

重置链接导致任意用户密码重置

问题站点: <http://www.xxx.com/>

第一种: 邮箱 md5 加密

先用测试账号, 登陆的地方点击忘记密码。会叫你填写邮箱, 点击发送, 然后注意看上面的 URL 后面的参数！！！

邮箱接收到的:

<http://www.xxx.com/password/reset/64396cee7eaa02381352e642f6d9421a>

可以发现, reset 参数后面跟着的就是邮箱的 md5 值

现在来重置管理员的账号, 邮箱输入 `admin@xx.com`, 点击忘记密码

然后构造链接:

<http://www.xxx.com/password/reset/579f6c57312090c41b8560b404eb79f1>



The screenshot shows a web-based password cracking interface. At the top, there is a search bar with the text '密文: admin@xx.com' and a dropdown menu set to '自动' (Automatic). Below the search bar are two buttons: '查询' (Search) in orange and '加密' (Encrypt) in white. The main area is titled '查询结果:' (Search Results). It displays two lines of text: 'md5(admin@xx.com,32) = 579f6c57312090c41b8560b404eb79f1' and 'md5(admin@xx.com,16) = 312090c41b8560b4'. The first line is highlighted with a red box.

点击上面链接即可重置管理员密码

第二种: 时间戳 md5 加密

重置密码, 会得到一个这样的链接

https://www.xxxxcom/user/reset_100038_e91e556f1685c4a8a5e060b64d38a5e2.htm

100038 为 ID, e91e556f1685c4a8a5e060b64d38a5e2 为时间戳的 md5!!!



The screenshot shows a web-based password cracking interface. At the top, there is a search bar with the text 'e91e556f1685c4a8a5e060b64d38a5e2' and a green '解密' (Decrypt) button. Below the search bar is a green bar with the text 'md5'. The main area displays the text '1384924658'.

所以, 这样重置别人的密码

先去找回他的密码, 记下服务器返回页面的时间

测试了一次, 时间为 Wed, 20 Nov 2013 05:23:56 GMT

加 8, 变成我们的时间, 然后转换成时间戳

得到 1384925036

进行 md5

`6539115614e15fe72da242dea5d0560c`

成功进入重置页面！

https://www.xxx.com/user/reset_100038_6539115614e15fe72da242dea5d0560c.htm

Tips: 有时候也会是 base64 加密或者其他类型的有规律的加密方式，都可以进行构造重置链接