LD

Bug bounty [2025]

Программа компании LiveDune, которая предлагает вознаграждение людям за нахождение и
сообщение о ошибках (багах) и уязвимостях в их программном обеспечении или системах.

Структура

Область действий

1. Где искать уязвимости? →
2. Какие уязвимости искать? →
3. Что не нужно присылать? →
4. Что не претендует на вознаграждение? →

Вознаграждения

1. Таблица выплат →

Правила участия

1. Общие правила →
2. Правила тестирования →
3. Политика раскрытия информации об уязвимостях →
4. Политика тестирования RCE →
5. Политика тестирования SQL инъекций →
6. Политика загрузки и чтения файлов →

2. Определение критичности уязвимости →
3. Примечания →

FAQ

1. Как составить хороший отчет? →
2. Предоставляются ли учетные данные для тестирования? →
3. Как и в какие сроки проверяются отчеты? →
4. Как осуществляется работа с дубликатами? →

Область действий

Где искать уязвимости?

Уязвимости можно искать на нашем ресурсе, а именно: *.livedune.com. Однако максимальные выплаты предусмотрены только за обнаружение проблем в указанных ниже сервисах. Для всех остальных ресурсов выплаты будут снижены (в некоторых случаях до нуля). Эти сервисы включают основные домены.

Какие уязвимости искать?

Мы в первую очередь заинтересованы в нахождении критических уязвимостей на сервере и в сервисе, однако мы также приветствуем обнаружение других типов уязвимостей. Если у вас есть сомнения, стоит ли сообщать о найденной проблеме, проверьте ее наличие в списке "Что не нужно присылать?". Если ваша проблема там не указана, не стесняйтесь

отправлять отчет с подробным описанием. Инструкции о том, как лучше сообщить о уязвимости, можно найти в разделе FAQ.

Ниже приведены примеры уязвимостей, за обнаружение которых мы готовы выплатить вознаграждение (приведенный список не исчерпывающий):

- Удаленное исполнение кода (RCE);
- Инъекции (например, SQL-инъекции или XML-инъекции);
- LFR/LFI/RFI;
- SSRF;
- Утечки памяти;
- Уязвимости бизнес-логики;
- IDOR;
- Уязвимости контроля доступа;
- Раскрытие чувствительной информации;
- Угон аккаунта;
- Недостатки аутентификации/авторизации;
- XSS и CSRF с воздействием на чувствительные данные.

Что не нужно присылать?

- Проблемы, никак не связанные с безопасностью
- Сообщения об уязвимостях в сервисах, не относящихся к LiveDune;
- Сообщения о возможных DDOS-атаках;
- Информацию об IP-адресах, DNS-записях и открытых портах;
- Отчеты сканеров уязвимостей и других автоматизированных средств;
- Сообщения о публично доступных панелях входа;

Что не претендует на вознаграждение?

- Self-XSS, XSS в непопулярных или устаревших браузерах, Flash-based XSS;
- CSRF и XSS без воздействия на чувствительные данные;
- Отсутствие рекомендованных механизмов защиты* (например, HTTP заголовков безопасности, флагов безопасности cookie или защиты от CSRF);
- Ошибки в настройке CORS*;
- Использование устаревшего или потенциально уязвимого стороннего ПО*;
- Атаки, связанные с мошенничеством или кражей;
- Возможность неограниченной отправки СМС и email;
- Атаки типа DOS*;
- Небезопасно сконфигурированные TLS или SSL*;
- Разглашение информации о существовании в системе данного имени пользователя, email или номера телефона;
- Full Path Disclosure;
- Разглашение технической или нечувствительной информации* (например, версии продукта или используемого ПО, stacktrace);
- Open Redirect без дополнительного вектора атаки (например, кражи токена авторизации);
- Подмена контента на странице;
- Tabnabbing;
- Уязвимости, требующие выполнения сложного или маловероятного сценария взаимодействия с пользователем;
- Уязвимости, необходимым условием эксплуатации которых является наличие вредоносного ПО, root-прав или jailbreak на устройстве;
- Атаки, требующие MITM чужого соединения или физической близости с чужим устройством (например, атаки через NFC, Bluetooth, Wi-Fi и shoulder surfing);

- Маловероятные или теоретические атаки без доказательств возможности их осуществления

> 💡 * — без детального описания вектора атаки и доказательств потенциального нанесения ущерба или вреда.

Правила участия

Участвуя в нашей bug-bounty программе, вы подтверждаете, что прочитали и согласились с "Правилами Участия". Нарушение любого из этих правил может привести к лишению права на вознаграждение.

Общие правила

- Если у вас возникли проблемы, которые не связаны с безопасностью, пожалуйста, обратитесь в службу поддержки клиентов, поскольку bug-bounty программа компании ограничивается только техническими уязвимостями в её сервисах.
- При нахождении 0-day или 1-day уязвимости, чей патч был выпущен менее недели назад, выплата вознаграждения будет рассмотрена командой безопасности LiveDune по каждому конкретному случаю.

Правила тестирования

- Для проведения тестирования используйте только свои собственные учетные записи либо учетные записи пользователей, который явно выразили свое согласие. Не пытайтесь получить доступ к чужим аккаунтам или любой конфиденциальной информации.

- Во время поиска уязвимостей следует избегать нарушения конфиденциальности, целостности и доступности информации в наших сервисах.
- Запрещена любая деятельность, которая может нанести ущерб приложениям компании, ее инфраструктуре, клиентам и партнерам. Примеры запрещенных действий: социальная инженерия, фишинг, атаки типа "Отказ в обслуживании", физическое воздействие на инфраструктуру.
- Для подтверждения наличия уязвимости используйте минимально возможный POC (Proof of Concept). В случае, если это может повлиять на других пользователей или же работоспособность системы, свяжитесь с нами для получения разрешения. Дальнейшая эксплуатация уязвимостей строго запрещена.
- Автоматическое сканирование должно быть ограничено 3 запросами в секунду.

Политика раскрытия информации об уязвимостях

- Запрещено раскрывать уязвимости или делиться какими-либо подробностями без письменного разрешения команды безопасности LiveDune.
- Мы оставляем за собой право отклонить любой запрос на публичное раскрытие отчета.

Политика тестирования RCE

Тестирование уязвимостей, которые могут приводить к удаленному исполнению кода, должно выполняться в соответствии с данной политикой.

Во время тестирования запрещены любые действия на сервере кроме:

- Выполнения команд `ifconfig` (`ipconfig`), `hostname`, `whoami` ;
- 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 командой безопасности LiveDune.

Политика тестирования SQL инъекций

Тестирование уязвимостей, которые могут приводить к внедрению команд SQL, должно выполняться в соответствии с данной политикой.

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 командой безопасности LiveDune.

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 данной политикой.

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 командой безопасности LiveDune.

Вознаграждения

Мы выплачиваем вознаграждения внешним исследователям безопасности только за обнаружение ранее неизвестных проблем при выполнении всех "Правил участия".

Все отчеты о уязвимостях анализируются по отдельности, учитывая критичность системы, в которой обнаружена уязвимость, и критичность самой уязвимости. Ниже приведена таблица максимальных вознаграждений.

Таблица выплат

Критичность	Critical	High	Medium	Low
Максимальная выплата	100 000 ₽	50 000 ₽	25 000 ₽	7 500 ₽

Определение критичности уязвимости

Мы оставляем за собой право принимать окончательное решение в отношении серьезности найденной уязвимости. После получения отчета мы

проводим внутреннее расследование и определяем степень критичности, учитывая множество факторов, в том числе:

- Уровень привилегий, необходимый для реализации атаки;
- Трудность обнаружения и эксплуатации;
- Наличие требования взаимодействия с пользователем;
- Влияние на целостность, доступность и конфиденциальность затронутых данных;
- Влияние на бизнес-риски и репутационные риски;
- Количество затронутых пользователей.

Примечания

- Почта для связи: bug-hunters@livedune.com;
- При отправке письма на почту, указывайте тему письма “bug-hunter”
- Вознаграждение выплачивается только в случае, если команда безопасности LiveDune посчитает, что все условия правил выполнены и выявленная уязвимость является значимой;
- Размер выплаченной награды является окончательным и не подлежит обсуждению.

FAQ

Как составить хороший отчет?

Один отчет должен описывать одну уязвимость. Исключением являются те случаи, когда уязвимости либо связаны между собой, либо их можно скомбинировать в цепочку.

Хороший отчет об уязвимости должен включать в себя следующие составляющие:

- Описание уязвимости;
- Шаги воспроизведения;
- Анализ критичности;
- Рекомендации по устранению.

В отчете также должны содержаться:

- URL уязвимого приложения;
- Тип обнаруженной уязвимости;
- Скриншоты или видеозапись, подтверждающие наличие уязвимости и демонстрирующие шаги воспроизведения;
- Пример форматированного запроса из BurpSuite (или любой другой POC);
- В некоторых случаях куски кода.

Несоблюдение минимальных требований может привести к снижению суммы вознаграждения. Если в отчете недостаточно данных, чтобы проверить наличие уязвимости, выплата вознаграждения не осуществляется.

Вся информация о найденной уязвимости (включая вложения) должна храниться только в отчете, который вы отправляете. Не размещайте ее на внешних ресурсах.

Предоставляются ли учетные данные для тестирования?

Мы не выдаем дополнительные доступы и учетные данные (включая тестовые). Используйте собственные аккаунты для проведения тестирования.

Как и в какие сроки проверяются отчеты?

Отчеты об уязвимостях проверяются нашей внутренней командой безопасности. Время ответа зависит от загруженности, однако мы стараемся прикладывать все усилия, чтобы обработать запрос в течение двух недель.

Как осуществляется работа с дубликатами?

Мы выплачиваем вознаграждение только за первый полученный отчет (при условии, что он содержит всю необходимую информацию для воспроизведения уязвимости). Любые последующие отчеты, затрагивающие ту же уязвимость, будут помечаться как дублирующие. Отчеты, содержащие схожие векторы атак также могут считаться дублирующими, в случае если команда безопасности считает, что информации из одного отчета достаточно для исправления всех зарегистрированных векторов атак или ошибок. Отчет может быть дубликатом отчета другого исследователя или отчета внутренней команды безопасности.