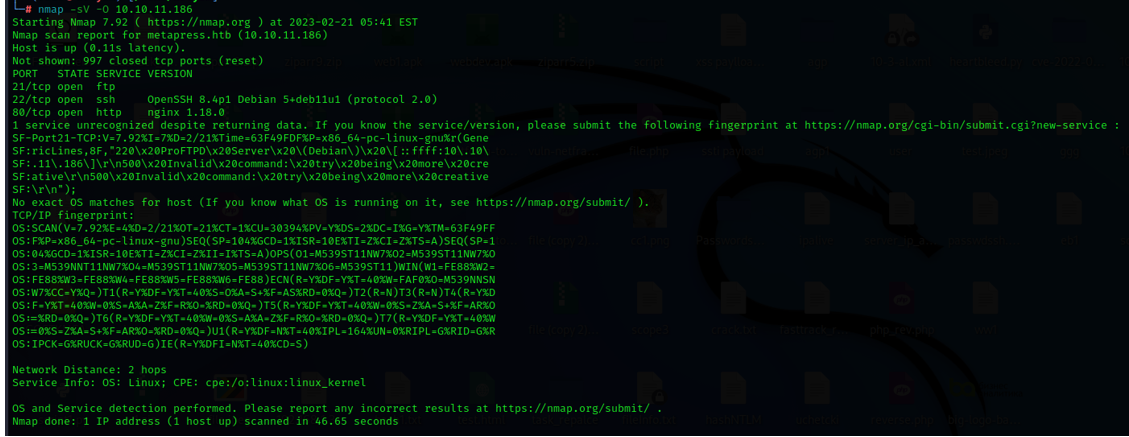
Metatwo-HackTheBox

1. С помощью сканирования nmap-ом были найдены порты 21 ftp и 22 ssh:

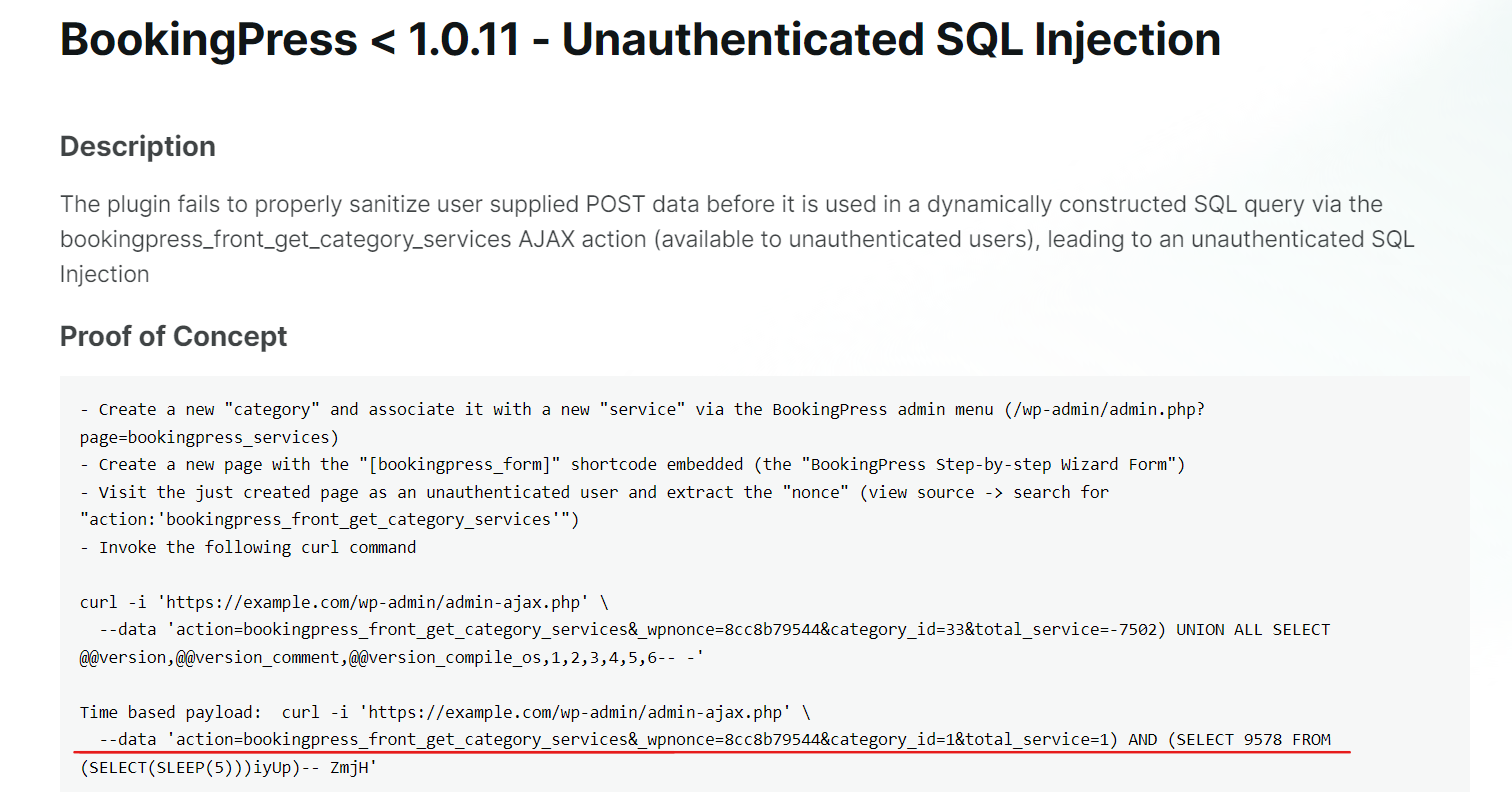


1. Результат скрининга сайта: используется WordPress и BookingPress версии до 1.0.11

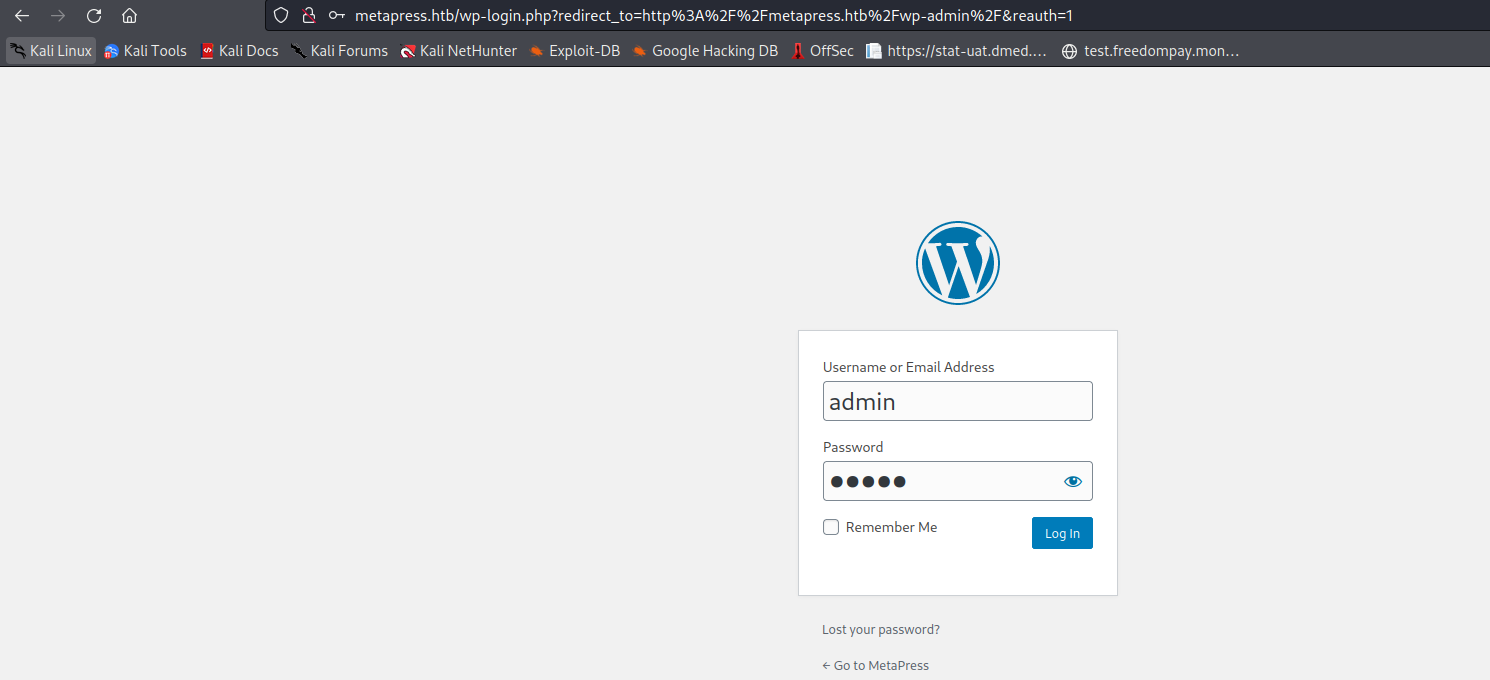
Изображение выглядит как текст

Автоматически созданное описание

1. Нахождение уязвимости SQL-injection, с помощью которой можно попробовать получить какие-либо данные:



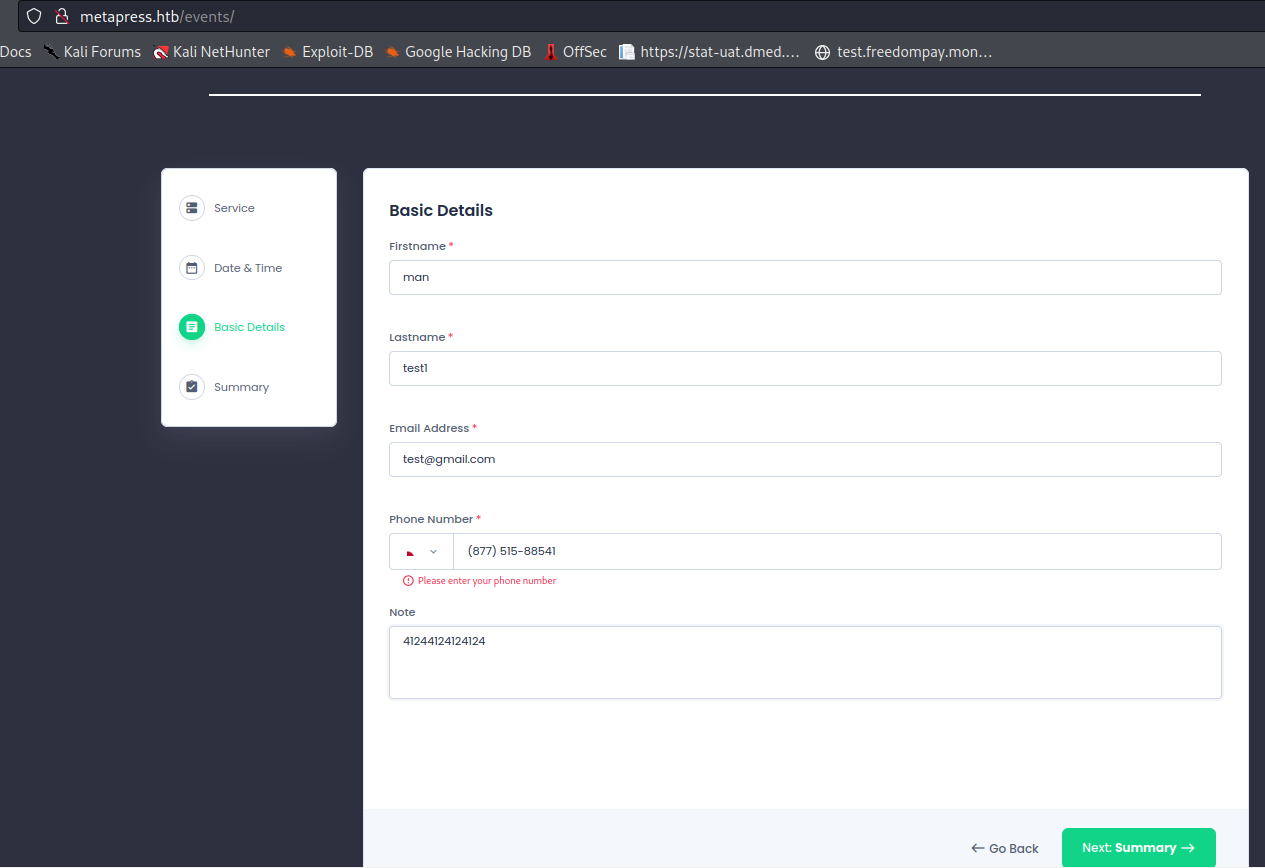
1. Сервис WordPress и авторизация:



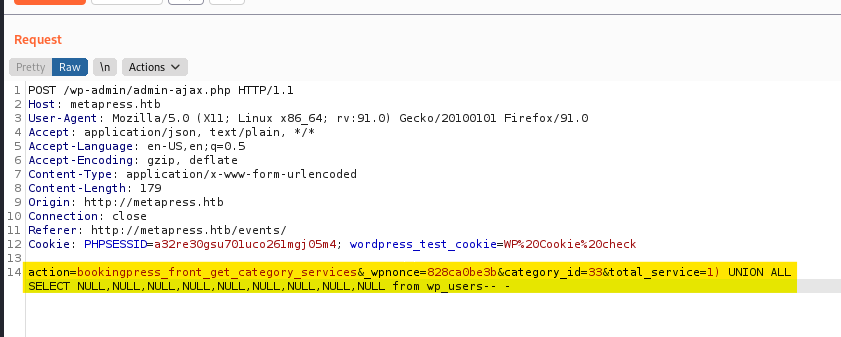
1. Проведение перехвата данных на главной странице сайта:

Изображение выглядит как текст

Автоматически созданное описание



1. Так как используется старая версия сервиса, то здесь можно провести атаку SQL injection для просмотра базы данных и находящиеся в ней данные пользователей, она подключения к базе даных WordPress:



1. Ответ от сервера с обнаруженной SQL-injection:

Изображение выглядит как текст

Автоматически созданное описание

1. Подмена даных вместо NULL (использовались стандартные названия таблиц WordPress):

Изображение выглядит как текст

Автоматически созданное описание

1. При подмене и правильно названым таблицам в ответе были выведены существующие пользователи в данной базе данных и во втором столбце были указаны пароли пользователей, в результате были получены учетные данные пользователей с паролями, захешированные хешем SHA256:

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. Подбор пароля брутом хеша с использованием словарика и указанием необходимой хеш-функции:

Изображение выглядит как текст

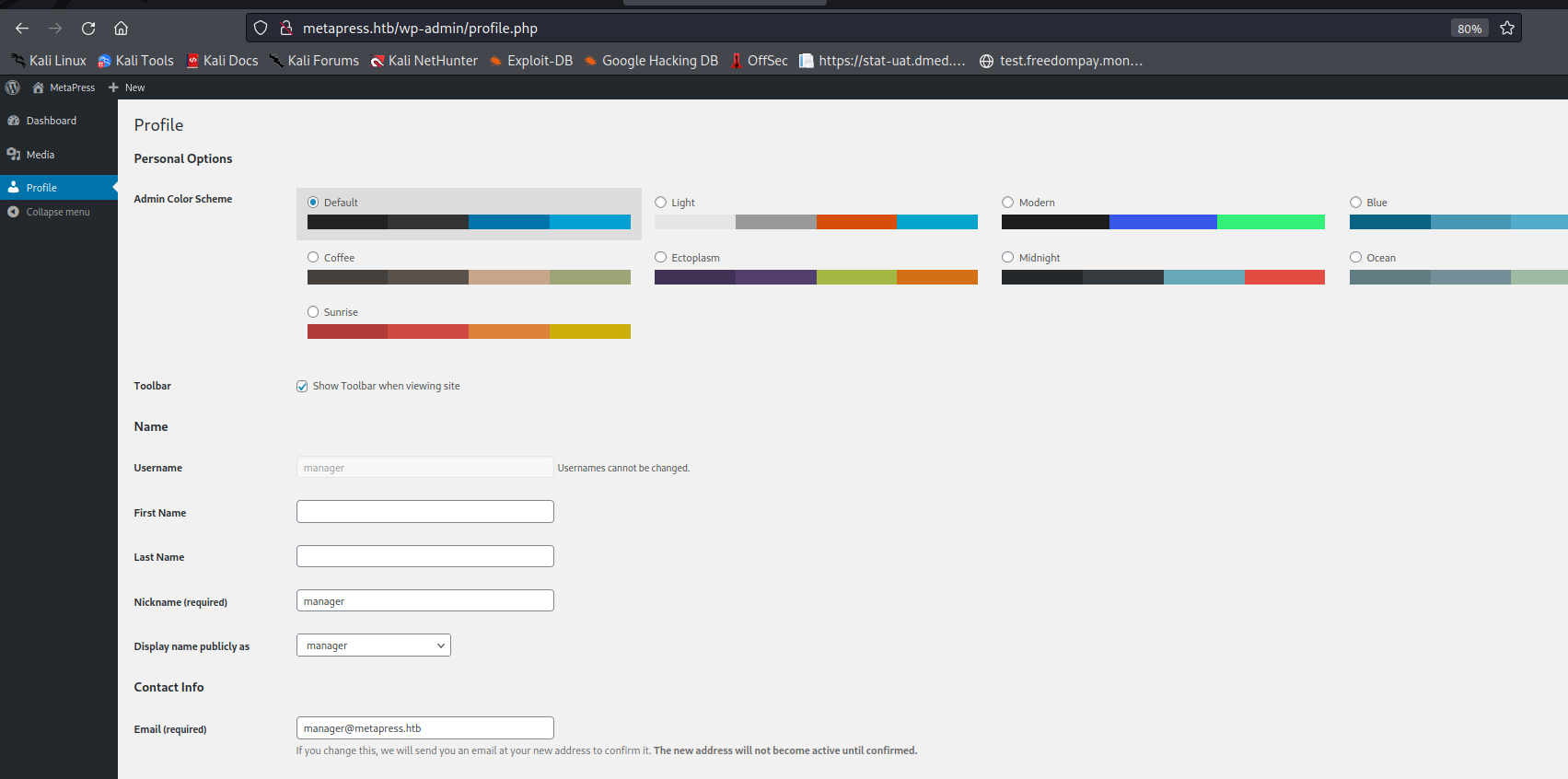
Автоматически созданное описание

1. В результате был подобран пароль для пользователя manager с паролем partylikearockstar:

Изображение выглядит как текст

Автоматически созданное описание

1. Подключение к wp-admin и обнаружение версии WP:



Изображение выглядит как текст

Автоматически созданное описание

1. C помощью эксплойта CVE-2021-29447 на основе уязвимости XXE можно получить LFI и просматривать файлы на стороне сервера. Поэтому необходимо загрузить файл формата wav видеоролик и dtd файл с указанием пути конвертации кодировки base64 и указанным путем для просмотра:

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. В результате запущенного сервера php -S 0.0.0.0:9001 произошел перехват, в котором было закодированное сообщение с информацией о данных веб-сериса, декодировав которое через Base 64, получаем список пользователей:

Изображение выглядит как текст

Автоматически созданное описание

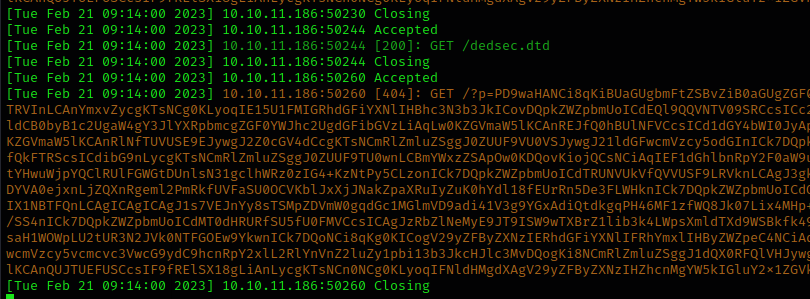
Изображение выглядит как текст

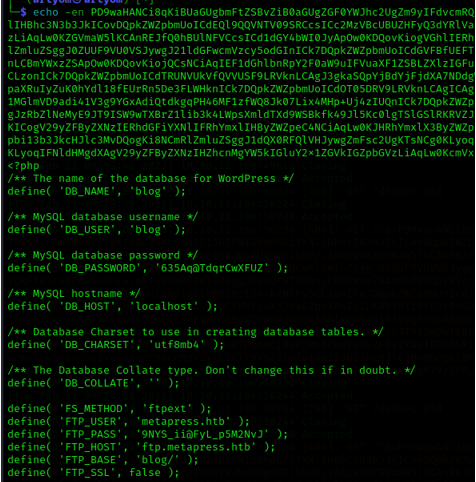
Автоматически созданное описание

1. Нахождение файла конфигурации WP, в котором возможно находятся какие-либо данные для подключения к 21 и 22 порту:

Изображение выглядит как текст

Автоматически созданное описание





Изображение выглядит как текст

Автоматически созданное описание

1. Просмотр директорий и отправка файла email.php:

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. Подключение к юзеру через FTP [jnelson@metapress.htb](mailto:jnelson@metapress.htb) и нахождение флага user.txt:

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. Для получения root флага повышаем полномочия при помощи инструмента линпис:

Изображение выглядит как текст

Автоматически созданное описание

1. Нахождение флага с помощью утилиты:

Изображение выглядит как текст

Автоматически созданное описание