Наименование тест-кейса	*ТС-001: Проверка использования не безопасного соединения - HTTP.*
Краткое описание	Проверяется, использует ли тестируемый сайт соединение по протоколу HTTP.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Перейти на сайт http://testfire.net/feedback.jsp 2. Убедиться, что сайт загрузился.
Постусловие	Проверить, выполняется ли автоматическая переадресация на сайт https://testfire.net/feedback.jsp
Ожидаемый результат	Сайт доступен по протоколу HTTP.

Наименование тест-кейса	*ТС-002: Проверка использования безопасного соединения - HTTPs.*
Краткое описание	Проверяется, использует ли тестируемый сайт соединение по протоколу HTTPs.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Перейти на сайт https://testfire.net/feedback.jsp 2. Убедиться, что сайт загрузился.
Постусловие	Отсутствует.
Ожидаемый результат	Сайт доступен по протоколу HTTPs.

Наименование тест-кейса	*ТС-003: Проверка параметров сертификата безопасного соединения - HTTPs.*
Краткое описание	Проверяется, использует ли тестируемый сайт сертификат, удовлетворяющий параметрам: срок действия(Valid to), DNS Name, Subject Alternate Name(SAN).
Предусловие	Тест-кейс ТС-002 протестирован с успешным результатом.
Шаги к выполнению	1. Перейти на сайт https://testfire.net/feedback.jsp 2. Убедиться, что сайт загрузился. 3. Выполнить проверку параметра «Valid to», убедиться что срок действия не соответствует текущей дате. 4. Выполнить проверку параметра «DNS Name», убедиться что параметр соответствует имени сайта - testfire.net. 5. Выполнить проверку параметра «SAN», убедиться что параметр соответствует имени сайта - testfire.net.
Постусловие	Отсутствует.
Ожидаемый результат	Параметры «Valid to», «DNS Name», «SAN» соответствуют значениям определенным в шагах п.3-5.

Наименование тест-кейса	*ТС-004: Проверка информации в HTTP-заголовке.*
Краткое описание	Проверяется, имеется ли в ответе на HTTP-запрос, информация(поля) представляющая ценность для злоумышленника.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Выполнить запрос: «curl -I testfire.net». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку параметра «Server», «X-Powered-By», убедиться что в поле(-ях) присутствует информация о наименовании и версии web-сервера и\или компонент web-сервера.
Постусловие	Отсутствует.
Ожидаемый результат	Параметр «Server» и\или «X-Powered-By» содержат информацию, содержащую наименование и\или версию web-сервера и\или компонент web-сервера.

Наименование тест-кейса	*TC-005: Тестирование HTTP Strict Transport Security (HSTS)*
Краткое описание	Проанализировать наличие заголовка HSTS и убедиться в его работоспособности.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Выполнить запрос: «curl -I testfire.net I grep «strict»». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку заголовка «Strict-Transport-Security», убедиться что в заголовке присутствует информация о времени преобразования HTTP-запросов в HTTPs(max-age).
Постусловие	Отсутствует.
Ожидаемый результат	Заголовок «Strict-Transport-Security» содержит информацию о параметра max-age.

Наименование тест-кейса	*ТС-006: Проверка доступных методов HTTP.*
Краткое описание	Проверяется, какие методы доступны для запроса и есть ли среди них потенциально опасные.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Выполнить запрос: «curl -X имя метода testfire.net». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку методов «GET», «HEAD», «POST», «PUT», «DELETE», «CONNECT», «OPTIONS», «TRACE», «TRACK», «PATCH».
Постусловие	1. Убедиться, что в ответе для «GET», «HEAD», «POST» присутствует значение «200 OK». 2. Убедиться, что в ответе для «PUT», «DELETE», «CONNECT», «OPTIONS», «TRACE», «TRACK», «PATCH» присутствует значение отличное от «200 OK».
Ожидаемый результат	В ответах на запросы «GET», «HEAD», «POST» присутствует значение «200 OK». В ответах на остальные запросы присутствует значение отличное от «200 OK».

Наименование тест-кейса	*ТС-007: Поиск на странице JS-скриптов.*
Краткое описание	Проверяется, имеется ли в HTML-разметке код JavaScript.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Выполнить запрос: «curl testfire.net | grep «<script>». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку вывода, убедиться что присутствует информация о ссылке(-ах) на внешние файлы JS и\или JS-код присутствует в самой HTML-разметке.
Постусловие	Отсутствует.
Ожидаемый результат	Тег «<script>» присутствует в HTML-разметке.

Наименование тест-кейса	*ТС-008: Поиск в JS-скриптах чувствительной информации.*
Краткое описание	Проверяется, имеется ли в коде JavaScript, чувствительная информация: токены, пароли и т.д.
Предусловие	Тест-кейс ТС-007 протестирован с успешным результатом.
Шаги к выполнению	1. Выполнить запрос: «curl testfire.net | grep «<script>». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку вывода, на наличие ключевых слов: token, password, key, config, admin и соответствующей чувствительной информации. 4. Проверка п.3 может выполняться посредством grep «ключевое слово».
Постусловие	Отсутствует.
Ожидаемый результат	В JS-скриптах на сайте не содержится чувствительной информации.

Наименование тест-кейса	*ТС-009: Поиск в HTML-разметки комментариев с чувствительной информации.*
Краткое описание	Проверяется, имеется ли в HTML-разметке сайта чувствительная информация: токены, пароли и т.д.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Выполнить запрос: «curl testfire.net I grep ‘<!—‘. 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку вывода, на наличие ключевых слов: token, password, key, config, admin и т.д. и соответствующей чувствительной информации.
Постусловие	Отсутствует.
Ожидаемый результат	В HTML-разметке на сайте не содержится чувствительной информации.

Наименование тест-кейса	*ТС-010: Тестирование cookies на наличие чувствительной информации.*
Краткое описание	Проанализировать наличие содержимого cookies на наличие чувствительной информации.
Предусловие	Сайт доступен для запроса. Используются cookies.
Шаги к выполнению	1. Выполнить запрос: «curl -I testfire.net/feedback.jsp». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку вывода, на наличие слов: token, password, key, config, admin и т.д. и соответствующей чувствительной информации.
Постусловие	Отсутствует.
Ожидаемый результат	В cookies на сайте не содержится чувствительной информации.

Наименование тест-кейса	*ТС-011: Тестирование cookies на наличие безопасных параметров.*
Краткое описание	Проанализировать наличие содержимого cookies на наличие параметров: «Path», «HttpOnly», «Secure», «SameSite».
Предусловие	Сайт доступен для запроса. Используются cookies.
Шаги к выполнению	1. Выполнить запрос: «curl -I testfire.net/feedback.jsp». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку вывода, на наличие параметра «Set-Cookie» и подпараметров «Path=/», «HttpOnly», «Secure», «SameSite=Strict» .
Постусловие	Отсутствует.
Ожидаемый результат	В cookies на сайте используются параметры «Path=/», «HttpOnly», «Secure», «SameSite=Strict».

Наименование тест-кейса	*ТС-012: Тестирование уязвимостей межсайтовых скриптов (XSS)*
Краткое описание	Проанализировать каждый входной вектор, с целью обнаружения потенциальных уязвимостей XSS.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Определить доступные для ввода поля. 2. Ввести в первое поле строку: <script>alert(«!!!»)</script>, нажать клавишу Enter. 3. Убедиться, что не появилось окно со значением: «!!!». 4. Выполнить действия п.2, 3 для всех оставшихся полей ввода.
Постусловие	Отсутствует.
Ожидаемый результат	В процессе тестирования не появилось окно со значением «!!!».

Наименование тест-кейса	*TC-013: Тестирование SQL (SQLi)*
Краткое описание	Проанализировать каждый входной вектор, с целью обнаружения потенциальных уязвимостей SQL Injection.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. В строке браузера ввести значение: https://testfire.net/feedback.jsp?username=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%20'1, нажать клавишу Enter. 2. Убедиться, что не появилось окно ошибкой и\или выводом значений БД. 3. В строке браузера ввести значение: https://testfire.net/feedback.jsp?username=1'%20or%20'1'%20=%20'1'))%20LIMIT%201/*&password=foo, нажать клавишу Enter. 4. Убедиться, что не появилось окно ошибкой и\или выводом значений БД. 5. В строке браузера ввести значение: https://testfire.net/feedback.jsp?id=10 AND 1=1, нажать клавишу Enter. 6. Убедиться, что не появилось окно ошибкой и\или выводом значений БД. 7. В строке браузера ввести значение: https://testfire.net/feedback.jsp?id=10|| UTL_INADDR.GET_HOST_NAME((SELECT user FROM DUAL))--, нажать клавишу Enter. 8. Убедиться, что не появилось окно ошибкой и\или выводом значений БД. 9. В строке браузера ввести значение: https://testfire.net/feedback.jsp?id=1; UPDATE users SET PASSWORD=chr(114)||chr(111)||chr(111)||chr(116)--, нажать клавишу Enter. 10. Убедиться, что не появилось окно ошибкой и\или выводом значений БД.
Постусловие	Отсутствует.
Ожидаемый результат	В процессе тестирования не выявилось выдачи информации из БД.

Наименование тест-кейса	*TC-014: Тестирование перехвата клика (Clickjacking)*
Краткое описание	Определить возможность выполнения атаки Clickjacking.
Предусловие	Сайт доступен для запроса.

Шаги к выполнению	1. Определить доступные для ввода поля.
	2. Ввести в первое поле строку: <script>
	var prevent_bust = 0;
	window.onbeforeunload = function() {
	prevent_bust++;
	};
	setInterval(
	function() {
	if (prevent_bust > 0) {
	prevent_bust -= 2;
	window.top.location = «http://ya.ru";
	}
	}, 1);
	</script>
	<iframe src=«http://ya.ru">, нажать клавишу Enter.
	3. Убедиться, что на странице сайте не появилось изменений и\или стороннего контента.
	4. Выполнить действия п.2, 3 для всех оставшихся полей ввода.

Постусловие	Отсутствует.
Ожидаемый результат	В процессе тестирования не появилось изменений и\или стороннего контента.

Наименование тест-кейса	*TC-015: Тестирование уязвимости переполнения буфера*
Краткое описание	Определить возможность выполнения атаки Buffer Overflow.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Определить доступные для ввода поля. 2. Ввести в первое поле строку: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF, нажать клавишу Enter. 3. Убедиться, что на странице сайте не появилось изменений и\или стороннего контента. 4. Выполнить действия п.2, 3 для всех оставшихся полей ввода.
Постусловие	Отсутствует.
Ожидаемый результат	В процессе тестирования не появилось изменений и\или стороннего контента.

Наименование тест-кейса	*ТС-016: Тестирование инъекций в строке форматирования*
Краткое описание	Строка форматирования — это последовательность символов, заканчивающаяся нулём (т.е. нуль-терминированная), которая также содержит спецификаторы преобразования, интерпретируемые или преобразуемые во время выполнения. Если код на стороне сервера конкатенирует пользовательский ввод со строкой форматирования, злоумышленник может добавить дополнительные спецификаторы преобразования, чтобы вызвать ошибку во время выполнения, раскрытие информации или переполнение буфера.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Определить доступные для ввода поля. 2. Ввести в первое поле последовательно строки: « alice», «%s%s%s%n», «%p%p%p%p%p», «{event.__init__.__globals__[CONFIG][SECRET_KEY]}», нажать клавишу Enter. 3. Убедиться, что на странице сайте не появилось изменений и\или стороннего контента. 4. Выполнить действия п.2, 3 для всех оставшихся полей ввода.
Постусловие	Отсутствует.
Ожидаемый результат	В процессе тестирования не появилось изменений и\или стороннего контента.

Наименование тест-кейса	*ТС-017: Тестирование инъекций команд ОС*
Краткое описание	Метод, используемый через web-интерфейс для выполнения команд ОС на web-сервере.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Определить доступные для ввода поля. 2. Ввести в первое поле последовательно строки: «/bin/lsl», «cmd.exe», «cat /etc/passwd», «dir /p», нажать клавишу Enter. 3. Убедиться, что на странице сайте не появилось изменений и\или стороннего контента. 4. Выполнить действия п.2, 3 для всех оставшихся полей ввода.
Постусловие	Отсутствует.
Ожидаемый результат	В процессе тестирования не появилось изменений и\или стороннего контента.

Наименование тест-кейса	*ТС-018: Проверка информации в ответе на API-запрос.*
Краткое описание	Проверяется, имеется ли в ответе на API-запрос, информация представляющая ценность для злоумышленника.
Предусловие	Сайт доступен для запроса.
Шаги к выполнению	1. Выполнить запрос: «curl -X POST testfire.net/api/feedback/123». 2. Получить ответ на HTTP-запрос. 3. Выполнить проверку вывода, убедиться что отсутствует информация о наименовании и версии web-сервера и\или компонент web-сервера.
Постусловие	Отсутствует.
Ожидаемый результат	Вывод не содержит информацию, содержащую наименование и\или версию web-сервера и\или компонент web-сервера.