بسم الله الرحمن الرحیم

آشنایی با حملات

Directory Traversal Attacks
Ver 1.0

حملات Directory Traversal Attack چه هستند؟

شاید کنترل دسترسی به محتویات وب در یک وب سرور ،نکته ی مهمی برای داشتن یک وب سرور امن است.حملات Directory Traversal نوعی HTTP اکسپلویت هستند که به هکرها اجازه ی مشاهده ی دایرکتوری های موجود بر روی سرور و اجرای دستورات در خارج از دایرکتوری root را می دهد.

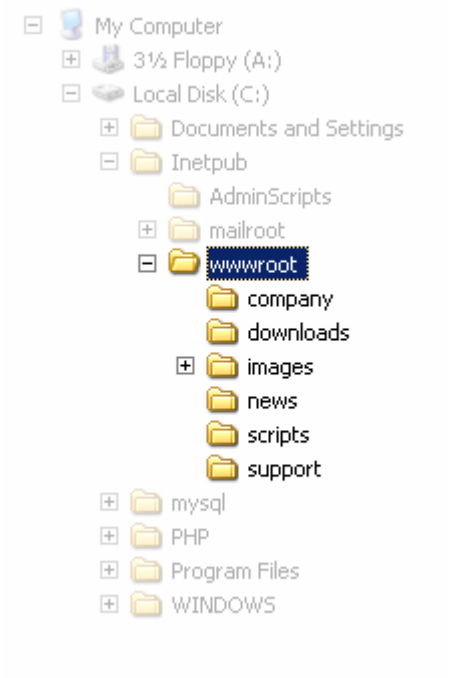
وب سرور ها در مجموع دو نوع mechanism امنیتی دارند:

1) Access Control Lists (ACLs)
2) Root Directory

لیست کنترل دسترسی یا Access Control Lists در تعیین دسترسی کاربران به فایل ها و دایرکتوری ها استفاده می شود.این لیست توسط مدیران سرورها برای تعیین دسترسی کاربران و یا گروه های کاربری برای اجرا و یا تنظیم کردن قابلیت های سیستم ، استفاده می شود.

دایرکتوری root یا root directory دایرکتوری مشخص شده ای در سیستم فایل سرور است که کاربران اجازه ی دسترسی به هیچ یک از محتویات آن را ندارند.

برای مثال : دایرکتوری root در IIS در ویندوز در مسیر C:\Inetpub\wwwroot و C:\Windows قرار دارد اما با این وجود ، کاربران اجازه ی دسترسی به C:\Windows را ندارند اما می توانند به C:\Inetpub\wwwroot\news و تمامی دایرکتوری ها و فایل هایی که زیر مجموعه ی root هستند ، دسترسی داشته باشند.



دایرکتوری root در ویندوز از دسترسی کاربران به فایل های مهم مانند cmd.exe جلوگیری می کند و در سیتسم های یونیکس و لینوکس نیز ، از دسترسی کاربران به فایل passwd که حاوی کلمات عبور کاربران است ، جلوگیری می کند.

آسیب پذیری گفته شده در هردو نرم افزار سرویس دهنده ی وب یا درون کد برنامه های اینترنتی ممکن است وجود داشته باشد.

برای اجرا کردن حملات directory traversal attack تنها چیزهایی که هکر به آن ها نیاز دارد ، یک مرورگر وب و آشنایی با مسیرهای اولیه ی فایل ها و دایرکتوری ها در سرور است.

اگر سایت شما آسیب پذیر باشد ، یک هکر چه کارهایی می تواند انجام دهد؟

با یک سیستم آسیب پذیر به حملات directory traversal ، هکر می تواند از دایرکتوری root بیرون آمده و به سایر دایرکتوری های موجود بر روی سرور برود و به سایر قسمت های سیستم دسترسی داشته باشد.این کار به هکر اجازه ی دیدن فایل های مهم و یا خطرناک تر از آن ، اجرای دستورات قدرتمند سیستمی بر روی سرور را بدهد که باعث مدیریت تمامی منابع موجود بر روی سیستم توسط هکر می شود.

منوط به این که دسترسی کاربران یک وب سایت چگونه تنظیم شده است ، ابتدا هکر خود را به عنوان بازدیدکننده از وب سایت معرفی می کند.بنابراین تمامی دسترسی هایی که در آن وب سایت برای بازدیدکنندگان معمولی در نظر گرفته شده است ، به آن اختصاص می یابد.

نمونه ای از حمله ی Directory Traversal **به وسیله ی کد یک برنامه ی وب:**

در برنامه های وب که در صفحه های داینامیک قرار دارند ، ورودی های معمولا توسط دستورات و یا method های در خواستی GET و POST دریافت می شوند.در اینجا نمونه ای از درخواست GET HTTP در URL نشان داده شده است:

http://test.webarticles.com/show.asp?view=oldarchive.html

با URL بالا ، مرورگر از صفحه ی داینامیک می خواهد که show.asp را از سرور نمایش دهد و همچنین همراه این درخواست ، پارامتر view را با مقدار oldarchive.html ، بفرستد.هنگامی که این درخواست در سرور اجرا شود show.asp همراه با oldarchive.html در سرور جستجو و به مرورگر فرستاده می شوند تا به کاربر نشان داده شوند.هکر می تواند show.asp را به صورت تقلبی در بیاورد و URL متفاوتی را ارسال کند:

http://test.webarticles.com/show.asp?view=
../../../../../Windows/system.ini

این کار باعث می شود تا صفحه ی داینامیک فایل system.ini را از سرور بگیرد و به کاربر نشان دهد.خط /.. باعث می شود تا سیستم به دایرکتوری بالاتر که بیشتر دایرکتوری است که سیستم عامل از آن استفاده می کند ، بر گردد.هکر باید حدس بزند که چند دایرکتوری دیگر باید بالا برود تا به دایرکتوری Windows سیستم برسد.این کار بسیار آسان است زیرا هکر آن قدر این کار را تکرار می کند و از سیستم خطا دریافت می کند که در نهایت به دایرکتوری مورد نظر می رسد.

قسمتی از این آسیب پذیری ها در کد سرور ها و نرم افزارها وجو دارد ، با این حال خود وب سرور نیز می تواند دایرکتوری های درخواست شده را در این حملات باز کند.این مساله در هر دوی آن ها می تواند روی دهد به این شکل که اسکریپتی فایلی که در سرویس دهنده ی وب موجو است را بیرون بیاورد.

این آسیب پذیری در آخرین نسخه ی نرم افزارهای سرویس دهنده ی وب برطرف شده است ، اما با این حال هنوز سرورهایی هستند که از نسخه های قدیمی IIS یا Apache استفاده می کنند و به این گونه حملات آسیب پذیر هستند.هنگامی که شما ازآخرین نسخه ی سرویس دهنده ی وب نیز استفاده می کنید ، هنوز نیز ممکن است شما به این گونه حملات آسیب پذیر باشد زیرا هکرها اسکریپت هایی را برای نشان دادن دایرکتوری های موجود در وب سرور استفاده می کنند که جدید هستند و راه مقابله ای هنوز برای آن ها ارایه نشده است.

برای مثال ، URL زیر درخواستی را به وسیله ی اسکریپتی به وب سرور IIS ارسال می کند که در آن ، ابتدا به دایرکتوری Windows\System32 رفته و سپس دستوری را اجرا می کند:

http://server.com/scripts/..%5c../Windows/System32/
cmd.exe?/c+dir+c:\

این درخواست لیستی از تمامی فایل هایی که در C:\ قرار دارند را به وسیله ی اجرای دستور dir c:\ در cmd.exe یا خط فرمان ، به کاربر ارسال می کند.کد 5c% که در URL درخواستی وجود داشت یک کد خروجی وب سرور است که به جای کاراکترهای معمولی استفاده می شود.در این حالت 5c% به معنی کاراکتر \ است.

نسخه های جدیدتر سرویس دهنده های وب ، این کدها را چک کرده و اگر وجود داشته باشند ، اجازهی اجرای آن ها را نمی دهند.نسخه های قدیمی تر ، این کدها را در دایرکتوری root فیلتر نمی کنند و به هکر اجازه می دهند تا دستوراتی سیستمی را در آن اجرا کند.

چگونه وجود این آسیب پذیری ها را در سایت خود چک کنیم؟

بهترین راه برای چک کردن وجود این آسیب پذیری های ، استفاده از یک اسکنر آسیب پذیری برنامه های وب است.یک اسکنر آسیب پذیری برنامه های وب هر دو برنامه و سرویس دهنده ی شما را چک کرده و سپس گزارشی را به شما ارایه می دهد و شما را از وجود آسیب پذیری بر روی وب سایت خود مطلع می کند و در صورتی پیدا شدن آسیب پذیری راه بر طرف کردن آن را نیز به شما می گوید.علاوه بر آسیب پذیری گفته شده ، یک اسکنر آسیب پذیری برنامه وب به دنبال آسیب پذیری های دیگر مانند:

1) SQL injection
2) Cross site scripting
3) Google hacking

نیز می گردد.

جلوگیری از حملات Directory Traversal Attacks به یک وب سرور:

اول از همه چیز از این که از آخرین نسخه ی سرویس دهنده ی وب استفاده می کنید و تمامی وصله های امنیتی را نصب کرده اید اطمینان حاصل کنید.

کار دیگری که می توانید انجام دهید ، تمامی ورودی هایی که توسط کاربران فرستاده می شوند را چک کنید.تمامی کاراکترهای اضافه و خطرناک را که وارد می شوند ، به جز اطلاعات صحیح ، پاک کنید و یا از ورودی بردارید.

acunetix

Scan group - saved on 14/7/2006, 13:32 , profile : default

Scan Thread 1 (http://testphp.acunetix.com) 214 alerts found

Scan Thread 1 (http://testphp.acunetix.com)

Alerts summary

Threat level

acunetix threat level

Level 3: High

Acunetix threat level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts found

Total alerts found	214
High	131
Medium	8
Low	24
Informational	51

Executive summary

Alert group	Number of alerts in this group
SQL injection	84
Script source code disclosure	1
Directory traversal (Windows)	1
Cross Site Scripting	32
PHP version vulnerable	1
Blind SQL/XPath injection for string inputs (double quotes)	1
Blind SQL/XPath injection for numeric inputs	8
Common files found	6
PHP code injection	1
Blind SQL/XPath injection for string inputs	1

نمونه از Web Application Vulnerability Scanner

Copyright© by Siahacker
2005-2006 All Rights Reserved
Email:Siahacker@gmail.com