acunetix

Developer Report

Acunetix Security Audit

2021-02-16

Generated by Acunetix

Scan of va.navy.lk

Scan details

Scan information	
Start time	2021-02-16T15:26:37.572525+05:30
Start url	http://va.navy.lk/
Host	va.navy.lk
Scan time	50 minutes, 35 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 2

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

Alerts distribution

Total alerts found	13
High	0
Medium	2
Low	5
Informational	6

Alerts summary

Application error messages

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
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
CWE	CWE-200

Affected items	Variation
Web Server	1

User credentials are sent in clear text

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: High Remediation Level: Workaround Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310

Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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
CWE	CWE-16

Affected items	Variation
Web Server	1

Login page password-guessing attack

Classification

CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L 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
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
CWE	CWE-307

Affected items	Variation
/manager/	1

Possible sensitive directories

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
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

CWE	CWE-200	
Affected items		Variation
Web Server		1

Possible sensitive files

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 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
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
CWE	CWE-200

Affected items	Variation
Web Server	1

Unencrypted connection

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None

CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial 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
CWE	CWE-310

Affected items	Variation
Web Server	1

Content Security Policy (CSP) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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
CWE	CWE-16

Affected items	Variation
Web Server	1

Insecure Referrer Policy

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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
CWE	CWE-16

Affected items	Variation
Web Server	1

No HTTP Redirection

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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

CWE	CWE-16	
Affected items		Variation
Web Server		1

Password type input with auto-complete enabled

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 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
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
CWE	CWE-200

Affected items	Variation
Web Server	1

Possible server path disclosure (Unix)

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None

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
CWE	CWE-200

Affected items	Variation
Web Server	1

Subresource Integrity (SRI) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
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
CWE	CWE-16

Affected items	Variation
Web Server	1

Alerts details

Application error messages

Severity	**Medium**
Reported by module	/httpdata/text_search.js

Description

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server
Details
Application error messages: • http://va.navy.lk/core/cache/logs/error.log **Unknown database 'malimaclubhousedb'** • http://va.navy.lk/core/cache/logs/error.log **Unknown database 'malimaclubhousedb'**
Request headers

```
GET /core/cache/logs/error.log HTTP/1.1

Referer: http://va.navy.lk/core/cache/logs/

Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

User credentials are sent in clear text

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

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

Web Server

Details

Forms with credentials sent in clear text:

- http://va.navy.lk/manager/

```
Form name: <empty>
Form action: <empty>
Form method: POST
Password input: password
```

Request headers

```
POST /manager/ HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://va.navy.lk/manager/

Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 112

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive



login=1&login_context=mgr&modahsh=1&password=g00dPa%24%24w0rD&rememberme=1&returnUrl=/man
ager/&username=pHqghUme
```

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
Securing cookies with cookie prefixes (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
Cookies: HTTP State Management Mechanism (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
SameSite Updates - The Chromium Projects (https://www.chromium.org/updates/same-site)
draft-west-first-party-cookies-07: Same-site Cookies (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server
Verified vulnerability

Details

List of cookies with missing, inconsistent or contradictory properties:

- http://va.navy.lk/

  Cookie was set with:

```
Set-Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34; expires=Tue, 23-Feb-2021 09:56:39 G
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and someti
```

Request headers

```
GET / HTTP/1.1

Referer: http://va.navy.lk/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Login page password-guessing attack

Severity	**Low**
Reported by module	/httpdata/html_auth_weak_creds.js

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 (https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

Affected items

/manager/
Details

Request headers

```
POST /manager/ HTTP/1.1

Referer: http://va.navy.lk/manager/

Cookie: PHPSESSID=v30021bmtrvbe7o8b0dcksv313;

Content-Type: application/x-www-form-urlencoded

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 103

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive



login_context=mgr&modahsh=&returnUrl=/manager/&username=username&password=testing&remembe
rme=1&login=1&
```

Possible sensitive directories

Severity	**Low**
Reported by module	/Scripts/PerFolder/Possible_Sensitive_Directories.script

Description

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to these directories or remove them from the website.

References

Web Server Security and Database Server Security (https://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

Web Server
Details
Possible sensitive directories: • http://va.navy.lk/**manager**
Request headers

```
GET /manager/ HTTP/1.1

Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Possible sensitive files

Severity	**Low**
Reported by module	/Scripts/PerFolder/Possible_Sensitive_Files.script

Description

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security (https://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

Web Server

Details
Possible sensitive files: • http://va.navy.lk/core/cache/logs/**error.log**
Request headers

```
GET /core/cache/logs/error.log HTTP/1.1

Accept: acunetix/wvs

Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Unencrypted connection

Severity	**Low**
Reported by module	/RPA/no_https.js

Description

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Affected items

Web Server
Verified vulnerability
Details
Request headers

```
GET / HTTP/1.1

Referer: http://va.navy.lk/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Content Security Policy (CSP) not implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Paths without CSP header: • http://va.navy.lk/ • http://va.navy.lk/index.php • http://va.navy.lk/ext2/ • http://va.navy.lk/ext2/resources/images/default/grid/ • http://va.navy.lk/ext2/resources/ • http://va.navy.lk/manager/ • http://va.navy.lk/ext2/resources/images/default/ • http://va.navy.lk/ext2/resources/images/ • http://va.navy.lk/core/docs/ • http://va.navy.lk/manager/assets/modext/util/filetree/img/silk/icons/ • http://va.navy.lk/manager/assets/modext/util/filetree/img/silk/ • http://va.navy.lk/manager/assets/ext3/'+this.emptyIcon+' • http://va.navy.lk/manager/assets/ext3/',Ext.BLANK_IMAGE_URL,' • http://va.navy.lk/manager/templates/default/css/images/ • http://va.navy.lk/manager/assets/ext3/',c,' • http://va.navy.lk/manager/assets/ext3/',k.icon||this.emptyIcon,' • http://va.navy.lk/manager/assets/ext3/',this.emptyIcon,' • http://va.navy.lk/manager/assets/modext/util/filetree/img/ • http://va.navy.lk/manager/assets/modext/util/filetree/
Request headers

```
GET / HTTP/1.1

Referer: http://va.navy.lk/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Insecure Referrer Policy

Severity	**Informational**
Reported by module	/httpdata/insecure_referrer_policy.js

Description

Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

Impact

In some situations, an attacker may leak a user's private data

Recommendation

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

References

Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

Affected items

Web Server
Details

URLs where Referrer Policy configuration is insecure:

- http://va.navy.lk/
- http://va.navy.lk/index.php
- http://va.navy.lk/ext2/
- http://va.navy.lk/ext2/resources/images/default/grid/
- http://va.navy.lk/ext2/resources/
- http://va.navy.lk/manager/
- http://va.navy.lk/ext2/resources/images/default/
- http://va.navy.lk/ext2/resources/images/
- http://va.navy.lk/core/docs/
- http://va.navy.lk/manager/assets/modext/util/filetree/img/silk/icons/
- http://va.navy.lk/manager/assets/modext/util/filetree/img/silk/
- http://va.navy.lk/manager/assets/ext3/'+this.emptyIcon+'
- http://va.navy.lk/manager/assets/ext3/',Ext.BLANK_IMAGE_URL,'
- http://va.navy.lk/manager/templates/default/css/images/
- http://va.navy.lk/manager/assets/ext3/',c,'
- http://va.navy.lk/manager/assets/ext3/',k.icon||this.emptyIcon,'
- http://va.navy.lk/manager/assets/ext3/',this.emptyIcon,'
- http://va.navy.lk/manager/assets/modext/util/filetree/img/
- http://va.navy.lk/manager/assets/modext/util/filetree/

Request headers

```
GET / HTTP/1.1

Referer: http://va.navy.lk/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

No HTTP Redirection

Severity	**Informational**
Reported by module	/target/http_redirections.js

Description

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections (https://infosec.mozilla.org/guidelines/web_security#http-redirections)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Password type input with auto-complete enabled

Severity	**Informational**
Reported by module	/Crawler/12-Crawler_Password_Input_Autocomplete.js

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

Web Server
Details

Pages with auto-complete password inputs:

- http://va.navy.lk/manager/

```
Form name: <empty>
Form action: <empty>
Form method: POST
Password input: password
```

Request headers

```
POST /manager/ HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://va.navy.lk/manager/

Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 112

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive



login=1&login_context=mgr&modahsh=1&password=g00dPa%24%24w0rD&rememberme=1&returnUrl=/man
ager/&username=pHqghUme
```

Possible server path disclosure (Unix)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

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

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server
Details
Pages with paths being disclosed: • http://va.navy.lk/core/cache/logs/error.log **/var/www/malima/www.clubhouseuswetakeiyawa.lk/html/core/xpdo/xpdo.class.php**
Request headers

```
GET /core/cache/logs/error.log HTTP/1.1

Referer: http://va.navy.lk/core/cache/logs/

Cookie: PHPSESSID=gl2u2gto7ei4lro300pc4fth34

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Subresource Integrity (SRI) not implemented

Severity	**Informational**
Reported by module	/RPA/SRI_Not_Implemented.js

Description

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
        integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
        crossorigin="anonymous"></script>
```

References

Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)
SRI Hash Generator (https://www.srihash.org/)

Affected items

Web Server
Details
Pages where SRI is not implemented: • http://va.navy.lk/ Script SRC: **https://ajax.googleapis.com/ajax/libs/jquery/1.8.2/jquery.min.js**
Request headers

```
GET / HTTP/1.1

Referer: http://va.navy.lk/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.61 Safari/537.36

Host: va.navy.lk

Connection: Keep-alive
```

Scanned items (coverage report)

http://va.navy.lk/
http://va.navy.lk/assets/
http://va.navy.lk/assets/images/
http://va.navy.lk/core/
http://va.navy.lk/core/cache/
http://va.navy.lk/core/cache/includes/
http://va.navy.lk/core/cache/logs/
http://va.navy.lk/core/cache/logs/error.log
http://va.navy.lk/core/cache/menu/
http://va.navy.lk/core/cache/rss/
http://va.navy.lk/core/cache/scripts/
http://va.navy.lk/core/config/
http://va.navy.lk/core/docs/
http://va.navy.lk/core/error/
http://va.navy.lk/core/export/
http://va.navy.lk/core/import/
http://va.navy.lk/ext2/
http://va.navy.lk/ext2/resources/
http://va.navy.lk/ext2/resources/images/
http://va.navy.lk/ext2/resources/images/default/
http://va.navy.lk/ext2/resources/images/default/grid/
http://va.navy.lk/index.php
http://va.navy.lk/manager/
http://va.navy.lk/manager/assets/
http://va.navy.lk/manager/assets/ext3/
http://va.navy.lk/manager/assets/ext3/',c,'
http://va.navy.lk/manager/assets/ext3/',Ext.BLANK_IMAGE_URL,'
http://va.navy.lk/manager/assets/ext3/',k.icon||this.emptyIcon,'
http://va.navy.lk/manager/assets/ext3/',this.emptyIcon,'
http://va.navy.lk/manager/assets/ext3/'+this.emptyIcon+'
http://va.navy.lk/manager/assets/ext3/adapter/
http://va.navy.lk/manager/assets/ext3/adapter/ext/
http://va.navy.lk/manager/assets/ext3/adapter/ext/ext-base.js
http://va.navy.lk/manager/assets/ext3/ext-all.js
http://va.navy.lk/manager/assets/ext3/resources/
http://va.navy.lk/manager/assets/ext3/resources/css/
http://va.navy.lk/manager/assets/ext3/resources/css/ext-all-notheme-min.css
http://va.navy.lk/manager/assets/ext3/resources/images/
http://va.navy.lk/manager/assets/ext3/resources/images/access/
http://va.navy.lk/manager/assets/ext3/resources/images/access/menu/
http://va.navy.lk/manager/assets/ext3/resources/images/default/
http://va.navy.lk/manager/assets/ext3/resources/images/default/editor
http://va.navy.lk/manager/assets/ext3/resources/images/default/editor/
http://va.navy.lk/manager/assets/ext3/resources/images/default/form/
http://va.navy.lk/manager/assets/ext3/resources/images/default/menu/
http://va.navy.lk/manager/assets/modext/
http://va.navy.lk/manager/assets/modext/core/
http://va.navy.lk/manager/assets/modext/core/modx.component.js
http://va.navy.lk/manager/assets/modext/core/modx.js
http://va.navy.lk/manager/assets/modext/sections/
http://va.navy.lk/manager/assets/modext/sections/login.js
http://va.navy.lk/manager/assets/modext/sections/security/
http://va.navy.lk/manager/assets/modext/sections/security/access/
http://va.navy.lk/manager/assets/modext/sections/security/profile/
http://va.navy.lk/manager/assets/modext/sections/security/user/
http://va.navy.lk/manager/assets/modext/sections/system/
http://va.navy.lk/manager/assets/modext/sections/system/file/
http://va.navy.lk/manager/assets/modext/sections/system/import/

http://va.navy.lk/manager/assets/modext/util/
http://va.navy.lk/manager/assets/modext/util/filetree/
http://va.navy.lk/manager/assets/modext/util/filetree/img/
http://va.navy.lk/manager/assets/modext/util/filetree/img/silk/
http://va.navy.lk/manager/assets/modext/util/filetree/img/silk/icons/
http://va.navy.lk/manager/assets/modext/util/utilities.js
http://va.navy.lk/manager/assets/modext/widgets/
http://va.navy.lk/manager/assets/modext/widgets/core/
http://va.navy.lk/manager/assets/modext/widgets/core/modx.panel.js
http://va.navy.lk/manager/assets/modext/widgets/core/modx.window.js
http://va.navy.lk/manager/assets/modext/widgets/media/
http://va.navy.lk/manager/assets/modext/widgets/security/
http://va.navy.lk/manager/assets/modext/widgets/system/
http://va.navy.lk/manager/assets/modext/widgets/system/mysql/
http://va.navy.lk/manager/templates/
http://va.navy.lk/manager/templates/default/
http://va.navy.lk/manager/templates/default/css/
http://va.navy.lk/manager/templates/default/css/images/
http://va.navy.lk/manager/templates/default/css/index-min.css
http://va.navy.lk/manager/templates/default/css/login-min.css
http://va.navy.lk/manager/templates/default/fonts/
http://va.navy.lk/manager/templates/default/images/
http://va.navy.lk/manager/templates/default/images/modx-theme/
http://va.navy.lk/manager/templates/default/images/modx-theme/box/
http://va.navy.lk/manager/templates/default/images/modx-theme/button/
http://va.navy.lk/manager/templates/default/images/modx-theme/dd/
http://va.navy.lk/manager/templates/default/images/modx-theme/editor
http://va.navy.lk/manager/templates/default/images/modx-theme/editor/
http://va.navy.lk/manager/templates/default/images/modx-theme/form/
http://va.navy.lk/manager/templates/default/images/modx-theme/grid/
http://va.navy.lk/manager/templates/default/images/modx-theme/layout/
http://va.navy.lk/manager/templates/default/images/modx-theme/menu/
http://va.navy.lk/manager/templates/default/images/modx-theme/panel/
http://va.navy.lk/manager/templates/default/images/modx-theme/qtip/
http://va.navy.lk/manager/templates/default/images/modx-theme/shared/
http://va.navy.lk/manager/templates/default/images/modx-theme/sizer/
http://va.navy.lk/manager/templates/default/images/modx-theme/slider/
http://va.navy.lk/manager/templates/default/images/modx-theme/tabs/
http://va.navy.lk/manager/templates/default/images/modx-theme/toolbar/
http://va.navy.lk/manager/templates/default/images/modx-theme/tree/
http://va.navy.lk/manager/templates/default/images/restyle/
http://va.navy.lk/manager/templates/default/images/restyle/fileup/
http://va.navy.lk/manager/templates/default/images/restyle/i/
http://va.navy.lk/manager/templates/default/images/restyle/icons/
http://va.navy.lk/manager/templates/default/images/style/
http://va.navy.lk/manager/templates/default/js/
http://va.navy.lk/manager/templates/default/security/
http://va.navy.lk/manager/templates/default/security/user/
http://va.navy.lk/manager/templates/default/system/
http://va.navy.lk/robots.txt
http://va.navy.lk/sitemap.xml