

Michele Orru'

Address: Via San Donato, 9
40057, Quarto Inferiore
Bologna (Italy)

Nationality - Italian
DOB – 14/05/1985

Mobile Number: +39 338 4605410
Email: michele.orrui@antisnatchor.com
LinkedIn: <http://www.linkedin.com/in/micheleorrui>

Education

Sept 2004 – July 2008 University of Bologna Bologna

Bachelor Degree in Internet Sciences

✓ My degree has dealt with methods, techniques and tools used for the development of the systems and economic, organizational and scientific ICT-based applications.

✓ Some of the most treated topics were: Software engineering, Operating Systems, Java Programming, Financial Computation and Organization processes.

✓ My thesis (lead by professor Ozalp Babaoglu) has been focused on research about Exploiting Web Session Management: “Analisi hacker del Session Management nelle applicazioni Web”. In my work I’ve enumerated all the common and uncommon attack vectors (from Session fixation/hijacking to HTTP Request Smuggling, XST, statistical analysis and FIPS tests), with emphasis on real world attack cases on the main web application used by my university to manage student careers (with high impact bugs discovered by me - and censored by them). Finally, I did some research on scalable defense techniques as the usage of WAFs and Honey-pots in production environments.

January 2008 - March 2008 ENEA Bologna

Internship

I’ve developed a secure Web Service to show the ENEA developers how to use effectively the latest OASIS security standards, like WS-security, WS-SecurityPolicy, WS-reliability, WS-Trust.

I also did a security analysis and vulnerability assessment on Moda-ML, an ENEA standard for enterprise web service messaging (based on EB-XML): I discovered some security flaws (wrong implementation of hash functions and public key cryptography) and I’ve organized a two hours presentation privately disclosing the bugs.

September 2007 – December 2007 University of Bologna Bologna

Computer Security

✓ Lead by professor Ozalp Babaoglu, the course was focused on mathematic and cryptography related topics such as PKI, SSL, PGP, Kerberos, ACL, DAC, MAC, Capabilities and Multi-Level Security, Ipsec and DDOS.

✓ The professor personally charged me to present a two-hours practical lecture on hacking related stuff:

✓ SSL/TLS sniffing through fake certificate injection;

✓ rooting an XP machine through IE(vm_rectfill bug);

✓ web application security (practical demos of XSS, cookie stealing, phishing with XSS, and a path traversal attack – all of them were founded during my pen tests)

The collaboration continued until early 2010, with one security seminar organized every semester for new students.

August 2006 - December 2006 University of Bergen Bergen(NO)

Develop Secure Net-based Applications

Lead by professor Khalid Azim Mughal, the course was an in-depth study of Security Patterns (RBAC, DMZ, I&A, front door, non-repudiation, risk determination and management, threat assessment) and Web application vulnerabilities (XSS, blind SQL injection, buffer overflows, weak encryption, MITM attacks, spoofing and sniffing). Creation of video- based attack demonstrations about cookie stealing/injection, SSL/TLS certificate injection and IE browser remote exploits.

January 2006 - May 2006

University of Bergen

Bergen(NO)

Advanced Topics in Java and Security Systems

Lead by professor Khalid Azim Mughal, the course consisted in some really advanced topics about Java 1.6 Concurrency (Thread Safety, JMM, Liveness, Performance, Thread Pools) and Generics (Wildcards, Reification, Reflection, Sets, Lists and Maps).

Research project: Enforcing default security behavior of Java 2 Applications through reflection. I was arrived to really good results, writing also an Eclipse plugin.

Sept 1999 – Jun 2004

Liceo Scientifico

Lanusei

High School Diploma

Main subjects: Mathematics, Physics. Scien Statistic and

Experience

March 2011 – now Royal Bank of Scotland Warsaw

Penetration testing specialist

✓ Penetration testing of worldwide banking systems. Vulnerability research activities.

✓ Main areas: Web Application security, Infrastructure penetration testing, development of custom fuzzers, build reviews on *NIX/Windows, issue mitigation guidelines.

Skills: Metasploit, BurpSuite, Firebug, BeEF, GreaseMonkey, Ruby, custom fuzzers, manual assessment.

October 2010 – now BeEF project Bologna/Warsaw

Core developer

As Web Application Security is one of my main research fields, I couldn't continue without being part of a good open source project. I was using BeEF (<http://beefproject.com>) from many years during pentests and security seminars, and now I'm proud to be part of the core development team. I'm also usually presenting the latest BeEF development at various hacking conferences.

Some of my works:

- ✓ Tunneling Proxy, XssRays integration
- ✓ JBoss/ColdFusion exploits
- ✓ MySQL support
- ✓ core optimization with Thin and Rack
- ✓ many enhancements, command modules and general bug fixing

Skills: Ruby, jQuery, ExtJS, sqlite, custom exploit development, event-machine, Thin, Rack.

May 2009 – May 2010 INFN (National Institute of Nuclear Physic) Bologna

OGF-eu fellow and JEE developer

✓ Working for OGF-europe on Grid/Cloud computing content dissemination: I've also organized and presented some in-depth tutorials on security (Kerberos, Shibboleth, VOMS, and attacks on these applications) and grid/cloud integration, distributed on the OGF-europe portal in a webinar-style.

✓ Main INFN representative at OGF27 (12-16 Oct, Banff, Alberta, Canada): I presented a talk about my main grid/cloud integration research work at INFN, named: "INFN OCCI implementation on Grid Infrastructure". Speaker in three "Grid and Virtualization" sessions at OGF28 (15-18 Mar, Munich, Germany).

✓ Lead architect and Java developer of the Cloud Interface integration on top of the INFN Tier-1 Grid: the OGF OCCI cloud interface API was implemented to add a second IaaS layer on top of the actual grid resources. Java application built with industry standards (Spring, Hibernate/JPA, Restlet, Jetty).

✓ Creator and maintainer of a small private cloud for the R&D group of INFN: the cloud was engineered using Eucalyptus, with a total of 48 cores and 64 Gb RAM, 6 Tb shared storage (gpfs).

✓ Penetration tester on some INFN web application deployed in the Tier-1 production grid. Another independent vulnerability assessment was conducted on INDICO, a world-known web application developed by CERN: the anti-XSS filter has been bypassed and patched have been coordinated with the CERN CSO.

Skills: Java, Spring, Hibernate/JPA, Restlet, Jetty, MySQL, Platform LSF, Eucalyptus, Xen, KVM, Amazon EC2, OCCI cloud standard, web application security, Kerberos, Shibboleth, VOMS.

November 2008 - March 2009 Logital S.P.A. Bologna

Lead Java Programmer

Develop Java/JEE applications to manage access control devices, implementing proprietary and closed source communication protocols.

Build a custom Linux distribution (based on Gentoo) to run Java applications in production environments on custom built hardware (Intel Atom based).

October 2008 - now AntiSnatchOr.com

Vulnerability Research and Penetration Tester

Independent vulnerability researcher: all my posts can be found in my own website

<http://antisnatchor.com>.

- ✓ Penetration Testing and Threat Assessment for private customers.
- ✓ Invited Speaker at Ludwig Maximilians Universitat (Munich) and Hacktivity 2011.
- ✓ Frequent speaker at hacking conferences: CONFidence, Hacktivity, SecurityByte, DeepSec, OWASP.

Random vulnerabilities:

Pentaho BI [<http://jira.pentaho.com/browse/BISERVER-2698>]

Apache OFBiz [<https://issues.apache.org/jira/browse/OFBIZ-1959>]

Konakart [<http://www.konakart.com/knownproblemsfaq.php>]

Eclipse BIRT [https://bugs.eclipse.org/bugs/show_bug.cgi?id=259127]

Skills: Metasploit, BurpSuite, SWFINtruder, Firebug, BeFF, GreaseMonkey, ImmunityDebugger, Peach, Sulley, Ruby, custom fuzzers, manual assessment.

May 2007 – October 2010 IntegratingWeb.com London/Bologna

JEE developer and Lead Security Engineer

✓ Customize Opentaps ERP/CRM for customers to reflect their business needs. Integration with Magento ecommerce creating a REST layer on both sides, and using Pentaho Data Integration to synch the two systems.

✓ Threat Assesment, Penetration Tests and Code Review for customers with ecommerce and ERP systems exposed to Internet. Special attention to mitigation aspects of security threats after the discovery through Black or White Box pen tests.

✓ Build a secure, reliable and powerful BSD based platform for IntegratingWeb.com with FreeBSD and CentOS. Admin and daily maintenance of the network infrastructure.

✓ Implement and manage the security of the web applications with Acegi Security, OWASP ESAPI, mod_security and regular scans.

✓ Writing applications in JEE with Open Source frameworks such as: Alfresco, Spring, OpenTaps, FreeMarker, Beanshell, Groovy, Javascript, Hibernate/JPA, GWT.

Skills: Alfresco, Opentaps, FreeBSD, Gentoo Hardened, CentOS, Grsecurity, PAX, Tomcat, Apache (AJP13 connectors), MySQL, PostgreSQL, vsftpd, Zimbra, OpenVPN, iptables

February 2007 – May 2007 University of Bergen Bergen

Teaching assistant

Teaching assistant in the course of Computer Networks (Tanenbaum's book) at High Technology Center. My work was help the students during labs with exercises and in-depth explanations about security topics related with the course.

November 2006 – now Hakin9 magazine <http://en.hakin9.org>

Writer and beta-tester [<http://en.wikipedia.org/wiki/Hakin9> (second Top Contributor)]

Official writer, reviewer and beta-tester of articles in English and Italian. I've written three articles by now:

- ✓ Introduction to Firewalls: from ISO/OSI stack to DMZ (published in English and Italian)
- ✓ Gentoo Hardened: portare la sicurezza di Linux all'estremo (published in Italian, November 2007);
- ✓ Sniffing SSL/TLS connections through fake certificate injection (published in English, January 2008).

Sept 2006 – Nov 2006 Fantoft Studentboliger Network Group Bergen

System administrator and Security Engineer

Help the Network Group to mitigate and prevent arp-spoofing/sniffing into the Fantoft network, managing HP and D-link switches with SNMP and implementing IDS sensors to statically monitor the arp:IP association of main servers.

Skills: OpenBSD, Snort, SnortSam, MySQL, iptables, dsniff, ettercap.

August 2006 – February 2007 Det Akademiske Kvarter Bergen

System administrator and Security Engineer

✓ Build two IDS servers with FreeBSD and OpenBSD;
✓ Penetration Testing of the remotely exposed servers and the e-ticket application <https://intern.kvarteret.no/ticket/> used by all the students (700 c.a.).

Skills: *BSD, Debian, arpwatsh, Snort, Postgresql, pf, OpenLDAP, Apache, Exim, BIND, MySQL, Paros, nmap, amap, webscarab.

IT Skills

Languages and frameworks: Java, JEE, Ruby, XML (and OASIS security standards), Restlet, FreeMarker, JavaScript, jQuery, ExtJS, Groovy, Beanshell, Spring, Spring Security (old Acegi), Hibernate, JPA, Apache Geronimo (for transactions), Apache OFBiz (contributor), Opentaps (contributor), BeEF (core developer), GWT.

Databases: MySQL, PostgreSQL, Apache Derby, HSQL

Daemons: Apache, Apache Tomcat, Jetty, Apache Axis, vsftpd, ProFTP, Postfix, Courier, OpenSSH, Samba, CIFS, Zimbra, OpenVPN, BIND, Snort

Operating Systems: Mac OS X, Linux (Gentoo, CentOS, Debian), BSD (FreeBSD, OpenBSD), Windows.

Security: Web application security (exploitation and mitigation), Penetration Testing (OSSTMM and OWASP methodologies), Security engineering, SSO systems (Kerberos, Shibboleth), NIDS, HIDS, Linux/*BSD hardening.

Key Skills

Hard working, resourceful, creative and solution oriented person. Ability for problem solving, intuition and perseverance. Acquired presentation skills through presenting projects in Norway at University during Erasmus period, and during Grid/Cloud conferences (OGF27). Leadership and management acquired leading projects team at the university (Operating System and Java security projects) and at INFN (IaaS layer on top of the grid), and with customers while working in IntegratingWeb.com. Good presentation skills acquired speaking in various IT Security conferences: CONFidence 2011, SecurityByte 2011, Hacktivity 2011, DeepSec 2011, OWASP Poland 2011.

Language Skills

My mother tongue is Italian. Studying during my Erasmus period in Norway, I've increased to a good level my English knowledge, both oral and written. I can well understand Spanish too, and a bit of French.

Interests

Music, fishing, travels and philosophy.

References

Available on request.