Tible Security Fundamentals report

Scan of http://www.uwwebsite.nl

Terborchstraat 18
8011 GG Zwolle

T +3138 760 1 760
F +3138 760 1 769

E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01

Contents

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

1 Scan information

Scan information	
Domain	http://www.uwwebsite.nl
Starttime	16-4-2015 16:47:36
Finish time	16-4-2015 17:36:25
Scan time	48 minutes, 50 seconds
Profile	Default

Server information	
Responsive	True
Server banner	nginx
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	**8**
High	0
Medium	1
Low	2
Informational	5

2 Executive summary

Alert group	Severity	Alert count
PHP hangs on parsing particular strings as floating point number	Medium	1
Cookie without HttpOnly flag set	Low	1
Cookie without Secure flag set	Low	1
Broken links	Informational	1
Email address found	Informational	3
Possible username or password disclosure	Informational	1

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

3 Affected items

path/	
Parameter	

Alert group	**Cookie without HttpOnly flag set**
Severity	**Low**
Description	This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HTTPOnly flag for this cookie.
Alert variants	
Details	Cookie name: "cookie_user" Cookie domain: "www.uwwebsite.nl"

Alert group	**Cookie without Secure flag set**
Severity	**Low**
Description	This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.
Recommendations	If possible, you should set the Secure flag for this cookie.
Alert variants	
Details	Cookie name: "cookie_user" Cookie domain: "www.uwwebsite.nl"

path/js/dynamic.grid.gallery.js	
Parameter	

Alert group	**Email address found**
Severity	**Informational**
Description	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Pattern found: me@uwwebsite.nl

path/js/jquery-1.8.1.min.js	
Parameter	

Alert group	**Email address found**
Severity	**Informational**

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

Description	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Pattern found: v@1.8.1

Alert group	**Possible username or password disclosure**
Severity	**Informational**
Description	A username and/or password was found in this file. This information could be sensitive. This alert may be a false positive, manual confirmation is required.
Recommendations	Remove this file from your website or change its permissions to remove
Alert variants	
Details	Pattern found: password:

path/css/styles.css

Parameter	

Alert group	**Broken links**
Severity	**Informational**
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Web Server

Parameter	

Alert group	**PHP hangs on parsing particular strings as floating point number**
Severity	**Medium**
Description	This alert was generated using only banner information. It may be a false positive. PHP hangs when parsing '2.2235678585075011e-318' string as a floating point number. Affected PHP versions: 5.3 up to version 5.3.5 and 5.2 up to version 5.2.17
Recommendations	Upgrade PHP to the latest version.
Alert variants	
Details	Current version is : PHP/5.3.3

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

4 Compliance According to Categories: A Detailed Report

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

(A1) Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No alerts in this category.

(A2) Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

No alerts in this category.

(A3) Cross Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

No alerts in this category.

(A4) Insecure Direct Object Reference

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

No alerts in this category.

(A5) Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application,

Total number of alerts in this category: 3

Alerts in this category

Cookie without HttpOnly flag set

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	/
Affected parameter	
Variants	1

Cookie without Secure flag set

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	/
Affected parameter	
Variants	1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**path/css/styles.css**
Affected parameter	
Variants	1

(A6) Sensitive Data Exposure

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Total number of alerts in this category: 7

Alerts in this category

Cookie without HttpOnly flag set

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	/
Affected parameter	
Variants	1

Cookie without Secure flag set

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	/
Affected parameter	
Variants	1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**path/css/styles.css**
Affected parameter	
Variants	1

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected item	**path/js/dynamic.grid.gallery.js**
Affected parameter	
Variants	1

Affected item	**path/js/jquery-1.8.1.min.js**
Affected parameter	
Variants	1

Affected item	**path/contact**
Affected parameter	
Variants	1

Possible username or password disclosure

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

CWE	CWE-200

Affected item	**path/js/jquery-1.8.1.min.js**
Affected parameter	
Variants	1

(A7) Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in

No alerts in this category.

(A8) Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate

No alerts in this category.

(A9) Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Total number of alerts in this category: 4

Alerts in this category

PHP hangs on parsing particular strings as floating point number

This alert was generated using only banner information. It may be a false positive.

PHP hangs when parsing '2.2235678585075011e-318' string as a floating point number.

Affected PHP versions: 5.3 up to version 5.3.5 and 5.2 up to version 5.2.17

CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Partial
CWE	CWE-189
CVE	CVE-2010-4645

Affected item	**Web Server**
Affected parameter	
Variants	1

Cookie without HttpOnly flag set

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	/
Affected parameter	
Variants	1

Cookie without Secure flag set

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	/
Affected parameter	
Variants	1

Broken links

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected item	**path/css/styles.css**
Affected parameter	
Variants	1

(A10) UnvalidatedRedirects and Forwards

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

No alerts in this category.

Terborchstraat 18
8011 GG Zwolle
T +3138 760 1 760
F +3138 760 1 769
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01