Apache 2.x Module

MOD_BUT

March 8, 2006

Document Name:	mod_but_v2.2.doc
Version:	V 2.2
Author(s):	Ivan Buetler, Compass Security AG
Date of Delivery:	March 8, 2006
Classification:	PUBLIC

Table of Contents

Date: Mar 8, 2006

1 Introduction

1.1 News

This is version 2.0 of MOD_BUT. The most interesting changes are:

- Successfully compiled and tested with Microsoft Windows

- Configuration directive for URL's the user is authorized to access after successfull authenticated

- Configuration directive for authentication servers, who are allowed to send special meaning response headers (change authentication level)

1.2 Preamble

Apache has been the most popular web server on the Internet since April of 1996. The February 2005 Netcraft Web Server Survey[1] found that more than 68% of the web sites on the Internet are using Apache, thus making it more widely used than all other web servers combined.

Apache offers flexible programming interfaces, by which the core functionality is expandable. If such an additional functionality, in terms of Apache it is called a "module", is rather successful, it could be added to the main distribution. Examples of successful modules are mod_rewrite, mod_proxy or mod_ssl.

1.3 Goals of this Project

Large e-business infrastructures take advantage of so-called web application firewalls. These are placed in front of web infrastructures and used as security device. In Switzerland, we use the term "Entry Server" for such products and concepts. We will later use the term "Entry Server" in this document.

Ivan Buetler developed a proof-of-concept entry server, based on Apache 2.x web server APR (Apache Programming Runtime) interfaces. This module illustrates entry-server functionality in theory and in practice using a demonstration webpage. By doing so, we hope the reader will fully understand the concept of entry servers.

The module's name is "MOD_BUT". It is probably not the most common name for an Apache module, but rather unique in the Internet. The module is open source, in development stage and therefore not recommended for productive use.

The module is not only an entry-server. Additionally, it can be used in Web Security Assessments, because it simplifies session handling and tracking mechanisms. The assessment idea was the basic driver behind MOD_BUT.

---

[1] *Web Server Survey: http://news.netcraft.com/archives/web_server_survey.html*

1.4 About the Author

Ivan Buetler co-founded Compass Security AG[2] in February 1999 where he works as a Security Analyst and Managing Director. Compass Security is active in the domains of security assessments and forensic investigations and is located in Rapperswil Switzerland. Additionally, Ivan teaches at the University of Applied Sciences Rapperswil[3] and the HSW Lucerne[4]. He has published several security reports in the security field.

1.5 Web Application Security Lab

The strength of Compass Security is its web application-training infrastructure. This enables our customers and trainees to learn about web risks both theoretically and with practical exercises. The Application Security Lab[5] course deals with the security of Web applications. During the three-day course, the trainee dives into the world of browsers, cookies, sessions and secure coding.

Compass Security has incorporated the most common web developer mistakes into its training web applications. These applications are the target of lab exercises which deal with authentication, encryption, session handling, input validation, secure coding, design decisions, database access and authorization aspects. The new MOD_BUT will bring entry server knowledge to this training.

1.6 Solution Provider for Commercial Entry Servers

There are several commercial entry server products available.

- Seclutions AirLock[6]
- AdNovum Nevis Web[7]
- tetrade secure entry server[8]
- IBM Tivoli Access Manager (a.k.a. WebSEAL)[9]

Owing to the early development stage of MOD_BUT we recommend evaluating one of the above products, if you plan to use an entry server.

---

[2] *Compass Security Network Computing AG: http://www.csnc.ch*
[3] *HSR Hochschule für Technik Rapperswil: http://www.hsr.ch/*
[4] *HSW Hochschule für Wirtschaft Luzern: http://www.hsw.fhz.ch/*
[5] *Application Security Lab: http://www.csnc.ch/estatic/services/training/asl.html*
[6] *Seclutions AirLock - Application Security Gateway: http://www.seclutions.ch/en/ct_products_en.htm*
[7] *Adnovum Nevis Web: http://www.adnovum.ch/sol/nevis.html*
[8] *tetrade secure entry server: http://www.tetrade.ch/tt/de/competence/si.html*
[9] *IBM Tivoli Access Manager for e-Business: http://www-306.ibm.com/software/tivoli/products/access-mgr-e-bus/*

1.7 Version Control

Version	Date	Changes	Author
1.0	18.11.2005	Initial Version Register module in modules.apache.org Publication via Compass Security	Ivan Buetler
1.1	18.01.2006	Reduce default SHM size in mod_but.h Delete mod_but_input_filter.c from source	Ivan Buetler
2.0	28.02.2006	Support for Authorization URL Compiles with Microsoft Windows	Ivan Buetler
2.1	03.03.2006	Add description how to compile mod_but with Microsoft Windows	Ivan Buetler

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 5   Date: Mar 8, 2006

2 MOD_BUT Apache 2.x Module

2.1 Introduction

This document describes the core functionality of MOD_BUT, an Apache 2.x module designed to operate as a reverse proxy enhancement component. MOD_BUT integrates with other standard modules (e.g. mod_rewrite, mod_proxy, mod_ssl).

MOD_BUT implements the following functionality:

- Authentication. Requests from authenticated users are sent to backend systems. This document refers other servers "behind" the reverse proxy as backend systems. Unauthenticated requests are denied from being sent to backend systems. By doing so, only authenticated users are allowed to access an entry server-protected web site. MOD_BUT allows you to define special URLs for which authentication is not enforced.

- Cookie based session handling between the client and the reverse proxy. This session is referred to as "***MOD_BUT session***".

- Cookie hiding of backend application cookies within a shared memory store. This type of shared memory segment is referred as "Cookie Store", "Cookie Bag" or "Session Store". The session between the reverse proxy and the backend system is referred as "***Backend Session***". For example the *jsessionid* is the backend session for Java based web application servers, like Tomcat, WebSphere or BEA WebLogic.

- Centralized session termination implements the logout feature.

- HttpOnly[10] cookie flag support.

- Support for "free" cookies which are not handled by MOD_BUT and are sent transparently between the client and the backend system.

- MOD_BUT has another URL-based authorization layer. Once the user is authenticated at MOD_BUT by default, he or she will have access to any backend system URL. The login application can setup a URL restriction for which the user is authenticated.

MOD_BUT does *not* offer the following features:

- MOD_BUT is not compatible with Apache 1.x web servers.

- Request filtering is not implemented by MOD_BUT. We recommend using mod_security instead.

- MOD_BUT only handles cookie-based sessions.

---

[10] *Mitigating Cross-site Scripting With HTTP-only Cookies:*
   http://msdn.microsoft.com/workshop/author/dhtml/httponly_cookies.asp

- MOD_BUT does not have nice configuration interfaces like Seclutions Airlock. Configuration is achieved through changes in the Apache configuration files.

- MOD_BUT is unable to use the SSL session id as additional session information. This is something we consider implementing later.

The core of MOD_BUT is its shared memory management, which enables a standard Apache reverse proxy to handle its own sessions. Shared memory is implemented via Apache APR interfaces.

MOD_BUT uses a variety of configuration directives, and is not one of the easy "download, configure, make, make install" modules. Therefore, we have created a demonstration application, where you can play around with MOD_BUT before putting it to use yourself.

2.2 Demo Application

There is an Internet demonstration application available at http://www.but.ch/mod_but/ . It will help you fully understanding the functionality of MOD_BUT. However – before really testing MOD_BUT, we recommend reading through this chapter first, which describes the demonstration setup and its architecture. Especially when you step through the test cases it is important to know, in what setup and infrastructure you are.
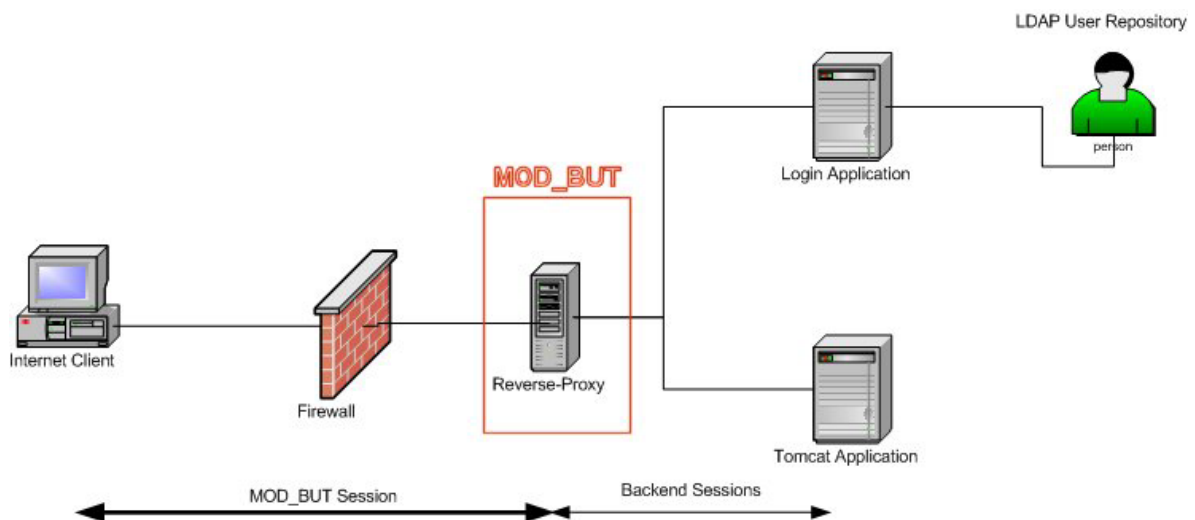
The demo application consists of the following components:

- Firewall
- Apache 2.0.55 Web Server with enabled MOD_BUT. This component is configured as reverse proxy. It does nothing more than forwarding requests to backend systems.
- Tomcat Test Servlet
  - Login Application
  - EchoRequest Servlet – this implements the test backend system
  - SetCookie Servlet – this implements the test backend system

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 7   Date: Mar 8, 2006

- OpenLDAP user repository

MOD_BUT is designed as an entry server. Hence the reverse proxy inserts its own session (MOD_BUT session) between the client computer and itself. If a backend application (in our case the demonstration servlets) wants to set a cookie, they will not be wired to the client by default. The cookie (in our case we regard the cookie as a backend system session) will be stored in the user's cookie store shared memory segment on the reverse proxy.

Later, while the user requests a backend server URL, MOD_BUT will first verify the existence and validity of the MOD_BUT session and if it is correct, lookup further backend system cookies from its cookie store and insert them into the final mod_proxy backend HTTP request header.

Additionally, MOD_BUT checks whether the user is already authenticated or not. If the requesting URL requires authentication and the user is not authenticated yet, the user will be redirected to a login page. If provided login credentials match, the Login Application will set a special cookie telling MOD_BUT to flag the user's session as authenticated.

The demonstration application stores user credentials within the OpenLDAP database. But this is independent of MOD_BUT and not really interesting in this demo application. Information exchange between the Login Application and MOD_BUT is implemented via HTTP headers.

The demo suite has the following look & feel:

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 8   Date: Mar 8, 2006
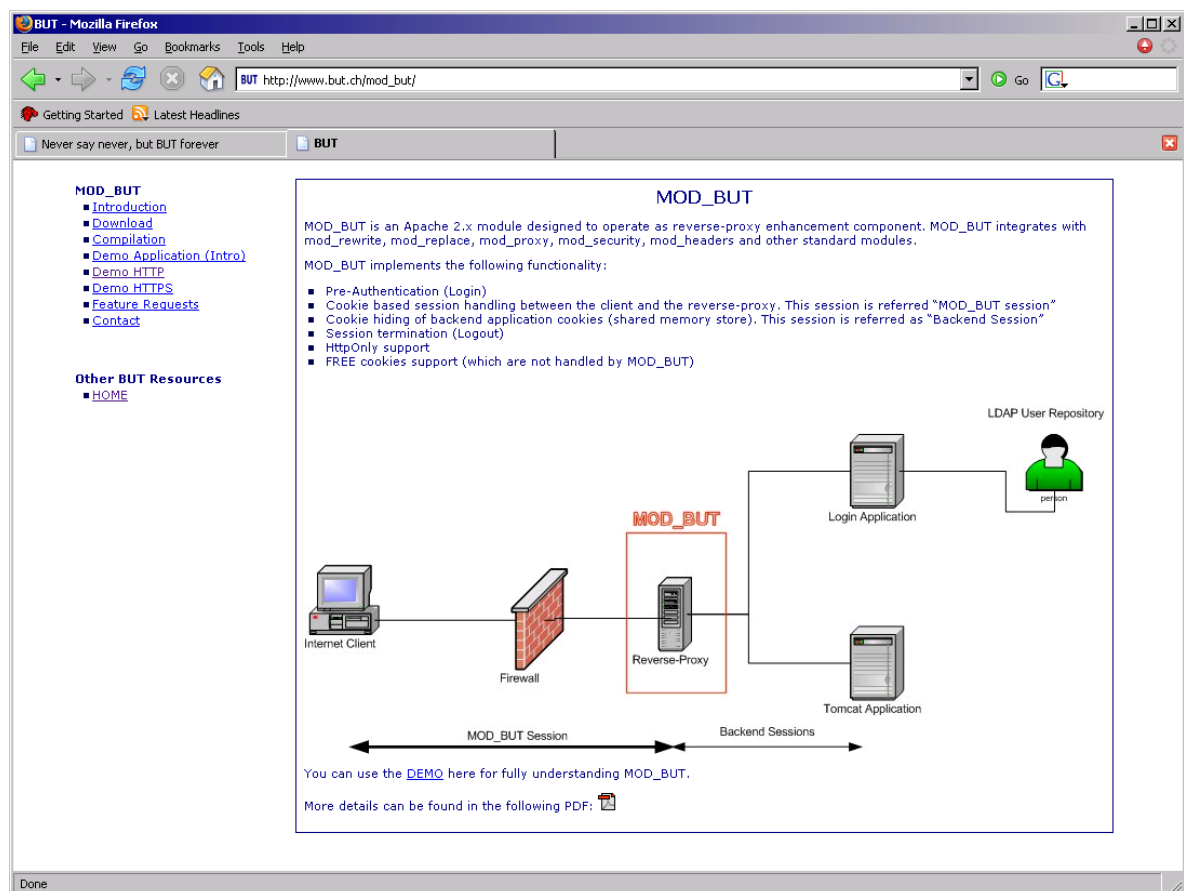
2.3 Test Cases

This chapter introduces some test cases that can be run from your local computer using a cookie-enabled browser. These test cases will help you fully understand MOD_BUT and its pros and cons.

The demo is available via HTTP or HTTPS. But please keep in mind the SSL certificate is self-signed. The HTTP demo will give you the chance snooping network packets to verify the traffic content. We recommend *Ethereal*[11] as a network sniffer. It is available for all major Unix derivates and Microsoft Windows systems. Another valuable client side analyzing tool is *Paros*[12]. It acts as client proxy and you get the chance to view, modify request and responses between your client and MOD_BUT. Please refer to the Ethereal and Paros page if you plan using this software. Another nice Firefox plug-in is called *LiveHTTPHeaders*[13]. It opens another Firefox window containing request header and response header information.

The demo application requires authentication! Please use the following user credentials while testing MOD_BUT:

Username = **mod_but**
Password = **demo**

Now – we wish you happy testing using the test cases below…

---

[11] *Ethereal: http://www.ethereal.com/*
[12] *Paros Proxy: http://www.parosproxy.org/*
[13] *LiveHTTPHeaders: http://livehttpheaders.mozdev.org/installation.html*

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

2.3.1 Cookie Support

Goal	Browser must have cookie support enabled
Preparation	Configure your browser – Ask me every time
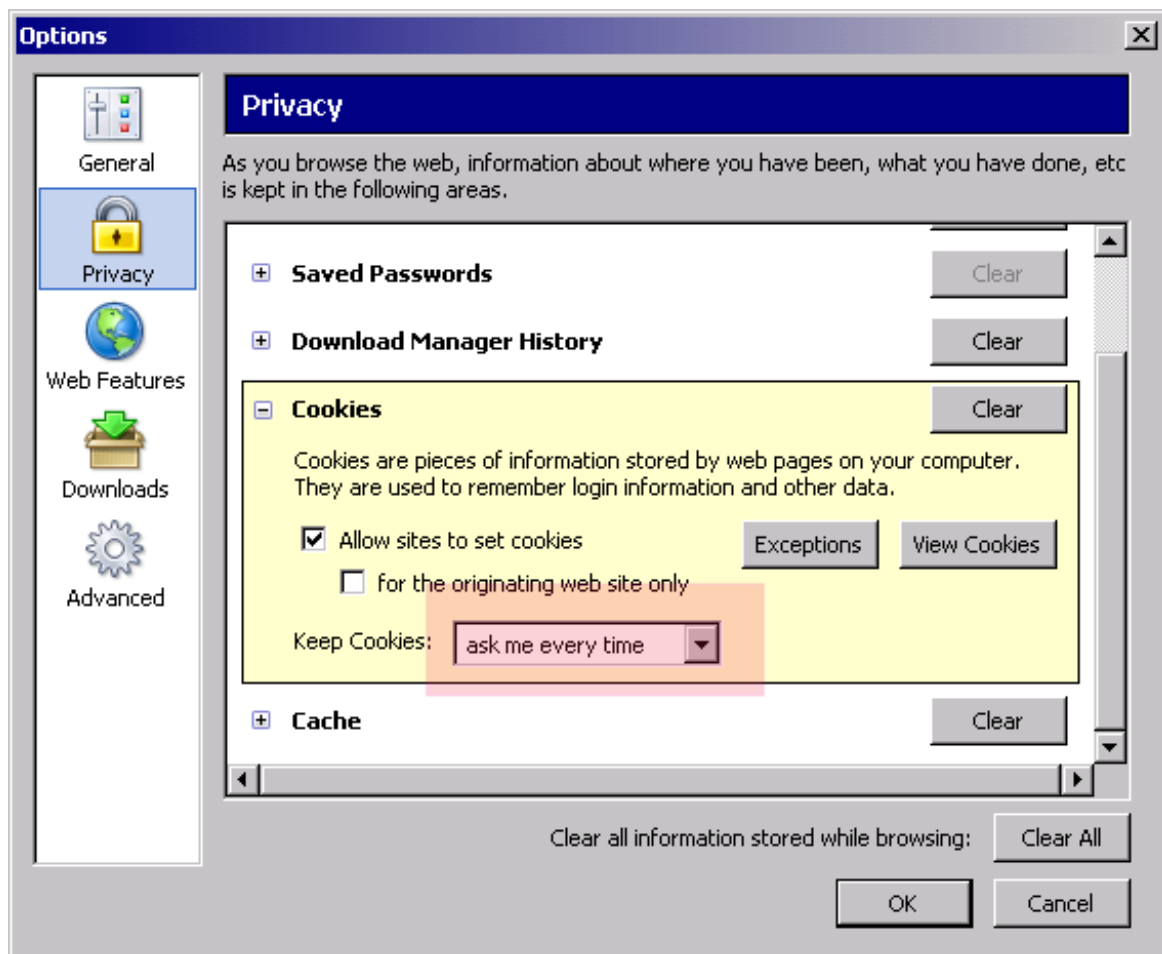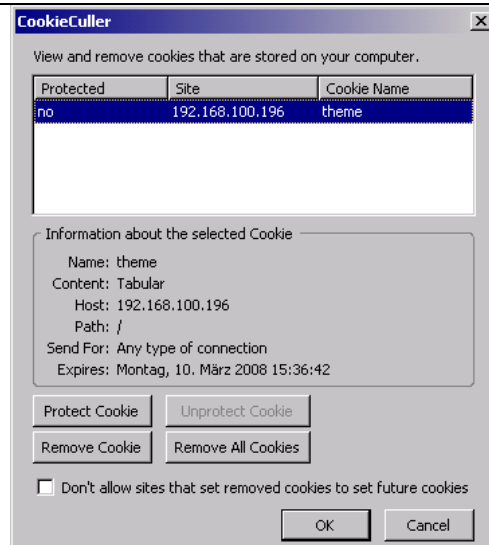
No	Description of Test	Expected Result	Actual Result	PASS FAIL
1	Go to the following URL and do not accept the set cookie for several times http://www.but.ch/mod_but/protected/	After 3 cookie tries, the browser is redirected to a "information" page. Cookies are required for MOD_BUT to run properly.		

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 10   Date: Mar 8, 2006

2.3.2 Login and Logout Test Cases

Goal	Login and Logout
Preparation	Internet

First of all, let us test the login and logout behavior. Go through the test cases below and verify if our expected result meets your own test results. If they diverge, we will gladly receive suggestions for improvement. We recommend enabling the option "ask cookies before accepting" within your browser.

The Firefox CookieCuller[14]. plug-in will help you doing the next test cases:

	CookieCuller plug-in helps you in removing cookies.

No	Description of Test	Expected Result	Actual Result (Please fill in here your test results)
1	a) Delete all cookies from your browser[15]. b) Go to the following URL (this is a protected page) http://www.but.ch/mod_but/protected/index.html c) Authenticate in the login form correctly using the given credentials.	b) Redirect to login page c) Redirect to /protected/index.html After c) you should be logged into MOD_BUT.	

---

[14] *We use Firefox CookieCuller Plug-In for cookie deletion tasks. You can close/open your browser instead.*
[15] *We use Firefox CookieCuller Plug-In for cookie deletion tasks. You can close/open your browser instead.*

No	Description of Test	Expected Result	Actual Result (Please fill in here your test results)
2	a) Delete all cookies from your browser. b) Go to the following URL and authenticate correctly http://www.but.ch/mod_but/protected/index.html c) Go to the following URL http://www.but.ch/logout/	c) You are logged out. Press "Browser BACK" button. You should not be able to "see" the content you saw before the logout	
3	a) Make sure you have done step 2) properly and you have clicked the logout button. b) Go to the following URL http://www.but.ch/mod_but/protected/index.html	You are logged out. This means, that MOD_BUT really destroys its session. You can click on "renew" session if desired.	
4	Download the Firefox CookieCuller plug-in[16]. Afterwards; you can edit cookies within your browser instances. a) Go to the following URL and authenticate correctly http://www.but.ch/mod_but/protected/index.html b) Modify the cookie **value** of the MOD_BUT session with the CookieCuller plug-in to "another" value. Just add/remove something to the cookie value. c) Type Refresh Button after you have saved b).	You are redirected to a "hacker attempting" web page. MOD_BUT thinks you are a hacker, because you have sent an unknown MOD_BUT session and this is evaluated as hacking attack.	

---

[16] *CookieCuller: https://addons.mozilla.org/extensions/moreinfo.php?id=82*

No	Description of Test	Expected Result	Actual Result (Please fill in here your test results)
5	a) Go to the following URL and authenticate correctly http://www.but.ch/mod_but/protected/index.html b) Open the CookieCuller and remember the session value. Copy the session value into a temporary text file. c) Logout d) Close the browser or delete all cookies. e) Go to the following URL and authenticate correctly http://www.but.ch/mod_but/protected/index.html f) Use the CookieCuller and replace the current session value with the session you have remembered previously in step b).	You are redirected to a page where you get informed that you are using a "history" session. A history session is a session used earlier in MOD_BUT. This behavior will not send a "hacking attempt" page to the client, as we did in step 5 Used MOD_BUT sessions are held within a shared memory history store for a configurable duration. The current configuration keeps such history sessions for 8 hours.	
6	a) Go to the following URL and authenticate correctly http://www.but.ch/mod_but/protected/index.html b) Logout using the logout button. c) Press the browser's back-button several times. Vulnerable login services offer a "resend POST data again". But because MOD_BUT uses redirects after successful authentication, MOD_BUT is not vulnerable to such attacks.	You should not see a message "resend POST data" at any time. It would mean that your login service is vulnerable to a "post data resend attack".	

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 13   Date: Mar 8, 2006

2.3.3 Cookie Store

Goal	Session Handling
Preparation	Internet

MOD_BUT offers a session store, which holds back backend-session within the shared memory and hides them from the client. Backend sessions are referenced via the MOD_BUT session and are added automatically to the HTTP request headers between the reverse proxy and the backend application or are removed from the HTTP response headers when inserted by a backend application.

MOD_BUT supports "free" cookies. These cookies are not handled by MOD_BUT but transparently wired between the client and the backend system. Such cookies are not held within the shared memory segment. The demonstration application has two free cookies configured. They are named as *trustme* and *language*.

No	Description of Test	Expected Result	Actual Result (please fill in here your test results)
7	a) Go to the following URL and authenticate correctly http://www.but.ch/webapp/but/SetCookie b) You should see a form where you can enter two cookie names, values and path properties. Now you can play around with the SetCookie Servlet. This Servlet gives you the chance to set cookies in exactly the same manner as BEA WebLogic, IBM WebSphere or any other J2EE containers. We recommend trying it without a specific "expected result". Just play around with the SetCookie Servlet. Go to the following Servlet, if you want to see all request headers sent from MOD_BUT to the backend application http://www.but.ch/webapp/but/EchoRequest	N/A	

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 14   Date: Mar 8, 2006

No	Description of Test	Expected Result	Actual Result (please fill in here your test results)
8	After you have played with previous test case #7, we continue with specific test cases. They should be more understandable if you have previously tried test case #7! a) Go to the following URL and authenticate correctly http://www.but.ch/webapp/but/SetCookie b) Configure a cookie with Cookie name = Cool4You Cookie value = **12345** Path = / Click submit button c) Check your browser's stored cookies. (Use CookieCuller you have installed in test case #4). d) Go to the EchoRequest Servlet http://www.but.ch/webapp/but/EchoRequest	b) You should not see a *Cool4You* cookie within your browser c) The *Cool4You* cookie should be sent to the backend system. The cookie was held within the shared memory segment and automatically inserted to your c)-request header.	
9	a) Make sure you performed test case #8 and you have not deleted cookies afterwards. b) Go to the following URL and authenticate correctly http://www.but.ch/webapp/but/SetCookie c) Configure a cookie with Cookie name = Cool4You Cookie value = **abcdefg** Path = / Click submit button d) Check your browser's stored cookies. (Use CookieCuller you have installed in test case #4). d) Go to the EchoRequest Servlet http://www.but.ch/webapp/but/EchoRequest	c) You should not see a *Cool4You* cookie within your browser d) MOD_BUT has detected that you want to change the cookie value from test case #8. The EchoRequest Servlet should show you an updated *Cool4You* cookie value. In this test case, the value should be **abcdefg**.	

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 15   Date: Mar 8, 2006

No	Description of Test	Expected Result	Actual Result (please fill in here your test results)
10	a) Make sure you performed test case #9 and you have not deleted cookies afterwards. b) Go to the following URL and authenticate correctly http://www.but.ch/webapp/but/SetCookie c) Configure a **first** cookie with Cookie name = MyCookie Cookie value = **foobar** Path = / and a second cookie.. Cookie name = Cool4You Cookie value = **7777777** Path = / Click the submit button. d) Check your browser's stored cookies. (Use CookieCuller you have installed in test case #4). e) Go to the EchoRequest Servlet http://www.but.ch/webapp/but/EchoRequest	d) You should still not see application cookies; only the MOD_BUT session should be visible. e) You should see a new cookie *MyCookie* and an updated *Cool4You* cookie.	

No	Description of Test	Expected Result	Actual Result (please fill in here your test results)
11	a) Make sure you performed test case #9 and you have not delete cookies afterwards. b) Go to the following URL and authenticate correctly http://www.but.ch/webapp/but/SetCookie c) Configure a **first** cookie with Cookie name = Cool4You Cookie value = **998899** Path = / and a second cookie.. Cookie name = AnotherCookie Cookie value = **qwertz** Path = / Click the submit button. d) Check your browser's stored cookies. (Use CookieCuller you have installed in test case #4). e) Go to the EchoRequest Servlet http://www.but.ch/webapp/but/EchoRequest	d) You should still not see application cookies, only the MOD_BUT session e) You should see a new cookie *AnotherCookie* and an updated *Cool4You* cookie. This test is very similar to the test case #10. But we want to make sure MOD_BUT works independent from the set-cookie order. If you performed test case #10 and #11 with the expected result you have proof that MOD_BUT handles known and new cookies correctly. This is important, because if MOD_BUT receives a change request for a known cookie, everything needs to be newly assigned within the shared memory.	

No	Description of Test	Expected Result	Actual Result (please fill in here your test results)
12	Now it is time to start with a clean setup. Please remove all cookies or close and start again your browser. This test verifies the "free" cookies support. These are cookies which are not held within MOD_BUT but are transparently wired between the client and the backend system. a) Go to the following URL and authenticate correctly http://www.but.ch/webapp/but/SetCookie b) Configure a cookie with Cookie name = **trustme** Cookie value = 12345 Path = / Click the submit button c) Check your browser's stored cookies. (Use CookieCuller you have installed in test case #4). d) Go to the EchoRequest Servlet http://www.but.ch/webapp/but/EchoRequest	b) You should see the cookie *trustme* within your browser's cookie store. Test this via CookieCuller plug-in. This means, that MOD_BUT did not store the *trustme* cookie to your session store. Instead, it is sent to your browser. d) Check with the EchoRequest Servlet if your *trustme* cookie is wired to the backend system	
13	Find new test cases by yourself. Try combinations and remember MOD_BUT handles *trustme* and *language* cookie names as "free".	N/A	
14	How does MOD_BUT handle unexpected cookies? Download the *Add N Edit Cookie* Plug-in[17] for Firefox, which enables the client to manipulate cookie attributes within the client's browser instance. Go to the demo application, authenticate correctly and set some cookies of your choice. Now add another cookie name with the Cookie Editor for Firefox and go to the EchoRequest Servlet afterwards. If you do so, MOD_BUT receives an unexpected cookie from the outside and shall not wire the unexpected cookie to the backend system.	Your self-defined "unexpected" cookie shall not be seen within the EchoRequest Servlet. Only the cookies declared to MOD_BUT shall be seen. These are: a) MOD_BUT session b) Optionally: trustme cookie c) Optionally: language cookie d) Optionally: your self defined cookies from the SetCookie Servlet	

---

[17] *Add & Edit Cookies - Cookies Editor: http://addneditcookies.mozdev.org/*

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 18   Date: Mar 8, 2006

2.3.4 Important URLs

There are several test cases you can perform against MOD_BUT. Use the information below for further test cases you like to perform.

- http://www.but.ch/mod_but/   Public accessible (anonymous access)
- http://www.but.ch/mod_but/protected/   **Authentication required**
- http://www.but.ch/logout/   Session termination URL
- http://www.but.ch/webapp/but/EchoRequest   **Authentication required**
- http://www.but.ch/webapp/but/SetCookie   **Authentication required**

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61   Page: 19   Date: Mar 8, 2006
team@csnc.ch   www.csnc.ch
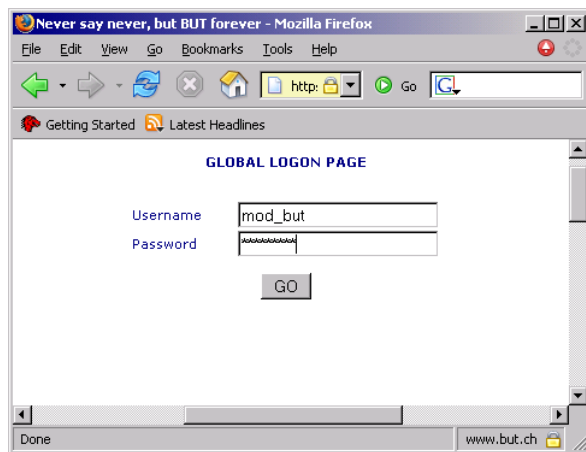
2.4 UML Sequence Diagram

The sequence diagram below introduces the initial login phase and backend system initialization phase.

- Client   Internet client using a browser (IE, Firefox, Mozilla, …)
- MOD_BUT   Apache 2.x reverse proxy with enabled MOD_BUT
- Login Service   Tomcat login application (Servlet)
- User Repository   LDAP directory
- Web-Application   http://www.but.ch/mod_but/protected/index.html
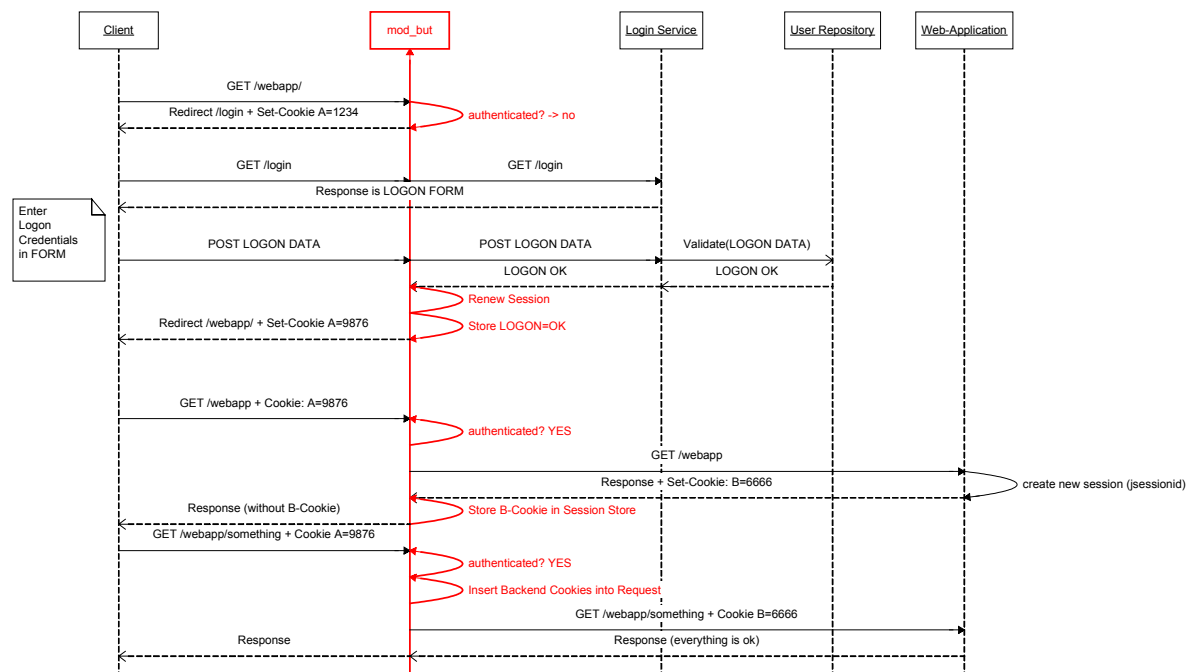
MOD_BUT offers pre-authentication if configured. Only authenticated sessions are sent to the backend web-application server. MOD_BUT will check all client requests for the existence of a MOD_BUT session and does only process those client request having one. Once the client sends a MOD_BUT session and it is marked as "authenticated", the request will be fed into mod_proxy for the final backend destination.

MOD_BUT keeps its sessions in its local shared memory segment[18] (including authentication status, last requested URL, backend cookies etc). By this technique, backend sessions are hidden from the client.

The URL of the Login Service is configurable in MOD_BUT, globally or per directory level (Location directive in httpd.conf).

---

[18] Some name the local shared memory as „Session Store", „Cookie Store" or "Cookie Bag". This document refers to it as "Cookie Store", because MOD_only handles cookie-based session handling.

2.5 Compatibility

MOD_BUT was designed to operate properly with the following standard Apache modules:

- mod_rewrite[19]
- mod_proxy[20]
- mod_ssl[21]

Additionally the following non-standard module is supported:

- mod_security[22]
- mod_replace[23]

MOD_BUT was successfully tested and compiled on:

- Solaris 8 / Sparc / gcc / Apache 2.0.55
- Solaris 10 / Sparc / gcc / Apache 2.2.0
- Linux 2.6.12 / Intel / gcc / Apache 2.0.55
- Microsoft Windows / VC++ / Apache 2.0.55

MOD_BUT is a new module. It was developed in Q1/Q2 2005. If you feel like sending bug reports or other comments, please this e-mail address: e1@but.ch.

2.6 Limitations

Limitation	Possible remedy; future enhancement
MOD_BUT integrates properly into a "real" reverse proxy configuration. In mixed-mode, where you deliver static content locally (at the reverse-proxy) and send other requests to backend systems, MOD_BUT will fail.	N/A
MOD_BUT does accept control cookies from any backend system.	Another improvement step can be just accepting authentication=ok messages from the login service.
MOD_BUT does not support URL-based access control. This is on the wish list too, because once you have been authenticated in MOD_BUT, you can reach all backend systems and URLs.	The improvement could be implemented by inserting a "role" to the LDAP directory and binding users to such roles. Once the user authenticates successfully, he or she has access to the URLs for that role.

---

[19] mod_rewrite: http://httpd.apache.org/docs/2.0/mod/mod_rewrite.html

[20] mod_proxy: http://httpd.apache.org/docs/2.0/mod/mod_proxy.html

[21] mod_ssl: http://httpd.apache.org/docs/2.0/mod/mod_ssl.html

[22] mod_security: http://www.modsecurity.org/

[23] mod_replace: http://mod-replace.sourceforge.net/docs.html

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 21   Date: Mar 8, 2006

Limitation	Possible remedy; future enhancement
MOD_BUT does not filter requests, parameters and values.	Such functionality is usually implemented in commercial entry server software. We use mod_security instead, which is compatible with MOD_BUT.
MOD_BUT is not SSL session ID aware.	Commercial products are able to use the SSL session id as additional session handling mechanism. Potentially, the use of the SSL session id will be implemented in future versions of MOD_BUT.
MOD_BUT has not been improved for the use with client certificates.	This is potentially another update step.

2.7 Mailing List

If you want to keep track of MOD_BUT and its development, please subscribe to the following mailing list. Send an e-mail and use "subscribe" in the message subject.

Mailing List: mod_but@but.ch

2.8 Browsers with disabled Cookie Support

MOD_BUT requires the client to have cookie support enabled. **Otherwise, MOD_BUT does not work**. Therefore, MOD_BUT implements some test routines at the initialization phase. If a client denies the *Set-Cookie* header several times, the user will be redirected to an error page. This error page is configurable in httpd.conf and informs the user that he or she has to enable cookies while using the MOD_BUT protected site.

Make sure this error page is configured somewhere where MOD_BUT does not enforce the existence of a MOD_BUT session. Otherwise Apache will loop infinitely.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 22   Date: Mar 8, 2006

3 MOD_BUT Configuration Directives

3.1 List of Configuration Directives

```
MOD_BUT_ENABLED                             Chapter 3.2
MOD_BUT_CLIENT_REFUSES_COOKIES_URL          Chapter 3.3
MOD_BUT_COOKIE_NAME                         Chapter 3.4
MOD_BUT_COOKIE_DOMAIN                       Chapter 3.4
MOD_BUT_COOKIE_PATH                         Chapter 3.4
MOD_BUT_COOKIE_EXPIRATION                   Chapter 3.4
MOD_BUT_COOKIE_SECURE                       Chapter 3.4
MOD_BUT_COOKIE_HTTPONLY                     Chapter 3.4
MOD_BUT_SESSION_FREE_URL                    Chapter 3.5
MOD_BUT_SESSION_TIMEOUT                     Chapter 3.5
MOD_BUT_SESSION_TIMEOUT_URL                 Chapter 3.5
MOD_BUT_SESSION_RENEW_URL                   Chapter 3.5
MOD_BUT_SESSION_INACTIVITY_TIMEOUT          Chapter 3.5
MOD_BUT_SESSION_INACTIVITY_TIMEOUT_URL      Chapter 3.5
MOD_BUT_SESSION_HACKING_ATTEMPT_URL         Chapter 3.5
MOD_BUT_SESSION_TIMEOUT_HISTORY             Chapter 3.5
MOD_BUT_SESSION_DESTROY                     Chapter 3.5
MOD_BUT_SESSION_DESTROY_URL                 Chapter 3.5
MOD_BUT_SESSION_STORE_FREE_COOKIES          Chapter 3.5
MOD_BUT_ALL_SHM_SPACE_USED_URL              Chapter 3.6

MOD_BUT_AUTHORIZATION_ENABLED               Chapter 3.7
MOD_BUT_GLOBAL_LOGON_SERVER_URL             Chapter 3.7
MOD_BUT_GLOBAL_LOGON_AUTH_COOKIE_NAME       Chapter 3.7
MOD_BUT_GLOBAL_LOGON_AUTH_COOKIE_VALUE      Chapter 3.7
MOD_BUT_AUTHORIZED_LOGON_URL                Chapter 3.7    New since Version 2.0

MOD_BUT_LOGON_SERVER_URL                    Chapter 3.8
MOD_BUT_LOGON_REQUIRED                      Chapter 3.8

MOD_BUT_SERVICE_LIST_ENABLED                Chapter 3.9    New since Version 2.0
MOD_BUT_SERVICE_LIST_COOKIE_NAME            Chapter 3.9    New since Version 2.0
MOD_BUT_SERVICE_LIST_COOKIE_VALUE           Chapter 3.9    New since Version 2.0
MOD_BUT_SERVICE_LIST_AUTH_ERROR_URL         Chapter 3.9    New since Version 2.0
```

3.2 Enable/Disable

It is possible to Enable/Disable MOD_BUT per VirtualHost.

Context: virtual host

Key	Parameter	Description
MOD_BUT_ENABLED	On, Off	Enable/Disable MOD_BUT per VirtualHost Default: Off

3.3 Cookie Test

MOD_BUT requires HTTP cookies to work properly. If the client multiple time denies Set-Cookie headers, MOD_BUT will send an error page. The configuration directive configures the URL of this error page.

Context: virtual host

Key	Parameter	Description
MOD_BUT_CLIENT_REFUSES_ COOKIES_IN_URL	String	Configure error URL, if browser denies Set-Cookie headers Default: none

Note: Be aware that **MOD_BUT_CLIENT_REFUSES_COOKIES_IN_URL** must be part of the **FREE URL section**. Otherwise Apache will **loop with URL redirections**.

3.4 Cookie Settings

The following configuration directives define the MOD_BUT_SESSION. This is the cookiethat is used between the client and MOD_BUT.

Context: virtual host

Key	Parameter	Description
MOD_BUT_COOKIE_NAME	String	Configure cookie name Default: MOD_BUT
MOD_BUT_COOKIE_DOMAIN	String	Configure cookie domain Default: not specified

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 24   Date: Mar 8, 2006

Key	Parameter	Description
MOD_BUT_COOKIE_PATH	String	Configure cookie path Default: /
MOD_BUT_COOKIE_EXPIRATION	String	Configure cookie expiration date Default: not specified
MOD_BUT_COOKIE_SECURE	String	Configure cookie secure Default: secure
MOD_BUT_COOKIE_HTTPONLY	String	Configure HttpOnly (IE 6.0 SP1) Default: HttpOnly

Note: Be aware that **MOD_BUT_COOKIE_EXPIRATION** should be left empty so the session will reside within the browser's memory only and is not stored to the hard disk. HttpOnly is a special flag for Microsoft Internet Explorer 6.0, SP1. It denies JavaScript from accessing cookies.

3.5 Session Settings

Context: virtual host

Key	Parameter	Description
MOD_BUT_SESSION_FREE_URL	String	Regular expression: Configure patterns, for which MOD_BUT will not apply its session tests Default: not specified
MOD_BUT_SESSION_TIMEOUT	Integer	Configure max session time of MOD_BUT (elapsed time). Default: 3600 (seconds)
MOD_BUT_SESSION_TIMEOUT_URL	String	Error URL in case the session is timed out Default: not specified
MOD_BUT_SESSION_RENEW_URL	String	Regular expression: Renew pattern for which MOD_BUT will create a new session, independent of what the client sent previously Default: not specified

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

Page: 25 Date: Mar 8, 2006

Key	Parameter	Description
MOD_BUT_SESSION_INACTIVITY_TIMEOUT	Integer	Configure inactivity timeout. This timeout is below the session timeout Default: 900 (seconds)
MOD_BUT_SESSION_INACTIVITY_TIMEOUT_URL	String	Error URL in case the inactivity timeout is reached Default: not specified
MOD_BUT_SESSION_HACKING_ATTEMPT_URL	String	Error URL in case the client is "guessing" sessions Default: not specified
MOD_BUT_SESSION_TIMEOUT_HISTORY	Integer	Configure how long MOD_BUT shall "remember" used session. I have configured this value to 24 hours Default:
MOD_BUT_SESSION_DESTROY	String	Regular expression: Logout pattern (session destroy) Default:
MOD_BUT_SESSION_DESTROY_URL	String	Error URL in case the client has logged out Default:
MOD_BUT_SESSION_STORE_FREE_COOKIES	String	Regular expression: Configure cookie names, which are not handled by MOD_BUT. They pass the reverse proxy without being kept within the shared memory session store Default: not specified

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 26   Date: Mar 8, 2006

3.6 Shared Memory Settings

Context: virtual host

Key	Parameter	Description
MOD_BUT_ALL_SHM_SPACE_USED_URL	String	Error URL in case MOD_BUT is not able to store a session to the shared memory segment Default: not specified

Note: The shared memory size is not configurable in httpd.conf, because the configuration file is parsed after Apache is started. Therefore, some configuration settings need to be configured in mod_but.h before compiling MOD_BUT.

mod_but.h

Key	Parameter	Description
MOD_BUT_SESSION_COUNT	Integer	Define number of MOD_BUT sessions (most important) Default: 1000
MOD_BUT_SESSION_HISTORY_COUNT	Integer	Define number of history count (the history of used sessions) Default: 1000
MOD_BUT_COOKIESTORE_COUNT	Integer	Define cookie store count. This shared memory segment stores the backend cookies (sessions) Default: 5000

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 27   Date: Mar 8, 2006

3.7 Global Authentication and Authorization

Context: Virtual Host

Key	Parameter	Description
MOD_BUT_AUTHORIZATION_ENABLED	On, Off	If set to "On", MOD_BUT will test the MOD_BUT session for authentication. Only authenticated users are allowed requesting protected URL's If set to "Off", MOD_BUT will not enforce authentication to any URL. Default: off
MOD_BUT_GLOBAL_LOGON_SERVER_URL	String	Defines the URL where the login application resides. The GLOBAL value is used, if the Location directive does not configure it's own login service URL. Default: not specified
MOD_BUT_GLOBAL_LOGON_AUTH_COOKIE_NAME	String	Define cookie name of MOD_BUT, which changes the authentication status. This cookie is sent from a backend-system as response header Default: LOGON
MOD_BUT_GLOBAL_LOGON_AUTH_COOKIE_VALUE	String	Define cookie value of MOD_BUT, which changes the authentication status. Default: ok

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 28   Date: Mar 8, 2006

Key	Parameter	Description
MOD_BUT_AUTHORIZED_LOGON_URL	String	Regular expression. This is a new setting since V2.0. If configured, one can configure an URL, which is allowed to flag a session as authenticated. Without this setting, all URL's are allowed to manipulate the authentication state- Default: (^/.*$)

3.8 Authentication and Authorization (Location)

Context: location

Key	Parameter	Description
MOD_BUT_LOGON_SERVER_URL	String	Defines its own login server URL within a "Location" directive. If set, it overwrites the GLOBAL_LOGON_SERVER_URL Default: not specified
MOD_BUT_LOGON_REQUIRED	yes, no	If set to yes within a Location directive, MOD_BUT will enforce an authenticated session If set to no, the URL within the Location is open for all and authentication is not enforced. Default: no

3.9 Service List Authorization

These are new configuration directives since version 2.0. The version 1.0 did not allow selectively access to backend systems based on the user's role after successful authentication. Once the user is authenticated, he or she is allowed to access any backend system. However – this concept is insufficient if the user of MOD_BUT exactly knows for what URL a use should have access granted and for which URL's access is denied. We are naming this concept as "service list authorization".

Since this version 2.0, MOD_BUT supports the concept of service lists. It must be turned on first and does only affect such URL's for which authentication is required. If the login application inserts a "special" service list authorization Set-Cookie header, the service list can be changed for the specific user.

Context: Virtual Host

Key	Parameter	Description
MOD_BUT_SERVICE_LIST_ENABLED	String	Turns the service list authorization on and off. Default: Off
MOD_BUT_SERVICE_LIST_COOKIE_NAME	String	Name of the service list authorization Set-Cookie header. Default: MOD_BUT_SERVICE_LIST

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 30   Date: Mar 8, 2006

Key	Parameter	Description
MOD_BUT_SERVICE_LIST_COOKIE_VALUE	String	Regular expressions for the URL's the user is authorized. This regular expression has a default value, which allowes "all URL's". If the login application sets another regular expression value, for example ("^/webapp/asl|^/webapp/bsl), the user is only authorized for the above URL's. Default: (^/.*$)
MOD_BUT_SERVICE_LIST_AUTH_ERROR_URL	String	This value configures the error page URL, if the user is authenticated but unauthorized for requesting a certain URL. Default: /mod_but/error/authorization_error.html

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 31   Date: Mar 8, 2006

4 Installing MOD_BUT

4.1 Introduction

This chapter introduces the steps we walked through while bringing the demo reverse proxy online. We start from the very beginning, where we compile our reverse-proxy from scratch. These instructions have been done on a Solaris 8.0 server.

4.2 Preparation

MOD_BUT uses standard and additional modules. If you want to follow these instructions, you need the following packages

- Newest apache 2.x source code
- Mod_replace source code
- MOD_BUT source code
- OpenSSL (recommended)

This setup guide goes through the following steps

Step	Link to Chapter	Description	Status
1	4.3	Disable TRACE within the Apache source code	Optional
2	4.4	Change Apache server banner in Apache source code	Optional
3	4.5	Enable mod_replace by adding mod_replace.c to the Apache source tree	Optional
4	4.6	Compile Apache without MOD_BUT	Required
5	4.7	Test your Apache without MOD_BUT	Required
6	4.8	Compiling MOD_BUT	Required
7	4.10	Sample configuration of http://www.but.ch/mod_but/	For your information
8	N/A	The login servlets are not part of mod_but. They are very simple servlets, which authenticates against the OpenLDAP directory. Once the user is authenticated, the login servlets sets the specific LOGON cookies and MOD_BUT will learn by these response headers whether the user is MOD_BUT-authenticated or not.	N/A[24]

---

[24] *The source of the login servlets is not a secret. If required, we can send it to you as a sample login application. But please note, the login servlets is a "hack". It is not designed for production.*

4.3 Disable "TRACE" in the Apache Source Code

Please note that disabling the HTTP method TRACE is not required for the properly running of MOD_BUT. But we urge you to disable TRACE either by removing the functionality from the code, or by mod_rewrite pattern for security reasons. We prefer the source code solution.

Edit $APACHE_SRC/modules/http/http_protocols.c
        remove the register_one_method(p, "TRACE", M_TRACE); definition.

Before

```
AP_DECLARE(void) ap_method_registry_init(apr_pool_t *p)
{
    methods_registry = apr_hash_make(p);
    apr_pool_cleanup_register(p, NULL,
                                ap_method_registry_destroy,
                                apr_pool_cleanup_null);

    /* put all the standard methods into the registry hash to ease the
       mapping operations between name and number */
    register_one_method(p, "GET", M_GET);
    register_one_method(p, "PUT", M_PUT);
    register_one_method(p, "POST", M_POST);
    register_one_method(p, "DELETE", M_DELETE);
    register_one_method(p, "CONNECT", M_CONNECT);
    register_one_method(p, "OPTIONS", M_OPTIONS);
    register_one_method(p, "TRACE", M_TRACE);
    register_one_method(p, "PATCH", M_PATCH);
    register_one_method(p, "PROPFIND", M_PROPFIND);
    register_one_method(p, "PROPPATCH", M_PROPPATCH);
    register_one_method(p, "MKCOL", M_MKCOL);
    register_one_method(p, "COPY", M_COPY);
    register_one_method(p, "MOVE", M_MOVE);
    register_one_method(p, "LOCK", M_LOCK);
    register_one_method(p, "UNLOCK", M_UNLOCK);
    register_one_method(p, "VERSION-CONTROL", M_VERSION_CONTROL);
    register_one_method(p, "CHECKOUT", M_CHECKOUT);
    register_one_method(p, "UNCHECKOUT", M_UNCHECKOUT);
    register_one_method(p, "CHECKIN", M_CHECKIN);
    register_one_method(p, "UPDATE", M_UPDATE);
    register_one_method(p, "LABEL", M_LABEL);
    register_one_method(p, "REPORT", M_REPORT);
    register_one_method(p, "MKWORKSPACE", M_MKWORKSPACE);
    register_one_method(p, "MKACTIVITY", M_MKACTIVITY);
    register_one_method(p, "BASELINE-CONTROL", M_BASELINE_CONTROL);
    register_one_method(p, "MERGE", M_MERGE);
}
```

After

```
AP_DECLARE(void) ap_method_registry_init(apr_pool_t *p)
{
    methods_registry = apr_hash_make(p);
    apr_pool_cleanup_register(p, NULL,
                                ap_method_registry_destroy,
                                apr_pool_cleanup_null);

    /* put all the standard methods into the registry hash to ease the
       mapping operations between name and number */
    register_one_method(p, "GET", M_GET);
    register_one_method(p, "PUT", M_PUT);
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 33   Date: Mar 8, 2006

```
    register_one_method(p, "POST", M_POST);
    register_one_method(p, "DELETE", M_DELETE);
    register_one_method(p, "CONNECT", M_CONNECT);
    register_one_method(p, "OPTIONS", M_OPTIONS);
    register_one_method(p, "PATCH", M_PATCH);
    register_one_method(p, "PROPFIND", M_PROPFIND);
    register_one_method(p, "PROPPATCH", M_PROPPATCH);
    register_one_method(p, "MKCOL", M_MKCOL);
    register_one_method(p, "COPY", M_COPY);
    register_one_method(p, "MOVE", M_MOVE);
    register_one_method(p, "LOCK", M_LOCK);
    register_one_method(p, "UNLOCK", M_UNLOCK);
    register_one_method(p, "VERSION-CONTROL", M_VERSION_CONTROL);
    register_one_method(p, "CHECKOUT", M_CHECKOUT);
    register_one_method(p, "UNCHECKOUT", M_UNCHECKOUT);
    register_one_method(p, "CHECKIN", M_CHECKIN);
    register_one_method(p, "UPDATE", M_UPDATE);
    register_one_method(p, "LABEL", M_LABEL);
    register_one_method(p, "REPORT", M_REPORT);
    register_one_method(p, "MKWORKSPACE", M_MKWORKSPACE);
    register_one_method(p, "MKACTIVITY", M_MKACTIVITY);
    register_one_method(p, "BASELINE-CONTROL", M_BASELINE_CONTROL);
    register_one_method(p, "MERGE", M_MERGE);
}
```

4.4 Hide Banner Info in the Apache Source Code

Please note that hiding Apache server banners is not required for the properly running of MOD_BUT but is advisable for security reasons. You could follow the instructions below, accept the Apache banners or hide them with mod_security.

Edit $APACHE_SRC/include/ap_release.h

Before modification (Original):

```
#define AP_SERVER_BASEVENDOR "Apache Software Foundation"
#define AP_SERVER_BASEPRODUCT "Apache"
#define AP_SERVER_MAJORVERSION "2"
#define AP_SERVER_MINORVERSION "0"
#define AP_SERVER_PATCHLEVEL "$"
#define AP_SERVER_MINORREVISION AP_SERVER_MAJORVERSION "." AP_SERVER_MINORVERSION
#define AP_SERVER_BASEREVISION  AP_SERVER_MINORREVISION "." AP_SERVER_PATCHLEVEL
#define AP_SERVER_BASEVERSION AP_SERVER_BASEPRODUCT "/" AP_SERVER_BASEREVISION
#define AP_SERVER_VERSION  AP_SERVER_BASEVERSION
```

After modification:

```
#define AP_SERVER_BASEVENDOR "BUT SOLUTIONS"
#define AP_SERVER_BASEPRODUCT "Microsoft IIS"
#define AP_SERVER_MAJORVERSION "2077"
#define AP_SERVER_MINORVERSION "8"
#define AP_SERVER_PATCHLEVEL "03"
#define AP_SERVER_MINORREVISION AP_SERVER_MAJORVERSION "." AP_SERVER_MINORVERSION
#define AP_SERVER_BASEREVISION  AP_SERVER_MINORREVISION "." AP_SERVER_PATCHLEVEL
#define AP_SERVER_BASEVERSION AP_SERVER_BASEPRODUCT "/" AP_SERVER_BASEREVISION
#define AP_SERVER_VERSION  AP_SERVER_BASEVERSION
```

4.5 Enable mod_replace

There is no better module designed to alter HTTP response bodies than mod_replace. It is a proprietary module (like MOD_BUT) but very powerful and fast.

You can use MOD_BUT without mod_replace. But if you want to alter URL directives from your backend system, mod_replace is a good choice.

```
cp mod_replace.c $APACHE_SRC/modules/filters/
```

Edit $APACHE_SRC/modules/filter/config.m4

Before modification (Original)

```
APACHE_MODULE(ext_filter, external filter module, , , most)
APACHE_MODULE(include, Server Side Includes, , , yes)
```

After modification:

```
APACHE_MODULE(ext_filter, external filter module, , , most)
APACHE_MODULE(replace, replace filter module, , , most)
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 35   Date: Mar 8, 2006

```
APACHE_MODULE(include, Server Side Includes, , , yes)
```

Run **autoconf** in $APACHE_SRC directory. Afterwards you will "see" the –config-replace switch of the ./configure script. You can test proper configuration of mod_replace by

./configure --help | grep replace

4.6 Compile your Reverse proxy (without MOD_BUT)

```
cd $APACHE_SRC
autoconf

./configure --prefix=/opt/applic/reverse_proxy/ \
--enable-so \
--enable-ssl \
--enable-rewrite \
--enable-replace \
--enable-proxy \
--enable-headers \
--enable-expires \
--enable-auth-digest \
--enable-unique-id \
--enable-log-forensic
```

Note: run autoconf after editing config.m4 (see one step before). Otherwise, mod_replace will not compile.

4.7 Install and Test

Now do the following

```
make
make install
```

Test your httpd.conf by

```
/opt/applic/reverse_proxy/bin/apachectrl –t
```

Start your Apache server manually

```
/opt/applic/reverse_proxy/bin/apachectrl start
```

If you have problems here, please use the standard Apache *readme* and *docs*. You will find more useful information at http://httpd.apache.org/

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 36   Date: Mar 8, 2006

4.8 Compilation MOD_BUT with Unix

The MOD_BUT package consists of the following components

```
e1@hakka:~/apache$ ls -al
-rw-r--r--  1 hobo csnc   516 2006-02-06 15:25 Makefile
-rw-r--r--  1 hobo csnc  6155 2006-02-03 13:33 mod_but_access.c
-rw-r--r--  1 hobo csnc  4305 2006-02-03 13:33 mod_but_authorization.c
-rw-r--r--  1 hobo csnc 39039 2006-02-07 09:55 mod_but.c
-rw-r--r--  1 hobo csnc  9673 2006-02-07 09:58 mod_but_config.c
-rw-r--r--  1 hobo csnc  8308 2006-02-03 13:32 mod_but_cookiestore.c
-rw-r--r--  1 hobo csnc   180 2006-02-02 11:20 mod_but.dep
-rw-r--r--  1 hobo csnc  5369 2006-02-02 11:20 mod_but.dsp
-rw-r--r--  1 hobo csnc 15106 2006-02-07 09:56 mod_but.h
-rw-r--r--  1 hobo csnc 10528 2006-02-02 11:20 mod_but.mak
-rw-r--r--  1 hobo csnc 11645 2006-02-07 10:24 mod_but_output_filter.c
-rw-r--r--  1 hobo csnc   986 2006-02-02 11:20 mod_but.rc
-rw-r--r--  1 hobo csnc  5691 2006-02-03 15:24 mod_but_request_filter.c
-rw-r--r--  1 hobo csnc 15795 2006-02-03 13:32 mod_but_session.c
-rw-r--r--  1 hobo csnc 17420 2006-02-03 13:31 mod_but_shm.c
```

Makefile

Please consult the documentations at http.apache.org, if you need further explanation of the APXS flags.

-c	=	compile
-i	=	install in $APACHE_SRC/modules
-a	=	configure LOAD directive into httpd.conf

```
###########################################
#
# mod_but Makefile V1.0 by BUT
#
###########################################

APXS=/opt/applic/httpd-2.0.55/bin/apxs
APXSFLAGS=-c -i -a -Wc,-O8 -Wc,-Wall
SRC=mod_but.c mod_but_access.c mod_but_request_filter.c mod_but_output_filter.c
mod_but_config.c mod_but_session.c mod_but_shm.c mod_but_cookiestore.c
mod_but_authorization.c

all: mod_but


mod_but: $(SRC)
        $(APXS) $(APXSFLAGS) $(SRC)

clean:
        rm -r *.la *.slo *.o  *.lo .libs
```

You can adapt the Makefile to meet your needs. Please configure APXS and APXSFLAGS.

Configuration directive	Description
APXS	Path to Apache apxs binary. In our example: /opt/applic/reverse_proxy/bin/apxs

Configuration directive	Description
APXSFLAGS -c -I -a	-c "compile as DSO module" -i "install into modules dir of http" -a "add LoadModule into httpd.conf"
APXSFLAGS -I	Include directory for Openssl.

Note: OpenSSL is required for future features I have planned to integrate. I will us the SSL-ID as improvement for the cookie-based session handling mechanism. It's some kind of mixed mode between cookies and the SSL-ID.

For the current release of MOD_BUT, OpenSSL is not required.

make

```
e1@hakka:~/apache$ make
hobo@h00k:~/mod_but/src$ date
Tue Feb  7 14:31:53 CET 2006
hobo@h00k:~/mod_but/src$ make
/opt/applic/httpd-2.0.55/bin/apxs -c -i -a -Wc,-O8 -Wc,-Wall mod_but.c mod_but_access.c mod_but_request_filter.c
mod_but_output_filter.c mod_but_config.c mod_but_session.c mod_but_shm.c mod_but_cookiestore.c mod_but_authorization.c
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o mod_but.lo
mod_but.c && touch mod_but.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_access.lo mod_but_access.c && touch mod_but_access.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_request_filter.lo mod_but_request_filter.c && touch mod_but_request_filter.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_output_filter.lo mod_but_output_filter.c && touch mod_but_output_filter.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_config.lo mod_but_config.c && touch mod_but_config.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_session.lo mod_but_session.c && touch mod_but_session.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o mod_but_shm.lo
mod_but_shm.c && touch mod_but_shm.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_cookiestore.lo mod_but_cookiestore.c && touch mod_but_cookiestore.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=compile gcc -prefer-pic -DAP_HAVE_DESIGNATED_INITIALIZER -DLINUX=2
-D_REENTRANT -D_XOPEN_SOURCE=500 -D_BSD_SOURCE -D_SVID_SOURCE -D_GNU_SOURCE -g -O2 -pthread -I/opt/applic/httpd-
2.0.55/include -I/opt/applic/httpd-2.0.55/include  -I/opt/applic/httpd-2.0.55/include  -O8 -Wall  -c -o
mod_but_authorization.lo mod_but_authorization.c && touch mod_but_authorization.slo
/opt/applic/httpd-2.0.55/build/libtool --silent --mode=link gcc -o mod_but.la  -rpath /opt/applic/httpd-2.0.55/modules -
module -avoid-version  mod_but_authorization.lo mod_but_cookiestore.lo mod_but_shm.lo mod_but_session.lo
mod_but_config.lo mod_but_output_filter.lo mod_but_request_filter.lo mod_but_access.lo mod_but.lo
/opt/applic/httpd-2.0.55/build/instdso.sh SH_LIBTOOL='/opt/applic/httpd-2.0.55/build/libtool' mod_but.la
/opt/applic/httpd-2.0.55/modules
/opt/applic/httpd-2.0.55/build/libtool --mode=install cp mod_but.la /opt/applic/httpd-2.0.55/modules/
cp .libs/mod_but.so /opt/applic/httpd-2.0.55/modules/mod_but.so
cp .libs/mod_but.lai /opt/applic/httpd-2.0.55/modules/mod_but.lai
cp .libs/mod_but.a /opt/applic/httpd-2.0.55/modules/mod_but.a
ranlib /opt/applic/httpd-2.0.55/modules/mod_but.a
chmod 644 /opt/applic/httpd-2.0.55/modules/mod_but.a
PATH="$PATH:/sbin" ldconfig -n /opt/applic/httpd-2.0.55/modules
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 38   Date: Mar 8, 2006

Additionaly, MOD_BUT has been successfully compiled under Sparc/Solaris8 and Sparc/Solaris10 using gcc.

4.9 Compilation MOD_BUT with Microsoft Windows

Task	Description
Download Apache Source Code	http://httpd.apache.org/download.cgi
Create your compilation environment	http://httpd.apache.org/docs/2.0/platform/win_compiling.html
Create directory structure in original apache source tree	Create a mod_but directory in $APACHE_SOURCE\modules
Copy mod_but files from mod_but.tar.gz to the apache source tree	Copy all data from mod_but.tar.gz -> mod_but directory into the Apache source tree
Configure mod_but in BaseAddr.ref	Edit $APACHE_SOURCE\modules\os\win32\BaseAddr.ref Configure a max size of 0x00300000 Example: mod_but.so 0x6F82000 0x00300000 Important!! Addition of 0x6F82000 + 0x00300000 MUST result into the value above the mod_but entry!
Configure Makefile.win	Edit $APACHE_SOURCE\Makefile.win Configure the mod_but snippets below.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 39   Date: Mar 8, 2006

Task	Description

```
...
!IF EXIST("srclib\openssl")
cd modules\ssl
$(MAKE) $(MAKEOPT) -f mod_ssl.mak CFG="mod_ssl - Win32
$(LONG)" RECURSE=0 $(CTARGET) .\$(LONG)\mod_ssl.so
cd ..\..
cd modules\mod_but
$(MAKE) $(MAKEOPT) -f mod_but.mak CFG="mod_but - Win32 $(LONG)"
RECURSE=0 $(CTARGET)
cd ..\..
cd support
$(MAKE) $(MAKEOPT) -f abs.mak CFG="abs - Win32 $(LONG)"
RECURSE=0 $(CTARGET)
cd ..
!ENDIF
...



...
!IF EXIST("srclib\openssl")
copy modules\ssl\$(LONG)\mod_ssl.$(src_so) "$(inst_so)" <.y
copy modules\mod_but\$(LONG)\mod_but.$(src_so) "$(inst_so)" <.y
$(quiet)copy srclib\openssl\$(SSLBIN)\openssl.$(src_exe) "$(inst_exe)" <.y
$(quiet)copy srclib\openssl\$(SSLBIN)\libeay32.$(src_dll)
"$(inst_dll)" <.y
$(quiet)copy srclib\openssl\$(SSLBIN)\ssleay32.$(src_dll)
"$(inst_dll)" <.y
copy support\$(LONG)\abs.$(src_exe) "$(inst_exe)\ab.$(src_exe)" <.y
!ELSE
copy support\$(LONG)\ab.$(src_exe) "$(inst_exe)" <.y
!ENDIF
...
```

Compilation	Please use the following howto: http://httpd.apache.org/docs/2.0/platform/win_compiling.html Only release-build will work! nmake /f Makefile.win _apacher

4.10 Sample Configuration MOD_BUT

The following configuration is used in http://www.but.ch/mod_but/. Please feel free to use it as an example:

```
##################################################
# Description:  Apache Configuration
# Author:       BUT
# Target:       VirtualHost www.but.ch on 80.254.178.109
# Date:         September 2005
# Contact:      e1@but.ch
##################################################


<VirtualHost 80.254.178.109:80>

#############################################
#       GLOBAL CONFIG
#############################################
```

```
    ServerAdmin         webmaster@but.ch
    DocumentRoot        "/opt/applic/www/www.but.ch/htdocs"
    ServerName          www.but.ch
#   AddDefaultCharset UTF-8

    ErrorLog /var/virtmp/logs/www.but.ch/error_www.but.ch.log
    CustomLog /var/virtmp/logs/www.but.ch/access_www.but.ch.log common
    CustomLog /var/virtmp/logs/www.but.ch/combined_www.but.ch.log combined
    CustomLog /var/virtmp/logs/www.but.ch/referer_www.but.ch.log referer


#############################################
#     GLOBAL CONFIG
#############################################
    #ForensicLog /var/virtmp/logs/www.but.ch/www.but.ch.forensic.log


#############################################
#     MOD_PROXY
#############################################

    ProxyVia    Off

#############################################
#     MOD_HEADER
#############################################

    RequestHeader append SSL_CIPHER "%{SSL_CIPHER}e"
    Header set Cache-Control no-cache
    Header add Cache-Control no-store
    Header set Pragma no-cache


#############################################
#     MOD_REWRITE
#############################################
    RewriteEngine On
    RewriteRule         ^mod_but$  mod_but/  [P]
    RewriteRule         ^/(.*)                  /root/$1        [P]




#############################################
#     MOD_SECURITY
#############################################
    SecFilterEngine On
    SecAuditEngine On
    SecFilterScanPost On
    SecFilterScanOutput On
    SecFilterCheckUnicodeEncoding On
    SecFilterCheckURLEncoding On
    # SecFilterCheckCookieFormat On
    SecFilterForceByteRange 0 255
    #SecServerSignature "Secure But Webserver"
    SecFilterDebugLog           logs/www.but.ch.modsec_debug.log
    SecFilterDebugLevel         4
    SecAuditLog                 logs/www.but.ch.modsec_audit.log

    Include          conf/mod_security.conf

#############################################
#     MOD_UNIQ
#############################################
    RequestHeader append UNIQUE_ID "%{UNIQUE_ID}e"

#############################################
#     MOD_BUT
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 41   Date: Mar 8, 2006

```
##############################################
    MOD_BUT_ENABLED                            On
    MOD_BUT_CLIENT_REFUSES_COOKIES_URL         /mod_but/error/refused_cookies.html
    MOD_BUT_COOKIE_NAME                        E1HTTP
    MOD_BUT_COOKIE_DOMAIN                       but.ch
    MOD_BUT_COOKIE_PATH                        /
#   MOD_BUT_COOKIE_EXPIRATION                              "3-Jan-2006 00:00:01 GMT"
#   MOD_BUT_COOKIE_SECURE                secure
    MOD_BUT_COOKIE_HTTPONLY           HttpOnly

    MOD_BUT_SESSION_FREE_URL          "(^/$)|(^/robots.txt)|(.*but.css)|(.*.gif)|
(^/_shared/)|(^/cgi-bin/.*)|(^/mod_but/error/)|(^/root/error/)|(^/renew/)|
(^/favicon.ico)|(^/public/)|(^/index.*)"

    MOD_BUT_SESSION_TIMEOUT                    14400
    MOD_BUT_SESSION_TIMEOUT_URL                /mod_but/error/session_expired.html
    MOD_BUT_SESSION_RENEW_URL                  "(^/renew/)"
    MOD_BUT_SESSION_INACTIVITY_TIMEOUT         3600
    MOD_BUT_SESSION_INACTIVITY_TIMEOUT_URL     /mod_but/error/session_inactivity.html
    MOD_BUT_SESSION_HACKING_ATTEMPT_URL        /mod_but/error/session_invalid.html
    MOD_BUT_SESSION_TIMEOUT_HISTORY            86400
    MOD_BUT_ALL_SHM_SPACE_USED_URL             /mod_but/error/session_shm_used.html
    MOD_BUT_SESSION_DESTROY                    "(^/logout.*)"
    MOD_BUT_SESSION_DESTROY_URL                /mod_but/error/session_destroy.html
    MOD_BUT_AUTHORIZATION_ENABLED              On
    MOD_BUT_GLOBAL_LOGON_SERVER_URL            /mod_but/login.html
    MOD_BUT_GLOBAL_LOGON_AUTH_COOKIE_NAME      LOGON
    MOD_BUT_GLOBAL_LOGON_AUTH_COOKIE_VALUE     ok
    MOD_BUT_SESSION_STORE_FREE_COOKIES         "(^language=.*)|(^trustme=.*)"
    MOD_BUT_SERVICE_LIST_ENABLED        On
    MOD_BUT_AUTHORIZED_LOGON_URL        "(^/webapp/login/.*)"




##############################################
#       ROOT GOES TO BACKEND
##############################################




    <Location /webapp>
            ProxyPass                          http://127.0.0.1:35080/
            ProxyPassReverse                   http://www.but.ch/webapp/
            MOD_BUT_LOGON_REQUIRED  no
    </Location>

    <Location /webapp/but>
            ProxyPass                          http://127.0.0.1:35080/but/
            ProxyPassReverse                   http://www.but.ch/webapp/but/
            MOD_BUT_LOGON_REQUIRED  yes
    </Location>

    <Location /mod_but>
            ProxyPass                          http://127.0.0.1:20060/mod_but/
            ProxyPassReverse                   http://www.but.ch/mod_but/
            MOD_BUT_LOGON_REQUIRED  no
    </Location>

    <Location /mod_but/protected>
            ProxyPass                          http://127.0.0.1:20060/mod_but/protected/
            ProxyPassReverse                   http://www.but.ch/mod_but/protected/
            MOD_BUT_LOGON_REQUIRED  yes
    </Location>

    <Location /loginok>
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch   www.csnc.ch

Page: 42   Date: Mar 8, 2006

```
        ProxyPass                        http://127.0.0.1:20060/mod_but/
        ProxyPassReverse                 http://www.but.ch/loginok/
        MOD_BUT_LOGON_REQUIRED  yes
</Location>


<Location /root>
        ProxyPass                        http://127.0.0.1:20060/
        ProxyPassReverse                 http://www.but.ch/root/
        MOD_BUT_LOGON_REQUIRED  no
</Location>


Include        conf/error.conf

</VirtualHost>
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.   +41 55-214 41 60
Fax   +41 55-214 41 61
team@csnc.ch www.csnc.ch

Page: 43   Date: Mar 8, 2006