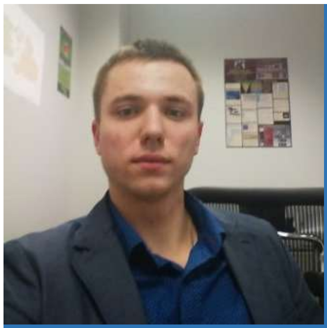
# Murashka Uladzislau

**Senior Security Engineer**



Total Work Experience: 7+

Information Security, Web development, databases and Linux administration. Doing manual and automated security testing, working with specific security tools & scripts, was writing some own scripts and applications.  Also have done some information security investigations for projects I worked for including deanonymization services.  Have experience in infrastructure information security designing & hardening. Worked with SIEM system, analytics, security issues investigation. Participated in bug bounty programs and was spoke person on IBM & ScienceSoft security conference in Belarus.

## SKILLS

### Other

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| iptables | 4 | Expert | 2017 |
| ipset | 3 | Advanced | 2017 |
| fail2ban | 3 | Advanced | 2017 |
| rsyslog | 3 | Advanced | 2017 |
| syslog-ng | 3 | Advanced | 2017 |
| IDA Pro | 2 | Medium | 2016 |
| OllyDBG | 2 | Medium | 2016 |
| Android | 3 | Advanced | 2016 |
| Apache | 5 | Expert | 2017 |
| nginx | 3 | Advanced | 2016 |
| Apache-Tomcat | 1 | Medium | 2017 |
| snort | 1 | Medium | 2018 |
| suricata | 1 | Medium | 2018 |
| IBM QRadar SIEM | 1 | Novice | 2018 |

### Source Control Systems

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Git | 2 | Medium | 2017 |
| SVN | 1 | Medium | 2016 |

### Performance Testing

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Apache JMetter | 1.5 | Medium | 2017 |
| Siege | 1 | Advanced | 2017 |

## Reporting Systems

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Jira | 3 | Advanced | 2017 |

## Document Output Management

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Microsoft Word | 3 | Advanced | 2017 |
| Microsoft Excel | 3 | Advanced | 2017 |
| Microsoft Project Plan | 3 | Advanced | 2017 |
| Microsoft PowerPoint | 3 | Advanced | 2017 |

## Frameworks and Libraries

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Yii Framework | 1 | Novice | 2016 |
| Twitter Bootstrap | 4 | Expert | 2017 |

## Desktop Virtualization

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| VMware Workstation | 4 | Advanced | 2017 |
| VirtualBox | 3 | Advanced | 2017 |

## CMS & CMF

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Joomla | 3 | Expert | 2017 |
| Wordpress | 5 | Expert | 2017 |
| Droopal | 2 | Medium | 2017 |
| MaxSite CMS | 1.5 | Medium | 2016 |

## Operating Systems

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| CentOS | 3 | Expert | 2017 |
| Debian | 5 | Expert | 2017 |
| Ubuntu | 3 | Expert | 2017 |
| MS Windows Server 2003 | 0.5 | Novice | 2013 |
| Windows 7 | 5 | Expert | 2016 |
| Windows XP | 4 | Expert | 2012 |
| MS Windows Server 2008R2 | 1 | Medium | 2014 |
| Kali Linux | 3 | Expert | 2017 |
| BackTrack | 3 | Expert | 2014 |
| MS Windows 10 | 1 | Expert | 2017 |

## Relational Database Management Systems (RDBMS)

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Oracle | 2 | Medium | 2016 |
| MSSQL | 2 | Medium | 2016 |
| MySQL | 4 | Advanced | 2017 |

## Programming Languages

| | Experience, years | Level | Last used, year |
|---|---|---|---|

| | | | |
|---|---|---|---|
| X++ | 1 | Novice | 2013 |
| C# | 1 | Novice | 2016 |
| Batch | 1 | Novice | 2016 |
| Bash | 2.5 | Advanced | 2017 |
| Action Script | 1 | Novice | 2014 |
| HTML/CSS | 4 | Advanced | 2017 |
| PHP | 4 | Advanced | 2017 |
| Python | 2 | Advanced | 2017 |
| PowerShell | 2 | Medium | 2016 |
| SQL | 4 | Advanced | 2017 |

### Automated Testing

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Checkmarx | 2 | Advanced | 2017 |
| Netsparker | 3 | Expert | 2017 |
| Metasploit | 5 | Expert | 2017 |
| BurpSuite | 5 | Expert | 2017 |
| sqlmap | 5 | Expert | 2017 |
| nmap | 5 | Expert | 2017 |
| w3af | 4 | Expert | 2017 |
| Acunetix Web Vulnerability Scanner | 4.5 | Expert | 2017 |
| OWASP ZAP | 3 | Advanced | 2017 |
| IBM AppScan | 3 | Expert | 2017 |
| OpenVAS | 3 | Expert | 2017 |
| Nessus | 4 | Expert | 2017 |
| nikto | 5 | Expert | 2017 |
| hydra | 4 | Expert | 2017 |
| Selenium | 0.5 | Novice | 2014 |
| WireShark | 4 | Expert | 2017 |
| tcpdump | 3 | Expert | 2017 |

### Monitoring Tools

| | Experience, years | Level | Last used, year |
|---|---|---|---|
| Cacti | 1 | Medium | 2015 |
| Zabbix | 2 | Advanced | 2016 |
| Nagios | 2 | Advanced | 2016 |
| Monit | 1 | Medium | 2018 |

## WORK EXPERIENCE

### IT Senior Security Engineer

**October 2016 to October 2016**

**Company:** International Bank (name is under NDA)

**Project Name:** Web application pentest (customers area)

**Project description:** Penetration testing of customers personal area web application.

**Responsibilities:** Project documentation, pentesting, reporting, consulting.

**Team size:** 1

**Technologies and Tools:** OWASP TOP10 classification, BurpSuite, Nessus, Acunetix, nmap, sqlmap, metasploit, hydra, Chrome Developer Tools

## IT Senior Security Engineer

**Jan 2015 to ... (still working on this position)**

**Company:** ScienceSoft Inc.

**Project description:** Company internal security projects & external security activities (commercial projects)

**Responsibilities:** Security testing, reporting and fixing recommendations

**Team size:** 1

**Technologies and Tools:** Suricata, Snort, IBM Qradar, Kali, nmap, sqlmap, IBM AppScan, AppScan Source, Acunetix, metasploit, nessus, openvas, dirb, nikto, BurpSuite, hping etc

## IT Senior Security Engineer

**July 2016 to August 2016**

**Company:** ScienceSoft Inc.

**Project Name:** Checking company pen testing (part 3) (NDA)

**Project description:** Pen testing of checking company infrastructure (external)

**Responsibilities:** Security testing, reporting and fixing recommendations

**Team size:** 1

**Technologies and Tools:** bash, BurpSuite, ZAP Proxy, Nessus, Acunetix, nmap, sqlmap, metasploit, kali, NTLM auth, Java, Oracle

## IT Senior Security Engineer

**June 2016 to July 2016**

**Company:** ScienceSoft Inc.

**Project Name:** Big credit monitoring company pen test

**Project description:** Internal pen testing of world popular credit monitoring company for PCI DSS compliance

**Responsibilities:** Remote configuration of all tools and OS for pen testing, pen testing execution, report creation, fixing recommendations.

**Team size:** 1

**Technologies and Tools:** BurpSuite, Nessus, OpenVAS, nmap, sqlmap, WireShark, tcpdump, bash, python, metasploit, w3af, kali, vnc, wifi, vSphere, arp-scan

## IT Senior Security Engineer

**June 2016 to July 2016**

**Company:** ScienceSoft Inc.

**Project Name:** One of the world's largest retail company website pen test (NDA)

**Project description:** One of the world's largest retail company website pen test (NDA)

**Responsibilities:** Pen testing, reporting

**Team size:** 1

**Technologies and Tools:** w3af, metasploit, nmap, sqlmap, BurpSuite, OpenVAS, Qualys, dig

## IT Senior Security Engineer

**May 2016 to June 2016**

**Company:** ScienceSoft Inc.

**Project Name:** Checking company pen testing (part 2) (NDA)

**Project description:** Pen testing of checking company infrastructure (external)

**Responsibilities:** Security testing, reporting and fixing recommendations

**Team size:** 1

**Technologies and Tools:** nmap, Nessus, metasploit, w3af, python

## PHP Developer

**May 2016 to May 2016**

**Company:** ScienceSoft inc.

**Project Name:** Twitter Security Monitoring

**Project description:** Small twitter monitoring service for security purposes of company

**Responsibilities:** Architecture, design, development, testing

**Team size:** 1

**Technologies and Tools:** PHP, MySQL, Debian, curl, cron, Twitter API, UI Framework Twitter Boostrap, sendmail

## IT Security Engineer

**March 2016 to April 2016**

**Company:** ScienceSoft

**Project Name:** Checking company pen testing

**Project description:** Pen testing of checking company infrastructure and web applications (external)

**Responsibilities:** Security testing, reporting and fixing recommendations

**Team size:** 1

**Technologies and Tools:** OWASP TOP10 methodology, nmap, sqlmap, python, nessus, IBM AppScan, Acunetix, fierce, openvas, metasploit (integrated with Nessus), BurpSuite (manual testing, work with requests)

## IT Security Engineer

**March 2016 to April 2016**

**Company:** ScienceSoft

**Project Name:** IBM QRadar SIEM system integration and pen testing of infrastructure

**Project description:** Project was onsite in USA. Main aim of project was to integrate IBM QRadar SIEM security system and provide pen testing services.

**Responsibilities:** IBM QRadar SIEM system integration, pen testing of infrastructure, documentation, communication.

**Team size:** 3

**Technologies and Tools:** IBM QRadar, python, nmap, sqlmap, nessus, metasploit, IBM AppScan, BurpSuite, w3af, Kali Linux, Red Hat Linux, iptables, snort, rsyslog, syslog-ng, routing, networking

## Senior Security Test Engineer

**February 2016 to March 2016**

**Company:** "Reliable Technologies" ltd. (Hoster.by)

**Project Name:** hoster.by, auction.cctld.by, nurhost.kz

**Project description:** Penetration testing services for web applications and additional 3rd party vendor software. Mass scanning of hosting servers for vulnerabilities and miss configurations, weak passwords

**Responsibilities:** Project management & security testing

**Team size:** 1

**Technologies and Tools:** metasploit, kali, IBM AppScan, sqlmap, nmap, zmap, some own scripts, burpsuite, siege, php, python, WASC metholodogy

## IT Security Engineer

**November 2015 to December 2015**

**Company:** ScienceSoft inc.

**Project Name:** Security testing & firewall configuration for sales lead generation company

**Project description:** Security testing & firewall configuration for sales lead generation company

**Responsibilities:** Security testing and firewall configuration

**Team size:** 1

**Technologies and Tools:** nmap, w3af, Acunetix, IBM AppScan, metasploit, BurpSuite

## IT Security Engineer

**September 2015 to November 2015**

**Company:** ScienceSoft

**Project Name:** Penetration testing for company which works with virtual biosphere and materials (NDA).

**Project description:** Security testing of web application with OWASP TOP10 methodology

**Responsibilities:** Planning, testing, reporting, recommendations.

**Team size:** 1

**Technologies and Tools:** OWASP TOP10 methodology, BurpSuite, Acunetix, IBM AppScan, OpenVAS, metasploit, nmap, sqlmap, WireShark, JavaScript, SQL, Oracle 11g, WebLogic

## IT Security Engineer

**September 2015 to October 2015**

**Company:** French psychologists online catalog (NDA)

**Project Name:** French psychologists online catalog (NDA)

**Project description:** Malware removal, pen testing, security hardening for online catalog

**Responsibilities:** Project consisted of 3 parts: 1. Remove malware 2. Find out how website was hacked (pen testing & logs research) 3. Help to improve security level of website

**Team size:** 1

**Technologies and Tools:** bash, php, python, IBM AppScan, Acunetix, w3af, Kali, nmap, sqlmap, Qualys, rkhunter, ai-bolit, RIPS, dig, OpenVAS, metasploit, OWASP, CentOS, ssh, tunneling, regular expressions

## Security Engineer

**January 2015 to June 2015**

**Company:** ScienceSoft

**Project Name:** Penetration testing for a mobile operator (NDA)

**Project description:** Penetration testing was conducted in 2 phases: testing of the network perimeter and testing of the public web applications. Testing was carried out using the "black box" method – only the company name and the URLs of the web applications were known The testing was conducted based on the following attacker models: intruder has access to the Internet, to GPRS/3G data services, to Ethernet data service (B2B), to guest Wi-Fi network. We have gathered information about the perimeter, public services, software versions, potential vulnerabilities, then performed attacks on vulnerable targets to elevate privileges. Although the internal information system was not the target of the penetration testing, our team managed to access the Customer's internal network. Web applications testing was performed based on WASC methodology. Finally, we prepared a technical description of the detected system vulnerabilities with their classification according to how harmful for the system and business they potentially are. We also delivered actionable recommendations to eliminate the revealed security issues, as well as strategic security measures to secure the company's resources in the long run.

**Responsibilities:** Mobile operator external security audit (penetration testing): web applications security testing, servers and services security testing, scanning, security improvment.

**Team size:** 2

**Technologies and Tools:** Penetration testing, Application security, Vulnerabilities, Network scanning, Exploit development, IDS/IPS, Routers Nmap, OpenVAS, Web application scanners, Burpsuite, Havij, Skipfish, w3af, Zaproxy, Exploits, Metasploit, Immunity debugger, Dradis, Bash Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), Web Application Security Consortium Threat Classification (WASC-TC)

## Information Security Specialist

**November 2014 to December 2014**

**Company:** ScienceSoft inc.

**Project Name:** BelToll Infrastructure information security designing and recommendations

**Project description:** Design infrastructure information security requirements for BelToll organization (Belarus national organization) to provide them for World Bank accreditation with all required standards and best practices including ISO 27001

**Responsibilities:** Plan and create information security recommendations.

**Team size:** 1

**Technologies and Tools:** ISO 27001

### Web application security specialist

**August 2014 to February 2015**

**Company:** The University of Queensland (Australia)

**Project Name:** NDA

**Project description:** Web application

**Responsibilities:** Security testing.

**Team size:** 1

**Technologies and Tools:** w3af, AWVS, sqlmap, nmap, manual testing, burpsuite, ZAP

### TechOps Engineer

**August 2014 to January 2015**

**Company:** ScienceSoft inc.

**Project Name:** WordPress Hosting Infrastructure Support

**Project description:** Managed Services for Linux data centers (Two data centers with more than 2000 Virtual Machines). 24/7 Operations.

**Responsibilities:** Administration of the Linux virtual servers (more than 2,000 virtual machines.)Ensure the smooth operation of web services (Apache, Nginx, MySQL, PHP) and Web clients on the platform WordPress (more than 20 000 web sites).Incident management, keeping systems up and running, communication with WEB developers to solve L3 issues.

**Team size:** 5

**Technologies and Tools:** Apache 2, Ubuntu Server 12.04, BASH, Shell, MySQL, Nginx, PHP, Nagios, Zabbix, WordPress, HTTP/HTTPS, SSL

### LAMP developer & web application security

**February 2014 to March 2014**

**Company:** Viacon (Denmark)

**Project Name:** viacon.de

**Project description:** Web development & consultancy

**Responsibilities:** Security incident investigation, web application patching, web application security hardening.

**Team size:** 1

**Technologies and Tools:** PHP, MySQL, Debian, OWASP

### Information Security Specialist

**January 2014 to August 2014**

**Company:** Life:) (LifeTech division)

**Project Name:** Mobile Operator Company

**Project description:** Turk Cell subsidiary company in Belarus under brand of "life:)".

**Responsibilities:** Data security, SIEM system configuration and modification, parsers creation, security infrastructure design, incidents investigation, reports creation and analysis, ISO 27001.

**Team size:** 3

**Technologies and Tools:** SIEM system RSA EnVision, Microsoft Office, Windows Server 2008, Red Hat Enterprise Linux, xSpyder, nmap, manual testing, bash, php, VPN, Oracle, MSSQL, infrastructure security scanning and hardening, security analytics, reports creation, infrastructure security improvement with ISO 27001 standard and best practices.

### WebApp Security & InfoSec.

**September 2013 to present**

**Company:** OZ.by

**Project Name:** OZ.by

**Project description:** Penetration testing for online retailer company.

**Responsibilities:** Web application security hardening, information security consulting. Providing them with manual and automated security testing. For manual testing using WASC methodology and some automated tools & scanners.

**Team size:** 1

**Technologies and Tools:** PHP, WASC, manual testing, social engineering, AppScan, Acunetix, Nessus, nikto, BurpSuite, nmap, sqlmap.

### Information Security Specialist

**June 2013 to August 2013**

**Company:** Bubble Gum Interactive (Australia)

**Project Name:** spaceheroes.com

**Project description:** Online game for kids.

**Responsibilities:** Data protection, incidents investigation, script kiddie deanonymization, project security hardening.

**Team size:** 1

**Technologies and Tools:** ActionScript 3, CentOS, social engineering, nmap, AC3 debugger, FlashFireBug (pro version was presented from developers), sniffer (javascript + php). Main aim of my task was to find and deanonymize a hacker who continuously attacked online project, help in creating of letter for police and fix security issues on this project. All tasks were fully completed.

### Microsoft Navision Axapta consultant

**July 2012 to December 2013**

**Company:** BelWillesden

**Project Name:** ERP System consulting

**Project description:** Company consultant for ERP system Microsoft Navision Axapta.

**Responsibilities:** Consulting users with ERP system MS Navision Axapta, writing some scripts on X++

**Team size:** 2

**Technologies and Tools:** Microsoft Navision Axapta, X++ language

### Technical support

**December 2009 to July 2012**

**Company:** BelWillesden

**Project Name:** Technical support

**Project description:** Remote users support

**Responsibilities:** Operation system configuration (Windows 2000, Windows XP, Windows 7), Thin client (based on Citrix) configuration, Lotus notes installation and configuration, software installation (Microsoft Office packeg, 1C, Microsoft Navision Axapta and some others).

**Team size:** 3

**Technologies and Tools:** RDP, VNC, Lotus notes, Microsoft Navision Axapta, 1C, Microsoft Office, Windows XP / 7, Windows Server 2003 / 2008, Citrix.

## EDUCATION

### Minsk trade college

**2008 - 2009**

**Graduate, Commercial activity**

**Diploma/Degree Work:** Diploma

## CERTIFICATES AND TRAININGS

### Dr.Web CureIt! User
**June 19th 2017**

**Details:** Dr.Web code: 87944253
**Link:** http://st.drweb.com/upload/138d0380ff4fa538c5d99011ed07459d_1497865117_5140214_tcrt.png

### Penetration Testing and Ethical Hacking
**April 17th 2017**

**Details:** Cybrary code: C-f1031ade0-a2f5b1
**Link:** https://www.cybrary.it/

### System protection against encryption ransomware
**August 22nd 2017**

**Details:** Dr.Web code: 35231252
**Link:** https://st.drweb.com/upload/2d9415b9710b73ae0dddaeb37b4adb39_1503389838_5229438_tcrt.png

### Mobile Device Security
**August 22nd 2017**

**Details:** Dr.Web code: 44833833
**Link:** https://st.drweb.com/upload/e69d14413b16bb256b9a5d9e56333f2f_1503388150_5229263_tcrt.png

### Certified Ethical Hacker (CEH) from EC-Council
**August 21st 2017**

**Details:** Check code: ECC73069404856
**Link:** https://www.eccouncil.org/

### Web Applications Security Fundamentals
**March 1st 2017**

**Details:** SC-8e96e0fcb-b85e56
**Link:** https://www.cybrary.it/

### SANS Security Awareness Training
**March 21st 2016**

### Network Security Fundamentals
**September 12th 2016**

**Details:** Retratech license: 207912
**Link:** http://certifications.ru/resume/207912/76/en/

### Windows 7: Administration
**September 9th 2016**

**Details:** NOU "INTUIT" License: 100991254
**Link:** http://www.intuit.ru/verifydiplomas/100991254

### HTML "4.01"
**September 8th 2016**

**Details:** NOU "INTUIT" License: 207912100991100
**Link:** http://www.intuit.ru/verifydiplomas/100991100

### PHP: Basics
**September 8th 2016**

**Details:** NOU "INTUIT" License: 100991122
**Link:** http://www.intuit.ru/verifydiplomas/100991122

### Python: Basics
**September 8th 2016**

**Details:** NOU "INTUIT" License: 100991087
**Link:** http://www.intuit.ru/verifydiplomas/100991087

### Information Security

**September 8th 2016**

**Details:** NOU "INTUIT" License: 100991111
**Link:** http://www.intuit.ru/verifydiplomas/100991111

### Apache 2.4 Administration

**September 8th 2016**

**Details:** BrainBench License: 13257149
**Link:** http://sm0k3.net/wp-content/certs/apacheUMurashka.pdf

### Information Technology Security Fundamentals

**September 9th 2016**

**Details:** Retratech License: 207912
**Link:** http://certifications.ru/resume/207912/112/en/

### MySQL databases: Basics

**October 1st 2012**

**Details:** BelHard

## LANGUAGES

### Russian

**Reading:** Native
**Writing:** Native
**Speaking:** Native

### English

**Reading:** Upper Intermediate
**Writing:** Intermediate
**Speaking:** Intermediate

## PERSONAL INFORMATION

**Department:** ICT
**Date of Birth:** November 4th 1989
**Gender:** Male
**Marital Status:** Married
**Military Status:** Does not apply
**Willingness to business travel:** 12 month

## CONTACT INFORMATION

**Phone #:** +375 25 909 05 57

**Mobile #:** +375 33 335 40 20
**E-mail:** info@sm0k3.net
**Skype:** vlad__89
**Bug Bounty:** https://hackerone.com/sm0k3
**LinkedIn:** https://www.linkedin.com/in/sm0k3
**Github:** https://github.com/sm0k3net?tab=repositories