Результаты анализа защищенности веб-ресурсов банков второго уровня Республики Казахстан 2021

WEBTOTEM.AI

Сравнительный анализ уровня безопасности 2020 –2021 годов

Согласно проведенному анализу за период с января 2020 года по май 2021 года все банки второго уровня, вошедшие в периметр анализа, показали рост показателей уровня защищенности официального веб-ресурса банка. Средний рост уровня безопасности составил 19.6%. Отрицательной тенденции в обеспечении информационной безопасности среди банков второго уровня не обнаружено. В приведенной ниже таблице официальные web-ресурсы банков второго уровня были оценены по шкале от 0 до 100, разработанной экспертами ЦАРКА, где 100 является наивысшей оценкой уровня защищенности web-ресурса.

URL	2020	2021	Дельта
alfabank.kz	65	85	20
bankrbk.kz	60	83	23
citibank.com	20	81	61
halykbank.kz	80	81	1
bankffin.kz	80	80	0
jysanbank.kz	55	79	24
kaspi.kz	70	78	8
hcsbk.kz	45	77	32
bcc.kz	50	75	25
kzibank.kz	55	75	20
altyn-i.kz	65	75	10
sberbank.kz	40	74	34
homecredit.kz	65	73	8
forte.kz	45	72	27
kz.icbc.com.cn	71	71	0
vtb-bank.kz	45	70	25
eubank.kz	55	70	15
alhilalbank.kz	45	69	24
nurbank.kz	50	69	19
boc.kz	30	67	37
shinhan.kz	40	67	27
atfbank.kz	65	67	2
zamanbank.kz	40	66	26
jscnbp.kz	65	66	1
capitalbank.kz	40	65	25

Глоссарий

Информационная безопасность – это состояние информационной системы при котором она способна обеспечить конфиденциальность, целостность и доступность хранимых данных.

Уязвимость – недостаток или недоработка информационной системы, которая может быть использована с целью несанкционированного доступа к данным, их изменению или удалению.

Риск – потенциальный ущерб, который может быть нанесен организации в случае использования уязвимостей системы в преступных целях.

Кибер-атака – использование технологий с целью несанкционированного доступа в систему и получения контроля над ней.

Введение

Сегодня банкам доверено беспрецедентное количество конфиденциальных данных. Ставки очень высоки: взлом банковских веб – сервисов ставит под угрозу защиту персональных данных граждан, а также доверие казахстанцев к банковской системе.
Содействуя концепции кибербезопасности "Киберщит Казахстана", утвержденной постановлением Правительства Республики Казахстан (далее – РК) № 407 от 30 июня 2017 года , продукт собственной разработки Центра анализа и расследования кибер атак (далее - ЦАРКА) WebTotem AI на постоянной основе ведет мониторинг защищенности веб-сайтов казнета.
Данный отчет был подготовлен ЦАРКА по результатам тестирования веб-ресурсов банков второго уровня РК, проведенного с использованием системы WebTotem AI в мае 2021 года.
Система WebTotem AI основана на алгоритме искусственного интеллекта, который позволяет выявлять уязвимости и угрозы в киберпространстве.
ЦАРКА искренне надеется, что проделанная работа поможет отделам информационной безопасности банков обратить внимание на выявленные уязвимости, которые потенциально могут быть использованы злоумышленниками, а также будет способствовать повышению уровня защиты в соответствии с лучшими мировыми практиками.

Информация об исследовании

Цель исследования

Основной целью данного исследования было выяснить, как банки второго уровня РК обеспечивают безопасность своих веб-ресурсов. Оценка уровня безопасности проводилась в соответствии с лучшими практиками в области информационной безопасности такими как OWASP Top-10, ISO 27001-2013.

Метод исследования

Эксперты ЦАРКА использовали неинвазивные методы сканирования, изучая основной домен банка, его главную страницу и почтовый сервер. Тестирование проводилось без нарушения функционирования веб-ресурсов, по средствам отправки «легких» HTTP и DNS-запросов и анализа ответов с сервера. Работа включала в себя анализ использования подходов по выполнению рекомендованных настроек для веб-серверов и связанных компонентов.
Были выбраны ключевые точки контроля, доступные для проверки, не вмешиваясь в работу веб-ресурса банка и исключая таким образом какой-либо технический ущерб.

Периметр аудита

В рамках исследования в периметр вошли веб-ресурсы банков второго уровня Республики Казахстан. Указанные веб-ресурсы были оценены по десяти критериям, которые позволили дать объективное заключение по уровню их защищенности.

25

веб-ресурсов были проверены на предмет наличия уязвимостей

- Состав и скорость работы программного обеспечения
- Репутация домена
- Безопасность контента и передачи данных
- Шифрование трафика и утечки информации
- Настройки безопасности
- Соответствие стандартам

Полный перечень Банков, официальные веб-ресурсы которых вошли в периметр анализа защищенности, указаны далее:

- Kaspi Bank
- Национальный Банк Пакистана
- Сбербанк
- Банк ЦентрКредит
- Altyn Bank
- Народный Банк Казахстана
- АТФ Банк
- КЗИ Банк
- Bank RBK
- Альфа Банк
- Евразийский Банк
- ВТБ
- Citi Bank
- Исламский Банк "Al Hilal"
- Отбасы Банк
- Freedom finance Bank
- Capital Bank Kazakhstan
- First Heartland Jýsan Bank
- Хоум Кредит
- Банк Китая в Казахстане
- Fortebank
- НурБанк
- Шинхан Банк Казахстан
- Bank of China Kazakhstan
- Заман Банк

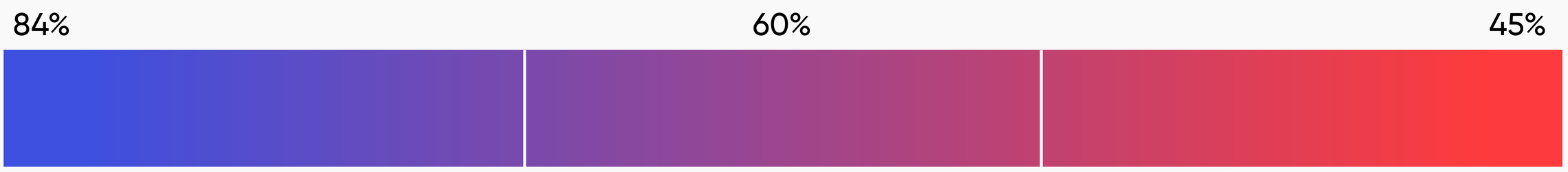
Результаты оценки защищенности

Далее приведены результаты оценки уровня защищенности веб-ресурсов. Согласно результатам оценки, которая состояла из десяти критериев таких как: репутация домена, шифрование трафика, утечка информации, открытые порты, Security. txt, безопасность email, состав программного обеспечения, скорость работы, HTTPS заголовки и безопасность контента – средний показатель защищенности составил 70%.

Топ-5 банков

Показали максимальные результаты оценки уровня безопасности

- Альфа Банк
- Bank RBK
- Citi Bank
- Народный Банк Казахстана
- Freedom finance Bank



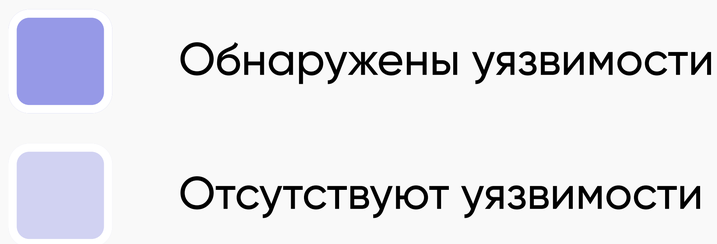
- Альфа Банк
- Bank RBK
- Citi Bank
- Народный Банк Казахстана
- Freedom finance Bank
- First Heartland Jýsan Bank
- Kaspi Bank
- Отбасы Банк
- Банк ЦентрКредит
- КЗИ Банк
- Altyn Bank
- Сбербанк
- Хоум Кредит
- Fortebank
- Банк Китая в Казахстане
- ВТБ
- Евразийский Банк
- Исламский Банк "Al Hilal"
- НурБанк
- Bank of China Kazakhstan
- Шинхан Банк Казахстан
- АТФ Банк
- Заман Банк
- Национальный Банк Пакистана
- Capital Bank Kazakhstan

Security.txt

Цель Security.txt – формализация взаимодействия между внутренней ИБ службой и внешними исследователями, давая четкое указание как и куда направлять информацию об уязвимостях или проблемах безопасности веб-ресурса.

Негативные последствия: отсутствия канала связи, который может быть использован пользователями веб-ресурса и исследователями в случае обнаружения уязвимых мест или разглашения нежелательной информации.

Детальный анализ приведен далее:



Следующие веб-ресурсы не имеют security.txt:

- Kaspi Bank
- Bank of China Kazakhstan
- Заман Банк
- Bank RBK
- Capital Bank Kazakhstan
- Хоум Кредит
- Евразийский Банк
- АТФ Банк
- Fortebank
- Банк Китая в Казахстане
- Исламский Банк "Al Hilal"
- Банк ЦентрКредит
- Сбербанк
- Altyn Bank
- НурБанк
- ВТБ
- First Heartland Jýsan Bank
- Народный Банк Казахстана
- Отбасы Банк
- КЗИ Банк
- Citi Bank
- Шинхан Банк Казахстан
- Национальный Банк Пакистана
- Freedom finance Bank

Банки реализовавшие Security.txt

- Альфа Банк

Software composition

- Описание критерия: в данном разделе описана подверженность главной страницы веб-ресурса атакам и списка OWASP Top 10.
- Описание потенциальной атаки: различные виды атак направленные основным образом на получение данных пользователей.
- Негативные последствия: неправомерный доступ к данным.

Детальный анализ приведен далее:

Обнаружены уязвимости

Отсутствуют уязвимости

Следующие веб-ресурсы имеют уязвимости к атакам OWASP Top 10:

- Заман Банк
- Bank of China Kazakhstan
- Отбасы Банк
- Capital Bank Kazakhstan
- Евразийский Банк
- Altyn Bank
- Банк ЦентрКредит
- Шинхан Банк Казахстан
- НурБанк

Банки второго уровня показавшие наилучшие результаты:

- Bank RBK
- First Heartland Jýsan Bank
- Альфа Банк
- Citi Bank
- Сбербанк

Шифрование трафика

- Описание критерия: согласно мировым стандартам, личные данные, которые передаются между веб-сервисом и клиентом, подлежат шифрованию. Практика шифрования данных при передаче обеспечивает надежную защиту от перехвата логинов и паролей людьми, которые находятся в одной сети.
- Описание потенциальной атаки: в ситуациях когда трафик не зашифрован на должном уровне, передаваемые сообщения могут быть перехвачены или изменены по средствам атаки типа «человек по середине».
- Негативные последствия: Злоумышленникам могут быть доступны все отправляемые пользователем данные (логин, пароль, ПИН-код и т. п.). Это приводит к утечке данных клиентов, финансовым убыткам.

Детальный анализ и перечень проверок, которые проводились относительно шифрования трафика приведены далее:

- Рейтинг (SSL Lab)
- Недостатки в конфигурировании алгоритма Диффи – Хеллмана
- Уязвимость POODLE
- Уязвимость FREAK
- Возможность проведения атаки Logjam
- Уязвимость ROBOT
- Уязвимость Beast
- Поддержка NPN и ALPN
- Уязвимость CVE-2016-2107
- Уязвимость Heartbleed
- Уязвимость Ticketbleed
- SSL Renegotiation
- Поддержка RC4
- Поддержка Forward Secrecy
- Версия TLS
- Поддержка SSL 2.0 и SSL 3.0

Уязвимости связанные с шифрованием передаваемых данных были обнаружены в следующих веб-страницах:

- Банк Китая в Казахстане
- Отбасы Банк
- Freedom finance Bank
- Исламский Банк "Al Hilal"
- ВТБ
- АТФ Банк

Банки второго уровня показавшие наилучшие результаты:

- Bank RBK
- First Heartland Jýsan Bank
- Альфа Банк
- Citi Bank
- Сбербанк

Скорость работы

- Описание критерия: оценка скорости загрузки основана на данных FCP и FID, полученных методом имитации загрузки сайта. Тестирование наилучшей практики производительности выполняется для анализа устойчивости сайта к нагрузкам.
- Описание потенциальной атаки: Низкая производительность позволит злоумышленникам перегружать веб-ресурс путем специально подобранных запросов, тем самым затруднив или полностью прекратив доступ граждан на веб-ресурс
- Негативные последствия: недоступность веб ресурса для пользователей.

Детальный анализ приведен далее:

Обнаружены уязвимости

Отсутствуют уязвимости

Следующие веб-ресурсы имеют низкую производительность:

- Банк Китая в Казахстане
- Отбасы банк
- Банк ЦентрКредит
- Евразийский Банк

Банки второго уровня показавшие наилучшие результаты:

- Kaspi Bank
- КЗИ Банк
- Freedom finance Bank
- АТФ Банк
- Национальный Банк Пакистана

Утечка данных

- Описание критерия: Любая утечка информации несет в себе негативные финансовые, репутационные последствия для компании.
- Описание потенциальной атаки: получение доступа к корпоративной почте, рабочей переписке, рабочей документации компании. Получение доступа к чувствительной информации злоумышленниками может быть использовано для осуществления атаки на информационные системы государственных органов.
- Негативные последствия: неправомерный доступ к данным, финансовые и репутационные потери.

Детальный анализ приведен далее:

Обнаружены уязвимости

Отсутствуют уязвимости

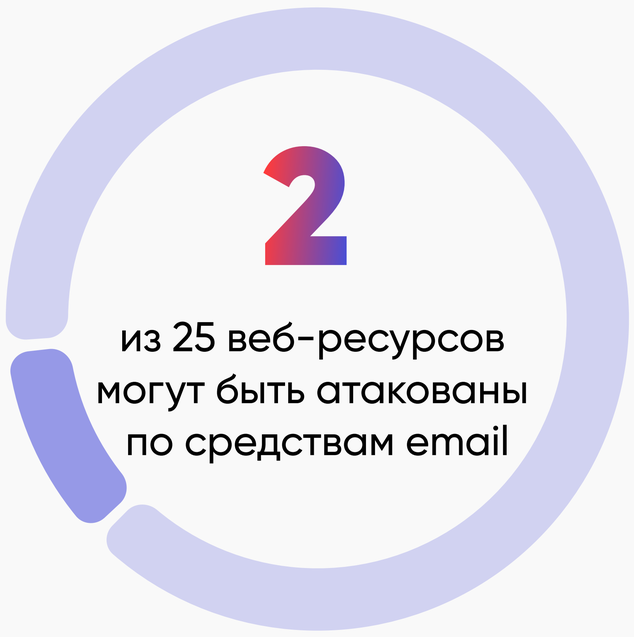
Следующие веб-ресурсы имеют установленные случаи утечки данных:

- Kaspi Bank
- КЗИ Банк
- Заман Банк
- Народный Банк Казахстана
- Евразийский Банк
- Хоум Кредит
- НурБанк
- Отбасы Банк

Email security

- Описание критерия: Более 90% почтового трафика содержит спам, фишинг, вредоносные программы и другие электронные угрозы. Электронная почта является основным вектором заражения для вымогателей и вредоносных программ. Данный пункт проверяет, правильно ли настроен почтовый сервер веб-ресурса для предотвращения этих распространенных угроз.
- Описание потенциальной атаки: email является наиболее вероятным способом заражения вредоносными программными продуктами
- Негативные последствия: Получение нежелательной почтовой рассылки, несущей бесполезную информацию и содержащей в себе вредоносный код (бот-сети, трояны, черви), вектор для проведения фишинговой атаки.

Детальный анализ приведен далее:



Обнаружены уязвимости

Отсутствуют уязвимости

Следующие веб-ресурсы имеют недостаточные показатели по Email Security:

Народный Банк Казахстана

Altyn Bank

Банки второго уровня показавшие наилучшие результаты:

Kaspi Bank

Альфа Банк

Freedom finance Bank

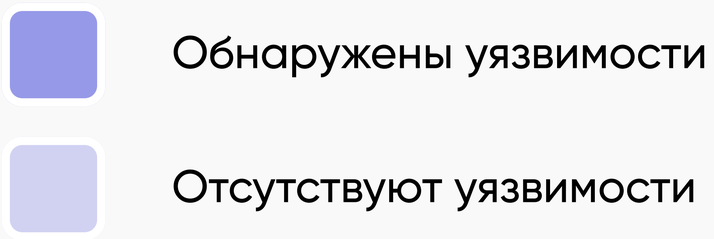
First Heartland Jýsan Bank

Citi Bank

Репутация домена

- Описание критерия: анализ открытых источников, содержащих рейтинги доменов в сети интернет.
- Описание потенциальной атаки: если веб-ресурс занесен в черный список, доступ на него может быть заблокирован браузерами или иными системами.
- Негативные последствия: Это в первую очередь приводит к потере трафика, доверия клиентов и, следовательно, денег. Проверка репутации домена в различных базах антивирусных ПО.

Детальный анализ приведен далее:



HTTP Security заголовки

- Описание критерия: при передачи данных от веб-сервера к клиенту, могут передаваться мета – данные, которые могут быть использованы при атаке. В процессе анализа проверялись такие заголовки как: Strict-Transport-Security, Content-Security-Policy, X-XSS-Protection, HTTP Strict Transport Security, X-Frame-Options, Expect-CT
- Описание потенциальной атаки: атаки направленные на добавления вредоносного содержания в структуру веб-ресурса, такие как инъекция вредоносного кода, XSS и изменения контента веб-ресурса
- Негативные последствия: несанкционированный доступ к данным, получение злоумышленником контроля над веб-ресурсом.

Детальный анализ приведен далее:

Обнаружены уязвимости

Отсутствуют уязвимости

Следующие веб-ресурсы имеют низкие показатели по HTTP Security :

- Capital Bank Kazakhstan
- Fortebank

Банки второго уровня показавшие наилучшие результаты:

- Kaspi Bank
- Альфа Банк
- Freedom finance Bank
- Bank RBK
- Citi Bank

Национальная площадка BugBounty.kz

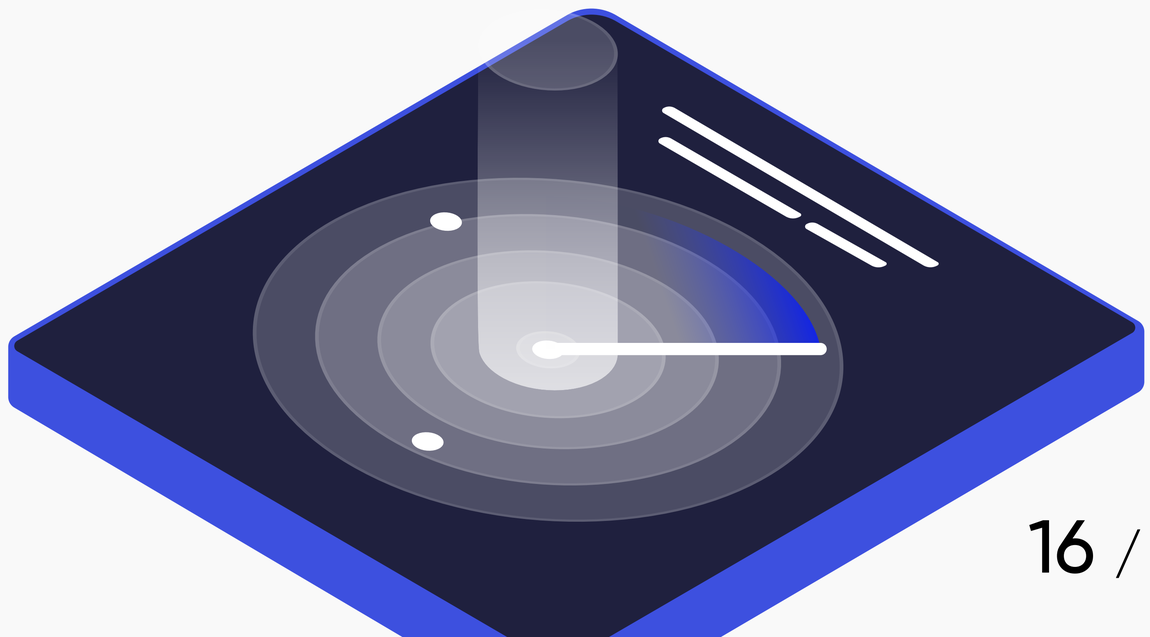
Баг-баунти программа — это специальная программа, в ходе которой компания привлекает сторонних специалистов по кибербезопасности (в индустрии называемых «белыми хакерами» или «исследователями», «ресечерами») для тестирования своего программного обеспечения на уязвимости, за монетарное вознаграждение.

Площадка **Bugbounty.kz** помогает выявить угрозы, оценить риски, раскрыть уязвимости в организации, прежде чем они могут быть использованы злоумышленниками. С помощью площадки **bugbounty.kz** государственным и частным организациям представлена возможность выявлять, устранять критические уязвимости и поддерживать целостность своих веб-ресурсов.

Содействуя концепции кибербезопасности «Киберщит Казахстана», утвержденной постановлением Правительства Республики Казахстан № 407 от 30 июня 2017 года , платформа **Bugbounty.kz** помогает в достижении и поддержании уровня защищенности электронных информационных ресурсов и информационных систем государственных органов Республики Казахстан от внешних и внутренних угроз.

Перспективность внедрения:

С помощью площадки **Bugbounty.kz**. организации, занимающиеся бизнесом могут находить и устранять критические уязвимости, поддерживать целостность приложений, избегать затрат на устранение потенциальных инцидентов. Информационная безопасность, с применением проверок хакеров, дает конкурентные преимущества такие как непревзойденная скорость, глубина и широта охвата кибербезопасности с более низкими затратами. К дополнению, для снижения репутационных рисков, сотрудничество с ИТ-сообществом способствует повышению квалификации штатных специалистов по информационной безопасности и разработчиков.



Анализ уязвимостей веб-ресурсов, обнаруженных в рамках программы Bug Bounty

Согласно проведенному анализу за период функционирования национальной площадки Bugbounty.kz с декабря 2020 года по июнь 2021 года были определены веб-ресурсы банков второго уровня Республики Казахстан, которые подвержены различным видам уязвимостей. В приведенной ниже таблице указаны найденные уязвимости и уровни их критичности.

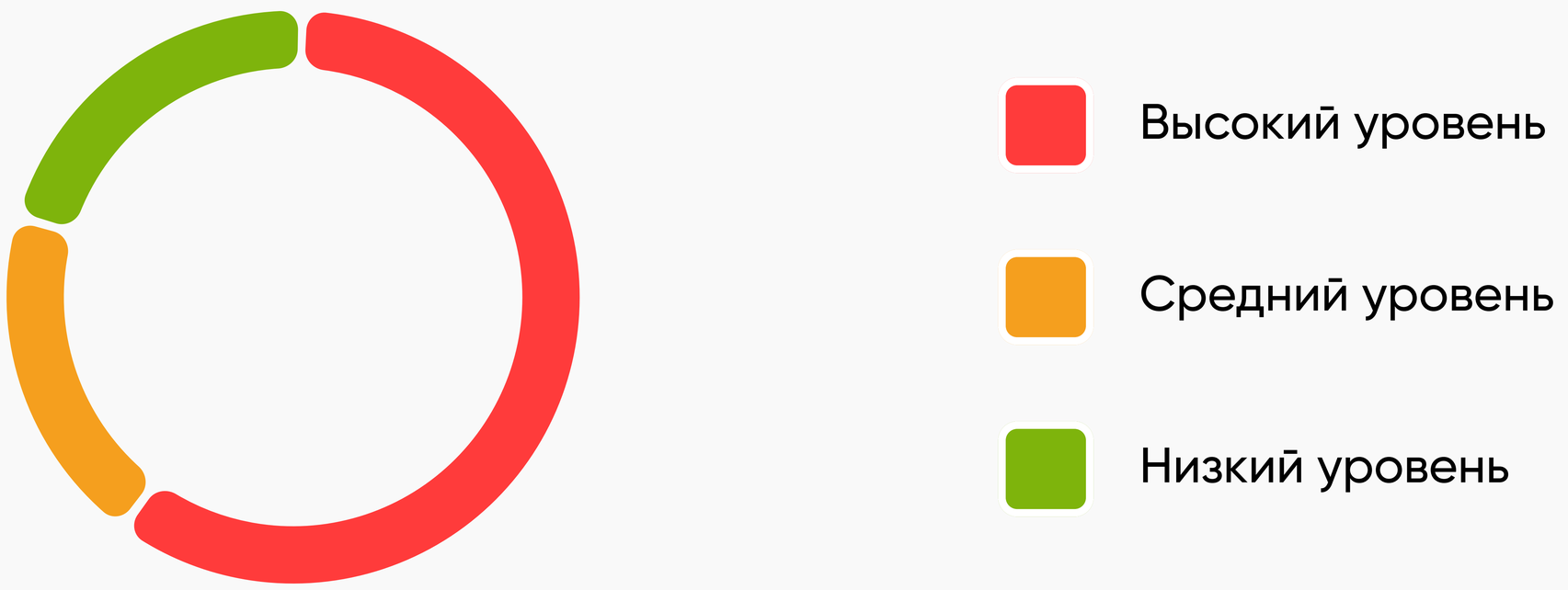
Уровень критичности:	Высокий	Средний	Низкий
	Уязвимость виртуального помощника	SMS flood	Sensitive Data Exposure
	Уязвимость виртуального помощника	Using Default Credentials	Sensitive Data Exposure
	Using Default Credentials	Using Default Credentials	Exposed Admin Portal
	Server Side Request Forgery		Directory Listing Enabled
	Authentication Bypass		
	Sensitive Data Exposure		
	Sensitive Data Exposure		
	Weak Password		
	Insecure Direct Object References (IDOR)		
	Sensitive Data Exposure		

Процентный показатель

Согласно вышеуказанному анализу в период с декабря 2020 года по июнь 2021 года на вебресурсах банков второго уровня Республики Казахстан было обнаружено 17 уязвимостей с различными уровнями критичности

В нижеприведенной таблице выведен процентный показатель уровней критичности уязвимостей, которым больше всего подвержены веб-ресурсы:

Уровни критичности:



Большая часть веб-ресурсов банков, приведенные в предыдущей таблице подверженыуязвимостям с высоким уровнем критичности, что определяет низкий уровень обеспеченияинформационной безопасности.

Описание обнаруженных уязвимостей

Уязвимость виртуального помощника

В данном кейсе появилась возможность вести чат от имени другого человека, что привело к уязвимости no userinput validation (отсутствие валидации входных данных).

Sensitive Data Exposure

Раскрытие конфиденциальных данных происходит в результате некорректной защиты базы данных, в которой хранится информация. Это может быть результатом множества факторов, таких как слабое шифрование, отсутствие шифрования, недостатки программного обеспечения или когда кто-то по ошибке загружает данные в неправильную базу данных.

Exposed Admin Portal

Уязвимость, позволяющая получить доступ к административной панели в следствие небезопасного менеджмента (Не является уязвимостью, как таковой, а является её следствием. Например, использование учетных записей по умолчанию приводит к раскрытию административной панели).

Default credentials

Это тип уязвимости, который чаще всего встречается у таких устройств, как модемы, маршрутизаторы, цифровые камеры и другие устройства, имеющие некоторые предварительно установленные учетные данные администратора для доступа ко всем параметрам конфигурации.

Authentication Bypass

Обход аутентификации - это несанкционированный доступ к административному разделу или разделам сайта и скриптам обеспечивающим прямое взаимодействие с базой данных и файловой системой сервера. Authentication Bypass может быть выполнен эксплуатируя уязвимости кода сайта, ошибки публикации ресурса, а так же из-за ошибок в настройках и уязвимостями программного обеспечения сервера.

Directory Listing Enabled

это функция, при которой веб-серверы выводят список содержимого каталога при отсутствии индексного файла (например, index.php или index.html). Поэтому, если запрос сделан в каталог, в котором включен список каталогов, и нет индексного файла, такого как index.php или index.asp, даже если есть файлы из веб-приложения, веб-сервер отправляет список каталогов как ответ. Когда это происходит, возникает проблема утечки информации, и злоумышленники могут использовать эту информацию для реализации других атак, включая уязвимости прямого воздействия, такие как XSS.

Небезопасные прямые ссылки на объекты (IDOR)

Это уязвимость, которая возникает, когда разработчик веб-приложения использует идентификатор для прямого доступа к внутреннему объекту реализации, но не обеспечивает дополнительный контроль доступа и / или проверки авторизации. Например, уязвимость IDOR может возникнуть, если URL-адрес транзакции может быть изменен посредством пользовательского ввода на стороне клиента для отображения неавторизованных данных другой транзакции.

Уязвимости подделки запросов на стороне сервера (SSRF)

Позволяют злоумышленнику отправлять созданные запросы с внутреннего сервера уязвимого веб-приложения. Злоумышленники обычно используют атаки SSRF для нацеливания на внутренние системы, которые находятся за брандмауэрами и недоступны из внешней сети. Злоумышленник может также использовать SSRF для доступа к службам, доступным через интерфейс обратной связи эксплуатируемого сервера

SMS flood

Уязвимость приводящая к истощению ресурсов компании и массовой рассылке smscообщений. Возникает вследствие отсутствия ограничений отправляемых запросов.

Заключение

Результаты анализа защищенности веб-ресурсов банков второго уровня Республики Казахстан показали наличие тенденции к увеличению уровня информационной безопасности, однако в ряде веб-ресурсов были выявлены серьезные уязвимости, которые нуждаются в исправлении в кратчайшие сроки. Среди наиболее распространённой проблемы для веб-ресурсов, можно выделить, отсутствие security.txt, а именно контактов отдела ИБ, которые позволят пользователям на прямую обращаться в отдел ИБ банка в случае выявления нарушений в работе веб-ресурса. Широко распространённой проблемой является отсутствие шифрования трафика и принудительного использования безопасной версии подключения.

Стоит отметить, что анализ защищенности веб-ресурсов банков второго уровня, не выявил ресурсов, которые бы представляли опасность для пользователей при их посещении.

Уязвимости, обнаруженные за время функционирования площадки BugBounty.kz, определили подверженность веб-ресурсов банков раскрытию конфиденциальных данных, что в свою очередь, может привести к раскрытию различных типов данных, как номера банковских счетов, номера кредитных карт, токены сеанса, домашний адрес, номера телефонов, даты рождения и информация об учетных записях клиентов, такие, как имена пользователей и пароли. Это напрямую может привести к репутационным и денежным рискам банка и его клиентской базы.

О продукте

WebTotem- это инструмент для мониторинга безопасности веб-ресурсов, защищающий компании от вторжений и постоянно развивающихся киберугроз.

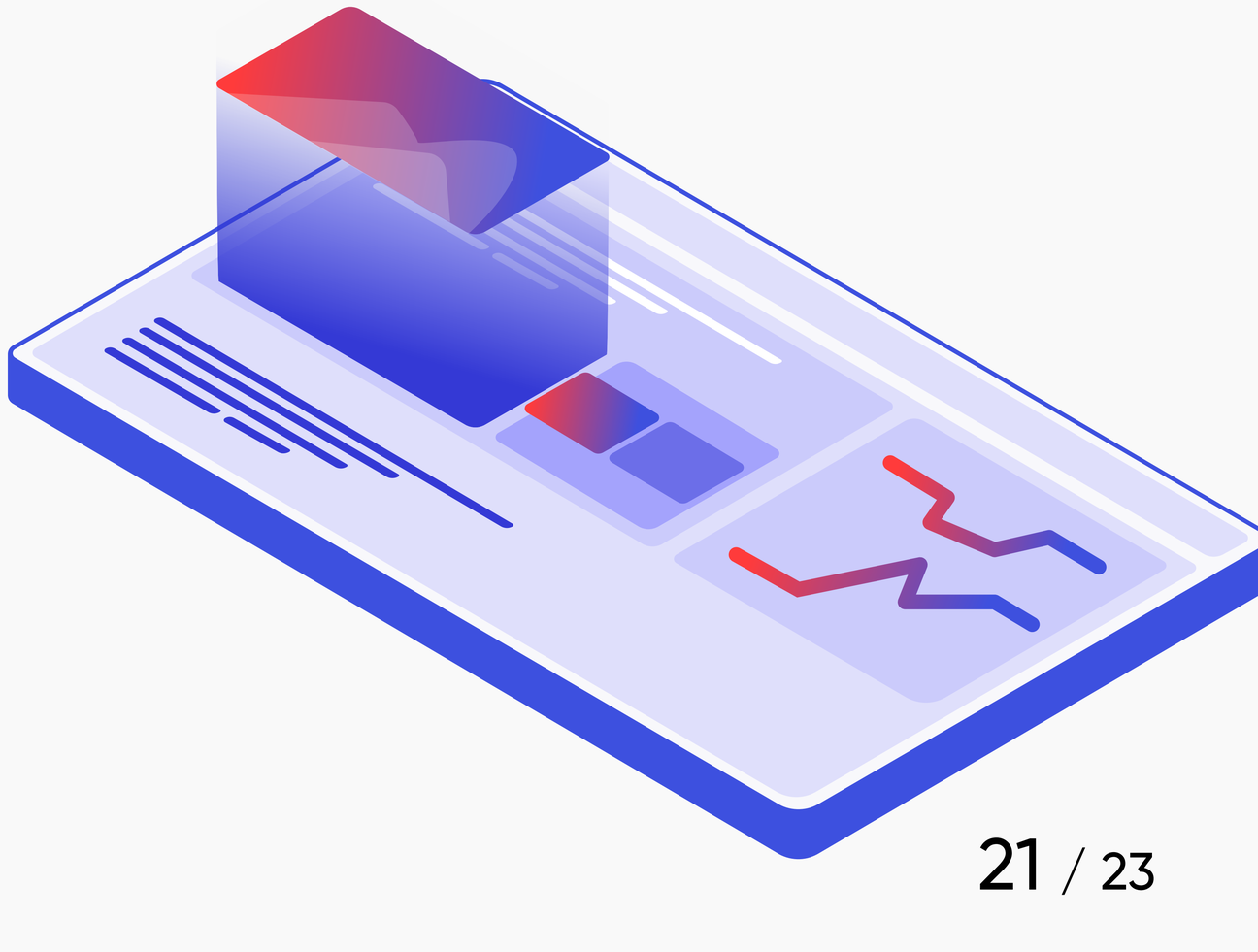
Клиент **WebTotem** может:

- Предотвращать взломы с помощью пошаговых рекомендаций по обеспечению безопасности
- Получать проактивную защиту от новых киберугроз
- Оценивать и управлять рисками кибербезопасности

Кибербезопасность все еще стоит дорого и достаточно сложно найти инженера безопасности в штат компании. Миссия **WebTotem** заключается в том, чтобы донести революционный продукт, постренный на основе искуственного интелекта, до людей из нетехнической сферы, чтобы они имели возможность защитить свой бизнес в один клик.

Мы поднимаем стандарты в области безопасности бизнес-сайтов по всему миру.

WebTotem признан лучшим SaaS решением для бизнеса (B2B, Saas and Enterprise Solution) на Echelon Asia Summit 2018 в Сингапуре. Так же **WebTotem** является региональным победителем Seedstars Kazakhstan. В 2019 году **WebTotem** был выбран для прохождения программы Cybernorth в лучшем европейском акселлераторе StartupWiseGuys в Эстонии и бизнес программы GIST (Global Innovation through Science and Technology) при поддержке правительства США.



О компании

ЦАРКА – одна из ведущих организаций в области информационной безопасности в Центральной Азии. Организация была образована в 2015 году и за время своего существования завоевала признание специалистов по информационной безопасности по всему миру. Первый частный CERT в Казахстане.

Организация предоставляет широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов ИБ и тестирований на проникновение, анализ защищенности банковских систем и бизнес приложений, веб приложений, информационных инфраструктур.

Более 50 экспертов. Эксперты **ЦАРКА** обладают сертификатами OSCP, OSWP, OSWE, OSCE, CEH, CHFI, BSI ISO/IEC 27001:2013 и регулярно принимают участие в международных конференциях, таких как PHDays, ZeroNights, Инфофорум, КодИБ. Эксперты организации являются авторами публикаций на таких ресурсах как журнал Xakep, HabraHabr, DigitalReport, ProfIT.kz и др.

Команда **ЦАРКА** занимала 1 и 2 места в соревновании The Standoff на международной конференции по информационной безопасности PositiveHackDays с 2017 по 2019 г.

Контакты

info@wtotem.com

г.Нур-Султан, проспект
Мангилик ел С3.5, 4 этаж