Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.05.03

ОТЧЕТ

по вариативной части задания

Студент: Палехова Мария Алексеевна Группа: 241-372

Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Руководитель практики: Кесель Сергей Александрович

Москва 2025

**Настройка веб-инфраструктуры**

В рамках лабораторной работы была развернута веб-инфраструктура, включающая:

* **Apache2:** Установлен и настроен веб-сервер Apache2 для обработки HTTP-запросов.
* **MariaDB:** Установлена и сконфигурирована СУБД MariaDB. Создана база данных для последующего использования WordPress.
* **WordPress:** Произведена установка и настройка системы управления контентом WordPress. WordPress был успешно подключён к созданной базе данных.

На выходе получен полнофункциональный веб-сайт на платформе WordPress, готовый для проведения моделирования атак.

**Моделирование инцидентов информационной безопасности**

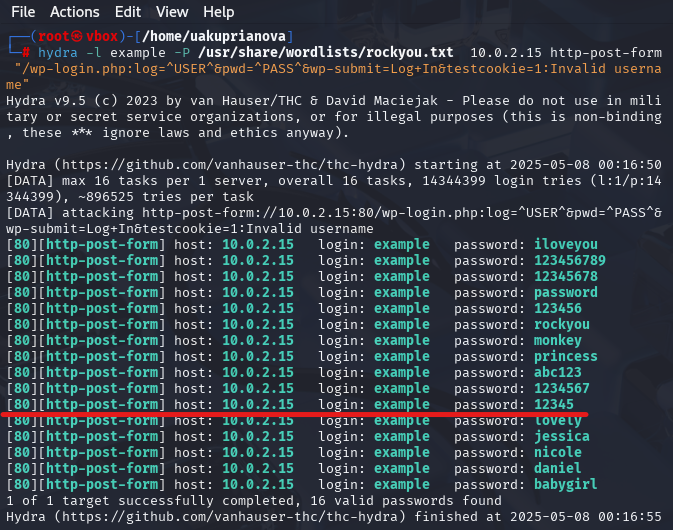
**Атака перебора паролей (Brute-force)**

Было проведено моделирование компрометации учетной записи пользователя WordPress методом перебора паролей.

Инструменты, использованные при атаке:

* **Wpscan:** применялся для сканирования WordPress-сайта и получения списка зарегистрированных пользователей. Это позволило получить логин: example.
* **Hydra:** использовалась для перебора паролей к известному логину. Была проведена атака методом подбора, в результате которой удалось обнаружить правильный пароль: 12345.

С помощью утилиты Hydra удалось успешно подобрать пароль и получить несанкционированный доступ к учетной записи пользователя example. Это подтвердило уязвимость системы при использовании слабых паролей.



**Что теоретически можно сделать с сайтом под скомпрометированным аккаунтом**

После того, как удалось получить доступ к учётной записи WordPress, возможности зависят от уровня привилегий этой учётной записи.

**Если это администратор:**

* Полностью управлять сайтом: изменять темы, устанавливать или удалять плагины.
* Вставить вредоносный код в темы/плагины (например, для XSS или бекдоров).
* Добавить новых пользователей, выдать себе дополнительные права.
* Слить базу данных (например, с помощью плагина экспорта).
* Подменить или удалить контент.

**Если это редактор/автор:**

* Менять или удалять публикации.
* Загружать вредоносные файлы, если разрешён аплоад.
* Использовать уязвимости плагинов, доступных этим ролям, для повышения привилегий.

**Реагирование на инцидент**

После того, как произошла компрометация аккаунта, нужно:

1. Сбросить пароль скомпрометированного пользователя.
2. Проверить другие аккаунты на предмет использования одинаковых или слабых паролей.
3. Отключить или ограничить доступ к админке, особенно по IP.
4. Проанализировать логины веб-сервера и базы данных — определить, когда и как произошёл доступ.
5. Провести аудит системы безопасности: обновить WordPress, плагины и темы до последних версий; убедиться, что нет следов закладок или вредоносного кода.
6. Включить двухфакторную аутентификацию для всех пользователей.
7. Усилить защиту от перебора паролей. (ограничить число попыток входа; использовать капчу)