Защищаем веб-сервер

Как справедливо замечают умные и опытные люди (я к ним не отношусь), защита веб-сервера - это комплексная задача, не решаемая нажатием волшебной кнопки «Сделать мне хорошо».

Есть такое высказывание: «Скорость всего каравана равна скорости самого медленного верблюда» - точно так же и здесь, степень защищенности определяется по наименее защищенному компоненту. Имейте это в виду.

Все описанное ниже является некими упрощенными и усредненными советами, так как в зависимости от требований что-то может оказаться ненужным или наоборот, нужно еще и еще допиливать оборону. К тому же, жизнь интересная штука - все меняется со временем, и явно будут новые способы проведения атак и новые методы защиты. Сражение меча со щитом будет длиться бесконечно.

Основные направления обороны:

- Защита средствами операционной системы
  - Следим за системой
  - Логирование - ведем логи сервисов, при необходимости это можно вынести на отдельную машину.
  - Обнаружение атаки
    - fail2ban
  - Фаервол нам в помощь
- Веб-сервер
  - Базовые вещи: /var/www (или где там все живет?) смонтировать с noexec; установить права 644 для файлов и 755 для директорий
  - Защита Apache: общий подход, ModSecurity
  - Защита nginx
- Защищаем PHP
- Защищаем CMS и скрипты
  - Общие советы
    - Скрыть административный вход (переименование папки/скрипта или закрыть паролем через .htpasswd)
    - Включить SEF (они же ЧПУ)
  - Joomla
- Защита со стороны администратора
  - не храним пароли в FTP-клиентах, средствах разработки и т.д.
  - используем разные пароли для разных сайтов/сервисов и т.д.
  - генерируем надежные пароли, не используем '1234567' - например утилитками apg или pwgen

вебсервер, защита