Техническое задание №00136/24-вн от 24.08.2021 на оказание услуг по анализу защищенности web-приложения по работе с картами Visa Virtual Prepaid с предоставлением исходного кода

Наименование тендера	Комплексный анализ защищенности web-приложения по работе с картами Visa Virtual Prepaid с предоставлением исходного кода
Адрес направления ТКП	obit@sngb.ru
Срок предоставления ТКП	15.09.2021г
Контакты	+7 (3462) 39-88-88 доб. 21-81, 21-25, 21-07
Платформа	с предоставлением исходного кода.
Этапы проведения работ	Проведение комплексной проверки действующего функционала и последующей перепроверки устранения выявленных уязвимостей приложения для платформ WEB-приложение с учетом международных стандартов, рекомендаций и лучших практик: - Open Web Application Security Project Mobile Security Testing Guide (https://owasp.org) - Open Web Application Security Project Web Security Testing Guide (https://owasp.org) - Open Source Security Testing Methodology Manual (https://www.isecom.org) - Penetration Testing Execution Standard (http://www.pentest-standard.org) - Web Application Security Consortium (WASC) Threat Classification (http://www.webappsec.org); - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (www.nist.gov); - PCI DSS (Payment Card Industry Data Security Standard); - Penetration Testing Guidance «Payment Card Industry Data Security Standard»
Состав и цели работ:	1. Получение объективной оценки защищенности приложения Заказчика от внешних/внутренних злоумышленников. 2. Выявление недостатков в применяемых Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем; 3. Выявление векторов раскрытие данных в том числе методом перебора запросов. 4. Практическая демонстрация возможности использования выявленных уязвимостей / недостатков; 5. Предложение адекватного комплекса организационных, технических и управляющих мер, направленных на предотвращение угроз информационной безопасности, а также перечня неотложных технических мер для повышения защищенности приложения Заказчика. 6. Выработка рекомендаций по устранению выявленных уязвимостей и недостатков с целью повышения уровня защищенности приложения Заказчика. 7. Проверка корректности устранения выявленных уязвимостей

	Данная услуга подразумевает проверку корректности устранения уязвимостей, обнаруженных по результатам анализа защищенности программного продукта. Специалисты Исполнителя оценивают степень эффективности предпринятых Заказчиком мер по устранению уязвимостей. Проверка проводится для векторов атаки, выявленных в результате соответствующих этапов анализа защищенности. Исполнитель подготавливает экспертное заключение по результатам перепроверки выявленных уязвимостей и несоответствий. 8. Вектор раскрытия защищаемой информации: • Основной номер держателя карты (PAN); • Имя держателя карты; • Имя держателя карты; • Сервисный код; • Полные данные дорожки магнитной полосы или ее эквивалент на чипе; • CAV2/CVC2/CVV2/CID; • PIN/PIN-блоки; • Транзакционная информация; • Персональные данные.

Дополнительные требования к участникам и оказания услуг	1. Исполнитель не имеет права привлекать внешних исполнителей. 2. Опыт оказания подобных работы организациям в финансово-кредитном секторе, не менее 3 лет. 3. Все работы проводятся Исполнителем удаленно. (Командировок и выездов на площадки Заказчика, находящиеся не в г. Москва, не предусмотрено.) 4. Исполнитель должен подтвердить отсутствие в секционном списке https://sanctionssearch.ofac.treas.gov/. 5. Условия по оплате, с указанием отдельно стоимости НДС: 100% оплата поэтапная по факту выполнения работ каждого этапа. Стоимость командировочных расходов указывается отдельной позицией. Необходимо предоставить стоимость по каждому этапу с указанием объема и формы предоставления услуги. 6. Исполнитель должен иметь возможность работать в системе электронного документа «Диадок» или совместимой с ней. 7. Участник тендера должен представить в ТКП методику проведения тестирования, а также стоимость и сроки работ по каждому этапу. 8. Заказчик в праве осуществлять передачу отчета по результатам работ, разработчику ПО (третьей стороне) для устранения выявленных уязвимостей, а также получать консультацию от Исполнителя посредством телефонной связи, с привлечением третьей стороны. 9. Наличие лицензии на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации». 10. Обязательное указание в ТКП сроков и стоимости по каждому этапу работ. 11. Срок исполнения обязательств по работам, не позднее 30.09.2021г. 12. По окончании каждого этапа работ Исполнитель предоставляет отчет с результатами проделанной работы.

Требования к методике и составу работ:	Анализ защищенности приложений проводится в соответствии с: - Open Web Application Security Project Mobile Security Testing Guide (https://owasp.org) - Open Web Application Security Project Web Security Testing Guide (https://owasp.org) - Open Source Security Testing Methodology Manual (https://www.isecom.org) - Penetration Testing Execution Standard (http://www.pentest-standard.org) - Web Application Security Consortium (WASC) Threat Classification (http://www.webappsec.org); - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (www.nist.gov); - PCI DSS (Payment Card Industry Data Security Standard); - Penetration Testing Guidance «Payment Card Industry Data Security Standard» Идентификация уязвимостей осуществляется на основе рекомендаций производителей по безопасной конфигурации ПО, материалов свободных исследовательских групп по поиску уязвимостей Open Web Application Security Project (OWASP), каталогов уязвимостей Common Vulnerabilities and Exposures (CVE). Для систематизации выявленных уязвимостей по степени критичности необходимо использовать международный стандарт оценки уязвимостей Common Vulnerability Scoring System (CVSS) версии 3. В процессе проведения работ допустимо использовать ручные и автоматические проверки.
	Модель нарушителя: Внешний злоумышленник без логического доступа к приложению (Б1) Злоумышленник в канале связи без логического доступа к приложению (Б2) Злоумышленник с физическим доступом к устройству, с которого осуществляется доступ к приложению (Б3) Злоумышленник с логическим доступом к приложению (В1) Злоумышленник в канале связи с логическим доступом к приложению (В2) Злоумышленник с физическим доступом к устройству с приложением и логическим доступом к приложению (В3)
	Анализ защищенности клиентской части приложения методом черного ящика, то есть путем анализа функций и параметров настройки приложения со стороны нарушителя, не обладающего логическим доступом к приложению; методом серого ящика, то есть путем анализа функций и параметров настройки приложения со стороны нарушителя, обладающего пользовательским или иным доступом к приложению; методом белого ящика, то есть путем анализа исходного кода клиентской части приложения.

	Анализ защищенности серверной части приложения методом черного ящика, то есть со стороны нарушителя, не обладающего логическим доступом к приложению; методом серого ящика, то есть со стороны нарушителя, обладающего пользовательским или иным доступом к приложению; методом белого ящика, то есть путем анализа исходного кода серверной части приложения.
	Анализ защищенности **канала передачи** данных между серверной и клиентской -методом черного ящика, то есть со стороны нарушителя, не обладающего логическим доступом к Системе; -методом серого ящика, то есть со стороны нарушителя, обладающего пользовательским или иным доступом к Системе.
Результат оказания услуг	По результатам проекта Заказчик получает объективную и независимую оценку защищенности приложения, которая позволяет определить, насколько эффективны на практике применяемые меры защиты информации. Отчет о результатах проверки / перепроверки защищенности приложения -общие сведения о проведенном анализе защищенности приложения, с указанием версий исследуемого продукта и версия протокола обмена; -результаты проведенных проверок/перепроверок; -выводы (как развернутые технические, так и более краткие для руководства); -оценка состояния защищенности приложения Заказчика; -перечень и описание существующих угроз; -описание хода работ, выявленных уязвимостей, ранжирование их по степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей оценкой критичности уязвимостей по международному стандарту Common Vulnerability Scoring System (v.3).; -рекомендации по устранению выявленных уязвимостей - рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения и т.п.; -результаты эксплуатации выявленных уязвимостей / недочетов, включая информацию о полученном уровне привилегий в приложении на различных этапах работы.
Сведения об объекте оценки	**Virtcard (webview)** Python (.py) – файлов: 92, строк: 3521 HTML+Django/Jinja (.html) – файлов: 23, строк: 775 Библиотеки: virtcard_web_libs.txt – предоставляется по доп.запросу. **Virtcard (API)** Python (.py) – файлов: 11, строк: 382 Библиотеки: virtcard_api_libs.txt – предоставляется по доп.запросу