Оферта о программе по вознаграждению за найденные уязвимости ООО «Городской супермаркет» (ИНН 7705466989, ОГРН 1027705012312) (Далее — «Компания»)

1. Предмет оферты, сроки её действия, вознаграждение

В случае обнаружения уязвимостей любого рода мы предлагаем Вам сообщить о них по адресу: **bug@azbukavkusa.ru**.

Срок действия оферты: с «7» июля 2020 года по «1» августа 2020 года. Лица, которые первыми найдут и сообщат об уязвимости, в рамках условий настоящей оферты, получат денежное вознаграждение. Минимальное вознаграждение за найденную уязвимость составляет 1 рубль, ориентировочная стоимость вознаграждения в зависимости от классификации уязвимостей, указана в приложении. [1] Все суммы указаны до вычета налога на доходы физических лиц. Максимальный размер вознаграждения будет зависеть только от критичности обнаруженной проблемы и оцениваться уполномоченными сотрудниками Компании самостоятельно, принимая во внимание следующие критерии:

- качество отчета;
- возможность эксплуатации уязвимости;
- тип сервиса, в котором обнаружена уязвимость;
- оценка финансовых, репутационных и других рисков, связанных с наличием уязвимости.

Вознаграждение выплачивается в течение 20 (двадцати) рабочих дней с момента подтверждения наличия уязвимости уполномоченными сотрудниками Компании, переводом денежных средств на указанный в заявлении банковский счёт, при условии подписания лицом, обнаружившим уязвимость, следующих документов (а также при условии соблюдении всех остальных положений настоящей оферты): акта оказанных услуг[2], заявления на выплату вознаграждения[3], согласия на обработку персональных данных[4] в офисе Компании по адресу: г. Москва, Кутузовский проспект, д.36, стр.6. Наличие паспорта в целях удостоверения личности при выплате вознаграждения обязательно.

По желанию участника, выраженному его письменным согласием, вместо перевода денежных средств на банковский счёт, вознаграждение может быть выплачено зачислением эквивалента (в рублях) бонусами на счёт участника программе «Вкусомания», с Правилами которой можно ознакомиться по ссылке https://vkusomania.ru/rules/main/.

При нарушении требований настоящей оферты, результаты могут быть аннулированы, вознаграждение в таком случае не выплачивается.

---

[1] Стоимость вознаграждения (ориентировочная) в зависимости от классификации уязвимостей является Приложением 1 к настоящей оферте.

[2] Образец Акта оказанных услуг является Приложением 2 к настоящей оферте.

[3] Образец Заявления на выплату вознаграждения является Приложением 3 к настоящей оферте.

[4] Образец Согласия на обработку персональных данных является Приложением 4 к настоящей оферте.

2. Обязательные условия оферты об обнаружении уязвимостей

– Не разглашать сведения об уязвимостях публично и не передавать сведения третьим лицам. Публичное или частное раскрытие сведений о любой уязвимости, обнаруженной в рамках настоящей оферты, разрешено через 30 дней после устранения этой уязвимости и только с письменного согласия Компании.

Любая конфиденциальная информация, случайно полученная в ходе поиска уязвимостей или демонстрации, не должна раскрываться. Эта информация включает (но этим не ограничивается): сведения об инфраструктуре, интерфейсах и деталях реализации, внутреннюю документацию, исходный код, данные пользователей и сотрудников. Преднамеренный доступ к этой информации строго запрещен и может быть признан незаконным применимым законодательством.

– Участниками данной программы не могут являться сотрудники Компании (действующими или бывшими), а равно аффилированными с ними лицами.

– Не осуществлять рассылку спама и атаки социальной инженерии на клиентов и сотрудников Компании.

– Не использовать обнаруженную уязвимость для своей собственной и/или иной выгоды, за исключением выгоды самого выгодоприобретателя. Выгодоприобретателем в рамках настоящей оферты является Компания (ООО «Городской супермаркет»). Данное требование включает демонстрацию дополнительных рисков, попытка раскрыть конфиденциальные данные или найти другие уязвимости.

– Не использовать инструменты тестирования уязвимостей, которые автоматически генерируют значительные объемы и/или частоту сетевого трафика.

– Не осуществлять атаки, которые могут нанести вред надёжности и/или целостности служб/сервисов Компании или данных (атаки типа «отказ в обслуживании» и другие).

– Если необходимо, использовать свои собственные учетные записи для поиска уязвимостей. Не взаимодействовать с другими учетными записями без разрешения их владельцев.

3. Область обнаружения уязвимостей в рамках настоящей оферты

В область обнаружения уязвимостей входят:

- Сервисы, расположенные на доменных именах: av.ru (и субдоменах), azbukavkusa.ru (и субдоменах);
- Сервисы, расположенные на сетевых адресах: 195.19.210.0/24;
- Сервисы, доступные в беспроводных сетях Компании и сами беспроводные сети, принадлежащие Компании.

Область действия оферты ограничена исключительно техническими уязвимостями в наших сервисах и веб-приложениях. Любая уязвимость дизайна или реализации, которая существенно влияет на конфиденциальность или целостность данных, вероятно, будет применима к настоящей оферте. Примеры релевантных уязвимостей:

- удаленное исполнение кода на стороне сервера;
- уязвимости в реализации протоколов аутентификации или авторизации;
- уязвимости бизнес-логики;
- CSRF-уязвимости;
- XSS-уязвимости.

Список может быть дополнен Компанией в любое время в рамках сроков проведения программы.

4. Требования к отчетам об уязвимостях

В аналитику Компанией принимаются отчеты на русском или английском языке.

Предоставляя отчет об уязвимостях, вы соглашаетесь соблюдать политику информационной безопасности. Отчеты принимаются по почте**: bug@azbukavkusa.ru**, с темой письма: «*Отчёт по программе по вознаграждению за найденные уязвимости*».

Отчет должен содержать подробное описание обнаруженной уязвимости:

- уязвимые узлы и компоненты;
- обнаруженная уязвимость и ее влияние на безопасность;
- этапы воспроизведения;
- сценарий атаки;
- рекомендации по устранению.

Этапы воспроизведения описывают процесс эксплуатации уязвимости, шаг за шагом, в правильном порядке.

В сценарии атаки описывается информация о том, как злоумышленник может использовать обнаруженную Вами уязвимость, необходимые условия для ее эксплуатации и то, что атакующий может получить в случае успешной атаки.

Отчеты, которые четко и лаконично идентифицируют затронутый компонент, описывают сценарий атаки и включают этапы воспроизведения, рассматриваются более оперативно.

Компания не принимает и не рассматривает отчеты, сгенерированные автоматическими сканерами уязвимостей, а также отчеты о:

- CSRF-уязвимостях для некритичных действий (logout и другие);
- Уязвимостях типа Self-XSS без демонстрации реального воздействия на безопасность пользователей или систем;
- Framing- и clickjacking-уязвимостях без документированной серии кликов, подтверждающей существование уязвимости;
- Отсутствии механизма безопасности / несоответствии лучшим практикам без демонстрации реального воздействия на безопасность пользователей или систем;
- Отсутствии SSL/TLS, использовании небезопасных шифров SSL/TLS;
- Атаках, требующих полного доступа к паролям, токенам, профилю браузера или локальной системе;
- Раскрытии некритичной информации (такой, как версия продукта, протокола и т.д.);
- Ошибках, которые не затрагивают последние версии современных браузеров и ошибках, связанных с расширениями браузеров;
- Уязвимостях, которые затрагивают только пользователей с определенными браузерами;
- Атаках, требующих чрезвычайно маловероятного пользовательского взаимодействия;
- Атаках типа «отказ в обслуживании» или уязвимостях, связанных с ограничением частоты запросов;
- Временных атаках, которые доказывают существование учетной записи пользователя и т.п.;
- Небезопасных настройках cookie (для некритичных cookie);
- Ошибках в содержании / сервисах, которые не принадлежат или не управляются Компанией (сюда входят сторонние службы, работающие на субдоменах);
- Уязвимостях, которые Компания определяет, как уязвимости с приемлемым уровнем риска;
- Скриптинге или другой автоматизации, переборе предполагаемой функциональности и параметров.

Приложение 1

Стоимость вознаграждения (ориентировочная) в зависимости от классификации уязвимостей

№п/п	Классификация уязвимостей	Стоимость в рублях
1	Удалённое выполнение кода (RCE)	от 50 000 рублей;
2	Манипуляции с файлами, чтение/запись (LFR, RFI, XXE	от 50 000 рублей;
3	Инъекции (SQLi или эквивалент)	от 25 000 рублей;
4	Межсайтовый скриптинг (XSS)	от 5 000 рублей (кроме self-XSS);
5	Межсайтовая подделка запросов (CSRF, Flash crossdomain requests)	от 5 000 рублей;
6	Иное	от 1 рубля.

Приложение 2

Акт оказанных услуг

РФ, город Москва «___» _____ 2020 года

Общество с ограниченной ответственностью «Городской супермаркет», именуемое в дальнейшем «Компания», в лице Президента Сологуба Дениса Николаевича, действующего на основании Устава, с одной стороны, и Гражданин РФ _____ _____ (Ф.И.О.), именуемый(-ая) в дальнейшем «Исполнитель», с другой стороны, совместно именуемые «Стороны», составили настоящий Акт о нижеследующем:

1. Услуги по обнаружении уязвимостей Компании на условиях оферты, размещённой на сайте Компании от «7» июля 2020 года по ссылке: https://av.ru/lp/bugbonuty/, в период с 7 июля 2020 года по 1 августа 2020 года, оказаны в срок и в полном объеме.

2. Стоимость услуг составила _____ (_____) рублей. Стоимость включает в себя НДФЛ 13%

3. Стороны друг к другу претензий не имеют.

4. Настоящий Акт составлен в двух экземплярах, по одному для каждой Стороны.

Подписи Сторон:

От Компании

_____ Сологуб Д.Н.

От Исполнителя

_____

Приложение 3

Президенту

ООО «Городской супермаркет»

ИНН 7705466989

Сологубу Д.Н.

От _____ (Ф.И.О.)

Паспорт гражданина _____

Выдан (кем, когда) _____

_____

Адрес: _____

ИНН: _____

З А Я В Л Е Н И Е

о перечислении денежных средств физическому лицу

Прошу выплатить мне вознаграждение за оказание услуг по поиску уязвимостей на условиях оферты ООО «Городской супермаркет» в период с 7 июля 2020 года по 1 августа 2020 года, в сумме _____ (_____) рублей, включая НДФЛ 13%.

Денежные средства прошу мне перечислить по нижеследующим реквизитам:

Ф.И.О. Получателя: _____

_____ года рождения,

Зарегистрированный(-ая) по адресу: _____

Номер счета карты:

Банк:

БИК:

Корреспондентский счет:

ИНН:

КПП:

Дата: «___» _____ 2020 года

_____/_____ Подпись, расшифровка

Приложение 4

С О Г Л А С И Е

на обработку персональных данных

Я, _____ (Ф.И.О.),
проживающий по адресу (по месту регистрации) _____
паспорт гражданина _____, выдан (кем, когда) _____
_____ в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", даю своё согласие ООО «Городской супермаркет», ИНН 7705466989, ОГРН 1027705012312, юр. адрес: 115054, г. Москва, ул. Валовая, д. 8/18 на автоматизированную, а также без использования средств автоматизации, обработку моих персональных данных, включающих фамилию, имя, отчество, паспортные данные, ИНН в целях получения от ООО «Городской супермаркет» вознаграждения за оказание услуг по поиску уязвимостей на условиях оферты ООО «Городской супермаркет» в период с 7 июля 2020 года по 1 августа 2020 года.

Предоставляю ООО «Городской супермаркет» право осуществлять действия (операции) с моими персональными данными, включая сбор, хранение, уточнение (обновление, изменение), использование, блокирование, уничтожение.

Срок действия настоящего согласия — период времени до истечения установленных нормативными актами сроков хранения соответствующей информации.

Настоящее согласие на обработку персональных данных может быть отозвано в порядке, установленном Федеральным законом Российской Федерации от 27.07.2006 N 152-ФЗ "О персональных данных". В случае не предоставления согласия на обработку персональных данных или отзыва данного согласия, ООО «Городской супермаркет» не гарантирует исполнение своих обязательств в соответствии с вышеуказанной офертой .

Подпись субъекта персональных данных _____ _____

подпись *Ф.И.О.*

«___» _____ 20__ года.