کوکیها، پایش‌افزارهای نهان و آشکار!؟

□تورج صارمی راد

آشنایی

ردنماها یا **کوکیها** (cookies) پرونده‌های نوشتاری کوچکی هستند که هنگام بازدید **وب‌گردان** از پایگاههای وب، در رایانهٔ کاربران جای می‌گیرند. این پرونده‌های نوشتاری دارای دانستیهایی هستند که به پایگاه وب یاری می‌رساند کارکرد وبگرد را ردگیری کند و نیازهای او را بشناسد.

ولی برخی می‌انگارند ردنماها برنامه‌هایی هستند که پایگاه‌های وب گوناگون آنها را در رایانه‌های کاربران اینترنت می‌گذارند. آنها می‌توانند اجرا شوند و دانستیهایی دربارهٔ وبگردی کاربران گردآورند. این گونه دانستیها می‌توانند هنگام نیاز پایگاه وب، به آن جا فرستاده شوند. این تعریف، نادرست و نارسا است، زیرا:

۱. ردنماها پرونده‌های نوشتاری هستند نه برنامه‌های اجرایی؛

۲. از آن جایی که ردنماها برنامه‌های اجرایی نیستند، نمی‌توانند اجرا شوند؛

۳. از آن جایی که نمی‌توان آنها را اجرا کرد، نمی‌توانند به شیوهٔ خودکار دانستیهایی دربارهٔ کاربران اینترنت گردآورند.

بنابراین، تعریف درست و رسای ردنماها این است که آنها بسته‌ها یا تکه‌های کوچک نوشتاری هستند که **کارساز وب** (Web server) می‌توانند در دیسک سخت کاربران ذخیره کند و در آنها مجموعه‌ای از دانستیهای گوناگون مانند **گذرواژه، نام کاربری** و هر آن چه وبگرد در آن پایگاه وب نوشته است، بگذارد. بنابراین، اگر نشانی **رایانامه‌ای** (e-mail)، شمارهٔ تلفن و... را در اختیار پایگاه وب گذاشته باشید، شاید آنها را بتوان در پرونده‌های ردنمای نوشتاری دید. افزون بر این، داده‌های دیگری چون زمان و تاریخ وبگردی، پیوندهای مورد بهره نیز در آنها نوشته می‌شوند. برای نمونه، گوگل، نشانی پایگاه‌های وب، زمان، تاریخ، گونهٔ مرورگر وب، نام نظام عامل و شمارهٔ ردنما را می‌نویسد. در ضمن، اگر کاربر واژه یا گزاره‌ای را کاویده باشد آنها را نیز در ردنما می‌نویسد. بدین گونه، گوگل و برخی دیگر از کاوشگران می‌توانند کارهای زیر را انجام دهند:

۱. سیاهه‌ای از کسانی که واژه یا گزاره‌ای را کاویده‌اند، تهیه کنند؛

۲. وارونهٔ مورد «۱»، می‌توانند با بهره‌گیری از نشانیهای اینترنتی، سیاهه‌ای از واژه‌ها و گزاره‌های کاویده‌شدهٔ کاربران نشانی ویژه‌ای، تهیه کنند؛

۳. با بهره‌گیری از پردازش وارونهٔ مسیر (redirection)، پیوندهایی که دیگران به کار برده‌اند را بیابند.

ولی اگر از پرگویی دست برداریم، می‌توان گفت:

۱. در نخستین بازدید از پایگاه وب، هیچ پیشینه‌ای از کاربر در دست نیست؛

۲. در نخستین بازدید از پایگاه وب، پروندهٔ نوشتاری کوچکی در رایانهٔ کاربر جای می‌گیرد؛

۳. در صورتی که کاربر ردنمای نخستین بازدید را پاک نکند، پس از آن، هنگام بازدید، پروندهٔ ردنمای پیشین بهنگام می‌شود؛

۴. در بیشتر وقتها در ردنماها داده‌های شخصی مانند شمارهٔ تلفن، شمارهٔ کارت اعتباری و نشانی نوشته نمی‌شود؛ بلکه در آنها تنها نشانی پایگاه وب و شناسهٔ یکتایی نوشته می‌شود. این شناسهٔ یکتا به جدولی در بانک داده‌ای پایگاه موردنظر اشاره دارد. بدین گونه، پایگاه وب از آن برای بازیابی داده‌ها بهره می‌گیرد. این شیوهٔ بهره‌گیری از داده‌ها باعث می‌شود:

الف- داده‌های شخصی کاربر در بانک داده‌ای امن نگهداری شود؛

ب- دشواریهای حاصل از بهره‌گیری چند کاربر از یک رایانه، یا بهره‌گیری یک کاربر از چند رایانه از بین برود؛

پ- در صورتی که کاربر رایانه همهٔ پرونده‌های ردنما را پاک کند بازهم بتوان او را ردگیری کرد.

بدین گونه دانسته می‌شود:

۱. ردنماها پرونده‌های نوشتاری کوچکی هستند؛

۲. در بیشتر ردنماها داده‌های شخصی کاربر نگهداری نمی‌شود. یعنی، می‌شود این کار را انجام داد. برای همین، گاهی این کار انجام می‌گیرد؛

۳. دادهٔ همگانی در ردنماها، نشانی پایگاه وب و شناسهٔ یکتایی است که به بانک داده‌ای کاربر در پایگاه وب اشاره دارد؛

۴. از ردنماها برای ردیابی کاربران و اعمال تنظیمهای پیشین آنها بهره گرفته می‌شود؛

۵. بیشتر وقتها پرونده‌های ردنما بی‌زیان هستند. با وجود این، اغلب، از آنها، برای فرستادن پیامهای ناخواسته و پیامهای بازرگانی بهره گرفته می‌شود.

کاربرد ردنماها

با توجه به آن چه گذشت، دانسته می‌شود در ردنماها دانستنیهای گوناگونی می‌تواند ذخیره شود. برای همین، آنها را می‌توان برای کاربردهای گوناگونی به کار برد. برای نمونه، پایگاه‌های وب هواشناسی می‌توانند با ذخیرهٔ شمارهٔ شناسایی منطقهٔ زندگی کاربر اینترنت، به راحتی وضع آب و هوای منطقهٔ کاربر را نشان دهند. یا می‌توان در ردنماها گذرواژه و نام کاربری را ذخیره کرد. در نتیجه، لازم نیست در هر بار وبگردی وبگرد، آنها را بنویسد. یا با بهره‌گیری از داده‌های پرونده‌های ردنما، می‌توان ضربه‌های تقلبی ماوس بر روی آگهی‌های بازرگانی در پایگاه‌های وب را، از ضربه‌های راستین شناخت. بدین گونه، از افزایش هزینهٔ آگهی‌دهندگان پیشگیری کرد. با توجه به این نمونه‌ها، می‌توان کاربردهای ردنماها را در موردهای زیر دانست:

۱. شمارش‌شمار راستین بازدیدکنندگان از پایگاه‌های وب؛

۲. پیشگیری از افزایش هزینهٔ آگهی‌دهندگان در پایگاه‌های وب؛

۳. نگه‌داری پیشینهٔ خریدها در بازرگانی الکترونیکی و خریدهای بر خط (online)؛

۴. پیشگیری از بازنویسی گذرواژه و نام کاربری در پایگاه‌های وب ویژه؛

۵. سفارشی کردن نتیجهٔ کاوشهای شخصی؛

۶. گزینش موضوعهای دلخواه در پایگاه‌های وب؛

۷. ....

برای انجامش این گونه کارها، هنگامی که کاربری از پایگاه وبی بازدید می‌کند، مرورگر وب نشانی پایگاه وب را می‌سنجد و دنبال ردنمای آن پایگاه وب، در دیسک سخت وبگرد می‌گردد. اگر ردنمای پایگاه وب را بیابد، آن را به کارساز وب می‌فرستد تا از داده‌های آن بهره گیرد؛ ولی اگر مرورگر وب ردنمایی نیابد، کارساز وب دانستنیهای ردنما را در رایانهٔ وبگرد می‌گذارد.

گاهی کارساز وب پرسشهایی چون نام کاربری و گذرواژهٔ وبگرد را می‌پرسد، پس از آن، با بهره‌گیری از آنها ردنما را در رایانهٔ وبگرد می‌سازد.

بخش‌بندی

اندیشهٔ نخستین کاربرد ردنماها این بود که پایگاه وب مورد بازدید وبگرد، مشهور به **پایگاه‌های وب گروه اصلی** (نخست [1])، بتوانند داده‌هایشان را بر پایهٔ نیازهایشان تهیه و تنظیم کنند. افزون بر این، وبگردان را از زحمت بازنویسی داده‌های پیشین، هنگام بازدید از پایگاه‌های وب رها کنند؛ ولی اکنون پایگاه‌های وب دیگری نیز که در پایگاه وب مورد بازدید وبگرد، دارای آگهی بازرگانی و... هستند، می‌توانند به محتوای ردنماها دست یابند. به این گونه پایگاه‌های وب، **گروه سوم** [2] می‌گویند. با توجه به آن چه گذشت، می‌توان ردنماها را به دو گروه زیر بخش کرد:

۱. **ردنماهای یکتا:** این گونه از ردنماها، تنها به پایگاه وب وابسته فرستاده می‌شوند. کار این گونه از ردنماها، اغلب، یادآوری دانستنیهای وبگردان به پایگاه وب است.

۲. **ردنماهای چندگانه:** این گونه از ردنماها افزون بر پایگاه وب اصلی، در اختیار پایگاه‌های وب گروه سوم نیز قرار می‌گیرند. رخنه‌گران می‌توانند از این گونه ردنماها بهره‌برداری کنند.

برای نمونه، کرم **باگ‌بیر.ای** (Bugbear.E)، سه پرونده از گونهٔ «دی‌ال‌ال» با نامهای تصادفی در پوشهٔ سیستم ویندوز می‌سازد که با بهره‌گیری از آنها می‌تواند ضرب کلیدهای صفحه‌کلید رایانهٔ آلوده را بنگارد و داده‌های حساس کاربر رایانهٔ آلوده را بدزدد. این کرم می‌تواند داده‌های موجود در ردنماها، نوشته‌های گوناگون پنجره‌های ویندوز، ضرب کلیدهای صفحه‌کلید، داده‌های موجود در **رابط جابه‌جایی** (clipboard) در حافظه را بدزدد. بدین گونه، می‌توان گفت:

۱. این گفته درست نیست که دیگر پایگاه‌های وب، نمی‌توانند ردنماهای وابسته به سایر پایگاه‌های وب را بخوانند.

۲. این گفته درست نیست که داده‌های ردنما به صورت مستقل به کار می‌روند و مورد بهره‌برداری اشتراکی قرار نمی‌گیرند.

۳. این گفته درست نیست که ردنماها خطری برای رایانه‌های وبگردان ندارند؛ زیرا آنها می‌توانند مورد بهره‌برداری رخنه‌گران، پیام‌پراکنان و ویروس‌نویسان قرار گیرند.

۴. این گفته درست نیست که ردنماها ویروس هستند، بنابراین آنها نمی‌توانند به عنوان ویروس به کار روند. به راستی، آنها تاکنون توانایی این که بتوانند محتوای ویروسی داشته باشند از خود نشان نداده‌اند؛ زیرا آنها پرونده‌های نوشتاری هستند. با وجود این، از پرونده‌های ردنما می‌توان برای شناسایی کاربران اینترنت و تشکیل پروندهٔ پیشینهٔ کاربران بهره گیرند. برای نمونه، گوگل، یاهو، مایکروسافت و... نتیجهٔ کاوشهای کاربران اینترنت را با بهره‌گیری از ردنماها به صورت نامحدود نگه می‌دارند. یعنی، کاوشگران اینترنتی نتیجهٔ کاوشهای کاربران اینترنت را گرد می‌آورند.

۵. شاید کاستیهای مرورگرهای وب باعث شود، رخنه‌گران بتوانند ردنماها را به کار گیرند. برای نمونه، نگارشهای نخستین نت‌اسکیپ

---

[1] first party
[2] third party

کاستی‌ای داشتند که بر پایهٔ آن، می‌شد کاری کرد که ردنماها به پایگاه‌های وب دیگری نیز فرستاده شوند.

۶. داده‌های موجود در ردنماها بدون هیچ رمزی ذخیره می‌شوند. بنابراین، امکان یافتن و خواندن آنها وجود دارد. در نتیجه، می‌توان هنگام برنامه‌نویسی کاری کرد که داده‌های موجود در ردنماها به رمز درآیند. بدین‌گونه، آنها را درک‌ناپذیر کرد.

۷. با بهره‌گیری از ردنماها می‌توان به عادتها، رفتارها و علاقه‌مندی‌های وبگردان پی برد.

بخش‌بندی دیگری از ردنماها بر پایهٔ زمان پایداری انجام می‌شود. آنها را بر پایهٔ زمان پایداری به دو گروه زیر بخش می‌کنند:

۱. **ردنماهای پایدار (persistent):** این گونه از ردنماها دارای تاریخ پایان کار ویژه‌ای هستند. یعنی، آنها هنگام بازدید از پایگاه‌های وب ساخته می‌شوند و تا تاریخ پایان کار در دیسک سخت کاربر می‌مانند؛ مگر این که کاربر آنها را پاک کند. برای نمونه، به داده‌های جدول شمارهٔ «۱» بنگرید.

سال پایان کار ردنما	نام شرکت
۲۰۱۱	آمریکا آن‌لاین
۲۰۲۸	گوگل
۲۰۱۶	مایکروسافت
۲۰۱۰	یاهو

جدول ۱: تاریخ پایداری ردنماهای چند شرکت سرشناس

این گروه از ردنماها دارای ویژگیهای زیر هستند:

الف- پس از بستن مرورگر وب پاک نمی‌شوند؛

ب- توانایی به هنگام شدن توسط پایگاه وب وابسته به ردنما را دارند؛

پ- در صورتی که کاربر رایانه آنها را پاک نکند، یا دیسک سخت خراب نشود، تا پایان تاریخ کار در دیسک سخت باقی می‌مانند؛

ت- درون آنها داده‌های پرکاربرد یا طولانی ذخیره می‌شوند. برای نمونه، اگر کاربری نخواهد گذرواژهٔ ورود به وبگاهی را در هر بار بازدید بنویسد، گذرواژه، درون ردنما ذخیره می‌شود. داده‌های بسیاری را می‌توان نام برد که وبگرد حوصلهٔ بازنویسی آنها را در هر بار بازدید از پایگاه وب ندارد. این داده‌ها می‌توانند درون ردنماها ذخیره شوند. بدین گونه، کاستی ایمنی به وجود می‌آید.

۲- **ردنماهای گذرا (persession):** این گونه از ردنماها هنگام بازدید از پایگاه‌های وب ساخته و مورد بهره‌گیری واقع می‌شوند؛ ولی پس از بستن مرورگر وب، یا خروج از پایگاه وب پاک می‌شوند. یعنی، این گونه از ردنماها درون حافظه و هنگام بازدید از پایگاه‌های وب به وجود می‌آیند و دورن خود **شناسهٔ نشست** (session ID) را نگه می‌دارند.

رخنه‌گران دسترسی مستقیم به ردنماهای گذرا ندارند. برای همین، برخی از برنامه‌نویسان وب می‌گویند: ردنماهای گذرا اعتمادپذیر و دگرگون‌ناپذیر هستند. در نتیجه، دگرگونی در شناسهٔ نشست ناممکن است. با وجود این، در اکتبر سال ۲۰۰۰ نرم‌افزاری با نام «آشیل» (Achilles) شناسایی شد که توانایی یورش به ردنماهای گذرا و هر رشتهٔ پنهان «اچ‌تی‌تی‌پی» را داشت. این برنامه، می‌تواند بین مرورگر وب و کارساز آماج یورش جای گیرد و داده‌های جابه‌جایی را بگیرد و در اختیار رخنه‌گر بگذارد. این داده‌ها را رخنه‌گر می‌تواند ویرایش و دگرگون کند. پس از دگرگونی، رخنه‌گر می‌تواند آنها را به مقصد بفرستد.

بخش‌بندی دیگری نیز از ردنماها می‌شود و آن جای دادن آنها در گروه **پایش‌افزارها**ست. یعنی، برخی در گروه‌بندی پایش‌افزارها، ردنماها را جای می‌دهند؛ زیرا آنها به پایگاه وب این توانایی را می‌دهند که وضع مرورگر را در بازه‌های زمانی با هم بسنجد و با گذشت زمان داده‌هایی دربارهٔ رفتار کاربران پایگاه وب گرد آورد. با این داده‌ها می‌توان کاربران وب را بر پایهٔ رفتارشان رده‌بندی و هدفهای بازرگانی را بر پایهٔ آنها تنظیم کرد. افزون بر این، کاوشگران اینترنتی توانایی گردآوری نتیجهٔ کاوشها و ارتباط دادن آنها به هم را دارند.

باید توجه داشت هر ردنما با کلید ویژه‌ای پاسداری می‌شود. بنابراین، در بیشتر موردها بهره‌برداری از آنها بدون کلید ویژه امکان‌پذیر نیست. در نتیجه، هر پایگاه وب، مجموعه داده‌هایی را گرد می‌آورد به همراه داده‌های دیگری دربارهٔ مرورگر، نشانی «آی‌پی» و... به پروندهٔ ردنمایی که با کلید رمز پاسداری می‌شود، می‌فرستد. این پایگاه وب، می‌تواند کلید را به دیگران بفروشد. آنها نیز بدون آگاهی کاربر می‌توانند از آن برای باز کردن پرونده‌های ردنما بهره گیرند. برای نمونه، پایگاه وب «دبل‌کلیک»، شرکتی است که از این روش برای ارائهٔ پیامهای بازرگانی بهره می‌گیرد.□

ادامهٔ مقاله در شمارهٔ آینده