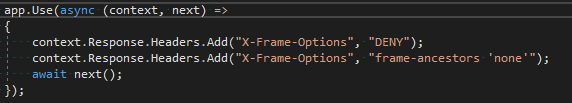
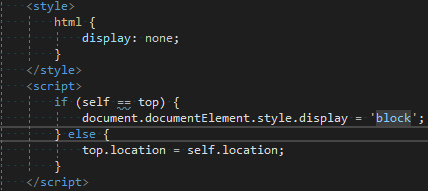
**Найденные уязвимости на сайте:**

* X-Frame-Options Header Not Set & X-Frame-Options Setting Malformed

**Атаки с использованием кликджекинга** обманом **заставляют** веб-пользователей выполнить действие, которое они не планировали, обычно путем визуализации невидимого элемента страницы поверх действия, которое, по мнению пользователя, они выполняют.

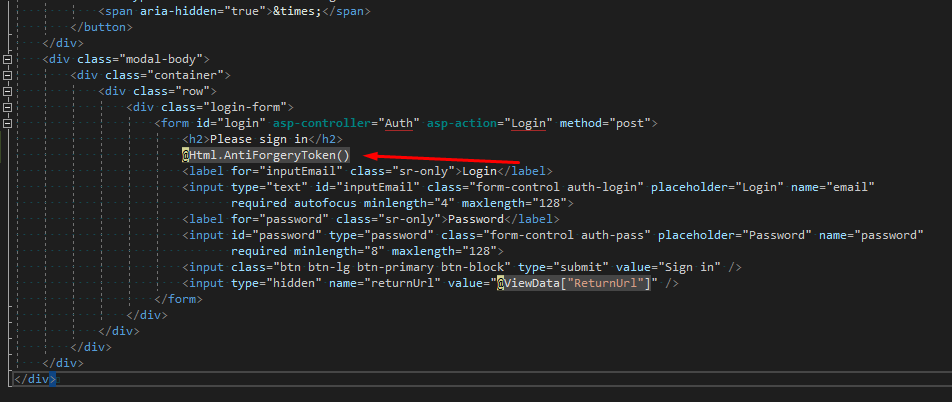
Исправляется очень легко + для старых браузеров были добавлены спец команды.

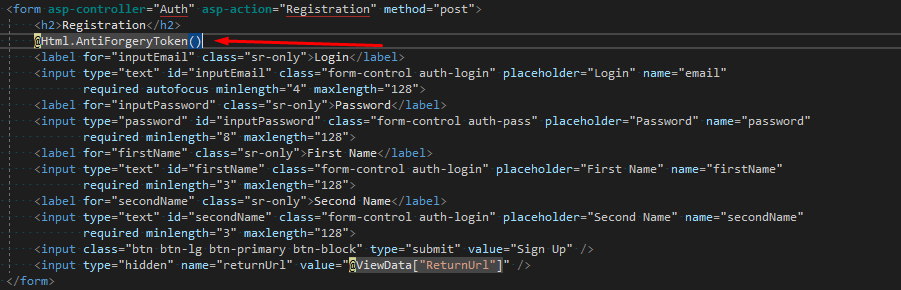


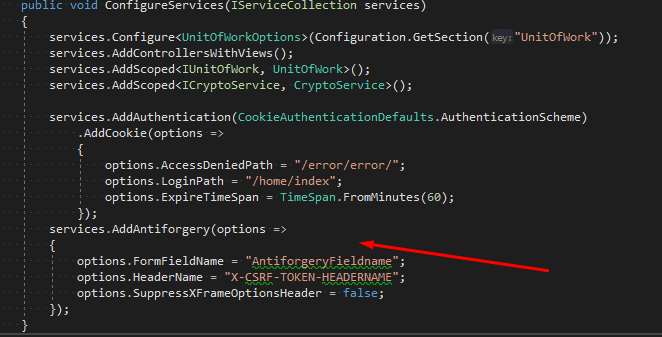


* CSRF

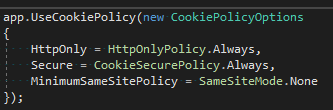
Подделка межсайтовых запросов (также известная как XSRF или CSRF) - это атака на размещенные в Интернете приложения, при которой вредоносное веб-приложение может влиять на взаимодействие между клиентским браузером и веб-приложением, которое доверяет этому браузеру. Эти атаки возможны, потому что веб-браузеры автоматически отправляют некоторые типы токенов аутентификации с каждым запросом на веб-сайт. Эта форма эксплойта также известна как атака одним щелчком мыши или атака на сеансе, поскольку атака использует ранее аутентифицированный сеанс пользователя.

Как была исправлена данная уязвимость



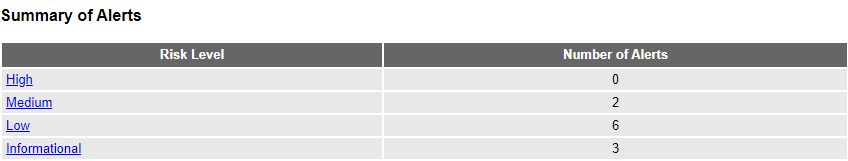


Разного рода ошибки с cookie были исправлены добавлением нескольких параметров



Далее используя утилиту OWASP Zap был проверен сайт

**до исправления**



**после исправления**

