ΠΡΟΣΩΠΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

Γρηγόρης Παπουτσής

Δωδεκανήσου 16Α, Ηλιούπολη Αθήνα, ΤΚ 16342
+30 – 6977972600
gpapoutsis@outlook.com

Φύλο Άρρεν | Ημερομηνία γέννησης 25/01/1992 | Εθνικότητα Ελληνική
Εκπληρωμένες στρατιωτικές υποχρεώσεις.

Innovation Engineer στην εταιρία Hack The Box με ιδιαίτερο ενδιαφέρον στο Mobile Security και εμπειρία στη δημιουργία ευπαθών σεναρίων με σκοπό την εκπαίδευση στο χώρο της κυβερνοασφάλειας. Στο παρελθόν έχω εργαστεί ως penetration tester και system administrator, και έχω συμμετάσχει σε διεθνείς cyber security CTF διαγωνισμούς και συνέδρια. Είμαι κάτοχος μεταπτυχιακού διπλώματος στην ασφάλεια ψηφιακών συστημάτων και προπτυχιακού στην πληροφορική, και μέλος τις ερευνητικής ομάδας INSSec του Πανεπιστημίου Δυτικής Αττικής.

ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

Απρίλιος 2021 – Σήμερα

Innovation Engineer
Διεξαγωγή market research, technical research, feasibility analysis για νέα πιθανά προϊόντα, καθώς και δημιουργία των αντίστοιχων PoC (Proof of Concept), σχηματισμός νέας ομάδας με subject matter experts από διαφορετικά τμήματα, με τελικό σκοπό την δημιουργία του τελικού προϊόντος.
Hack The Box

Απρίλιος 2020 – Απρίλιος 2021

Content Developer
Δημιουργία, τεκμηρίωση και έλεγχος ορθής λειτουργίας τον ευπαθών εικονικών υπολογιστών και σεναρίων, για πελάτες, CTF event, και την κύρια πλατφόρμα.
Hack The Box

Ιανουάριος 2019 – Απρίλιος 2021

Penetration Tester
Εφαρμογή διαδικασιών penetration testing σε εσωτερικές υποδομές του εργαστηρίου, όπως web applications, internal networks και άλλα projects, καθώς και σχεδιασμός και ανάπτυξη εργαλείων για την αυτοματοποίηση διαδικασιών penetration testing.
NCSR Demokritos (National Center of Scientific Research)

ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΚΑΤΑΡΤΙΣΗ

2019 - 2022

Μεταπτυχιακός Τίτλος Σπουδών
Απόφοιτος - Ασφάλεια Ψηφιακών Συστημάτων.
Τμήμα Ψηφιακών Συστημάτων.
Πανεπιστήμιο Πειραιά.

2010 - 2019

Προπτυχιακός Τίτλος Σπουδών

Απόφοιτος – Μηχανικός Πληροφορικής.
Τμήμα Μηχανικών Πληροφορικής.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Αθήνας.

2010

Απολυτήριο Επαγγελματικού Λυκείου
Πτυχίο ειδικότητας: Υποστήριξη Συστημάτων, εφαρμογών και δικτύων Η/Υ.
Επαγγελματικό Λύκειο Ζευγολατιού Κορινθίας.

ΑΤΟΜΙΚΕΣ ΔΕΞΙΟΤΗΤΕΣ

Μητρική Γλώσσα

Ελληνικά

Λοιπές Γλώσσες | Αγγλικά

ΚΑΤΑΝΟΗΣΗ		ΟΜΙΛΙΑ		ΓΡΑΦΗ
Προφορική	Γραπτή (ανάγνωση)	Επικοινωνία	Προφορική έκφραση	
C1	C1	C1	C1	C1
TOEIC ADVANCED LEVEL CERTIFICATE				

Ψηφιακές δεξιότητες

Γλώσσες Προγραμματισμού
- HTML, CSS, JS, JSP, PHP, MySQL, C, C++, JAVA, PYTHON

Εργαλεία Penetration Testing
- Nmap, Metasploit framework, Burp Suit, Wireshark, Ghidra, Frida, APKTool, JADX, Autopsy

RDBMS – NoSQL
- SQL (MariaDB, MySQL, PostgreSQL) – Elasticsearch

System Administration and Security
- Elastic Stack, Forensics procedures

Virtualization Technologies
- Docker (native/compose/swarm)

Λειτουργικά Συστήματα
- Windows, Linux, MacOS, Android, iOS

Εγκατάσταση και διαχείριση δικτύων
- Άριστη γνώση της τεχνολογίας TCP/IP

Office Suites
- Microsoft Office, MS Access, MS Excel, MS PowerPoint, MS Word, MS Visio, MS Outlook

	Version Control • Git
Επαγγελματικές δεξιότητες	Διαχείριση χρόνου, ομαδικό πνεύμα συνεργασίας, γρήγορη απορρόφηση νέων γνώσεων και ενσωμάτωση και εφαρμογή νέων διαδικασιών, debugging & troubleshooting, testing & documenting.
Ενδιαφέροντα	Offensive Security, CTF Challenges, Mobile Hacking, Game Developing, Αθλητισμός, Μουσική, Ταξίδια.
ΠΡΟΣΘΕΤΕΣ ΠΛΗΡΟΦΟΡΙΕΣ	
Δραστηριότητες	**UniWA CTF 2019 – 2022 | INSSec | UniWA CTF** Δημιουργία 3-ήμερου cyber security Capture The Flag (CTF) διαγωνισμού για ελληνικά πανεπιστήμια. **EESTech Challenge Patras 2021 | INSSec | UniWA CTF** Δημιουργία 3-ήμερου cyber security Capture The Flag (CTF) διαγωνισμού για το EESTech Challenge Patras. **Εθνική Άσκηση Κυβερνοασφάλειας Πανόπτης – NCSR Demokritos | 2019** Δημιουργία ενός επεισοδίου με θέμα την στεγανογραφία, για την άσκηση Πανόπτη, σε συνεργασία με το NCSR Demokritos.
Σεμινάρια / Συνέδρια	**Black Hat USA 2022** Παρακολούθηση/Ολοκλήρωση workshop σχετικά με Mobile Security. **DEF CON 30 USA 2022** Παρακολούθηση ομιλιών και συμμέτοχή σε διάφορα CTF games.
Διαγωνισμοί	**8th - 9th InfoCom Security Conference (3ο- 4 EthiHak Contest 2018 - 2019)** • 2-ήμερος Ethical Hacking διαγωνισμός στο συνέδριο InfoCom Security Conference (2018 - 2019). • 11η θέση. **Deloitte Hacking Challenge 2019** • 1-ήμερος Ethical Hacking διαγωνισμός που διοργανώθηκε από την Deloitte (2018 - 2019). • 8th place. **Εθνική Άσκηση Κυβερνοάμυνας ΠΑΝΟΠΤΗΣ - ΤΕΙ ΑΘΗΝΑΣ** • 2017: Επεισόδιο: Capture The Flag. • 2016: Επεισόδιο: Capture The Flag. • 2015: Επεισόδιο: Windows Forensics. **SETE Tourism crowdhackathon**

	• Διήμερος Μαραθώνιος Ανάπτυξης Εφαρμογών με θέμα τον Τουρισμό, Ομάδα τριών ατόμων, Εφαρμογή ATHENIZER (WEB εφαρμογή - Ηλεκτρονικό Τουριστικό Πρακτορείο) (2015). **Μονάδα Αριστείας ΕΛ/ΛΑΚ** • Τρίμηνο σεμινάριο του ΤΕΙ ΑΘΗΝΑΣ με Θέμα την Ανάπτυξη Εκπαιδευτικής Εφαρμογής Αυτοεκπαίδευσης και Αυτοαξιολόγησης γνώσεων βασισμένης σε ερωτήσεις πολλαπλής επιλογής σε πλατφόρμα Android (2015).
Λογισμικό ανοιχτού κώδικα	**AutoInjector** • Ένα εργαλείο γραμμένο σε Python που αυτοματοποιεί τις διαδικασίες ελέγχου ευπαθειών τύπου SQL Injection και Reflected XSS. • https://github.com/grpapoutsis/AutoInjector **Stegit** • Ένα εργαλείο γραμμένο σε Python που αυτοματοποιεί την διαδικασία εύρεσης πιθανών κρυμμένων μηνυμάτων με τεχνικές στεγανογραφίας, σε αρχεία πολυμέσων. • https://github.com/grpapoutsis/Stegit
Διπλωματική εργασία	**Creation of an Android Security Training Lab** Ανάλυση των ευπαθειών και τον προβλημάτων ασφαλείας που υπάρχουν σήμερα στα Android applications, του αντίκτυπου που μπορεί να έχουν αυτά σε έναν ιδιώτη ή μια επιχείρηση, και των πιθανών τρόπων αντιμετώπισης. Στη συνέχεια γίνεται αναλυτική περιγραφή ρεαλιστικών σεναρίων, δείχνοντας βήμα βήμα τους διάφορους τρόπους εκμετάλλευσης των ευπαθειών, καθώς και πώς να στηθεί η αντίστοιχη web based εφαρμογή στην οποία εγκαθιστούνται τα ευπαθή σενάρια.
Πτυχιακή Εργασία	**Αυτοματοποίηση Εντοπισμού των Κενών Ασφαλείας σε Εφαρμογές Web** Η πτυχιακή εργασία υλοποιεί την αυτοματοποίηση εντοπισμού των κενών ασφαλείας σε εφαρμογές web που αποκρύπτουν ή εμφανίζουν τα μηνύματα λάθους. Καλύπτει όλες τις περιπτώσεις που οι παράμετροι εισόδου σε SQL queries, μέσω γλώσσας προγραμματισμού (π.χ. PHP), είναι μέσα (ή όχι) σε αποστρόφους (‘ ‘) ή εισαγωγικά (“ ”) και αν αυτά φιλτράρονται/αντικαθίστανται (ή όχι) με backslashes (‘\’). Επιπλέον, καλύπτει τη χρήση παρενθέσεων, Union και βασικές αλγεβρικές παραστάσεις. Η αυτοματοποίηση εντοπισμού των κενών ασφάλειας γίνετε στην ευρέως διαδεδομένη βάση δεδομένων MySQL και δοκιμάζετε στην εκπαιδευτική βάση πρότυπο Damn Vulnerable Web App (DVWA), καθώς και στην διαδικτυακή web based εφαρμογή E-Shop, που κατασκευάστηκε αποκλειστικά για τις ανάγκες της εργασίας. Η εφαρμογή αναπτύχθηκε σε γλώσσα προγραμματισμού Python και είναι σχεδιασμένη για να τρέχει σε περιβάλλον Linux ενώ η εφαρμογή E-shop και DVWA είναι ανεπτυγμένες σε Java και PHP αντίστοιχα.