ХАКИНГ FIREFOX

СОДЕРЖАНИЕ ЭТОЙ СТАТЬИ

0. INTRO

Эта статья предназначается в основном для новичков, или для тех, кто не знает какие возможности скрываются в браузере Mozilla Firefox.

В ней рассказывается о дополнительных примочках (расширениях), которые могут помочь, скажем, при реализации XSS или веб разработчикам.

1. УСТАНАВЛИВАЕМ FIREFOX

Фаерфокс появился совсем недавно, но уже успел завоевать огромную популярность. Я начал работать с браузером, начиная с первой версии. Сейчас уже появилась бета версия 2.0.

Для того, чтобы сделать все о чем здесь написано вам надо скачать, прежде всего, сам браузер. Я предлагаю скачивать версию Фаерфокса, которая не требует установки и хороша для хакера, потому что настройки программы не хранятся в реестре. Эта версия называется Portable Firefox и занимает на диске около 15.7 МБ. Сам же скачиваемый .zip архив занимает 6.2 МБ. Все, что описано ниже будет испытываться на версии 1.5.0.3 Portable Firefox.

Архив можно скачать со страницы с зеркалами:
http://prdownloads.sourceforge.net/...us.zip?download
Сайт поддержки этой версии находится здесь:
http://portableapps.com/apps/intern...ortable_firefox

2. О РАСШИРЕНИЯХ

У Фаерфокса существует огромное количество расширений, за счет которых можно добавлять в браузер новые возможности. Только надо уметь отличать плагины (plugins) и расширений (extensions). Если кратко пояснить разницу между ними, то она заключается в том, что плагины - это программы, которые нужны для того, чтобы просматривать в окне браузера Firefox различные типы документов и специфичное содержание страниц в Интернете (Acrobat-PDF, Flash, Java, QuickTime, RealPlayer, Shockwave, DjVu, WindowsMedia и др.). А расширения - это маленькие (иногда не очень) и полезные дополнения, которые нужны для увеличения функциональности и привнесения новых возможностей в браузер. Это, например, поисковые расширения и новые возможности навигации, просмотр текущей погоды и новые способы коллекционирования закладок, новые возможности для веб-дизайнеров и различные способы управления многооконностью, различные панели, банерорезки и т. д. и т. п. К слову, плагинов пока на порядок меньше (десятки), по сравнению с огромным количеством расширений (сотни, если не тысячи).

Расширения это .xpi файлы, представляющие ничто иное, как простые .zip архивы. Вы можете взять архиватор и заглянуть внутрь любого расширения. Существует несколько способов установки расширений. Лично я предпочитаю ставить их руками. Для этого нужно скачать .xpi файл, а потом выбрать его из главного меню: File → Open File.

Когда расширение установлено, его файлы появляются в директории PortableFirefoxDataprofilesextensionGUID при условии, что вы разархивировали браузер в папку PortableFirefox. Здесь GUID (Globally Unique Identifier) это обычная папка, которой при установке расширения, присваивается уникальное имя (идентификатор). Вот несколько примеров GUID: {c36177c0-224a-11da-8cd6-0800200c9a66}, {761a54f1-8ccf-4112-9e48-dbf72adf6244}. Все установленные расширения доступы через главное меню: Tools → Extensions.

Помимо этого для установки можно просто скопировать старые GUID-папки (если они у вас есть) в новую директорию extension. Если все сделано правильно, вы увидите расширение через Tools → Extensions.

3. СТАВИМ ПОЛЕЗНЫЕ РАСШИРЕНИЯ

Все описанные ниже расширения можно скачать отсюда: http://www.extensionsmirror.nl/
https://addons.mozilla.org/firefox/extensions/
http://mozmonkey.com/
Кстати, еще один способ поиска расширений, это просто вставить его название в строку браузера, где вы обычно вводите URL.

Вот список расширений, которые мы установим с кратким описанием (номера версий я опустил):

- **Add N Edit Cookies** - позволяет создавать и редактировать кукки.

- **Fasterfox** - увеличивает скорость браузера.

- **ImgLikeOpera** - добавляет кнопку, позволяющую включать и выключать отображение рисунков на страницах (аналогично браузеру Opera). Кроме этого может вырубать флэш (нужно включить вкладку "Экспериментальные настройки").

- **LinkChecker** - проверяет все ссылки на странице и в зависимости от того работает ссылка или нет, окрашивает ее в соответственно светло-зеленый или розовый цвет.

- **MR Tech Local Install** - мощная утилита для управления конфигурацией Firefox.

- **SwitchProxy Tool** - утилита, позволяющая быстро и лекго управлять проксями.

- **UrlParams** - показывает значения параметров в боковой панели, передаваемых методами GET и POST. С помощью этого расширения можно передать серверу произвольные параметры, используя эти методы.

- **Web Developer** - большое расширение, дополняющее меню и панель с различными тулзами, полезными как для веб-разработчика, так и для хакера.

- **FormFox** - когда курсор находится над кнопкой отправки данных из формы, выводится информация о том, куда они будут переданы.

- **Tamper Data** - перехватывает запросы и позволяет изменять в их заголовках разные поля.

- **User Agent Switcher** - позволяет изменить браузер, так, что другие будут думать, что вы просматриваете их страничку, скажем, Оперой или это вообще Googlebot. Это достигается изменением поля User-Agent заголовка запроса.

- **Live HTTP Headers** - с этим расширением вы можете снифать (просматривать) HTTP-заголовки. Удобно использовать при написании скриптов, которые работают с сокетами.

Возможно, вам также окажутся полезными для отладки JavaScript-кода следующие два расширения:
- **Venkman**
- **Firebug**

Только имейте в виду: при большом кол-ве расширений Фаерфокс будет тормозить! Так что пробуйте сами, выбирая для себя лучшие и удаляя лишние.

После скачки можно вынести любимые расширения на новую панель. Панель создается через главное меню: View → Toolbars → Customize... в появившемся окне нужно нажать

на кнопку Add New Toolbar. После ввода имени панели, перетащите на нее нужные кнопки.

Если какие-то расширения вам не нравятся, их можно легко удалить в окне, вызываемом через меню Tools → Extensions. В нем надо выбрать нужное расширение и нажать кнопку Uninstall. Или это можно сделать руками, узнав название GUID папки. Но тут возникает вопрос - как это сделать? Это очень просто - нужно щелкнуть правой кнопкой мыши на расширении и в самом низу будет пункт Copy GUID (этот пункт появится только при установке MR Tech Local Install).

Бывают слачаи, когда вам надо поставить расширение, но оно предназначено для предыдущей версии браузера и не поддерживается текущей. Установим для примера, расширение DOM Inspector, поставляемое в стандартной комплектации и отсутствующее в Portable Firefox.

Зайдем в директорию где находится стандартный вариант Мозиллы (у меня он версии 1.5.0.1) и найдем там нашего Инспектора DOM. Папка с его файлами называется inspector@mozilla.org
и находится в директории extensions (кстати, вот вам еще один способ задания GUID). Скопируем ее полностью в директорию с расширениями Portable Firefox. После этого запустим его и глянем в меню Tools. Как и ожидалось, расширение не установлено, о чем свидетельствует красноречивая надпись: «Disabled – not compatible with Firefox 1.5.0.3». Это надо исправлять.

Закроем браузер и найдем в папке inspector@mozilla.org текстовый файл install.rdf. Откроем его чем-нибудь и найдем такие строки:

Код:

```
<em:targetApplication>  <!-- Firefox -->  <Description>
<em:id>{ec8030f7-c20a-464f-9b0e-13a3a9e97384}</em:id>

<em:minVersion>1.5.0.1</em:minVersion>

<em:maxVersion>1.5.0.1</em:maxVersion>
```

```
    </Description>

  </em:targetApplication>
```

В строке <em:maxVersion>1.5.0.1</em:maxVersion> меняем номер максимальной версии, для которого создано расширение на нужный и сохраняем файл. Можно вместо цифры поставить звездочку, тогда расширение будет поддерживать целый диапазон браузеров, например:

Код:

```
    <em:maxVersion>1.5.0.*</em:maxVersion>
```

После этого нужно перенести куда-нибудь папку inspector@mozilla.org , открыть браузер, закрыть его и вернуть директорию с Инспектором обратно. Это хитроумное действие заставит перечитать Фаерфокс директорию с расширениями. Конечно, все это можно было сделать проще, кликнув правой кнопкой в окне Extensions на расширении и выбрав Make Compatible. Но этот способ хорош, если у вас установлено соответствующее расширение.

Рассмотреть возможности всех расширений практически нереально, зато можно кое-что рассказать о встроенных средствах. По умолчанию с Мозиллой поставляется консоль JavaScript. Ее можно вызвать через главное меню: Tools → JavaScript Console. Консоль это отладочный инструмент и позволяет выявить ошибки в сценариях JavaScript, возникающие при загрузке страницы. Она способна выдавать три типа информации:
- ошибки;
- предупреждения;
- сообщения.

Всю отладочную информацию можно посмотреть, щелкнув по нужной кнопке в консоли. А их всего там пять штук, и называются они точно так же - "Ошибки", "Предупреждения" и "Сообщения". Четвертая кнопка называется "Все" и позволяет просмотреть все найденные баги разом. Пятая кнопка называется "Очистить" и как можно понять из ее

названия очищает консоль.

4. КОНФИГУРАЦИОННЫЕ ФАЙЛЫ

Браузер хранит расширения (extensions), темы (themes), закладки (bookmarks), сохраненные значения форм, пароли в профиле пользователя. Для разных операционных систем профили хранятся в разных местах, но в нашем случае он будет находиться в директории PortableFirefoxDataprofile.

Приведу список и описание ключевых конфигурационных файлов Мозиллы:
- bookmarks.html: В этом файле сохраняются закладки.
- cookies.txt: В этом файле сохраняются кукки.
- pref.js: Здесь сохраняются изменения в настройках браузера. Например, вы изменили домашнюю страничку, или размещение папки для закачки и т. д.
- hostperm.1: Содержит настройки прав для куккисов и рисунков.
- formhistory.dat: Содержит содержимое полей форм для автозаполнения на веб-страницах.
- user.js, chromeuserContent.css и chromeuserChrome.css: Это файлы с личными предпочтениями пользователя и должны создаваться вручную.

Некоторые из этих файлов вы можете редактировать, используя только что установленные расширения. Но дело в том, что они имеют множество тонкостей, поэтому за описанием их формата я посоветую сходить сюда: http://preferential.mozdev.org/preferences.html

5. ИЗМЕНЯЕМ НАСТРОЙКИ БРАУЗЕРА

Для начала надо ввести, где вы обычно вводите адрес такую строку:

Код:

```
about:config
```

После нажатия Enter, появится окно настроек Фаерфокса, содержащее четыре колонки.
- Preference Name
- Status
- Type
- Value

Каждая строка отвечает за определенный элемент браузера. Скажем, меняя значение настройки под названием javascript.enabled с true на false мы отключаем JavaScript. Действие этого способа можно проверить, зайдя в опции: Tools → Option и потом перейти на вкладку Content.

Нужную настройку можно поискать, введя ее имя в строке Filter. По мере того, как вы будете печатать название, из списка удалятся все настройки, имена которых не содержат то, что вы ввели. Обратно к полному списку можно вернуться, нажав кнопку «Show All».
Измененные настройки (это напротив которых в столбце Status стоит user set) выделяются жирным шрифтом и сохраняются в файле prefs.js. Который, к слову, можно редактировать и вручную.

Выше мы сказали, что существует еще один файл – user.js. При установке Portable Firefox он пуст, а при стандартной - его вообще не существует. Настройки в файле user.js перекрывают одноименные из файла prefs.js. Браузер ничего не пишет в файл user.js, а только считывает оттуда информацию. Основное назначение файла user.js – это сохранение таких настроек, которые не сможет никто изменить. Этот файл может быть полезен для администратора компьютерного клуба. Он может создать один файл, а затем разослать его копии по всем машинам. Или, если вы боитесь, если какое-то расширение или человек изменит настройки браузера, просто сохраните нужные в фале user.js.

Файлы user.js и prefs.j имеют очень простую структуру. Настройки хранятся в виде строк:

Код:

```
user_pref("название_настройки", значение);
```

Значение может быть всего трех типов: целого (Integer), булевского (Boolean) и строки (String). Если вы учили программирование, то наверное, знаете, что строки должны заключаться в кавычки.

Файлы userContent.css и userChrome.css отвечают за визуальное поведение браузера. Например, за такие вещи как главное меню, размер шрифта на веб-страницах, расстояние между иконками на панели инструментов или рисунками на веб-страницах, скрытие меню и других элементов. Файл userChrome.css отвечает за интерфейс Фаерфокса, а userContent используется для настройки веб-страниц. Словом chrome разработчики Мозиллы называют визуальные элементы. Чтобы редактировать эти файлы тебе придется подучить CSS (Cascading Style Sheets).

В директории chrome при установке создаются два файла примера - userContent-example.css и userChrome-example.css. Вы можете их переименовать в userContent.css и в userChrome.css и попробовать что-нибудь в них изменить.

В заключении хочу поделиться полезными ссылками.
Исходники браузера можно найти здесь: ftp://ftp.mozilla.org/pub/mozilla.org
Сайт поддержки: http://developer.mozilla.org/en/doc...d_Documentation

Для Windows, чтобы расспаковать архив с расширением *.bz2 сходите на сайт http://www.7-zip.org/
за классным архиватором.

6. ЗАКЛЮЧЕНИЕ

Ну вот и все о чем я хотел рассказать. Принимаются любые замечания. Скажите, если есть какая-то неточность или чем еще можно дополнить статью.

Источники инфы: Hacking Firefox: More Than 150 Hacks, Mods, and Customizations
Благодарности:
+toxa+ за полезное дополнение.

оригинал: http://forum.antichat.ru/printthread.php?t=20265&pp=40

{jcomments on}