Web Application Security [WAS]

Responsable Buchs Christian

MRU TIC / HEIG-VD

Domaines de spécialisation TIC

Capacité d'accueil min. 5

Capacité d'accueil max. 16

Résumé

A la fin de ce cours, l'étudiant-e est capable de :
- décrire les types d'attaques les plus courants contre une application web;
- identifier et expliquer les vulnérabilités typiques dans les applications web et de proposer et appliquer les mesures de protection adaptées;
- évaluer et appliquer les méthodes et outils pour tester la sécurité des applications web;
- développer des applications web avec un niveau de sécurité approprié.

Contenu

Sujet	Temps [%]
1) Sécurité dans le cycle de vie du développement d'applications web : processus de développement, activités, rôles - Introduction au "WAS Contest"	10
2) Vulnérabilités et attaques dans les applications web, Top 10 présenté par le resp. de l'OWASP Geneva, et expérimentation pratique : exploitation de vulnérabilités réelles d'une application web avec WebGoat (application J2EE délibérément non sécurisée)	25
3) Développement d'applications web sécurisées : principes de programmation web sécurisée, paiements e-commerce, services web, ajax et autres technologies d'interfaces	20
4) Tests de la sécurité des applications web : revue de code, outils, tests de pénétration- Travail pratique : test d'une application web	25
5) WAS Contest : afin d'appliquer et pratiquer les notions (sécurisation, tests) vues, en fin de module, 4 équipes sont formées et "s'affrontent"	20

Connaissances préalables

- Notions de base en sécurité de l'information technique (menaces, mécanismes de défenses, etc.) qui peuvent être acquises par exemple avec le module central "IT Security".
- Bases du web (HTTP, X/HTML, Apache, bases de données, ...)
- Notions de programmation web (SQL, PHP, JSP, scripts côté client comme JavaScript, etc.)
- Avoir au moins une fois fait un peu de développement web (base de données, programmation côté serveur et côté client)

Méthodes d'enseignement

Mode	Périodes d'enseignement	Volume de travail (en heures)
Exposés	21	45
Exercices	6	12.86
Travaux pratiques	15	32.14
TOTAL	42	90
Crédits ECTS		3

Évaluation Examen écrit

Pondération de l'examen 70 %

Web Application Security [WAS]

Compétences visées

Gérer le projet	**0%**
Sait choisir et appliquer la méthode adéquate de gestion de projet, pour des projets de complexité moyenne	
Sait identifier les contraintes économiques et les formuler (business plan)	
Sait exploiter les ressources internes et identifier les ressources externes permettant de mettre en oeuvre une solution	
Est capable de s'intégrer dans un groupe; est en mesure d'animer, motiver et convaincre les membres du groupe	
A le sens de l'initiative personnelle et des responsabilités	
Analyser et spécifier des produits / services	**10%**
Est capable d'analyser les besoins du client dans le domaine de spécialisation et sait traduire les exigences et contraintes dans le contexte technico-scientifico-économique et environnemental adéquat	
Est capable de spécifier, planifier, concevoir et mettre en oeuvre des architectures de systèmes spécifiques au domaine de spécialisation, en intégrant des composants hétérogènes et en respectant les exigences d'interopérabilité et d'évolutivité des systèmes, ainsi que les normes et standards	X
Est capable de mener des études de faisabilité et de proposer des services de conseil	
Est capable de superviser et analyser (monitoring) la sécurité d'un système IT et développer des tableaux de bord renseignant sur l'état du système	
Est capable d'effectuer une analyse du risque IT et sait choisir la méthode adéquate et, le cas échéant, l'adapter ou en développer une nouvelle	
Est capable de spécifier, dans un cahier des charges, les besoins du client, après les avoir traduits dans le contexte technico-économique adéquat	
Est en mesure de proposer et comparer des solutions et peut justifier un choix avec des arguments techniques, économiques, organisationnels ou environnementaux appropriés	
Est capable de se mettre à la place de l'utilisateur pour conce-voir un produit répondant à ses attentes	
Développer et réaliser	**30%**
Sait choisir et mettre en oeuvre efficacement un outil de modé-lisation dans son domaine de spécialisation	X
Est capable de choisir et mettre en oeuvre efficacement une approche d'aide à la décision pour résoudre des problèmes complexes et, le cas échéant, de l'adapter ou en développer une nouvelle	
Est capable de choisir et mettre en oeuvre efficacement une méthode d'optimisation et, le cas échéant, de l'adapter ou en développer une nouvelle	
Est capable de choisir et mettre en oeuvre efficacement une méthode de gestion et de configuration de réseaux et de services	
A appris à comparer entre elles diverses méthodes de recherche et de traitement de l'information multimédia et est capable d'en développer de nouvelles	
A appris à comparer entre elles diverses méthodes de développement logiciel, de gestion de versions, de gestion de problèmes, de automatisée de logiciel et est capable de les appliquer, les adapter ou d'en développer de nouvelles	
Sait appliquer les bonnes pratiques et modèles de conception (design patterns) pour des systèmes logiciels	X
Sait utiliser à bon escient les concepts et techniques d'ingénierie et de stockage de l'information	
Est capable d'évaluer et choisir des systèmes de transport (SAN, WAN, ?) et serveurs de stockage de l'information multimédia	
Est capable de proposer des approches innovantes pour la réalisation d'interfaces d'utilisateur adaptatives et adaptables en fonction des besoins et des profils des utilisateurs, en adoptant une approche ergonomique	
Est capable de proposer des approches innovantes pour la réalisation d'interfaces adaptatives en fonction du contexte (p. ex. drivers, type de réseau)	
Maîtrise les technologies de simulation graphiques tri-dimensionnelles et réalité virtuelle, p. ex. les GIS (Geographic Information Systems)	
Sait évaluer et choisir une méthode de traitement de l'information multimédia appropriée	
Connaît les principes de l'informatique pervasive (ubiquitous computing) et sait les appliquer pour concevoir des solutions d'interaction homme-machine efficaces	
Connaît les techniques de parallélisation logicielles et matérielles et de distribution des processus et des données	
Sait comparer les méthodes de co-design et est en mesure de choisir la méthode appropriée	
Est capable de mettre en oeuvre un outil de simulation de système complexe et d'optimiser son architecture, sa performance (p. ex. qualité de service)	
Est capable de concevoir, vérifier, réaliser et valider un système numérique	
Sait appliquer les techniques de poly-publishing et de cross-média	
Est capable de développer, porter, adapter des composants logiciels de bas niveau (bootstrap, moniteur, driver, os, etc.) sur différentes architectures, en maîtrisant les aspects liés aux interactions logiciel-matériel	
Est capable de développer de nouvelles applications en respectant les contraintes propres aux environnements mobiles (os, transmission, consommation, interfaces, etc.)	
Est capable de modéliser un système physique en vue d'une implémentation informatique	
Sait appliquer des méthodologies de travail appropriées et organiser son temps	X
A été sensibilisé aux règles d'éthique et du développement durable	
Valider, améliorer et disséminer	**60%**
Sait choisir et mettre en oeuvre efficacement un outil de test et de validation	
A appris à auditer un système d'information et est capable de proposer des mesures appropriées pour son amélioration	X
A appris à auditer la sécurité d'un système IT et est capable de proposer des mesures appropriées pour son amélioration	X
A appris à auditer l'architecture d'un système de commu-nication et est capable de proposer des mesures appropriées pour son amélioration	X
A appris à auditer une architecture logicielle et le code y relatif et est capable de proposer des mesures appropriées pour son amélioration	X
Est capable de choisir et mettre en oeuvre efficacement une approche d'ontologie informationnelle et de gestion de connaissances et, le cas échéant, de l'adapter ou en développer une nouvelle	
Est capable de concevoir et réaliser une plate-forme d'essai permettant de valider des architectures de systèmes ainsi que des composants matériels ou logiciels et d'optimiser leur fonctionnement	
Est en mesure d'assurer la veille technologique dans son domaine et d'intégrer les connaissances nouvelles	X
Sait rédiger, présenter, communiquer et convaincre de manière pertinente	
Est intégré dans des réseaux profession-nels lui facilitant les échanges d'information, les expériences et la veille technologique	
Est en mesure d'acquérir de façon autonome des connaissances et compétences nouvelles	X