
Subject: Re: Reboot VPS

Posted by [kir](#) on Mon, 10 Apr 2006 21:25:38 GMT

[View Forum Message](#) <> [Reply to Message](#)

Actually you can use shell (or any other language, for that matter) to program simple CGIs. Or, yep, use php.

I can not teach you the basics of PHP, but I can tell you you are entering the high risk zone so, if implemented improperly (insecurely) your solution could do more harm than good.

So, here are a few ideas of how to do it more securely:

(1) do NOT run web server on a host system, use some dedicated VE for it.

(2) in the host system, create some user, say ovzss. Install sudo package if it's not there, and edit /etc/sudoers to allow this user execute vzctl start and vzctl stop commands as root without entering a password. The appropriate line in /etc/sudoers should look like this:
ovzss ALL=(ALL) NOPASSWD:/usr/sbin/vzctl start,/usr/sbin/vzctl stop

(3) in the VE you created for running a web server, create SSH keys for apache user (or another user from which account your httpd runs), and put ssh2 public key to host system as ~ovzss/.ssh/authorized_keys2, so apache user can login into host system via ssh without entering the password

(4) in the CGI you wrote, you should do something like
system("ssh ovzss@host.ip.add.ress sudo /usr/sbin/vzctl start \$VEID");

(5) in the CGI you wrote, CHECK that \$VEID passed from the web user is really a VEID, i.e. it should contain positive non-zero number not exceeding a few digits and only that.

(6) Limit access to the CGI script itself, using Apache Allow/Deny directives.

Surely this can be improved in a few ways, but I hope that as-is it creates a sensible minimum security.
