioni specifiche e test è dettato dalla funzionalità osservata dai componenti dell'applicazione analizzata. I seguenti vettori di attacco sono rappresentativi dell'approccio Minded Security.

Gli strumenti utilizzati per il test degli applicativi dai consulenti Minded Security saranno i seguenti:

- Minded Security BlueClosure BC Detect

- OWASP WebScarab
- OWASP ZAP
- Burp Suite
- Nmap

2.3.1 ELENCO DELLE ATTIVITÀ PROGETTUALI PER WAPT

Nella tabella seguente sono illustrate le differenti attività che compongono il progetto.

	Attività	Descrizione
1	Incontro Kick-off	Incontro mirato ad avviare le attività di progetto.
2	Manual Secure Code Review	L'attività di Code Review manuale delle applicazioni target utilizzando la metodologia proprietaria di Minded Security e strumenti open source.
3	Web Application Penetration Testing (WAPT)	Attività di analisi delle vulnerabilità dell'applicativo in esecuzione.
4	Report	Redazione Report tecnico ed executive summary.
5	Meeting	Incontro per la presentazione dei risultati e della reportistica tecnica con descrizione delle problematiche riscontrate e soluzione tecnica; analisi sugli impatti di business e valutazione del rischio per PagoPA.
6	Consulenza fixing	Consulenza per il fixing delle problematiche enunciate.
7	SCR e WAPT Retest	A valle dell'implementazione delle contromisure necessarie per il fixing delle vulnerabilità, verrà eseguito un retest al fine di verificare la correttezza delle soluzioni implementate.
8	Close-out	Incontro per la revisione finale del progetto e presentazione dei risultati.

Tabella 5: Elenco delle attività progettuali

2.4 API SECURITY ASSESSMENT

La realizzazione di API (Application Program Interface) si sta sempre più diffondendo grazie alla direttiva PSD2 e allo sviluppo sempre più crescente di API Economy.

Le API sono differenti da applicazioni Web standard: le API hanno una logica univoca, meccanismi di autenticazione e autorizzazione univoci e vulnerabilità univoche. Possono essere utilizzati da esseri umani, macchine o altre API. Le soluzioni di sicurezza tradizionali si

concentrano solo sui tipi di attacco noti e sulla mancanza di una comprensione granulare di questi aspetti delle API. Ciò rende le soluzioni tradizionali incapaci di rilevare o prevenire gli attacchi che sfruttano le vulnerabilità specifiche delle API. La figura seguente mostra la metodologia sviluppata da Minded Security per l'analisi di sicurezza di API:



Figura 4: Insieme delle minacce: attacchi, design flaw e codice vulnerabile

Dato l'insieme delle minacce sopra esposte, la metodologia per effettuare un API Security Assessment comprende vettori di test per assicurarsi un focus consistente e un approccio di analisi completo. I vettori forniscono una struttura alle attività dell'analisi e riflettono la reportistica contenuta all'interno del documento. L'utilizzo di azioni specifiche e test è dettato dalla funzionalità osservata dai componenti della singola API analizzata.

I seguenti vettori di test sono rappresentativi dell'approccio Minded Security per API Assessment:

Categoria di test	Attività di analisi
Information gathering	Analisi del perimetro da analizzare e raccolta informazioni
Authentication	Review del meccanismo di autenticazione
Authorization	Review del meccanismo di controllo degli accessi
Data Validation	Review dei parametri di ogni singola API per controllare i meccanismi di Data Validation (XSS, SQL Injection, ecc.)
Session Management	Review del meccanismo di gestione delle sessioni e della loro robustezza
Error handling	Analisi di come le API gestiscono gli errori applicativi

Cryptography	Review dei meccanismi crittografici
---------------------	-------------------------------------

Tabella 6: Attività di analisi di API Security Assessment

2.4.1 ELENCO DELLE ATTIVITÀ PROGETTUALI API ASSESSMENT

Nella tabella seguente sono illustrate le differenti attività che compongono il progetto.

	Attività	Descrizione
1	Incontro Kick-off	Incontro o call mirata ad avviare le attività di progetto.
2	API Security Assessment	Attività di API Security Assessment
3	Report	Redazione Report tecnico ed executive summary.
4	Close out	Incontro o call per la presentazione dei risultati e della reportistica tecnica con descrizione delle problematiche riscontrate e soluzione tecnica; analisi sugli impatti di business e valutazione del rischio per PagoPA..
5	Consulenza fixing	Consulenza per il fixing delle problematiche enucleate.
6	API Security Retest	A valle dell'implementazione delle contromisure necessarie per il fixing delle vulnerabilità, verrà eseguito un retest al fine di verificare la correttezza delle soluzioni implementate.
7	Retest Close-out	Incontro o call per la revisione finale del progetto e presentazione dei risultati.

Tabella 7: Elenco delle attività progettuali

2.5 DELIVERABLE

L'attività prevede i seguenti deliverable:

- Tutti i finding high risk saranno immediatamente notificati al cliente via mail cifrata
- A fine settimana sarà inviato un rapporto schematico delle vulnerabilità enucleate
- A fine attività saranno redatti i seguenti documenti:

Documento	Descrizione
-----------	-------------

Report	Report delle attività di Mobile Assessment, WAPT, API Assessment. Executive Summary: valutazione del rischio delle vulnerabilità enunciate. Technical Summary: reportistica tecnica con descrizione delle problematiche riscontrate e remedation da implementare.
Retest Report	Report della verifica della correttezza delle soluzioni implementate.

Tabella 8: Elenco dei deliverable di progetto

2.6 TEAM DI PROGETTO

Il team di progetto è stato così composto:

Numero Figure Professionali	Composizione Team	Seniority
1	Principal	> 10 anni
2	Senior Web Application Penetration Tester	> 5 Anni
3	Senior Code Reviewer	> 5 Anni

Principal Security Consultant

Il consulente ha una esperienza superiore a 10 anni per quanto concerne l'attività di analisi di sicurezza applicazioni.

Durante la sua esperienza in Minded Security, ha realizzato centinaia di attività di Penetration Testing applicativo e Secure Code Review, per importanti aziende come banche, TLC e aziende pubbliche. Partecipa da anni ai progetti OWASP ed in particolare alla realizzazione della OWASP Testing Guide. Tiene inoltre da diversi anni corsi sulla sicurezza delle applicazioni e partecipa come speaker in alcune delle più importanti riunioni di sicurezza nazionale.

Si occupa della supervisione delle attività in essere di testing e garantisce che i risultati ottenuti (vulnerabilità trovate, classificazioni di rischio e priorità, remediation proposte) siano in compliance con gli standard qualitativi di Minded.

Senior Web Application Penetration Tester/Senior Code Reviewer

Esperienza nel ruolo: 5+ anni

La figura ha una approfondita conoscenza ed esperienza relativamente alla verifica di sicurezza delle applicazioni Web e del codice.

In particolare ha maturato le seguenti esperienze:

- Esecuzione di decine di test dinamici e sul codice riguardo applicazioni web di clienti Finance, Banking, Energy, Retail, ecc

- Conoscenza approfondita di exploiting delle vulnerabilità web: Authentication Bypass, Authorization Bypass, Session Hijacking, CSRF , XSS, DomBased XSS, SQL Injection, JS Execution, Command Execution, HTTP Parameter Pollution, Business logic bypass, ecc.
- Conoscenza approfondita di tutte le tecnologie web, dai web server, application server ai framework ad oggi utilizzati
- Ricercatore riconosciuto nella community nell'ambito della sicurezza applicativa.

Partecipazione come speaker a conferenze internazionale per portare il proprio contributo sulla ricerca relativamente alla sicurezza web.

3 OFFERTA ECONOMICA

3.1 COSTI

Di seguito l'offerta economica strutturata in conformità alle proposte di servizi specialistici di Software Security.

Attività	Durata gg/uomo	Prezzo unitario	Valore (EUR)
Mobile Application Penetration Test della APP IO Android & iOS	14	€ 570,00	€ 7.980,00
Secure Code Review del codice sorgente dell'applicazione mobile IO Android & iOS	14	€ 570,00	€ 7.980,00
API ASSESSMENT	18	€ 570,00	€ 10.260,00
Retest dei fixing più importanti	4	€ 570,00	€ 2.280,00
WAPT Portale Sviluppatori e consulenza generale sulla sicurezza delle applicazioni	18	€ 570,00	€ 10.260,00
Totale (A)	68	€ 570,00	€ 38.760,00
		Trasferte (B)	€ 1.140,00
TOTALE A +B			€ 39.900,00

Tabella 9: Dettaglio dei costi IVA Esclusa

Le attività si svolgeranno prevalentemente presso gli uffici di Mind Security e all'occorrenza presso la sede di PagoPA.

3.2 FATTURAZIONE

La fatturazione verrà effettuata nella seguente modalità:

- A consuntivo delle prestazioni effettuate e delle trasferte occorse.

3.3 PAGAMENTI

Il pagamento degli importi in fattura dovrà essere effettuato a 60 gg. d.f.f.m. mediante bonifico bancario con valuta vincolata alla data di scadenza.

3.4 SPESE DI TRASFERTA

Le eventuali spese di trasferta che verranno sostenute da Mind Security sono quotate nel punto 3.1.

3.5 VALIDITÀ OFFERTA

I termini e le condizioni applicate nella presente offerta sono validi per una durata di 90 giorni dalla data di emissione. I prezzi si intendono IVA ESCLUSA.

3.6 RESPONSABILITÀ DI PAGOPA

PagoPA assegnerà una persona che sarà il coordinatore del progetto e sarà il contatto principale per Minded Security. Il coordinatore garantirà un efficiente scambio di informazioni che è fondamentale per l'esecuzione delle attività.

3.7 Autorizzazione All'esecuzione Delle Attività Ed Accesso Ai Sistemi Informativi

Con l'emissione di un eventuale incarico formale per Minded Security conseguente alla presente offerta il cliente accetta tutte le condizioni della presente Offerta ed inoltre dichiara di:

- Essere consapevole ed accettare che l'attività di MINDED SECURITY sarà esclusivamente finalizzata a verificare le vulnerabilità dell'applicazione /Sistema oggetto delle verifiche di sicurezza, onde consentire di realizzare le misure necessarie ad evitare così pericolose intrusioni dall'esterno.
- di possedere e controllare, direttamente o indirettamente, tutte le Attrezzature oggetto del Servizio, o, qualora tali Attrezzature siano messe a disposizione del Cliente da una terza parte, che quest'ultimo soggetto sia informato e consenziente;
- di avere la piena autorità per autorizzare MINDED SECURITY ad accedere alle suddette Attrezzature e fornire il Servizio in oggetto;
- che tutte le informazioni fornite a MINDED SECURITY secondo quanto stabilito dall'offerta commerciale sono precise e veritiere.
- di impegnarsi a non cambiare senza preavviso alcuna configurazione tale da rendere non significative le informazioni fornite.
- tenere indenne e manlevare MINDED SECURITY, rispetto a qualsivoglia danno, perdita, pretesa, responsabilità e/o rivendicazione e/o comunque conseguenza pregiudizievole che possano derivare direttamente o indirettamente in capo a MINDED SECURITY stessa, o a terzi, sia a cose che a persone, dall'esecuzione dell'incarico conferito.

Nel rispetto della normativa italiana sia civile che penale, il Cliente prende atto che MINDED SECURITY nell'espletamento del proprio incarico, utilizzano ogni mezzo atto a conseguire anche in parte gli scopi oggetto dell'incarico compresi:

- utilizzazione di operazioni tecniche, codici IP o profili utente reali o simulati al fine di ottenere l'accesso al sistema informativo;
- utilizzo di informazioni tecniche reperite all'interno del sistema del cliente;

Il Cliente autorizza l'effettuazione delle attività di penetration test relativamente alle applicazioni, agli indirizzi IP e/o classi di indirizzi IP e/o domini secondo quanto indicato nella presente offerta.


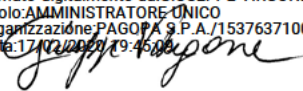
3.8 CONCLUSIONI E REFERENZE

Minded Security ringrazia PagoPA per l'opportunità di collaborazione fornita e di attenzione per il presente Documento di Offerta. Minded Security vanta una notevole esperienza nella formazione e realizzazione di progetti in ambito di sicurezza applicativa.

[REDACTED]

- [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]

OFFER ACCEPTANCE

Offer acceptance			
Minded Security		PagoPA S.p.A.	
Signature		Signature	Firmato digitalmente da: GIUSEPPE VIRGONE Ruolo: AMMINISTRATORE UNICO Organizzazione: PAGOPA S.p.A./15376371009 Data: 17/02/2020 09:45:00 
Name	Matteo Meucci	Name	
Date	17 Febbraio 2020	Date	

Billing Reference			
Client	PagoPA S.p.A.	Address	Piazza Colonna 370
Contact	Mirko Calvaresi	City	00187 Roma
Telephone		Country	Italy

MINDED SECURITY references	
Address	Minded Security Srl Via Duca d'Aosta, 20 50129 Firenze, ITALY
Commercial references	Giovanni Mazza, Managing Director [REDACTED] [REDACTED]
VAT	IT05756380480
Offer number	369

