UNEP

CBD

Convention on Biological Diversity

Distr.
GENERAL

UNEP/CBD/BS/COP-MOP/4/INF/19
2 May 2008

ENGLISH ONLY

CONFERENCE OF THE PARTIES TO THE CONVENTION ON BIOLOGICAL DIVERSITY SERVING AS THE MEETING OF THE PARTIES TO THE CARTAGENA PROTOCOL ON BIOSAFETY
Fourth meeting
Bonn, 12-16 May 2008
Item 5 of the provisional agenda*

REPORT OF EXTERNAL SECURITY AUDIT OF THE CENTRAL PORTAL OF THE BIOSAFETY CLEARING-HOUSE AND ITS INFRASTRUCTURE

Note by the Executive Secretary

I. INTRODUCTION

1. In its decision BS-III/2, the Conference of the Parties serving as the meeting of the Parties to the Cartagena Protocol on Biosafety (COP-MOP) requested the Executive Secretary, with a view to ensuring value for money, to undertake an external security audit of the Central Portal and its infrastructure and called upon Parties, Governments and other donors to provide the required financial resources.

2. Thanks to a generous contribution from the Swiss Government, this security audit was undertaken in April 2008. This was done in order to ensure full security of the information in the BCH and to minimize any chance of its loss.

3. This document contains the report of the security audit and a short response from the Secretariat.

II. SECRETARIAT'S RESPONSE TO THE SECURITY AUDIT

4. The Secretariat welcomes the security audit conducted by ESI Technologies, its recommendations and conclusions.

5. The executive summary of the security assessment stipulated: "Although no critical vulnerability has been found among all the elements analysed, some points require special attention."

6. In this response, the Secretariat wishes to provide answers to those points in the audit report marked as "requiring attention" and highlight the necessary actions to be taken.

Entry validation

7. The following paragraphs refer to remarks contained in section 3.1.1 and recommendations 6.4 and 6.6 of the audit report

* UNEP/CBD/BS/COP-MOP/4/1.

/…

8. The BCH performs data validation on the server side. Although the client side could provide better user experience and convenience (e.g. no page refresh), this would not provide any benefit in terms of security.

9. The BCH supports NULL value by design (e.g. a page without query string usually automatically falls back to search mode).

10. The BCH can properly handle data of virtually any length (i.e. only limited by memory available). Current safeguards limit POST DATA to 2MB. Being built on Microsoft .NET platform, the BCH is inherently foolproof against buffer overflow. Furthermore, the Secretariat does not believe that limiting the POST DATA size would significantly limit a hypothetical injection and may even significantly interfere with user experience.

11. The BCH properly handles the so called "dangerous characters" by escaping them, on a systematic basis, using the proper escape methods. The Secretariat considers that blocking those characters would not provide any security benefit and would definitely interfere with user experience (e.g. a risk assessment by using the character "less than" (i.e. "<") in its description).

12. The Secretariat took note of the auditor's comments and recommendation regarding cross-side scripting and, accordingly, made the appropriate changes to the potential URL concerned.

Page caching over SSL

13. The following paragraph refers to remarks contained in section 3.1.2 and recommendation 6.3 of the audit report.

14. On this particular issue, the Secretariat had to strike a balance between security and performance. In fact, a large number of BCH users is using very low bandwidth (less than 56 Kb/s). It should be noted that the cached information cannot grant unauthorized access to the BCH by any means. Accordingly, the Secretariat believes that the very negligible risks posed by caching over HTTPS are overcome by its benefits. In fact, the BCH actively contributes to page caching by systematically providing the date of last update and the date of expiry to its pages.

Password auto-complete

15. The following paragraph refers to remarks contained in section 3.1.3 and recommendation 6.2 of the audit report.

16. The Secretariat took note of the auditor's recommendation and, accordingly, made the appropriate changes to prevent any Auto-Complete in password fields.

Secure ciphering methods

17. The following paragraph refers to remarks contained in section 3.1.4 and recommendation 6.1 of the audit report.

18. The Secretariat took note of the auditor's recommendation and, accordingly, made the appropriate actions to disable SSL version 2.0 and force the use of SSL 3.0 or TLS 1.0.

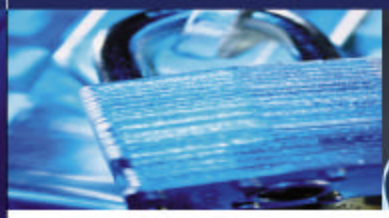
URL backtracking

19. The following paragraph refers to remarks contained in section 3.1.6 of the audit report.

20. The Secretariat took note of the auditors' recommendation and, accordingly, a validation hash will be added to all pages using URL backtracking to avoid any QUERY STRING/POST DATA crafting. The Secretariat will implement the necessary improvements in the next weeks/months as this issue does not pose any immediate risk to the security of the BCH.

ESI TECHNOLOGIES

Know-How



Convention on Biological Diversity

Biosafety Clearing-house security assessment

Prepared for : SCBD

Prepared by : ESI Techonologies

Date : April 29, 2008

Version : 1.0

ESI Technologies inc.
Montreal and surrounding areas:
(514) 745-3311
Across Canada:
1 800 260-3311
info@esitechnologies.com
www.esitechnologies.com

INDEX

1. Executive summary

The objective of this report is to answer the following question : Are *Biosafety clearing-house's* equipments and systems vulnerable to any damageable attacks from the Internet ? If so, wich is *Biosafety clearing-house* vulnerability level ?

Although no critical vulnerability has been found among all the elements analysed, some points require special attention. Details about those points, and lists of recommendations, are compiled in this document.

To help achieve this goal we have verified the eventuality of being able :

- to exploit functions to grant user privileges;
- to gain access of the operating systems of the computers of Biosafety clearing-house;
- to modify websites configuration;
- to affect integrity of the databases or to have an impact on availability of systems;
- to find out security flaws exposing Biosafety clearing-house websites to certain risks;
- to ensure that the security level of the secured connections is adequate and optimal.

We analyzed the different vectors that could give us information, from an attacker standpoint, trying to penetrate Biosafety clearing-house application. The depth of each area of test was delimited by the time period allowed to action each of them respectively.

The following pages contain information concerning the tests we have conducted from April 22, to April 28, 2008.

1.1. Summary of elements to monitor

This is a list of the three (3) most important elements that globally require attention of Biosafety clearing-house in the short term:

1.1.1: Review cryptographic methods used

The following cryptographic algorithms are no longer supported because of known vulnerabilities:

- Block cipher* : DES, RC2
- Stream cipher *: RC4
- Hach function : MD5

*with 40 or 56 bits key length

1.1.2 : Disable auto-complete

Auto-complete function should be disable in order to prevent sensitive information to be recorded potentially offering a fraudulent user to copy them.

1.1.3 : Avoid using File Transfer Protocol

File Transfer Protocol (FTP) should no longer be supported because all FTP information, including login information are transmitted in plain text.

2. Test parameters

2.1. Risks management

We assumed that during the tests, no changes were made to the applications of Biosafety clearing-house. We also took in consideration that all the services offered by the company were up and running at the time of the tests and that Biosafety clearing-house had a backup copy of all the data exposed to the analysis.

Risk level scale	
Level	**Description**
4	**Critical risk :** The presence of a flaw has been confirmed and is currently operated or readily exploitable by attackers on the Internet. Without immediate attention, reputation and business operations will be compromised.
3	**High risk :** A faulty behavior is confirmed. Exploitation of this vulnerability does not ask for very high technical abilities and / or material.
2	**Medium risk :** A faulty behavior is to confirm. Configuration is non optimal and shuold be improved. Nethertheless, this have no immediate impact on the system security.
1	**Low risk :** Presence of a flaw could not be determined with certainty, however, several signs point out that the system could be vulnerable so that more in-depth exploration should be made to confirm the existence of this vulnerability.
0	**Negligeable risk** : In the deadlines imposed by the mandate, no risk was found, and the system is well managed. It is important to note, however that the total absence of risk is impossible.

2.2. Evaluation of safety practices

To ensure the reliability of a Web application, it is convenient to adopt safety practices in the management of settings, access control, session, buffers and errors.

The following conventions will be used to evaluate safety practices:

- = red « X » intended for critical conditions requiring attention.
- = yellow « ! » in a triangle intended for points having to be examined closer.
- = « i » in a blue circle indicating interesting information.
- = a green bullet indicating a satisfying condition or information.

2.3. Technological environment

Biosafety clearing-house Website was tested from this following IP addresses :
209.41.143.68 et 209.41.143.101

This browser was used :
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12

2.4. Given Informations

DNS name	http://bch.cbd.int/
IP address	***69.90.183.250***

2.5. Tools nomenclature

This is the list of some of the tools used for this mandate :

Nessus : an automated vulnerability scanning software .

Nmap : an automated scanning tool for port scanning and security audit.

Netcat : Generate UDP and TCP connections.

Hping2 : A network scanner that uses spoofed source address packets to test firewall rules and to perform advanced TCP/IP related attacks

SamSpade : Software tools for tracking spam.

Nikto : A web server scanner which performs tests against web servers for multiple items potentially dangerous files/CGIs.

Paros proxy : security tool for web application vulnerability assessment.

Traceroute : network tool for tracking Ip packets.

Ping : used to test whether a particular host is reachable across an IP network.

Nbtstat : allows a refresh of the NetBIOS name cache and the names registered with Windows

Internet Name Service (WINS). Nbtstat is designed to help troubleshoot NetBIOS name resolution problems.

Nbtdump : Tool recognition of MS-Windows hosts that allows you to obtain the list of shares and files available.

RPCDump : Tool recognition of a MS-Windows local host that allows you to provide lists of references between in place tools and used ports.

Brutus : Password recovering tool covering different services such as HTTP, POP3, FTP, SMB et Telnet.

Dig : an advanced DNS query tool.

Nslookup : Tool used to find various details relating to DNS including IP addresses of a particular computer.

Hfnetchk : A tool that enables an administrator to check the patch status of all the machines in a network from a central location.

Firewalk : is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass.

Achilles : Web Proxy used for requests interception and alteration.

Sid2user : Enumeration tool to list MS-Windows system users.

Srvinfo : Command line tool displaying remote host informations.

Tscrack : brute force attack software against remote desktop MS-Windows service.

Pwdump : Get passwords of a MS Windows host from remote or local location.

HTTrack : website mirror utility that allow downloading an entire website.

Stunnel : an SSL encryption wrapper between remote client and local (inetd-startable) or remote server.

Curl : a command line tool for transferring files with URL syntax, supporting FTP, FTPS, HTTP, HTTPS, SCP, SFTP, TFTP, Telnet, DIC, File and LDAP.

3. Application tests results

Here's a summary of what we observed during the tests. You will find more details about those results in section 4 and 5. You will also find suggested remarks and recommendations that may help improve the security level of your application in section 6.

Categories	Remarks	Risk level[1]
Entry validation	All data types are accepted with no validation for the most pages. Furthermore, it doesn't seem client side data validation is performed.	1
Access control	Sensitive pages seem to be cacheable and password Auto-Complete might not deactivated. See Section 6.2.	2
Session management	Deprecated SSL version is used. User data seems to be partially ciphered. See Section 6.1.	2
Cross-site scripting (XSS)	Even though no cross-site scripting test succeeded in the entry fields the server seems to be exposed to this vulnerabilities. See Section 6.6.	2
Buffer overflow	None of the tests executed left the server or application left it in an unsafe state.	0
Command injection	The remote host could probably be vulnerable to command injection because dangerous characters are tolerated. See sections 6.4.	2
Error management	Error management seems to be safe.	0
Server analysis	Automated test shown that the ASP.NET web application seems to have tracing function enabled. However the IIS version used (version 6.0) have been retorted not vulnerable to this security flaw. See Section 5.2.	1
	Average risk level[2]	**1.25 / 4**

1 Numerical value of the risk level. See *Risk level scale* in section 2.1.

2 Global risk level for the entire tests. See *Risk level scale* in section 2.1.

3.1. Results of Biosafety clearing-house application analysis

This is the tests results for Biosafety clearing-house's web application.

3.1.1. Parameter requirements

From the application analysis we have been able to distinguish between three (3) groups of form parameter requirements result tests. Then results are presented grouped by URL.

Affected URLs

http://bch.cbd.int/protocol/meetings/
http://bch.cbd.int/protocol/notifications/
http://bch.cbd.int/protocol/decisions/
http://bch.cbd.int/database/resources/
http://bch.cbd.int/database/organizations/
http://bch.cbd.int/database/organisms/
http://bch.cbd.int/database/laws/
http://bch.cbd.int/database/experts/
http://bch.cbd.int/database/decisions/
http://bch.cbd.int/database/contacts/
http://bch.cbd.int/database/activities/
http://bch.cbd.int/database/bibliographic-references/
http://bch.cbd.int/resources/thesaurus/
https://bch.cbd.int/user/rate.shtml?pid=5804&key=223cccd92efdba2433570e2f2a93ed6e&returnurl=%2
(Same remarks for all “Rate this page” pages)

Results

Test	*Results*	*Remark*
Data types (*string*, *int*, *real*, etc.)		All data types are accepted.
Minimum and maximum length		No length limit checked. Fields fulfilled with very long length data generate a processing error.
Null value permitted		Null values are permitted.
Parameters required		Use of drop down lists when possible.
Specific values control		No specific value used apart from drop down lists.
Expression models used		Specific data format are imposed when necessary.
Dangerous characters blocking		All dangerous characters are accepted in all fields. See Section 6.6.
Replacement character used		The dangerous characters are not displayed although accepted.

Free value		Free value tolerated.

Affected URLs

http://bch.cbd.int/database/
http://bch.cbd.int/database/record.shtml?id=7517

Results

Test	*Results*	*Remark*
Data types (*string*, *int*, *real*, etc.)		Only integer values are accepted.
Minimum and maximum length		Length limit doesn't seem to be checked. It seems only the value transmitted to the server is checked. A “Record ID is invalid” error message is displayed when an invalid ID is submitted. Very long length data generate a processing error.
Null value permitted		Null values are permitted.
Parameters required		Use of drop down lists when necessary.
Specific values control		Adequate control.
Expression models used		Specific data format are imposed when possible.
Dangerous characters blocking		All dangerous characters are accepted in all fields.
Replacement character used		The dangerous characters are not displayed although accepted.
Free value		Free value tolerated.

URL affected

https://bch.cbd.int/user/signin.shtml?returnurl=%2f
https://bch.cbd.int/member/signup/general.shtml?returnurl=%2fdatabase%2frecord.shtml%3fid%3d11123

Results

Test	*Results*	*Remark*
Data types (*string*, *int*, *real*, etc.)		Any data type accepted.

Minimum and maximum length		Length limit doesn't seem to be checked.
Null value permitted		Null values are checked. An error message indicate required fields.
Parameters required		Required fields are checked.
Specific values control		Email address format is checked but it seems that you don't check if it is an existing one.
Expression models used		Specific data format specified by a message.
Dangerous characters blocking		All dangerous characters are accepted in all fields. See Section 5.1.3.
Replacement character used		The dangerous characters are not displayed although accepted.
Free value		Free value tolerated.

Miscellaneous

During analysis, some features have been found unavailable. Here are the URLs the affected services :

Search Roster of Experts :
http://bch.cbd.int/roster/experts.shtml

Search Reports on Biosafety Expert Assignments :
http://bch.cbd.int/roster/status/reportsonassignments.shtml

Sign Up for a BCH Account :
https://bch.cbd.int/member/signup/start.shtml

3.1.2. Access control

Test	*Results*	*Remark*
Identification made by cookies	---	Not applicable.
Files permissions	---	
Page cacheable		Caching seems to be activated on part of the sensitive pages. See Section 6.3.
Unauthenticated access		Unauthorized access hasn't been gained although it might seem possible because sensitive pages seem to be cacheable. See Sections 6.3.

Attacks on HTTP headers (« Referer » or « User-Agent »)	---	Not applicable.
Backdoors	✅	No backdoors discovered.
« Auto-Complete » function	❌	Password Auto-Complete do not seem to be deactivated. Refer to Section 6.2.

3.1.3. Session management

Test	*Results*	*Remark*
ID protected by SSL	❌	SSL version 2.0 activated. See Section 6.1.
Number of ID possibilities	❌	Low ciphers length. See Section 6.1.
Hidden tags used	---	Not applicable.
Brute force Password attack	✅	No password was discovered by brute force attack during tests.
Session information in cookies	---	Not applicable.
Session closing during inactivity	---	Not applicable.
Long session closing	---	Not applicable.
Errors in session closing	---	Not applicable.
Use of HTTP « GET » requests	✅	POST method used to transmit Record IDs.

3.1.4. Cross site-scripting (XSS)

Test	*Results*	*Remark*
Dangerous characters allowed (, >, <, (,), #, &,)	❌	All dangerous characters are allowed. No validation seems to be made on the client side.
Dynamic pages printing or using client informations.	✅	Any data type sent by the client is accepted but not displayed.
Scripting tests	⚠	None of the scripting tests succeeded but it mau still be vulnerable to Cross-site Scripting (XSS). See Section 6.4.

3.1.5. Buffer overflow

Test	Results	Remark
Request length control	✔	Long length requests seem to be well handled. Only an Error message is displayed. See Section 8.3.

3.1.6. Command injection

Test	Results	Remark
URL backtracking	✘	It is possible to navigate the URLs. Even in the pages source code the URL backtracking is used. See Sections 6.4.
SQL injection	✔	No SQL Injection command succeeded.

3.1.7. Error management

Test	Results	Remark
Printed error messages	✔	No information about the remote host displayed. See Section 8.3.
Failure method safe	✔	No test allowed us to leave the application in unsafe state.
HTTP errors, others	✔	See Section 4 and Section 8.3.

4. Hyperlink analysis

Broken links could lead visitors outside of the domain name controlled by the SCBD. Fraudsters could get control of the URL to which the bad link is pointing and pretend being the Biosafety Clearing-house application to extirpate confidential information from the users. Users won't notice they got out of the Biosafety Clearing-house website since they followed a legitimate link, and the TRUST they have in your application will be transferred to the fraudster's website making them very vulnerable. Here are some of the broken links. A comprehensive list could be found in the automated scan result on the CD-ROM.

Error code	*Relative informations*	
400 (Bad request)	**Link**	http://bch.cbd.int/database/record.shtml?id=15417
	Link text	Vector Tobacco Homepage
	Target	http://www.vectortobacco.com/
403 (Forbidden)	**Link**	http://bch.cbd.int/thesaurus/term.aspx?termid=444
	Link text	http://en.wikipedia.org/wiki/Agrobacterium_tumefa
	Target	http://en.wikipedia.org/wiki/Agrobacterium_tumefaciens
404 (Unreachable)	**Link**	http://bch.cbd.int/about/news/
	Link text	About this site
	Target	http://bch.cbd.int/about/about/
	Link	http://bch.cbd.int/about/news/
	Link text	Modalities of Operation
	Target	http://bch.cbd.int/about/about/modalities.shtml
	Link	http://bch.cbd.int/about/news/
	Link text	Biosafety Protocol website
	Target	http://bch.cbd.int/about/about/protocol.shtml
	Link	http://bch.cbd.int/resources/sitemap.shtml
	Link text	Clearing-house mechanism
	Target	http://bch.cbd.int/about/chm.shtml
	Link	http://bch.cbd.int/about/news/
	Link text	Competent National Authorities
	Target	http://bch.cbd.int/about/database/search.aspx
Others	**Link**	http://bch.cbd.int/about/news/

	Link text	Help
	Target	http://bch.cbd.int/about/help/
	Additional remark	Server message : The system cannot find the file specified.

5. Biosafety clearing-house's Web server analysis

5.1. Vulnerabilities discovered on the server

This test's objective is to search for potential vulnerability of the Web server hosting the application. Analysis will be performed in order to check whether the remote machine has a satisfactory security level and to highlight any problems along with solutions to correct them if any.

Maximum risk level	**Medium**	
DNS name	*http://bch.cbd.int/*	
IP address	***69.90.183.250***	
Opened TCP Ports	21	FTP
	80	HTTP (Microsoft-IIS/6.0)
	443	HTTPS (SSL version 2)
Opened UDP Ports	---	No UDP port discovered
ICMP Echo-Request	The remote host reply to ICMP ping request	
Operating System	OS scan wasn't able to find exact OS matches	
Miscellaneous informations	None.	

Detected vulnerabilities count	**Negligeable**	**Low**	**Medium**	**High**	**Critical**
	0	1	2	0	0

5.1.1. Port 443 : Deprecate SSL protocol usage

Risk : **Medium**

The remote service accepts connections encrypted using SSL version 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker might be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

The list of the ciphering algorithms used by the server is presented here after :

Force	OpenSSL Name	Description
Weak security	EXP-RC2-CBC-MD5	Key exchange=RSA(512); Authentication=RSA Encryption=RC2(40) ; MAC=MD5 export
	EXP-RC4-MD5	Key exchange=RSA(512) ; Authentication=RSA Encryption=RC4(40) ; MAC=MD5 export SSLv3
	EXP1024-DES-CBC-SHA	Key Exchange=RSA (EXPORT - 1024); Authentication=RSA; Encryption=DES(56); MAC= SHA1
	EXP1024-RC4-SHA	Key Exchange=RSA (EXPORT - 1024); Authentication=RSA; Encryption=RC4(56); MAC=MD5
	DES-CBC-SHA	Key Exchange=RSA; Authentication=RSA; Encryption=DES(56); MAC=SHA1
Strong security	RC4-MD5	Key Exchange=RSA; Authentication=RSA; Encryption=RC4(128); MAC=MD5
	RC4-SHA	Key Exchange=RSA; Authentication=RSA; Encryption=RC4(128); MAC=SHA1
	DES-CBC3-SHA	Key Exchange=RSA; Authentication=RSA; Encryption=3DES(128); MAC=SHA1

5.1.2. Port 21 : FTP port opened

Risk : **Medium**

The remote host seems to have an FTP server running on port 21. Whenever a user opens up a regular FTP session, the entire transmission made between the host and the user is sent in plain text. Anyone who has the ability to snoop on the network packets might be able to read the data, including the password information. If a fraudulent user could login, he could have the opportunity to compromise the system.

5.1.3. Port 80 : HTTP Trace enabled

Risk : **Low**

The web server seems to have application tracing enabled. This would allow an attacker to view the last 50 web requests made to the server, including sensitive information like Session ID values and the physical path to the requested file. However manual attempts to

exploit this potential vulnerability did not succeeded. Furthermore, it has been reported that IIS version 6.0 does not seem to be vulnerable to this exploit. Refer to the following link for more details: http://www.aqtronix.com/Advisories/AQ-2003-02.txt.

6. General recommendations

The recommendations objectives are aiming at strengthening security level of Biosafety clearing-house. More specifically, these recommendations are aimed at improving the protection of confidentiality, integrity and availability of information systems within Biosafety clearing-house.

The following recommendations are presented in descendant order: critical elements first then negligible ones. However, the overall is important.

6.1. Use only highly secure ciphering methods

We recommend using SSLv3 or TLSv1. More specifically, cryptography for these mechanisms are adequate and should be the only ones used:

For SSLv3 :

- Block cipher encryption : 3DES (with a key of 168-bit), IDEA (with a key 128 bits);
- Data flow encryption : RC4 (with a 128-bit key);
- HASH (FOOTPRINT): SHA1.

For TLSv1 :

- Block cipher encryption : 3DES (with a key of 168 bits), AES (with a key 128 or 256-bit), IDEA (with a 128-bit key);
- Data flow encryption : RC4 (with a 128-bit key);
- HASH (FOOTPRINT): SHA1.

6.2. Password auto-complete in browser

AUTOCOMPLETE attribute should be disabled in HTML FORM/INPUT element containing password type input to prevent them to be recorded. Passwords may be stored locally in browsers and retrieved. In the pages, the following fields of type “password”, the auto-complete function has not been disabled:

URL	https://bch.cbd.int/user/signin.shtml?returnurl=%2fmanagementcentre%2fdefault.shtml
Form field	<input name="ctl10$ctl00$ctl05$ctl00$CPassword" type="password" id= "ctl10_ctl00_ctl05_ctl00_CPassword" style="width:180px" />

URL	https://bchtraining.cbd.int/member/training-signin.aspx?returnurl=%2fdefault.shtml
Form field	<input name="CPassword" type="password" id="CPassword" style="width:180px;" />

Turn off AUTOCOMPLETE attributes in form or individual input elements containing password using AUTOCOMPLETE='OFF' like this:

```
<input name="CPassword" type="password" id="CPassword" style="width:180px;"
        AUTOCOMPLETE='OFF' />
```

6.3. Make sure Secure page browser cache is deactivated

It seems that secure page might be cached in browser because cache control does not seem to be set in HTTP header nor HTML header. Hence, sensitive content, such as session information and security controls included in the applications, might be recovered from browser storage. That information might be used to access the applications without having to get through the authentication process.

The URLs that seem to be vulnerable are the following:

https://bch.cbd.int/user/signin.shtml?returnurl=%2fmanagementcentre%2fdefault.shtml
https://bch.cbd.int/resources/thesaurus/default.shtml
https://bch.cbd.int/resources/solutions/default.shtml
https://bch.cbd.int/resources/glossary/default.shtml
https://bch.cbd.int/resources/thesaurus/
https://bch.cbd.int/resources/solutions/
https://bch.cbd.int/resources/sitemap.shtml
https://bch.cbd.int/resources/glossary/
https://bch.cbd.int/resources/mailinglist.shtml
https://bch.cbd.int/resources/downloads.shtml
https://bch.cbd.int/resources/commonformats.shtml
https://bch.cbd.int/protocol/text/default.shtml
https://bch.cbd.int/protocol/reporting/default.shtml
https://bch.cbd.int/protocol/parties/default.shtml
https://bch.cbd.int/protocol/notifications/default.shtml
https://bch.cbd.int/protocol/meetings/default.shtml
https://bch.cbd.int/protocol/decisions/default.shtml
https://bch.cbd.int/protocol/text/
https://bch.cbd.int/protocol/reporting/
https://bch.cbd.int/protocol/parties/
https://bch.cbd.int/protocol/notifications/
https://bch.cbd.int/protocol/meetings/
https://bch.cbd.int/protocol/decisions/
https://bch.cbd.int/onlineconferences/default.shtml
https://bch.cbd.int/member/signin.aspx?returnurl=%2fmanagementcentre%2fdefault.shtml
https://bch.cbd.int/help/training-modules/default.shtml
https://bch.cbd.int/help/interoperability/webservice3/default.shtml
https://bch.cbd.int/help/interoperability/webservice3/
https://bch.cbd.int/help/training-modules/

https://bch.cbd.int/help/faq.shtml
https://bch.cbd.int/help/error-404.shtml?aspxerrorpath=/images/splash/gmoam.gif
https://bch.cbd.int/help/error404.aspx?aspxerrorpath=/images/splash/gmoam.gif
https://bch.cbd.int/database/resources/default.shtml
https://bch.cbd.int/database/organizations/default.shtml
https://bch.cbd.int/database/organisms/uniqueidentifiers/default.shtml
https://bch.cbd.int/database/organisms/genes/default.shtml
https://bch.cbd.int/database/organisms/uniqueidentifiers/
https://bch.cbd.int/database/organisms/genes/
https://bch.cbd.int/database/organisms/organismslist.shtml
https://bch.cbd.int/database/organisms/default.shtml
https://bch.cbd.int/database/laws/default.shtml
https://bch.cbd.int/database/experts/default.shtml
https://bch.cbd.int/database/decisions/default.shtml
https://bch.cbd.int/database/contacts/focalpoints.shtml
https://bch.cbd.int/database/contacts/default.shtml
https://bch.cbd.int/database/bibliographic-references/default.shtml
https://bch.cbd.int/database/activities/default.shtml
https://bch.cbd.int/database/resources/
https://bch.cbd.int/database/organizations/
https://bch.cbd.int/database/organisms/
https://bch.cbd.int/database/laws/
https://bch.cbd.int/database/experts/
https://bch.cbd.int/database/decisions/
https://bch.cbd.int/database/contacts/
https://bch.cbd.int/database/bibliographic-references/
https://bch.cbd.int/database/activities/
https://bch.cbd.int/common/style.css
https://bch.cbd.int/common/common.css
https://bch.cbd.int/cms/web/cms.css
https://bch.cbd.int/bch/ui/templates/scripts/bchdropmenu.js
https://bch.cbd.int/bch/ui/templates/scripts/bchdropmenu-en.aspx
https://bch.cbd.int/bch/ui/navigation/countrylist-en.aspx
https://bch.cbd.int/bch/styles/bch.css
https://bch.cbd.int/about/policy/privacy.shtml
https://bch.cbd.int/about/policy/links.shtml
https://bch.cbd.int/about/policy/disclaimer.shtml
https://bch.cbd.int/about/news/default.shtml
https://bch.cbd.int/about/iac/default.shtml
https://bch.cbd.int/about/decisions/default.shtml
https://bch.cbd.int/about/news/
https://bch.cbd.int/about/mypow.shtml
https://bch.cbd.int/about/modalities.shtml
https://bch.cbd.int/about/latestadditions.shtml
https://bch.cbd.int/about/iac/
https://bch.cbd.int/about/development.shtml
https://bch.cbd.int/about/decisions/
https://bch.cbd.int/resources/
https://bch.cbd.int/protocol/
https://bch.cbd.int/onlineconferences/
https://bch.cbd.int/help/
https://bch.cbd.int/managementcentre/
https://bch.cbd.int/database/
https://bch.cbd.int/about/
https://bch.cbd.int/Common/RightMenu.js
https://bch.cbd.int/Common/Common.js

https://bch.cbd.int/Cms/Scripts/jquery-1.2.1.js
https://bch.cbd.int/Cms/Scripts/jquery.blockUI.js
https://bch.cbd.int/Cms/Scripts/AjaxScript.js
https://bchtraining.cbd.int/member/training-signin.aspx?returnurl=%2fdefault.shtml
https://bchtraining.cbd.int/Common/rightmenu.js
https://bchtraining.cbd.int/Common/Style.css
https://bchtraining.cbd.int/Common/Common.js
https://bchtraining.cbd.int/Common/Common.css
https://bchtraining.cbd.int/Cms/Web/Cms.css

The best way to deal with this vulnerability is to set HTTP header as follows:

'Pragma: No-cache'

'Cache-control: No-cache'.

Alternatively, but some browsers may have problem using this method, this can be set in the HTML header by adding the following HTML tags :

<META HTTP-EQUIV='Pragma' CONTENT='no-cache'>

<META HTTP-EQUIV='Cache-Control' CONTENT='no-cache'>

However, it is preferable to use HTTP header for compatibility with different web browsers.

6.4. Replace dangerous characters with ASCII code or UNICODE value

Dangerous characters such as >, <, (,), #, &, .. might make the application vulnerable if they are interpreted and executed. For example the interpretation of URLs containing those characters migh represents a vulnerability to directory traversal attacks.

All special characters should be replaced by their ASCII code or UNICODE values so that they would not be interpreted as a meta-function.

In addition the source code of the application should be modified in order to completely avoid use of dangerous characters. In fact, relative addresses that should be avoided are used in the code. Specifically, the following should not be permitted for the action parameter value:

<form name="CForm" method="post" action="**../**experts/" id="CForm">

It should be better to use absolute addresses.

6.5. Avoid using File Transfer Protocol

We recommend the use of Secure File Transfer Protocol (SFTP) instead of the File Transfer Protocol (FTP), because when using the entire login session, including transmission of password, the session is encrypted. It is therefore much more difficult for an outsider to observe and collect information such as passwords from a system using SFTP sessions.

6.6. Validate client information

Cross-site scripting or HTML injection might be possible. Malicious scripts might be injected into the browser which appeared to be genuine content from the original site. These scripts could be used to execute arbitrary code or steal customer sensitive information such as user password or cookies. Often this is in the form of a hyperlink with the injected script embedded within the query strings. However, XSS might be possible via FORM POST data, cookies; user data sent from another user or shared data retrieved from database.

This is the list of the potential URLs concerned by Cross-Site Scripting:

URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45888&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45833&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scr

	IPT%3E.parosproxy.org&eid=E45792&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45742&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45617&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45554&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45451&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45305&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org
URL	https://bch.cbd.int/cms/ajax/axcallback.aspx?uuid=bob@%3CSCRipt%3Ealert(Paros)%3C/scrIPT%3E.parosproxy.org&eid=E45355&method=_INIT&args=
Parameter	uuid=bob@<SCRipt>alert(Paros)</scrIPT>.parosproxy.org

Do not trust client side input even if there is client side validation. Sanitize potentially danger characters on the server side. Very often filtering the <, >, “characters prevent injected script to be executed in most cases. However, sometimes other danger meta-characters such as ' , (,), /, &, ..; etc are also needed. In addition (or if these characters are needed), HTML encode meta-characters in the response. For example, encode < as < Client entered data should not be displayed in case of an error of validation.

7. Conclusion

We hope that the results presented in this mandate will help Biosafety clearing-house to move toward the goal of having a more secure computing environment, at the same time offering the opportunity to better cope with external threats.

For assistance or in order to have more details, our information system security analysts will be available to lend the support you need.

8. Annexes

8.1. Partially ciphered connection

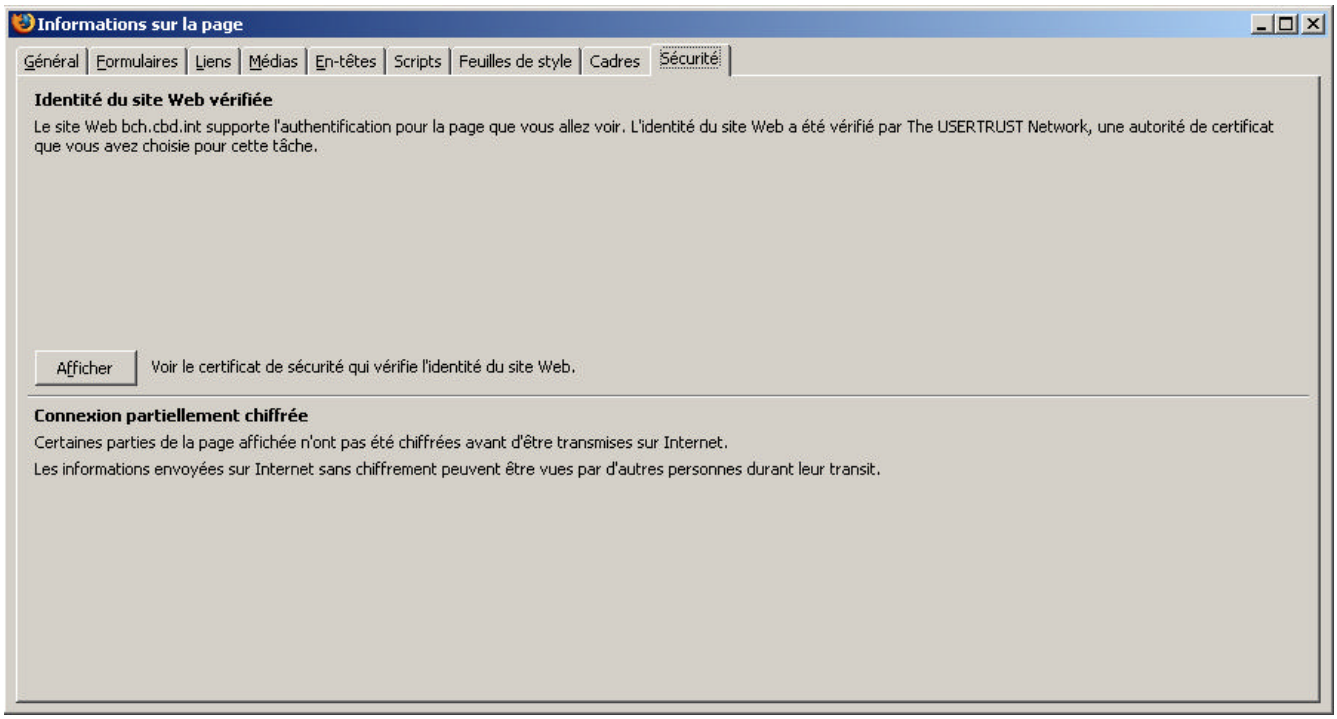


Figure 8.1 : Connection partially ciphered.

8.2. Sign up feature unavailable

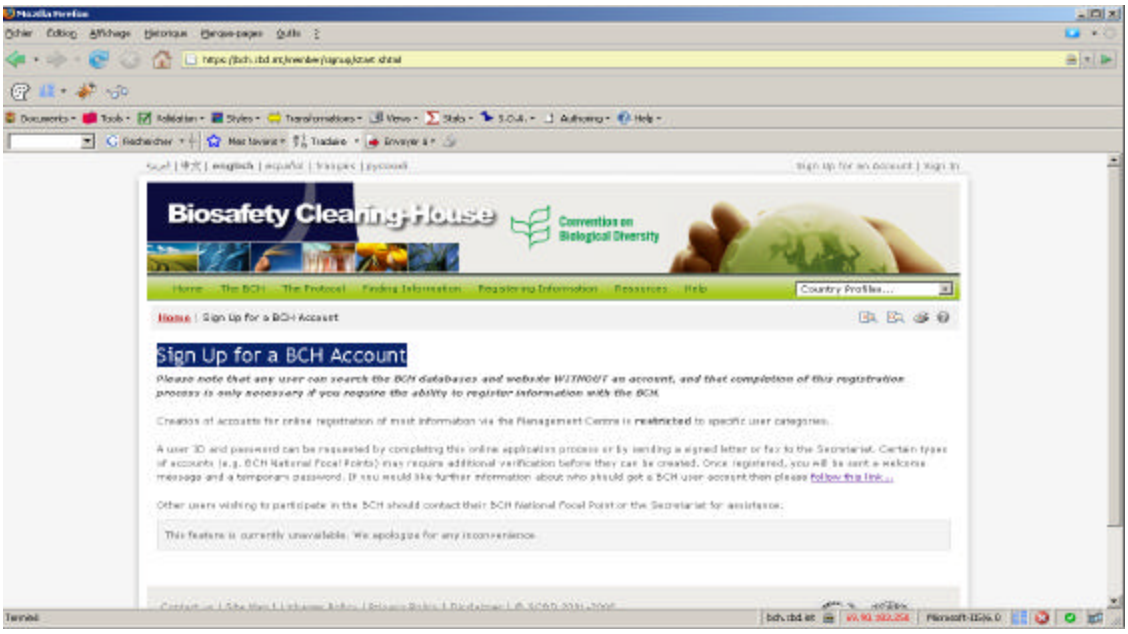


Figure 8.2 : Page returned for a Sign Up request.

8.3. Error messages

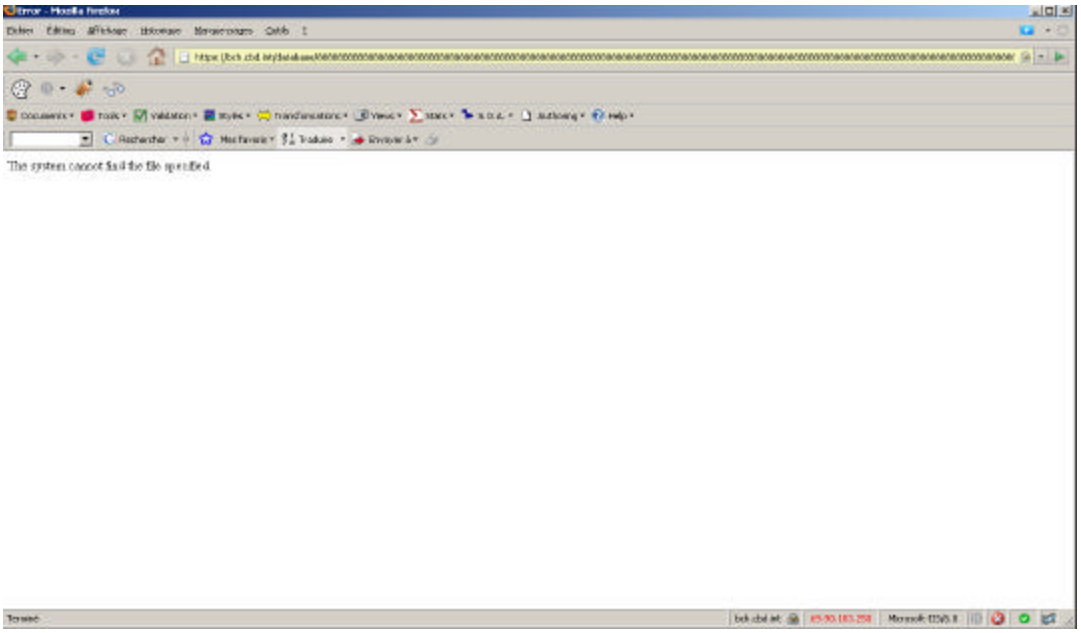


Figure 8.3 : System cannot find the file specified error page.

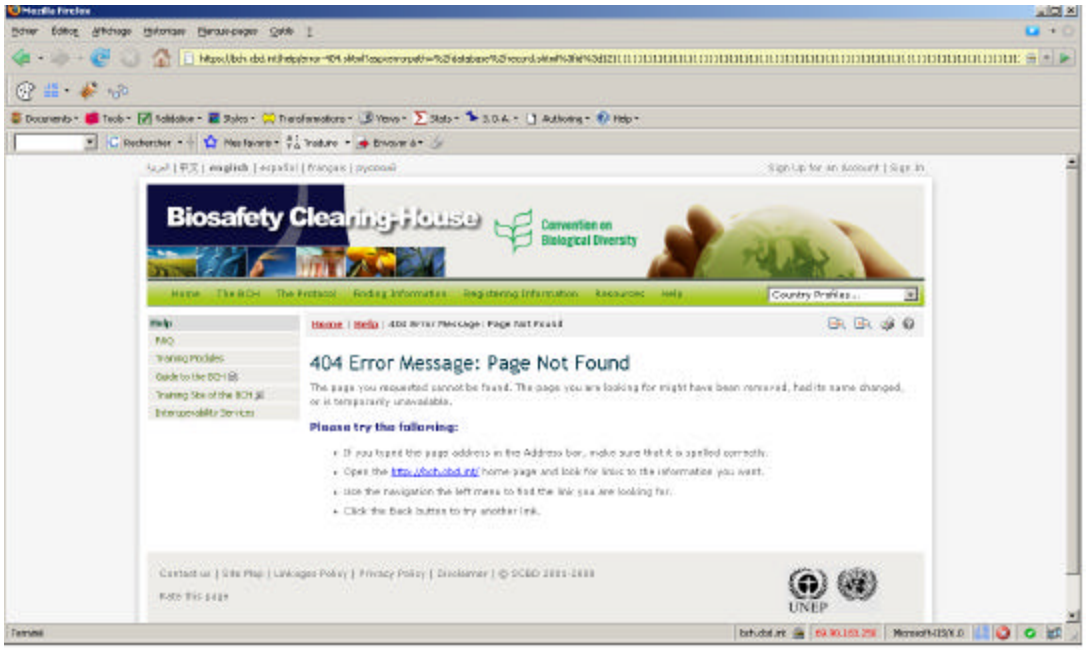


Figure 8.4 : 404 error page.