File 1

Имя файла: Задание 1
Тип уязвимости: XSS (Cross-Site Scripting)
Уязвимая строка кода:

```
<div class="recipe">
   <h2>Leave your feedback or question</h2>
   <p>Please enter your message or question, and we will respond as soon as possible!</p>
   <form method="GET" action="">
      <label for="message">Your message:</label>
      <input type="text" id="message" name="val" placeholder="Enter your feedback or question" />
      <button type="submit">Send</button>
   </form>
```

Пояснения к уязвимости: Тут злоумышленник сможет вставить кусок вредоносного кода для компрометации сайта.
Рекомендации по уязвимости: Использовать подходящие http заголовки, вроде Content-Type или X-Content-Type-Options, можно использовать CSP (Content Security Policy), не использовать PHP в html файле.
Возможная эксплуатация: в том куске кода: <form method="GET" action=""> можно вставить любой домен или файл, который можно использовать для эксплуатации.

File 2

Имя файла: Задание 2
Тип уязвимости: CRLF injection (Carriage Return Line Feed)
Уязвимая строка кода: `import ("net/http")`
Пояснения к уязвимости: При такой уязвимости злоумышленник сможет манипулировать результатом HTTP заголовка.
Рекомендации по уязвимости: Убрать любые не нужные заголовки на веб-сервере.
Возможная эксплуатация: Если имеется такая уязвимость, то можно например сменить статус http заголовка с 404/403 на 200.

File 3

Имя файла: Задание 3
Тип уязвимости: Включение файла PHP (PHP File Inclusion)
Уязвимая строка кода: `require_once '/path/to/vendor/autoload.php';`
Пояснения к уязвимости: данная уязвимость позволяет злоумышленнику обхитрить веб приложение, для того чтобы скомпрометировать чувствительную информацию, которая может привести к другим атакам, вроде XSS.
Рекомендации по уязвимости: Использовать базу данных, регистрация по ID, использовать только разрешённые файлы.
Возможная эксплуатация: возможность добраться до классового файла PHP, набрав его название в поисковике.
Дата выполнения: 21.05.2025