ВикипедиЯ

Google hacking

Материал из Википедии — свободной энциклопедии

Данная страница не проверялась участниками с соответствующими правами.

Google hacking, также называемый **Google dorking**[1] — это хакерский метод, который используется в Google Search и других приложениях Google для поиска дыр в конфигурации и компьютерном коде, которые используют веб-сайты.

Содержание

Основы

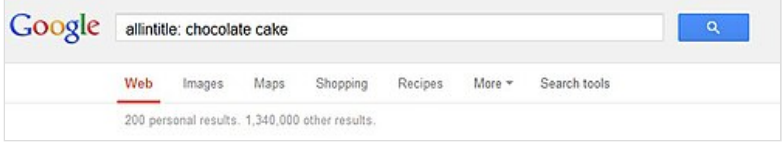
«Google hacking» предполагает использование расширенных операторов в поисковой системе Google для поиска определённых строк текста в результатах поиска. Один из популярных примеров — это поиск конкретных версий уязвимостей Веб-приложений. Поисковый запрос `intitle:admbook intitle:Fversion filetype:php` найдет все веб-страницы, содержащие этот конкретный текст. Обычно при установке приложений по умолчанию их текущая версия указывается на каждой странице, на которой они работают, например, «Powered by XOOPS 2.2.3 Final». Можно найти устройства, подключенные к Интернету.

Строка поиска, например `inurl: "ViewerFrame? Mode =`", найдет общедоступные веб-камеры.

Ещё один полезный вид поиска — это `intitle:index.of`, за которым следует ключевое слово поиска. Так можно получить список файлов на серверах. Например, `intitle: index.of mp3` предоставит все файлы MP3, доступные на различных типах серверов.

Продвинутые операторы

Есть много подобных продвинутых операторов, которые могут использоваться для эксплойтов на небезопасных веб-сайтах:



Пример ввода одной из команд

Оператор	Назначение	Миксовать ли с другими операторами?	Можно использовать отдельно?	Web	Images	Groups	News
intitle	Поиск по заголовку страницы	да	да	да	да	да	да
allintitle	Поиск по заголовку страницы	да	да	да	да	да	да
inurl	Поиск по URL	да	да	нет	да	полностью	как intitle
allinurl	Поиск по URL	да	да	да	да	да	как intitle
filetype: env	конкретные файлы	да	да	да	да	полностью	
intext	Искать только текст страницы	да	да	да	да	да	да
allintext	Искать только текст страницы		да	да	да	да	нет
site	Искать на конкретном сайте	да	да	нет	да	да	полностью
link	Искать ссылки на страницы	да	да	да	да	да	полностью
inanchor	Поиск по якорному тексту	да	да	да	да	полностью	да
numrange	Найти номер	да	да	да	да	да	полностью
daterange	Поиск в диапазоне дат	да	да	да	полностью	полностью	полностью
author	Поиск авторов группы	да	да	да	да	да	полностью
group	Поиск по названию группы		да	да	да	да	полностью
insubject	Поиск по теме группы	да	да	как intitle	как intitle	да	как intitle
msgid	Поиск по msgid группы	да	да	полностью		да	

История Google hacking

Концепция «Google hacking» восходит к 2002 году, когда Джонни Лонг начал собирать поисковые запросы Google, которые раскрывали уязвимости систем и/или раскрытие конфиденциальной информации, назвав их googleDorks.