Baptiste HASSENFRATZ
https://creagenic.com/

Développeur et testeur en sécurité freelance

COMPETENCES

Développement web : HTML, CSS, JavaScript (5 ans); PHP (4 ans); Node.js, WordPress / BuddyPress, JSON / XML, AJAX (2 ans); HTML5 canvas, CSS3 media queries, WebSocket, WebRTC, WebGL, Selenium WebDriver, WebExtensions, Greasemonkey, Xdebug / vdebug (1 an)
Développement desktop / mobile : C / C++, shell script (2 ans); Python, Perl, Qt, OpenGL, SDL (1 an)
Bases de données / SGBD : MariaDB / MySQL (3 ans); PostgreSQL, SQLite, LibreOffice Base, GeoNames / OpenStreetMap (1 an)
Réseaux : HTTP / HTTPS web server / Apache (3 ans); 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 an)
Logiciel graphique : GIMP (2 ans); Inkscape, Blender (1 an)
Système d'exploitation : GNU/Linux / Unix (5 ans); virt-manager, LXC, VNC / X2Go, Xephyr / VirtualGL, Wine / Waydroid (1 an)
Gestion de versions : Git (2 ans); SVN / git-svn (1 an)
Sécurité : tests de sécurité pour des applications utilisant n'importe quel langage de programmation / framework / base de données (3 ans), mitmproxy, sqlmap, Nikto, SSL pinning bypass / root detection bypass / Frida, analyse statique / analyse dynamique / MobSF, désassembleur / décompilateur, sslscan / sslyze, PGP, eCryptfs (1 an)

Langues : anglais (courant), allemand (bonnes connaissances)

FORMATION

Licence professionnelle Systèmes Informatiques et Logiciels, 2015
spécialité développeur informatique (LP SIL développeur informatique)
Diplômé (mention AB) à l'université de Haute-Alsace, à Mulhouse, en alternance

Brevet de technicien supérieur Informatique et Réseaux 2012
pour l'Industrie et les Services techniques (BTS IRIS)
Diplômé au lycée Blaise Pascal, à Colmar

Baccalauréat technologique Sciences et Technologies Industrielles, 2010
spécialité Génie Electronique (BAC STI Génie Electronique)
Diplômé au lycée Théodore Deck, à Guebwiller

EXPERIENCE PROFESSIONNELLE

Développeur et testeur en sécurité freelance **2017**
depuis le 18/08/2017

Mots-clés : *HTML, CSS, JavaScript, PHP, MySQL, WordPress, BuddyPress, Node.js, WebRTC, WebSocket, GeoNames, responsive web design, amélioration progressive, sécurité web, confidentialité*

Développement WordPress et personnalisation du plugin de réseau social BuddyPress en utilisant des "hooks" d'action et de filtre.

- Création d'une fonctionnalité pour chercher des personnes dans un rayon de kilomètres en utilisant la base de données GeoNames pour le géocodage auto-hébergé.
- Chat webcam WebRTC entre 2 personnes avec les "shims" adapter.js et fullscreen.js, en utilisant Node.js et WebSocket pour le signalement. Installation et configuration de coturn, un serveur STUN et TURN utilisé pour le NAT traversal. Une authentification limité dans le temps avec clé secrète permettant de générer un hash HMAC-SHA1 est utilisée pour accéder au serveur TURN afin d'éviter une utilisation non autorisée de la bande passante, ainsi que pour accéder au serveur de signalement afin d'éviter une authentification non autorisée. Il y a une sécurité en place pour être sûr que seul l'utilisateur appelé permette de rejoindre l'appel, en vérifiant le hash contenant le nom d'utilisateur de la personne connectée au site web. Dans le cas ou la clé secrète statique est découverte, une sécurité additionnelle est présente en envoyant une clé secrète aléatoire à l'autre utilisateur dans la notification permettant de rejoindre un appel.
  L'accès au site web, au serveur de signalement, au serveur STUN et TURN est encrypté en utilisant SSL/TLS.
  Utilisation de requêtes ping / pong avec WebSocket afin de garder la connexion active sur un reverse-proxy comme Cloudflare ainsi que de terminer la connexion quand quelqu'un se déconnecte de manière incorrecte sans envoyer de signal de déconnexion (par exemple en cas de déconnexion Wi-Fi ou Ethernet).
- Internationalisation et localisation de plugins WordPress en utilisant un textdomain avec gettext, afin d'utiliser une traduction en anglais ou français suivant la langue du site web. Utilisation des fonctions WordPress permettant d'éviter les failles XSS dans les traductions.
- Configuration d'un service systemd pour démarrer automatiquement un serveur WebSocket au démarrage de Linux et redémarrer le serveur automatiquement en cas d'erreur.

Tests de sécurité et création de rapports en anglais ou français en suivant les vulnérabilités d'applications décrites par les catégories de Open Web Application Security Project (OWASP) et Common Weakness Enumeration (CWE).

- Recherche et prévention de vulnérabilités telles que XSS, CSRF, injection SQL et NoSQL, OS command injection, LFI, RFI, SSRF, authentification ou contrôle d'accès non sécurisé, open redirect, clickjacking.

Développeur web chez Tschach Solutions, à Karlsruhe, Allemagne **2016**
du 07/03/2016 au 11/08/2017 (1 an, 5 mois)

Mots-clés : *HTML, CSS, JavaScript, PHP, MySQL, WordPress, responsive web design, amélioration progressive, sécurité web, confidentialité*

Développement web sur le système de gestion de contenu WordPress.

- Création de shortcodes (configurable via paramètres) et pages de menu d'administration. Utilisation de l'objet PHP wpdb de WordPress pour accéder à la base de données et des "hooks" comme l'action wp_ajax pour gérer les requêtes AJAX.
- Des boutons de contact et boîtes de contact ont été créés en utilisant la programmation orientée objet avec héritage de classe, pour afficher des informations sur l'auteur d'un article ou d'un contact personnalisé.
- Développement d'un outil pour créer, lire, actualiser et supprimer (CRUD) des questions qui seront envoyées à des clients par email. Un token aléatoire et unique est généré pour répondre aux questions.
  L'outil limite le nombre de questions et réponses affichées sur une page web, en utilisant une pagination (début, précédent, suivant, fin) avec un numéro de page et un compteur de pages.
- Découverte et prévention de vulnérabilités de sécurité web comme l'injection SQL, les failles XSS, CSRF, clickjacking et le contrôle d'accès.
- Initiative d'améliorer la confidentialité en supprimant les requêtes HTTP tierces comme Google Fonts et création de boutons de médias sociaux auto-hébergés.

Projet informatique pour Alsace Nature, à Strasbourg, France **2015**
du 11/07/2015 au 14/09/2015 (2 mois)

Mots-clés : *HTML, CSS, JavaScript, PHP, MySQL, API Google Maps, OpenStreetMap, responsive web design, sécurité web*

Travail bénévole pour une association de protection de l'environnement, réalisé dans le cadre de la licence professionnelle développeur informatique, à distance durant mon temps libre.
Le projet avait pour but la mise à jour d'une application web cartographique de recensement des zones humides et remblais en Alsace. L'application utilisait l'API JavaScript Google Maps version 2 mais n'était plus fonctionnelle après le passage en version 3.

Mes missions étaient d'assurer la compatibilité de l'application avec la nouvelle version de l'API Google Maps, de créer une galerie d'images permettant d'afficher des photos à partir de miniatures, au survol de la souris et de rendre l'application compatible mobile en utilisant le responsive web design (propriétés CSS3 media queries avec la balise HTML meta viewport).
L'application peut être configurée pour utiliser OpenStreetMap à la place de Google Maps. Proposition d'amélioration de la sécurité de l'application web.

- Remplacement des fonctions PHP obsolètes (mysql_*) par les nouvelles (mysqli_*), permettant l'accès à la base de données en utilisant des requêtes préparées (prepared statements).
- Correction de différentes failles d'injection SQL, failles XSS et de contrôle d'accès (un utilisateur non autorisé pouvait supprimer des données en utilisant des requêtes HTTP non protégées par une identification).

Des failles de sécurité CSRF ont été corrigées en utilisant un token d'authenticité et le HTTPS a été mis en place pour éviter les attaques de type man-in-the-middle.
- Stockage des mots de passe avec la fonction PHP password_hash générant un hash Bcrypt, correspondant à un mot de passe hashé avec "salage", qui est plus sécurisé que MD5.
- Modification de la fonction "mot de passe oublié" qui envoyait initialement le mot de passe en clair à l'adresse mail de l'utilisateur. Désormais, un nouveau mot de passe aléatoire et temporaire est créé et stocké dans une session PHP (identifiée par un cookie sur le navigateur web) avant d'être envoyé par mail (Postfix).
  Lorsqu'un utilisateur se connecte à l'application avec le mot de passe temporaire, il doit créer un nouveau mot de passe, en indiquant son mot de passe actuel (évite la modification du mot de passe et de l'adresse mail dans le cas où une personne non autorisée accède à la session).

Développeur web en alternance chez Jnesis, à Mulhouse, France **2014**
du 01/10/2014 au 30/09/2015 (1 an), 4 jours par semaine

Mots-clés : *HTML, CSS, JavaScript, PHP, MySQL, PostgreSQL, WordPress, VirtualBox, responsive web design, amélioration progressive*

Réalisation de différentes missions de développement web pour des clients en France et à l'étranger. Utilisation de la méthode agile Scrum avec les outils JIRA et Confluence. Travail sous Linux (Xubuntu) et en équipe avec le logiciel de gestion de versions Git.

- Intégration web (vidéo en arrière-plan, sticky footer, sprite CSS) afin de personnaliser un site web utilisant la plateforme sociale d'entreprise eXo Platform et le framework JavaScript Ext JS avec l'architecture MVC (modèle-vue-contrôleur).
- Maintenance d'un site WordPress rendu inaccessible à partir d'une faille de sécurité dans un plugin.
- Codage d'un email en HTML / CSS pour la communication de l'entreprise.
- Mise à jour du site web de l'entreprise en respectant les principes du responsive web design et de l'amélioration progressive (initiative afin d'avoir un site utilisable sans JavaScript).
  Programmation HTML, CSS et JavaScript pure ainsi qu'avec les librairies jQuery et Bootstrap depuis un CDN, avec local fallback. Utilisation de la template "HTML5 Boilerplate" avec les bibliothèques "Modernizr" et "Normalize.css".
- Sélection automatique de la version française ou anglaise du site en fonction de la langue du navigateur, avec PHP. Utilisation de la fonction URL rewriting du serveur web Apache pour la sélection manuelle de la langue.

Développeur (job d'été) chez Novartis Pharma, à Bâle, Suisse **2012**
du 30/07/2012 au 17/08/2012 (3 semaines)

Mots-clés : *Visual Basic, macro Excel*

Création d'une macro Excel pour copier des informations d'une feuille de calcul Excel à une autre. Au sein du département de bioinformatique, ce travail a permis de fusionner des données de cellules CHO, elles-mêmes collectées depuis diverses machines de laboratoire.
Utilisation du langage de programmation Visual Basic (VBA) et pratique de la langue anglaise.

Projet informatique pour le CRDP de Strasbourg, France **2012**
du 03/01/2012 au 05/07/2012 (6 mois)

Mots-clés : *HTML, CSS, JavaScript, PHP, MySQL, HTML5 canvas, sécurité web*

Projet ELAN (Enseigner la Langue Allemande par le Numérique) du BTS IRIS pour le Centre Régional de Documentation Pédagogique. Il fallait créer des applications web permettant l'apprentissage de la langue allemande aux enfants, de manière ludique.

Dans une équipe de 5 étudiants, ma partie consistait à créer une application graphique 2D pour relier des points entre eux, correspondant à des mots français qu'il faut relier à leur traduction allemande par exemple.
Il est possible d'annuler et répéter les tracés. L'application permet de créer, modifier et supprimer des exercices.
La conception de l'application était libre mais devait être validée par le responsable informatique. Autoformation sur les nouveautés du HTML5 ainsi que la sécurité web.

Utilisation de l'élément HTML5 canvas et du langage de programmation JavaScript.
Travail sous environnement LAMP avec Linux (Debian), Apache, MySQL et PHP.
Utilisation de PDO (PHP Data Objects) pour l'accès à la base de données. Données sérialisées en JSON et envoyées/reçues via AJAX. Mise à jour de la page HTML avec les APIs du DOM (Document Object Model). Positionnement CSS, prévention de failles XSS et injection SQL.

Stage base de données chez Emerson Process Management, à Cernay, France **2011**
du 23/05/2011 au 01/07/2011 (6 semaines)

Mots-clés : *MySQL, CSV, Excel*

Création d'une base de données MySQL à partir de fichiers CSV convertis depuis des fichiers Excel de l'entreprise afin de faciliter la recherche d'informations par les employés.
Utilisation de scripts SQL et batch ainsi que des applications XAMPP et phpMyAdmin.

CENTRES D'INTERET

- Informatique : sécurité, confidentialité, performance, accessibilité (amélioration progressive, responsive web design...)
- Sport : jogging, ski / snowboard, surf
- Environnement
- Dessin