ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

Разработка интерфейса пользователя. Характеристик недвижимости, влияющих на цену очень много, однако интерфейс для пользователя задающих эти характеристики должен быть прост и понятен. Было принято решение использовать простые, понятные, минималистичные переключатели.

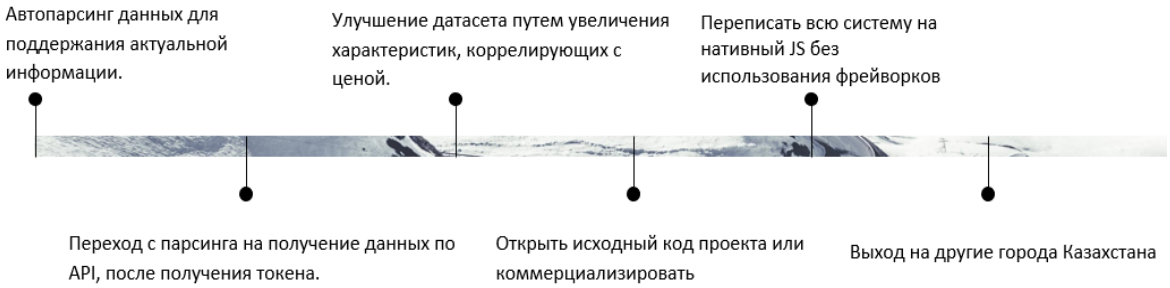


Рисунок 4 – Процесс формирования видения проекта

Одним из главных задачи данного проекта является разработка этапы коммерциализации проекта[3,6]:

- Анализ ситуации на рынке и оценка потребностей в данном продукте.
- Разработка и выполнение проекта. Основными пунктами данного этапа являются: разработка мобильного приложения; тестирование разработанного мобильного приложения; анализ возникших проблем в ходе работы приложения, анализ работы модели, решение возникших проблем; введение мобильного приложения в эксплуатацию; прохождение лицензирования и проведения защиты интеллектуальной собственной разработки.
- Мониторинг и оценка. Система мониторинга будет введена в действие для измерения хода выполнения каждого проекта в плане его ключевых показателей эффективности. Оценка будет составной частью этого процесса в целях проведения анализа эффективности и внесения улучшений.

В результате исследования была сформирована модель нейросети прогнозирования стоимости для объектов жилой недвижимости на сайте olx.kz, с использованием методов машинного обучения, с последующей коммерциализацией проекта в виде приложения, предоставляющего возможность расчета стоимости жилой недвижимости.

Список использованных источников

1. Асаул А. Н. Экономика недвижимости: Учебник для вузов. 3-е изд. Стандарт третьего поколения. — СПб.: Питер, 2018.
2. Willi Richert, Luis Pedro Coelho. Building Machine Learning Systems with Python Published by Packt Publishing Ltd, 2017
3. Терехов С.А. Лекции по теории и приложениям искусственных нейронных сетей. [Электронный ресурс]: – Режим доступа: http://alife.narod.ru/lectures/neural/Neu_ch04.htm
4. Andreas C. Mueller and Sarah Guido. Introduction to Machine Learning with Python. Published by O'Reilly Media, Inc. 2016
5. Коэльо, Л.П. Построение систем машинного обучения на языке Python //пер. с англ. Слинкин А. А. - Москва :ДМК Пресс, 2016.
6. Силен Дэви, Мейсман Арно, Али Мохамед. Основы Data Science и Big Data. Python и наука о данных. -СПб.: Питер, 2017. -336 с.

ӘОЖ 004.056

ВЕБ - ҚОСЫМШАЛАРДАҒЫ АВТОРИЗАЦИЯ КЕМШІЛІКТЕРІ

Ержанова Ерке Ержанқызы
yyerzhanova@mail.ru

Ақпараттық қауіпсіздік жүйелері мамандығының Л.Н.Гумилев атындағы ЕҰУ студенті, Астана, Қазақстан
Ғылыми жетекші – Е.Қайупов

Қазіргі таңда интернет желісінің қарқынды дамуымен қатар, веб - қосымшаларды қолданылуы, олардың біз үшін маңыздылығы күннен күнге артып келе жатыр. Веб - қосымшалардың ең маңызды элементтерінің бірі бұл авторизация, өйткені ол қандай пайдаланушылардың қолданбаның белгілі бір мүмкіндіктері мен деректеріне қол жеткізе алатынын анықтайды. Ал әрбір қосымша үшін қауіпсіздіктің үш бөлігінде, яғни қол жетімдігі, құпиялылығы және тұтастығы сақталына білуі қажет.

Кез-келген басқа функционалдылық сияқты веб - қосымшалардағы авторизацияның да әлсіз жақтары бар. Олардың кейбір кемшіліктері:

- Парольдерді есте сақтау қажеттілігі;
- Қол жетімділік мәселелері;
- Аутентификация механизмдерімен мәселелер;
- Парольдерді іріктеп тауып алу шабуылына осалдығы;
- man-in-the-middle шабуылына осалдығы және т.б.

Барлық қауіпсіздік шараларын ескере отырып, веб - қосымшаларда пайдаланушылардың авторизациясын жүзеге асыру бірнеше негізгі қадамдарды қамтиды, олар:

- Пайдаланушы құпия сөздерін хэштеу және тұз арқылы шифрланған түрде сақтау;
- Қауіпсіз HTTPS қосылымын пайдалану;
- Сәйкестендіру үшін сеанс кілттерін пайдалану;
- Қосымшаға кіру әрекеттерінің санын шектеу;
- Екі факторлы аутентификацияны жүзеге асыру;
- Сеанстың жарамдылық мерзіміне шектеулер қою;
- Авторизация процесіндегі қателер туралы толық ақпаратты ашпау;
- Қауіпсіздікті үнемі тексеріп отыру.

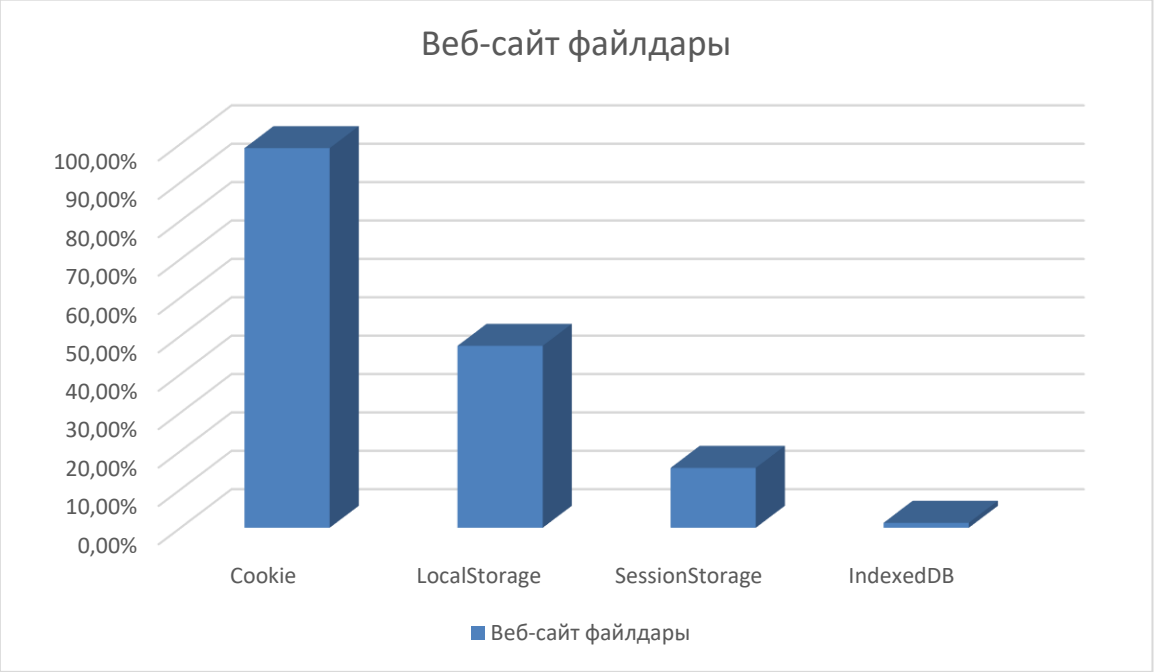
Сонымен жүйе қауіпсіздігін құрудан басқа оны тексере білу қажет. Авторизация қауіпсіздігін тексерудің бірнеше әдістері келесідей:

- **Brute Force Testing;**
- **Multiple Login Testing;**
- **SQL Injection Testing;**
- **Traffic Interception Testing;**
- **Session Vulnerability Testing;**
- **Role-based Access Testing.**

Жоғарыда аталған әдістерден басқа веб - қосымшаларда CSRF, XSS, аутентификация осалдықтары, жалпы ақпараттың шығып кетуіне және т.б. қауіпсіздікті тексерудің көптеген басқа әдістері мен құралдары бар. Сонымен қатар, веб - қосымшалардың қауіпсіздігінің ең жоғары деңгейін қамтамасыз ету үшін белгілі бір қосымшаның ерекшеліктерін, оның архитектурасын, әзірлеуде қолданылатын технологияларды ескеру қажет. Сондықтан, веб-қосымшалардың қауіпсіздігін сапалы тестілеу үшін ақпараттық қауіпсіздік саласында тәжірибе мен терең білімнің болуы маңызды.

W3Techs және HTTP Archive компанияларының 2020-2021 жылдары өткізген зерттеулері бойынша барлық веб - қосымшалардың 98,9% cookie файлдарын қолданады екен. Демек, cookie файлдарын ең кең тараған веб әзірлеу элементі деп санай аламыз.

Дегенмен, веб - қосымшалар үшін тек стандартты cookie файлдарды ғана қолданылмайды, басқа да деректерді сақтау түрлері қолданылады. Олардың бірі localStorage барлық веб - сайттардың 47,4%, sessionStorage 15,6% және тек 1,3% IndexedDB қолданады екен. Жалпы, сақтаудың бұл түрлерін сеанстың күйін басқару және пайдаланушының қалауын сақтау үшін cookie файлдарының орнына немесе оған қосымша пайдалануға болады.



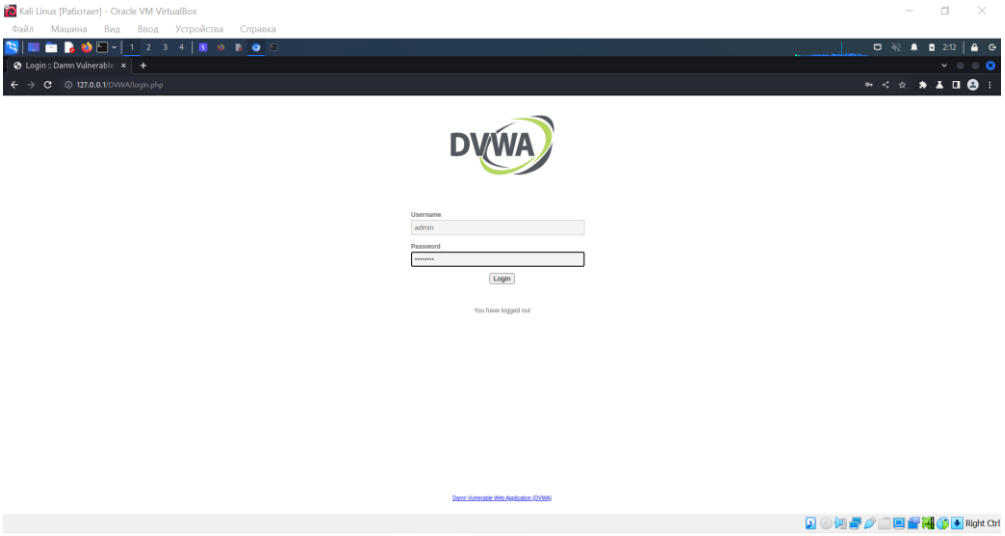
Сурет 1. – W3Techs және HTTP Archive компанияларының 2020-2021 жылдары өткізген зерттеулерінің нәтижесі.*
** ақпарат алынған источникті білдіреді.*

Айта өткеніміздей, cookie файлдарын барлық дерлік веб - сайттарда қолданады, ал бұл дегеніміз олардың сайтаралық сұранысты қолдан жасауға, яғни **Cross-Site Request Forgery** (CSRF) шабуылдарына өте осал екенін айтады. Жалпы CSRF шабуылдарына cookie файлдарымен бірге браузердің аутентификациясы немесе клиенттің авторизация сертификаттарын пайдаланатын веб - қосымшалар осал болып келеді.

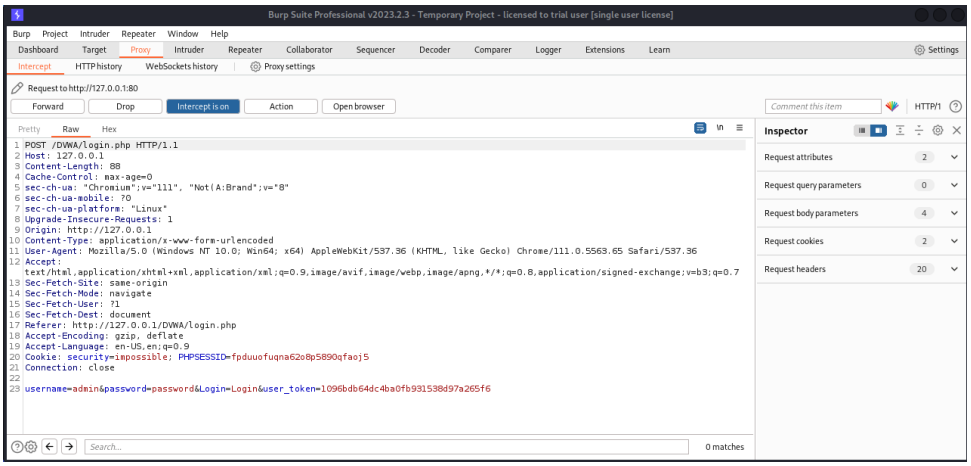
Пайдаланушының Cookies-і 30 күн бойы сақталады. Ал Google Analytics-те қолданылатын негізгі cookie файлы _ga деп аталады және браузерде екі жыл бойы сақталады. Енді сіздің ақпаратыңыздың осынша уақыт ішінде қаншама рет шабуылға ұшырай алатының, қанша уақыт бойғы мәліметтерді ала алатын болады.

Кратко описат алгоритм и инструменты, для чего будут применяться.2-3 предложения

Бұл шабуылға веб - қосымшалардың тәуелді екенін көрсету үшін Damn Vulnerable Web Application (DVWA) осалдықтарды тестілеу ортасын қолдандым. Қауіпсіздік деңгейін impossible деп таңдадым, бұл қазіргі уақытта веб - қосымшалардағы қол жеткізілген қорғаудың жоғары деңгейін береді. Қолданушы өз логинің және құпия сөзін енгізіп кіру батырмасын басқан уақытта PortSwigger компаниясының Burp Suit Professional веб - қосышаларды зерттеуге арналған құралынан proxy бөлімін қолданамыз. Бұл арқылы біздің қолданушыдан жіберілген сұрауынан мәлеметтерді ұстап ала аламыз.



Сурет 2. - Қолданушының веб - қосымшаға кіру кезінде өз логині мен құпия сөзін енгізу терезесінің көрінісі.



Сурет 3. - Қолданушының өз логині мен құпия сөзін жазып сұрау жіберген кезде қағып алынған мәліметтер көрінісі.

Біздің мақсатымызға қарай қауіпсіздік деңгейін және ең бастысы логин мен құпия сөзімізді ала алдық.

Егер басқа адамға веб - қосымшаға кіру сілтемесін жіберетін болсаңыз, жіберілген сілтеменің қандай бағытта екенін көрсетпес үшін encode, яғни кодтауды қолданамыз, бұл үшін де Burp Suit Professional құралында decode бөлімінде жүзеге асырдым. Себебі ешқандай өзгеріссіз жіберсек сілтеменің қандай жұмыс атқаратының бірден түсініп алуға болады:«http://127.0.0.1/DVWA/vulnerablities/csrf/?password_current=password&password_new=password&password_conf=password&Change=Change&user_token=7cb71fda29d27f392063af7e11d61db6#», ал егер бұны біз encode жасап түрлендірсек, кодтау туралы білмейтін адам көп мән бермейді: «http://127.0.0.1/DVWA/vulnerabilities/csrf/?%70%61%73%73%77%6f%72%64%5f%63%75%72%72%65%6e%74=%70%61%73%73%77%6f%72%64%5f%6e%65%77=%68%61%63%6b%65%71&%70%61%73%73%77%6f%72%64%5f%63%6f%6e%66=%68%61%63%6b%65%72&%43%68%61%6e%67%65=%75%73%65%72%5f%74%6f%6b%65%6e=7cb71fda29d27f392063af7e11d61db6#».

Көптеген кемшіліктеріне қарамастан, авторизация веб-қосымшалардың маңызды функционалдығы болып табылады және пайдаланушылардың құпия деректерін қорғау үшін қажет. Сондықтан ол барлық қауіпсіздік шараларын ескере отырып, тиісті түрде жүзеге асырылуы керек.

Қолданылған әдебиеттер тізімі

1. *"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" авторлары Даффиц (Dafydd Stuttard) және Маркус (Marcus Pinto).*
2. Безопасность приложений — Википедия (wikipedia.org)
3. Web Technologies of the Year 2021 (w3techs.com)
4. [All levels] DVWA Cross Site Request Forgery (CSRF) - YouTube
5. Мұнда кітіп көрсетіңіз диаграма алынған.

ӘОЖ 004

WEBSOCKET ПРОТОКОЛЫН ТАЛДАУ ЖӘНЕ ОНДАҒЫ ОСАЛДЫҚТАР

Есенпулов Айбек Бекзатұлы
aib.esen.02@bk.ru
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық қауіпсіздік жүйелері мамандығының студенті,
Астана, Қазақстан
Ғылыми жетекші – Е.Қайупов

WebSocket - бұл браузер мен веб-сервер арасында тұрақты байланысты пайдаланып, хабар алмасуға арналған TCP қосылымының үстіндегі байланыс протоколы. WebSocket әрбір онлайн чаттар мен онлайн-таблицаларды құруда және басқа да нақты уақыттағы хабар алмасу (в режиме реального времени) қажет IT-өнімдер мен проектілерде кеңінен қолданылады.

WebSocket - ті пайдаланатын кейбір танымал қосымшалардың мысалдары:

WhatsApp: WhatsApp серверлері мен пайдаланушының құрылғысында орнатылған клиенттік қолданба арасында нақты уақыттағы хабар алмасу үшін WebSockets пайдаланады.

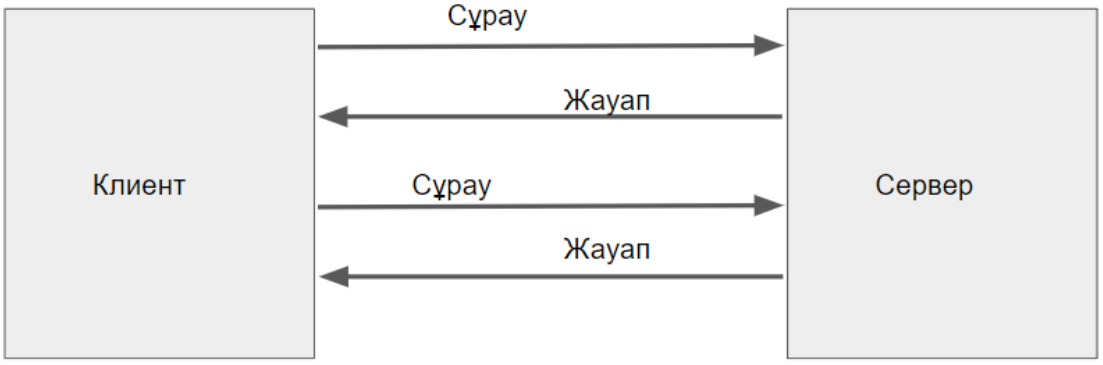
Slack: Slack пайдаланушыларына нақты уақыттағы хабар алмасу және бірлесіп жұмыс істеу мүмкіндіктерін беру үшін WebSockets пайдаланады.

Trello: Trello тақталарды, карталарды және хабарландыруларды нақты уақытта жаңарту үшін WebSockets пайдаланады.

Twitter: Twitter өзінің пайдаланушыларына твиттер, ретвиттер, ұнатулар және басқа әрекеттер үшін нақты уақытта жаңартуларды қамтамасыз ету үшін WebSockets пайдаланады.

Asana, Uber, Netflix, Twitch және тағы басқа да өзіміз пайдаланып жүрген қосымшалар.

WebSocket протоколы қалай жұмыс жасайтынын түсіну үшін, алдымен HTTP арқылы жүзеге асатын байланысқа назар аударайын.



Сурет 1 - HTTP арқылы клиент-серверлік байланыс

Суретте көріп тұрғанымыздай бір сұрауға бір жауап және одан кейін байланыс үзіледі. Клиент-серверлік архитектура HTTP протоколы арқылы осылай байланысады.

HTTP ерекшіліктері:

HTTP сұрауға жауап бергеннен кейін байланысты үзеді.