Pemburu – перебирает резервные копии на сервере.

Cangibrina – Ищет административные каталоги

Уязвимость unrestricted file upload

Многие веб-приложения разрешают пользователям загружать файлы. Как правило, такие файлы не явлюятся исполняемыми – к примеру, это могут быть картники, pdf-документы и т.п. Но такой процесс несет в себе угрозу, если его не контролировать

Злоумышленник может использовать эту возможность для загрузки, например, файлов, php

Локальный upload

Удаленный upload

Проект DVWA – сайт который можно взламывать с разными уровнями сложности.

Session Hijacking

Как работает механизм сессий:

* Пользователь вводит свои данные, они передаются на сервер
* Сервер проверяет данные и если они верны, то создает сессию и сохраняет данные о сессии у себя (зависит от реализации приложения, например в БД)
* Пользователю отдается ответ, в котором будет присутствовать некий параметр, который будет уникальным. Все дальнейшие ответы от пользователя должны будут содержать такой параметр, если такого параметра не будет то пользователь не будет считаться легитимным и доступ такого запроса на сервер должен блокироваться.

Некорректно настроен time out

Inclusion

Защита от LFI

При разработке приложений программистам часто необходимо подключать дополнительные ресурсы, расположенные локально или удаленно (картинки, темы, сценарии)