acunetix

Developer Report

Acunetix Security Audit

20 January 2025

Generated by Acunetix

Scan of www.sips.ntpc.edu.tw

Scan details

Scan information	
Start time	20/01/2025, 11:22:29
Start url	https://www.sips.ntpc.edu.tw/platform/
Host	www.sips.ntpc.edu.tw
Scan time	5 minutes, 32 seconds
Profile	Full Scan
Responsive	True

Threat level

Acunetix Threat Level 2

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

Alerts distribution

Total alerts found	7
High	0
Medium	1
Low	2
Informational	4

Alerts summary

HTML form without CSRF protection

Classification	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352

Affected items	Variation
Web Server	1

Login page password-guessing attack

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/platform	1

/platform/index.php	1

Email address found

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/platform	1
/platform/index.php	1

Possible username or password disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation

/platform	1
/platform/index.php	1

Alerts details

HTML form without CSRF protection

Severity	**Medium**
Reported by module	/Crawler/12-Crawler_Form_NO_CSRF.js

Description

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

Impact

An attacker could use CSRF to trick a victim into accessing a website hosted by the attacker, or clicking a URL containing malicious or unauthorized requests.

CSRF is a type of 'confused deputy' attack which leverages the authentication and authorization of the victim when the forged request is being sent to the web server. Therefore, if a CSRF vulnerability could affect highly privileged users such as administrators full application compromise may be possible.

Recommendation

Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.

The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes.

- The anti-CSRF token should be unique for each user session
- The session should automatically expire after a suitable amount of time
- The anti-CSRF token should be a cryptographically random value of significant length
- The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm
- The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent)
- The server should reject the requested action if the anti-CSRF token fails validation

When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.

References

What is Cross Site Reference Forgery (CSRF)? (https://www.acunetix.com/websitesecurity/csrf-attacks/)
Cross-Site Request Forgery (CSRF) Prevention Cheatsheet (https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)
The Cross-Site Request Forgery (CSRF/XSRF) FAQ (http://www.cgisecurity.com/csrf-faq.html)
Cross-site Request Forgery (https://en.wikipedia.org/wiki/Cross-site_request_forgery)

Affected items

Web Server
Details
Request headers
`GET /platform/ HTTP/1.1`

```
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Login page password-guessing attack

Severity	**Low**
Reported by module	/Scripts/PerScheme/Html_Authentication_Audit.script

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

Affected items

/platform

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /platform/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://www.sips.ntpc.edu.tw/platform/
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 150
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
ckCode=94102&hdCode=RlN0VzcxRWczRHJSZDB4VUI1T096djJBVkwxdHlURGpSTGVkZ2ZsVG9lQ2lZcVkrWjV5NmZq
TGw3QlU4ZDRhVg==&login_name=5OPSPFlb&login_passwd=AB2fHoF8
```

/platform/index.php

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /platform/index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://www.sips.ntpc.edu.tw/platform/
Connection: keep-alive
```

```
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 150
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
ckCode=94102&hdCode=Qzhzd2U1ZitzcnpYS1dpMmxhbGxNK0dsU3BMbHBNL3A2RldQS0RObnVBcUk1VUsrb3V6Zldk
bzlEVnBFOWRUZg==&login_name=jhdr3wpb&login_passwd=MDG7Xeog
```

Email address found

Severity	**Informational**
Reported by module	/Scripts/PerFolder/Text_Search_Dir.script

Description

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

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

/platform

Details

Pattern found:

```
vip@heimavista.com
```

Request headers

```
GET /platform/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/platform/index.php

Details

Pattern found:

```
vip@heimavista.com
```

Request headers

```
GET /platform/index.php HTTP/1.1
Cookie: PageLang=zh-tw; _counter=3098979
Accept: */*
```

```
Accept-Encoding: gzip,deflate
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Possible username or password disclosure

Severity	**Informational**
Reported by module	/Scripts/PerFolder/Text_Search_Dir.script

Description

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

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

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/platform

Details

Pattern found:

```
pwd=document
```

Request headers

```
GET /platform/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/platform/index.php

Details

Pattern found:

```
pwd=document
```

Request headers

```
GET /platform/index.php HTTP/1.1
Cookie: PageLang=zh-tw; _counter=3098979
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.sips.ntpc.edu.tw
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Scanned items (coverage report)

https://www.sips.ntpc.edu.tw/
https://www.sips.ntpc.edu.tw/platform
https://www.sips.ntpc.edu.tw/platform/index.php
https://www.sips.ntpc.edu.tw/platform/login
https://www.sips.ntpc.edu.tw/platform/login/images