Национальный аэрокосмический университет им. М.Е. Жуковского
"Харьковский авиационный институт"
Кафедра компьютерных систем и сетей

Средства автоматической настройки функций безопасности веб-сервера

ВЫПОЛНИЛ: СТУДЕНТ 545-И ГРУППЫ ПОДДУБНЫЙ К.А.

РУКОВОДИТЕЛЬ: СТ. ПРЕПОДАВАТЕЛЬ КАФ. 503 ЦУРАНОВ М.В.

Постановка задачи

Цель – разработка программного средства для автоматической настройки функций безопасности веб-сервера Apache.

Задачи:

1. Проанализировать наиболее распространенные веб-сервера.
2. Разработать bash-скрипт для автоматической настройки функций безопасности веб-сервера Apache.
3. Проверить настроенные функции безопасности веб-сервера Apache.
4. Рассчитать себестоимость разработанного программного средства.

Сравнительный анализ веб-серверов

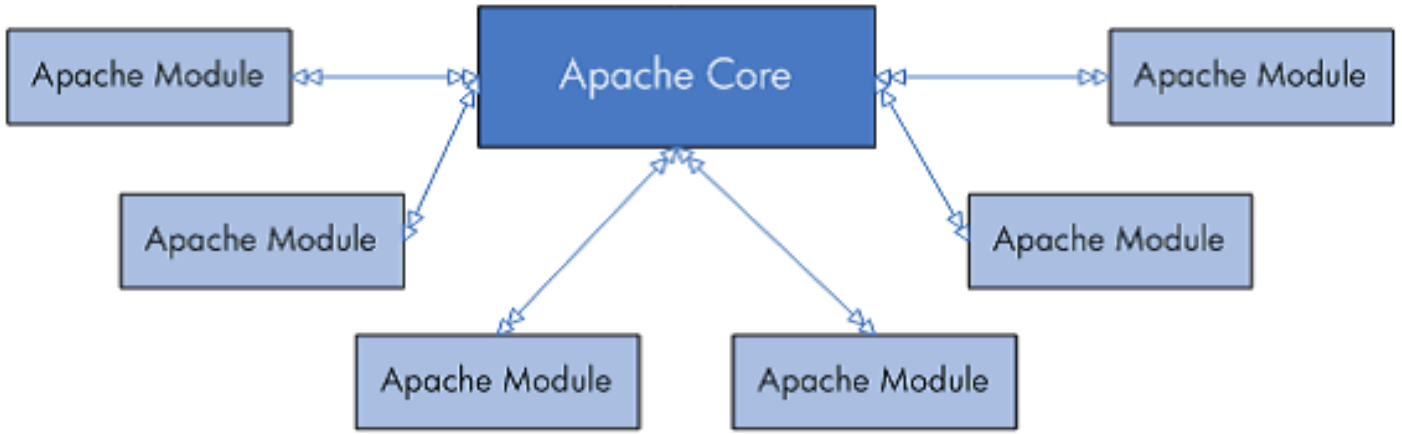
Таблица 1 – Краткое сравнение веб-серверов Apache, IIS и nginx

Название	Apache	IIS	nginx
Автор, год создания	Apache Software Foundation, 1995	Microsoft, 1995	Ігор Сисоєв, 2002
Распространение	Бесплатное	Включен в Windows NT	Бесплатное
Открытое ПО	+	-	+
Особенности	Акцент на надежность и гибкость. Модульность	Поддержка .NET и сценариев ASPX	Разрабатывался для серверов с высокой нагрузкой

Таблица 2 – Поддержка ОС веб-серверами Apache, IIS и nginx

Название	Apache	IIS	nginx
Windows	+	+	+
Linux	+	-	+
Mac OS X	+	-	+
BSD	+	-	+

Архитектура веб-сервера Apache



Популярные модули безопасности веб-сервера Apache

Название модуля	Выполняемые функции
mod_security	Модуль, с помощью которого создается первичный «щит» защиты веб-сервера.
mod_evasive	Модуль для организации защиты веб-сервера от DoS и brute force атак. Модулем осуществляется контроль интенсивности запросов с одного IP за период времени и числа параллельных запросов. После превышения определенного в конфигурации лимита, осуществляется временная блокировка доступа злоумышленника, возможен вызов внешнего скрипта для блокирования через фаервол.
mod_qos	При нехватке серверных ресурсов mod_qos может блокировать неприоритетные запросы, динамически изменять значения таймаутов, добавлять искусственную задержку перед выполнением запроса и принудительно завершать TCP-соединения.
mod_headers	Этот модуль обеспечивает директивы управления и изменения заголовков запроса и ответа HTTP.
mod_ssl	Модуль включающий поддержку протоколов безопасной передачи информации Secure Sockets Layer и Transport Layer Security.

Выбор инструмента разработки и программного обеспечения

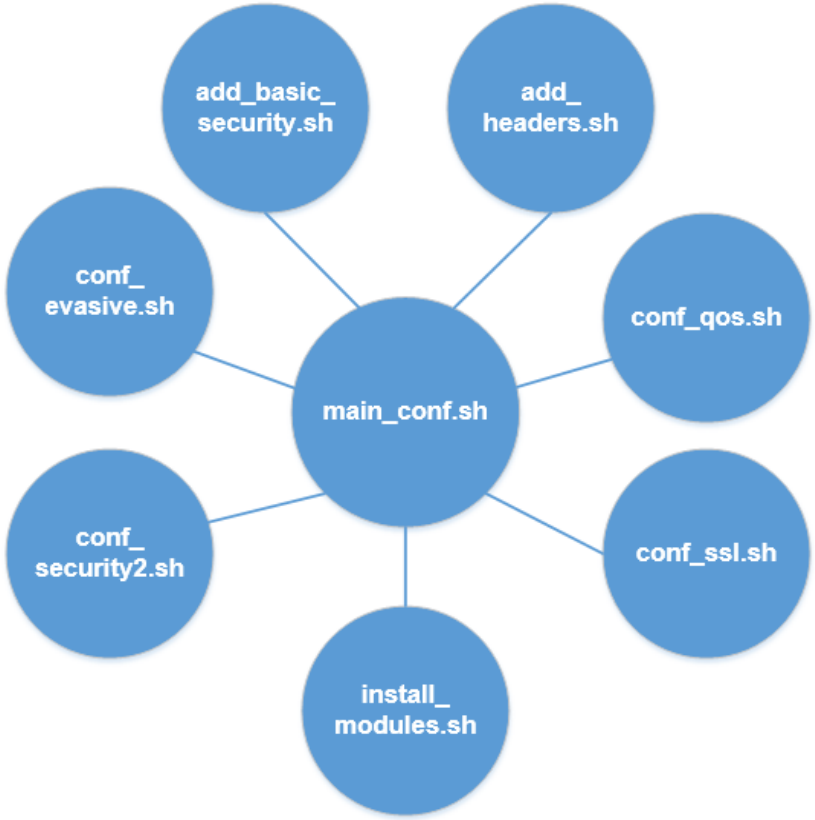
Разработка:

- Операционная система Ubuntu.
- Скриптовый язык bash.
- Текстовый редактор gedit.

Тестирование:

- Операционная система Kali Linux.
- Инструмент для моделирования атак «отказ в обслуживании» slowhttptest.
- Онлайн сканер HTTP заголовков securityheaders.io.

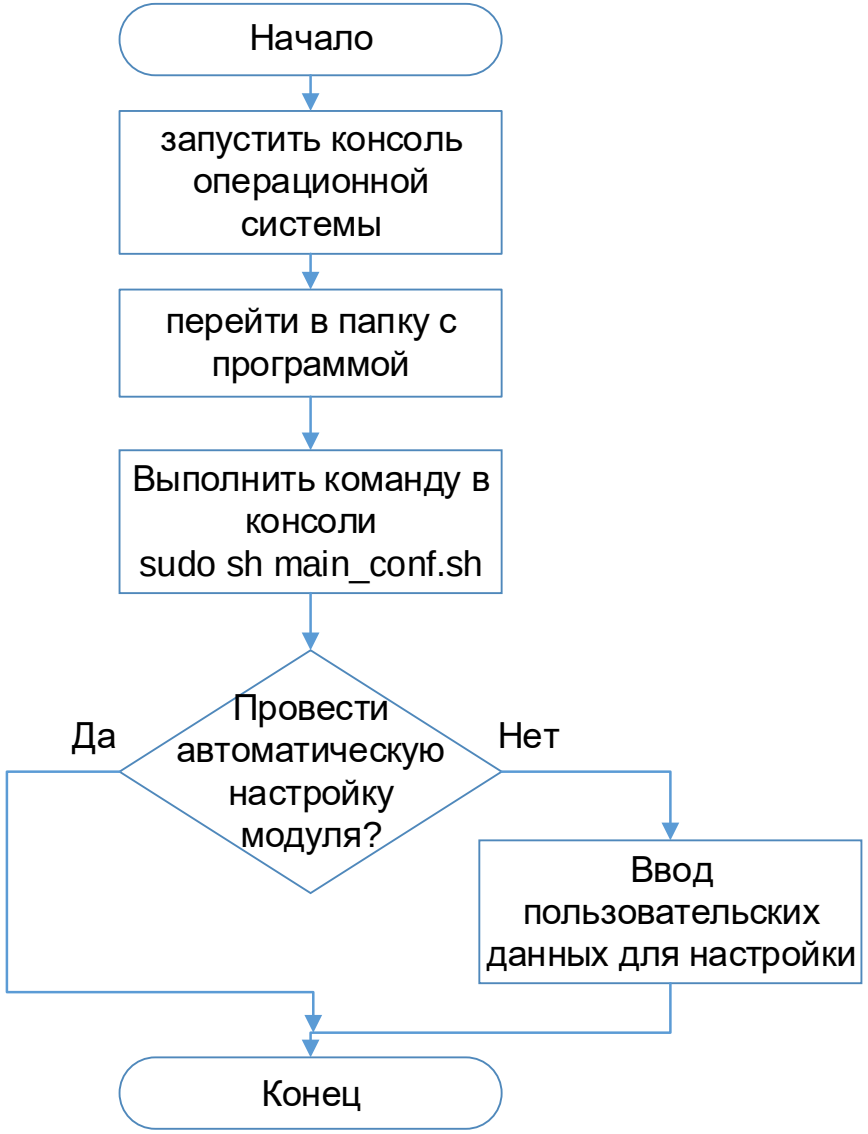
Архитектура разработанного продукта



Интерфейс разработанного продукта

```
kp@ubuntu:~/Desktop/SecurityConfiguration$ sudo sh main_conf.sh
Module headers already enabled

[Заголовки успешно добавлены!]


[Вывод информации о версиях ПО отключен!]

Module evasive already enabled
Провести автоматическую настройку mod_evasive? (y/n) y
Ввели «y», начинается автоматическая настройка...

[Конфигурация mod_evasive завершена!]

Module qos already enabled
Провести автоматическую настройку mod_qos? (y/n) y
Ввели «y», начинается автоматическая настройка...

[Конфигурация mod_qos завершена!]
```

Схема действий пользователя при автоматической настройке модуля



Тестирование продукта (1)

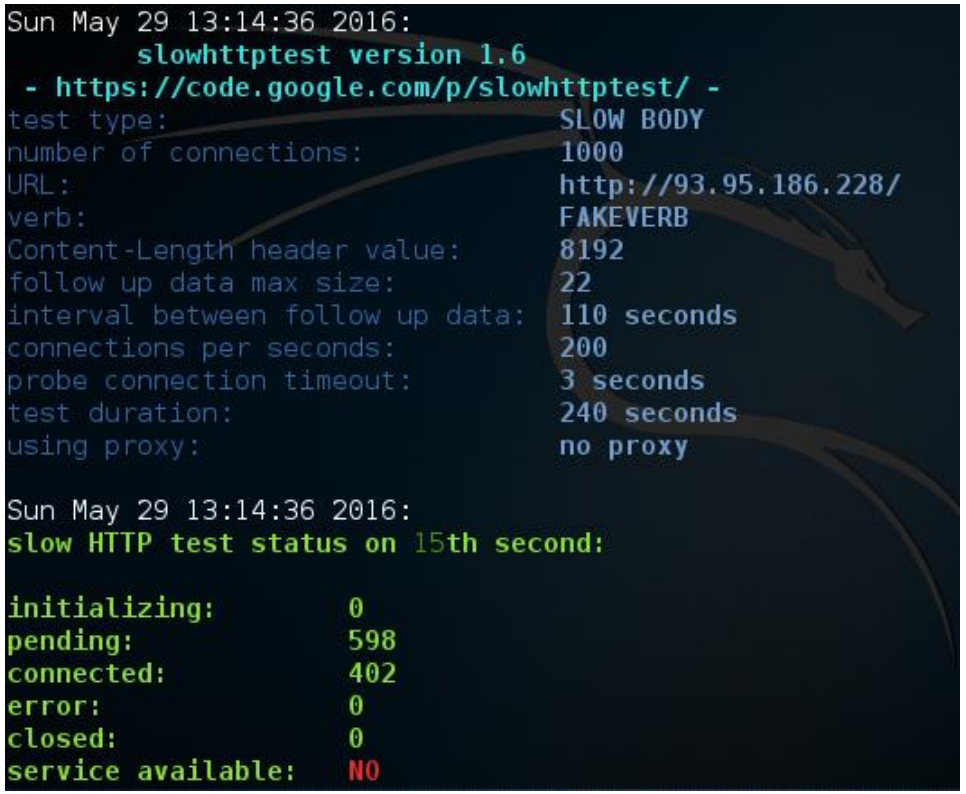


Рисунок 1 – Результат моделирования атаки «SLOW BODY» без проведения настройки модулей

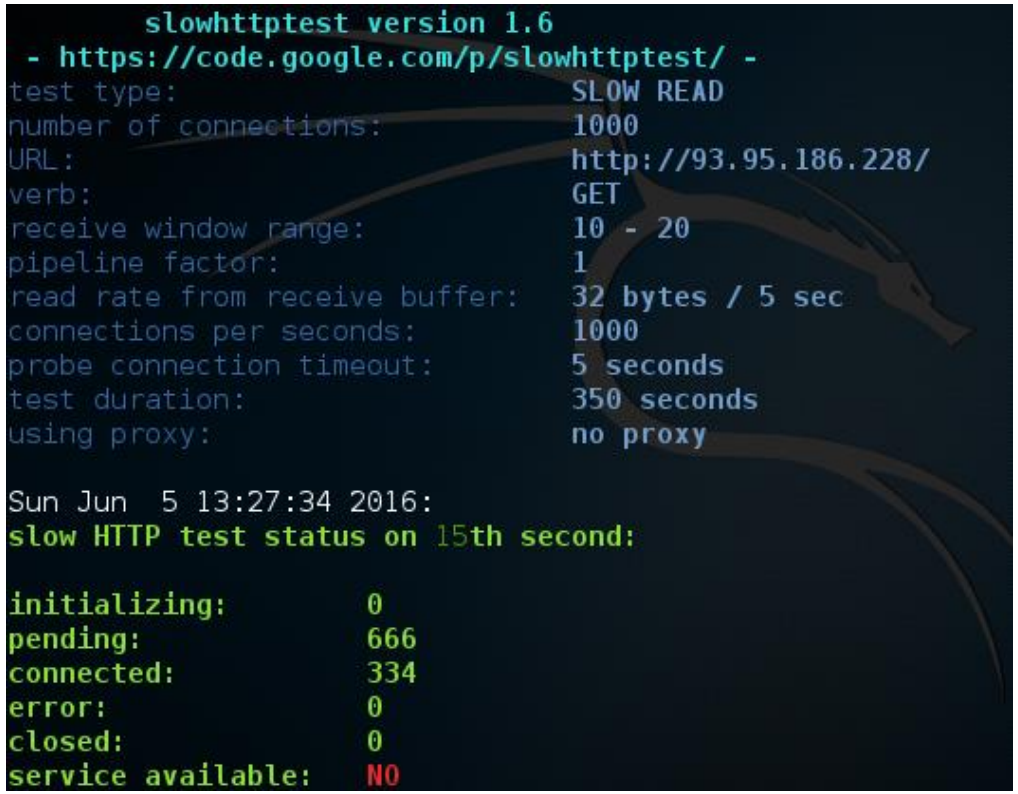


Рисунок 2 – Результат моделирования атаки «SLOW READ» без проведения настройки модулей

Тестирование продукта (2)

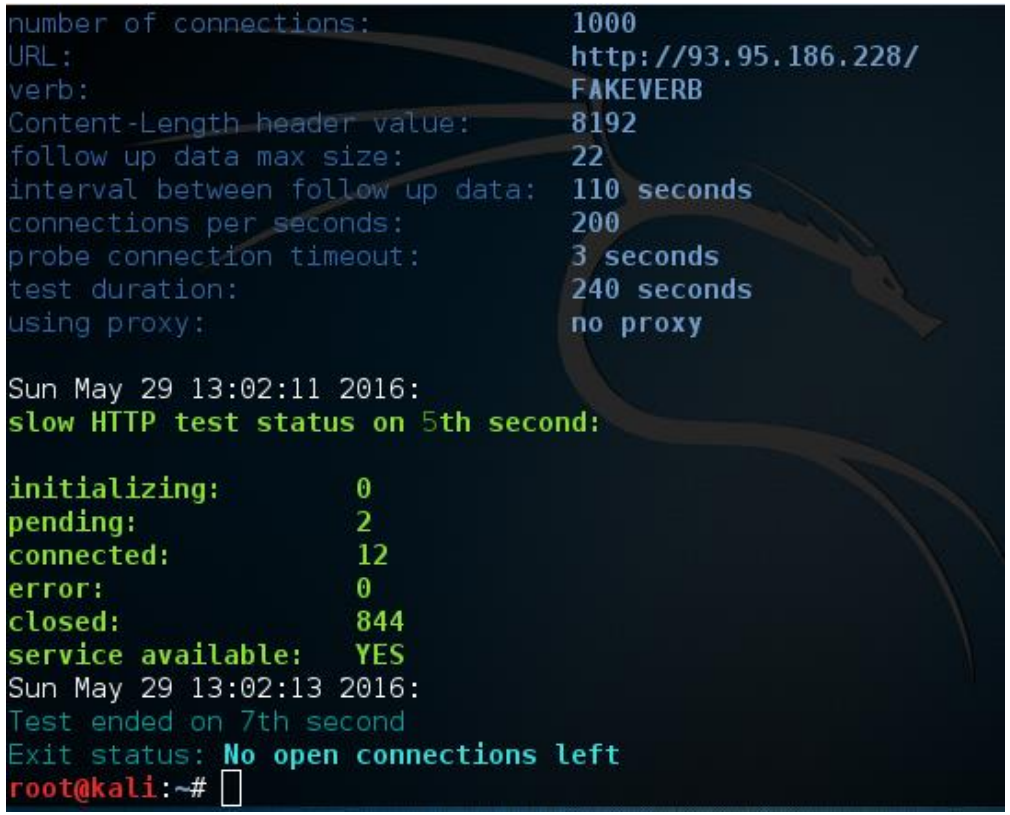


Рисунок 1 – Результат моделирования атаки «SLOW BODY» после проведения настройки модулей

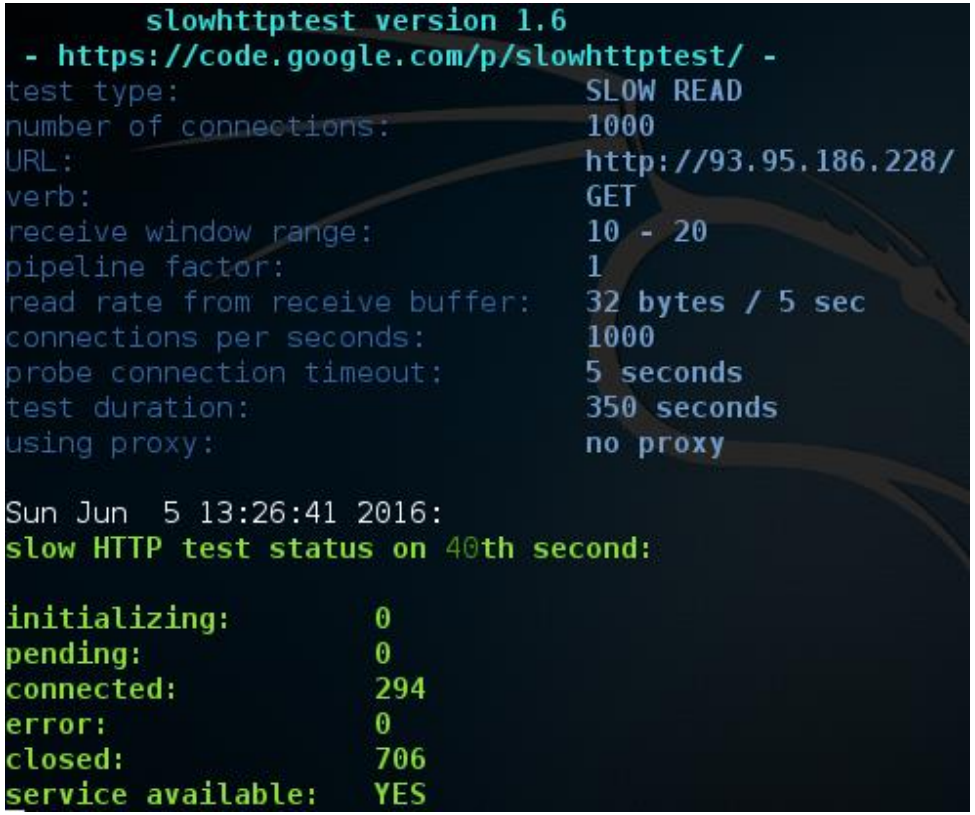


Рисунок 2 – Результат моделирования атаки «SLOW READ» после проведения настройки модулей

Тестирование продукта (3)

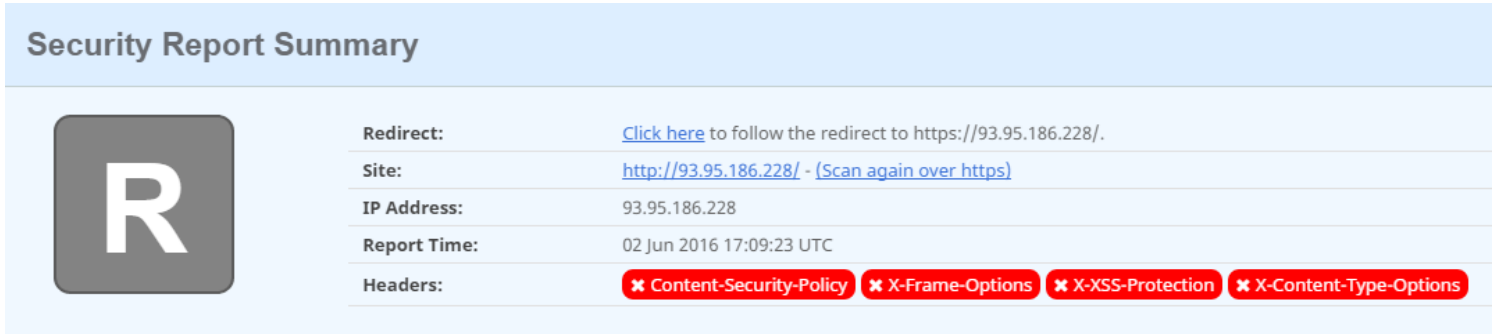


Рисунок 3 – Отчет сканера securityheaders.io без проведения настроек

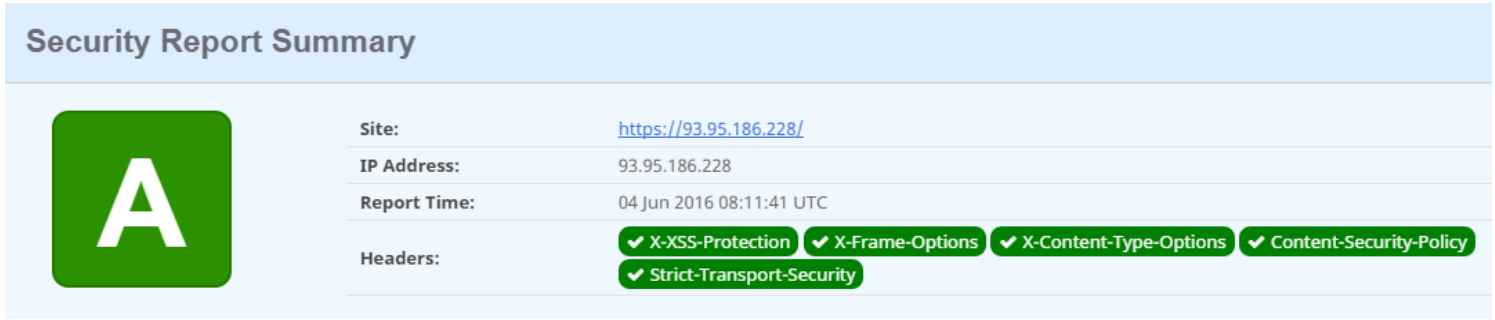


Рисунок 4 – Отчет сканера securityheaders.io после проведения настроек

Тестирование продукта (4)

```
<!DOCTYPE html>
<html>
<head>
        <meta charset="UTF-8">
        <title>Main page</title>
        <link rel="stylesheet" href="style.css">
        <script>
                alert('HACKED');
        </script>
</head>
```

Рисунок 5 – Инлайновый JavaScript-код выполняемый на странице

```
Refused to execute inline script because it violates        93.95.186.228/:7
the following Content Security Policy directive: "default-src 'self'".
Either the 'unsafe-inline' keyword, a hash ('sha256-
NB3gaBNAmqqNEpNiWX3dDtfJT2y/LTNZmKb7dJ4qde8='), or a nonce ('nonce-...')
is required to enable inline execution. Note also that 'script-src' was
not explicitly set, so 'default-src' is used as a fallback.
```

Рисунок 6 – Сообщение об ошибке выполнения инлайнового JavaScript-кода

Экономическая часть

Таблица 3 – Статьи калькуляции на разработку

Статья калькуляции	**Затраты, грн**
Материалы	4880,43
Основная заработная плата	7613,59
Дополнительная заработная плата	1522,72
Фонд заработной платы	9136,31
Начисления на заработную плату (единый и социальный взнос)	2009,99
Амортизационные отчисления	966
Затраты на электроэнергию	900
Себестоимость разработки	17892,73

Выводы

1. В ходе статистического анализа использования веб-серверов установлено, что наиболее распространенными и популярными на информационном рынке являются веб-сервера Apache, IIS и nginx. Проведенная сравнительная характеристика данных веб-серверов показывает преимущества веб-сервера Apache.

2. Для автоматической настройки функций безопасности веб-сервера Apache разработан bash-скрипт. В программном продукте использовалась модульная архитектура, которая позволяет настраивать как все модули одновременно, так и выборочно.

3. В ходе тестирования настроенных функций безопасности веб-сервера Apache с использованием моделирования сценариев атак «отказ в обслуживании» и XSS-атак веб-сервер успешно отразил их. Сканирование онлайн сканером HTTP заголовков securityheaders.io показало, что веб-сервер использует дополнительные HTTP заголовки безопасности. После автоматической настройки функций безопасности веб-сервера Apache подключение пользователя к сайту, размещенному на веб-сервере, выполнялось по безопасному протоколу с набором надежных шифров.

4. Себестоимость программного продукта по расчетам статей калькуляции составил 17892,73 грн.

Спасибо за внимание