

## List of Plugin IDs

The following plugin IDs have problems associated with them. Select the ID to review more detail.

PLUGIN ID# ▾	# OF ISSUES ▾	PLUGIN NAME ▾	SEVERITY ▾
<a href="#">57640</a>	1	Web Application Information Disclosure	Medium Severity problem(s) fo
<a href="#">46803</a>	1	PHP expose_php Information Disclosure	Medium Severity problem(s) fo
<a href="#">11213</a>	1	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) fo
<a href="#">51972</a>	1	CGI Generic Cross-Site Scripting (Parameters Names)	Medium Severity problem(s) fo
<a href="#">22964</a>	2	Service Detection	Low Severity problem(s) found
<a href="#">26194</a>	1	Web Server Uses Plain Text Authentication Forms	Low Severity problem(s) found
<a href="#">34850</a>	1	Web Server Uses Basic Authentication Without HTTPS	Low Severity problem(s) found
<a href="#">11032</a>	1	Web Server Directory Enumeration	Low Severity problem(s) found
<a href="#">42057</a>	1	Web Server Allows Password Auto-Completion	Low Severity problem(s) found
<a href="#">10662</a>	1	Web mirroring	Low Severity problem(s) found
<a href="#">10287</a>	1	Traceroute Information	Low Severity problem(s) found
<a href="#">25220</a>	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
<a href="#">10267</a>	1	SSH Server Type and Version Information	Low Severity problem(s) found
<a href="#">10881</a>	1	SSH Protocol Versions Supported	Low Severity problem(s) found
<a href="#">40665</a>	1	Protected Web Page Detection	Low Severity problem(s) found
<a href="#">11936</a>	1	OS Identification	Low Severity problem(s) found
<a href="#">19506</a>	1	Nessus Scan Information	Low Severity problem(s) found
<a href="#">10114</a>	1	ICMP Timestamp Request Remote Date Disclosure	Low Severity problem(s) found
<a href="#">24260</a>	1	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
<a href="#">10107</a>	1	HTTP Server Type and Version	Low Severity problem(s) found
<a href="#">39463</a>	1	HTTP Server Cookies Set	Low Severity problem(s) found
<a href="#">12053</a>	1	Host Fully Qualified Domain Name (FQDN) Resolution	Low Severity problem(s) found
<a href="#">49705</a>	1	Gathered e-mail Addresses	Low Severity problem(s) found
<a href="#">49704</a>	1	External URLs	Low Severity problem(s) found
<a href="#">54615</a>	1	Device Type	Low Severity problem(s) found
<a href="#">45590</a>	1	Common Platform Enumeration (CPE)	Low Severity problem(s) found
<a href="#">39470</a>	1	CGI Generic Tests Timeout	Low Severity problem(s) found
<a href="#">33817</a>	1	CGI Generic Tests Load Estimation (all tests)	Low Severity problem(s) found
<a href="#">40406</a>	1	CGI Generic Tests HTTP Errors	Low Severity problem(s) found
<a href="#">47830</a>	1	CGI Generic Injectable Parameter	Low Severity problem(s) found
<a href="#">40984</a>	1	Browsable Web Directories	Low Severity problem(s) found
<a href="#">39521</a>	1	Backported Security Patch Detection (WWW)	Low Severity problem(s) found
<a href="#">39520</a>	1	Backported Security Patch Detection (SSH)	Low Severity problem(s) found
<a href="#">18261</a>	1	Apache Banner Linux Distribution Disclosure	Low Severity problem(s) found
<a href="#">46180</a>	1	Additional DNS Hostnames	Low Severity problem(s) found

PORT WWW (80/TCP)

Plugin ID: [11032](#)

## Web Server Directory Enumeration

---

### Synopsis

It is possible to enumerate directories on the web server.

### List of Hosts

[10.95.102.158](#)

### Plugin Output

The following directories were discovered:

/cgi-bin, /sites, /docs, /error, /icons

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories require authentication:

/manager/html

---

### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

---

### Solution

n/a

---

### See also

<http://projects.webappsec.org/Predictable-Resource-Location>

---

### Risk Factor

None

---

### Other references

[OWASP:OWASP-CM-006](#)

---

**Plugin publication date:** 2002/06/26

**Plugin last modification date:** 2011/12/12

**PORT WWW (80/TCP)**

Plugin ID: [57640](#)

---

## Web Application Information Disclosure

### Synopsis

The remote web application discloses path information.

### List of Hosts

10.95.102.158

### Plugin Output

The request GET /sonar/?sort=%00ipwchi HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Language: en  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Connection: Close  
Pragma: no-cache  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, \*/\*

produces the following path information :

```
<li class="">  
<a href="/sonar/plugins/home/org.sonar.plugins.motionchart.MotionChartPa  
ge">Motion chart</a></li>  
  
<li class="">
```

---

### Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

---

### Solution

Filter error messages containing path information.

---

### Risk Factor

Medium/ CVSS Base Score: 5.0  
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

---

**Plugin publication date:** 2012/01/25

**Plugin last modification date:** 2012/01/25

**PORT WWW (80/TCP)**

Plugin ID: **40984**

### Browsable Web Directories

---

#### Synopsis

Some directories on the remote web server are browsable.

#### List of Hosts

10.95.102.158

### Plugin Output

The following directories are browsable :

http://ci-bizframe.hi.inet/widgets/

http://ci-bizframe.hi.inet/widgets/?C=N;O=D  
http://ci-bizframe.hi.inet/widgets/?C=M;O=A  
http://ci-bizframe.hi.inet/widgets/?C=S;O=A  
http://ci-bizframe.hi.inet/widgets/?C=D;O=A

---

**Description**

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

---

**Solution**

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. And use access restrictions or disable directory indexing for any that do.

---

**See also**

<http://projects.webappsec.org/Directory-Indexing>

---

**Risk Factor**

None

---

**Plugin publication date:** 2009/09/15

**Plugin last modification date:** 2011/04/29

**PORT (0/TCP)**

Plugin ID: [46180](#)

**Additional DNS Hostnames****Synopsis**

Potential virtual hosts have been detected.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

- ci-bizframe

---

**Description**

Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name-based virtual hosts.

---

**Solution**

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

---

**See also**

[http://en.wikipedia.org/wiki/Virtual\\_hosting](http://en.wikipedia.org/wiki/Virtual_hosting)

---

**Risk Factor**

None

---

**Plugin publication date:** 2010/04/29

**Plugin last modification date:** 2011/06/22

**PORT WWW (80/TCP)**

Plugin ID: [24260](#)

**HyperText Transfer Protocol (HTTP) Information**

---

**Synopsis**

Some information about the remote HTTP configuration can be extracted.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Wed, 01 Feb 2012 17:45:21 GMT

Server: Apache/2.2.15 (CentOS)

Last-Modified: Tue, 31 Jan 2012 17:49:58 GMT

ETag: "277e1-1fe-4b7d6976cbd61"

Accept-Ranges: bytes

Content-Length: 510

Connection: close

Content-Type: text/html; charset=UTF-8

---

**Description**

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2007/01/30

**Plugin last modification date:** 2011/05/31

**PORT WWW (80/TCP)**

Plugin ID: [42057](#)

## Web Server Allows Password Auto-Completion

---

### Synopsis

Auto-complete is not disabled on password fields.

### List of Hosts

[10.95.102.158](#)

### Plugin Output

Page : /jenkins/login?from=/jenkins/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/web-calculator/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/static/9f5bcf50/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/All/people/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/All/builds  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/All/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/projectRelationship

Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/fingerprintCheck  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/computer/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/QA/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/eXperimental/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/backupDevelenv/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/CppSample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/CSSample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/develenv/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/flexSample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/GroovySample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/j2meSample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/JMeterExample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/JSSample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/PHPSample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/PythonExample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/SeleniumGridExample/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/standalone-archetype/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/test-calculator/  
Destination Page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/test-develenv/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/legend  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /sonar/sessions/new  
Destination Page : /sonar/sessions/login  
Input name : password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/test-dev  
elenv/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/backupDe  
velenv/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/develenv  
/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/standalo  
ne-archetype/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/test-cal  
culator/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/Selenium

GridExample/jswidgets/  
Destination Page : j\_acegi\_security\_check  
Input name : j\_password

---

### Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

---

### Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

---

### Risk Factor

None

---

**Plugin publication date:** 2009/10/07

**Plugin last modification date:** 2011/09/28

### PORT (0/TCP)

Plugin ID: [19506](#)

### Nessus Scan Information

---

#### Synopsis

Information about the Nessus scan.

#### List of Hosts

[10.95.102.158](#)

#### Plugin Output

Information about this scan :

Nessus version : 4.4.1

Plugin feed version : 201202010437

Type of plugin feed : HomeFeed (Non-commercial use only)

Scanner IP : 10.95.146.127

Port scanner(s) : nessus\_syn\_scanner

Port range : default

Thorough tests : no

Experimental tests : no

Paranoia level : 1

Report Verbosity : 1

Safe checks : yes

Optimize the test : yes

Credentialed checks : no

Patch management checks : None

CGI scanning : enabled

Web application tests : enabled  
Web app tests - Test mode : some\_pairs  
Web app tests - Try all HTTP methods : no  
Web app tests - Maximum run time : 60 minutes.  
Web app tests - Stop at first flaw : CGI  
Max hosts : 80  
Max checks : 5  
Recv timeout : 5  
Backports : Detected  
Scan Start Date : 2012/2/1 16:47  
Scan duration : 5254 sec

---

## Description

This script displays, for each tested host, information about the scan itself :

- The version of the plugin set
  - The type of plugin feed (HomeFeed or ProfessionalFeed)
  - The version of the Nessus Engine
  - The port scanner(s) used
  - The port range scanned
  - Whether credentialed or third-party patch management checks are possible
  - The date of the scan
  - The duration of the scan
  - The number of hosts scanned in parallel
  - The number of checks done in parallel
- 

## Solution

n/a

---

## Risk Factor

None

---

**Plugin publication date:** 2005/08/26

**Plugin last modification date:** 2011/12/23

## PORT (0/TCP)

Plugin ID: [25220](#)

## TCP/IP Timestamps Supported

---

### Synopsis

The remote service implements TCP timestamps.

### List of Hosts

[10.95.102.158](#)

---

## Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

---

**Solution**

n/a

---

**See also**

<http://www.ietf.org/rfc/rfc1323.txt>

---

**Risk Factor**

None

---

**Plugin publication date:** 2007/05/16

**Plugin last modification:** 2011/03/20

**PORT SSH (22/TCP)**

Plugin ID: [10267](#)

**SSH Server Type and Version Information**

---

**Synopsis**

An SSH server is listening on this port.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

SSH version : SSH-2.0-OpenSSH\_5.3

SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password

---

**Description**

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 1999/10/12

**Plugin last modification:** 2011/10/24

**PORT WWW (80/TCP)**

Plugin ID: [51972](#)

**CGI Generic Cross-Site Scripting (Parameters Names)**

---

**Synopsis**

The remote web server is prone to cross-site scripting attacks.

**List of Hosts**

10.95.102.158

### Plugin Output

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to XSS (on parameters names) :

/sonar/drilldown/violations/com.softwaresano.examples.calculator:web-calculator?<<<<<<<foo"bar'314>>>>=1

----- request -----

```
GET /sonar/drilldown/violations/com.softwaresano.examples.calculator:web-calculator?<<<<<<<foo"bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: _sonar_session=BAh7BjoPc2Vzc2lvbI9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODg%3D--b6a6df3def0f02606935651406274266cebe2b89
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, /*
```

----- output -----

```
var rp = {
"<<<<<<<foo"bar'314>>>>":"1"
```

, "controller": "drilldown"

/sonar/drilldown/measures/158?<<<<<<<foo"bar'314>>>>=1

----- request -----

```
GET /sonar/drilldown/measures/158?<<<<<<<foo"bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: _sonar_session=BAh7BjoPc2Vzc2lvbI9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODg%3D--b6a6df3def0f02606935651406274266cebe2b89
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, /*
```

----- output -----

```
var rp = {
"<<<<<<<foo"bar'314>>>>":"1"
```

, "controller": "drilldown"

/sonar/drilldown/violations/com.softwaresano.develenv:JSSample?<<<<<<
<foo"bar'314>>>>=1

----- request -----

```
GET /sonar/drilldown/violations/com.softwaresano.develenv:JSSample?<<<<<<<foo"bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: _sonar_session=BAh7BjoPc2Vzc2lvbI9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODg%3D--b6a6df3def0f02606935651406274266cebe2b89
```

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, \*/\*

-----  
----- output -----  
var rp = {

"<<<<<<<<foo"bar'314>>>>"":1"  
, "controller": "drilldown"  
-----

/sonar/drilldown/measures/380?<<<<<<<<foo"bar'314>>>>=1

----- request -----  
GET /sonar/drilldown/measures/380?<<<<<<<foo"bar'314>>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: \_sonar\_session=BAh7BjoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTEzDYYMTFIODg%3D--b6a6df3def0f02606935651406274266cebe2b89  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, \*/\*

----- output -----  
var rp = {

"<<<<<<<<foo"bar'314>>>>"":1"  
, "controller": "drilldown"  
-----

/sonar/drilldown/violations/com.softwaresano.examples:j2meSample?<<<<<  
<<<foo"bar'314>>>>=1

----- request -----  
GET /sonar/drilldown/violations/com.softwaresano.examples:j2meSample?<<<<<<<<foo"bar'314>>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: \_sonar\_session=BAh7BjoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTEzDYYMTFIODg%3D--b6a6df3def0f02606935651406274266cebe2b89  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, \*/\*

----- output -----  
var rp = {

"<<<<<<<<foo"bar'314>>>>"":1"  
, "controller": "drilldown"  
-----

/sonar/drilldown/violations/com.softwaresano.develenv:GroovySample?<<<<  
<<<<foo"bar'314>>>>=1

----- request -----  
GET /sonar/drilldown/violations/com.softwaresano.develenv:GroovySample?<<<<<<<<foo"bar'314>>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1



GET /sonar/drilldown/violations/com.softwaresano.archetypes:standalone-archetype?<<<<<<foo"bar'314>>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie:  
\_sonar\_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG  
-ed1aea7d8bedf790891b811c081b9d2026eed131  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /\*  
-----  
----- output -----  
var rp = {  
"<<<<<<foo"bar'314>>>":"1"  
,"controller":"drilldown"  
-----  
/sonar/drilldown/measures/400?<<<<<<foo"bar'314>>>>=1  
----- request -----  
GET /sonar/drilldown/measures/400?<<<<<<foo"bar'314>>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: hudson\_auto\_refresh=true;  
\_sonar\_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG  
-ed1aea7d8bedf790891b811c081b9d2026eed131  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /\*  
-----  
----- output -----  
var rp = {  
"<<<<<<foo"bar'314>>>":"1"  
,"controller":"drilldown"  
-----  
/sonar/drilldown/measures/2?<<<<<<foo"bar'314>>>>=1  
----- request -----  
GET /sonar/drilldown/measures/2?<<<<<<foo"bar'314>>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,\*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: hudson\_auto\_refresh=true;  
\_sonar\_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG  
-ed1aea7d8bedf790891b811c081b9d2026eed131  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /\*  
-----  
----- output -----  
var rp = {  
"<<<<<<foo"bar'314>>>":"1"  
,"controller":"drilldown"

```
-----  
/sonar/drilldown/violations/com.softwaresano.develenv:CppSample?<<<<<  
<<foo"bar'314>>>=1
```

----- request -----

```
GET /sonar/drilldown/violations/com.softwaresano.develenv:CppSample?<<<<<<<foo"bar'314>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: hudson_auto_refresh=true;  
_sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG  
-ed1aea7d8bedf790891b811c081b9d2026eed131  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
```

----- output -----

```
var rp = {  
"<<<<<<<foo"bar'314>>>":"1"  
,"controller":"drilldown"
```

```
/sonar/drilldown/measures/39?<<<<<<<foo"bar'314>>>=1
```

----- request -----

```
GET /sonar/drilldown/measures/39?<<<<<<<foo"bar'314>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: hudson_auto_refresh=true;  
_sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG  
-ed1aea7d8bedf790891b811c081b9d2026eed131  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
```

----- output -----

```
var rp = {  
"<<<<<<<foo"bar'314>>>":"1"  
,"controller":"drilldown"
```

```
/sonar/drilldown/violations/com.softwaresano.develenv:CSample?<<<<<<  
foo"bar'314>>>=1
```

----- request -----

```
GET /sonar/drilldown/violations/com.softwaresano.develenv:CSample?<<<<<<<foo"bar'314>>>=1 HTTP/1.1  
Host: ci-bizframe.hi.inet  
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1  
Accept-Language: en  
Connection: Close  
Cookie: hudson_auto_refresh=true;  
_sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG  
-ed1aea7d8bedf790891b811c081b9d2026eed131  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)  
Pragma: no-cache  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
```

```
----- output -----
var rp = {

"<<<<<<<foo'bar'314>>>>":"1"

,"controller":"drilldown"
-----


/sonar/drilldown/violations/com.softwaresano.develenv:flexSample?<<<<<
<<<foo'bar'314>>>>=1

----- request -----
GET /sonar/drilldown/violations/com.softwaresano.develenv:flexSample?<<<<<<<foo'bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: hudson_auto_refresh=true;
_sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTEzDYYMTFIODgiCmZsYXNoSUM6J0FjdG
-ed1aea7d8bedf790891b811c081b9d2026eed131
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, /*

----- output -----
var rp = {

"<<<<<<<foo'bar'314>>>>":"1"

,"controller":"drilldown"
-----


/sonar/drilldown/measures/393?<<<<<<<foo'bar'314>>>>=1

----- request -----
GET /sonar/drilldown/measures/393?<<<<<<<foo'bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: hudson_auto_refresh=true;
_sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTEzDYYMTFIODgiCmZsYXNoSUM6J0FjdG
-ed1aea7d8bedf790891b811c081b9d2026eed131
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, /*

----- output -----
var rp = {

"<<<<<<<foo'bar'314>>>>":"1"

,"controller":"drilldown"
-----


/sonar/drilldown/violations/ironman1:PHPSample?<<<<<<<foo'bar'314>>>
>=1

----- request -----
GET /sonar/drilldown/violations/ironman1:PHPSample?<<<<<<<foo'bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
```

```
Cookie: hudson_auto_refresh=true;
 _sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG
-ed1aea7d8bedf790891b811c081b9d2026eed131
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*

-----
----- output -----
var rp = {

"<<<<<<<<foo'bar'314>>>>":"1"

,"controller":"drilldown"
-----


/sonar/drilldown/measures/385?<<<<<<<foo"bar'314>>>>=1

----- request -----
GET /sonar/drilldown/measures/385?<<<<<<<foo"bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: hudson_auto_refresh=true;
 _sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG
-ed1aea7d8bedf790891b811c081b9d2026eed131
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*

-----
----- output -----
var rp = {

"<<<<<<<<foo'bar'314>>>>":"1"

,"controller":"drilldown"
-----


/sonar/drilldown/measures/1?<<<<<<<foo"bar'314>>>>=1

----- request -----
GET /sonar/drilldown/measures/1?<<<<<<<foo"bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: hudson_auto_refresh=true;
 _sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTExZDYyMTFIODgiCmZsYXNoSUM6J0FjdG
-ed1aea7d8bedf790891b811c081b9d2026eed131
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*

-----
----- output -----
var rp = {

"<<<<<<<<foo"bar'314>>>>":"1"

,"controller":"drilldown"
-----


/sonar/drilldown/violations/com.softwaresano.examples.calculator:test-ca
lculator?<<<<<<<foo"bar'314>>>>=1
```

----- request -----

```
GET /sonar/drilldown/violations/com.softwaresano.examples.calculator:test-calculator?<<<<<<foo"bar'314>>>>=1 HTTP/1.1
Host: ci-bizframe.hi.inet
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: hudson_auto_refresh=true;
_sonar_session=BAh7BzoPc2Vzc2lvbl9pZCIINTA3YWZmNGMyNGI2MGUzMjMxMzJINTEzDYyMTFIODgiCmZsYXNoSUM6J0FjdG
-ed1aea7d8bedf790891b811c081b9d2026eed131
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
```

----- output -----

```
var rp = {
"<<<<<<foo"bar'314>>>>":"1"
,"controller":"drilldown"
-----
```

---

## Description

The remote web server hosts CGI scripts that fail to adequately sanitize parameters name of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

---

## Solution

Contact the vendor for a patch or upgrade.

---

## See also

[http://en.wikipedia.org/wiki/Cross\\_site\\_scripting](http://en.wikipedia.org/wiki/Cross_site_scripting)  
<http://capec.mitre.org/data/definitions/86.html>  
<http://projects.webappsec.org/Cross-Site+Scripting>

---

## Risk Factor

Medium/ CVSS Base Score: 4.3  
(CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

---

## Other references

[CWE:79](#)  
[CWE:80](#)  
[CWE:81](#)  
[CWE:83](#)  
[CWE:20](#)  
[CWE:74](#)  
[CWE:442](#)  
[CWE:712](#)  
[CWE:722](#)  
[CWE:725](#)  
[CWE:811](#)  
[CWE:751](#)  
[CWE:801](#)  
[CWE:116](#)

**Plugin publication date:** 2011/02/14  
**Plugin last modification date:** 2011/12/09

### PORT WWW (80/TCP)

Plugin ID: [10107](#)

#### HTTP Server Type and Version

---

##### Synopsis

A web server is running on the remote host.

##### List of Hosts

[10.95.102.158](#)

##### Plugin Output

The remote web server type is :

Apache/2.2.15 (CentOS)

You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

---

##### Description

This plugin attempts to determine the type and the version of the remote web server.

---

##### Solution

n/a

---

##### Risk Factor

None

---

**Plugin publication date:** 2000/01/04  
**Plugin last modification date:** 2011/11/30

### PORT WWW (80/TCP)

Plugin ID: [34850](#)

#### Web Server Uses Basic Authentication Without HTTPS

---

##### Synopsis

The remote web server seems to transmit credentials in clear text.

##### List of Hosts

[10.95.102.158](#)

##### Plugin Output

The following pages are protected.

/manager/html/: realm="Tomcat Manager Application"  
/nexus/service/local/: realm="Sonatype Nexus Repository Manager API"  
/nexus/service/local/?D=A:/ realm="Sonatype Nexus Repository Manager API"

**Description**

The remote web server contains web pages that are protected by 'Basic' authentication over plain text.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

---

**Solution**

Make sure that HTTP authentication is transmitted over HTTPS.

---

**Risk Factor**

Low/ CVSS Base Score: 2.6  
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

---

**Plugin publication date:** 2008/11/21

**Plugin last modification date:** 2011/09/15

**PORT (0/TCP)**

Plugin ID: [12053](#)

**Host Fully Qualified Domain Name (FQDN) Resolution**

---

**Synopsis**

It was possible to resolve the name of the remote host.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

10.95.102.158 resolves as ci-bizframe.hi.inet.

---

**Description**

Nessus was able to resolve the FQDN of the remote host.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2004/02/11

**Plugin last modification date:** 2011/07/14

**PORT WWW (80/TCP)**

Plugin ID: [39470](#)

**CGI Generic Tests Timeout**

---

**Synopsis**

Some generic CGI attacks ran out of time.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

The following tests timed out without finding any flaw :

- SQL injection (on parameters names)
  - SQL injection (on HTTP headers)
- 

**Description**

Some generic CGI tests ran out of time during the scan.

The results may be incomplete.

---

**Solution**

Run your run scan again with a longer timeout or less ambitious options :

- Combinations of arguments values = 'all combinations' is much slower than 'two pairs' or 'single'.
  - Stop at first flaw = 'per port' is quicker.
  - In 'some pairs' or 'some combinations' mode, try reducing web\_app\_tests.tested\_values\_for\_each\_parameter in nessusd.conf
- 

**Risk Factor**

None

---

**Plugin publication date:** 2009/06/19

**Plugin last modification date:** 2011/03/06

**PORT WWW (80/TCP)**

Plugin ID: [40665](#)

**Protected Web Page Detection**

---

**Synopsis**

Some web pages require authentication.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

The following pages are protected by the BASIC authentication scheme :

/manager/html  
/nexus/service/local  
/nexus/service/local/?D=A

---

**Description**

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest but the credential are sent in clear text.
  - NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
  - Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.
- 

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2009/08/21

**Plugin last modification date:** 2011/03/15

**PORT (0/TCP)**

Plugin ID: [54615](#)

**Device Type**

---

**Synopsis**

It is possible to guess the remote device type.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

Remote device type : general-purpose

Confidence level : 95

---

**Description**

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2011/05/23

**Plugin last modification date:** 2011/05/23

**PORT SSH (22/TCP)**

Plugin ID: [39520](#)

**Backported Security Patch Detection (SSH)**

---

**Synopsis**

Security patches are backported.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

Give Nessus credentials to perform local checks.

---

**Description**

Security patches may have been 'back ported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

---

**Solution**

N/A

---

**See also**

<http://www.nessus.org/u?d636c8c7>

---

**Risk Factor**

None

---

**Plugin publication date:** 2009/06/25

**Plugin last modification date:** 2011/03/16

**PORT WWW (80/TCP)**

Plugin ID: [11213](#)

**HTTP TRACE / TRACK Methods Allowed**

---

**Synopsis**

Debugging functions are enabled on the remote web server.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

To disable these methods, add the following lines for each virtual host in your configuration file :

RewriteEngine on

```
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request :

```
----- snip -----
TRACE /Nessus2100712131.html HTTP/1.1
Connection: Close
Host: ci-bizframe.hi.inet
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
```

```
----- snip -----
```

and received the following response from the remote server :

```
----- snip -----
HTTP/1.1 200 OK
Date: Wed, 01 Feb 2012 17:45:25 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus2100712131.html HTTP/1.1
Connection: Close
Host: ci-bizframe.hi.inet
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, /*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
```

```
----- snip -----
```

---

## Description

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

---

## Solution

Disable these methods. Refer to the plugin output for more information.

---

## See also

[http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\\_XST\\_ebook.pdf](http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf)  
<http://www.apacheweek.com/issues/03-01-24>  
<http://www.kb.cert.org/vuls/id/288308>  
<http://www.kb.cert.org/vuls/id/867593>  
<http://download.oracle.com/sunalerts/1000718.1.html>

---

## Risk Factor

Medium/ CVSS Base Score: 4.3  
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)  
CVSS Temporal Score: 3.9(CVSS2#E:F/RL:W/RC:C)

---

**CVE**

[\*\*CVE-2003-1567\*\*](#)  
[\*\*CVE-2004-2320\*\*](#)  
[\*\*CVE-2010-0386\*\*](#)

---

**Bugtraq ID**

[\*\*9506\*\*](#)  
[\*\*9561\*\*](#)  
[\*\*11604\*\*](#)  
[\*\*33374\*\*](#)  
[\*\*37995\*\*](#)

---

**Other references**

[\*\*OSVDB:877\*\*](#)  
[\*\*OSVDB:3726\*\*](#)  
[\*\*OSVDB:5648\*\*](#)  
[\*\*OSVDB:50485\*\*](#)  
[\*\*CWE:16\*\*](#)

---

**Vulnerability publication date:** 2003/01/20

**Plugin publication date:** 2003/01/23

**Plugin last modification date:** 2011/09/19

**Ease of exploitability:** Exploits are available

**PORT (0/UDP)**

Plugin ID: [\*\*10287\*\*](#)

**Traceroute Information**

---

**Synopsis**

It was possible to obtain traceroute information.

**List of Hosts**

[\*\*10.95.102.158\*\*](#)

**Plugin Output**

For your information, here is the traceroute from 10.95.146.127 to 10.95.102.158 :

10.95.146.127  
10.95.146.1  
10.52.255.227  
10.95.102.158

---

**Description**

Makes a traceroute to the remote host.

---

**Solution**

n/a

---

**Risk Factor**

None

**Plugin publication date:** 1999/11/27  
**Plugin last modification date:** 2012/01/30

**PORT (0/TCP)**Plugin ID: [18261](#)**Apache Banner Linux Distribution Disclosure****Synopsis**

The name of the Linux distribution running on the remote host was found in the banner of the web server.

**List of Hosts**[10.95.102.158](#)**Plugin Output**

The linux distribution detected was :

- CentOS 6

**Description**

This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.

**Solution**

If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.

**Risk Factor**

None

**Plugin publication date:** 2005/05/15  
**Plugin last modification date:** 2012/01/24

**PORT WWW (80/TCP)**Plugin ID: [33817](#)**CGI Generic Tests Load Estimation (all tests)****Synopsis**

Load estimation for web application tests.

**List of Hosts**[10.95.102.158](#)**Plugin Output**

Here are the estimated number of requests in miscellaneous modes for one method only (GET or POST) :  
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery : S=60 SP=60 AP=60 SC=60 AC=60  
SQL injection : S=12312 SP=13560 AP=15504 SC=15240 AC=24624  
unseen parameters : S=17955 SP=19775 AP=22610 SC=22225 AC=35910  
local file inclusion : S=513 SP=565 AP=646 SC=635 AC=1026  
web code injection : S=513 SP=565 AP=646 SC=635 AC=1026  
XML injection : S=513 SP=565 AP=646 SC=635 AC=1026  
format string : S=1026 SP=1130 AP=1292 SC=1270 AC=2052  
script injection : S=60 SP=60 AP=60 SC=60 AC=60  
cross-site scripting (comprehensive test): S=2052 SP=2260 AP=2584 SC=2540 AC=4104  
injectable parameter : S=1026 SP=1130 AP=1292 SC=1270 AC=2052  
cross-site scripting (extended patterns) : S=360 SP=360 AP=360 SC=360 AC=360  
directory traversal (write access) : S=1026 SP=1130 AP=1292 SC=1270 AC=2052  
SSI injection : S=1539 SP=1695 AP=1938 SC=1905 AC=3078  
header injection : S=120 SP=120 AP=120 SC=120 AC=120  
directory traversal : S=12825 SP=14125 AP=16150 SC=15875 AC=25650  
HTML injection : S=300 SP=300 AP=300 SC=300 AC=300  
arbitrary command execution (time based) : S=3078 SP=3390 AP=3876 SC=3810 AC=6156  
persistent XSS : S=2052 SP=2260 AP=2584 SC=2540 AC=4104  
SQL injection (2nd order) : S=513 SP=565 AP=646 SC=635 AC=1026  
directory traversal (extended test) : S=26163 SP=28815 AP=32946 SC=32385 AC=52326  
arbitrary command execution : S=8208 SP=9040 AP=10336 SC=10160 AC=16416  
blind SQL injection (4 requests) : S=2052 SP=2260 AP=2584 SC=2540 AC=4104  
HTTP response splitting : S=540 SP=540 AP=540 SC=540 AC=540  
blind SQL injection : S=6156 SP=6780 AP=7752 SC=7620 AC=12312

All tests : S=100962 SP=111050 AP=126764 SC=124630 AC=200484

Here are the estimated number of requests in miscellaneous modes

for both methods (GET and POST) :

[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery : S=135 SP=135 AP=135 SC=135 AC=135  
SQL injection : S=26064 SP=33960 AP=49728 SC=44520 AC=117648  
unseen parameters : S=38010 SP=49525 AP=72520 SC=64925 AC=171570  
local file inclusion : S=1086 SP=1415 AP=2072 SC=1855 AC=4902  
web code injection : S=1086 SP=1415 AP=2072 SC=1855 AC=4902  
XML injection : S=1086 SP=1415 AP=2072 SC=1855 AC=4902  
format string : S=2172 SP=2830 AP=4144 SC=3710 AC=9804  
script injection : S=135 SP=135 AP=135 SC=135 AC=135  
cross-site scripting (comprehensive test): S=4344 SP=5660 AP=8288 SC=7420 AC=19608  
injectable parameter : S=2172 SP=2830 AP=4144 SC=3710 AC=9804  
cross-site scripting (extended patterns) : S=810 SP=810 AP=810 SC=810 AC=810  
directory traversal (write access) : S=2172 SP=2830 AP=4144 SC=3710 AC=9804  
SSI injection : S=3258 SP=4245 AP=6216 SC=5565 AC=14706  
header injection : S=270 SP=270 AP=270 SC=270 AC=270  
directory traversal : S=27150 SP=35375 AP=51800 SC=46375 AC=122550  
HTML injection : S=675 SP=675 AP=675 SC=675 AC=675  
arbitrary command execution (time based) : S=6516 SP=8490 AP=12432 SC=11130 AC=29412  
persistent XSS : S=4344 SP=5660 AP=8288 SC=7420 AC=19608  
SQL injection (2nd order) : S=1086 SP=1415 AP=2072 SC=1855 AC=4902  
directory traversal (extended test) : S=55386 SP=72165 AP=105672 SC=94605 AC=250002  
arbitrary command execution : S=17376 SP=22640 AP=33152 SC=29680 AC=78432  
blind SQL injection (4 requests) : S=4344 SP=5660 AP=8288 SC=7420 AC=19608  
HTTP response splitting : S=1215 SP=1215 AP=1215 SC=1215 AC=1215  
blind SQL injection : S=13032 SP=16980 AP=24864 SC=22260 AC=58824

All tests : S=213924 SP=277750 AP=405208 SC=363110 AC=954228

Your mode : some\_pairs, GET or POST.

Maximum number of requests : 111050

## Description

This script computes the maximum number of requests that would be done

by the generic web tests, depending on miscellaneous options.  
It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or  
the complexity of additional manual tests.

Note that the script does not try to compute this duration based  
on external factors such as the network and web servers loads.

---

## Solution

n/a

---

## Risk Factor

None

---

**Plugin publication date:** 2009/10/26

**Plugin last modification date:** 2011/09/21

**PORT WWW (80/TCP)**

Plugin ID: [47830](#)

## CGI Generic Injectable Parameter

---

### Synopsis

Some CGIs are candidate for extended injection tests.

### List of Hosts

[10.95.102.158](#)

### Plugin Output

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'q' parameter of the /jenkins/view/All/job/test-develenv/search/ CGI :

/jenkins/view/All/job/test-develenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/standalone-archetype/search/ CGI :

/jenkins/view/All/job/standalone-archetype/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/SeleniumGridExample/search/ CGI :

/jenkins/view/All/job/SeleniumGridExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/PHPSample/search/ CGI :

/jenkins/view/All/job/PHPSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/j2meSample/search/ CGI :

/jenkins/view/All/job/j2meSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/flexSample/search/ CGI :

/jenkins/view/All/job/flexSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/develenv/search/ CGI :

/jenkins/view/All/job/develenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/CppSample/search/ CGI :

/jenkins/view/All/job/CppSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
```

```
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/PHPSSample/search/ CGI :

```
/jenkins/view/develenv%20samples/job/PHPSSample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/GroovySample/search/ CGI :

```
/jenkins/view/develenv%20samples/job/GroovySample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/JSSample/search/ CGI :

```
/jenkins/view/develenv%20samples/job/JSSample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/flexSample/search/ CGI :

```
/jenkins/view/develenv%20samples/job/flexSample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/j2meSample/search/ CGI :

```
/jenkins/view/develenv%20samples/job/j2meSample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/web-calculator/search/ CGI :

```
/jenkins/view/develenv%20samples/job/web-calculator/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/develenv/search/ CGI :

/jenkins/view/develenv%20samples/job/develenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/backupDevelenv/search/ CGI :

/jenkins/view/develenv%20samples/job/backupDevelenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/test-calculator/search/ CGI :

/jenkins/job/test-calculator/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/SeleniumGridExample/search/ CGI :

/jenkins/job/SeleniumGridExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/PHPSample/search/ CGI :

/jenkins/job/PHPSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/j2meSample/search/ CGI :

/jenkins/job/j2meSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/flexSample/search/ CGI :

/jenkins/job/flexSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/CppSample/search/ CGI :

/jenkins/job/CppSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/eXperimental/search/ CGI :

/jenkins/view/eXperimental/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/QA/search/ CGI :

/jenkins/view/QA/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/computer/search/ CGI :

/jenkins/computer/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/All/search/ CGI :

```
/jenkins/view/All/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'from' parameter of the /jenkins/login CGI :

```
/jenkins/login?from=%00ipwchi
```

----- output -----

```
if (AUDIO_CAPABLE) {  
_sounds_pollForSounds(_sounds_ajaxJsonFetcherFactory);  
[...] le><input name="from" value="&#0;ipwchi" type="hidden" /><input name="Su [...]  
$('j_username').focus();  
</script></form></div></td></tr></table><table width="100%"><tr><t [...]  
-----
```

+ The 'q' parameter of the /jenkins/search/ CGI :

```
/jenkins/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/web-calculator/search/ CGI :

```
/jenkins/job/web-calculator/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'lhs' parameter of the /jenkins/projectRelationship CGI :

```
/jenkins/projectRelationship?lhs=%00ipwchi
```

----- output -----

```
}</script></head><body class="yui-skin-sam"><a href="#skip2content [...]  
upstream project:  
[...] t id="lhs" name="lhs" value="&#0;ipwchi" class="combobox " autocomplete=" [...]  
downstream project:  
<input id="rhs" name="rhs" class="combobox " autocomplete="off" /> [...]  
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/search/ CGI :

/jenkins/view/develenv%20samples/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/backupDevelenv/search/ CGI :

/jenkins/job/backupDevelenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/CSSample/search/ CGI :

/jenkins/job/CSSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/develenv/search/ CGI :

/jenkins/job/develenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/GroovySample/search/ CGI :

/jenkins/job/GroovySample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/job/JMeterExample/search/ CGI :

/jenkins/job/JMeterExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/JSSample/search/ CGI :

```
/jenkins/job/JSSample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/PythonExample/search/ CGI :

```
/jenkins/job/PythonExample/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/standalone-archetype/search/ CGI :

```
/jenkins/job/standalone-archetype/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/job/test-develenv/search/ CGI :

```
/jenkins/job/test-develenv/search/?q=%00ipwchi
```

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'sort' parameter of the /sonar/ CGI :

```
/sonar/?sort=%00ipwchi
```

----- output -----

```
<div class="line-block">  
<div class="operations">  
<form action="/sonar/?sort=%00ipwchi" style="display: inline" method="ge  
t">  
<select name="period" onchange="submit()" class="small">  
<option value="">Evoluci n en el tiempo...</option>  
-----
```

+ The 'component' parameter of the /docs/downloadingVM.php CGI :

/docs/downloadingVM.php?component=%00ipwchi

----- output -----

```
<div id="bodyColumn">
<div id="contentBox">
[...] evelenvms.softwaresano.com/"><b>.ipwchi</b> </a>se han de seguir los sig [...]
<li><a href=".//downloadVMOk.php?artifact=.ipwchi">Comprobar integr [...]
<li><a href=".//virtualMachines.html#Importacin_mquina_virtual"> Im [...]
```

-----

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/test-develenv/search/ CGI :

/jenkins/view/develenv%20samples/job/test-develenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

-----

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/standalone-archetype/search/ CGI :

/jenkins/view/develenv%20samples/job/standalone-archetype/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

-----

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/test-calculator/search/ CGI :

/jenkins/view/develenv%20samples/job/test-calculator/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

-----

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/SeleniumGridExample/search/ CGI :

/jenkins/view/develenv%20samples/job/SeleniumGridExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

-----

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/CppSample/search/ CGI :

/jenkins/view/develenv%20samples/job/CppSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/CSample/search/ CGI :

/jenkins/view/develenv%20samples/job/CSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/JMeterExample/search/ CGI :

/jenkins/view/develenv%20samples/job/JMeterExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/develenv%20samples/job/PythonExample/search/ CGI :

/jenkins/view/develenv%20samples/job/PythonExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/All/job/backupDevelenv/search/ CGI :

/jenkins/view/All/job/backupDevelenv/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/All/job/CSample/search/ CGI :

/jenkins/view/All/job/Csample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]  
var _gaq = _gaq || [];  
_gaq.push(['_setAccount', 'UA-8116005-4']);  
-----
```

+ The 'q' parameter of the /jenkins/view/All/job/GroovySample/search/ CGI :

/jenkins/view/All/job/GroovySample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/JMeterExample/search/ CGI :

/jenkins/view/All/job/JMeterExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/JSSample/search/ CGI :

/jenkins/view/All/job/JSSample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/PythonExample/search/ CGI :

/jenkins/view/All/job/PythonExample/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/test-calculator/search/ CGI :

/jenkins/view/All/job/test-calculator/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
```

+ The 'q' parameter of the /jenkins/view/All/job/web-calculator/search/ CGI :

/jenkins/view/All/job/web-calculator/search/?q=%00ipwchi

----- output -----

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
```

```
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

+ The 'q' parameter of the /jenkins/computer/(master)/search/ CGI :

```
/jenkins/computer/(master)/search/?q=%00ipwchi
```

```
----- output -----
```

```
<title>Search for '.ipwchi' [Jenkins]</title><link rel="stylesheet" type [...]>
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-8116005-4']);
-----
```

Clicking directly on these URLs should exhibit the issue :  
 (you will probably need to read the HTML source)

```
http://ci-bizframe.hi.inet/jenkins/view/All/job/PHPSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/job/j2meSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/job/flexSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/job/develenv/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/job/CppSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/test-calculator/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/SeleniumGridExample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/PHPSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/j2meSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/flexSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/CppSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/eXperimental/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/QA/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/computer/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/login?from=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/web-calculator/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/projectRelationship?lhs=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/develenv%20samples/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/backupDevelenv/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/CSSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/develenv/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/GroovySample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/JMeterExample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/JSSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/PythonExample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/standalone-archetype/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/job/test-develenv/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/sonar/?sort=%00ipwchi
http://ci-bizframe.hi.inet/docs/downloadingVM.php?component=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/job/CSSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/view/All/job/JSSample/search/?q=%00ipwchi
http://ci-bizframe.hi.inet/jenkins/computer/(master)/search/?q=%00ipwchi
```

Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'from' parameter of the /jenkins/j\_acegi\_security\_check CGI :

```
/jenkins/j_acegi_security_check [from=ipwchi]
```

```
----- output -----
```

```
}</script></head><body class="yui-skin-sam"><a href="#skip2content [...]
Invalid login information. Please try again.
<br /><a href="login?from=ipwchi">Try again</a></div><div align="middle"
```

><div style="margin-top:2em; color:gray; width:20em">If you are a system administrator and suspect this to be a configuration problem, see the server console output for more details.</div></div></td></tr></table><table width="100%"><tr><td id="footer"><span style="padding-right:2em; color:gray">

Page generated:  
Feb 1, 2012 6:46:12 PM</span><a href="http://jenkins-ci.org/">Jenk [...]

---

## Description

Nessus was able to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

---

## Solution

n/a

---

## Risk Factor

Low

---

## Other references

[CWE:86](#)

---

**Plugin publication date:** 2010/07/26

**Plugin last modification date:** 2011/09/21

## PORT (0/TCP)

Plugin ID: [11936](#)

## OS Identification

---

### Synopsis

It is possible to guess the remote operating system.

### List of Hosts

[10.95.102.158](#)

### Plugin Output

Remote operating system : Linux Kernel 2.6 on CentOS Linux release 6

Confidence Level : 95

Method : HTTP

The remote host is running Linux Kernel 2.6 on CentOS Linux release 6

---

**Description**

Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.

---

**Solution**

N/A

---

**Risk Factor**

None

---

**Plugin publication date:** 2003/12/09

**Plugin last modification date:** 2012/01/09

**PORT WWW (80/TCP)**

Plugin ID: [22964](#)

**Service Detection**

---

**Synopsis**

The remote service could be identified.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

A web server is running on this port.

---

**Description**

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2007/08/19

**Plugin last modification date:** 2012/01/19

**PORT SSH (22/TCP)**

Plugin ID: [22964](#)

**Service Detection**

---

**Synopsis**

The remote service could be identified.

**List of Hosts**

## 10.95.102.158

### Plugin Output

An SSH server is running on this port.

---

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

---

### Solution

n/a

---

### Risk Factor

None

---

**Plugin publication date:** 2007/08/19

**Plugin last modification date:** 2012/01/19

## PORT WWW (80/TCP)

Plugin ID: [46803](#)

### PHP expose\_php Information Disclosure

---

#### Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

#### List of Hosts

## 10.95.102.158

### Plugin Output

Nessus was able to verify the issue using the following URL :

<http://ci-bizframe.hi.inet/docs/downloadVMOk.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000>

---

### Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such an URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

---

### Solution

In the PHP configuration file, php.ini, set the value for 'expose\_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

---

**See also**

[http://www.0php.com/php\\_easter\\_egg.php](http://www.0php.com/php_easter_egg.php)  
<http://seclists.org/webappsec/2004/q4/324>

---

**Risk Factor**

Medium/ CVSS Base Score: 5.0  
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

---

**Other references**

[OSVDB:12184](#)

---

**Vulnerability publication date:** 2004/11/28

**Plugin publication date:** 2010/06/03

**Plugin last modification date:** 2011/03/14

**PORT WWW (80/TCP)**

Plugin ID: [49704](#)

**External URLs****Synopsis**

Links to external sites were gathered.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

170 external URLs were gathered on this web server :

URL... - Seen on...

http://85.214.82.106/public/downloads/develenv\_centos\_62-1.9.0.ova - /docs/downloadingVM.php  
http://85.214.82.106/public/downloads/develenv\_ubuntu\_1110-1.9.0.ova - /docs/downloadingVM.php  
http://blog.softwaresano.com - /docs/  
http://ci-bizframe/grid - /docs/selenium/index.html  
http://ci-bizframe/grid/ - /docs/selenium/index.html  
http://ci-bizframe/grid/console - /docs/selenium/index.html  
http://ci-bizframe/hudson//static/9f5bcf50/images/24x24/user.png - /jenkins/people/  
http://ci-bizframe/sonar - /jenkins/job/web-calculator/  
http://code.google.com/p/develenv-plugins - /hudson/  
http://code.google.com/p/develenv-plugins/ - /docs/samples.html  
http://code.google.com/p/develenv/wiki/newProject - /docs/  
http://concordion.org - /docs/selenium/seleniumGridExample.html  
http://concordion.org/ - /docs/samples.html  
http://develenv-android-plugin.googlecode.com - /docs/plugins.html  
http://develenv-cpp-plugin.googlecode.com - /docs/plugins.html  
http://develenv-php-plugin.googlecode.com - /docs/plugins.html  
http://develenv-php-plugin.googlecode.com/svn/trunk/php\_plugin/samples/BankAccount - /sonar/  
http://develenv-plugins.googlecode.com - /docs/plugins.html  
http://develenv-python-plugin.googlecode.com - /docs/plugins.html  
http://develenv.googlecode.com/svn/tags/develenv-1.0.6/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.1.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.2.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.2.1/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.3.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.3.1/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.3.2/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.3.3/ - /docs/downloads/releases.html

http://develenv.googlecode.com/svn/tags/develenv-1.3.4/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.3.5/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.4.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.4.1/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.4.2/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.1/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.10/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.11/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.12/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.13/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.14/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.15/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.16/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.2/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.3/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.4/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.5/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.6/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.7/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.8/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.5.9/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.6.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.1/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.10/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.2/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.3/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.4/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.5/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.6/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.7/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.8/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.7.9/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.8.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.8.1/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.8.2/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.8.3/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.8.4/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.8.5/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.9.0/ - /docs/downloads/releases.html  
http://develenv.googlecode.com/svn/tags/develenv-1.9.1/ - /docs/downloads/releases.html  
http://develenv.softwaresano.com - /docs/  
http://develenv.softwaresano.com/develenv/ - /docs/project-summary.html  
http://develenv.softwaresano.com/developer/developer/ - /docs/developer/project-summary.html  
http://develenv.softwaresano.com/jenkins/jenkins/ - /docs/jenkins/project-summary.html  
http://develenv.softwaresano.com/jmeter/jmeter/ - /docs/jmeter/project-summary.html  
http://develenv.softwaresano.com/nexus/nexus/ - /docs/nexus/project-summary.html  
http://develenv.softwaresano.com/notFound.html - /docs/document.getElementsByTagName(  
http://develenv.softwaresano.com/selenium/selenium/ - /docs/selenium/project-summary.html  
http://develenv.softwaresano.com/sites/com.softwaresano.examples/j2meSample - /sonar/  
http://develenv.softwaresano.com/soapui/soapui/ - /docs/soapui/project-summary.html  
http://develenv.softwaresano.com/sonar/sonar/ - /docs/sonar/project-summary.html  
http://develenvms.softwaresano.com/public/downloads/develenv\_centos\_62-1.9.0.ova - /docs/downloadingVM.php  
http://develenvms.softwaresano.com/public/downloads/develenv\_ubuntu\_1110-1.9.0.ova - /docs/downloadingVM.php  
http://developer.softwaresano.com - /docs/developer/index.html  
http://downloads.softwaresano.com/download.php?artifactId=develenv&version=1.9.1&classifier=.sh - /docs/downloads/releases.htm  
http://downloads.softwaresano.com/last.php?artifactId=develenv - /docs/downloads/releases.html  
http://downloads.softwaresano.com/last.php?type=SNAPSHOT&artifactId=develenv&classifier=.sh - /docs/downloads/snapshots.htm  
http://extdevelenv.googlecode.com/svn/trunk/j2meSample - /sonar/  
http://ironman1.hi.inet/hudson/job/PHPSSample - /sonar/  
http://ironman1/jenkins/job/standalone-archetype - /sonar/  
http://ironman1/jenkins/job/CSample - /sonar/  
http://ironman1/jenkins/job/CppSample - /sonar/  
http://ironman1/jenkins/job/GroovySample - /sonar/  
http://ironman1/jenkins/job/JSSample - /sonar/  
http://ironman1/jenkins/job/flexSample - /sonar/

http://ironman1/jenkins/job/j2meSample - /sonar/  
http://ironman1/jenkins/job/test-calculator - /sonar/  
http://ironman1/jenkins/job/web-calculator - /sonar/  
http://ironman1/sites/com.softwaresano.archetypes/standalone-archetype - /sonar/  
http://ironman1/sites/com.softwaresano.develenv/CSample - /sonar/  
http://ironman1/sites/com.softwaresano.develenv/CppSample - /sonar/  
http://ironman1/sites/com.softwaresano.develenv/GroovySample - /sonar/  
http://ironman1/sites/com.softwaresano.develenv/JSSample - /sonar/  
http://ironman1/sites/com.softwaresano.develenv/flexSample - /sonar/  
http://ironman1/sites/com.softwaresano.examples.calculator/test-calculator - /sonar/  
http://ironman1/sites/com.softwaresano.examples.calculator/web-calculator - /sonar/  
http://ironman1/sites/ironman1/PHPSample - /sonar/  
http://jakarta.apache.org/jmeter/ - /docs/  
http://java.sun.com - /docs/developer/index.html  
http://java.sun.com/javase/downloads/index.jsp - /docs/compilation.html  
http://jenkins-ci.org/ - /hudson/  
http://jenkins.softwaresano.com - /docs/jenkins/index.html  
http://jetty.mortbay.org - /grid/resources/images  
http://jira.codehaus.org/browse/develenv-1 - /docs/changelog.html  
http://jtreemap.sourceforge.net - /docs/statscm/repomap.html  
http://maven.apache.org - /docs/  
http://maven.apache.org/guides/mini/guide-3rd-party-jars-remote.html - /docs/repositories.html  
http://maven.apache.org/plugins/maven-antrun-plugin/ - /docs/plugin-management.html  
http://maven.apache.org/plugins/maven-assembly-plugin/ - /docs/plugin-management.html  
http://maven.apache.org/plugins/maven-changes-plugin-2.1 - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-clean-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-compiler-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-dependency-plugin/ - /docs/plugin-management.html  
http://maven.apache.org/plugins/maven-deploy-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-install-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-jar-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-release-plugin/ - /docs/plugin-management.html  
http://maven.apache.org/plugins/maven-resources-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/plugins/maven-site-plugin/ - /docs/selenium/plugins.html  
http://maven.apache.org/surefire/maven-surefire-plugin - /docs/selenium/plugins.html  
http://mojo.codehaus.org/buildnumber-maven-plugin - /docs/selenium/plugins.html  
http://nexus.softwaresano.com - /docs/nexus/index.html  
http://nexus.sonatype.org - /nexus/index.html  
http://nexus.sonatype.org/ - /docs/nexus/index.html  
http://pimpam.googlecode.com/files/builtByPimpam.png - /docs/  
http://pimpam.googlecode.com/files/favicon.ico - /docs/  
http://pimpam.googlecode.com/svn/trunk/standalone-archetype - /sonar/  
http://pimpam.googlecode.com/svn/trunk/test-calculator - /sonar/  
http://pimpam.googlecode.com/svn/trunk/web-calculator - /sonar/  
http://pimpam.googlecode.com/svn/trunk/web-  
calculator/src/test/java/com/softwaresano/examples/calculator/test/acceptance/WebCalculator.java -  
/docs/selenium/seleniumGridExample.html  
http://pimpam.googlecode.com/svn/trunk/web-  
calculator/src/test/resources/com/softwaresano/examples/calculator/test/acceptance/WebCalculator.html -  
/docs/selenium/seleniumGridExample.html  
http://selenium.softwaresano.com - /docs/selenium/index.html  
http://seleniumhq.org - /docs/  
http://seleniumhq.org/ - /docs/selenium/index.html  
http://sonar-plugins.codehaus.org - /sonar/  
http://sonar.codehaus.org/documentation - /sonar/  
http://sonar.codehaus.org/support/ - /sonar/  
http://sonar.softwaresano.com - /docs/sonar/index.html  
http://stat-scm.sourceforge.net/ - /docs/statscm/statscm.html  
http://subversion.apache.org/ - /docs/source-repository.html  
http://svnbook.red-bean.com/ - /docs/source-repository.html  
http://wiki.jenkins-ci.org/display/JENKINS/M2+Release+Plugin - /docs/developer/index.html  
http://wiki.jenkins-ci.org/display/JENKINS/Search+Box - /hudson/  
http://www.apache.org/dyn/closer.cgi/maven/binaries/apache-maven-2.2.1-bin.tar.gz - /docs/developer/index.html  
http://www.apache.org/dyn/closer.cgi/maven/binaries/apache-maven-3.0.3-bin.tar.gz - /docs/developer/index.html  
http://www.javaworld.com/javaworld/jw-08-2011/110823-atdd-for-web-apps.html - /docs/samples.html  
http://www.oracle.com/technetwork/java/javase/downloads/index.html - /docs/installation.html  
http://www.soapui.org - /docs/

http://www.soapui.org/ - /docs/soapui/index.html  
http://www.softwaresano.com - /docs/  
http://www.softwaresano.com/ - /docs/  
http://www.softwaresano.com/widgets/builtBy.php - /docs/selenium/index.html  
http://www.softwaresano.com/widgets/foot.php - /  
http://www.softwaresano.com/widgets/head.php - /docs/  
http://www.softwaresano.com/widgets/jenkinsViewBuiltBy.php - /hudson/  
http://www.softwaresano.com/widgets/jobBuitlyBy.php - /jenkins/job/web-calculator/  
http://www.sonarsource.com - /sonar/  
http://www.sonarsource.org/ - /sonar/  
http://www.sonarsource.org/documentation/license/ - /sonar/  
http://www.statsvn.org - /docs/statscm/  
http://www.virtualbox.org - /docs/virtualMachines.html

---

**Description**

Nessus gathered HREF links to external sites by crawling the remote web server.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2010/10/04

**Plugin last modification date:** 2011/08/19

**PORT WWW (80/TCP)**

Plugin ID: [39463](#)

**HTTP Server Cookies Set****Synopsis**

Some cookies have been set by the web server.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

```
path = /jenkins
name = ACEGI_SECURITY_HASHED_REMEMBER_ME_COOKIE
value = ""
version = 1
expires = Thu, 01-Jan-1970 00:00:10 GMT
secure = 0
httponly = 0
```

This cookie was set by Tomcat(servlet/jsp engine) :

```
path = /jenkins/
name = JSESSIONID
value = 6887B4EB3CC715E7C356B97AE7199EA3
version = 1
secure = 0
httponly = 1
```

```
path = /
```

```
name = iconSize
value = 24x24
version = 1
expires = Sun, 27-May-2012 11:30:18 GMT
secure = 0
httponly = 0
```

```
path = /
name = hudson_auto_refresh
value = false
version = 1
expires = Fri, 02-Mar-2012 17:44:47 GMT
secure = 0
httponly = 0
```

This cookie was set by Tomcat(servlet/jsp engine) :

```
path = /manager/
name = JSESSIONID
value = 36241179541326DA23492A43491399FA
version = 1
secure = 0
httponly = 1
```

```
path = /
name = _sonar_session
value = BAh7BjoPc2Vzc2lvbl9pZCIIN2Q5OGU2MjZkOTQ3MmRIOGU4OTFmZDcwM2NIYzQ5ZWY%3D-
-028e35525f87e555a490deff091796bc94328cb9
version = 1
expires = Wed, 01-Feb-2012 18:04:47 GMT
secure = 0
httponly = 1
```

---

## Description

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser. As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions.

This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

---

## Solution

n/a

---

## Risk Factor

None

---

**Plugin publication date:** 2009/06/19  
**Plugin last modification date:** 2011/03/15

**PORT WWW (80/TCP)**

Plugin ID: [40406](#)

---

**CGI Generic Tests HTTP Errors**

---

**Synopsis**

Nessus encountered errors while running its generic CGI attacks.

**List of Hosts**[10.95.102.158](http://10.95.102.158)**Plugin Output**

Nessus encountered :

- 1 error involving SSI injection (on HTTP headers) checks :  
. reading the HTTP status line: errno=1 (operation timed out)
  - 33 errors involving SQL injection (on HTTP headers) checks :  
- 23 errors involving SQL injection (on parameters names) checks :
- 

**Description**

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

---

**Solution**

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check\_read\_timeout)
  - Options -> Number of hosts in parallel (max\_hosts)
  - Options -> Number of checks in parallel (max\_checks)
- 

**Risk Factor**

None

---

**Plugin publication date:** 2009/07/28

**Plugin last modification date:** 2011/09/21

**PORT WWW (80/TCP)**

Plugin ID: [49705](#)

**Gathered e-mail Addresses**

---

**Synopsis**

e-mail addresses were gathered.

**List of Hosts**[10.95.102.158](http://10.95.102.158)**Plugin Output**

The following email address has been gathered :

- 'carlosg@softwaresano.com', referenced from :  
/docs/developer/team-list.html  
/docs/selenium/team-list.html  
/docs/jenkins/team-list.html

/docs/jmeter/team-list.html  
/docs/team-list.html  
/docs/sonar/team-list.html  
/docs/soapui/team-list.html  
/docs/nexus/team-list.html

---

**Description**

Nessus gathered mailto: HREF links and extracted e-mail addresses by crawling the remote web server.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2010/10/04

**Plugin last modification date:** 2011/03/18

**PORT (0/TCP)**

Plugin ID: [45590](#)

**Common Platform Enumeration (CPE)**

---

**Synopsis**

It is possible to enumerate CPE names that matched on the remote system.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

The remote operating system matched the following CPE :

cpe:/o:centos:centos:6

Following application CPE's matched on the remote system :

cpe:/a:openbsd:openssh:5.3

cpe:/a:apache:http\_server:2.2.15 -> Apache Software Foundation Apache HTTP Server 2.2.15

---

**Description**

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

---

**Solution**

n/a

**See also**

<http://cpe.mitre.org/>

---

**Risk Factor**

None

---

**Plugin publication date:** 2010/04/21

**Plugin last modification date:** 2012/01/19

**PORT SSH (22/TCP)**

Plugin ID: [10881](#)

**SSH Protocol Versions Supported**

---

**Synopsis**

A SSH server is running on the remote host.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

The remote SSH daemon supports the following versions of the SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : 7a:ba:e4:3b:32:4a:fc:fe:85:be:0a:58:5e:cb:4c:0f

---

**Description**

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2002/03/06

**Plugin last modification date:** 2011/03/30

**PORT (0/ICMP)**

Plugin ID: [10114](#)

**ICMP Timestamp Request Remote Date Disclosure**

---

**Synopsis**

It is possible to determine the exact time set on the remote host.

**List of Hosts**[10.95.102.158](#)**Plugin Output**

The difference between the local and remote clocks is -6810 seconds.

---

**Description**

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine.

This may help an attacker to defeat all time-based authentication protocols.

---

**Solution**

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

---

**Risk Factor**

None

---

**CVE**[CVE-1999-0524](#)**Other references**[OSVDB:94](#)[CWE:200](#)

**Vulnerability publication date:** 1995/01/01

**Plugin publication date:** 1999/08/01

**Plugin last modification date:** 2011/11/15

**PORT WWW (80/TCP)**

Plugin ID: [10662](#)

**Web mirroring****Synopsis**

Nessus crawled the remote web site.

**List of Hosts**[10.95.102.158](#)**Plugin Output**

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/sonar/drilldown/violations/com.softwaresano.develenv:CppSample (severity [BLOCKER] )  
/hudson/job/CSample/ws/rssAll (flavor [rss20] )  
/sonar/images/images/ci.png (1328034139 [] )  
/jenkins/static/9f5bcf50/job/develenv/enable ()  
/sonar/images/sonar.png (1328034139 [] )

/jenkins/view/develenv%20samples/job/web-calculator/rssChangelog (flavor [rss20] )  
/sonar/sessions/login (login [] password [] remember\_me [1] commit [Conectar] )  
/jenkins/job/PythonExample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PHPSSample/ (auto\_refresh [true] )  
/jenkins/job/test-develenv/buildTimeTrend (auto\_refresh [true] )  
/sonar/images/priority/INFO.png (1328034139 [] )  
/jenkins/view/All/job/CppSample/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/backupDevelenv/rssAll (flavor [rss20] )  
/hudson/job/j2meSample/ws/rssFailed (flavor [rss20] )  
/sonar/resource/index/384 (tab [violations] )  
/hudson/ (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/test-calculator/disable ()  
/jenkins/view/All/job/flexSample/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/GroovySample/rssFailed (flavor [rss20] )  
/jenkins/job/SeleniumGridExample/ws/ (auto\_refresh [true] )  
/sonar/chart (cht [sl] v [1=135.496;2=0.0] chv [20120119173803,100.0,20120119174504,...])  
/sonar/feeds/project/com.softwaresano.archetypes:standalone-archetype (category [Alert] )  
/jenkins/view/All/job/test-calculator/rssFailed (flavor [rss20] )  
/jenkins/job/CSSample/disable ()  
/jenkins/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/JMeterExample/search/ (q [search] )  
/jenkins/static/9f5bcf50/job/JMeterExample/disable ()  
/jenkins/static/9f5bcf50/job/test-calculator/rssAll (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/test-develenv/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/PythonExample/rssAll (flavor [rss20] )  
/jenkins/view/QA/search/ (q [search] )  
/sonar/resource/index/265 (metric [duplicated\_lines\_density] )  
/jenkins/job/backupDevelenv/rssAll (flavor [rss20] )  
/nexus/js/repoServer/nexus-lvo-plugin-all.js (1.9.2.4 [] )  
/hudson/job/web-calculator/ws/rssChangelog (flavor [rss20] )  
/hudson/job/SeleniumGridExample/browser=firefox/ (auto\_refresh [true] )  
/sonar/images/priority/MINOR.png (1328034139 [] )  
/hudson/job/backupDevelenv/rssAll (flavor [rss20] )  
/hudson/job/CppSample/ws/rssChangelog (flavor [rss20] )  
/nexus/js/sonatype-all.js (1.9.2.4 [] )  
/jenkins/job/GroovySample/ (auto\_refresh [false] )  
/jenkins/job/test-calculator/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/j2meSample/rssAll (flavor [rss20] )  
/hudson/job/test-calculator/ws/rssFailed (flavor [rss20] )  
/jenkins/view/eXperimental/builds (auto\_refresh [true] )  
/jenkins/job/GroovySample/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-calculator/search/ (q [search] )  
/sonar/resource/index/11 (tab [violations] )  
/sonar/drilldown/violations/com.softwaresano.develenv:flexSample (rule [flexplugin:com.adobe.ac.pmd.rules.maintanability.forbidder]  
/hudson/job/CSSample/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/GroovySample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PHPSSample/disable ()  
/jenkins/job/CppSample/ws/ (auto\_refresh [true] )  
/jenkins/job/test-develenv/disable ()  
/jenkins/view/develenv%20samples/job/test-calculator/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/view/develenv%20samples/job/PHPSSample/rssFailed (flavor [rss20] )  
/jenkins/job/GroovySample/ws/rssFailed (flavor [rss20] )  
/hudson/job/PythonExample/ (auto\_refresh [false] )  
/sonar/resource/index/291 (tab [violations] )  
/jenkins/static/9f5bcf50/job/backupDevelenv/ (auto\_refresh [false] )  
/jenkins/view/All/job/test-develenv/ (auto\_refresh [true] )  
/jenkins/view/All/job/develenv/search/ (q [search] )  
/sonar/resource/index/242 (tab [violations] )  
/jenkins/doFingerprintCheck (name [] Submit [Check] )  
/jenkins/job/JSSample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PythonExample/rssAll (flavor [rss20] )  
/hudson/job/JSSample/disable ()  
/jenkins/job/PHPSSample/ws (auto\_refresh [true] )  
/hudson/job/test-develenv/disable ()  
/sonar/feeds/project/com.softwaresano.develenv:GroovySample (category [Alert] )  
/jenkins/job/test-develenv/ws/rssAll (flavor [rss20] )  
/hudson/job/flexSample/ (auto\_refresh [false] )

/jenkins/job/backupDevelenv/ (auto\_refresh [false] )  
/jenkins/view/develenv%20samples/job/test-develenv/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/j2meSample/rssAll (flavor [rss20] )  
/jenkins/people/ (auto\_refresh [true] )  
/jenkins/job/test-develenv/changes (auto\_refresh [true] )  
/jenkins/job/flexSample/changes (auto\_refresh [true] )  
/jenkins/job/PHPSSample/rssChangelog (flavor [rss20] )  
/jenkins/job/web-calculator/changes (auto\_refresh [false] )  
/jenkins/job/web-calculator/buildTimeTrend (auto\_refresh [false] )  
/hudson/job/JSSample/rssFailed (flavor [rss20] )  
/jenkins/job/SeleniumGridExample/buildTimeTrend (auto\_refresh [true] )  
/jenkins/job/JSSample/disable ()  
/jenkins/view/All/job/PHPSSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/flexSample/rssAll (flavor [rss20] )  
/jenkins/job/web-calculator/rssAll (flavor [rss20] )  
/hudson/job/test-develenv/ (auto\_refresh [false] )  
/sonar/resource/index/7 (tab [violations] )  
/hudson/job/CppSample/rssAll (flavor [rss20] )  
/hudson/job/CSSample/changes (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/backupDevelenv/search/ (q [search] )  
/jenkins/job/CSSample/ws/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/j2meSample/disable ()  
/sonar/plugins/resource/301 (page [CsvExportPage] )  
/hudson/job/web-calculator/ws (auto\_refresh [true] )  
/jenkins/job/standalone-archetype/buildTimeTrend (auto\_refresh [true] )  
/hudson/job/flexSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/CSSample/disable ()  
/hudson/job/develenv/enable ()  
/jenkins/view/develenv%20samples/job/web-calculator/jswidgets/ (auto\_refresh [false] )  
/jenkins/view/All/job/SeleniumGridExample/rssFailed (flavor [rss20] )  
/sonar/images/asc12.png (1328034139 [])  
/docs/downloadingVM.php (size [2653M] route [public/downloads/develenv\_ubuntu\_1110-1.9.0.ova] c...)  
/docs/selenium/gridConsole.php (config [true] configDebug [true] )  
/hudson/job/CppSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/develenv/rssFailed (flavor [rss20] )  
/hudson/job/flexSample/changes (auto\_refresh [true] )  
/hudson/job/GroovySample/changes (auto\_refresh [true] )  
/jenkins/view/All/job/backupDevelenv/enable ()  
/jenkins/job/backupDevelenv/search/ (q [search] )  
/jenkins/job/web-calculator/modules (auto\_refresh [false] )  
/hudson/job/develenv/ws/rssAll (flavor [rss20] )  
/hudson/job/SeleniumGridExample/ (auto\_refresh [false] )  
/hudson/job/backupDevelenv/ws/rssAll (flavor [rss20] )  
/jenkins/job/CppSample/ws/rssAll (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/test-develenv/ (auto\_refresh [false] )  
/jenkins/job/PythonExample/search/ (q [search] )  
/jenkins/view/develenv%20samples/job/test-calculator/ (auto\_refresh [true] )  
/jenkins/job/JSSample/ws/rssAll (flavor [rss20] )  
/jenkins/view/All/job/GroovySample/search/ (q [search] )  
/jenkins/view/develenv%20samples/job/GroovySample/ (auto\_refresh [true] )  
/jenkins/view/All/job/develenv/rssFailed (flavor [rss20] )  
/sonar/dashboard/index/385 (search [Buscar] period [1] sort [1] cmp\_dist [class\_complexity\_distrib...] )  
/jenkins/view/develenv%20samples/job/standalone-archetype/ (auto\_refresh [true] )  
/hudson/job/JSSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/flexSample/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/CSSample/rssAll (flavor [rss20] )  
/jenkins/job/PHPSSample/rssFailed (flavor [rss20] )  
/jenkins/view/eXperimental/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/backupDevelenv/rssFailed (flavor [rss20] )  
/sonar/dashboard/index/380 (search [Buscar] period [1] sort [1] cmp\_dist [file\_complexity\_distribu...] )  
/jenkins/static/9f5bcf50/job/test-calculator/disable ()  
/jenkins/view/develenv%20samples/job/GroovySample/jswidgets/ (auto\_refresh [false] )  
/hudson/job/PythonExample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/eXperimental/rssAll (flavor [rss20] )  
/jenkins/job/test-calculator/ws (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/develenv/ (auto\_refresh [false] )  
/jenkins/view/All/job/SeleniumGridExample/search/ (q [search] )

/jenkins/job/develenv/enable ()  
/jenkins/view/develenv%20samples/job/PythonExample/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/web-calculator/rssFailed (flavor [rss20] )  
/sonar/resource/index/377 (tab [violations] )  
/sonar/resource/index/295 (metric [blocker\_violations] tab [violations] )  
/hudson/job/JMeterExample/ws/ (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/CSSample/ (auto\_refresh [true] )  
/jenkins/job/test-develenv/rssAll (flavor [rss20] )  
/jenkins/job/CSSample/changes (auto\_refresh [true] )  
/jenkins/job/j2meSample/modules (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/j2meSample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/job/flexSample/ws/rssAll (flavor [rss20] )  
/sonar(feeds/project/ironman1:PHPSample (category [Alert] )  
/hudson/job/GroovySample/rssChangelog (flavor [rss20] )  
/jenkins/job/j2meSample/changes (auto\_refresh [true] )  
/jenkins/job/flexSample/disable ()  
/jenkins/view/All/job/test-develenv/disable ()  
/jenkins/job/SeleniumGridExample/ws/rssAll (flavor [rss20] )  
/hudson/job/GroovySample/ws (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/test-develenv/disable ()  
/jenkins/view/develenv%20samples/job/PythonExample/rssFailed (flavor [rss20] )  
/jenkins/job/PHPSample/ws/hudson\_docs/pdepend.svg (auto\_refresh [true] )  
/jenkins/job/CSSample/ (auto\_refresh [false] )  
/hudson/job/GroovySample/ws/rssAll (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/backupDevelenv/enable ()  
/hudson/job/test-develenv/rssFailed (flavor [rss20] )  
/hudson/job/PythonExample/changes (auto\_refresh [true] )  
/hudson/job/PHPSample/rssChangelog (flavor [rss20] )  
/sonar/drilldown/violations/com.softwaresano.develenv:CSSample (severity [BLOCKER] )  
/hudson/job/CppSample/ws/rssAll (flavor [rss20] )  
/jenkins/job/test-calculator/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/PHPSample/ (auto\_refresh [false] )  
/jenkins/job/j2meSample/ws/rssFailed (flavor [rss20] )  
/nexus/js/repoServer/nexus-plugin-console-plugin-all.js (1.9.2.4 [] )  
/sonar/images/tendency/-2-black-small.png (1328034139 [] )  
/jenkins/view/develenv%20samples/job/PythonExample/ (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/CppSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/standalone-archetype/disable ()  
/jenkins/job/backupDevelenv/ws/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-develenv/jswidgets/health/ (skipDescription [true] html [true] )  
/hudson/job/SeleniumGridExample/browser=firefox/rssAll (flavor [rss20] )  
/jenkins/job/JMeterExample/ws/rssChangelog (flavor [rss20] )  
/jenkins/job/flexSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/CppSample/rssFailed (flavor [rss20] )  
/hudson/job/PythonExample/rssAll (flavor [rss20] )  
/hudson/job/web-calculator/ws/rssAll (flavor [rss20] )  
/jenkins/job/PHPSample/ws/hudson\_docs/ (auto\_refresh [true] )  
/jenkins/projectRelationship (lhs [] rhs [] Submit [Compare] )  
/hudson/job/CSSample/disable ()  
/jenkins/view/develenv%20samples/job/develenv/rssAll (flavor [rss20] )  
/jenkins/job/PythonExample/ws (auto\_refresh [true] )  
/jenkins/job/JMeterExample/rssChangelog (flavor [rss20] )  
/jenkins/job/flexSample/ws/rssFailed (flavor [rss20] )  
/hudson/job/PythonExample/rssFailed (flavor [rss20] )  
/jenkins/job/JMeterExample/ws/ (auto\_refresh [true] )  
/hudson/job/test-develenv/ws/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/GroovySample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/JSSample/rssAll (flavor [rss20] )  
/sonar/images/links/scm\_dev.png (1328034139 [] )  
/jenkins/view/All/job/CSSample/rssAll (flavor [rss20] )  
/hudson/job/CSSample/ws/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/flexSample/disable ()  
/jenkins/job/test-calculator/search/ (q [search] )  
/sonar/drilldown/measures/39 (metric [comment\_lines\_density] highlight [duplicated\_lines\_density] )  
/hudson/job/backupDevelenv/ws/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/standalone-archetype/rssFailed (flavor [rss20] )  
/hudson/job/standalone-archetype/rssAll (flavor [rss20] )

/jenkins/job/SeleniumGridExample/ws/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/JMeterExample/rssFailed (flavor [rss20] )  
/jenkins/job/PHPSSample/ws/rssFailed (flavor [rss20] )  
/hudson/job/JMeterExample/rssChangelog (flavor [rss20] )  
/hudson/job/SeleniumGridExample/rssChangelog (flavor [rss20] )  
/sonar/feeds/project/com.softwaresano.develenv:JSSample (category [Alert] )  
/jenkins/job/CSSample/rssChangelog (flavor [rss20] )  
/hudson/job/test-calculator/changes (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/JMeterExample/rssChangelog (flavor [rss20] )  
/jenkins/job/JMeterExample/search/ (q [search] )  
/jenkins/job/test-calculator/disable ()  
/jenkins/job/flexSample/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/PHPSSample/disable ()  
/jenkins/view/develenv%20samples/job/flexSample/disable ()  
/jenkins/view/develenv%20samples/job/j2meSample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/j2meSample/rssChangelog (flavor [rss20] )  
/jenkins/job/standalone-archetype/ws/ (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/test-develenv/rssChangelog (flavor [rss20] )  
/jenkins/job/CSSample/buildTimeTrend (auto\_refresh [true] )  
/jenkins/job/CppSample/disable ()  
/jenkins/view/develenv%20samples/job/JMeterExample/jswidgets/ (auto\_refresh [false] )  
/hudson/job/JSSample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PHPSSample/jswidgets/ (auto\_refresh [false] )  
/hudson/job/PHPSSample/changes (auto\_refresh [true] )  
/hudson/job/GroovySample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/standalone-archetype/rssAll (flavor [rss20] )  
/sonar/feeds/project/com.softwaresano.examples.calculator:web-calculator (category [Alert] )  
/jenkins/job/PythonExample/ws/rssChangelog (flavor [rss20] )  
/jenkins/job/test-calculator/ (auto\_refresh [false] )  
/sonar/drilldown/violations/ironman1:PHPSSample (severity [BLOCKER] )  
/jenkins/job/JSSample/rssAll (flavor [rss20] )  
/jenkins/view/All/job/JSSample/disable ()  
/jenkins/static/9f5bcf50/job/CSSample/ (auto\_refresh [false] )  
/jenkins/job/backupDevelenv/ws/ (auto\_refresh [true] )  
/jenkins/view/All/job/PythonExample/disable ()  
/jenkins/static/9f5bcf50/job/SeleniumGridExample/rssChangelog (flavor [rss20] )  
/jenkins/job/CSSample/ws/rssAll (flavor [rss20] )  
/jenkins/job/SeleniumGridExample/rssChangelog (flavor [rss20] )  
/jenkins/job/web-calculator/ws/rssFailed (flavor [rss20] )  
/jenkins/job/test-develenv/search/ (q [search] )  
/jenkins/view/eXperimental/search/ (q [search] )  
/hudson/job/j2meSample/ws (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/PythonExample/search/ (q [search] )  
/jenkins/job/develenv/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-calculator/rssAll (flavor [rss20] )  
/hudson/job/develenv/rssAll (flavor [rss20] )  
/jenkins/job/PHPSSample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-develenv/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/JSSample/rssAll (flavor [rss20] )  
/sonar/dashboard/index/393 (search [Buscar] period [1] sort [1] cmp\_dist [class\_complexity\_distrib...] )  
/hudson/job/standalone-archetype/ws/rssChangelog (flavor [rss20] )  
/hudson/job/test-develenv/ws/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/CppSample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/view/develenv%20samples/job/CSSample/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/CppSample/ (auto\_refresh [false] )  
/hudson/job/SeleniumGridExample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PHPSSample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/flexSample/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/test-calculator/search/ (q [search] )  
/jenkins/job/develenv/buildTimeTrend (auto\_refresh [true] )  
/jenkins/job/CSSample/ws (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/web-calculator/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/ (auto\_refresh [false] )  
/sonar/feeds/project/com.softwaresano.develenv:CSSample (category [Alert] )  
/jenkins/static/9f5bcf50/job/PythonExample/rssAll (flavor [rss20] )  
/jenkins/job/JMeterExample/ (auto\_refresh [false] )  
/jenkins/job/CSSample/rssFailed (flavor [rss20] )

/jenkins/job/PHPSSample/changes (auto\_refresh [true] )  
/jenkins/ (auto\_refresh [true] )  
/jenkins/view/All/job/CppSample/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/web-calculator/ (auto\_refresh [true] )  
/jenkins/job/web-calculator/disable ()  
/sonar/resource/index/247 (tab [violations] )  
/jenkins/view/All/job/j2meSample/ (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/develenv/search/ (q [search] )  
/jenkins/job/CSSample/rssAll (flavor [rss20] )  
/hudson/job/JSSample/ws (auto\_refresh [true] )  
/jenkins/job/JMeterExample/ws/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/backupDevelenv/ (auto\_refresh [true] )  
/hudson/job/GroovySample/ws/rssChangelog (flavor [rss20] )  
/jenkins/job/test-calculator/changes (auto\_refresh [true] )  
/jenkins/view/All/job/CppSample/disable ()  
/hudson/job/GroovySample/rssAll (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/JMeterExample/rssAll (flavor [rss20] )  
/nexus/static/js/nexus-ldap-realm-plugin-all.js (1.9.2.4 [] )  
/sonar/plugins/resource/216 (page [CsvExportPage] )  
/sonar/images/priority/BLOCKER.png (1328034139 [] )  
/jenkins/job/web-calculator/ws (auto\_refresh [false] )  
/jenkins/job/SeleniumGridExample/rssAll (flavor [rss20] )  
/sonar/plugins/resource/158 (page [CsvExportPage] )  
/jenkins/job/develenv/ (auto\_refresh [false] )  
/sonar/drilldown/violations/com.softwaresano.examples:j2meSample (rule [pmd:CompareObjectsWithEquals] severity [BLOCKER] rule [MAJOR] )  
/hudson/job/standalone-archetype/changes (auto\_refresh [true] )  
/jenkins/job/JSSample/ws/ (auto\_refresh [true] )  
/jenkins/job/CppSample/ (auto\_refresh [false] )  
/hudson/job/SeleniumGridExample/browser=chrome/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/backupDevelenv/rssChangelog (flavor [rss20] )  
/jenkins/job/j2meSample/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/SeleniumGridExample/disable ()  
/jenkins/view/All/job/backupDevelenv/rssFailed (flavor [rss20] )  
/jenkins/job/CppSample/buildTimeTrend (auto\_refresh [true] )  
/jenkins/computer/ (auto\_refresh [false] )  
/jenkins/view/develenv%20samples/job/backupDevelenv/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-develenv/ (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/builds (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/flexSample/search/ (q [search] )  
/jenkins/view/All/job/JSSample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/SeleniumGridExample/disable ()  
/jenkins/view/All/job/SeleniumGridExample/rssChangelog (flavor [rss20] )  
/jenkins/job/standalone-archetype/ws (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/JMeterExample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/static/9f5bcf50/job/GroovySample/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/PythonExample/search/ (q [search] )  
/jenkins/view/All/job/standalone-archetype/search/ (q [search] )  
/jenkins/view/All/job/PythonExample/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/JMeterExample/rssChangelog (flavor [rss20] )  
/jenkins/job/CSSample/ws/rssChangelog (flavor [rss20] )  
/jenkins/job/test-develenv/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/PythonExample/rssFailed (flavor [rss20] )  
/jenkins/job/backupDevelenv/rssFailed (flavor [rss20] )  
/sonar/resource/index/387 (tab [violations] )  
/sonar/feeds/project/com.softwaresano.develenv:CppSample (category [Alert] )  
/jenkins/job/JSSample/search/ (q [search] )  
/jenkins/view/All/job/PythonExample/ (auto\_refresh [true] )  
/jenkins/job/PythonExample/ (auto\_refresh [false] )  
/jenkins/static/9f5bcf50/job/PythonExample/disable ()  
/sonar/plugins/resource/1 (page [CsvExportPage] )  
/sonar/dashboard/index/216 (search [Buscar] period [1] sort [1] cmp\_dist [class\_complexity\_distrib...] )  
/jenkins/job/PythonExample/ws/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/flexSample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/view/All/job/SeleniumGridExample/ (auto\_refresh [true] )  
/jenkins/view/eXperimental/ (auto\_refresh [false] )  
/jenkins/view/All/job/GroovySample/rssFailed (flavor [rss20] )

/sonar/resource/index/297 (metric [blocker\_violations] )  
/jenkins/static/9f5bcf50/job/GroovySample/rssFailed (flavor [rss20] )  
/hudson/job/web-calculator/rssChangelog (flavor [rss20] )  
/sonar/drilldown/measures/301 (metric [comment\_lines\_density] highlight [duplicated\_lines\_density] )  
/jenkins/view/develenv%20samples/job/develenv/jswidgets/health/ (skipDescription [true] html [true] )  
/sonar/resource/index/263 (metric [duplicated\_lines\_density] )  
/jenkins/view/All/job/j2meSample/search/ (q [search] )  
/jenkins/job/JMeterExample/ws (auto\_refresh [true] )  
/sonar/dashboard/index/2 (search [Buscar] period [1] sort [1] D [A] asc [true] did [1] )  
/jenkins/static/9f5bcf50/job/PythonExample/rssChangelog (flavor [rss20] )  
/jenkins/view/All/search/ (q [search] )  
/sonar/images/transparent.gif (1328034139 [] )  
/sonar/api/plugins/Pdfreport/getReport (resource [400] )  
/jenkins/job/PHPSSample/ws/hudson\_docs/rssFailed (flavor [rss20] )  
/jenkins/job/test-calculator/rssAll (flavor [rss20] )  
/jenkins/job/SeleniumGridExample/ws/rssFailed (flavor [rss20] )  
/sonar/ (search [Buscar] period [1] sort [1] D [A] asc [true] )  
/hudson/job/SeleniumGridExample/browser=firefox/rssFailed (flavor [rss20] )  
/hudson/job/GroovySample/ws/ (auto\_refresh [true] )  
/hudson/job/web-calculator/rssFailed (flavor [rss20] )  
/hudson/job/flexSample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/PythonExample/rssFailed (flavor [rss20] )  
/hudson/job/flexSample/ws/ (auto\_refresh [true] )  
/jenkins/job/GroovySample/ws/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/standalone-archetype/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/iconSize (24x24 [] 16x16 [] 32x32 [] )  
/hudson/job/test-develenv/ws/rssAll (flavor [rss20] )  
/sonar/images/tendency/2-black-small.png (1328034139 [] )  
/sonar/javascripts/jit-yc.js (1328034139 [] )  
/jenkins/static/9f5bcf50/job/develenv/rssAll (flavor [rss20] )  
/hudson/job/j2meSample/rssFailed (flavor [rss20] )  
/jenkins/job/flexSample/ws/rssChangelog (flavor [rss20] )  
/sonar/drilldown/violations/com.softwaresano.develenv:JSSample (rule [JavaScript:UNDEF] severity [BLOCKER] rule\_sev [CRITICAL]  
/jenkins/job/j2meSample/ws (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/PHPSSample/jswidgets/health/ (skipDescription [true] html [true] )  
/sonar/drilldown/violations/com.softwaresano.examples.calculator:test-calculator (rule  
[checkstyle:com.puppycrawl.tools.checkstyle.checks.coding.Redunda...])  
/jenkins/view/develenv%20samples/job/j2meSample/rssFailed (flavor [rss20] )  
/sonar/resource/index/371 (tab [violations] )  
/jenkins/view/develenv%20samples/job/JMeterExample/disable ()  
/hudson/job/flexSample/rssFailed (flavor [rss20] )  
/sonar/plugins/home/org.sonar.plugins.radiator.RadiatorPage (search [Buscar] color\_metric [new\_it\_line\_coverage] layout [false] siz  
/jenkins/static/9f5bcf50/ (auto\_refresh [true] )  
/jenkins/job/standalone-archetype/ws/rssChangelog (flavor [rss20] )  
/jenkins/view/All/people/ (auto\_refresh [false] )  
/hudson/job/standalone-archetype/ws (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/develenv/jswidgets/ (auto\_refresh [false] )  
/sonar/drilldown/measures/385 (metric [coverage] highlight [line\_coverage] )  
/hudson/job/standalone-archetype/ws/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-develenv/search/ (q [search] )  
/jenkins/view/All/job/flexSample/ (auto\_refresh [true] )  
/jenkins/view/All/job/JSSample/search/ (q [search] )  
/jenkins/job/CSSample/search/ (q [search] )  
/jenkins/view/QA/rssAll (flavor [rss20] )  
/hudson/job/develenv/rssChangelog (flavor [rss20] )  
/sonar/plugins/resource/400 (page [CsvExportPage] )  
/jenkins/static/9f5bcf50/job/standalone-archetype/rssAll (flavor [rss20] )  
/jenkins/job/web-calculator/rssChangelog (flavor [rss20] )  
/jenkins/job/GroovySample/ws (auto\_refresh [true] )  
/jenkins/job/GroovySample/rssFailed (flavor [rss20] )  
/hudson/job/flexSample/rssAll (flavor [rss20] )  
/jenkins/job/test-calculator/ws/ (auto\_refresh [true] )  
/jenkins/view/All/job/flexSample/search/ (q [search] )  
/jenkins/view/All/job/test-develenv/rssChangelog (flavor [rss20] )  
/hudson/job/GroovySample/ (auto\_refresh [false] )  
/jenkins/job/standalone-archetype/rssFailed (flavor [rss20] )  
/jenkins/job/standalone-archetype/rssAll (flavor [rss20] )

/jenkins/job/JMeterExample/changes (auto\_refresh [true] )  
/jenkins/view/All/job/CSSample/disable ()  
/jenkins/search/ (q [search] )  
/jenkins/job/develenv/search/ (q [search] )  
/jenkins/static/9f5bcf50/job/test-calculator/ (auto\_refresh [false] )  
/hudson/job/CSSample/ws/rssFailed (flavor [rss20] )  
/jenkins/job/JMeterExample/rssAll (flavor [rss20] )  
/jenkins/job/JMeterExample/ws/rssFailed (flavor [rss20] )  
/sonar/resource/index/370 (tab [violations] )  
/hudson/job/PHPSSample/disable ()  
/jenkins/job/PHPSSample/ws/rssAll (flavor [rss20] )  
/jenkins/job/CppSample/ws/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/standalone-archetype/ (auto\_refresh [false] )  
/sonar/drilldown/measures/216 (metric [duplicated\_lines\_density] highlight [duplicated\_lines\_density] )  
/hudson/job/test-calculator/ws (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/JMeterExample/rssAll (flavor [rss20] )  
/sonar/dashboard/index/158 (search [Buscar] period [1] sort [1] cmp\_dist [class\_complexity\_distrib...] )  
/jenkins/job/standalone-archetype/disable ()  
/docs/downloadVMOk.php (artifact [develenv\_ubuntu\_1110-1.9.0.ova] )  
/sonar/images/tick.png (1328034139 [] )  
/jenkins/job/test-calculator/modules (auto\_refresh [true] )  
/hudson/job/develenv/ws (auto\_refresh [true] )  
/hudson/job/SeleniumGridExample/browser=chrome/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-calculator/rssFailed (flavor [rss20] )  
/jenkins/job/j2meSample/ws/ (auto\_refresh [true] )  
/jenkins/job/standalone-archetype/ws/rssFailed (flavor [rss20] )  
/jenkins/job/PythonExample/disable ()  
/jenkins/view/All/job/flexSample/rssFailed (flavor [rss20] )  
/hudson/job/PythonExample/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/SeleniumGridExample/rssAll (flavor [rss20] )  
/jenkins/view/All/job/JSSample/ (auto\_refresh [true] )  
/sonar/javascripts/sonar.js (1328034139 [] )  
/sonar/plugins/resource/380 (page [CsvExportPage] )  
/jenkins/job/JSSample/rssFailed (flavor [rss20] )  
/jenkins/job/SeleniumGridExample/browser=firefox/search/ (q [search] )  
/hudson/job/backupDevelenv/ (auto\_refresh [false] )  
/jenkins/legend (auto\_refresh [false] )  
/hudson/job/develenv/ws/ (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/CSSample/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/flexSample/rssAll (flavor [rss20] )  
/hudson/job/j2meSample/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/SeleniumGridExample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/view/All/job/GroovySample/disable ()  
/jenkins/job/develenv/rssFailed (flavor [rss20] )  
/hudson/job/CppSample/rssFailed (flavor [rss20] )  
/jenkins/job/JSSample/ (auto\_refresh [false] )  
/hudson/job/JMeterExample/ (auto\_refresh [false] )  
/jenkins/job/GroovySample/ws/rssChangelog (flavor [rss20] )  
/hudson/job/CSSample/rssAll (flavor [rss20] )  
/hudson/job/standalone-archetype/ (auto\_refresh [false] )  
/hudson/job/j2meSample/disable ()  
/jenkins/view/All/job/JMeterExample/ (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/j2meSample/rssFailed (flavor [rss20] )  
/jenkins/view/QA/builds (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/PHPSSample/search/ (q [search] )  
/hudson/job/PHPSSample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/test-calculator/ (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/test-calculator/rssChangelog (flavor [rss20] )  
/jenkins/job/backupDevelenv/changes (auto\_refresh [true] )  
/hudson/job/SeleniumGridExample/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-calculator/jswidgets/ (auto\_refresh [false] )  
/sonar/images/loading.gif (1328034139 [] )  
/jenkins/job/SeleniumGridExample/rssFailed (flavor [rss20] )  
/hudson/job/web-calculator/changes (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/CSSample/jswidgets/ (auto\_refresh [false] )  
/jenkins/job/CppSample/search/ (q [search] )  
/hudson/job/CppSample/ws (auto\_refresh [true] )

/jenkins/view/develenv%20samples/job/SeleniumGridExample/search/ (q [search] )  
/sonar/resource/index/299 (metric [blocker\_violations] )  
/hudson/job/j2meSample/ws/ (auto\_refresh [true] )  
/hudson/job/test-calculator/ (auto\_refresh [false] )  
/jenkins/job/j2meSample/buildTimeTrend (auto\_refresh [true] )  
/jenkins/view/All/job/GroovySample/rssChangelog (flavor [rss20] )  
/hudson/job/JSSample/ws/rssChangelog (flavor [rss20] )  
/jenkins/view/All/job/CppSample/ (auto\_refresh [true] )  
/jenkins/job/j2meSample/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/JMeterExample/rssAll (flavor [rss20] )  
/jenkins/job/web-calculator/build (delay [0sec] )  
/jenkins/job/develenv/ws/ (auto\_refresh [true] )  
/sonar/filters/index/1 (search [Buscar] period [1] sort [1] asc [true] )  
/jenkins/static/9f5bcf50/job/test-calculator/rssFailed (flavor [rss20] )  
/hudson/job/web-calculator/ (auto\_refresh [false] )  
/sonar/drilldown/violations/com.softwaresano.archetypes:standalone-archetype (severity [BLOCKER] )  
/jenkins/computer/(master)/ (auto\_refresh [true] )  
/jenkins/job/backupDevelenv/enable ()  
/jenkins/job/test-calculator/ws/rssChangelog (flavor [rss20] )  
/hudson/job/develenv/ (auto\_refresh [false] )  
/jenkins/view/All/job/j2meSample/rssChangelog (flavor [rss20] )  
/hudson/job/JMeterExample/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/test-develenv/rssAll (flavor [rss20] )  
/hudson/job/CppSample/ws/rssFailed (flavor [rss20] )  
/jenkins/view/All/ (auto\_refresh [false] )  
/jenkins/view/develenv%20samples/job/CSSample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/static/9f5bcf50/job/flexSample/disable ()  
/sonar/filters/index/4 (search [Buscar] period [1] sort [23] asc [false] )  
/jenkins/view/All/job/test-calculator/rssChangelog (flavor [rss20] )  
/jenkins/job/GroovySample/rssAll (flavor [rss20] )  
/hudson/job/PythonExample/ws/ (auto\_refresh [true] )  
/hudson/job/JSSample/ws/ (auto\_refresh [true] )  
/jenkins/view/All/job/GroovySample/ (auto\_refresh [true] )  
/hudson/job/flexSample/ws/rssChangelog (flavor [rss20] )  
/jenkins/job/web-calculator/ws/rssAll (flavor [rss20] )  
/jenkins/job/develenv/ws/rssFailed (flavor [rss20] )  
/jenkins/job/SeleniumGridExample/ (auto\_refresh [false] )  
/hudson/job/CppSample/changes (auto\_refresh [true] )  
/jenkins/view/All/job/standalone-archetype/rssChangelog (flavor [rss20] )  
/sonar/drilldown/measures/158 (metric [it\_coverage] highlight [it\_line\_coverage] )  
/jenkins/view/All/job/CSSample/rssFailed (flavor [rss20] )  
/jenkins/job/JSSample/ws (auto\_refresh [true] )  
/jenkins/view/All/job/web-calculator/rssChangelog (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/develenv/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/CSSample/disable ()  
/jenkins/view/All/job/CppSample/search/ (q [search] )  
/jenkins/view/QA/ (auto\_refresh [false] )  
/jenkins/static/9f5bcf50/job/CSSample/rssChangelog (flavor [rss20] )  
/sonar/feeds/project/com.softwaresano.examples:j2meSample (category [Alert] )  
/hudson/job/PHPSSample/ws/ (auto\_refresh [true] )  
/jenkins/view/All/job/JMeterExample/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/backupDevelenv/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/test-calculator/rssChangelog (flavor [rss20] )  
/hudson/job/PHPSSample/ (auto\_refresh [false] )  
/jenkins/view/develenv%20samples/job/flexSample/rssChangelog (flavor [rss20] )  
/jenkins/job/backupDevelenv/rssChangelog (flavor [rss20] )  
/hudson/job/develenv/ws/rssFailed (flavor [rss20] )  
/hudson/job/JMeterExample/disable ()  
/sonar/drilldown/measures/400 (metric [tests] )  
/jenkins/view/develenv%20samples/job/backupDevelenv/rssChangelog (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/web-calculator/rssFailed (flavor [rss20] )  
/hudson/job/backupDevelenv/enable ()  
/hudson/job/CppSample/ws/ (auto\_refresh [true] )  
/hudson/job/PHPSSample/rssFailed (flavor [rss20] )  
/jenkins/job/web-calculator/ws/ (auto\_refresh [false] )  
/sonar/images/links/external.png (1328034139 [] )  
/jenkins/view/develenv%20samples/job/standalone-archetype/rssFailed (flavor [rss20] )

/jenkins/view/All/job/CSample/search/ (q [search] )  
/jenkins/job/GroovySample/search/ (q [search] )  
/jenkins/view/develenv%20samples/job/CppSample/jswidgets/ (auto\_refresh [false] )  
/jenkins/job/GroovySample/buildTimeTrend (auto\_refresh [true] )  
/jenkins/view/All/job/backupDevelenv/search/ (q [search] )  
/jenkins/job/j2meSample/search/ (q [search] )  
/jenkins/view/develenv%20samples/job/j2meSample/search/ (q [search] )  
/jenkins/job/JSSample/changes (auto\_refresh [true] )  
/jenkins/view/All/job/JSSample/rssFailed (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/SeleniumGridExample/ (auto\_refresh [false] )  
/jenkins/view/develenv%20samples/job/web-calculator/rssAll (flavor [rss20] )  
/hudson/job/test-calculator/rssAll (flavor [rss20] )  
/jenkins/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PHPSSample/rssChangelog (flavor [rss20] )  
/hudson/job/j2meSample/ws/rssAll (flavor [rss20] )  
/jenkins/computer/(master)/search/ (q [search] )  
/jenkins/job/SeleniumGridExample/ws (auto\_refresh [true] )  
/sonar/dashboard/index/301 (search [Buscar] period [1] sort [1] cmp\_dist [class\_complexity\_distrib...] )  
/jenkins/static/9f5bcf50/job/JSSample/rssFailed (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/PythonExample/disable ()  
/hudson/job/standalone-archetype/rssFailed (flavor [rss20] )  
/jenkins/view/All/job/standalone-archetype/ (auto\_refresh [true] )  
/nexus/js/repoServer/nexus-rrb-plugin-all.js (1.9.2.4 [] )  
/jenkins/job/test-develenv/ws/rssFailed (flavor [rss20] )  
/hudson/job/test-develenv/rssAll (flavor [rss20] )  
/jenkins/job/CppSample/rssAll (flavor [rss20] )  
/jenkins/job/JSSample/buildTimeTrend (auto\_refresh [true] )  
/hudson/job/JSSample/changes (auto\_refresh [true] )  
/sonar/resource/index/382 (tab [violations] )  
/jenkins/job/CSample/ws/ (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/web-calculator/ (auto\_refresh [false] )  
/jenkins/projectRelationship-help (auto\_refresh [true] )  
/jenkins/job/backupDevelenv/ws (auto\_refresh [true] )  
/jenkins/static/9f5bcf50/job/j2meSample/rssChangelog (flavor [rss20] )  
/jenkins/job/PythonExample/buildTimeTrend (auto\_refresh [true] )  
/jenkins/job/GroovySample/changes (auto\_refresh [true] )  
/jenkins/cigame/ (auto\_refresh [true] )  
/jenkins/jswidgets/runs/ (count [5] html [true] )  
/jenkins/job/test-calculator/buildTimeTrend (auto\_refresh [true] )  
/hudson/job/standalone-archetype/ws/rssFailed (flavor [rss20] )  
/hudson/job/JMeterExample/rssAll (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/test-develenv/disable ()  
/jenkins/view/develenv%20samples/job/flexSample/jswidgets/ (auto\_refresh [false] )  
/jenkins/job/PythonExample/changes (auto\_refresh [true] )  
/hudson/job/CSample/ws/ (auto\_refresh [true] )  
/jenkins/job/standalone-archetype/changes (auto\_refresh [true] )  
/sonar/dashboard/index/com.softwaresano.examples.calculator:test-calculator (cmp\_dist [function\_complexity\_distribution] cmp\_dist [class\_complexity...] )  
/hudson/job/test-develenv/ws/ (auto\_refresh [true] )  
/jenkins/view/All/job/JMeterExample/search/ (q [search] )  
/hudson/job/web-calculator/ws/ (auto\_refresh [true] )  
/jenkins/job/SeleniumGridExample/browser=chrome/search/ (q [search] )  
/jenkins/view/develenv%20samples/job/standalone-archetype/jswidgets/ (auto\_refresh [false] )  
/jenkins/view/All/job/develenv/rssAll (flavor [rss20] )  
/jenkins/view/develenv%20samples/job/web-calculator/disable ()  
/jenkins/view/develenv%20samples/job/flexSample/ (auto\_refresh [true] )  
/jenkins/view/develenv%20samples/job/GroovySample/jswidgets/health/ (skipDescription [true] html [true] )  
/jenkins/view/develenv%20samples/job/web-calculator/jswidgets/health/ (skipDescription [true] html [true] )  
/hudson/job/j2meSample/ (auto\_refresh [false] )  
/jenkins/view/All/job/test-calculator/rssAll (flavor [rss20] )  
/jenkins/static/9f5bcf50/job/GroovySample/disable ()  
/jenkins/view/develenv%20samples/job/standalone-archetype/search/ (q [search] )  
/jenkins/jswidgets/ (auto\_refresh [true] )  
/jenkins/job/PHPSSample/disable ()  
/jenkins/job/GroovySample/disable ()  
/jenkins/view/develenv%20samples/job/CppSample/search/ (q [search] )  
/jenkins/job/web-calculator/rssFailed (flavor [rss20] )

```

/jenkins/job/backupDevelenv/buildTimeTrend (auto_refresh [true] )
/hudson/job/test-develenv/ws (auto_refresh [true] )
/hudson/job/test-calculator/ws/ (auto_refresh [true] )
/jenkins/static/9f5bcf50/job/JMeterExample/rssFailed (flavor [rss20] )
/jenkins/static/9f5bcf50/job/CppSample/disable ()
/jenkins/view/develenv%20samples/job/JSSample/ (auto_refresh [true] )
/jenkins/view/develenv%20samples/job/JMeterExample/ (auto_refresh [true] )
/hudson/job/PythonExample/ws/rssChangelog (flavor [rss20] )
/jenkins/job/j2meSample/build (delay [0sec] )
/sonar/reviews (severities[] [CRITICAL] author_login [] statuses[] false_positives ... )
/sonar/images/links/homepage.png (1328034139 [] )
/hudson/job/PHPSSample/ws (auto_refresh [true] )
/jenkins/job/flexSample/rssAll (flavor [rss20] )
/jenkins/view/develenv%20samples/job/j2meSample/jswidgets/ (auto_refresh [false] )
/jenkins/job/PHPSSample/ws/ (auto_refresh [true] )
/sonar/resource/index/373 (tab [violations] )
/hudson/job/JMeterExample/changes (auto_refresh [true] )
/jenkins/job/CppSample/ws (auto_refresh [true] )
/jenkins/static/9f5bcf50/job/JSSample/ (auto_refresh [false] )
/jenkins/static/9f5bcf50/job/PythonExample/ (auto_refresh [false] )
/jenkins/job/backupDevelenv/ws/rssChangelog (flavor [rss20] )
/jenkins/static/9f5bcf50/job/PHPSSample/rssFailed (flavor [rss20] )
/jenkins/static/9f5bcf50/job/standalone-archetype/rssChangelog (flavor [rss20] )
/hudson/job/test-develenv/rssChangelog (flavor [rss20] )
/jenkins/job/standalone-archetype/search/ (q [search] )
/jenkins/static/9f5bcf50/job/flexSample/rssFailed (flavor [rss20] )
/jenkins/job/SeleniumGridExample/changes (auto_refresh [true] )
/jenkins/job/PHPSSample/search/ (q [search] )
/jenkins/static/9f5bcf50/job/JSSample/rssChangelog (flavor [rss20] )
/hudson/job/PHPSSample/rssAll (flavor [rss20] )
/hudson/job/j2meSample/changes (auto_refresh [true] )
/jenkins/job/develenv/changes (auto_refresh [true] )
/sonar/plugins/resource/393 (page [CsvExportPage] )
/jenkins/job/test-develenv/ws/rssChangelog (flavor [rss20] )
/jenkins/static/9f5bcf50/job/web-calculator/disable ()
/jenkins/login (from [/jenkins/] )
/jenkins/job/web-calculator/ws/rssChangelog (flavor [rss20] )
/jenkins/view/All/job/standalone-archetype/rssAll (flavor [rss20] )
/sonar/images/priority/CRITICAL.png (1328034139 [] )
/jenkins/job/backupDevelenv/ws/rssAll (flavor [rss20] )
/jenkins/view/develenv%20samples/job/develenv/rssChangelog (flavor [rss20] )
/hudson/job/flexSample/ws/rssAll (flavor [rss20] )
/jenkins/job/j2meSample/disable ()
/sonar/dashboard/index/400 (search [Buscar] period [] sort [1] D [A] asc [true] did [1] )
/jenkins/view/develenv%20samples/job/j2meSample/ (auto_refresh [true] )
/jenkins/job/test-develenv/ (auto_refresh [false] )
/hudson/job/SeleniumGridExample/disable ()
/jenkins/static/9f5bcf50/job/backupDevelenv/rssChangelog (flavor [rss20] )
/sonar/resource/index/258 (metric [blocker_violations] )
/sonar/resource/index/262 (metric [duplicated_lines_density] )

```

Directory index found at /widgets/  
 Directory index found at /widgets/?C=N;O=D  
 Directory index found at /widgets/?C=M;O=A  
 Directory index found at /widgets/?C=S;O=A  
 Directory index found at /widgets/?C=D;O=A

### Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the

'Options' section of the client.

---

**Solution**

n/a

---

**Risk Factor**

None

---

**Plugin publication date:** 2001/05/04

**Plugin last modification date:** 2012/01/04

**PORT WWW (80/TCP)**

Plugin ID: [26194](#)

**Web Server Uses Plain Text Authentication Forms**

---

**Synopsis**

The remote web server might transmit credentials in cleartext.

**List of Hosts**

[10.95.102.158](#)

**Plugin Output**

Page : /jenkins/login?from=/jenkins/

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/jswidgets/

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/web-calculator/

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/static/9f5bcf50/

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/All/people/

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/All/builds

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/All/

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/projectRelationship

Destination page : j\_acegi\_security\_check

Input name : j\_password

Page : /jenkins/login?from=/jenkins/fingerprintCheck  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/computer/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/QA/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/eXperimental/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/backupDevelenv/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/CppSample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/CSSample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/develenv/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/flexSample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/GroovySample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/j2meSample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/JMeterExample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/JSSample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/PHPSample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/PythonExample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/SeleniumGridExample/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/standalone-archetype/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/test-calculator/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/job/test-develenv/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/legend  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /sonar/sessions/new  
Destination page : /sonar/sessions/login  
Input name : password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/test-develenv/jswidgets/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/backupDevelenv/jswidgets/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/develenv/jswidgets/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/standalone-archetype/jswidgets/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/test-calculator/jswidgets/

Destination page : j\_acegi\_security\_check  
Input name : j\_password

Page : /jenkins/login?from=/jenkins/view/develenv%20samples/job/SeleniumGridExample/jswidgets/  
Destination page : j\_acegi\_security\_check  
Input name : j\_password

---

### Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

---

### Solution

Make sure that every sensitive form transmits content over HTTPS.

---

### Risk Factor

Low/ CVSS Base Score: 2.6  
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

---

### Other references

[CWE:522](#)  
[CWE:523](#)  
[CWE:718](#)  
[CWE:724](#)

---

**Plugin publication date:** 2007/09/28  
**Plugin last modification date:** 2011/09/15

### PORT WWW (80/TCP)

Plugin ID: [39521](#)

### Backported Security Patch Detection (WWW)

---

#### Synopsis

Security patches are backported.

#### List of Hosts

[10.95.102.158](#)

#### Plugin Output

Give Nessus credentials to perform local checks.

---

### Description

Security patches may have been 'back ported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

---

**Solution**

N/A

---

**See also**

<http://www.nessus.org/u?d636c8c7>

---

**Risk Factor**

None

---

**Plugin publication date:** 2009/06/25

**Plugin last modification date:** 2011/03/18

**10.95.102.158**

**Scan Time**

Start time: Wed Feb 1 16:47:21 2012

End time: Wed Feb 1 18:14:55 2012

**Number of vulnerabilities**

High 0

Medium 4

Low 32

**Remote Host Information**

Operating System: Linux Kernel 2.6 on CentOS Linux release 6

DNS name: ci-bizframe.hi.inet

IP address: 10.95.102.158