FrontPage:bugs
[Хакерство в Интернете]

Итак, мои маленькие любители крепких спиртных напитков, сегодня мы поговорим о дырах в очень известном и популярном сервере FrontPage Server. Эти баги известны всем, так что кто их не знает - пусть первый бросит в меня камень(в "мнениях" не ругаться и по почкам не бить:)). Короче, мегакульхацкеры, эта статья для вас:).

Шо це таке?
Frontpage все еще остается одним из самых распространненых инструментов не только по созданию сайта, но и размешения его в сети. Но, что свойственно продукции доблестной фирмы МийкроСакс, содержит огромное количество дыр и уязвимостей. Сам понимаешь, что паролей в одной голове на сто приложений не удержишь, исходя из этого можно сделать заключение - ПАРОЛИ 70%-ОВ ДОСТУПОВ НА КОМПЕ ОДНОГО ЮЗВЕРЯ ОДИНАКОВЫ! Чем и будем злоупотреблять. Можно предположить, что половина паролей фронтпага совпадут с логином к шеллу на сам сервер. А дальше стандартная схема: ломись на телнет, логися , доставай соответствующий системеме эксплойт и копмилируй. Ну а дальше главный бонус - приятный статус привиллегированного пользователя Root.

Рассмотрим самые распространненые баги/глюки/дырки в безопасности сайтов под управлением Microsoft Frontpage Server:

1) Один из самых старых багов. Сейчас этот баг уже не является актуальным, но все же иногда бывают прецеденты. Любой юзер может просматривать файлы на том же диске что и фронтпаг не прилагая больших усилий. Исключением являются файлы в папках самого Frontpage, например /_vti_pvt/. Пример:
http://www.zlob-porno-portal.com/..../Windows/Lamo.pwl
Такой урл позволяет слить файл Lamo.pwl. И так далее со всеми "чувствительными" файлами! Данный баг замечен на системах с Frontpage-PWS32/3.0.2.926, а также некоторых других.

2) Довольно часто на Frontpage сервер стаят расширения pwd или grp, позволяющие администратору или вебдизайнеру удаленно закачивать на сервер файлы. Эти дополнения позволяют хакеру получить контроль чуть-ли не над всем сервером. Все файлы, которыми может воспользоваться хакер, лежат в системной директории Frontpage, а именно, в /_vti_pvt. Эта папка находится в корневой директории сервера. Каждая папка, куда есть доступ посредством Microsoft FrontPage, имеет уникальные права на доступ, и пароли, их определяющие находятся в файлах service.pwd и service.grp. Также можно встретить следующие файлы:

administrators.pwd - для администраторов
authors.pwd - для авторов закачиваемых страниц
users.pwd - для обычных пользователей
В них тоже содержаться пароли

Расширения ФронтПаги создают резервную копию каждого редактируемого файла. Если тв найдешь подобный сайт, прото - поищи в любой директории папку _vti_cnf - вы получите полный список файлов в ней. Скачав любой *.pwd файл, ты увидишь что-то вроде: User:7JyxuUUYY9sgQ. Это всем нам знакомый DES - так что переписывай его в

формат 7JyxuUUYY9sgQ:10:200:User:/users/User:/bin/bash и кормите этим очередного btuteforce cracker'a типа Johna the ripper'a или Shadow Crack`a.
Пример файла users.pwd:

-FrontPage-
jmitchel:7JyxuUUYY9sgQ
wolfe:70yTVencjVNUs
cwolfe:7hT30qItX/v2s

3) Надеюсь, никто не будет спорить, что Microsoft Frontpage - это в первую очередь не веб-сервер, а комплект для разработки и создания сайтов. Наверное, многие из вас, кто занимался дизигном, сталкивались с термином map, т.е. разметка какой-то части рисунка на чуствительные области, например, гиперссылки. Разработчики компании Microsoft включили в свой Frontpage две утилиты, облегчающие жизнь дизайнеру, но довольно-таки сильно затрудняющие жизнь админа: htimage.exe и imagemap.exe. Эти файлы обычно можно найти или в директории /scripts или в /cgi-bin.
Примерное таким способом их и используют:

http://target/path/htimage.exe/mapname?x,y

При запросе с сервера части этой карты (map) диной свыше 741 символа http://target/path/htimage.exe/?0,0 - FrontPage зависает и перестает работать, в отличии от операционной системы. При этом возможно удаленно обратится к регистру EIP на сервере и это делает вполне возможным исполнение удаленно произвольного кода.

Эти поистине многофункциональные утилиты облегчают хакеру еще одну задачу - выяснение расположения Frontpage на сервере. Это возможно, благодаря тому, что при GET запросе к htimage.exe может вернуться путь, показывающий структуру диска.
Для примера:

http://target/cgi-bin/htimage.exe?2.2 может вернуть скажем такой резульатат:
E:websitecgi.

UKR-ХЫР:"....Здесь я, пожалуй, сделаю небольшое лирическое отступление и покажу структуру Frontpage сервера на примере установки его на Windows NT:

Полный путь :
Путь в броузере:

C:InetPubwwwroot

C:InetPubscripts
/Scripts

C:InetPubftproot

C:InetPubwwwroot_vti_bin
/_vti_bin

C:InetPubwwwroot_vti_bin_vti_adm
/_vti_bin/_vti_adm

C:InetPubwwwroot_vti_bin_vti_aut
/_vti_bin/_vti_aut

C:InetPubcgi-bin
/cgi-bin

C:InetPubwwwrootsrchadm
/srchadm

C:WINNTSystem32inetserviisadmin
/iisadmin

C:InetPubwwwroot_vti_pvt...."

4) Рассмотрим следующие файлы ФП: shtml.exe или shtml.dll (в зависимости от операционной системы, установленной на серваке). При попытке открыть с помощью этих вайлов некие несуществующие файлы (html, htm, asp или shtml) на сервере произойдет ошибка и он выдаст сообщение, в котором укажет полный путь к корневой директории сервера. Для примера, выполним запрос:

http://target/_vti_bin/shtml.dll/non_existant_file.html и в ответ вы увидите примерно следующее:

"Cannot open "C:localpath on_existant_file.html": no such file or folder" Примеры запросов:

http://target/_vti_bin/shtml.exe/non-existent-file.html
http://target/_vti_bin/shtml.exe/non-existent-file.htm
http://target/_vti_bin/shtml.exe/non-existent-file.shtml
http://target/_vti_bin/shtml.exe/non-existent-file.asp

5) С фронтПагой в стандартном комплекте поставляется каунтер(типа счетчик посещений), находится он здесь :/scripts/fpcount.exe. Хотя бы один такой счетчик может подвесить весь сервер! Использование:
Данный счетчик выполняется с параметрами:

fpcount.exe?Page=default.htm|Image=3|Digits=6.
Т.е. http://www.zlop-porno-portal.com/scripts/fpcount.exe?Page=default.htm|Image=3|Digits=6
Интерес представляет последний параметр - количество разрядов. Попросив счетчик показать, к примеру, 32767 цифр вы получите переполнение буфера и запуск доктор ватсона (или другого отладчика, запущенного по умолчанию), который отожрет примерто 4 мегабайта памяти на сервере. Заставив сервер выполнить такой вопрос 20-30 раз(зависит от тачки), вы забъете всю память на атакуемом компе и в следующий раз свалится уже не fpcount.exe, а сам Internet Information Server. Итак, "смертельный" URL - http://www.zlob-porno-portal.com/scripts/fpcount.exe?Page=default.htm|Image=3|Digits=99999, где www.zlob-porno-portal.com - URK жертвы. 5) Каким макаром?

Найти сервак на ФронтПаге очень просто! Идешь на www.altavista.com и и задаешь для поиска строку /_vti_pvt. Далее перебирай все найденные ссылки и ищи сайты,на которых стоит Front Page со всеобщим обозрением фалов паролей.
Еще один способ:
З.Ы. Сайт http://www.zlob-porno-portal.com использовался как домен жертвы, а не как мой порно сервер:). Кстати хорошая идея...

З.Ы. Благодарности за помощь в создании статьи объявляются следующим перцам: UkR-XblP, cluz, группа GIN.

zLOB