**Портал государственных и муниципальных услуг Московской области**

**Раздел «Здоровье» портала государственных и муниципальных услуг МО (**[**zdrav.mosreg.ru**](https://zdrav.mosreg.ru/)**)**

Участник программы получает уникальное строковое значение, которое должен использовать в виде HTTP-заголовка X-BugBounty-Id: 00-00-00. Данное строковое значение не подлежит разглашению. Выданный HTTP-заголовок должен быть добавлен к каждому HTTP-запросу, который отправляет участник программы с целью выявить уязвимость. При отсутствии данного заголовка, а также в случае его разглашения третьим лицам, вознаграждение не выплачивается, а атака может считаться несанкционированной атакой на систему.

Программа действует с 22 апреля 2024 00:00 до 20 мая 23:59 2024 года

**## Правила для нас**

Мы уважаем время и усилия наших исследователей;

Мы отвечаем в течение 5 рабочих дней;

Мы обрабатываем отчеты в течение 15 рабочих дней после ответа;

Мы можем увеличить сроки обработки отчетов, но в таком случае мы проинформируем вас о задержке;

Мы определим сумму вознаграждения в течение 15 рабочих дней после обработки, обращаем внимание, что общий фонд вознаграждений ограничен;

Мы сделаем все возможное, чтобы в процессе обработки отчета вы были в курсе нашего прогресса.

**## Правила для вас**

Будьте этичным хакером и уважайте конфиденциальность других пользователей;

Старайтесь избегать нарушений конфиденциальности, уничтожения данных, а также прерывания или ухудшения качества наших услуг;

Инструменты автоматического сканирования должны быть ограничены 10 запросами в секунду к одному целевому узлу, суммируя все инструменты и потоки, работающие параллельно;

Перед началом исследований ознакомьтесь с правилами, указанными в этой программе;

Старайтесь эффективно представлять информацию об уязвимостях;

В случае если эксплуатация уязвимости в производственной среде Заказчика может привести к нарушению бизнес- и технологических процессов Заказчика, Участник обязуется воздержаться от действий по эксплуатации такой уязвимости и указать в направляемом им отчете все данные, необходимые для проверки возможности эксплуатации найденной уязвимости вне производственной среды;

Если при исследовании сервисов портала государственных и муниципальных услуг Московской области вы обнаружили несколько проблем безопасности, подготовьте отчеты о каждой из выявленных уязвимостей отдельно.

**## Размеры вознаграждений в зависимости от критичности (будет находиться в отдельной панели)**

Критический: 35 000 – 75 000

Высокий: 15 000 – 35 000

Средний: 5 000 – 15 000

Низкий: 0 – 5 000

Отсутствует: 0 - 0

**## Принимаемые языки**

\* Русский

**## Область действия программы**

\* https://[**zdrav.mosreg.ru**](https://zdrav.mosreg.ru/).

**## Политика раскрытия информации**

Раскрытие информации не предусмотрено

**Мы НЕ выплачиваем вознаграждение за:**

* отчеты сканеров безопасности и других автоматизированных инструментов;
* информацию об IP-адресах, DNS-записях и открытых портах;
* проблемы и уязвимости, которые основаны на версии используемого продукта, без демонстрации их эксплуатации;
* уязвимости, эксплуатацию которых блокируют СЗИ, без демонстрации обхода СЗИ (например WAF);
* отчеты о небезопасных шифрах SSL и TLS без демонстрации их эксплуатации;
* уязвимости, информацию о которых ранее передали другие участники конкурса (дубликаты отчетов);
* уязвимости 0-day и 1-day, о которых стало публично известно менее 30 дней назад, и уязвимости с CVSS выше 8, о которых стало известно менее 14 дней назад;
* Self-XSS и другие уязвимости, напрямую не влияющие на пользователей или данные приложения.
* Уязвимости, для которых требуются версии браузера, выпущенные за 6 и более месяцев (либо прекращена поддержка) до представления отчета;
* Ошибки в настройке CORS без демонстрации их эксплуатации;
* Разглашение информации о существовании в системе данного имени пользователя, email или номера телефона;
* Разглашение технической или нечувствительной информации (например, версии продукта или используемого ПО, stacktrace);
* Tabnabbing;
* Clickjacking;
* Отчеты, связанные с CSP, для доменов без CSP и доменных политик с небезопасными eval и/или небезопасными inline;
* Атаки, требующие полного доступа к локальной учетной записи или профилю браузера;
* Раскрытие конфиденциальной информации пользователей через внешние ресурсы, не контролируемые Порталом государственных и муниципальных услуг Московской области, например данные со шпионского ПО;
* Уязвимости, требующие выполнения сложного или маловероятного сценария взаимодействия с пользователем;
* Отсутствие лучших практик в конфигурации DNS и почтовых сервисов (DKIM/DMARC/SPF/TXT);
* Неработающие ссылки на страницы социальных сетей или невостребованные ссылки в социальных сетях и подобные страницы;
* Возможность выполнить действие, недоступное через пользовательский интерфейс, без выявленных рисков безопасности;
* Возможность создавать учетные записи пользователей без каких-либо ограничений;
* Перечисление пользователей;
* Разглашение публичной информации о пользователях;
* Отсутствие уведомлений о важных действиях пользователя.
* Утечка конфиденциальных маркеров (например, маркера сброса пароля) доверенным
* третьим лицам по защищенному соединению (HTTPS);
* Проблемы, никак не связанные с безопасностью (если вы обнаружите проблемы не связанные с безопасностью, направляйте их в техническую поддержку https://support.mosreg.ru/)
* Отсутствие механизма защиты или лучших практик без демонстрации реального влияния на безопасность пользователя или системы принимаются как информативные (например: отсутствие HTTP заголовков безопасности (CSP, HSTS, и т.д.), флагов безопасности cookie (HttpOnly, Secure и т.д.) или защиты от CSRF, SSL сертификатов);

**## Требования к участникам**

Участвовать в программе могут все заинтересованные исследователи в возрасте от 18 лет.

Исследователи в возрасте от 14 до 18 лет имеют право участвовать в программе только при наличии письменного согласия родителей или законного представителя.

Сотрудники портала государственных и муниципальных услуг Московской области и члены их семей не могут участвовать в программе. Так же существует запрет на участие для контрагентов с действующими договорами на разработку ПО, эксплуатацию и/или оказание услуги в области информационной безопасности.

**##Обязанности портала государственных и муниципальных услуг Московской области:**

* Отдавать приоритет задачам безопасности, оперативно подходить к устранению обнаруженных уязвимостей.
* Уважать исследователей, не препятствовать раскрытию информации об отчете без четких на то оснований.
* Не выдвигать исследователям необоснованные обвинения, связанные с участием в конкурсе.
* Публичное раскрытие информации об уязвимости
* Публичное раскрытие по взаимному соглашению. Портал государственных и муниципальных услуг Московской области обязуется открыто общаться с исследователями о сроках раскрытия информации. Стороны могут выбрать время, в которое будет обнародовано содержание отчета.
* Окончательное решение о раскрытии информации об уязвимости остается за Заказчиком.

**## Недопустимые действия**

**Исследователям запрещено:**

* Получать доступ к данным другого пользователя без его согласия, изменять и уничтожать их, а также раскрывать любую конфиденциальную информацию, случайным образом полученную в ходе поиска уязвимостей или их демонстрации. Преднамеренный доступ к этой информации запрещен и может быть признан незаконным.
* Воздействовать на учетные записи других пользователей без их разрешения.
* Использовать обнаруженную уязвимость в личных целях.
* Использовать инструменты тестирования уязвимостей, автоматически генерирующие значительные объемы трафика и приводящие к атакам с исчерпанием ресурсов.
* Проводить атаки, наносящие вред целостности и доступности сервисов (например, DoS-атаки, брутфорс-атаки), пытаться эксплуатировать уязвимость, нацеленную на исчерпание ресурсов. Следует сообщить о проблеме команде по безопасности портала государственных и муниципальных услуг Московской области которая проведет атаку в тестовой среде.
* Проводить физические атаки на персонал, дата-центры и офисы компании.
* Проводить атаки на системы портала государственных и муниципальных услуг Московской области с использованием техник социальной инженерии (фишинг, вишинг и т. д.) и спам-рассылок клиентам, партнерам и сотрудникам.
* Исследовать серверную инфраструктуру, где размещены веб-приложения.
* Разглашать сведения об уязвимости до их публичного раскрытия порталом государственных и муниципальных услуг Московской области.
* осуществлять физическое вмешательство в инфраструктуру Заказчика (в том числе в офисы и вычислительные центры);
* использовать методы социальной инженерии, направленной как на работников Заказчика, так и на работников Исполнителя;
* совершать попытки получения доступа к учетным записям, данным пользователей ИС Заказчика или к любым другим конфиденциальным данным, выходящим за пределы действий, минимально необходимых для демонстрации найденной уязвимости;
* реализовывать уязвимости в производственной среде Заказчика, способные привести к нарушению бизнес- и технологических процессов Заказчика (включая DoS-атаки и другие атаки типа «отказ в обслуживании»);
* проникновение во внутренние системы веб-сервисов и приложений ИС Заказчика, а также иных информационных ресурсов Заказчика, не указанных в настоящем техническом задании. Поиск уязвимостей в веб-сервисах и приложениях ИС Заказчика, в рамках Программы размещенной на Платформе, должен заканчиваться взломом порталов и закреплением на них, строго без дальнейшего проникновения Участником во внутренние системы веб-сервисов и приложений ИС Заказчика;
* осуществлять целенаправленную выгрузку персональных данных граждан из внутренних систем веб-сервисов и приложений ИС Заказчика, а также иных информационных ресурсов Заказчика, не указанных в настоящем техническом задании;

**Политика тестирования RCE**

Тестирование уязвимостей, которые могут приводить к удаленному исполнению кода, должно выполняться в соответствии с изложенными ниже правилами:

Во время тестирования запрещены любые действия на сервере кроме:

* Выполнения команд ifconfig (ipconfig), hostname, whoami, id;
* Чтения содержимого файлов /etc/passwd и /proc/sys/kernel/hostname ("drive:/boot.ini, drive:/install.ini);
* Создания пустого файла в каталоге текущего пользователя.
* При необходимости проведения иных действий необходимо предварительно согласовать их с нашими специалистами безопасности.

**Политика тестирования SQL инъекций**

Тестирование уязвимостей, которые могут приводить к внедрению команд SQL, должно выполняться в соответствии с изложенными ниже правилами:

Во время тестирования запрещены любые действия на сервере кроме:

* Получения данных о текущей БД (SELECT database()), ее версии (SELECT @@version), текущего пользователя (SELECT user(), SELECT system\_user()) или имени хоста (SELECT @@hostname);
* Получения схемы БД (SELECT table\_schema), списка таблиц в ней (SELECT table\_name) и имен столбцов в таблицах (SELECT column\_name);
* Выполнения математических, конверсионных или логических запросов (включая использование SLEEP) без извлечения данных (кроме тех, что перечислены выше).

При необходимости проведения иных действий необходимо предварительно согласовать их с нашими специалистами безопасности.

**Политика загрузки и чтения файлов**

Тестирование уязвимостей, которые могут приводить к чтению произвольных файлов на сервере или произвольной загрузке файлов, должно выполняться в соответствии с изложенными ниже правилами:

Запрещенные действия при загрузке файлов:

* Изменение, модификация, удаление и замена любых файлов на сервере (включая системные), кроме тех, что ассоциированы с вашей учетной записью либо с учетной записью пользователя, который явно выразил свое согласие;
* Загрузка файлов, которые могут вызвать отказ в обслуживании (например, файлов большого размера);
* Загрузка вредоносных файлов (например, малвари или шпионского ПО).
* При получении возможности чтения произвольных файлов на сервере запрещены любые действия кроме чтения таких файлов, как /etc/passwd и /proc/sys/kernel/hostname (drive:/boot.ini, drive:/install.ini). При необходимости проведения иных действий необходимо предварительно согласовать их с нашими специалистами.