بسم الله الرحمن الرحیم

آشنایی با حملات

Google hacking
Ver 1.0

حملات Google hacking چیست؟

این گونه حملات با استفاده از نتایج و روش های جستجو در گوگل طراحی می شوند.هکرها با فرستادن مسیرها و یا نام فایل های مهم به گوگل و Search کردن آن ها سعی دارند تا به آدرس های مهم بر روی سرور های مختلف دسترسی پیدا کنند.پایگاه داده ی Google Hacking یا GHDB شامل اطلاعات مهمی در مورد این آدرس ها و داده های مهم است.
بنابراین گوگل بعضی از جستجوها را که می توانند خطرناک باشند را مسدود می کند.

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

پایگاه داده ای Google Hacking می تواند موارد زیر را شامل شود:

۱) آسیب پذیری ها و مشکلات امنیتی سرور
۲) پیغام های خطا که شامل اطلاعات بسیار مفیدی می شوند
۳) فایل هایی که شامل کلمه ی عبور کاربران می شوند
۴) دایرکتوری های مهم
۵) صفحاتی که شامل اطلاعات LOGIN می شوند
۶) صفحاتی که شامل logifle ها و اطلاعاتی در مورد آسیب پذیری های موجود در سرور می شوند

چگونه Google hacking را چک نماییم؟

بهترین راه استفاده از یک آسیب پذیری برنامه های وب است.یک اسکنر آسیب پذیری برنامه های وب محتویات سایت شما را چک کرده و به دنبال صفحاتی که آسیب پذیری Google hacking در آن ها وجود دارد می گردد.البته باید اسکنر شما قادر به فرستادن مقادیر Google hacking باشد.

چگونه از حملات Google hacking جلوگیری کنیم؟

برای جلوگیری از این گونه حملات باید تمام موارد خطرناک را از وب سایت خود حذف کنید.

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