2014

کوکی ها (Cookies)

کوکی ها فایل هایی متنی هستند که وب سرور ها بر روی هارد دیسک کاربران و بازدیدکنندگان خود ایجاد می کنند.

F4RY4R RED

TNX : X3NON , IMN

کوکی ها فایل هایی متنی هستند که وب سرور ها بر روی هارد دیسک کاربران و بازدیدکنندگان خود ایجاد می کنند. این فایل ها عموما برای این منظور ساخته می شوند که وب سرور ها بتوانند اطلاعاتی در مورد کاربران خود ذخیره کنند. این فایل ها که معادل فایل های session در سمت کلاینت هستند اطلاعاتی در قالب زوج های کلید – مقدار (key-value) را در خود نگهداری می کنند.

هنگامی که برای اولین بار وب سایتی توسط کاربری بازدید می شود، وب سرور یک فایل کوکی را بر روی سیستم کاربر ذخیره می کند (در صورت اجازه کاربر). یکی از اصلی ترین اطلاعاتی که در کوکی ایجاد می شود شناسه ای بنام session-id است که به ازای برقراری یک نشست (session) بین وب سرور و کلاینت ایجاد شده و در سمت کلاینت ذخیره می شود. هنگامی که از طریق مرورگر در حال بازدید و استفاده از یک وب سایت هستیم به ازای هر درخواست به سمت سرور این شناسه نیز ارسال می شود تا هویت کلاینت درخواست کننده برای سرور قابل تشخیص باشد. نکته مهم در رابطه با این شناسه اینست که در سمت سرور نیز ذخیره می شود و اعتبار یا عدم اعتبارش توسط سرور تعیین می گردد.

بعنوان نمونه بازدید از یک سایت در کوکی رکوردی با محتوای زیر را ایجاد می کند :

session-id 002-4135256-7625846 amazon.com

در صورتی که کاربر مرور گر خود را ببندد، نشست دیگر معتبر نخواهد بود و در بازدید های بعدی مجددا سرور session-id جدیدی ایجاد می نماید و در کلاینت ذخیره می نماید.

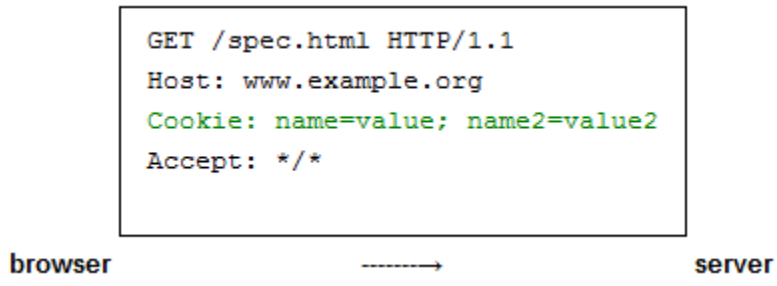
از آنجایی که کوکی ها عمسوما اطلاعاتی مربوط به هویت کاربر را در خود نگهداری می کنند و سرور ها امکان خواندن آنها را دارند، امکان ایجاد یک حفره امنیتی وجود دارد. بهمین دلیل

بمنظور بالابردن امنیت کاربر کوکی ها تنها در پوشه ای خاص از سیستم کاربر (که بستگی به مرورگر دارد) ذخیره می شوند و هر وب سرور تنها می تواند به کوکی مربوط به خود دسترسی داشته باشد. همچنین دسترسی به سایر پوشه ها نیز مسدود می گردد.

مکانسیم عمل کوکی ها :

هنگامی که کاربر سایتی را از طریق URL آن توسط مرورگر خود باز می کند، مرورگر درخواستی را به وب سرور مربوطه بمنظور دریافت صفحه مورد تقاضای کاربر ارسال می کند. بعنوان مثال هنگامی که شما آدرس http://www.amazon.com را در مرورگر خود وارد می کنید، مرورگر به سرور آمازون متصل شده و صفحه اصلی آن را درخواست می کند.

قبل از ارسال در خواست به سرور آمازون، مرورگر در هارد دیسک کلاینت ابتدا بدنبال فایل کوکی مربوط به سایت آمازون می گردد. در صورتی که فایلی قبلا ایجاد شده باشد مرورگر تمامی اطلاعات آن را به همراه درخواست خود به سرور آمازون ارسال می کند. در صورتی که فایل مورد نظر را پیدا نکند، درخواست خود به سرور اطلاع می دهد که هیچ کوکی ای وجود ندارد. این کار از طریق هدر های HTTP صورت می پذیرد.



هنگامی که درخواست توسط سرور دریافت شد، ابتدا چک می کند که آیا اطلاعات کوکی به همراه درخواست ارسال شده است یا خیر؟ اگر هیچ داده ای دریافت نشد سرور متوجه می

شود که بازدید کننده اولین بار است که از سایت بازدید می کند. بنابراین یک نشست جدید ایجاد می کند و شناسه آن را (session-id) هم بر روی ماشین خود (سرور) ذخیره می کند و هم آن را بصورت یک زوج کلید – مقدار در هدر مربوط به پاسخ درخواست کاربر به سمت کلاینت ارسال می کند. هنگامی که مرورگر پاسخ درخواست خود را از سرور دریافت کرد session-id را از هدر HTTP خوانده و در قالب یه فایل کوکی جدید بر روی سیستم کلاینت ذخیره می کند. چنانچه سرور در درخواست کاربر اطلاعات کوکی را بیابد متوجه می شود که کاربر قبلا از سایت بازدید کرده است. بنابراین اطلاعات کوکی را می تواند برای کاربرد های موردنظر خود بکار ببرد.

در پاسخ به هر درخواست بنا به نیاز، وب سرور می تواند اطلاعات جدیدی را به اطلاعات کوکی کاربر اضافه کند و در قالب پاسخ کاربر به سیستم او ارسال نماید تا در کوکی ذخیره شود. در شکل زیر نمونه ای مقداردهی این مقادیر در هدر HTTP را مشاهده می کنید.

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: name=value
Set-Cookie: name2=value2; Expires=Wed, 09 Jun 2021 10:18:14 GMT

(content of page)
```

browser ←-------- server

برای بالابردن امنیت کاربران در مقابل وب سرور های خطرناک، امکانی به کاربران داده شده است که می توانند تعیین نماید تا کوکی ها بر روی سیستم وی ذخیره شوند یا خیر. این کار را کاربران کامپیوترهای خانگی از طریق مرورگر خود می توانند انجام دهند.

ساختار کوکی ها :

فایل کوکی از شش بخش تشکیل شده است که به شرح زیر می باشند :

- نام کوکی
- مقدار کوکی
- تاریخ انقضاء کوکی
- مسیر کوکی
- دومین کوکی
- اینکه کوکی از نوع Secure Cookie می باشد یا خیر؟
- اینکه کوکی از نوع HttpOnly Cookie می باشد یا خیر؟

در بین این اجزاء، موارد اول و دوم حتما باید به صراحت مشخص شوند.

در شکل زیر نمونه ای از مقدار دهی این مقادیر در هدر HTTP نشان داده شده است:

```
Set-Cookie: LSID=DQAAAK…Eaem_vYg; Domain=docs.foo.com; Path=/accounts; Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
Set-Cookie: HSID=AYQEVn….DKrdst; Domain=.foo.com; Path=/; Expires=Wed, 13 Jan 2021 22:23:01 GMT; HttpOnly
Set-Cookie: SSID=Ap4P….GTEq; Domain=.foo.com; Path=/; Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
 ......
```

کاربرد کوکی ها در سرور :

فلسفه وجودی کوکی ها را در یک جمله می توان چنین بیان نمود که کوکی ها استفاده می شوند تا سرور ها بتوانند وضعیت (state) کاربران خود را مشخص نمایند. از آنجایی که ارتباط بین کاربران و وب سرور ها ارتباطی سست است و هر لحظه امکان شکسته شده آن وجود دارد، کوکی ها به سرور این امکان را می دهند تا اخرین وضعیت کاربر را بخاطر بسپارد. بعنوان مثال اگر در درخواست کاربر session-id وجود داشت سرور می فهمد که این کاربر قبلا وب سایت را بازدید کرده است.

یکی از کاربرد های دیگر کوکی می تواند شمارش تعداد بازدیدکنندگان یک سایت باشد. از انجایی که به ازای هر بازدیدکننده ای یک شناسه منحصر به فرد در کوکی ذخیره می شود می توان به کمک آن تعداد بازدید کنندگان یک سایت را محاسبه نمود. بعنوان نمونه دیگری از کاربرد های

کوکی می توان به نگهداری تنظیمات شخصی کاربران (از قبیل زبان سایت، رنگ و قالب سایت و ...) اشاره نمود. این اطلاعات به همراه هر درخواست کاربر ارسال می شود تا سرور پاسخی متناسب با نیاز و علایق کاربر به او ارائه دهد و به این ترتیب تجربه بهتری را به کاربر منتقل نماید.

البته نکته ای که در اینجا اشاره به آن لازم به نظر می رسد اینست که اغلب وب سرور ها بدلیل حفظ امنیت اطلاعات کاربران اطلاعات زیادی را در کوکی ذخیره نمی کنند. در عوض این اطلاعات در بانک اطلاعاتی سرور دخیره می شود و تنها شناسه ای که مشخص کننده این اطلاعات باشد در سمت کلاینت نگهداری می گردد.

نگرانی در مورد کوکی ها :

اگرچه کوکی ها ویروس و یا بد افزار نیستند و قابل اجرا بر روی سیستم کاربر نمی باشند، اما بدلیل انکه اطلاعاتی مهم در مورد هویت کاربر و سوابق اعمال او در یک سایت را در خود دارند نگرانی در مورد حفظ حریم شخصی کاربر وجود دارد. بعنوان مثال برخی از وبسایت ها ممکن است رمز عبور کاربر و یا اطلاعات مربوط به کارت اعتباری او را در کوکی ذخیره کنند. در این صورت از آنجایی که این فایل ها متنی هستند شخص مهاجم این امکان را دارد که آنها را باز نموده و مورد سوء استفاده قرار دهد.

انواع کوکی ها :

بسته به نیاز و کاربرد انواع مختلفی از کوکی ها را می توان ایجاد نمود که در این جا به برخی از انواع آنها اشاره می کنیم.

Session Cookies

این کوکی ها بمنظور نگهداری Session-id مورد استفاده قرار می گیرند. این کوکی ها موقتی هستند و پس از بسته شدن مرورگر و یا پایان اعتبارشان از سیستم کاربر حذف می گردند.

Persistent Cookies

این کوکی ها طول عمر بالایی دارند و عموما برای ذخیره اطلاعات کاربر در یک دوره طولانی مورد استفاده قرار می گیرند. به این نوع از کوکی ها Tracking Cookies نیز گفته می شود

Secure Cookies

این کوکی ها عموما برای ذخیره اطلاعات حیاتی و امنیتی استفاده می شوند. نکته مهم در مورد آنها اینست که همواره از طریق HTTPS باید استفاده شوند تا این اطمینان حاصل شود که محتویات آنها در حین ارسال کد گذاری می گردند.

HttpOnly Cookies

این کوکی ها تنها از طریق درخواست ها HTTP و HTTPS قابل استفاده و ارسال هستند. به این ترتیب این اطمینان را به کاربر می دهند که از طریق سایر API ها از قبیل JavaScript و غیره نمی توان به کوکی ها دسترسی پیدا نمود. البته باید این نکته را ذکر کرد که این محدودیت مصونیتی در مقابل حملات XSS بوجود نمی آورد.

Third-Party Cookies

این دسته از کوکی ها مربوط به دومین هایی غیر از دومین اصلی و مورد درخواست کاربران می باشند. بعنوان مثال در یک صفحه وب ممکن است فریم هایی تبلیغاتی از وب سایت های دیگر قرار داده شود. این وبسایت ها نیز قادر به ذخیره کوکی هایی بر روی ماشین کاربر می باشند. البته در اغلب مرورگر ها امکان بلاک کردن این دسته از کوکی ها بطور جداگانه وجود دارد.

موفق و پیروز باشید

منابع :

www.wikipedia.com
www.howstuffwork.com
www.hamcodi.ir