УТВЕРЖДАЮ
Генеральный директор
ООО «ЯНДЕКС»

_____ Волож А.Ю.

01 декабря 2012

ПОЛОЖЕНИЕ О ПУБЛИЧНОМ КОНКУРСЕ «ОХОТА ЗА ОШИБКАМИ»
(Редакция № 2)

Москва, 2012

Оглавление

ПРЕАМБУЛА

Настоящее Положение (далее – Положение) регулирует порядок организации и проведения публичного конкурса «Охота за ошибками».

1. ТЕРМИНЫ

Далее по тексту Положения используются следующие термины:

1.1. КОНКУРС – конкурс «Охота за ошибками», проводимый Организатором в соответствии с Положением, Гражданским кодексом Российской Федерации, другими федеральными законами и иными нормативными правовыми актами Российской Федерации.

1.2. УЧАСТНИК – дееспособное и правоспособное физическое лицо, не состоящие в трудовых или иных договорных отношениях с Организатором или аффилированных с ним лиц, не являющееся автором кода, в котором обнаружена уязвимость, сообщившее Организатору о найденной уязвимости в соответствии с требованиями Положения.

1.3. УЯЗВИМОСТЬ - технический недостаток в веб-сервисах и мобильных приложениях Яндекса, используя который возможно нарушить целостность, доступность или конфиденциальность пользовательской информации.

1.4. ПОБЕДИТЕЛЬ – Участник, которого Конкурсная комиссия приняла решение наградить по итогам оценки обнаруженной им уязвимости.

2. ЦЕЛИ И ПРЕДМЕТ КОНКУРСА

2.1. Целями Конкурса являются привлечение внимания к вопросам информационной безопасности веб-сервисов и приложений и стимулирование исследований в этой области, а также развитие сообщества и популяризация данной отрасли в целом.

2.2. Предметом конкурса является поиск уязвимостей в веб-сервисах и мобильных приложениях Яндекса и его аффилированных лиц, перечисленных в п. 2.3 настоящего Положения, которые хранят, обрабатывают или каким-либо образом используют конфиденциальную информацию пользователей. Примерами конфиденциальной информации могут быть аутентификационные данные, переписка, фото- и видеоальбомы. В отношении веб-сервисов Яндекса, расположенных в доменах yandex.net, yandex.st принимаются сообщения о найденных уязвимостях только вида "Инъекции" или "Ошибки конфигурации веб-окружения".

2.3. Объектами для поиска уязвимостей в рамках Конкурса являются:

2.3.1. Веб-сервисы Яндекса и его аффилированных лиц, расположенные в доменах yandex.ru, yandex.com, yandex.com.tr, yandex.kz, yandex.ua, yandex.by, yandex.net, yandex.st, ya.ru, moikrug.ru (кроме доменов сервиса "Яндекс.Народ")

2.3.2. Мобильные приложения для iOS и Android:

- Яндекс.Карты;
- Яндекс.Навигатор;
- Яндекс.Музыка;
- Яндекс.Такси;
- Яндекс.Почта;
- Яндекс.Маркет;

- Яндекс.Метро;
- Яндекс.Фотки;
- Яндекс.Электрички
- Яндекс.Диск.

3. ОРГАНИЗАТОР КОНКУРСА

3.1. Организатором Конкурса является Общество с ограниченной ответственностью «ЯНДЕКС».

3.2. Сведения об Организаторе:

Юридический адрес: 119021, Россия, г. Москва, ул. Льва Толстого, д. 16
ОГРН: 1027700229193
ИНН: 7736207543
КПП: 997750001
р/счет 40702810300001003838 в «ИНГ БАНК (ЕВРАЗИЯ) ЗАО»
к/счет 30101810500000000222 в ОПЕРУ Московского ГТУ Банка России
БИК 044525222

4. СРОКИ КОНКУРСА

4.1. Сообщения о найденных уязвимостях принимаются с 21 сентября 2012 года по 31 декабря 2017 года (включительно).
4.2. Итоги Конкурса подводятся ежеквартально.
4.3. Выплата наград победителям производится в порядке и сроки, предусмотренные в разделе 9 Положения.

5. ИНФОРМИРОВАНИЕ ОБ УСЛОВИЯХ КОНКУРСА

5.1. Организатор размещает условия Конкурса по адресу: http://company.yandex.ru/security/.

6. ПОРЯДОК УЧАСТИЯ В КОНКУРСЕ

6.1. Сообщения о найденных уязвимостях направляются Организатору через форму https://company.yandex.ru/security/report.xml или по адресу: security-report@yandex-team.ru. Сообщение о найденной уязвимости считается полученным Организатором на следующий рабочий день после отправки сообщения Участником.

6.2. Организатор вправе запросить у Участников следующие сведения:

– фамилия, имя, отчество;

– адрес электронной почты;

– контактный телефон.

6.3.Направляя Организатору сообщение о найденных уязвимостях в порядке, предусмотренном п. 6.1. Положения, и становясь Участником Конкурса, Участник дает согласие на обработку Организатором персональных данных, предоставленных Организатору в порядке, предусмотренном п.п. 6.2., 9.3. и 9.4. Положения, любыми способами в том числе на совершение Организатором действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», а также на размещение фамилии, имени, отчества Участника (или псевдонима по выбору Участника) на английском языке в разделе «Зал славы» на сайте Организатора, в случае принятия Комиссией решения о награждении Участника. Данное согласие действует в течение 5 (пяти) лет и может быть отозвано Участником путем направления письменного уведомления об отзыве согласия на обработку персональных

данных по адресу 119021, Москва, ул. Льва Толстого, дом 16.

7. ПОРЯДОК И КРИТЕРИИ ОЦЕНКИ УЯЗВИМОСТЕЙ

7.1. Для оценки уязвимостей создается конкурсная комиссия из сотрудников Организатора. Персональный состав Комиссии утверждается Генеральным директором Организатора.

7.2. Оценка уязвимостей для целей принятия решения о выплаты награды Участнику складывается из следующих факторов:

– критичность того или иного веб-сервиса или мобильного приложения Организатора, в котором обнаружена уязвимость;

– классификации уязвимости по OWASP Top-10 для веб-сервисов и OWASP Mobile Top-10 для мобильных приложений;
– субъективная оценка Комиссии об уровне сложности обнаружения и эксплуатации уязвимости.

7.3. Окончательное решение о выплате или об отказе в выплате награды Участнику Комиссия принимает по собственному усмотрению.

7.4.Организатор сообщает Участнику о результатах оценки найденной уязвимости и о принятом Комиссией решении не позднее 30 (тридцати) дней с даты получения Организатором сообщения от Участника об обнаруженной уязвимости.

8. РАЗМЕР НАГРАДЫ

8.1. Размер награды победителей за найденные уязвимости зависит от веб-сервиса или мобильного приложения, в котором они были обнаружены и классификации уязвимостей.

8.2. Сервисы Яндекса делятся на две группы: критичные и прочие сервисы. В перечень критичных сервисов входят:

- Паспорт;
- Яндекс.Почта;
- Яндекс.Карты;
- Яндекс.Календарь;
- Яндекс.Диск;
- МойКруг;
- Главная страница Яндекса;
- Страница поисковой выдачи.

8.3. Награды за найденные уязвимости в веб-сервисах устанавливаются в следующем размере:

Классификация уязвимости по OWASP Top-10	**Критичные сервисы**	**Прочие сервисы**
A01. Инъекции	30000 руб.	25000 руб.
A02. Межсайтовый скриптинг – A05. Межсайтовая подделка запросов	10000 руб.	5000 руб.
A06. Ошибки конфигурации веб-окружения – A10. Открытое перенаправление	5000 руб.	3000 руб.

8.4. Мобильные приложения делятся на две группы: критичные и прочие приложения. В перечень критичных мобильных приложений входят:

- Яндекс.Карты;
- Яндекс.Навигатор;
- Яндекс.Музыка;
- Яндекс.Почта;
- Яндекс.Маркет.

8.5. Награды за найденные уязвимости в мобильных приложениях устанавливается в следующем размере:

Классификация уязвимости по OWASP Mobile Top-10	**Критичные приложения**	**Прочие приложения**
M01. Небезопасное хранилище данных – M05. Недостатки в механизмах аутентификации и авторизации	10000 руб.	5000 руб.
M06. Недостатки в управлении сессией – M08. Утечка данных	5000 руб.	3000 руб.

8.6. Организатор оставляет за собой право в особых случаях повысить размер награды.

8.7. Награда за обнаруженные уязвимости вида XSS и CSRF выплачивается только в случае, если их эксплуатация не требует иных действий пользователя, кроме как перехода на специально сформированную страницу, и затрагивает чувствительные данные пользователя.

8.8. Суммы наград, указанные в пп. 8.3 и 8.5 настоящего Положения, указаны за вычетом налога на доходы физических лиц (НДФЛ), который будет начислен и уплачен Яндексом в соответствии с законодательством РФ.

9. ПОРЯДОК ВЫПЛАТЫ НАГРАДЫ

9.1. Выплата награды осуществляется Организатором не позднее 3 (трех) месяцев со дня сообщения Организатором Участнику о результатах оценки найденной уязвимости в соответствии с п. 7.4. Положения и при условии предоставления Победителем документов, перечисленных в п. 9.3. или п.9.4 настоящего Положения.

9.2. Выплата награды, осуществляется одним из следующих способов по выбору Победителя:

9.2.1. через систему «Яндекс.Деньги»;

9.2.2. путем банковского перевода денежных средств на банковский счет Победителя. При этом в случае, если Победителем является иностранный гражданин, перевод денежных средств на банковский счет осуществляется в долларах США по курсу ЦБ РФ на дату выплаты денежных средств.

9.3. Для получения награды, через систему «Яндекс.Деньги» Победителю необходимо в течение 10 (десяти) рабочих дней с даты получения сообщения от Организатора, указанного в п. 7.4 Положения, предоставить Организатору следующую информацию:

9.3.1. Номер счета Победителя в Яндекс.Деньгах;

9.3.2. Сканированную копию документа, удостоверяющего личность (Для граждан РФ - разворот с личными данными, а также страницу с адресом места жительства

(прописки). Для иностранных граждан - разворот с личными данными, страницы с российскими визами (если Вы фактически проживаете в России), а также информацию об адресе Вашего места жительства);

9.4. Для получения награды путем банковского перевода денежных средств Победителю необходимо в течение 10 (десяти) рабочих дней с даты получения сообщения от Организатора, указанного в п. 7.4 Положения, предоставить Организатору следующие документы и информацию:

9.4.1. Сканированную копию документа, удостоверяющего личность (Для граждан РФ - разворот с личными данными, а также страницу с адресом места жительства (прописки). Для иностранных граждан - разворот с личными данными, страницы с российскими визами (если Вы фактически проживаете в России), а также информацию об адресе Вашего места жительства),

9.4.2. Реквизиты рублевого или валютного банковского счета Победителя;

9.5. Документы и информация предоставляются Победителем Организатору в офисе Организатора по адресу: 119021, Москва, ул. Льва Толстого, дом 16, в рабочие дни с 10-00 до 19-00, по почте по адресу 119021, Москва, ул. Льва Толстого, дом 16 (с пометкой «Поиска уязвимостей в Яндексе, 2012») или через форму https://company.yandex.ru/security/reward.xml.

9.6. В случае не предоставления документов и информации, перечисленных в пп. 9.3 или 9.4 Положения, в полном объеме, и/или не обращения за наградой в течение срока, указанного в пп. 9.3 или 9.4 Положения, а также в случае предоставления Победителем Организатору недостоверной информации, награда Победителю не выплачивается.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Конкурс проводится в соответствии с законодательством Российской Федерации.

10.2. Сообщение участником о найденной уязвимости в порядке, предусмотренном п. 6.1 Положения, означает безоговорочное согласие Участника со всеми условиями Конкурса, а также Политикой ответственного разглашения информации, размещенной в сети Интернет по адресу http://company.yandex.ru/security/policy.xml.

10.3. Во всем, что не урегулировано Положением, Организатор и Участники руководствуются действующим законодательством Российской Федерации.

10.4. Все споры и разногласия, которые возникают в связи с участием в Конкурсе, подлежат разрешению путем переговоров. Спорные вопросы, не урегулированные путем переговоров, подлежат разрешению в суде по месту нахождения Организатора.

10.5 Положение составлено на русском и английском языках. При толковании версия Положения на русском языке имеет преимущественную силу.