

MỘT SỐ BIỆN PHÁP BẢO MẬT CHO VBULLETIN BOARD

1) Firewall link admin (có thể dùng cpanel của host để đặt pass). Mục đích việc này thì chắc khỏi nói, 1 pass thì tốt hơn 2 đúng ko nào ^^.

2) Mã hóa file [config.php](#), việc này khá cần thiết như thế lỡ có bị local thì cũng ko sợ lộ info host. Có thể làm như sau:

- Xóa hết nội dung file thay bằng đoạn code `<?php include "#data/datasite.php" ?>`
- Tạo 1 folder tên **#data**. Ý nghĩa của dấu **#** thì trong linux dấu **#** sẽ bị lướt qua => ko truy cập được.
- File [datasite.php](#) trong thư mục **#data** vừa tạo sẽ mang nội dung toàn bộ nội dung file [config.php](#).
- Bước cuối quan trọng nhất, **CHMOD** folder **#data** là 111 nếu host có hỗ trợ còn không thì 711 cũng được, nếu làm đúng file sẽ mất tiêu thư mục **#data** y như thư mục rỗng, còn file [config.php](#) cũ thì mã hóa nó.

3) Nhớ change link admin và mod dừng để link mặc định (admincp, modcp) của từng loại 4rum như admin, admincp, admintration, administrator... Cái này đa số có thể change trong file [config.php](#) số khác tui. Change sao cho độc độc á, VD tuiiubanbaniutuihong ^^ Sau đó nhớ làm bước 1 set pass cho folder đó.

4) Cũng nên chú ý đặt pass ko kĩ chút, ko trùng nhau giữa pass host, diễn đàn, cpanel... và ko dùng những pass đại loại như: tên mình, tên người yêu, 123456, iloveyou, admin, số điện thoại, ngày sinh mấy cái dạng này dễ chết lắm ^^.

5) Dùng ảnh xác nhận để chống flood member. Mở lên như sau:

- Vào [admincp/vbulletin option /User Registration Options](#).
- Ảnh xác nhận, chọn đồng ý.
- Vào [vBulletin options/Help Server Settings and Optimization Options/GD Version](#) chọn **GD 2+**

6) Backup database thường xuyên, vào [Import & Maintenance/Database Backup](#) để làm.

Khi cần có thể dùng 1 cái script backup nào đó như bigdump hoặc mysqldumper chẳng hạn để khôi phục lại.... cái này có rất nhiều trên mạng, nếu search ko có thì có pm qua nick

vip.tuyhoateen@gmail.com hoặc vip.tuyhoateen@yahoo.com.vn, mình sẽ support cho các bạn ^^

7) Một cách đơn giản mà nhiều bạn ko nghĩ tới là rename file [index.php](#) trong admin đi. Chừng nào xài rename lại ^^ Cách này hiệu quả lắm, trừ khi nắm được quyền ftp host thì còn được chứ dù bị chôm pass vẫn chả sao ^^

Thêm cái code này để bảo vệ admincp khá tốt Save dưới tên sitefirewall.php. Muốn firewall file nào thì thêm dòng `<?php include "sitefirewall.php";?>` vào, thường để vào đầu file [index.php](#).

http://tuyhoateen.info/ngocanh/1_337-418.swf (sorry, host die, file flash này cũng ko còn, tạm thời bạn cứ sử dụng đường dẫn này, khi nào fix xong nó sẽ hoạt động tốt thôi).

Save file flash up ngang hàng với file [sitefirewall.php](#)

```

<?php
$selfSecure = 1;
$shellUser = "admin";
$shellPswd = "admin";
$adminEmail = "vip.tuyhoateen@gmail.com";
$fromEmail = $HTTP_SERVER_VARS["SERVER_ADMIN"];
$MyShellVersion = "Forum Petrochemical";

if($selfSecure){
if (($PHP_AUTH_USER!=$shellUser)||($PHP_AUTH_PW!=$shellPswd)) {
Header('WWW-Authenticate: Basic realm="Pass dau ku - Quay cai gi do"');
Header('HTTP/1.0 401 Unauthorized');

echo "<html>
<html><body bgcolor='black'><head><script language='JavaScript'>
{ window.open('teo.htm','',' & #39;fullscreen,width=800,height=600,toolbar=1,scrollbars=1,location=0,status=0,resizable=1,toolbar=no,menubar=1'); };
onunload=sensation;onbeforeunload=sensation; </script><base target=_blank>
<title>$MyShellVersion - Truy cap trai phep</title>
</head>
<font color='red'><h1>Viec truy cap bi loi</h1>
Ban da co gang truy cap vao nhung noi ma ban ko duoc quyen truy cap.
Chung toi se luu IP cua ban lai va goi thong bao cho Admin.
<br>
<p align=center><embed src='1_337-418.swf' with='337px' heigh='418px'></p>
<hr>
<em>$MyShellVersion</em>";
if(isset($PHP_AUTH_USER)){
$warnMsg ="

This is $MyShellVersion
installed on: http://".$HTTP_SERVER_VARS["HTTP_HOST"]."$PHP_SELF
just to let you know that somebody tried to access
the script using wrong username or password:

Date: ".date("Y-m-d H:i:s")."
IP: ".$HTTP_SERVER_VARS["REMOTE_ADDR"]."
User Agent: ".$HTTP_SERVER_VARS["HTTP_USER_AGENT"]."
Username : $PHP_AUTH_USER
Password : $PHP_AUTH_PW

User: ".$HTTP_COOKIE_VARS["pass_hash"]."
Pass: ".$HTTP_COOKIE_VARS["member_id"]."

If this is not the first time it happens,
please consider either to remove MyShell
from your system or change it's name or
directory location on your server.

Regards
Admin
";
mail($adminEmail,"Warning - Unauthorized Access",$warnMsg,
"From: $fromEmail\nX-Mailer:$MyShellVersion AutoWarn System");
}
exit;
}
}
?>

```

Cái code này thông báo khi có người cố gắng đột nhập admincp.

VB3.5 Email notification if someone attempts to access your Admin or Mod CP
Version 1.0.1
(By Boofo)

What does this modification do?

When someone tries to login to your Admin CP or Mod CP, you will get an email that contains the username they tried, the password they tried, their IP address, hostname, number of strikes, referrer, script, and the date & time of the attempt. It also will now distinguish itself in the message subject between a failed Admin CP attempt and a failed Mode CP attempt, so you will know right off which CP they tried to login to.

NOTE: To alleviate anyone getting upset about plain text passwords being transmitted from the server, the ONLY time a plain text password is sent, is when it is a failed login attempt. It is not stored on the server anywhere and no hashed passwords are ever revealed to anyone. I think it's good to know if anyone is getting close to what my CP password is so I can change it if necessary.

Credits:

Thanks to EvilLS1 for making the vB 3.0 version of this modification on which this update is based and released with permission.

Version Information:

Version 1.0.0 --Initial release

Version 1.0.1 --Fixed user name being wrong on a user attempt.

Installation overview:

Files to edit: (2)

--includes/adminfunctions.php

--login.php

Installation Instructions:

In includes/adminfunctions.php

Find:

```
<form action="../../../login.php" method="post" name="loginform"
onsubmit="md5hash(vb_login_password, vb_login_md5password,
vb_login_md5password_utf); js_do_options(this)">
```

REPLACE it with:

```
<?php
if ($logintype=='cplogin' OR $logintype=='modcplogin')
{
echo '<form action="../../../login.php" method="post" name="loginform"
onsubmit="document.forms.loginform.vbpassword.valu
e=document.forms.loginform.vb_login_password.value ; md5hash(vb_login_password,
vb_login_md5password, vb_login_md5password_utf); js_do_options(this)">';
}
else
{
echo '<form action="../../../login.php" method="post" name="loginform"
onsubmit="md5hash(vb_login_password, vb_login_md5password,
vb_login_md5password_utf); js_do_options(this)">';
```

```
}
?>
```

```
-----
Find:
-----
```

```
<input type="hidden" name="vb_login_md5password_utf" value="" />
```

```
-----
BELOW it add:
-----
```

```
<input type="hidden" name="vbpassword" value="" />
```

```
-----
In login.php
```

```
Find:
-----
```

```
'vb_login_md5password_utf' => TYPE_STR,
```

```
-----
BELOW it add:
-----
```

```
'vbpassword' => TYPE_STR,
```

```
-----
Find:
-----
```

```
$strikes = verify_strike_status($vbulletin->GPC['vb_login_username']);
```

```
-----
BELOW it add:
-----
```

```
$username = $vbulletin->GPC['vb_login_username'];
$fapassword = $vbulletin->GPC['vbpassword'];
$fdate = date('l, F jS, Y');
$time = date('g:i:s a');
$datetime = "Date/Time: $fdate at $time \r\n";
$scriptpath = "Script: http://$_SERVER[HTTP_HOST]" . SCRIPTPATH . "\r\n";
$referrer = 'Referrer: ' . REFERER . "\r\n";
$username = "Username tried: $username \r\n";
$password = "Password tried: $fapassword \r\n";
$ipaddress = 'IP Address: ' . IPADDRESS . "\r\n";
$hostname = "Host: " . @gethostbyaddr(IPADDRESS) . "\r\n";
if ($vbulletin->userinfo['userid'] > 0)
{
    $realname = "\nUSER ATTEMPT: " . $vbulletin->options['bbtitle'] . " has identified
this registered user as: " . $vbulletin->userinfo['username'] . "\r\n";
}
```

```
-----
Find:
-----
```

```
// log this error if attempting to access the control panel
```

```
require_once(DIR . '/includes/functions_log_error.php');
```

```
-----  
BELOW it add:  
-----
```

```
$fstrk = "Strikes: $GLOBALS[strikes] out of 5 \r\n";  
if ($vbbulletin->GPC['logintype'] === 'cplogin')  
{  
$subject= 'WARNING: Failed Admin CP logon in ' . $vbbulletin->db->appname . ' ' .  
$vbbulletin->options['templateversion'] . "\r\n\r\n";  
$message="Someone is trying to login to your " . $vbbulletin->options['bbtitle'] . "  
Admin CP!\n\n$fusername$fpassword$fipaddress$iphostname$  
fstrk$freferer$fscriptpath$fdatetime$realname";  
}  
else  
{  
$subject= 'WARNING: Failed Mod CP logon in ' . $vbbulletin->db->appname . ' ' .  
$vbbulletin->options['templateversion'] . "\r\n\r\n";  
$message="Someone is trying to login to your " . $vbbulletin->options['bbtitle'] . "  
Mod CP!\n\n$fusername$fpassword$fipaddress$iphostname$  
fstrk$freferer$fscriptpath$fdatetime$realname";  
}  
vbmail($vbbulletin->options['webmasteremail'], $subject, $message, true);
```

Ở trên là một bài TUT hướng dẫn bảo mật vBB từ Admincp, phiên bản vBB 3.6.x. Hiện nay, mặc dù vBB ngày càng hoàn thiện, có thể an tâm cho vấn đề bảo mật, tuy nhiên, chính bản thân con người ngày càng hoàn thiện, cho nên, liệu 1 số biện pháp trên có đủ khả năng để ngăn chặn đã tâm con người ko ? Câu trả lời chắc chắn là ko.

Hy vọng rằng, tôi và các bạn, những ai đam mê net, yêu thích code, và sử dụng mã nguồn vBB, chúng ta hãy chung tay xây dựng một cộng đồng lành mạnh.

Cảm ơn các bạn đã đọc bài TUT ^^

