بسم الله الرحمن الرحیم

آشنایی با حملات

Authentication Hacking attack

حملات Authentication Hacking attack **چه هستند؟**

حملات Authentication با قاعده ی خاصی از امنیت برنامه های وب بازی می کنند.هنگامی که کاربری با نام کاربری و کلمه ی عبورش هویت خود را مشخص کرده و login می کند ، بر اساس تنظیمات سیستم اختیارات مربوط به او داده می شود.

پروتکل HTTP می تواند شامل انواع مختلفی از پروتکل های هویت شود:

1) Basic : شامل متن های تمیز مانند نام کاربری یا کلمه ی عبور ، Base-64 encode ((نیمه رمز شده))
2) Digest : مانند مورد بالا بدون کلمات عبور
3) Form-based : از فرمت مختلفی برای ورود نام کاربری و کلمات عبور استفاده شده است و در پردازش آن ها از روش های منطقی متفاوتی استفاده شده است.
4) NTLM : پروتکل هویت شرکت مایکروسافت ، که در داخل پروتکل HTTP و با header های درخواست و پاسخگویی ساخته شده است.
5) Negotiate : پروتکل جدیدی از شرکت مایکروسافت که هر نوع از موارد بالا را به صورت داینامیکی در client و server قبول می کند.همچنین این پروتکل Kerberos را به وسیله ی مرورگر اینترنت اکسپلورر برای client ها اضافه می کند.
6) Client-side Certificates : به غیر از موارد بالا ، SSL/TLS گزینه ای برای چک کردن هویت certificate های دیجیتال که به وسیله ی Web client فرستاده می شوند است ، و آن ها را به صورت هویت های مهم در می آورند.
7) Microsoft Passport : سرویس single-sign-in (SSI) به وسیله ی شرکت مایکروسافت اجرا می شود و به وب سایت ها اجازه می دهد تا کاربران مخصوص موجود در اعضای خود را هویت بندی کنند.این مکانیسم از کلید به اشتراک گذاری شده بین شرکت مایکروسافت و سایت شرکت سرویس گیرنده است که cookie های متفاوتی را برای جداسازی کاربران از یک دیگر درست می کند.

این عملگرهای هویتی بر روی پروتکل HTTP (یا SSL/TSL) با گواهی نامه های معتبر ، در ترافیک درخواست و پاسخگویی ، کار می کنند.

این قسمت از حمله یک مشکل امنیتی تکنیکی بر روی سیستم عامل یا نرم افزار سیستم نیست.این حملات منوط به این است که امنیت در سرور چگونه پیاده سازی می شوند و کلمه ی عبور کاربر در سیستم چگونه نگه داری می شود و برای هکر دست یابی به کدام یک آسان تر است.

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

هنگامی که یک هکر به وسیله ی دسترسی به برنامه های وب به عنوان یک کاربر صحیح به سیستم وارد می شود ،به تمامی اختیاراتی را که مدیر به آن کاربر داده است ، دست می یابد.
این به معنی است که اگر یک هکر به عنوان یک کاربر عادی وارد سیستم شود ، او می تواند بعضی از اطلاعات مهم را ببنید.اما اگر هکر به عنوان یک کاربر مدیر وارد سیستم شود ، ممکن است به اطلاعات مهمتری در سیستم دست پیدا کند و برنامه های وب را در اختیار خود بگیرد ((به همراه تنظیماتی که در برنامه های وب است)).

برنامه های مورد نیاز هکر برای حمله به سایت:

بیشتر در اولین کار برای نفوذ ، هکر ابتدا سعی می کند که به صفحات login و با برنامه هایی که نام کاربری و کلمه ی عبور را می خواهند دست ، پیدا کند.در کار بعدی برای نفوذ ، هکر یک نام کاربری و کلمه ی عبور صحیح را وارد می کند که برنامه ی وب ممکن است او را به عنوان یک کاربر با دسترسی بالا قبول کند.
اما این همه ی این کار حمله نیست ، حدس زدن کلمه ی عبور یکی از راه های نفوذ به سیستم است.در این کار هکر به وسیله ی یک برنامه و یا به صورت حدسی کلمه ی عبور را پیدا می کند و به سیستم وارد می شود.
در اینجا نمونه ای از نام کاربری و کلمه ی عبور استفاده شده در حمله به صورت حدسی توسط هکر نشان داده شده است:

Username Guesses	Password Guesse
[NULL]	[NULL]
root, administrator, admin	[NULL] , root, administrator, admin, password, [company_name]
operator, webmaster, backup	[NULL] , operator, webmaster, backup
guest, demo, test, trial	[NULL] , guest, demo, test, trial
member, private	member, private
[company_name]	[NULL] ,[company_name], password
[known_username]	[NULL] ,[known_username]

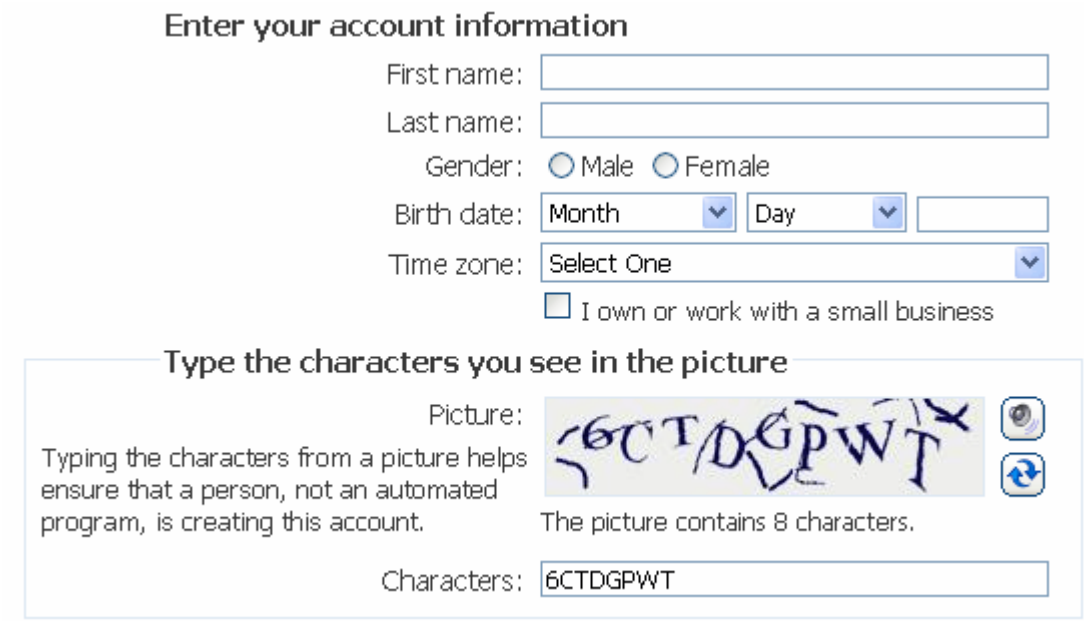
اگر حدس زدن کلمه ی عبور برای هکر نتیجه ای نداشت ، کار بعدی استفاده از یک نرم افزار حدس زننده ی کلمه ی عبور است.
این برای حمله به سیستم از یک لیست از پیش آماده شده از نام کاربری و رمز عبور استفاده می کنند.در این حمله ، برنامه از لیست خود برای حدس زدن کلمه ی عبور استفاده می کند و با تلفیقی از مجموعه ی لیست خود سعی در پیدا کردن کلمه ی عبور دارد.در برخی از حملات دیگر ، این برنامه ها سعی می کنند با قرار دادن حروف و نشانه های مخصوص در کنار هم و فرستادن آن ها به برنامه ی وب ، کلمه ی عبور را پیدا کنند.

چگونه صفحات مختلف مربوط به هویت کاربران را چک کنیم؟

برای چک کردن صفحات خود از وجود این آسیب پذیری ، از یک برنامه ی چک کننده ی هویت است.یک اسکنر آسیب پذیری برنامه های وب شامل این برنامه است.پس از چک کردن صفحات سایت شما گزارشی از آسیب پذیری های یافت شده تهیه می شود و راه برطرف نمودن آن ها را نیز به شما می گوید.

جلوگیری از حملات Authentication Hacking attacks **به سایت ها:**

برای چک کردن این که آیا یک حمله به سایت درست انجام شده است یا نه استفاده از ابزارهای خودکار که کد خطاها و صفحات اطلاعاتی را از سرور بر می گردانند می تواند مفید باشد.
کار مهمی که می تواند از حملات ابزارهای حدس زننده ی کلمه ی عبور ، که از یک لیست برای این کار استفاده می کنند ، جلوگیری کند این است که در صفحاتی که هویت کاربران مشخص می شود از تلفیقی از حروف و اعداد مختلف استفاده شود که در این صورت کاربر باید به درستی این ها را وارد کند.بهترین راه برای نمایش این موارد استفاده از فرمت های گرافیکی GIF ، JPG ، PNG است که در هر زمان نمایش این تصاویر گرافیکی از فونت ها و رنگ های مختلفی استفاده شود.همچنین این کار حملات برنامه های حدس زننده ی کلمه ی عبور به وسیله ی یک لیست را بسیار کمتر می کند.نمونه ای از این تصاویر را در زیر می بینید:



برای این که بدانید این آسیب پذیری در سایت وجود دارد ، بهترین کار استفاده از یک اسکنر آسیب پذیری برنامه های وب است که می تواند به شما کمک کند.

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 ای از یک Web Vulnerability Scanner

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