

با استفاده از دستور SQL

نفوذ به فرومها آسان است

خود را فراموش کنید و به هر دلیلی توانید به خود خود Login Account کنید. حتی با استفاده از Forget Password هم به نتیجه نرسید. در این هنگام استفاده از این دستور بهترین راه برای گرفتن کلمه عبور جدید است. همچنین اگر از روش‌های معمول، کلمه عبور کنترل پل یک سایت را به دست آورده‌اید و می‌خواهید کلمه عبور Account این فروم را عوض کنید نیز می‌توانید از این دستور استفاده کنید. برای این کار مطابق شکل زیر به کنترل پل آن سایت Login کنید.

سپس از قسمت Database گزینه MySQL را انتخاب کنید و مانند شکل زیر به صفحه این برنامه بروید.

در مرحله بعد و باز شدن صفحه به Database گزینه SQL بروید و در قسمت خالی مستطیل شکل دستور زیر را بنویسید:

```
UPDATE user SET password = MD5
('mypassword') WHERE userid = #;
```

که البته به جای mypassword کلمه عبوری را که می‌خواهید آن کاربر به آن تغییر پیدا کند، می‌نویسید و به جای هم که از userid که شماره است که به هر کاربر که در فروم ثبت نام کنند، داده می‌شود می‌توانید با رفتن به Profile ادمین یک فروم و کمی رفتگو در آن user id گستجو در آن شخص مورد نظر را پیدا کنید. برای درک بیشتر این موضوع به عکس زیر توجه کنید.

برای مثال دستور زیر را به SQL دهیم:

```
UPDATE user SET password = MD5
('hiyane') WHERE userid = 116;
```

کلمه Go و با زدن دکمه کلیک عبور کاربری که از ۱۱۶ userid است، به کلمه عبور دلخواه ما که در این مثال ashiyane است، عرض می‌شود. همچنین همانطور که مشاهده کردید، برای هک کردن هم می‌شود از این دستور جالب استفاده کرد. برای آشنایی بیشتر با تالارهای گفتمان می‌توانید به سایت www.ashiyane.org مراجعه کنید.

بهروز کمالیان

عبور گشته شده Account ادمین شما در یک فروم کمک می‌کند. بیشتر فرم‌های کامپیوتری و برنامه‌هایی که با زبان برنامه نویسی PHP نوشته می‌شوند، احتیاج به بانک اطلاعاتی دارند که تمام اطلاعات کاربران و تمام Postها و بحث‌هایی که در آن داده می‌شود را ذخیره کنند. برای این بانک اطلاعاتی کلمه عبوری از سوی مدیر آن فروم داده می‌شود که تنها آن شخص باید از این کلمه عبور آگاه باشد. برای فرم‌های PHP مثل Board - PHPNuke - phpbb - Invision Power

MySQL از دیتابیس

استفاده می‌شود که در فرم عضو

روی سرورهای لینوکس نصب می‌شود. برای مدیریت پایگاه داده‌ها، بیشتر کنترل پل مدیریت وب سایت‌ها مثل Cpanel و Plesk از برنامه‌ای به نام

phpmyadmin استفاده می‌کنند. گاهی اوقات ممکن

کاربری با این سطح دسترسی در فروم وجود نداشته

باشد و شما کلمه عبور

تایله حال برایتان پیش آمد است که به کنترل پل یک سایت و آن نفوذ کنید ولی برای نفوذ به فروم (Forum) آن سایت به مشکل برخورد نماید؟ همانطور که می‌دانید، فرم‌ها تالار گفتمان‌هایی هستند که به کاربران سایت امکان عضویت و بحث و گفتگو را در محیطی ساده و مشخص فراهم می‌کنند. تفاوت فرم‌ها با محیط‌هایی چت در این است که در تالار گفتمان‌ها تمام بحث‌هایی که می‌شود ثبت می‌شود و در ساعت‌ها و روزهای آینده به آن بحث‌ها یا سوال‌ها توسعه اشخاص دیگری که در فروم عضو هستند، پاسخ داده خواهد شد. در صورتی که در محیط چت تنها به صورت زنده می‌توان بحث و گفتگو کرد. در این مقاله قصد داریم دستوری را به شما معرفی کنیم که از طریق آن می‌توانید کلمه عبور ادمین یک فروم کامپیوتری مثل VBulletin را عرض کنید.

این دستور هم به شما برای عرض کردن کلمه

عور یک User با هر سطح

دسترسی و هم برای

عرض کردن کلمه

حمله به نرم افزارهای مولتی مدیا

روی کامپیوتر هر یک از مایک یا چند نرم افزار مولتی مدیا برای پخش موزیک و فیلم وجود دارد. به همین دلیل هکرها توجه خاصی به بعضی از این نرم افزارهای windows media player معروف از قبیل Real player و winamp حفظه‌های امنیتی موجود در آنها توانسته اند کنترل بسیاری از سیستم‌های رایانه ای را به دست آورند و از اطلاعات موجود در آنها استفاده کنند.

به عنوان مثال، به تازگی کارشناسان امنیتی به کاربران توصیه کردند به لیل وجود حفره امنیتی خطرناکی، نرم افزار RealPlayer خود را به نگارش‌های جدید تر ارتقا دهند.

به گفته کارشناسان یک شرکت امنیتی، حفره نسخه ۱۰/۵ Real Player و نگارش ۱x هلیکس پلیر به هکرها امکان کنترل کامل سیستم رایانه‌ی کاربر را می‌دهد. نگارش‌های جدید هلیکس پلیر که نسخه متن باز Real Player است، در وب سایت طراح خود موجود است.

هچنین به دنبال بروز مشکلات امنیتی در نرم افزار محبوب Winamp، کارشناسان معتقدند که این نرم افزار به زودی بخش عظیمی از مخاطبان خود را از دست خواهد داد.

گزارش‌های رسانیده نشان می‌دهد برخی هکرها موفق شده‌اند با استفاده از نقص‌هایی که در نرم افزار Winamp وجود دارد، وارد رایانه شخصی کاربران شوند و به اطلاعات آنها آسیب برسانند.

شرکت‌های امنیتی هشدار داده‌اند، با توجه به اینکه نرم افزار Winamp تسبیت به zero day بسیار آسیب پذیر است، استفاده از آن توسعه کاربران می‌تواند مشکلات زیادی را به وجود آورد.

در حالی که هنوز هیچ وصله‌ای برای رفع این مشکل عرضه نشده است، کارشناسان یک شرکت دانمارکی اعلام کردند که حفره امنیتی نسخه ۵/۱۲ Winamp بسیار مشکل‌ساز و خطرناک است.

با این حفره هکرها می‌توانند کنترل کامل رایانه شخصی کاربران را در دست گیرند و ویروس‌های مخرب را روی آنها بارگذاری کنند.

زمانی که Winamp در حال پخش موسیقی‌های بارگذاری شده از اینترنت است، هکرها به آسانی می‌توانند تمام فعالیت‌های خرابکارانه خود را انجام دهند.

علیرضا صالحی

Q&A

پرسش و پاسخ

Clickhelp@jamejamonline.ir

محمد نوری از لاهیجان: آیا سرور gmail سرویس pop3 دارد؟

بله، gmail ۳POP دارد و می‌توانید با فعل کردن آن ای‌میل‌های خود را از طریق Outlook دریافت

برای outlook gmail را هم بینید.

می‌شود و در صورتی که گزینه دیگر را انتخاب کنید

فقط ای‌میل‌هایی که از این تاریخ به بعد برای شما

ارسال شده است را می‌توانید در Outlook Forward and POP کلیک کنید. در قسمت

POP Download یکی از دو گزینه‌ای را که با POP

شروع می‌شود، انتخاب کنید.

البته بهتر است فیل از این کار روی Instructions

Configuration هم کلیک کنید تا نحوه تنظیم