

The screenshot shows a web browser window with the URL `challenge01.root-me.org/web-serveur/ch17/index.php.bak`. The page features the Root Me logo, which includes a skull with a brain inside. Below the logo, the text "Root Me" is displayed. A large heading "Authentication v 0.05" is centered on the page. Below the heading is a text input field labeled "Password".

Sau khi tìm hiểu về paper thì ta cần tìm xem file backup ở đâu. Em tìm được nó bằng file index.php.bak

```
if (( isset ($password) && $password!="" && auth($password,$hidden_password)==1 ) || (is_array($_SESSION) && $_SESSION["logged"]==1 )){  
    $aff=display("well done, you can validate with the password : $hidden_password");  
} else {  
    $aff=display("try again");  
}  
  
echo $aff;
```

Kiểm tra source code thì ta thấy có thể điều chỉnh password và hidden\_password để bypass được server.

The screenshot shows a web browser window with the URL `challenge01.root-me.org/web-serveur/ch17/?password=1&hidden_password=1`. The page features the Root Me logo and the heading "Authentication v 0.05". Below the heading is a text input field labeled "Password" containing the value "1". At the bottom of the page, there is a button labeled "connect". A success message "well done, you can validate with the password : 1" is displayed in a green box.

← → ⌛ Not secure | challenge01.root-me.org/web-serveur/ch17/



# Root Me

## Authentication v 0.05

Password

connect

**well done, you can validate with the password : NoTQYipcRKkgrqG**

Sau khi về lại trang đầu tiên. Password ngay từ đầu sẽ hiện ra như hình trên. Đây cũng chính là flag của server.