СОӨЖ №2. Веб-қосымшалардағы осалдықтарды анықтау тәсілдерін салыстыру

Жұмыстың мақсаты

Веб-қосымшалардың осалдықтарын анықтауда қолданылатын статикалық, динамикалық және қолмен талдау тәсілдерін салыстыру, XSS, SQL Injection және CSRF сияқты қауіптер үшін олардың қолданылу шекарасын анықтау және семестрлік жобаға сәйкес тексеру стратегиясын негіздеу.

Пәнмен және жеке семестрлік жобамен байланысы

СОӨЖ №2 ПЖ №11–12-дегі веб-қосымшаның кіру нүктелері, XSS, SQL Injection, CSRF және secure coding тақырыптарын біріктіреді. Нәтиже семестрлік жобада веб-қосымша attack surface және қорғаныс бақылауларын бағалау бөлімі ретінде пайдаланылады.

Қысқаша теориялық мәліметтер

Веб-қосымшаның қауіпсіздігін бағалау бір ғана сканермен шектелмейді. Осалдықтар серверлік кодта, клиенттік логикада, конфигурацияда, access control механизмінде немесе деректерді өңдеу тәсілінде пайда болуы мүмкін. Сондықтан тексеру тәсілі зерттелетін компонент пен қауіп түріне сәйкес таңдалады.

Статикалық талдау бағдарламалық кодты немесе оның құрылымын орындатпай зерттеуге бағытталады. Ол қауіпті функцияларды, енгізу деректерінің өңделуін және кейбір secure coding бұзушылықтарын ертерек анықтауға көмектеседі. Бірақ runtime конфигурациясы мен нақты пайдаланушы ағынын толық көрсете алмауы мүмкін.

Динамикалық талдау жұмыс істеп тұрған зертханалық веб-қосымшаның HTTP сұраныстары мен жауаптарын зерттейді. Ол URL parameter, form, API endpoint, cookie және HTTP header сияқты нақты кіру нүктелеріндегі мінез-құлықты бағалауға мүмкіндік береді. Автоматтандырылған DAST құралдары ықтимал белгілерді жылдам таба алады, бірақ false positive нәтижелерді қолмен растау қажет.

Қолмен талдау trust boundary, access control, бизнес-логика және күрделі контекстік мәселелерді зерттеуде маңызды. Автоматтандырылған құрал көрмейтін рөлдер арасындағы құқық айырмашылығы немесе қолданбаның ерекше жұмыс логикасы сараптамалық талдауды қажет етуі мүмкін.

XSS тәуекелі пайдаланушы енгізуінің браузер контекстінде қауіпсіз өңделмеуімен байланысты. Оны бағалауда input flow және output encoding зерттеледі. SQL Injection пайдаланушы дерегінің SQL сұранысының құрылымына араласу тәуекелімен байланысты, сондықтан parameterized query және серверлік өңдеу тәсілі маңызды.

CSRF белсенді сессия контекстін пайдаланушының ниетінсіз сұраныс орындауға қолдану тәуекелімен байланысты. Мұнда anti-CSRF token, SameSite cookie және маңызды операциялардың серверлік тексеруі қарастырылады. Осы үш қауіптің түпкі себептері әртүрлі болғандықтан, бір ғана жалпы сканер немесе фильтр жеткіліксіз.

Салыстыру кезінде coverage, false positive, false negative, evidence сапасы, орындау уақыты, сарапшыға қойылатын талап және CI/CD-ге интеграция мүмкіндігі қарастырылады. Нәтижесінде статикалық, динамикалық және қолмен тексеруді біріктіретін қорғаныстық стратегия ұсынылуы мүмкін.

Әдістемелік нұсқаулар

ПЖ №11-де жасалған веб-қосымшаның attack surface картасын пайдаланып, тексерілетін URL parameter, form, API endpoint, cookie, header және file upload нүктелерін таңдаңыз. Әр нүкте үшін ықтимал осалдық класын белгілеңіз.

Кемінде үш тәсілді салыстырыңыз: статикалық талдау, динамикалық талдау және қолмен тексеру. Әр тәсіл үшін қандай evidence алынатынын, қандай осалдықтарды жақсы анықтайтынын және қандай шектеулер бар екенін көрсетіңіз.

XSS, SQL Injection және CSRF үшін қорғаныс механизмдерін бөлек бағалаңыз. Зертханалық ортада ғана қауіпсіз тексеру жүргізіп, нақты бөгде жүйелерге әсер етпеңіз.

Оқытушымен аралық нәтижені талқылап, семестрлік жобаға арналған web security verification strategy дайындаңыз. Стратегияда қандай тәсіл қай кезеңде және қандай критерий бойынша қолданылатыны көрсетілсін.

Орындау тәртібі

1. Веб-қосымшаның attack surface картасынан негізгі кіру нүктелерін таңдау.
2. Статикалық, динамикалық және қолмен талдау тәсілдерін кемінде 7 критерий бойынша салыстыру.
3. XSS үшін анықтау белгілері мен output encoding бақылауын талдау.
4. SQL Injection үшін енгізу ағыны мен parameterized query қолданылуын бағалау.
5. CSRF үшін token, SameSite және сессиялық контекстті бағалау.
6. Автоматтандырылған finding-тердің false positive ықтималдығын көрсету.
7. Әр тәсілдің coverage және evidence сапасын салыстыру.
8. Семестрлік жоба үшін біріктірілген web security verification strategy ұсыну.

Тапсырмалар

1. Веб-қосымшаның attack surface картасынан негізгі кіру нүктелерін таңдау.
2. Статикалық, динамикалық және қолмен талдау тәсілдерін кемінде 7 критерий бойынша салыстыру.
3. XSS үшін анықтау белгілері мен output encoding бақылауын талдау.
4. SQL Injection үшін енгізу ағыны мен parameterized query қолданылуын бағалау.
5. CSRF үшін token, SameSite және сессиялық контекстті бағалау.
6. Автоматтандырылған finding-тердің false positive ықтималдығын көрсету.
7. Әр тәсілдің coverage және evidence сапасын салыстыру.
8. Семестрлік жоба үшін біріктірілген web security verification strategy ұсыну.

Орындау мысалы

Мысалы, зертханалық веб-қосымшадағы іздеу формасы үшін статикалық талдау деректің кодтағы өңделуін, динамикалық талдау HTTP сұраныс/жауап мінез-құлқын, ал қолмен талдау output encoding және контекстік қауіпсіздікті тексереді. Үш тәсілдің нәтижелері бір кестеде салыстырылып, қайсысы қандай evidence бергені көрсетіледі.

Жеке тапсырма

Әр магистрант өз семестрлік жобасындағы немесе оқытушы берген зертханалық веб-қосымшадағы жеке функцияны таңдайды: авторизация, іздеу, API, профиль өзгерту, файл жүктеу және т.б. Сол функция үшін үш тексеру тәсілін салыстырып, жеке verification strategy әзірлейді.

Нәтижелерді ұсыну формасы

– 5–7 бет аналитикалық есеп
– web attack surface фрагменті
– үш тәсілді салыстыру кестесі
– XSS/SQL Injection/CSRF қорғаныс бақылауларының матрицасы
– evidence мысалдары

– семестрлік жобаға арналған verification strategy

Есепке қойылатын талаптар

Есепте жұмыстың мақсаты, зерттеу сұрағы, пайдаланылған деректердің немесе қауіпсіздік артефактілерінің шығу тегі, талдау әдісі, салыстыру критерийлері, нәтижелер және олардың интерпретациясы берілуі тиіс. Қорытынды әрбір сандық немесе сапалық нәтижемен байланыстырылып, жұмыстың шектеулері көрсетіледі.

Код қолданылған жағдайда random_state немесе seed, split, preprocessing кезеңдері, негізгі параметрлер және бағдарламалық орта тіркеледі. Нәтижені тек кесте немесе метрика түрінде беру жеткіліксіз: магистрант алынған айырмашылықтардың себебін және нәтижені қандай жағдайда жалпылауға болмайтынын түсіндіреді.

Бағалау критерийлері

Критерий	**Үлес салмағы**
Теориялық негіз және терминдерді дұрыс қолдану	15%
Әдіс пен критерийлерді негіздеу	15%
Деректер/артефактілермен жұмыс	20%
Салыстыру және нәтижелерді талдау	20%
Жеке тапсырма және семестрлік жобамен байланыс	20%
Есепті рәсімдеу және дереккөздер	10%

Бақылау сұрақтары

1. Статикалық және динамикалық талдаудың айырмашылығы қандай?
2. Қолмен тексеру қандай жағдайда қажет?
3. DAST нәтижесі неліктен қосымша растауды талап етеді?
4. XSS-тің негізгі түпкі себебі қандай?
5. Output encoding не үшін қолданылады?
6. Parameterized query SQL Injection тәуекелін қалай азайтады?
7. CSRF token қандай міндет атқарады?
8. SameSite cookie қандай рөл атқарады?
9. Coverage пен evidence сапасы қалай ерекшеленеді?
10. Неліктен веб-қосымшаны бағалауда бірнеше тәсілді біріктіру тиімді?

Әдебиеттер тізімі

1. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2024. 72 с.

2. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2018. 45 с.

3. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Издательство Уральского университета, 2019. 204 с.

4. Шаньгин В.Ф. Информационная безопасность: учебное пособие. Москва: ДМК Пресс, 2014. 702 с.

5. Назарян А.К., Карцан И.Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. 2025. Т. 4, № 1. С. 1001–1007.

6. Лукьянец С.Е. Гибридные системы кибербезопасности: искусственный интеллект и анализ сетевого трафика для противодействия современным угрозам.

7. Сигалов Д.А. Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода: диссертация. Москва: МГУ имени М.В. Ломоносова, 2024.

8. Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Кибератаки и методы их предотвращения в информационных системах // Дискуссия. 2024. Вып. 128. С. 120–126.