ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	2
Low	5
Informational	0

Alert Detail

High (Medium)	Injeção SQL
Description	Injeção SQL pode ser possível.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/lp/coursecompetencies.php?mod=12&courseid=4%2F2
Method	GET
Parameter	courseid
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/backup/restorefile.php
Method	POST
Parameter	contextid
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/backup/restorefile.php?contextid=169-2
Method	GET
Parameter	contextid
Attack	169-2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cache/admin.php
Method	POST
Parameter	lock
Attack	cachelock_file_default' OR '1'='1' --
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cache/admin.php?action=addstore&plugin=file&sesskey=l6mFFR8eoe+AND+1%3D1+--+
Method	GET
Parameter	sesskey
Attack	l6mFFR8eoe AND 1=1 --
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/log/index.php?chooselog=1&showusers=0&showcourses=0&id=4%2F2&user=8&date=&modid=&modaction=&origin=&edulevel=-1&logreader=logstore_standard
Method	GET
Parameter	id
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/user/view.php?id=2&course=4%2F2
Method	GET
Parameter	course
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cache/admin.php
Method	POST
Parameter	editing
Attack	' OR '1'='1' --
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/roles/override.php?contextid=7-2&roleid=3
Method	GET
Parameter	contextid
Attack	7-2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/user/index.php?id=4%2F2
Method	GET
Parameter	id
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/roles/override.php?contextid=88-2&amp%3Broleid=5
Method	POST
Parameter	contextid
Attack	88-2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/filter/manage.php?contextid=4%2F2
Method	GET
Parameter	contextid
Attack	4/2

URL	https://hom.ead.sesec.fortaleza.ce.gov.br/course/view.php?id=4%2F2
Method	GET
Parameter	id
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/lp/coursecompetencies.php?courseid=4%2F2
Method	GET
Parameter	courseid
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/enrol/manual/ajax.php?mform_showmore_main=0&id=4%2F2&action=enrol&enrolid=1&sesskey=wcfvZrFvES&_qf__enrol_manual_enrol_users_form=1&mform_showmore_id_main=0
Method	GET
Parameter	id
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cache/admin.php
Method	POST
Parameter	action
Attack	addstore OR 1=1 --
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cache/admin.php
Method	POST
Parameter	name
Attack	tst AND 1=1 --
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/grade/report/history/index.php?id=4%2F2
Method	GET
Parameter	id
Attack	4/2
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cache/admin.php
Method	POST
Parameter	_qf__cache_mode_mappings_form
Attack	1 OR 1=1 --
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/roles/permissions.php?contextid=169-2&returnurl=%2Fcourse%2Fmanagement.php%3Fcategoryid%3D3
Method	GET
Parameter	contextid
Attack	169-2
Instances	42
Solution	Não confie na entrada vinda do lado cliente, mesmo se houver uma validação deste lado. Em geral, valide todos os dados no lado servidor. Se a aplicação utilizar JDBC, utilize PreparedStatement ou CallableStatement com os parâmetros passados por '?' Se a aplicação utilizar ASP, utilize o ADO Command Objects com verificação forte de tipagem e consultas parametrizadas. Se for possível utilizar Stored Procedures, use-os. NÃO concatene strings nas consultas dentro dos Stored Procedures ou use 'exec', 'exec immediate' ou função equivalente! Não crie consultas SQL dinâmicas utilizando concatenação simples de strings. Sanitize todos os dados recebidos do cliente. Aplique uma 'whitelist' de caracteres permitidos ou uma 'blacklist' com os caracteres proibidos na entrada dos usuários. Aplique o princípio do privilégio mínimo ao ter o usuário do banco de dados com as menores permissões necessárias para uso do sistema. Em particular, evite o uso dos usuários 'sa' e 'db-owner'. Isto não elimina a injeção SQL, mas minimiza seu impacto. Garante o mínimo acesso a base de dados aplicação.
Other information	Os resultados da página original foram replicados com sucesso utilizando a expressão [4/2] como o valor de parâmetro. O valor do parâmetro foi modificado era , retirado da saída HTML para propósitos de comparação
Reference	https://www.owasp.org/index.php/Top_10_2010-A1 https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE Id	89
WASC Id	19
Source ID	1

High (Medium) **Path Traversal**

Description

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences.

The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding ("..%255c") of the backslash character.

	Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable script. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/purgecaches.php
Method	POST
Parameter	returnurl
Attack	purgecaches.php
Instances	1
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exclude directory separators such as "/". Use a whitelist of allowable file extensions. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass whitelist schemes by introducing dangerous inputs after they have been checked. Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links. Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	http://projects.webappsec.org/Path-Traversal http://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Source ID	1
Medium (Medium)	**Multiple X-Frame-Options Header Entries**
Description	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=modsettingresource
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/lp/competencyframeworks.php?pagecontextid=1
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/usertours/configure.php?action=listtours
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/configlog/index.php?sort=value&dir=ASC&page=0&perpage=30
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/cohort/index.php?search=teste&contextid=1&showall=1
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/user/forum.php?id=2&course=1
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/security/index.php
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/blog/index.php?courseid=2

Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/uploaduser/index.php
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/user/index.php?contextid=163&id=4&perpage=20&unified-filters%5B0%5D=4%3A3&tifirst=E
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/task/scheduledtasks.php
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/question/export.php?courseid=1&cat=4%2C1
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/blog/index.php?userid=2
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=mobilesettings
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/enrol/index.php?id=2
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/calendar/managesubscriptions.php?course=1
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/mod/forum/view.php?id=13
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/webservice/testclient.php
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/course/management.php?categoryid=3&perpage=20
Method	GET
Parameter	X-Frame-Options
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/user.php
Method	GET
Parameter	X-Frame-Options
Instances	549
Solution	Ensure only a single X-Frame-Options header is present in the response.
Reference	https://tools.ietf.org/html/rfc7034
CWE Id	16
WASC Id	15
Source ID	3

Medium (Medium)	**Pesquisa de Diretório**
Description	É possível visualizar a listagem de diretórios. A listagem de diretórios podem revelar scripts escondidos, incluindo arquivos, arquivos de origem de backup etc que podem ser acessados para ler informações de dados sensíveis.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/themes/advanced/skins/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/webservice/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/question/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/lists/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/inlinepopups/skins/clearlooks2/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/

Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/themes/advanced/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/print/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/preview/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/inlinepopups/skins/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/task/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/style/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/themes/advanced/skins/moodle/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/roles/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/emotions/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/themes/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/visualchars/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/backup/
Method	GET
Attack	Parent Directory
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/lib/editor/tinymce/tiny_mce/3.5.11/plugins/directionality/
Method	GET
Attack	Parent Directory
Instances	60
Solution	Desabilita a pesquisa de diretório. Se isso for necessário, certifique-se que os arquivos listados não induzem risco.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html
CWE Id	548
WASC Id	48
Source ID	1
Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/searchareas.php
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/mod/forum/discuss.php?d=2&mode=1
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/theme/styles_debug.php?theme=boost&type=plugin&subtype=block_blog_tags

Method	GET
Parameter	Pragma
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/theme/styles_debug.php?theme=boost&type=plugin&subtype=block_course_summary
Method	GET
Parameter	Pragma
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/theme/yui_combo.php?3.17.2/datatable-base/assets/skins/sam/datatable-base.css&3.17.2/datatable-message/assets/skins/sam/datatable-message.css&3.17.2/datatable-sort/assets/skins/sam/datatable-sort.css&3.17.2/autocomplete-list/assets/skins/sam/autocomplete-list.css
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=31104000, immutable
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=ajax
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/backup/backupfilesedit.php
Method	POST
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=tinymcemoodleemoticonsettings
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/notes/index.php?user=2
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/theme/styles_debug.php?theme=boost&type=plugin&subtype=filter_mediaplugin
Method	GET
Parameter	Pragma
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/theme/styles_debug.php?theme=boost&type=plugin&subtype=tool_messageinbound
Method	GET
Parameter	Cache-Control
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=privacysettings
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=managecustomfields
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/enrol/test_settings.php?enrol=database&sesskey=l6mFFR8eoe
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=cachestore_memcached_settings
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/theme/styles_debug.php?theme=boost&type=plugin&subtype=mnetservice_enrol
Method	GET
Parameter	Cache-Control
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/blog/preferences.php
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/course/editcategory.php?parent=1
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=messagesettingjabber
Method	GET
Parameter	Cache-Control
	private, pre-check=0, post-check=0, max-age=0, no-transform

Evidence	
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/grade/report/history/index.php?id=2
Method	GET
Parameter	Cache-Control
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Instances	824
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/badges/mybadges.php
Method	POST
Parameter	https://backpack.openbadges.org/issuer.js
Evidence	<script type="text/javascript" src="https://backpack.openbadges.org/issuer.js"></script>
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/badges/mybadges.php
Method	GET
Parameter	https://backpack.openbadges.org/issuer.js
Evidence	<script type="text/javascript" src="https://backpack.openbadges.org/issuer.js"></script>
Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Source ID	3

Low (Medium)	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/user/profile.php?id=2
Method	GET
Evidence	172.30.200.125
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=httpsecurity
Method	GET
Evidence	192.168.10.1
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/phpinfo.php
Method	GET
Evidence	172.30.200.125
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/log/index.php?chooselog=1&showusers=0&showcourses=0&id=1&user=&date=&modid=&modaction=&origin=&edulevel=-1&logreader=logstore_standard
Method	GET
Evidence	172.30.200.125
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/log/user.php?id=2&course=1&mode=today
Method	GET
Evidence	172.30.200.125
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/configlog/index.php?sort=lastname&dir=ASC&perpage=30&page=1
Method	GET
Evidence	172.30.198.23
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/user/view.php?id=2&course=2
Method	GET
Evidence	172.30.200.125
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/log/index.php?chooselog=1&showusers=0&showcourses=0&id=2&user=8&date=&modid=&modaction=&origin=&edulevel=-1&logreader=logstore_standard
Method	GET
Evidence	172.30.199.152
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=ipblocker
Method	GET
Evidence	192.168.10.1
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/usersessions/user.php
Method	GET
Evidence	172.30.200.125
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/report/log/user.php?id=2&course=1&mode=all

Method	GET
Evidence	172.30.200.125
Instances	11
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Other information	172.30.200.125 172.30.200.125
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Source ID	3

Low (Medium)	**Web Browser XSS Protection Not Enabled**
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/lp/edittemplate.php?pagecontextid=1
Method	GET
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/uploadcourse/index.php
Method	POST
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/course/management.php?categoryid=3
Method	POST
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/pluginfile.php/2/question/export/4/gift/withcategories/withcontexts/questionario-EAD%20SESECAMSEC-Padr%C3%A3o%20para%20Sistema-20190617-1751.txt?forcedownload=1
Method	GET
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/iplookup/index.php?ip=172.30.200.125
Method	GET
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/question/import.php
Method	GET
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/lp/editcompetencyframework.php?pagecontextid=1
Method	GET
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/tool/lpmigrate/frameworks.php
Method	POST
Parameter	X-XSS-Protection
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/backup/backupfilesedit.php
Method	GET
Parameter	X-XSS-Protection
Instances	9
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/search.php

Method	GET
Parameter	MoodleSession
Evidence	Set-Cookie: MoodleSession
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/login/index.php
Method	POST
Parameter	MoodleSession
Evidence	Set-Cookie: MoodleSession
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=sessionhandling
Method	POST
Parameter	MoodleSession
Evidence	Set-Cookie: MoodleSession
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/
Method	GET
Parameter	MoodleSession
Evidence	Set-Cookie: MoodleSession
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/admin/settings.php?section=sessionhandling
Method	GET
Parameter	MoodleSession
Evidence	Set-Cookie: MoodleSession
URL	https://hom.ead.sesec.fortaleza.ce.gov.br/login/index.php
Method	POST
Parameter	MOODLEID1_
Evidence	Set-Cookie: MOODLEID1_
Instances	6
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3