ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ PSYCHOLOG-TUT.RU

№	Сайт	Уязвимость	Тест-кейсы	Баг-репорт	Отчёт QA инженер
1	https://psycholog-tut.ru/index.html	SQL-Injection	1. Проверка корректной отправки номера телефона при вводе обычного номера телефона. 2. Проверка возможности ввода SQL-запроса в поле номера телефона. 3. Проверка поведения системы при вводе некорректного формата номера телефона.	**Название:** Уязвимость SQL-инъекции в блоке ввода номера телефона **Описание:** При вводе SQL-запроса в поле номера телефона, сайт возвращает данные из базы данных. `SELECT * FROM clients` — Сайт возвращает 'Вскоре с вами свяжутся по этому номеру: ' и ответ содержит в себе данные из базы данных. **Ожидаемое поведение:** Сайт не должен выполнять SQL-запросы, введенные пользователем в поле номера телефона.	Выявлена уязвимость SQL-инъекции в блоке ввода номера телефона. При вводе SQL-запроса в поле номера телефона сайт выдает базу клиентов. Уязвимость может привести к утечке конфиденциальной информации и потенциальному нарушению безопасности данных пользователей. Рекомендуется немедленно исправить данную уязвимость путем использования параметризованных запросов или других методов защиты от SQL-инъекций.
2	https://psycholog-tut.ru/index.html	Sensitive Data Exposure (SDX)	1. Проверка корректной отправки номера телефона при вводе обычного номера телефона. 2. Проверка возможности ввода `'{{return "/requirements.txt"}}'` в поле номера телефона. 3. Проверка поведения системы при вводе некорректного формата номера телефона.	**Название:** Уязвимость в блоке ввода номера телефона **Описание:** При вводе `'{{return "/requirements.txt"}}'` в поле номера телефона, сайт возвращает данные из файла requirements.txt. Сайт возвращает 'Вскоре с вами свяжутся по этому номеру: ' и ответ содержит в себе данные из файла requirements.txt. **Ожидаемое поведение:** Сайт не должен выполнять некорректные запросы, введенные пользователем в поле номера телефона.	Обнаружена уязвимость SDX в блоке ввода номера телефона. При вводе `'{{return "/requirements.txt"}}'` в поле номера телефона, сайт возвращает данные из файла requirements.txt. Уязвимость может привести к утечке конфиденциальной информации. Рекомендуется немедленно исправить данную уязвимость путем корректного управления доступом к файлам и ресурсам.
3	https://psycholog-tut.ru/index.html	Insecure Direct Object References (IDOR)	1. Проверка корректной отправки номера телефона при вводе обычного номера телефона. 2. Проверка возможности ввода `'{{return os.system("hostnamectl && uname -s && uname -o")}}'` в поле номера телефона. 3. Проверка поведения системы при вводе некорректного формата номера телефона.	**Название:** Уязвимость в блоке ввода номера телефона **Описание:** При вводе `'{{return os.system("hostnamectl && uname -s && uname -o")}}'` в поле номера телефона, сайт возвращает данные о системе. Сайт возвращает 'Вскоре с вами свяжутся по этому номеру: ' и ответ содержит в себе данные о системе. **Ожидаемое поведение:** Сайт не должен выполнять системные команды, введенные пользователем в поле номера телефона.	Обнаружена уязвимость IDOR в блоке ввода номера телефона. При вводе `'{{return os.system("hostnamectl && uname -s && uname -o")}}'` в поле номера телефона, сайт возвращает данные о системе. Уязвимость может привести к утечке конфиденциальной информации о сервере. Рекомендуется немедленно исправить данную уязвимость путем корректного управления доступом к системным ресурсам.
4	https://psycholog-tut.ru/index.html	XSS	1. Проверка корректной отправки номера телефона при вводе обычного номера телефона. 2. Проверка возможности ввода `'<script>window.location.href="https://gb.com"</script>'` в поле номера телефона. 3. Проверка поведения системы при вводе некорректного формата номера телефона.	**Название:** Уязвимость XSS в блоке ввода номера телефона **Описание:** При вводе `'<script>window.location.href="https://gb.com"</script>'` в поле номера телефона, скрипт выполняется при отображении страницы. Фронтенд произвольно использует JS код. **Ожидаемое поведение:** Сайт должен фильтровать вводимые данные и не допускать выполнения XSS скриптов.	Обнаружена уязвимость XSS в блоке ввода номера телефона. При вводе `'<script>window.location.href="https://gb.com"</script>'` в поле номера телефона, скрипт выполняется при отображении страницы. Уязвимость может привести к внедрению вредоносного кода на страницу и выполнению нежелательных действий на стороне клиента. Рекомендуется немедленно исправить данную уязвимость путем использования механизма фильтрации и экранирования вводимых данных.
	https://psycholog-	Insufficient Logging and	1. Проверка логирования и мониторинга при вводе обычного номера телефона. 2. Проверка логирования и мониторинга при отсутствии	**Название:** Уязвимость недостаточного логирования и мониторинга в блоке ввода номера телефона **Описание:** Сайт не логирует и не мониторит запросы к серверу и действия пользователей при вводе номера	Обнаружена уязвимость недостаточного логирования и мониторинга в блоке ввода номера телефона. Сайт не логирует и не мониторит запросы к серверу и действия пользователей. Уязвимость может привести к

5	tut.ru/index.html	Monitoring (ILM)	ввода в поле номера телефона. 3. Проверка поведения системы при вводе некорректного формата номера телефона.	телефона. **Ожидаемое поведение:** Сайт должен логировать и мониторить все запросы к серверу и действия пользователей.	незамеченному выполнению вредоносных действий. Рекомендуется немедленно исправить данную уязвимость путем внедрения механизма логирования и мониторинга всех запросов и действий пользователей.