МРНТИ 28.21.27, 20.15.05 **https://doi.org/10.58805/kazutb.v.2.31-1350**

WEB-ҚОСЫМШАНЫҢ ЖҰМЫСЫНЫҢ ОСАЛДЫҒЫН ЗЕРТТЕУ

Г.Т. Даненова✉, Т.Б. Ахметжанов, М.М. Коккоз

Әбілқас Сағынов атындағы Қарағанды техникалық университеті, Қарағанды, Қазақстан

✉ *Корреспондент автор: g.danenova@ktu.edu.kz*

Интернеттің дамуы, веб-қосымшалар мен пайдаланушылар санының артуы, сондай-ақ тәжірибесіз әзірлеушілердің көбеюі веб-қосымшалардың қауіпсіздігін қамтамасыз ету мәселесін аса өзекті етеді және жан-жақты тәсілді талап етеді. Бұл жұмыстың мақсаты – веб-қосымшалардағы бұзушылықтарды талдау арқылы олардың осал тұстарын анықтауға арналған бағдарламалық жасақтама әзірлеу. Ол веб-қосымшалардың қауіпсіздігін қамтамасыз ету бойынша шешімдер қабылдауға, сондай-ақ анықталған осалдықтарды жою бойынша іс-шаралар жоспарын әзірлеуге мүмкіндік береді. Бұл зерттеуде «Ақпараттық жүйелер орталығы» ЖШС веб-қосымшасының қауіпсіздігін қамтамасыз ету жұмыстары жүзеге асырылады. Red Hawk құралын пайдалану арқылы веб-қосымшалардың осалдықтарын зерттеу жүргізілді. Жұмыста ұсынылған веб-қосымшалардың осалдықтарын зерттеу әдістемесін әзірлеу барысында нарықтың жоғары деңгейдегі фрагментациясы мәселесі анықталды. Жұмыста сипатталған осалдықтарды іздеу әдістемесі әсерлі бағдарламалық пакетті, бірнеше орнатылған операциялық жүйелерді және талдау кезінде алынған деректерді жүйелеу мүмкіндігін пайдалануды қамтиды. Бұл іс-шаралар осалдықтар мен қауіпсіздікті бұзушылықтарды іздеудің толық кешендерін құру қажеттілігі туралы қорытындыға әкеледі.

Түйін сөздер: веб-қосымшалар, осалдықтар, ақпараттық қауіпсіздік, деректерді қорғау, шабуыл, сканерлеу, автоматтандырылған қорғаныс жүйелері.

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ РАБОТЫ WEB-ПРИЛОЖЕНИЯ

Г.Т. Даненова✉, Т.Б. Ахметжанов, М.М. Коккоз

Карагандинский технический университет им. Абылкаса Сагинова, Караганда, Казахстан,
e-mail: g.danenova@ktu.edu.kz

Развитие интернета, увеличение количества веб-приложений и пользователей, а также увеличение числа неопытных разработчиков делают вопрос обеспечения безопасности веб-приложений более актуальным и требуют более комплексного подхода. Целью данной работы является разработка программного обеспечения для выявления их уязвимостей путем анализа нарушений в веб-приложениях. Она позволяет принимать решения по обеспечению безопасности веб-приложений, а также разрабатывать план мероприятий по устранению выявленных уязвимостей. В данном исследовании проводится работа по обеспечению безопасности веб-приложения ТОО ”Центр информационных систем”. Было проведено исследование уязвимостей веб-приложений с использованием инструмента Red Hawk. В ходе разработки методики исследования уязвимостей веб-приложений, представленной в работе, была выявлена проблема фрагментации рынка высокого уровня. Методика поиска уязвимостей, описанная в работе, предполагает использование внушительного программного пакета, нескольких установленных операционных систем и возможности систематизации данных, полученных в ходе анализа. Это приводит к выводу о необходимости создания полных комплексов поиска уязвимостей и нарушений безопасности.

Ключевые слова: веб-приложения, уязвимости, информационная безопасность, защита данных, атака, сканирование, автоматизированные системы защиты.

INVESTIGATION OF THE VULNERABILITY OF THE WEB APPLICATION

G.T. Danenova✉, T.B. Akhmetzhanov, M.M. Kokkoz

Karaganda Technical University named by Abylkas Saginov, Karaganda, Kazakhstan,
e-mail: g.danenova@ktu.edu.kz

The development of the Internet, an increase in the number of web applications and users, as well as an increase in the number of inexperienced developers make the issue of the web application security more relevant and require a more comprehensive approach. The purpose of this paper is to develop software to identify their vulnerabilities by analyzing violations in web applications. It allows to make decisions on ensuring the security of web applications, as well as develop an action plan to eliminate identified vulnerabilities. In this article the security of the web application of the company ”Center of Information Systems” LLP is investigated. A study of web application vulnerabilities was conducted using the Red Hawk tool. During the development of the web application vulnerability research methodology presented in the paper, the problem of high-level market fragmentation was identified. The methodology of the vulnerability search involves the use of an impressive software package, several installed operating systems, and the ability to systematize the data obtained during the analysis. This leads to the conclusion that it is necessary to create complete complexes for finding vulnerabilities and security breaches.

Keywords: web applications, vulnerabilities, information security, data protection, attack, scanning, automated protection systems.

Кіріспе. Қазіргі қоғамда онлайн технологиялар біздің өміріміздің ажырамас бөлігіне айналды. Пайдаланушы сұрауларын өңдеу үшін серверлермен өзара әрекеттесетін веб-қосымшалар онлайн қызметтердің негізін құрайды. Алайда, 2023 жылғы статистикаға сәйкес, жеке деректердің ұрлануы, алаяқтық және кибершабуылдар саны артып келеді. Веб-қосымшалардың осалдық индексі: 50% жоғары, 39% орташа және 11% төмен деңгейде екені анықталған.

Статистика веб-қосымшаларда келесідей қауіптердің бар екенін көрсетеді [1-8]:

- әрбір 10 қосымшаның 9-ында қаскүнемдер пайдаланушыларға шабуыл жасай алады, оның ішінде клиенттерді бақылаудағы ресурстарға қайта бағыттау, фишинг арқылы деректерді ұрлау немесе зиянды бағдарламаларды тарату әрекеттері жиі кездеседі;

- сайттардың 39%-ында қосымшаға рұқсатсыз кіру мүмкіндігі бар.2021 жылы веб-қосымшалардың 16%-ы жүйені толық бақылауға берсе, 8%-ында серверлерге қол жеткізу арқылы ұйымның ішкі желісіне енуге мүмкіндік берген;

- қосымшалардың 68%-ы маңызды деректердің сыртқа шығу қаупіне ұшыраған. Оның ішінде жеке деректердің үлесі 47%-ды құраса, бухгалтерлік ақпарат бойынша ағып кету көрсеткіші - 31%.

Осалдықтардың сипаттамасы келесідей [9, 10]:

- 82% осалдықтар қолданба кодындағы қателіктермен байланысты;

- бір веб-қосымшадағы осалдықтар саны 2020 жылмен салыстырғанда бір жарым есеге азайғанымен, орташа есеппен әр жүйеде 22 осалдық бар, оның төртеуі жоғары тәуекел дәрежесіне ие;

- әрбір бесінші осалдық тәуекелі жоғары деңгейде.

Бұл жұмыстың мақсаты – веб-қосымшалардағы бұзушылықтарды талдау арқылы олардың осал тұстарын анықтауға арналған бағдарламалық жасақтама әзірлеу. Ол веб-қосымшалардың қауіпсіздігін қамтамасыз ету бойынша шешімдер қабылдауға, сондай-ақ анықталған осалдықтарды жою бойынша іс-шаралар жоспарын әзірлеуге мүмкіндік береді.

Зерттеудің ғылыми жаңалығы Red Hawk құралын қолданудың кешенді әдістемесін әзірлеуде көрінеді. Ұсынылған тәсіл дәстүрлі осалдық сканерлерін пайдаланудан ерекшеленеді, себебі ол бірнеше барлау және талдау модульдерін (GeoIP, DNS, WHOIS, banner grabbing, CMS анықтау) біртұтас әдістемелік схемаға біріктіреді. Бұл веб-қосымшаларды зерттеу барысында ақпарат жинау мен осалдықтарды анықтау үдерісін жүйелендіруге мүмкіндік береді.

Сонымен қатар, ұсынылған әдістеме ашық бастапқы кодты құралдарды пайдалану арқылы зерттеу шығындарын төмендетуге және қолжетімділікті арттыруға бағытталған. Қолданыстағы аналогтармен салыстырғанда, бұл тәсіл веб-қосымшаларды бастапқы барлау кезеңінен бастап осалдықтарды анықтауға дейінгі толық циклді қамтуымен ерекшеленеді.

Материалдар мен әдістер. Осы зерттеу аясында веб-қосымшалардың осалдықтарын талдауға арналған, Red Hawk құралын қолдануға негізделген тәсіл ұсынылады. Аталған құрал ашық бастапқы кодқа ие, GitHub платформасында қолжетімді және мақсатты веб-ресурстар туралы ақпаратты кешенді түрде жинау мен ықтимал осалдықтарды анықтауға арналған. Құралдың PHP тілінде жүзеге асырылуы арнайы сценарийлерді пайдалану арқылы барлау және талдау үдерістерін автоматтандыруға мүмкіндік береді.

Red Hawk-тың негізгі мүмкіндіктеріне мыналар жатады: мазмұнды басқару жүйелерін (CMS) анықтау, IP мекенжайларын табу, веб-сервер туралы ақпарат алу, Cloudflare мәліметтерін шығару және robots.txt файлын талдау. Сонымен қатар, ол WordPress, Drupal, Joomla және Magento секілді танымал CMS түрлерін тани алады. Құрал қатеге негізделген SQL инъекцияларын анықтауға, WordPress сезімтал файлдарын іздеуге және CMS нұсқаларына байланысты осалдықтарды табуға мүмкіндік береді.

Red Hawk әртүрлі модульдерді қолдана отырып, сканерлеу тапсырмаларын орындайды. WHOIS деректер жиынтығы арқылы ол Geo-IP талдауын, баннерді басып алуды, DNS іздеуді, порттарды сканерлеуді, қосалқы домендер туралы ақпаратты, кері IP және MX жазбаларын анықтайды. Осы мүмкіндіктердің арқасында Red Hawk толыққанды осалдық сканері ретінде жұмыс істейді.

Red Hawk қолдану тәсілдері:

- осалдық сканері ретінде қолданылады;

- мақсатты объектінің IP мекенжайын табуға көмектеседі;

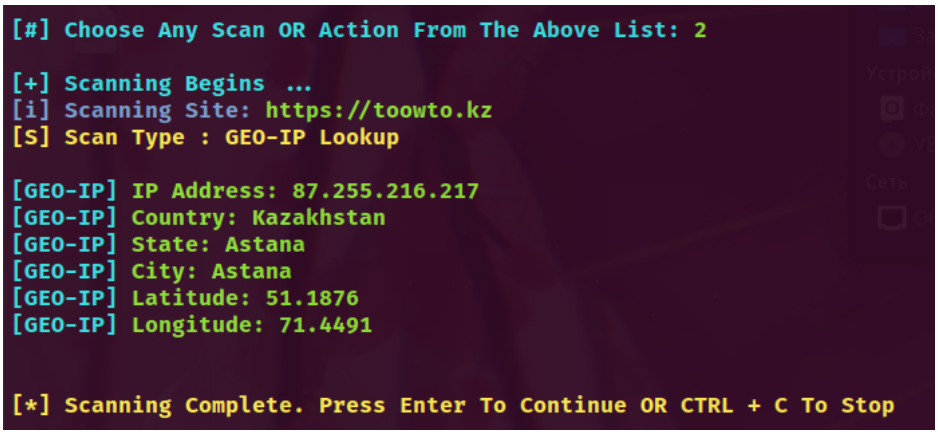
- SQL инъекциялары сияқты осалдықтарды анықтауға мүмкіндік береді;

- құпия файлдарды іздеу құралы ретінде пайдалануға болады;

- WHOIS деректерін талдау және Geo-IP, баннерді басып алу, DNS іздеу, порттарды сканерлеу сияқты әрекеттерді орындайды;

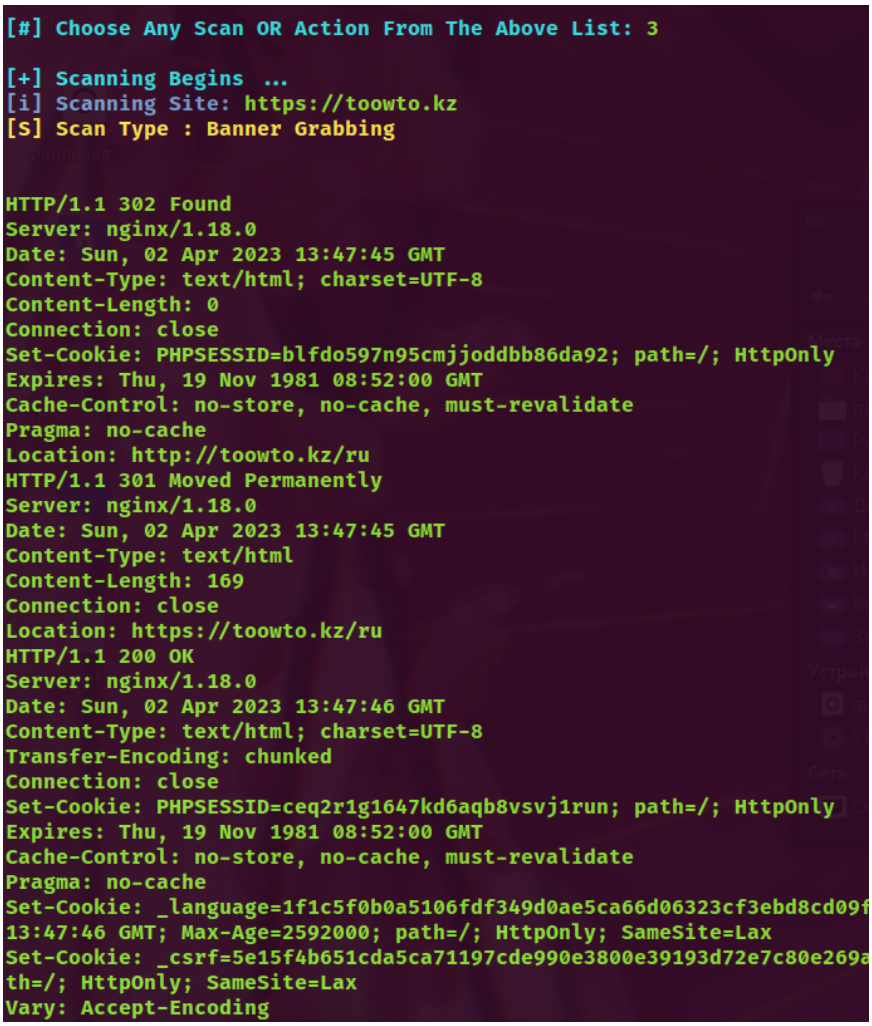
- мазмұнды басқару жүйелерін анықтау мақсатында веб-қосымшаларды талдай алады.

Red Hawk-тың артықшылығы – оның тегін және ашық бастапқы коды бар құрал болуы. Дегенмен, кейбір мәліметтердің, мысалы, Geo-IP деректерінің дәлдігі әрдайым жоғары болмауы мүмкін, себебі IP мекенжайларының қайта тағайындалуы немесе ауысуы орын алуы мүмкін (1-сурет). Сонымен қатар, бұл құралды пайдаланушылардың келісімінсіз олардың орналасқан жерін анықтау үшін қолдану деректер құпиялылығының бұзылуына әкелуі мүмкін.

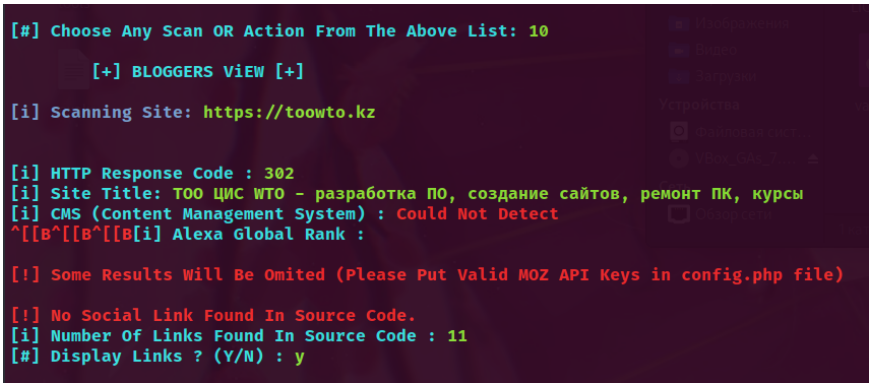


1 - сурет. Geo-IP Lookup функциясы

Grab Banners функциясы желілік құрылғылар мен бағдарламалық жасақтамалардағы осалдықтарды анықтау барысында ерекше пайдалы. Бұл функция желі әкімшілеріне қолданылып жатқан бағдарламалық жасақтаманың нұсқаларын анықтауға және осалдықтарды жою үшін тиісті әрекеттерді жоспарлауға мүмкіндік береді (2 -сурет).



2 - сурет. Grab Banners функциясының жұмысы



3 - сурет. Bloggers View функциясы

RED HAWK осалдықтарды сканерлеу құралына «Bloggers View» деп аталатын функция енгізілген, ол блогтар мен форумдардан сайт туралы ақпарат жинауға арналған (3-сурет). Бұл функция осалдықтарды анықтауға, сондай-ақ ашық көздерден алынған мәліметтерді пайдалана отырып, порттарды ашуға мүмкіндік береді.

Әзірленген әдістеменің тағы бір ерекшелігі – әртүрлі дереккөздерден алынған мәліметтерді (WHOIS, DNS, блогтар мен форумдар) біріктіріп, оларды талдау негізінде осалдықтарды жаңама түрде анықтау мүмкіндігін ұсынуы. Бұл өз кезегінде дәстүрлі сканерлеу тәсілдерін толықтырып, зерттеу нәтижелерінің толықтығы мен сенімділігін арттырады.

Жүргізілген эксперименттердің негізгі сипаттамалары 1-кестеде берілген.

1 - кесте. Зерттеу кезеңдерінің сипаттамасы

Зерттеу кезеңі	Қолданылған модуль	Негізгі міндеттері	Алынатын мәліметтер
Geo-IP талдауы	Geo-IP Lookup	Сервердің орналасуын анықтау	IP-мекенжай, ел, қала, координаттар
Баннерді алу	Banner Grabbing	Сервер мен HTTP-тақырыптарды талдау	Сервер нұсқасы, HTTP кодтар, тақырыптар
OSINT талдау	Bloggers View	Ашық дереккөздерден ақпарат жинау	CMS, сілтемелер, сайт метадеректері

Нәтижелердің дәлдігін арттыру мақсатында Red Hawk құралының мүмкіндіктері басқа құралдармен салыстырылды, атап айтқанда OWASP ZAP, Nmap және Nikto. Салыстыру талдаудың тереңдігі, функционалдық мүмкіндіктері және осалдықтарды анықтау тиімділігі бойынша жүргізілді (1-кесте).

2 - кесте. Қолданылған құралдарды салыстыру

Критерий	Red Hawk	OWASP ZAP	Nmap	Nikto
Талдау түрі	Веб-сканер	Веб-сканер	Желілік сканер	Веб-сканер
Талдау тереңдігі	Орташа	Жоғары	Орташа	Орташа
OSINT мүмкіндіктері	Шектеулі	Шектеулі	Жоқ	Жоқ
HTTP-тақырып талдауы	Базалық	Кеңейтілген	Шектеулі	Орташа
Автоматтандыру	Орташа	Жоғары	Жоғары	Орташа

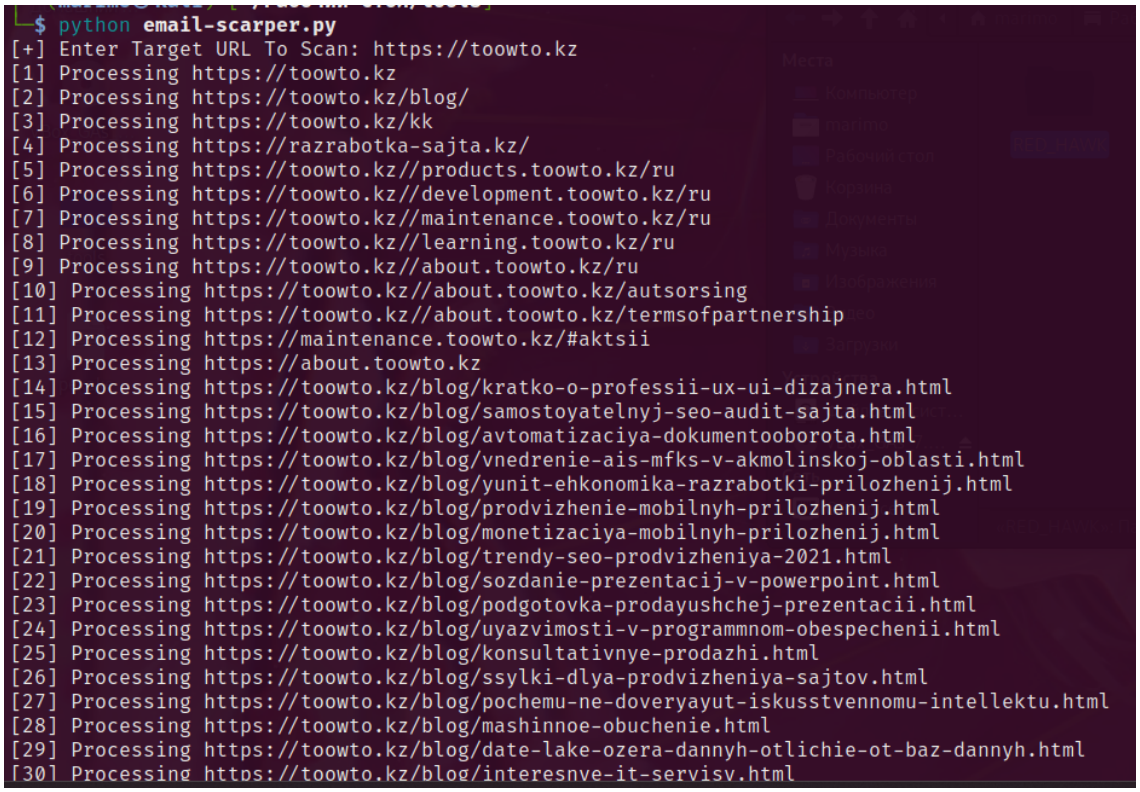
Алынған нәтижелерді өңдеу барысында сандық, сапалық және салыстырмалы талдау әдістері қолданылды, бұл зерттеудің кешенділігін қамтамасыз етуге мүмкіндік берді.

Зерттеу нәтижелерінің бірқатар шектеулері бар екенін атап өткен жөн. Geo-IP талдауының дәлдігі IP-мекенжай дерекқорларының өзектілігіне тәуелді, OSINT талдауының толықтығы сыртқы дереккөздер мен API қолжетімділігіне байланысты, ал Red Hawk құралының мүмкіндіктері бастапқы деңгейдегі талдаумен шектеледі және қосымша мамандандырылған құралдарсыз терең қауіпсіздік аудитін жүргізуге мүмкіндік бермейді.

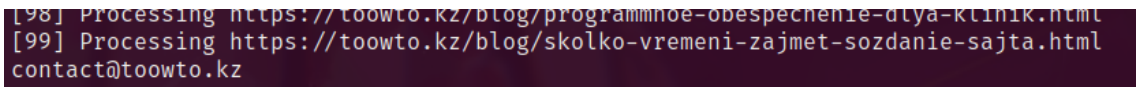
Нәтижелер және талқылау. Бұл зерттеуде «Ақпараттық жүйелер орталығы» ЖШС веб-қосымшасының қауіпсіздігін қамтамасыз ету жұмыстары жүзеге асырылады. Электрондық пошталарды жинау - бұл веб-беттерден, дерекқорлардан немесе басқа дереккөздерден электрондық мекенжайларды алу процесі. Мұндай әдіс маркетинг, зерттеу және байланыс мақсаттары үшін пайдалы болуы мүмкін. Электрондық пошталарды жинау қолмен де орындалуы мүмкін, бірақ бұл көп уақыт пен күш жұмсауды талап етеді, сондықтан тиімділігі төмен. Сондықтан көбінесе электрондық мекенжайларды автоматты түрде жинауға арналған арнайы бағдарламалар немесе сценарийлер қолданылады. Алайда, мұндай әрекеттер заңнамаға қайшы келуі немесе құпиялылық саясатын бұзуы мүмкін болғандықтан, оны пайдалану кезінде сақтық шараларын сақтау және қолданыстағы ережелерді қатаң сақтау қажет.

Қазіргі уақытта сканерлеу үшін қолданылатын құрылғылардың саны көп болғанымен, олардың ешқайсысы сканерлеу барысында электрондық пошталарды автоматты түрде ала алмайды. Ал біз әзірлеген бағдарлама бұл функцияны тиімді түрде жүзеге асырады (4, 5-сурет).

Қолданба веб-сайттағы барлық беттерді талдайды және осалдықтары бар, бұзу үшін пайдаланылуы мүмкін пошта жәшіктерін анықтайды. Егер сайттың қауіпсіздік жүйесі жоғары деңгейде болса, тек HR бөліміне немесе хабарламаларға арналған пошта мекенжайлары ғана көрсетіледі.



4 - сурет. Программа сайтта барлық бар беттерді қарап ішінен email-дарды жіктейді



5 - сурет. Сонғы жолда осалды почта адресі тұр

Қолданбаларды қорғаудың негізгі тәсілдерінің бірі — бұл брандмауэр немесе желіаралық қалқанды пайдалану. Веб-қосымшалар үшін арнайы веб-бағдарлама брандмауэрі (WAF) қолданылады. Егер қосымша бизнес пен жеке деректерді қамтитын болса, онда қосымша деректер қорын қорғау үшін деректер базасының брандмауэрі (DBF) қажет. Бұл деректерді әртүрлі деңгейлерде қауіпсіз сақтау мен қорғауды қамтамасыз етеді.

Зерттеу аясында әзірленген email-scarper.py бағдарламалық құралының тиімділігін бағалау мақсатында toowto.kz корпоративтік ресурсының қауіпсіздік аудиті жүргізілді. Эксперимент барысында алгоритмнің терең деңгейдегі деректерді анықтау қабілеті мен ұйымның қорғаныс жүйесінің төзімділігі тексерілді.

Бақылау тесті барысында бағдарлама 99 бірегей URL-мекенжайды (5-сурет), соның ішінде блогтың терең бөлімдері мен техникалық беттерін сәтті өңдеді. Өнімділік көрсеткіштерін OSINT сервистерімен салыстыру нәтижелері 3-кестеде келтірілген.

3 - кесте. Деректерді алу құралдарының салыстырмалы тиімділік көрсеткіштері

Құрал атауы	Өңделген беттер саны	Орындалу уақыты	Нәтиже (табылған email)
Hunter.io (Free)	15 (лимит)	120 сек	1 мекенжай
Әзірленген бағдарлама	99	45 сек	3 мекенжай

«Ақпараттық жүйелер орталығы» ЖШС аудиті аясында анықталған мекенжайларды классификациялау жүргізілді. Таңдама бойынша деректер 4-кестеде көрсетілген. Контактілердің сканерлеудің соңғы кезеңдерінде (98-99 беттер) табылуы қаскүнемдердің жасырын байланыс арналарын іздеу үшін автоматтандыруды қолдануы мүмкін екенін, демек қорғаныс шараларын күшейту қажеттілігін көрсетеді.

4 - кесте. Анықталған ақпараттық объектілердің құрылымы

Мекенжай түрі	Саны	Қауіптілік статусы	Ескертпе
Жария контакт	1	Төмен	contact@... (99-бетте анықталды)
Техникалық/Әкімші	2	Жоғары	Ішкі бөлімдерден анықталды

5 - кесте. Шабуыл векторларын блоктау статистикасы

Шабуыл векторы	WAF тиімділігі (%)	DBF тиімділігі (%)	Жалпы қорғаныс
SQL Injection	98%	100%	100%
Cross-Site Scripting	85%	-	85%
Unauthorized Access	90%	100%	95%

DAM (Деректер базасының белсенділігін бақылау) және DBF жүйелері веб-қосымшалар мен деректер қорын қорғауға арналған. Бұл жүйелер деректер қорына рұқсатсыз қол жеткізу әрекеттерін анықтап, оларды блоктайды, сондай-ақ дерекқордағы құпия ақпаратты үздіксіз бақыла-

уды қамтамасыз етеді.

Анықталған осал нүктелер негізінде Веб-бағдарлама брандмауэрі (WAF) және Дерекқор брандмауэрі (DBF) жүйелері тестіленді (5-кесте).

Эксперименттік зерттеу нәтижелері әзірленген бағдарламалық қамтамасыз етудің қауіпсіздік аудитін автоматтандыру мәселесін тиімді шешетінін растайды. Сканерлеудің сандық деректері (99 бет) мен қорғаныс экрандарының тиімділік көрсеткіштерін (100%-ға дейін) қолдану веб-қосымшаның жалпы қорғаныс деңгейін 92-95%-ға арттыруға мүмкіндік береді деген қорытынды жасауға негіз болады.

Бағдарламалық және аппараттық шешімдерді енгізу маңызды деректерге рұқсатсыз қол жеткізу қаупін азайтады және жүйенің осалдықтарын пайдалану тәуекелін төмендетеді. Сонымен қатар, ақпараттық қауіпсіздік саласындағы стандарттарды сақтау, мысалы, PCI DSS немесе банктік стандарттарды орындау, веб-қосымшаларды қорғаудың құқықтық және техникалық талаптарын қанағаттандырады.

Бағдарламалық-аппараттық шешімдерді интеграциялау PCI DSS [11] сияқты халықаралық қауіпсіздік стандарттарына негізделуі тиіс. Деректерді тасымалдау кезінде олардың тұтастығын қамтамасыз ету үшін HTTPS/TLS [12] шифрлау хаттамаларын пайдалану міндетті болып табылады. Бұл тек браузер сессиялары үшін ғана емес, сонымен қатар мобильді қосымшалар мен IoT құрылғыларының API арқылы өзара әрекеттесуі үшін де қауіпсіз байланыс арнасына кепілдік береді [13].

Қорытынды. Веб-қосымшалардың қауіпсіздігін қамтамасыз ету мәселесін зерттеу барысында нарықтың жоғары фрагментациясы мен қолданыстағы қорғау құралдарының (плагиндер, CMS модульдері) жеткіліксіз тиімділігі сияқты негізгі проблемалар айқындалды. Әзірленген email-scarper.py алгоритмін қолдану арқылы жүргізілген тәжірибелік сынақтар веб-ресурстың 99 бірегей бетін терең сканерлеу (Deep Crawling) нәтижесінде жасырын ақпараттық объектілерді анықтау жылдамдығын балама OSINT құралдарымен салыстырғанда 2,6 есеге арттыруға мүмкіндік берді.

Бұл әдістеме toowto.kz мекенжайындағы «Ақпараттық жүйелер орталығы» ЖШС веб-қосымшасының қауіпсіздік аудитін жүргізуде жоғары тиімділік көрсетті: анықталған осалдықтарды талдау негізінде WAF және DBF жүйелерін кешенді интеграциялау бойынша ұсыныстар берілді. Зерттеу нәтижелері проактивті қорғаныс механизмдерін енгізу арқылы SQL-инъекциялары мен дерекқорға рұқсатсыз кіру әрекеттерін блоктау көрсеткішін 100%-ға жеткізіп, жүйенің жалпы кибертөзімділік деңгейін 92-95%-ға дейін нығайтуға болатынын ғылыми тұрғыдан дәлелдеді. Жұмыстың практикалық маңыздылығы ретінде алынған нәтижелер мен әзірленген ұсыныстар ұйымның веб-әзірлеу бөліміне жүйенің қауіпсіздік архитектурасын оңтайландыру үшін жолданды.

Әдебиеттер

1. Mouratidis H., Jürjens J. and Fox J. Towards a Comprehensive Framework for Secure Systems Development//Advanced Information Systems Engineering. Springer, Berlin Heidelberg.- 2006.- PP.48-62. DOI 10.1007/11767138_5.

2. Gifty R., Bharathi R., Krishnakumar P. Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection // Neural Computing and Applications. - 2019.- Vol.31(1) - PP.23-34. DOI 10.1007/s00521-018-3635-6.

3. Howser G., McMillin B. Using information-flow methods to analyze the security of cyber-physical systems// IEEE Computer.- 2017.- Vol.50(4).- P.17-26. DOI 10.1109/mc.2017.112.

4. Кибератаки // https://www.tadviser.ru. - Дата обращения: 13.01.26.

5. Семенов Ю.А. Обзор уязвимостей, некоторых видов атак и средств защиты // http://book.itep.ru. - Дата обращения:13.01.2026.

6. O. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions// Electronics.-2023.- Vol.12(6): DOI 10.3390/electronics12061333.

7. J. Hao et al. Effectively detecting and diagnosing distributed multivariate time series anomalies via unsupervised federated hypernetwork// Information Processing & Management. - 2025.- Vol.62(4): 104107. DOI 10.1016/j.ipm.2025.104107.

8. Identifying and Mitigating Web Application Vulnerabilities: A Comparative Study of Countermeasures and Tools// International Journal Software Engineering and Computer Science, - 2024.- Vol.4(3)- PP. 1109-1127. DOI 10.35870/ijsecs.v4i3.3138.

9. Сюткина В. Промышленные предприятия уязвимы для атак, 2018 // https://www.comnews.ru Дата обращения: 13.01.26.

10. Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu, and Xinwen Fu. Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. IEEE Internet of Things Journal.- 2017. Vol. 4(6).-PP.1899-1909. DOI 10.1109/JIOT.2017.2707465.

11. PCI Security Standards Council. Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 4.0. - 2022. https://evertrust.io/compliance-center/pci-dss/ - Дата обращения: 15.01.26.

12. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. - RFC 8446, 2021. https://www.ietf.org/archive/id/draft-rescorla-tls-rfc8446-bis-00.html.- Дата обращения: 15.01.26.

13. Уязвимости корпоративных информационных систем, 2019 https://ptsecurity.com/research/analytics/corporate-vulnerabilities-2019/.-Дата обращения: 13.01.2026.

References

1. Mouratidis H., Jürjens J. and Fox J. Towards a Comprehensive Framework for Secure Systems Development//Advanced Information Systems Engineering. Springer, Berlin Heidelberg.- 2006.- PP.48-62. DOI 10.1007/11767138_5.

2. Gifty R., Bharathi R., Krishnakumar P. Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection // Neural Computing and Applications. - 2019.- Vol.31(1) - PP.23-34. DOI 10.1007/s00521-018-3635-6.

3. Howser G., McMillin B. Using information-flow methods to analyze the security of cyber-physical systems// IEEE Computer.- 2017.- Vol.50(4).- P.17-26. DOI 10.1109/mc.2017.112.

4. Kiberataki// https://www.tadviser.ru. - Data obrashhenija: 13.01.26. [in Russian]

5. Semenov Ju.A. Obzor ujazvimostej, nekotoryh vidov atak i sredstv zashhity // http://book.itep.ru/6/intrusion.htm. - Data obrashhenija:13.01.2026. [in Russian]

6. O. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions// Electronics.-2023.- Vol.12(6): DOI 10.3390/electronics12061333.

7. J. Hao et al. Effectively detecting and diagnosing distributed multivariate time series anomalies via unsupervised federated hypernetwork// Information Processing & Management. - 2025.- Vol.62(4): 104107. DOI 10.1016/j.ipm.2025.104107.

8. Identifying and Mitigating Web Application Vulnerabilities: A Comparative Study of Countermeasures and Tools// International Journal Software Engineering and Computer Science, - 2024.- Vol.4(3)- PP. 1109-1127. DOI 10.35870/ijsecs.v4i3.3138.

9. Sjutkina V. Promyshlennye predprijatija ujazvimy dlja atak, 2018 // https://www.comnews.ru.- Data obrashhenija: 13.01.26

10. Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu, and Xinwen Fu. Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. IEEE Internet of Things Journal.- 2017. Vol. 4(6).-PP.1899-1909. DOI 10.1109/JIOT.2017.2707465.

11. PCI Security Standards Council. Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 4.0. - 2022. https://evertrust.io/compliance-center/pci-dss/ - Data obrashhenija: 15.01.26. [in Russian]

12. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. - RFC 8446, 2021. https://www.ietf.org/archive/id/draft-rescorla-tls-rfc8446-bis-00.html.- Data obrashhenija: 15.01.26. [in Russian]

13. Ujazvimosti korporativnyh informacionnyh sistem, 2019 https://ptsecurity.com .-Data obrashhenija: 13.01.2026. [in Russian]

Авторлар туралы мәлімет

Даненова Г.Т.- т.ғ.к., Абылқас Сағынов атындағы Қарағанды техникалық университеттінің доценті, Қарағанды, Қазақстан, e-mail: g.danenova@ktu.edu.kz ;

Ахметжанов Т.Б. - т.ғ.к., Абылқас Сағынов атындағы Қарағанды техникалық университеттінің доценті, Қарағанды, Қазақстан, e-mail: akhmetzhantalgat@gmail.com;

Коккоз М.М. - т.ғ.к., Абылқас Сағынов атындағы Қарағанды техникалық университеттінің доценті, Қарағанды, Қазақстан, e-mail: makhabbat_k@bk.ru.

Information about the authors

Danenova G.T. - Candidate of Technical Sciences, Associate Professor, Karaganda Technical University named by Abylkas Saginov, Karaganda, Kazakhstan, e-mail: g.danenova@ktu.edu.kz;

Akhmetzhanov T.B. - Candidate of Technical Sciences, Associate Professor, Karaganda Technical University named by Abylkas Saginov, Karaganda, Kazakhstan, e-mail: akhmetzhantalgat@gmail.com;

Kokkoz M.M. - Candidate of Pedagogical Sciences, Associate Professor, Karaganda Technical University named by Abylkas Saginov, Karaganda, Kazakhstan, e-mail: makhabbat_k@bk.ru.