Scan Report

May 13, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "RSUD Sumedang". The scan started at Thu May 13 05:46:42 2021 UTC and ended at Thu May 13 09:31:08 2021 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
36.78.27.51	1	8	1	0	0
Total: 1	1	8	1	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 10 results selected by the filtering described above. Before filtering there were 340 results.

2 Results per Host

2.1 36.78.27.51

Host scan start	Thu May 13 05:46:54 2021 UTC
Host scan end	Thu May 13 09:30:42 2021 UTC

Service (Port)	Threat Level
80/tcp	High
8181/tcp	Medium
80/tcp	Medium
8183/tcp	Medium
8182/tcp	Medium
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)
NVT: HTTP negative Content-Length buffer overflow

Summary
The web server was crashed by sending an invalid POST HTTP request with a negative Content-Length field.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker may exploit this flaw to disable the service or even execute arbitrary code on the system.

Solution
Solution type: VendorFix
Upgrade your web server.

Affected Software/OS
Null HTTPD 0.5.0

Vulnerability Detection Method
Details: `HTTP negative Content-Length buffer overflow`
OID:1.3.6.1.4.1.25623.1.0.11183

[return to 36.78.27.51]

2.1.2 Medium 8181/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213

References
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.kb.cert.org/vuls/id/867593
url: http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
url: https://www.owasp.org/index.php/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result
```
The cookies:
Set-Cookie: PHPSESSID=***replaced***; path=/
```

... continues on next page ...

... continued from previous page ...

are missing the "httpOnly" attribute.

Solution
Solution type: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS
Application with session handling in cookies.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: Missing 'httpOnly' Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.105925

References
url: https://www.owasp.org/index.php/HttpOnly
url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
The following input fields where identified (URL:input name):
http://rsud.sumedangkab.go.id:8181/:access_password

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

... continues on next page ...

. . . continued from previous page . . .

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 36.78.27.51]

2.1.3 Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213

References
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.kb.cert.org/vuls/id/867593
url: http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
url: https://www.owasp.org/index.php/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

[return to 36.78.27.51]

2.1.4 Medium 8183/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary

... continues on next page ...

... continued from previous page ...

Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213

References
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`bid: 9506`
`bid: 9561`
`bid: 11604`
`bid: 15222`
`bid: 19915`
`bid: 24456`
`bid: 33374`
`bid: 36956`

... continues on next page ...

... continued from previous page ...

```
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.kb.cert.org/vuls/id/867593
url: http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
url: https://www.owasp.org/index.php/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

[return to 36.78.27.51]

2.1.5 Medium 8182/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.kb.cert.org/vuls/id/867593
url: http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
url: https://www.owasp.org/index.php/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.0)
NVT: WordPress Multiple Vulnerabilities - July09

Summary
The host is running WordPress and is prone to Multiple Vulnerabilities.

Vulnerability Detection Result
`Vulnerable URL: http://rsud.sumedangkab.go.id:8182/wordpress/wp-settings.php`

Impact
Successful exploitation will allow attackers to view the content of plugins configuration pages, inject malicious scripting code, or gain knowledge of sensitive username information.

Solution
Solution type: VendorFix
Update to Version 2.8.1 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

WordPress version prior to 2.8.1 on all running platform.

Vulnerability Insight
- Error in 'wp-settings.php' which may disclose the sensitive information via a direct request.
- username of a post's author is placed in an HTML comment, which allows remote attackers to obtain sensitive information by reading the HTML source.
- Error occur when user attempt for failed login or password request depending on whether the user account exists, and it can be exploited by enumerate valid usernames.
- wp-admin/admin.php does not require administrative authentication to access the configuration of a plugin, which allows attackers to specify a configuration file in the page parameter via collapsing-archives/options.txt, related-ways-to-take-action/options.php, wp-security-scan/securityscan.php, akismet/readme.txt and wp-ids/ids-admin.php.

Vulnerability Detection Method
Details: `WordPress Multiple Vulnerabilities - July09`
OID:1.3.6.1.4.1.25623.1.0.800657

References
`cve: CVE-2009-2432`
`cve: CVE-2009-2431`
`cve: CVE-2009-2336`
`cve: CVE-2009-2335`
`cve: CVE-2009-2334`
`bid: 35581`
`bid: 35584`
`url: http://www.vupen.com/english/advisories/2009/1833`
`url: http://securitytracker.com/alerts/2009/Jul/1022528.html`
`url: http://www.securityfocus.com/archive/1/archive/1/504795/100/0/threaded`
`dfn-cert: DFN-CERT-2010-0125`
`dfn-cert: DFN-CERT-2009-1593`
`dfn-cert: DFN-CERT-2009-1208`
`dfn-cert: DFN-CERT-2009-1188`
`dfn-cert: DFN-CERT-2009-1144`
`dfn-cert: DFN-CERT-2009-1081`

Medium (CVSS: 5.0)
NVT: WordPress / WordPress MU Multiple Vulnerabilities - July09

Summary
The host is running WordPress / WordPress MU and is prone to multiple vulnerabilities

Vulnerability Detection Result
`Vulnerable URL: http://rsud.sumedangkab.go.id:8182/wordpress/wp-settings.php`

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to view the content of plugins configuration pages, inject malicious scripting code, or gain knowledge of sensitive username information.

Solution
Solution type: VendorFix
Update to Version 2.8.1 or later.

Affected Software/OS
WordPress / WordPress MU version prior to 2.8.1.

Vulnerability Insight
- Error in 'wp-settings.php' which may disclose sensitive information via a direct request.
- Error occur when user attempt for failed login or password request depending on whether the user account exists, and it can be exploited by enumerate valid usernames.
- Error in wp-admin/admin.php is does not require administrative authentication to access the configuration of a plugin, which allows attackers to specify a configuration file in the page parameter via collapsing-archives/options.txt, related-ways-to-take-action/options.php, wp-security-scan/securityscan.php, akismet/readme.txt and wp-ids/ids-admin.php.

Vulnerability Detection Method
Details: `WordPress / WordPress MU Multiple Vulnerabilities - July09`
OID:1.3.6.1.4.1.25623.1.0.800662

References
`cve: CVE-2009-2432`
`cve: CVE-2009-2336`
`cve: CVE-2009-2335`
`cve: CVE-2009-2334`
`bid: 35581`
`bid: 35584`
`url: http://www.vupen.com/english/advisories/2009/1833`
`url: http://securitytracker.com/alerts/2009/Jul/1022528.html`
`url: http://www.securityfocus.com/archive/1/archive/1/504795/100/0/threaded`
`dfn-cert: DFN-CERT-2010-0125`
`dfn-cert: DFN-CERT-2009-1593`
`dfn-cert: DFN-CERT-2009-1208`
`dfn-cert: DFN-CERT-2009-1188`
`dfn-cert: DFN-CERT-2009-1144`
`dfn-cert: DFN-CERT-2009-1081`

[return to 36.78.27.51]

2.1.6 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 231063527
Packet 2: 231063634
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091

References
```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 36.78.27.51]