ӘОЖ 004.056

LARAVEL ЖӘНЕ BOOTSTRAP НЕГІЗІНДЕГІ ВЕБ-ҚОСЫМШАЛАРДЫҢ ҚАУІПСІЗДІГІ: ҚАЗІРГІ ЗАМАНҒЫ ҚАУІПТЕР МЕН ҚОРҒАНЫС ӘДІСТЕРІН ТАЛДАУ

Рашитов Ришат Жұмабекұлы
reesang.dev@gmail.com
«Білім беру жүйесіндегі информатика және АКТ» білім бағдарламасының 3 курс студенті Х.Досмұхамедов атындағы Атырау университеті, Атырау қ, Қазақстан Республикасы Ғылыми жетекшісі, магистр, аға оқытушы – **Жанузакова З.Ж.**

Қазіргі цифрлық әлемде веб-қосымшалардың қауіпсіздігі әзірлеушілер мен пайдаланушылар үшін басымдыққа айналуда. Веб-платформаларға қауіп-қатерлер мен шабуылдардың көбеюімен бағдарламалық жасақтаманы жобалау және әзірлеу кезінде қауіпсіздік басты назарда болуы керек екендігі айқын болады. Бұл тұрғыда Laravel және Bootstrap сияқты құрылымдар мен кітапханалар веб-қосымшаларды тиімді құруды ғана емес, сонымен қатар қауіп-қатерден қорғау құралдарын да қамтамасыз етуде маңызды рөл атқарады. Осы мақалада Laravel шеңбері мен Bootstrap кітапханасын қолдана отырып, веб-қосымшалардың қазіргі заманғы қауіпсіздік қатерлерін және оларды жеңу әдістерін қарастырыңыз. Біз әрбір құралдың қауіпсіздіктегі рөлін бағалаймыз, сонымен қатар веб- қосымшалардың бэкендімен фронтендін барынша қорғау үшін олардың интеграциясын қарастырамыз.

Веб-қосымшалардағы заманауи қауіп-қатерлер

Бүгінгі таңда веб-қосымшалар көптеген қауіп-қатерлерге ұшырайды, олардың ішінде аутентификация және авторизация шабуылдары, сайтаралық сценарий (XSS), сайтаралық сұранысты қолдан жасау (CSRF), SQL инъекциялары және мобильді құрылғылар мен API-ге қатысты қауіптер бар. Аутентификация және авторизация шабуылдары пайдаланушының тіркелгі деректеріне немесе қолданбаның маңызды ресурстарына рұқсатсыз кіру әрекеттерін қамтиды. Сайтаралық сценарий (XSS) сеанс деректерін ұрлау немесе пайдаланушыларды зиянды сайттарға бағыттау мақсатында веб-беттерге зиянды кодты енгізуге бағытталған. Сайтаралық сұранысты қолдан жасау (CSRF) уәкілетті пайдаланушының атынан оның келісімінсіз қажетсіз әрекеттерді орындау болып табылады. SQL инъекциялары шабуылдаушы құпия ақпаратты алу немесе деректерді басқару мақсатында дерекқор сұрауларына зиянды SQL кодын енгізетін шабуылдардың ең көп таралған түрлерінің бірі болып табылады. Сонымен қатар, мобильді құрылғылар мен API қауіпсіздігіне төнетін қатерлер мобильді қосымшалардың дамуымен және API арқылы сыртқы қызметтермен өзара әрекеттесуімен өзекті бола түсуде. Осы және басқа қауіптер веб-қосымшалардың қауіпсіздігін қамтамасыз ету үшін тиісті қорғаныс шараларын мұқият талдауды және әзірлеуді қажет етеді. Аталған веб-қосымшалардың қауіпсіздік қатерлерімен күресу үшін техникалық және ұйымдастырушылық қорғау шараларын қамтитын кешенді тәсілдерді қолдану қажет. Laravel мен Bootstrap кітапханасы веб-қосымшаларды әзірлеу кезінде қауіпсіздік құралдарын ұсынады.

Мысалы, Laravel CSRF және XSS сияқты шабуылдардың көптеген түрлеріне қарсы кіріктірілген қорғаныс механизмдерін қамтиды, сонымен қатар аутентификация мен авторизацияны жүзеге асырудың ыңғайлы құралдарын

ұсынады. Laravel деректер қорымен байланысу үшін Eloquent ORM қолданғандықтан SQL инъекциясынан қорғалған.

Bootstrap, керісінше, XSS және CSRF сияқты көптеген шабуылдардың алдын алуға көмектесетін модальды терезелер мен формалар сияқты қауіпсіздікті қолдайтын компоненттерді ұсынады. Bootstrap дизайн тақырыптары сонымен қатар шабуыл әрекеттері кезінде де мазмұнның дұрыс көрсетілуін және өзара әрекеттесуін қамтамасыз ететін заманауи қауіпсіздік талаптарын ескереді.

Laravel және Bootstrap интеграциясы әзірлеушілерге сервер деңгейінде де, клиент деңгейінде де күшті қауіпсіздік шаралары бар веб-қосымшаларды құруға мүмкіндік береді. Бұл аутентификация және авторизация шабуылдарынан қорғауды, пайдаланушы деректерінің енгізілуін бақылауды, құпия ақпараттың жария етілуіне жол бермеуді және қауіпсіздіктің басқа да көптеген аспектілерін қамтиды.

Веб-қосымшалардың қауіпсіздігін қамтамасыз ету үшін Laravel және Bootstrap пайдалану тек осы құралдардың мүмкіндіктерін білуді және түсінуді ғана емес, сонымен қатар қауіптерді мұқият талдауды, тиісті қорғаныс шараларын жүзеге асыруды қажет етеді. Келесі бөлімдерде біз осы құрылымдар мен кітапханаға қатысты қауіпсіздіктің нақты аспектілерін егжей-тегжейлі қарастырамыз және оларды веб-қосымшаларды әзірлеудің практикалық сценарийлерінде тиімді пайдалану бойынша ұсыныстар береміз.

Laravel негізіндегі веб-қосымшалардың қауіпсіздігін талдау

Laravel ең танымал PHP кітапханасының бірі бола отырып, қауіпсіздік мәселелеріне белсенді назар аударады. Оның қауіпсіздігінің маңызды сәттерінің бірі - веб-қосымшаларға шабуыл жасаудың ең көп таралған түрлерінің бірі болып табылатын CSRF (сайтаралық сұраныс) және XSS (сайтаралық сценарий) шабуылдарынан қорғау. Laravel бұл шабуылдардан қорғанудың ыңғайлы құралдарын ұсынады, мысалы, CSRF таңбалауыштарын құру және тексеру механизмдері және Blade шаблондарын пайдаланып пайдаланушы енгізген деректерін автоматты түрде өңдейді.

Сонымен қатар, Laravel аутентификация мен авторизацияның көптеген мүмкіндіктерін ұсынады, бұл әзірлеушілерге қауіпсіздік тетіктерін өз қосымшаларына оңай енгізуге мүмкіндік береді. Бұған сеанстарды немесе таңбалауыштарды пайдаланатын дайын аутентификация жүйелері, рөлдер мен рұқсаттарға негізделген қол жеткізу механизмдері кіреді.

Laravel негізіндегі веб-қосымшалардың қауіпсіздігінің тағы бір маңызды аспектісі-SQL инъекциясынан қорғау. Eloquent сияқты ORM (object-Relational Mapping) механизмдерін пайдалану арқылы Laravel қолданбаларды SQL сұрауларын дұрыс пайдаланбауға байланысты шабуылдардың көптеген түрлерінен автоматты түрде қорғайды, бұл дерекқорға зиянды кодты енгізу мүмкіндігін болдырмайды.

Дегенмен, веб-қосымшалардың қауіпсіздігі бір реттік оқиға емес, процесс екенін есте ұстаған жөн. Laravel көптеген қауіпсіздік құралдарын ұсынғанымен, оның негізінде қосымшаларды әзірлеу кезінде жақтау жаңартуларын қадағалау, қауіпсіздіктің ең жақсы тәжірибесін қолдану маңызды. Бұған тәуелділікті үнемі жаңарту, осалдықтар үшін кодты мұқият талдау және әзірлеушілерге шабуылдардан қорғаудың заманауи әдістерін үйрету кіреді.

Bootstrap негізіндегі веб-қосымшалардың қауіпсіздігін талдау

Bootstrap ең кең таралған кітапханалардың бірі ретінде веб-қосымшалардың қауіпсіздігін қамтамасыз ететін кейбір құралдарды ұсынады. Алайда, фронтенд кітапханалардан айырмашылығы, оның қауіпсіздікке қосқан үлесі көбінесе шабуылдардың нақты түрлерінен қорғаныс механизмдерімен емес, мазмұнмен

дұрыс дисплей мен өзара әрекеттесуді қамтамасыз етумен байланысты.

Bootstrap қауіпсіз формаларды, модальды терезелерді, навигациялық мәзірлерді және XSS (сайтаралық сценарий) және CSRF (сайтаралық сұраныс) сияқты шабуылдардың алдын алуға көмектесетін басқа интерфейс элементтерін жасауға арналған компоненттерді ұсынады. Мысалы, Bootstrap модальды терезелері фишинг әрекеттерінен немесе пайдаланушыны зиянды веб-ресурстарға бағыттаудан қорғайды.

Дегенмен, осыған қарамастан, Bootstrap негізіндегі веб-қосымшалардың қауіпсіздігі тек кітапханаға ғана емес, сонымен қатар қолданбаның басқа компоненттерімен дұрыс пайдалану мен интеграцияға байланысты екенін есте ұстаған жөн. Әзірлеушілер Bootstrap жаңартуларын қадағалап, қауіпсіз және тұрақты пайдаланушы интерфейстерін жасау үшін оның функционалдығын белсенді пайдалануы керек.

Laravel және Bootstrap қауіпсіздік механизмдерін интеграциялау

Laravel және Bootstrap қауіпсіздік механизмдерін интеграциялау қауіпсіз веб- қосымшаларды құрудың маңызды аспектісін ұсынады. Екі платформаның мүмкіндіктерін біріктіру әзірлеушілерге тиімді және стильді ғана емес, сонымен қатар ықтимал қауіптерден сенімді түрде қорғалған қолданбаларды жасауға мүмкіндік береді.

Біріншіден, Laravel-де жасалған веб-қосымшалар бэкенд деңгейдегі шабуылдардың алдын алу үшін CSRF және XSS-тен қорғаныс сияқты фронтендтің қауіпсіздік тетіктерін қолдана алады. Bootstrap көмегімен жасалған қолданбаның фронтенді пайдаланушы деректерін дұрыс көрсету және зиянды JavaScript кодының орындалуын болдырмау сияқты қауіпсіздік нұсқауларын ескере отырып реттелуі мүмкін.

Екіншіден, Laravel аутентификация және авторизация механизмдерін Bootstrap пайдаланушы интерфейстерімен бөлісу пайдаланушы деректері мен ресурстарының қауіпсіздігін қамтамасыз ету үшін бэкендіде фронтендіде өзара әрекеттесетін қауіпсіз кіру және кіруді басқару жүйелерін құруға мүмкіндік береді.

Laravel және Bootstrap қауіпсіздік механизмдерін интеграциялау мұқият жоспарлау мен әзірлеуді қажет етеді, бірақ нәтижесінде жоғары функционалдылық пен тартымды дизайнды сенімділік пен қауіпсіздікпен біріктіретін қуатты және қауіпсіз веб-қосымшалар пайда болуы мүмкін.

Практикада іске асырудың мысалдары

Laravel және Bootstrap қауіпсіздік механизмдерін біріктіруді практикалық іске асырудың мысалдары әртүрлі және келесі аспектілерді қамтиды:

1. Қауіпсіз формаларды әзірлеу: Bootstrap форма компоненттерін пайдалана отырып, пайдаланушы деректерін енгізу үшін формалар жасау және Laravel кірістірілген валидация құралдары арқылы осы деректерді сервер жағында тексеру және валидациялау. Бұл тәсіл SQL инъекциясы немесе XSS сияқты пайдаланушы деректерін дұрыс енгізбеуге байланысты шабуылдардан қорғауды қамтамасыз етеді.

2. Сессия шабуылдарынан қорғау және аутентификация: қолданбаға қауіпсіз кіру жүйесін құру үшін Laravel интеграцияланған аутентификация және авторизация құралдарын пайдалану. Бұған сеанстарды бақылау, CSRF таңбалауыштарын жасау және тексеру, құпия сөздерді шифрланған түрде сақтау және Laravel қамтамасыз ететін басқа қауіпсіздік шаралары кіреді.

3. Қателерін өңдеу: кіруге тыйым салу туралы ақпарат беттері, 404 және 500 қате беттері және формаларды тексеру қателері туралы хабарлар

сияқты пайдаланушылар үшін қауіпсіздік қателерін өңдеу және көрсету механизмдерін іске асыру. Bootstrap стильдерін пайдалану осы беттер мен жазбалар үшін таза және ақпараттандыратын пайдаланушы интерфейсін жасауға мүмкіндік береді.

4. Қауіпсіздік мониторингі және оқиғаларды журналдау: Laravel құралдары мен үшінші тарап қызметтерін пайдалана отырып, қолданбаға қауіпсіздік мониторингі және оқиғаларды журналдау механизмдерін енгізу. Бұған пайдаланушы кірулерін тіркеу, сәтсіз кіру әрекеттерін бақылау, құпия ресурстарға қол жеткізуді бақылау және ықтимал қауіпсіздік қатерлерін анықтау және оларға жауап беру үшін басқа шаралар кіруі мүмкін. Мұндай практикалық енгізулер Laravel және Bootstrap негізіндегі веб-қосымшаларды тиімді қорғауды қамтамасыз етеді, бұл пайдаланушыларға қолданбамен қауіпсіз және сенімді өзара әрекеттесуді қамтамасыз етеді.

Қорытынды.

Қорытындылай келе, Laravel және Bootstrap арасындағы қауіпсіздік механизмдерін интеграциялау қауіпсіз веб-қосымшаларды құрудың тиімді әдісін ұсынады. Екі құрылым да аутентификация мен авторизациядан бастап интерфейс деңгейіндегі шабуылдардан қорғауға дейін әртүрлі деңгейлерде қауіпсіздікті қамтамасыз ету үшін құралдар мен мүмкіндіктердің кең ауқымын ұсынады.

Бұл тәсіл әзірлеушілерге функционалды және эстетикалық қосымшаларды құруға ғана емес, сонымен қатар оларды заманауи қауіпсіздік қатерлерінен сенімді түрде қорғауға мүмкіндік береді. Laravel және Bootstrap арасындағы қауіпсіздік механизмдерінің дұрыс интеграциясы сервер жағында да, клиент жағында да қауіпсіздік талаптарын сәтті қанағаттандыра алатын тұрақты және сенімді веб-қосымшаларды құруға ықпал етеді.

Жоғарыда аталған барлық аспектілер Laravel мен Bootstrap арасындағы қауіпсіздік өзара әрекеттесуі веб-дамудың маңызды бағыты екенін көрсетеді. Ең жақсы тәжірибелерді қолдану және екі платформаның мүмкіндіктерін мұқият қолдану арқылы әзірлеушілер қауіпсіздіктің жоғары стандарттарына жауап беріп қана қоймай, сонымен қатар ыңғайлы UI/UX ұсынатын веб-қосымшалар жасай алады.

Қолданылған әдебиеттер тізімі:

1. Мэтт С. Laravel. Полное руководство. 2-е издание. – Питер, 2023, 512 с.
2. Основы безопасности веб-приложений. https://searchengines.guru/ru/forum/123522
3. Laravel кітапханасының ресми құжаттамасы. https://laravel.com/docs/10.x/