

Қазақстан Республикасының білім және ғылым министрлігі

Қарағанды мемлекеттік техникалық университеті

Бекітемін
Ғылыми кеңес төрағасы,
ректор, ҚР ҰҒА академигі
Ғазалиев А.М.

« ____ » _____ 2013ж.

СТУДЕНТКЕ АРНАЛҒАН ПӘН БОЙЫНША
ОҚЫТУ БАҒДАРЛАМАСЫ (SYLLABUS)

АР(II) 4312 «Арнайы пән II» пәні

АР 29 «Арнайы пән» модулі

5В100200 – «Ақпараттық қауіпсіздендіру жүйесі» мамандығы

Ақпараттық технологиялар факультеті

Ақпараттық технологиялар және қауіпсіздік кафедрасы

АЛҒЫ СӨЗ

Студентке арналған пән бойынша оқыту бағдарламасы (syllabus) әзірленеді:
АТҚ кафедрасының ғ.п.к. доцент Коккоз М.М.

«Ақпараттық технологиялар және қауіпсіздік» кафедрасының отырысында
талқыланған

« ____ » _____ 2013 ж. № _____ хаттама

Кафедра меңгерушісі _____ Көккөз М.М. « ____ » _____ 2013 ж.

Ақпараттық технологиялар факультетінің оқу-әдістемелік кеңесі мақұлдаған
« ____ » _____ 2013 ж. № _____ хаттама

Төраға _____ Мустафина Л.М. « ____ » _____ 2013 ж.

Оқытушы туралы мәлімет және қатынас ақпараты

Аты-жөні Көккөз Махаббат Мейрамқызы Ғ.п.к., доцент

ҚарМТУ (Б.Мира, 56) бас ғимарат, «Ақпараттық технологиялар және қауіпсіздік» кафедрасы, аудитория 429, телефон 56-75-98 қос. 1054.

Пәннің еңбек көлемділігі

Семестр	Кредиттер саны	ECTS	Сабак түрі					СӨЖ сағаттарының саны	Жалпы сағат саны	Бақылау түрі
			Қатынас сабақтарының саны			СОӨЖ сағаттарының саны	Барлық сағат саны			
			дәріс	практикалық сабақтар	зертханалық сабақтар					
7	3	5	15	-	30	45	90	45	135	емтихан

Пән сипаттамасы

«Арнайы пән II» мамандық бойынша бейіндік пәндердің таңдау бойынша компонент циклына кіреді.

Пәннің мақсаты

«Арнайы пән II» мақсаты - теориялық және практикалық әзірлеу қағидаттарын қорғау және WEB-қосымшаларын ескере отырып, қазіргі заманғы үрдістердің негізгі типтері шабуыл web-қосымшалар және олардың алдын-алу әдістерін зерттеу болып табылады.

Пән міндеттері

Пәннің міндеттері мынадай: жоспарлау жүйесінің қауіпсіздігі үшін web-қосымшалар құру; қорғалған web-беттер; кодтау, хэширование және подписывание деректер; web-қосымшалардың қауіпсіздік жүйесін тестілеу

Берілген пәнді оқу нәтижесінде студенттер міндетті: түсінігі болуы тиіс:

- принциптері туралы әзірлеу және оның жұмыс істеуі қазіргі заманғы қауіпсіз web қосымшаларды; бағдарламалық-аппараттық құралдарға талдау және қауіпсіздігін қамтамасыз ету, web-қосымшаларды; білу:
- ақпаратты қорғауды әзірлеу кезіндегі WEB-қосымшаларының түрлері мен тәсілдері;
- жіктелуін негізгі типті шабуылдар web-қосымшалар;
- негізгі әдістері мен құралдары іске асыру қашықтағы желілік шабуылдардағы WEB-қосымшалар;
- ұйымдық-құқықтық және нормативтік қорғау негіздеріндегі интернет технологиясы және WEB-қосымшаларды;
- негіздері жобалау және әзірлеу қорғалған WEB-қосымшаларды; меңгеруі керек:
- дұрыс жобалау және іске асырудың барлық негізгі компоненттеріндегі кешенді

WEB-қосымшалар;

– web-қосымшалардағы анықтау осалдығын;

– жобалау және іске асыру, кешенді қамтамасыз ету жүйесіндегі бір-ақ WEB-қосымшаларды;

– сынай және тестілеу нәтижелері негізінде жасауға негізделген қорғау құралдарын таңдау WEB-қосымшаларды;

дағдысы:

– бағдарламалық іске асырудағы WEB-қосымшалар;

– анықтау және жою осалдықтарын пайдалану арқылы бағдарламалық-аппараттық құралдардың қауіпсіздігін талдауға арналған web қосымшалар.

Пререквизиттер

Бұл пәнді оқу үшін келесі пәндерді игеру қажет: «Компьютерлік ақпаратты қорғау әдістері және құралдары», «Интернет-технологиялар», «Web-бағдарламалау»

Постреквизиттер

«Арнайы пән II» пәнін оқу кезінде алынған білім пәндерін игеру кезінде қолданылады: кезде қорытынды жұмысы (дипломдық жоба).

Пәннің тақырыптық жоспары

Тарау атауы, (тақыптар)	Сабақ түрлері бойынша еңбек көлемділігі, сағ.				
	дәріс	практикалық	зертханалық	СОӨЖ	СӨЖ
1 Web – қосымшалардың қосымшаларына кіріспе: терминология, статистика шабуыл web - ресурстары, жариялылық web-қосымшалардың бір факторы ретінде ерекше назар аударудағы зиянкестердің web - ресурстары.	1			5	1
2 Осалдық Web-қосымшалар. Талдау сәулеті. Сызбалар аутентификациясы. Ақпаратты қорғауды қамтамасыз ету саласындағы стандарттар	3			5	1
3 Клиенттік бөліктің осалдығы. Үлгілік Web-қосымшалардың осалдығы. Қарау кейстер: осалдығын мысалында open source-жобалар.	3			5	2
4 Web-қосымшалар архитектурасы. Үлгілік веб-қосымшалардың осалдығы. Сценарийлерді пайдалану. Қолданылу зиянкес кейін рұқсат алу (бекіту, тарату	3			10	2
5 Желілік деңгейі. Мақсаттары, практика аудит. Статикалық талдау кодын. Жергілікті осалдығын жүйелер.	3			10	2
6 Қорғалған Web-қосымшаларды жобалау. Құпиялылығын қамтамасыз ету. Деректер тұтастығын және жұмыс істеу кездегі Web-	2			10	2

қосымшасы. Web-қосымшаның тестілеу жүйесінің қауіпсіздігі					
7. Web-қосымшасы туралы ақпарат жинау			2		3
8.Транспорттық деңгейдің қорғалуын тестілеу			3		3
9. Қол жеткізуді басқару деңгейдің қорғалуын тестілеу			3		3
10. Басқару сессиялары механизмінің қорғалуын тестілеу			3		3
11. Қызмет көрсетуде шабуылдарға бас тарту тұрақтылығын тексеру			3		3
12. CSRF шабуылдарының осалдығын іздеу			3		4
13. XSS шабуылдарының осалдығын іздеу			3		4
14. SQL-injection шабуылдарының осалдығын іздеу			3		4
15. RCE шабуылдарының осалдығын іздеу			3		4
16. Web-қосымшалардың осалдығын сканерлеу			4		4
БАРЛЫҒЫ:	15		30	45	45

Зертханалық сабақтар тізімі

- 1 Web-қосымшасы туралы ақпарат жинау
- 2 Транспорттық деңгейдің қорғалуын тестілеу
- 3 Қол жеткізуді басқару деңгейдің қорғалуын тестілеу
- 4 Басқару сессиялары механизмінің қорғалуын тестілеу
- 5 Қызмет көрсетуде шабуылдарға бас тарту тұрақтылығын тексеру
- 6 CSRF шабуылдарының осалдығын іздеу
- 7 XSS шабуылдарының осалдығын іздеу
- 8 SQL-injection шабуылдарының осалдығын іздеу
- 9 RCE шабуылдарының осалдығын іздеу
- 10 Web-қосымшалардың осалдығын сканерлеу

СӨЖ-ге арналған бақылау тапсырмаларының тақырыптары

1. Шабуыл «функционалдыру ресістігі». Мысалдар келтіру. Ұсыныстар бойынша беруге барынша азайту тәуекелдер туындаған осы типті шабуылдар.
2. Шабуыл «өрескел күш». Мысалдар келтіру. Әдістері болдырмау шабуыл перебором нақты web-қосымшаларда көрсетілген.
3. Шабуыл «сайтаралық скриптинг ". Мысалдар келтіру. Қорғау тәсілдері.
4. Шабуыл "алып тастау саусақ": әдістері мен утилиттер. Қолданылатын шаралар азайту үшін сәтті осы типті шабуылдар.
5. Шабуыл "буфердің толуы". Себептері, мысалдар.
6. Шабуыл «қызмет көрсетуде бас тарту». Әдістерінің жіктелуі. Қолданылатын шаралар азайту үшін сәтті осы типті шабуылдар.
7. Түсінігі LDAP-репозиториясы (Lightweight Directory Access Protocol),

әдістері шабуыл LDAP. Мысалдар мен тәсілдері мүмкіндігін болдырмау осы типті шабуылдар.

8. Шабуыл "бойынша навигация құралдары және жолдары". Мысалдар мен тәсілдері мүмкіндігін болдырмау осы типті шабуылдар.

9. Шабуыл "SQL-инъекция". Мысалдар мен тәсілдері мүмкіндігін болдырмау осы типті шабуылдар.

10. Шабуыл "XML-инъекция". Мысалдар мен тәсілдері мүмкіндігін болдырмау осы типті шабуылдар

Студенттер білімін бағалау критерийлері

Пән бойынша емтихан бағасы межелік бақылаулар бойынша максимум көрсеткіштер (60%-ға дейін) мен қортынды аттестаттаудың (емтихан) (40%-ға дейін) сомасы ретінде анықталады және кестеге сәйкес 100%-ға дейінгі мәнді құрайды.

Пән бойынша берілген тапсырмаларды орындау мен тапсыру кестесі

Бақылау түрі	Тапсырма мақсаты мен мазмұны	Ұсынылатын әдебиет	Орындау ұзақтығы	Бақылау түрі	Тапсыру мерзімі	Балл
Лекцияларға және СӨЖ ге қатысу	Лекция тақырыптары бойынша білім деңгейін тексеру	Лекцияға конспект және пайдаланылған әдебиеттер	15 келісілген сағат	Ағымдық	Әр аптада	15
№ 1-10 зертханалық жұмыстарын тапсыру	Пән материалдарын меңгеру	Зертханалық жұмыстарды тапсыру	30 келісілген сағат	Ағымдық	2, 4, 6,7, 9,10,11, 12,13,15 апталар да	30
СӨЖ тақырыптарына тапсырам беру	Практикалық білім алу	СӨЖ тақырыптарын а сәйкес	45 келісілген сағат	Ағымдық	Күн сайын	5
Теориялық модуль	Пән материалдарын меңгеруді тексеру	Лекцияға конспект	4 келісілген сағат	Рубеждық	7,14 апталар да	10
Емтихан	Пән материалының игерілуін тексеру	Негізгі және қосымша әдебиет тізімі	2 қатынас сағаттары	Қоры тынды	Сессия кезінде	40
Барлығы						100

Саясат және процедуралар

«Арнайы пән II» пәнін оқу кезінде келесі ережелерді ұстануды сұраймын:

1 Сабаққа кешікпеу.

2 Сабақтан дәлелді себепсіз қалмау, ауырған жағдайда анықтама, ал басқа жағдайларда түсіндірме хат ұсынуды.

3 Сабақтың барлық түрлеріне қатысу студент міндеттерінің қатарына жатады.

4 Оқу процесінің күнтізбелік кестесіне сәйкес барлық бақылау түрін тапсыру.

5 Қатыспаған практикалық және зертханалық сабақтарды оқытушы көрсеткен уақытта өтеу.

Негізгі әдебиет тізімі

1. ИБ открытых систем: Учебник для ВУЗов. В 2-х томах. Том 1 – Угрозы уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская. А.И. Толстой, Д.В. Ушаков. – М.:Горячая линия – Телеком, 2006.

2. Прохода А. Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. -М.: Горячая линия-Телеком, 2007. - 180 с.

3 Лукацкий А. В. Обнаружение атак. СПб.: БХВ-Петербург, 2001. 624 с.

4 Мамаев М., Петренко С. Технология защиты в Интернете. Специальный справочник. СПб.:Питер, 2002. 848 с.

5. Касперски К. Техника сетевых атак. М.: Солон-Р, 2001. 396 с.

Қосымша әдебиет тізімі

6 Форристал Д. и др. Защита от хакеров Web-приложений / Джефф Форристал, Крис Брумс, Дрю Симонис, Брайн Бегнолл, Майкл Дайновиц, Джей Д. Дайсон, Джо Дьюлэй, Майкл Кросс, Эдгар Даниелян, Дэвид Г. Скабру ; Пер. с англ. В. Зорина –М. : Компания АйТи ; ДМК Пресс.,2008 – 496 с

7 Мак-Клар С, Скембрей Д., Курц Д. Секреты хакеров. Безопасность сетей - готовые решения.2-е изд.: Пер. с англ. М.: Изд. дом «Вильямс», 2001. 656 с.

**СТУДЕНТКЕ АРНАЛҒАН ПӘН БОЙЫНША
ОҚЫТУ БАҒДАРЛАМАСЫ (SYLLABUS)**

АР(II) 4312 «Арнайы пән II» пәні

АР 29 «Арнайы пән» модулі

31.03.2004 ж. № 50 мемл. бас. лиц..

Баспаға _____ 20__ ж. қол қойылды. Пішіні 90x60/16. Таралымы _____ дана

Көлемі ___ оқу бас. п.№ _____ тапсырыс Бағасы келісілген