

[SubWeb] NEW http proxy/reverse proxy

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-08/0058.html>

From: Stephane Aubert (Stephane.Aubert@hsc-labs.com)

Date: 08/13/01

Date: Mon, 13 Aug 2001 12:37:02 +0200
From: Stephane Aubert <Stephane.Aubert@hsc-labs.com>
To: pen-test@securityfocus.com
Subject: [SubWeb] NEW http proxy/reverse proxy
Message-ID: <20010813123702.A9769@safe.hsc.fr>

SubWeb v1.0

Stephane Aubert <Stephane.Aubert@hsc-labs.com>
kotao <kotao@kotao.org>
HSC security research labs
Hervé Schauer Consultants

Download: <http://www.hsc-labs.com/tools/subweb/>

SubWeb is a proxy (and also a reverse proxy). It allows to work on HTTP flows in the line of HTTPush, RFProxy or Achilles.

It becomes possible with SubWeb to handle and visualize on the fly the HTTP requests, the headers and/or HTML pages.

Main goal of SubWeb is to contribute to the tests of network applications based on HTTP. HTTPS is not directly managed in SubWeb, it is necessary, in order to test a SSL server, to use the stunnel program, for example.

SubWeb has 3 operating modes:

- * proxy (classical HTTP proxy)
- * midproxy (HTTP proxy which requires the pages of another proxy)
- * rproxy (reverse proxy, SubWeb mimic an HTTP server)

Another functionality, named virtual Web, allow SubWeb to answer certain requests (depending on keywords contained in these requests) without requiring anything to the server.

It is possible to visualize all the traffic between the customers and the servers. There are several options of visualization (only the headers, to display binary pages in Hexa, to display only the requests or only the answers...)

In the three modes it is possible to apply filtering at all the levels, ie. in the URL, the headers and the body of the pages, in the

SecurityFocus Penetration: [SubWeb] NEW http proxy/reverse proxy

requests and the answers.

Another type of filtering, named dynamic, is activable by adding the string subweb=on in the URL. These dynamic filters are interesting, for example, to change fields like a cookie or a session_id in a session after passing the authentication.

An experimental functionality was added to the reverse relay mode. It makes it possible to cipher the contents of the hidden fields sent by the server to the various customers and to decipher them when the customers send them back to the server in requests GET or POST requests.

This mechanism forbidden the users to modify the value of the hidden fields, which makes it possible to protect them and use them for example to manage the order of the requests required by a customer.

PS: SubWeb is not underground ;)

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- ***Previous message:*** Joshua Wright: "RE: sniffing X traffic."
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]