Responsible Disclosure

The good, the bad, and the (almost) funny

Who am I?

» Frank Breedijk

- Security Officer at Schuberg Philis
- Author of Seccubus
- Blogger for CupFigther.net

Email: fbreedijk@schubergphilis.com
Twitter: @Seccubus
Blog: http://cupfighter.net
Project: http://www.seccubus.com
Company: http://www.schubergphilis.com
(Yes, we're hiring…)

Responsible disclosure

» This talk isn't about good or bad
» This talk is about my experiences running a responsible disclosure

» If you want to debate, buy me a beer tonight

DISCLAIMER

» Do not attempt to run a responsible disclosure program if you do not have your security in order…

» Really, don't…

» I'm not a lawyer ™

The good

» Responsible disclosure works

» http://www.schubergphilis.com/newsroom/library/hall-of-fame/

The bad

» Responsible disclosure works

» http://www.schubergphilis.com/newsroom/library/hall-of-fame/

» WTF? I'm running a t-shirt shop now

The (almost) funny…

When reporting a vulnerability to a major photo site….

Subject: Re: FW: Vulnerability

Please type your reply at the top of the email...

Kevin Wilson

SEP 10, 2013 | 05:24PM PDT

Hi [redacted],

IT looks like you are trying to add in JavaScript for the name of your gallery which isn't possible. You would need to add in letters and numbers only for the name.

Kevin Wilson
[redacted] Support Hero

The (almost) funny…

» When trying to report to a major Telco

» Q: Do you have a PGP key?

» No, could you:

1. Make the file available to me via SFTP (text me the credentials please)
2. Make sure the file is 7zip with password (text me the password too)
3. Please text to 555-5555

The (almost) funny…

» Some ‘researchers’ found our dual factor secured SSL vpn

Then upppppppps :

https://www.schubergphilis.com/CookieAuth.dll?GetLogon?curl=Z2Fwp-adminZ2F&reason=0&formdir=14 (ISA Login Page)

https://www.schubergphilis.com/CookieAuth.dll?GetLogon?curl=Z2Fwp-adminZ2F&reason=0&formdir=13 (Domain Credentials)

I stop here , investigating more... These should normally be whitelisted, this could likely to lead a RDP access bypass. :) Furthermore, I believe you need a complete internal/external security assessment! :)

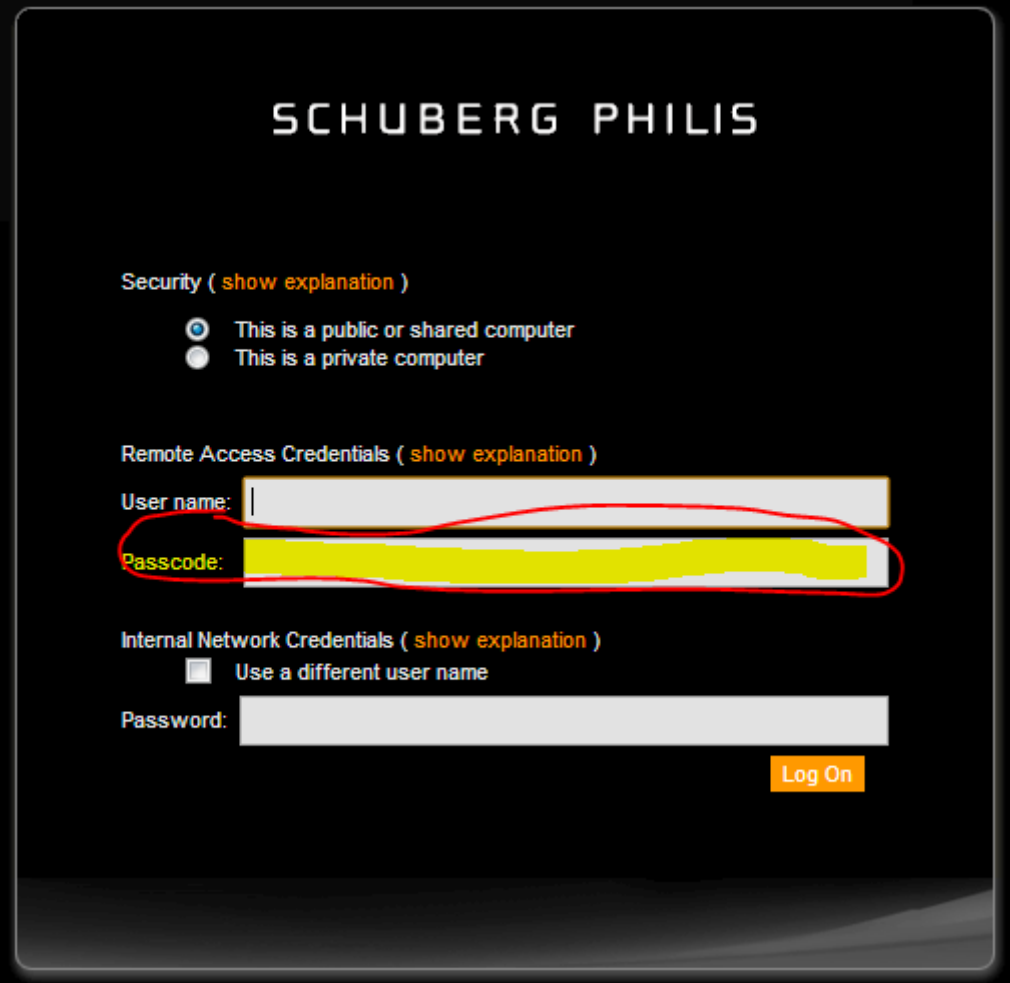
Here is PoC : https://www.schubergphilis.com/admin
it would be redirect to : https://www.schubergphilis.com/CookieAuth.dll?GetLogon?curl=Z2Fwp-adminZ2F&reason=0&formdir=11

Attached Screen Shot also !

Impact : If any attacker suggest username and password or found it , then they easily enter to your site , with admin panel ....They can create users on a given website. Users with the 'admin' permission can edit the website settings . Kindly , Fix it ASAP !

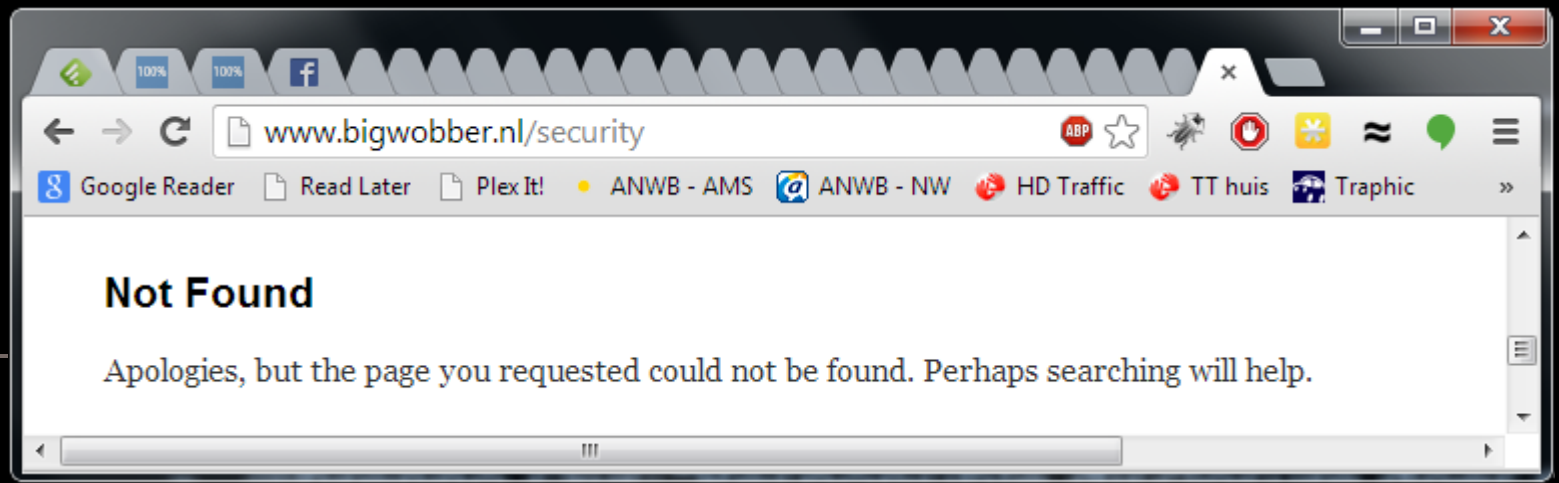
The (almost) funny

» Good luck brute forcing 2FA….



Dear @brenno

- @brenno says: “Responsible disclosure does not absolve you from legal prosecution”
- Dear @brenno, hacking is illegal, I cannot hide you from the law
- @brenno says: “It is bad that companies dictate what a hacker can and cannot do”
- Dear @brenno, I’m o.k. for you to check the locks on my house, I’m not o.k. for you to check if you can set it on fire
- Ps. @brenno



Lessons learned…

» Make it clear what researcher can expect from you
» Make it clear what you expect from the researcher

» It is not the size of the reward that counts…

» Shipping booze around the globe is not a good idea™

» If you want to do it right, you have to work on it™

» You will encounter the clueless, the greedy, the rude
» You will encounter willing and able people too. They make it worth it.