عنوان: **شرح یک مشکل امنیتی با فایرفاکس**
نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۴/۰۲ ۱۱:۶
آدرس: www.dotnettips.info
برچسب‌ها: Firefox, Security

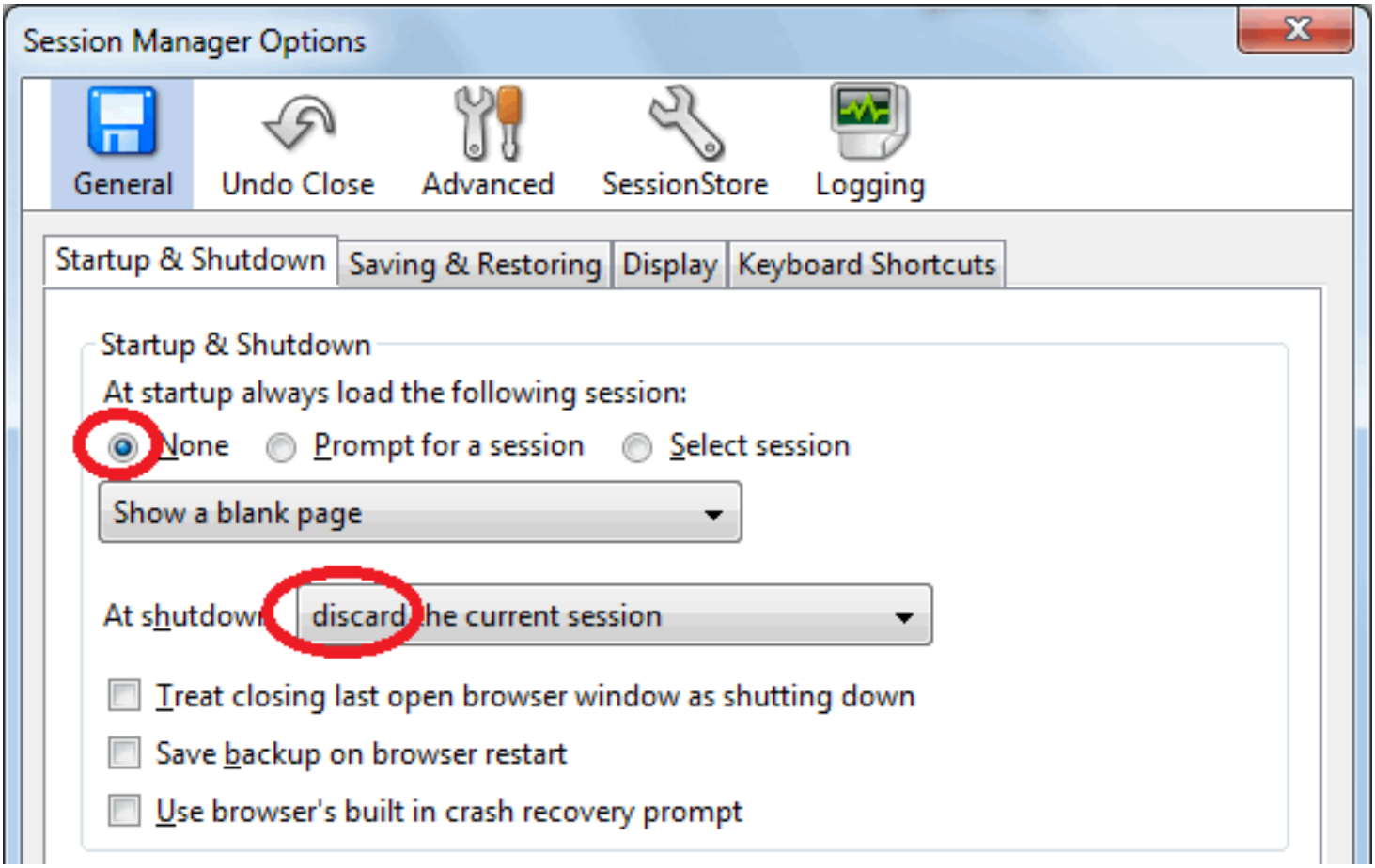
حدود دو ماه قبل دوبار از طریق میل‌باکس یاهو من به تمام contactهای تعریف شده در آن ایمیلی با محتوای زیر ارسال شده بود:

```
Hello,
you should definitely check this thing out http://www.newsl5.net/biz/?page=xyz
```

این ایمیل‌ها هم جعلی نبودند. یعنی واقعا از اکانت یاهوی من ارسال شده بودند و در قسمت sent وجود خارجی داشتند! فقط IP ارسال کننده آن (115.78.224.246) متعلق به کشور ویتنام بود (IP ارسال کننده را در هدر ایمیل ارسالی می‌توان مشاهده کرد).
این مساله باعث شد که من سیستم را چندین بار چک کنم؛ از لحاظ بحث ویروس تا اسپای‌ور و غیره. «هیچ» مشکلی مشاهده نشد.
مرحله بعد کمی در مورد یاهو جستجو کردم و مشخص شد که یاهو با session hijacking به شدت مشکل دارد. همچنین ابزار دیگری که می‌تواند به این session hijacking کمک کند خود «فایرفاکس» است. فایرفاکس حاوی گزینه‌ای است که سشن‌های قبلی شما را ذخیره می‌کند. زمانیکه مرورگر را بسته و پس از مدتی آن‌را باز می‌کنیم، یک راست و قشنگ همان سشن قبلی مثلا یاهو را بازیابی کرده و کار ادامه پیدا می‌کند.
کمی گشتم و این قابلیت رو به کل غیرفعال کردم. برای غیرفعال کردن آن «Disable Session Restore in Firefox» را در گوگل جستجو کنید.
و خلاصه آن به صورت زیر است:
در نوار آدرس فایرفاکس تایپ کنید about:config
در ادامه موارد زیر را یافته و غیرفعال کنید:

```
browser.sessionstore.resume_from_crash;false
browser.sessionstore.resume_session_once;false
browser.sessionstore.restore_pinned_tabs_on_demand;false
browser.sessionstore.restore_hidden_tabs;false
services.sync.prefs.sync.browser.sessionstore.restore_on_demand;false
```

راه ساده‌تر:
افزونه session manager را نصب کنید
در قسمت session manager options در برگه startup & shutdown آن کلا بحث ذخیره سازی سشن در حین بسته شدن مرورگر را غیرفعال کنید.



و به صورت خلاصه: تنظیمات پیش فرض فایرفاکس از لحاظ امنیتی مناسب نیستند.
ضمن اینکه ایمیل فوق رو من هفته‌ای یکی دو بار از تمام افرادی که می‌شناسم دریافت می‌کنم! به عبارتی خیلی‌ها گرفتار این مساله شده‌اند.
ذخیره سازی سشن‌ها به نظر کارها رو ساده می‌کنه. مرورگر رو باز می‌کنی همه چیز مثل قبل از بسته شدن آن است و ... همین یعنی مشکل امنیتی. خصوصا مراجعه به سایت‌ها و لینک‌هایی که از باگ‌های XSS سوء استفاده می‌کنند.

نظرات خوانندگان

نویسنده: میثم هوشمند
تاریخ: ۱۳۹۱/۰۴/۰۲ ۱۴:۱۱

خب یعنی فایر فاکس مشکل امنیتی دارد؛ و این مشکلی که برای شما به وجود آمده به دلیل ورود به سایتی بوده که حمله XSS صورت داده است؟

نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۴/۰۲ ۱۶:۲۹

بله. این مشکلی که نام بردم خیلی دامنه دار است. حدود چندماهی است که مدام برای تمام آشناهای من ارسال شده و همه مشکل پیدا کردن.
علت اینکه امروز این مطلب رو نوشتم دریافت مجدد چندباره یک چنین ایمیلی از آشناها بود.
مشخصات آن هم این است که به تمام contactهای تعریف شده شما ارسال شده و در قسمت sent قابل مشاهده است.

نویسنده: احسان
تاریخ: ۱۳۹۱/۰۴/۰۳ ۲۰:۲۳

من ابتدا session manager رو استفاده کردم و تنظیمات رو طبق راهنما انجام دادم
ولی هنوز browser.sessionstore.resume_from_crash در حالت فعال بود
بنابراین به صورت دستی هم کار رو انجام دادم که خاطر جمع باشه