Baptiste HASSENFRATZ
https://creagenic.com/

Freelance developer and security tester

SKILLS

Web development: HTML, CSS, JavaScript (5 years); PHP (4 years); Node.js, WordPress / BuddyPress, JSON / XML, AJAX (2 years); HTML5 canvas, CSS3 media queries, WebSocket, WebRTC, WebGL, Selenium WebDriver, WebExtensions, Greasemonkey, Xdebug / vdebug (1 year)
Desktop / mobile development: C / C++, shell script (2 years); Python, Perl, Qt, OpenGL, SDL (1 year)
Databases / DBMS: MariaDB / MySQL (3 years); PostgreSQL, SQLite, LibreOffice Base, GeoNames / OpenStreetMap (1 year)
Networks: HTTP / HTTPS web server / Apache (3 years); Nginx, HTTP / SOCKS proxy / Squid / Dante, SSL/TLS / Certbot, DNS / BIND / Dynamic DNS, SMTP / Postfix, IMAP / Dovecot, SpamAssassin / procmail, Roundcube, SPF / DKIM, SSH / port forwarding / screen, FTP / SFTP, OpenVPN, STUN / TURN / coturn, iptables, nmap / ncat, cURL, SMB / Samba, Wireshark / tcpdump, proxychains / redsocks / sshuttle, fail2ban, sslh, stunnel, Insomnia API Client (1 year)
Graphics software: GIMP (2 years); Inkscape, Blender (1 year)
Operating system: GNU/Linux / Unix (5 years); virt-manager, LXC, VNC / X2Go, Xephyr / VirtualGL, Wine / Waydroid (1 year)
Version control: Git (2 years); SVN / git-svn (1 year)
Security: security testing for applications using any programming language / framework / database (3 years); mitmproxy, sqlmap, Nikto, SSL pinning bypass / root detection bypass / Frida, static analysis / dynamic analysis / MobSF, disassembler / decompiler, sslscan / sslyze, PGP, eCryptfs (1 year)

Languages: French (native), English (fluent), German (good knowledge)

TRAINING

Bachelor degree in Computer Science (Licence professionnelle Systèmes Informatiques et Logiciels, spécialité développeur informatique) — 2015
Graduated (honors) at University of Upper Alsace, Mulhouse, in apprenticeship

Associate degree in Computer Science (Brevet de technicien supérieur Informatique et Réseaux pour l'Industrie et les Services techniques) — 2012
Graduated at Lycée Blaise Pascal, Colmar

High school diploma in Electronics (Baccalauréat technologique Sciences et Technologies Industrielles, spécialité Génie Electronique) — 2010
Graduated at Lycée Théodore Deck, Guebwiller

WORK EXPERIENCE

Freelance developer and security tester **2017**
since 18/08/2017

Keywords: *HTML, CSS, JavaScript, PHP, MySQL, WordPress, BuddyPress, Node.js, WebRTC, WebSocket, GeoNames, responsive web design, progressive enhancement, web security, privacy*

WordPress development and customization of the BuddyPress social networking plugin using action and filter hooks.

- Creation of a functionality to search people in a range of kilometers using GeoNames database for self-hosted geocoding.
- WebRTC webcam chat between 2 people with adapter.js and fullscreen.js shims, using Node.js and WebSocket for signaling. Installation and configuration of coturn STUN and TURN server for NAT traversal. A time-limited secret-based authentication generating an HMAC-SHA1 hash is used to access the TURN server in order to prevent unauthorized bandwidth usage, as well as the signaling server to prevent unauthorized login. There is a security check in place to make sure only the requested user can join the call, by verifying the hash containing the username of the person connected to the website. In case the static secret key is leaked, there is an additional security using a random key sent to the other user in the notification to join a call.
  The website, signaling server, STUN and TURN server access is encrypted using SSL/TLS. Use of WebSocket ping / pong requests to keep the connection alive on a reverse-proxy like Cloudflare as well as to detect and close the connection when someone disconnected improperly without sending a disconnect signal (e.g. Wi-Fi or Ethernet disconnection).
- Internationalization and localization of WordPress plugins using a textdomain with gettext, in order to use a translation in English or French depending on the website language. Use of WordPress functions preventing XSS vulnerabilities in translations.
- Systemd service setup to start automatically a WebSocket server at boot time of Linux and restart the server automatically in case of error.

Security testing and report creation in English or French following applications vulnerabilities described by the categories of Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE).

- Research and prevention of vulnerabilities like XSS, CSRF, SQL and NoSQL injection, OS command injection, LFI, RFI, SSRF, insecure authentication or access control, open redirect, clickjacking.

Web developer at Tschach Solutions, Karlsruhe, Germany **2016**
from 07/03/2016 to 11/08/2017 (1 year, 5 months)

Keywords: *HTML, CSS, JavaScript, PHP, MySQL, WordPress, responsive web design, progressive enhancement, web security, privacy*

Plugin development on the WordPress content management system.

- Creation of shortcodes (configurable via parameters) and administration menu pages.
  Use of WordPress's wpdb PHP object to access database and hooks like wp_ajax action to handle AJAX requests.
- Contact buttons and contact boxes were built using object-oriented programming with class inheritance, to display information of an article's author or a customized contact.
- Development of a tool to create, read, update and delete (CRUD) questions that will be sent to customers by email. A random and unique token is generated to answer questions.
  The tool limits the number of questions and answers displayed on a web page, by using a pagination (beginning, previous, next, end) with page number and page count.
  The results can be sorted alphabetically by clicking on a column name.
- Discovery and prevention of web security vulnerabilities like SQL injection, XSS, CSRF, clickjacking and access control.
- Initiative to enhance privacy by removing third-party HTTP requests like Google Fonts and creation of self-hosted social media buttons.

Computer science project for Alsace Nature, Strasbourg, France **2015**
from 11/07/2015 to 14/09/2015 (2 months)

Keywords: *HTML, CSS, JavaScript, PHP, MySQL, Google Maps API, OpenStreetMap, responsive web design, web security*

Volunteer work for an environmental organization, realized within my bachelor degree, as a remote work during my spare time.
The project goal was to update a cartographic web application making a census of wetlands and fills in Alsace region. The application used Google Maps JavaScript API version 2 but was not working anymore after the switch to version 3.

My missions were to make the application compatible with the new version of Google Maps API, to create an images gallery to show photos when moving mouse over thumbnails and to make the application mobile compatible using responsive web design (CSS3 media queries with HTML meta viewport).
The application can be configured to use OpenStreetMap instead of Google Maps. Suggestion to enhance the security of the web application.

- Replacement of deprecated PHP functions (mysql_*) with new ones (mysqli_*) to connect to the database using prepared statements.
- Correction of different SQL injection, XSS and access control vulnerabilities (a non-authorized user could delete data using HTTP requests not protected by an identification).
  CSRF vulnerabilities fixed by using an authenticity token and switch to HTTPS to prevent man-in-the-middle attacks.

- Password storage with the PHP password_hash function that generates a Bcrypt hash corresponding to a salted password hash, which is more secure than MD5.
- Modification of the "lost password" function which initially sent the password in clear text to the user email address. Henceforth, a new random and temporary password is created and stored in a PHP session (identified by a cookie in the web browser) before sending it via email (Postfix).
  When a user connects to the application with the temporary password, he must create a new password by indicating his current password (prevents password and email address modification in case if a non-authorized person gains access to the session).

Web developer apprenticeship at Jnesis, Mulhouse, France **2014**
from 01/10/2014 to 30/09/2015 (1 year), 4 days per week

Keywords: *HTML, CSS, JavaScript, PHP, MySQL, PostgreSQL, WordPress, VirtualBox, responsive web design, progressive enhancement*

Realization of different web development missions for clients in France and abroad.
Use of Scrum agile software development methodology with JIRA and Confluence tools. Work with Linux (Xubuntu) and in a team with Git revision control system.

- Web integration (background video, sticky footer, CSS sprite) in order to personalize a website using eXo Platform, an enterprise social platform and Ext JS, a JavaScript framework with MVC (model-view-controller) architectural pattern.
- Maintenance of a WordPress site made unavailable through a plugin security vulnerability.
- Email coding in HTML / CSS for the company communication.
- Company website update, following principles of responsive web design and progressive enhancement (initiative in order to have a website usable without JavaScript).
  Pure HTML, CSS and JavaScript programming as well as with jQuery and Bootstrap libraries from a CDN, with local fallback. Use of "HTML5 Boilerplate" template with "Modernizr" and "Normalize.css" libraries.
- Automatic selection of French or English version of the website, depending on the browser language, with PHP. Use of the URL rewriting functionality of Apache web server to select manually the language.

Developer summer job at Novartis Pharma, Basel, Switzerland **2012**
from 30/07/2012 to 17/08/2012 (3 weeks)

Keywords: *Visual Basic, Excel macro*

Excel macro creation to copy data from an Excel worksheet to another. Within the bioinformatics department, this work consisted in merging data from CHO cells, collected from different laboratory equipment.
Use of Visual Basic programming language (VBA) and practice of English language.

Computer science project for the CRDP of Strasbourg, France **2012**
from 03/01/2012 to 05/07/2012 (6 months)

Keywords: *HTML, CSS, JavaScript, PHP, MySQL, HTML5 canvas, web security*

ELAN (Enseigner la Langue Allemande par le Numérique) project was realized during my associate degree for the "Centre Régional de Documentation Pédagogique". The project consisted in creating web applications to teach the German language to children in a fun way.

In a team of 5 students, my part of the work was to create a 2D graphic application to connect points between them. Points can correspond to French words that have to be connected with their German translation for example.
It is possible to undo and redo drawn lines. The application can create, edit and delete exercises.
Application design was free but had to be validated by the IT manager. Self-education on HTML5 novelties and web security.

Use of the HTML5 canvas element and the JavaScript programming language.
Work in a LAMP environment with Linux (Debian), Apache, MySQL and PHP.
Use of PDO (PHP Data Objects) to access the database. Data serialized in JSON and sent/received using AJAX. HTML page updated with DOM (Document Object Model) APIs. CSS positioning, prevention of XSS vulnerability and SQL injection.

Database internship at Emerson Process Management, Cernay, France **2011**
from 23/05/2011 to 01/07/2011 (6 weeks)

Keywords: *MySQL, CSV, Excel*

Creation of a MySQL database using CSV files converted from Excel files of the company in order to ease the search of information by employees.
Use of SQL and batch scripts as well as XAMPP and phpMyAdmin applications.

INTERESTS

- Computer science: security, privacy, performance, accessibility (progressive enhancement, responsive web design...)
- Sport: jogging, skiing / snowboarding, surfing
- Environment
- Drawing