Scan Report

August 19, 2026

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Asia/Taipei", which is abbreviated "CST". The task was "APP_TEST". The scan started at Wed Aug 19 11:43:59 2026 CST and ended at Wed Aug 19 12:14:03 2026 CST. 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	Critical	High	Medium	Low	Log	False P.
140.131.1.36 imoving.lhu.edu.tw	0	0	5	2	0	0
Total: 1	0	0	5	2	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 7 results selected by the filtering described above. Before filtering there were 86 results.

2 Results per Host

2.1 140.131.1.36

Host scan start Wed Aug 19 11:44:48 2026 CST
Host scan end Wed Aug 19 12:13:59 2026 CST

Service (Port)	Threat Level
80/tcp	Medium
443/tcp	Medium
22/tcp	Low
general/icmp	Low

2.1.1 Medium 80/tcp

Medium (CVSS: 5.0)

NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The cookie(s):
Set-Cookie: deviceClassification=%7B%22pagetype%22%3A%22compliant%22%2C%22platfo
↪rm%22%3A%22computer%22%2C%22browser%22%3A%22unknown%22%7D; expires=Wed, 19-Aug
↪-2026 03:59:48 GMT; Max-Age=***replaced***; path=/
is/are missing the "HttpOnly" cookie attribute.
```

Solution:
Solution type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

...continues on next page ...

... continued from previous page ...

Affected Software/OS
Any web application with session handling in cookies.

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

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-13T00:12:12+08:00`

References
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`
`http://imoving.lhu.edu.tw/phpmyadmin/:pma_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
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
Version used: `2023-09-07T13:05:21+08:00`

References
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_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 140.131.1.36]

2.1.2 Medium 443/tcp

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /min/?g=file-/common/javascript/lib/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://imoving.lhu.edu.tw/min/?g=file-/common/javascript/lib
↪/jquery-1.8.3.min.js
- Referenced at:   https://imoving.lhu.edu.tw/home/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T13:06:08+08:00`

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2026-1752
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2025-1803
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 5.0)

NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The cookie(s):
Set-Cookie: deviceClassification=%7B%22pagetype%22%3A%22compliant%22%2C%22platfo
↪rm%22%3A%22computer%22%2C%22browser%22%3A%22unknown%22%7D; expires=Wed, 19-Aug
↪-2026 03:59:58 GMT; Max-Age=***replaced***; path=/
is/are missing the "HttpOnly" cookie attribute.
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Affected Software/OS
Any web application with session handling in cookies.

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

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-13T00:12:12+08:00`

References
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Medium (CVSS: 5.0)

NVT: Missing 'Secure' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The cookie(s):
Set-Cookie: deviceClassification=%7B%22pagetype%22%3A%22compliant%22%2C%22platfo
↪rm%22%3A%22computer%22%2C%22browser%22%3A%22unknown%22%7D; expires=Wed, 19-Aug
↪-2026 03:59:58 GMT; Max-Age=***replaced***; path=/
is/are missing the "Secure" cookie attribute.
```

Solution:
Solution type: Mitigation
- Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Affected Software/OS
Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

Vulnerability Insight
The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.
This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.
Details: `Missing 'Secure' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.902661
Version used: `2024-09-27T13:05:23+08:00`

References
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
url: https://owasp.org/www-community/controls/SecureCookieAttribute
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

[return to 140.131.1.36]

2.1.3 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T13:05:48+08:00

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565

References
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 140.131.1.36]

2.1.4 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2025-01-21T13:37:33+08:00

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 140.131.1.36]