heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Département des Technologies de l'Information et de la Communication (TIC)

Sécurité des Technologies Internet (STI)

3ème année Bachelor, orientations TS
Semestre 5 (17.09.2018 – 24.01.2019)
Année 2018-19

Organisation de l'unité

1. Versions du document

V1 – 13.09.2016
V2 – 17.09.2016
V3 – 22.09.2016
V4 – 23.09.2016
V5 – 10.09.2017
V7 – 20.08.2018
V8 – 10.09.2019

2. Objectifs

A la fin du cours les étudiants devront être capables

- d'expliquer les risques liés aux applications Web
- de développer de manière sécurisée et reconnaître des failles dans les applications Web
- d'expliquer les attaques des applications Web

3. Contenu

1. Sécurité des applications Web

1.1. Introduction

- Histoire du Web
- Evolution des applications Web
- La sécurité des applications
- OWASP

1.2. Technologies des applications Web

- Rappel sur le protocole HTTP
- HTTP stateless rendu stateful
- Encodage des pages
- Authentification HTTP

1.3. Cartographier l'application Web

- Énumérer le contenu et les fonctionnalités
- Analyser l'application

1.4. Attaques des applications Web

- Contourner les protections côté client
  - Champs cachés, cookies, paramètre dans l'URL, …
- Attaquer l'authentification
  - Erreur de conception (mauvais mdp, erreur bavarde, password change, …)
  - Erreur d'implémentation
  - Sécurisation
- Attaquer la gestion des sessions
  - Sessions et alternatives (gestion des tokens et sécurisation)
- Attaquer le contrôle d'accès
  - Vulnérabilités courantes (fonction non protégée, accès basé sur l'id, fichier statique, …)
- Attaquer le stockage
  - SQL injection
- Attaquer la logique de l'application
- Attaquer l'utilisateur
  - XSS
- Attaquer l'utilisateur
  - CSRF, cross-domain data, local privacy attacks, ActiveX, navigateur, …
- Automatisation des attaques (Burp Suite)

1.5. Autres attaques Web

- Information discolsure, compiled application, application architecture, application server, …

1.6. Méthodologie d'attaque

- Revue du code source
- La boîte à outils
- La méthodologie d'attaque

2. Développement Web sécurisé

2.1. Modélisation de menaces

4. Philosophie du cours

4.1. Cours

Certaines notions seront enseignées par le professeur.

4.2. Exercices théoriques et pratiques

Les exercices permettent à l'étudiant-e de tester et d'approfondir les concepts appris. Ce sont des questions théoriques, des études de cas, des problèmes à résoudre et des manipulations pratiques. Les exercices seront annoncés pendant les cours. Selon le temps à disposition, certains exercices pourront être démarrés ou effectués en classe. Sinon, ils seront à réaliser en tant que travail personnel.

De manière générale, les exercices ne seront pas notés.

4.3. Présentations par les étudiants

Les étudiants devront réaliser une présentation par équipes sur un sujet imposé. Chaque présentation aura une durée d'une période, questions comprises.

Plus d'informations se trouvent dans la section 12. Présentations par les étudiants à la page 10.

4.4. Laboratoires

Un laboratoire a pour but d'approfondir une ou plusieurs notions vues en cours en les mettant en pratique. Il est prévu de réaliser des périodes de laboratoires.

Chaque laboratoire est à effectuer individuellement par chaque étudiant.

De manière générale, les laboratoires ne seront pas à rendre et ne seront pas notés

L'assimilation des connaissances et l'acquisition des connaissances prévues dans les laboratoires seront également vérifiées lors de travaux écrits.

4.5. Projets

Pour chaque projet, les modalités détaillées seront expliquées dans un document séparé.

Pour rendre son projet, un email avec les éléments à fournir pour l'évaluation (voir les modalités précises décrites à la fin de chaque donnée) devra être envoyé au professeur et à l'assistant au plus tard à la date d'échéance.

L'assimilation des connaissances et l'acquisition des connaissances prévues dans les projets pourront être vérifiées lors de travaux écrits.

5. Examen

Pour cette unité d'enseignement, un examen final est prévu. Il se déroulera pendant la session d'examens, en fin de semestre. Il peut consister en :

- des questions théoriques
- des questions de type exercice, étude de cas
- des questions portant sur le contenu des laboratoires
- des QCMs
- des questions nouvelles, inconnues

Pour l'examen, sauf indication contraire, seules les feuilles de synthèse ainsi que 1 feuille A4 recto-verso de résumé personnel seront autorisées.

6. Documents de l'unité

Les éventuelles informations concernant l'unité seront disponibles à cet emplacement :

Mac OS X	cifs://eistore1.einet.ad.eivd.ch/profs/ARS/cours/STI
Windows	\\eistore1\profs\ARS\cours\STI

7. Sanctions

7.1. Rendu en retard

Pour les rendus en cours de semestre (archives, présentations, projets, etc.), en cas de retard, les pénalités suivantes seront appliquées sur la note du sujet :

Entre 0 et 1 heures :	-0.5pt
Entre 1 et 3 heures :	-1.0pt
Entre 3 et 12 heures :	-1.5pt
Entre 12 et 24 heures :	-2.0pt
Entre 1 et 2 jours :	-3.0pt
Dès 2 jours :	la note de 1 est assignée au sujet

7.2. Travail non-rendu, absence

Pour rappel, la note de "un" est attribuée par défaut pour tout laboratoire non rendu (projet) ou pour toute absence lors d'une évaluation (présentations) ou à l'examen final (EF) (sauf certificat médical ou autre justificatif valable validé par le secrétariat).

7.3. Plagiat

Les cas de plagiat ou de tricherie détectés lors de laboratoires, les travaux écrits (contributions au portfolio, présentations, feuillets de synthèse), ou l'examen final sont considérés comme graves. La note de "un" sera attribuée à toutes les personnes impliquées (y compris celles qui mettent leurs travaux "à disposition"), et le cas sera dénoncé au doyen.

8. Note finale

Calcul de la note de laboratoire :

La note de laboratoire est déterminée en calculant la moyenne des **projets**. La pondération sera définie en cours de semestre.

Calcul de la note de contrôle continu :

Le **70 % de la note de contrôle continu** est déterminée en assignant une pondération identique à tous les **sujets présentés par les étudiants**.

Pour chaque sujet, l'évaluation est pondérée de la manière suivante :

- 35% présentation, contenu
- 15% présentation, qualité
- 20% démonstration
- 30% feuille de synthèse

Le 30 % qui reste viendra d'un quiz qui sera réalisé à la fin de toutes les présentations des sujets.

Calcul de la note finale :

Conformément à la fiche d'unité, la note finale est composée de

- 25% de la note de laboratoires (**projets**),

- 25% de la note de contrôle continu (**sujets**),
- 50% de la note de l'**examen final**.

9. Répartition des heures

9.1. Répartition des heures selon la fiche d'unité

Travail encadré	48 périodes
Travail personnel	72 périodes
Total	120 périodes (soit ~90 heures) (~5.5 heures par sem. + prép. à l'examen)

9.2. Répartition du travail encadré

Exposés en classe	9 périodes
Exercices en classe (labos)	8 périodes
Contrôle continu (présentations)	11 périodes
Laboratoires (projets)	20 périodes
Total	36 périodes

9.3. Répartition du travail personnel

Révision du cours	9	Revue du cours et lecture de divers supports
Présentations des étudiants	30	Préparation des sujet et présentations
Exercices théoriques/pratiques	6	Résolution d'exercices et manipulations pratiques
Laboratoires/projets	15	Finalisation des laboratoires et projets et rédaction des rapports
Préparation au contôles	12	Préparation aux travaux écrits
Total	72 périodes	

10. Livres de référence et supports

Cf cours.

11. Calendrier prévu STI

Ce calendrier est donné à titre indicatif et peut être changé en tout temps.

S	S	Date	Chap.	Contenu	Rendus
1	38	18.11	1 – Admin	Administration 1.1 - Introduction 1.2 - Technologies des applications Web	
		20.11	1 – Sécurité Web	1.1 - Introduction 1.2 - Technologies des applications Web	
			Projet 1	Introduction au Projet 1	
2	39	25.09	Projet 1	Libre	
		27.09	Projet 1	Libre	
3	40	02.10	Projet 1	Libre	
		04.10	Projet 1	Libre	
4	41	09.10	Projet 1	Libre	
		11.10	Projet 1	Libre	
5	42	16.10	Projet 1	Libre	
		18.10	Projet 1	Présentation projet 1 (10 min/groupe)	Merc. 16.10 23h59 Fichiers projet 1
	43	23.10	Vacances	Vacances	
		25.10	Vacances	Vacances	
6	44	30.10	Projet 2	Introduction bWAPP & Burp Introduction au Projet 2	
			2 – Développement sécurisé	2.1 - Modélisation de menaces	
		01.11	2 – Développement sécurisé	2.1 - Modélisation de menaces	
7	45	06.11	Projet 2	Libre	
		08.11	Projet 2	Libre	
8	46	13.11	1 – Sécurité Web	Sujets 1-2	Lun. 11.11 12h00 Sujets 1-2-3
		15.11	1 – Sécurité Web	Sujet 3	Lun. 11.11 12h00 Sujets 1-2-3
9	47	20.11	1 – Sécurité Web	Sujets 4-5	Lun. 18.11 12h00 Sujets 4-5-6
		22.11	1 – Sécurité Web	Sujet 6	Lun. 18.11 12h00 Sujets 4-5-6
10	48	27.11	1 – Sécurité Web	Sujets 7-8	Lun. 25.11 12h00 Sujets 7-8-9
		29.11	1 – Sécurité Web	Sujet 9	Lun. 25.11 12h00 Sujets 7-8-9
11	49	04.12	1 – Sécurité Web	Sujets 10-11	Lun. 02.02 12h00 Sujets 10-11-12
		06.12	1 – Sécurité Web	Sujet 12	Lun. 02.03 12h00 Sujets 10-11-12
12	50	11.12	Projet 2	Libre	
		13.12	Projet 2	Libre	
13	51	18.12	Projet 2	Libre	
		20.12	Projet 2	Libre	
	52				
	1				
14	2	08.01	Projet 2	Libre	
		10.01	Projet 2	Libre	
			Quiz	Cours, présentations des étudiants, projets	
15	3	15.01	Projet 2	Libre	
		17.01	Projet 2	Présentation projet 2 (15 min/groupe)	Mer. 15.01 23h59 Fichiers projet 2
16	4	22.01	Projet 2	Présentation projet 2 (15 min/groupe)	Mer. 15.01 23h59 Fichiers projet 2
		24.01	Projet 2	Présentation projet 2 (15 min/groupe)	Mer. 15.01 23h59 Fichiers projet 2

12. Présentations par les étudiants

Chaque étudiant sera **évalué individuellement**. Des équipes de trois étudiants recevront 1 sujet parmi les 12 sujets proposés (il y aura 2 équipes de deux étudiants). Les documents à rendre seront :

- la présentation au format pdf
- les sources de la présentation (.ppt, .key, images, ...) dans une archive zip
- la feuille de synthèse en format pdf
- les sources de la feuille de synthèse (.tex, images, ...) dans une archive zip

Il est demandé de respecter les templates fournis par le professeur.

Il est également demandé de suivre la convention pour les noms de fichiers :

Pour un sujet S et les initiales des auteurs IN1, IN2, IN3, les documents doivent avoir les noms suivants :

L'archive globale sera nommée :
STI19_S_IN1_IN2_IN3.zip
qui contiendra les fichiers suivants :
STI19_S_IN1_IN2_IN3_presentation.pdf
STI19_S_IN1_IN2_IN3_presentation.zip
STI19_S_IN1_IN2_IN3_synthese.pdf
STI19_S_IN1_IN2_IN3_synthese.zip

Exemple :
STI19_AttaquesWeb_AD_AR_PZ.zip contient :
STI19_AttaquesWeb_AD_AR_PZ _ presentation.pdf
Il doit respecter le template.
STI19_AttaquesWeb_AD_AR_PZ _ presentation.zip
L'archive contient tout le nécessaire pour reproduire le pdf ci-dessus.
Cela inclut le PPT/Keynote ou autres ainsi que les images.
STI19_AttaquesWeb_AD_AR_PZ _synthese.pdf
Il doit respecter le template.
Il doit faire au maximum une 1 page (recto).
STI19_AttaquesWeb_AD_AR_PZ _synthese.zip
L'archive contient tout le nécessaire pour reproduire le pdf ci-dessus.
Le contenu doit compiler du premier coup.

Le rendu doit être annoncé par email au professeur et à l'assistant. L'email contiendra le lien sur un repo Github contenant l'archive de la présentation.

L'évaluation du sujet portera :

- sur la feuille de synthèse (voir feuille d'évaluation)
- sur la présentation (voir feuille d'évaluation)
- le **respect des noms de fichiers**, délais, templates, consignes, etc.

Les étudiants veilleront eux-mêmes à rendre **tous** les documents demandés avant le délai.