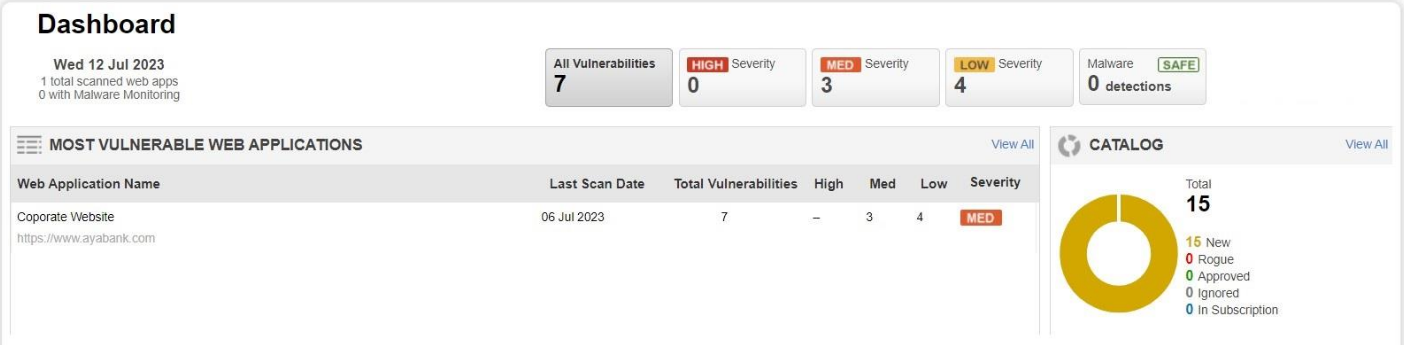
AYA Vulnerability Assessment Report

Requested By	: Enterprise IT Department
Actioned By	: IT Security Department
Target System	: Corporate Website
Target System Detail	: www.ayabank.com
Overall Security Risk	: Medium

Report Summary



Dashboard

Wed 12 Jul 2023
1 total scanned web apps
0 with Malware Monitoring

All Vulnerabilities	HIGH Severity	MED Severity	LOW Severity	Malware SAFE
7	0	3	4	0 detections

MOST VULNERABLE WEB APPLICATIONS — View All

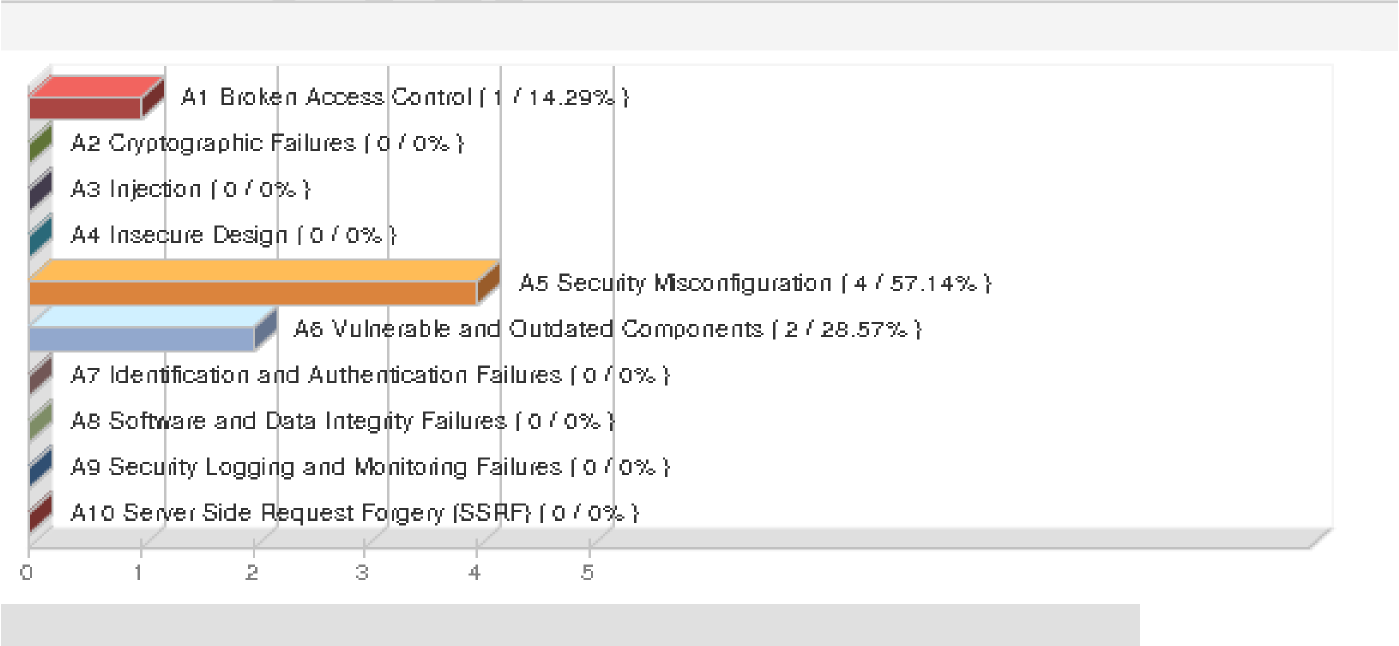
Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
Coporate Website https://www.ayabank.com	06 Jul 2023	7	–	3	4	MED

CATALOG — View All

Total 15

15 New
0 Rogue
0 Approved
0 Ignored
0 In Subscription

OWASP Top 10 Vulnerabilities



Security Levels [Confirmed Vulnerabilities]

Vulnerabilities (QIDs) are design flaws, programming errors, or misconfigurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can varies from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

■□□□□ Minimal Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.

■■□□□ Medium Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.

■■■□□ Serious Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non- encrypted channels.

■■■■□ Critical Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.

■■■■■ Urgent Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.

Potential Vulnerabilities

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section includes information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.

■□□□□ Minimal Presence of this vulnerability is indicative of basic information disclosure (e.g., web server type, programming language) and might enable intruders to discover other vulnerabilities. For example, in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.

■■□□□ Medium Presence of this vulnerability is indicative of basic information disclosure (e.g., web server type, programming language) and might enable intruders to discover other vulnerabilities. For example, version of software or session data can be disclosed, which could be used to exploit.

■■■□□ Serious Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.

■■■■□ Critical Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.

■■■■■ Urgent Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example, in this scenario, the web application users can potentially be targeted if the application is exploited.

Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

■□□□□ Minimal Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason, we recommend caution.

■■□□□ Medium Sensitive content was found in the web server response. Specifically, our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason, we recommend caution.

Serious

Sensitive content was found in the web server response - a valid social security number or credit card information. This information disclosure could result in a confidentiality breach, and it gives intruders.

Vulnerability (7)

Information Disclosure (7)

MED 150051 Open Redirect (1)

MED 150051 Open Redirect

URL: https://www.ayabank.com/enquiry_form_submit

Finding #	**1849888**(73640170)	**Severity**	Confirmed Vulnerability - Level 3
Unique #	**95b329fd-82b5-40d4-8c05-37cff9b4a877**		
Group	Information Disclosure	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	CWE-601		
OWASP	A1 Broken Access Control		
WASC	WASC-38 URL REDIRECTOR ABUSE		
CVSS V3 Base	6.5	**CVSS V3 Attack Vector**	Network
CVSS V3 Temporal	6.5		

Details

Threat

The web application creates a redirect based on a parameter from a query string or form field. The redirect destination can be changed by modifying the parameter's value. Redirects are used to automatically force the web browser to request a resource from a new destination. An open redirect occurs when the redirect destination may be any host unrelated to the original web application.

Impact

Open redirects or otherwise unvalidated redirects are often used as part of a social engineering or phishing attack because the initial malicious link sent to a victim can use a trusted, legitimate web site's URL to redirect to a link on a malicious web server.

Solution

Verify that the redirect behavior is acceptable according to your application's security or privacy policy. This determines whether redirecting to a host unrelated to the web application is permissible. Consider moving redirect logic to server-side code that verifies the redirect destination is allowed.

MED 150051 Open Redirect

URL: https://www.ayabank.com/enquiry_form_submit

Finding #	**1849888**(73640170)	Severity	Confirmed Vulnerability - Level 3
Unique #	**95b329fd-82b5-40d4-8c05-37cff9b4a877**		
Group	Information Disclosure	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-601		
OWASP	A1 Broken Access Control		
WASC	WASC-38 URL REDIRECTOR ABUSE		

CVSS V3 Base	6.5	CVSS V3 Temporal	6.5	CVSS V3 Attack Vector	Network

Details

Threat

The web application creates a redirect based on a parameter from a querystring or form field. The redirect destination can be changed by modifying the parameter's value. Redirects are used to automatically force the web browser to request a resource from a new destination. An open redirect occurs when the redirect destination may be any host unrelated to the original web application.

Impact

Open redirects or otherwise unvalidated redirects are often used as part of a social engineering or phishing attack because the initial malicious link sent to a victim can use a trusted, legitimate web site's URL to redirect to a link on a malicious web server.

Solution

Verify that the redirect behavior is acceptable according to your application's security or privacy policy. This determines whether redirecting to a host unrelated to the web application is permissible. Consider moving redirect logic to server-side code that verifies the redirect destination is allowed.

Detection Information

Parameter	It has been detected by exploiting the parameter **Referer** of the form located in URL **https://www.ayabank.com/enquiry** The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication	In order to detect this vulnerability, no authentication has been required.

Access Path Here is the path followed by the scanner to reach the exploitable URL:

https://www.ayabank.com/
https://www.ayabank.com/business/borrowing/corporate-business-loan
https://www.ayabank.com/enquiry

Payloads

#1 Request

```
POST https://www.ayabank.com/enquiry_form_submit
Referer: https://www.qualys.com
Cookie:

aya_bank_session=eyJpdiI6IkdqZkVLTlJ2TUR3dzBiZy95YTlMeWc9PSIsInZhbHVlIjoiTWs0OVpUL1dPTmhUT092a3BOQ1NReEFUZWxWQUFzL3hQUzZJeW5nQ1NSVV
XSRF-

TOKEN=eyJpdiI6ImFLajBla0hIYmpjT1hGMUY0WnU1Nmc9PSIsInZhbHVlIjoiTjBLbHhmZG9hQWpQZDFJY0lhS0NwM2h6SWNwdi9nUjFYaS9pcUFTNHh3NFlhNW5lb1


Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Content-Length: 231

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


_token=fWfQVQ6vvlzKkJORJ61CJBv09jjqxdmA7mSrIFtX&name_txt=John&phone_txt=8000000000&email_txt=was@qualys.com&division_select=1&company_tx
%20Financing&tnc_check=1
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Matched location header in response to the injected host in request.
Open redirection detected by changing "Referer" header.

MED MED 150162 Use of JavaScript Library with Known Vulnerability (1)

MED 150162 Use of JavaScript Library with Known Vulnerability

URL: https://www.ayabank.com/

Finding #	**1849882**(73640167)	Severity	Confirmed Vulnerability - Level 3
Unique #	**a1728eb4-57a2-4b13-8ce1-0a3126c8fa63**		
Group	Information Disclosure	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-937		
OWASP	A6 Vulnerable and Outdated Components		
WASC	-		

CVSS V3 Base	6.5	CVSS V3 Temporal	5.6	CVSS V3 Attack Vector	Network

Details

Threat

The web application is using a JavaScript library that is known to contain at least one vulnerability.

Impact

Attackers could potentially exploit the vulnerability in the JavaScript library. The impact of a successful exploit depends on the nature of the vulnerability and how the web application makes use of the library.

Solution

Please refer to the information provided in the response section. Also check the vendor's security advisories related to the vulnerable version of the library.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

```
GET https://www.ayabank.com/
Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Vulnerable javascript library: moment
version: 2.29.1
script uri: https://www.ayabank.com/js/moment.min.js

Details:
CVE-2022-24785: Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale.
Solution: Moment.js version 2.29.2 has been released to address the issue. Please refer to Vendor Documentation (https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4, https://nvd.nist.gov/vuln/detail/CVE-2022-24785) for latest security updates.

CVE-2022-31129: Moment.js is a lightweight JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) via the preprocessRFC2822() function in from-string.js, when processing a very long crafted string (over 10k characters).
Solution: Moment.js version 2.29.4 has been released to address the issue. Please refer to Vendor Documentation (https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g, https://nvd.nist.gov/vuln/detail/CVE-2022-31129) for latest security updates.

Found on the following pages (only first 10 pages are reported):
https://www.ayabank.com/
https://www.ayabank.com/?s=discovery
https://www.ayabank.com/privacy-notice-cookie-policy
https://www.ayabank.com/business/account-saving/call-deposit
https://www.ayabank.com/business/remittance-payments/local-payments https://www.ayabank.com/about-aya/governance/corporate-governance https://www.ayabank.com/personal-banking/insurance/life/universal
https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving
https://www.ayabank.com/business/insurance/oversea-marine-cargo https://www.ayabank.com/personal-banking/insurance/travel/aya-go

MED 151025 *Vulnerable JavaScript Library Detected - Moment.js* (1)

MED 151025 Vulnerable JavaScript Library Detected- Moment.js

URL: https://www.ayabank.com/

Finding #	**1849880**(73639766)	Severity	Confirmed Vulnerability - Level 3
Unique #	**9537f95d-503d-4508-9ab6-3818220fb703**		
Group	Information Disclosure	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-937		
OWASP	A6 Vulnerable and Outdated Components		
WASC	-		

CVSS V3 Base	7.5	CVSS V3 Temporal	6.6	CVSS V3 Attack Vector	Network

Details

Threat

Moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. The web application is using a JavaScript library that is known to contain at least one vulnerability.

Impact

Attackers could potentially exploit the vulnerability in the JavaScript library. The impact of a successful exploit depends on the nature of the vulnerability and how the web application makes use of the library.

Solution

Please refer to the information provided in the response section. Also check the vendor's security advisories related to the vulnerable version of the library.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

```
GET https://www.ayabank.com/
Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Vulnerable javascript library: moment
version: 2.29.1
script uri: https://www.ayabank.com/js/moment.min.js

Details:
CVE-2022-24785: Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale.
Solution: Moment.js version 2.29.2 has been released to address the issue. Please refer to Vendor Documentation (https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4, https://nvd.nist.gov/vuln/detail/CVE-2022-24785) for latest security updates.

CVE-2022-31129: Moment.js is a lightweight JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) via the preprocessRFC2822() function in from-string.js, when processing a very long crafted string (over 10k characters).
Solution: Moment.js version 2.29.4 has been released to address the issue. Please refer to Vendor Documentation (https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g, https://nvd.nist.gov/vuln/detail/CVE-2022-31129) for latest security updates.

Found on the following pages (only first 10 pages are reported):
https://www.ayabank.com/
https://www.ayabank.com/?s=discovery
https://www.ayabank.com/privacy-notice-cookie-policy
https://www.ayabank.com/business/account-saving/call-deposit
https://www.ayabank.com/business/remittance-payments/local-payments https://www.ayabank.com/about-aya/governance/corporate-governance https://www.ayabank.com/personal-banking/insurance/life/universal
https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving
https://www.ayabank.com/business/insurance/oversea-marine-cargo https://www.ayabank.com/personal-banking/insurance/travel/aya-go

LOW *150122 Cookie Does Not Contain The "secure" Attribute* (2)

LOW 150122 Cookie Does Not Contain The "secure" Attribute

URL: https://www.ayabank.com/digital-services/card-services/simple-pay

Finding #	**1849886**(73640169)	Severity	Confirmed Vulnerability - Level 2
Unique #	**7a1b5674-1291-434b-b580-6ed7047be113**		
Group	Information Disclosure	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-614		
OWASP	A5 Security Misconfiguration		
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION		

CVSS V3 Base	4.3	CVSS V3 Temporal	4.1	CVSS V3 Attack Vector	Network

Details

Threat

The cookie does not contain the "secure" attribute.

Impact

Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s)	**_gat_gtag_UA_228606560_1**
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

```
https://www.ayabank.com/
```

Payloads

#1 Request

```
GET https://www.ayabank.com/digital-services/card-services/simple-pay
Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
_gat_gtag_UA_228606560_1=1; expires=Thu Jul 6 04:40:52 2023; path=/; domain=ayabank.com
Cookies set via JavaScript do not have an associated HTTP response header.
```

LOW 150122 Cookie Does Not Contain The "secure" Attribute

URL: https://www.ayabank.com/

Finding #	**1849890**(73640171)	**Severity**	Confirmed Vulnerability - Level 2
Unique #	**7b069e4b-293a-4474-acbc-2a84f3e71846**		
Group	Information Disclosure	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	CWE-614		
OWASP	A5 Security Misconfiguration		
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION		

CVSS V3 Base 4.3 **CVSS V3 Temporal**4.1 **CVSS V3 Attack Vector** Network

Details

Threat

The cookie does not contain the "secure" attribute.

Impact

Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s)	**aya_bank_session, XSRF-TOKEN**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

VULNERABILITY ASSESSMENT REPORT

#1 Request

```
GET https://www.ayabank.com/
Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
aya_bank_session=
200 OK
Date: Thu, 06 Jul 2023 04:36:16 GMT
Server: Apache
Cache-Control: no-cache, private Content-
Encoding: gzip
Vary: Accept-Encoding,User-Agent Set-
Cookie: XSRF-
TOKEN=eyJpdiI6IitUY1UxekpZcDc3K28vY0VhSkYrYUE9PSIsInZhbHVlIjoia0I0Z29HaTVDQmM3Yk11cEFtWms5eWx6VGswTHp1MmlOSFpMbmJjbkhORE45a0ZiekpTNWo4Z1l1d243ckhlU0J
expires=Thu, 06-Jul-2023 06:36:16 GMT; Max-Age=7200; path=/; samesite=lax


aya_bank_session=eyJpdiI6IjNJSmJldmpNdmlNbnBHa0JFaUZQQWc9PSIsInZhbHVlIjoiUE9sT0hldWVJZGhMVnhkbk8zRUVEQithUHNYTWxOdCtBRFF3OWc0V0pJQlByTlV2ZTd6SzdXVEhCe
expires=Thu, 06-Jul-2023 06:36:16 GMT; Max-Age=7200; path=/; httponly; samesite=lax
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block Upgrade:
h2,h2c
Connection: Upgrade, Keep-Alive Access-
Control-Allow-Origin: * Access-Control-
Allow-Methods: GET Keep-Alive:
timeout=20, max=100 Transfer-Encoding:
chunked
Content-Type: text/html; charset=UTF-8


XSRF-TOKEN=
200 OK
Date: Thu, 06 Jul 2023 04:36:16 GMT
Server: Apache
Cache-Control: no-cache, private Content-
Encoding: gzip
Vary: Accept-Encoding,User-Agent Set-
Cookie: XSRF-
TOKEN=eyJpdiI6IitUY1UxekpZcDc3K28vY0VhSkYrYUE9PSIsInZhbHVlIjoia0I0Z29HaTVDQmM3Yk11cEFtWms5eWx6VGswTHp1MmlOSFpMbmJjbkhORE45a0ZiekpTNWo4Z1l1d243ckhlU0J
expires=Thu, 06-Jul-2023 06:36:16 GMT; Max-Age=7200; path=/; samesite=lax


aya_bank_session=eyJpdiI6IjNJSmJldmpNdmlNbnBHa0JFaUZQQWc9PSIsInZhbHVlIjoiUE9sT0hldWVJZGhMVnhkbk8zRUVEQithUHNYTWxOdCtBRFF3OWc0V0pJQlByTlV2ZTd6SzdXVEhCe
expires=Thu, 06-Jul-2023 06:36:16 GMT; Max-Age=7200; path=/; httponly; samesite=lax
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block Upgrade:
h2,h2c
Connection: Upgrade, Keep-Alive Access-
Control-Allow-Origin: * Access-Control-
Allow-Methods: GET Keep-Alive:
timeout=20, max=100 Transfer-Encoding:
chunked
Content-Type: text/html; charset=UTF-8
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

LOW *150123 Cookie Does Not Contain The "HTTPOnly" Attribute (*

LOW 150123 Cookie Does Not Contain The "HTTPOnly" Attribute

URL: https://www.ayabank.com/digital-services/card-services/simple-pay

Finding #	**1849884**(73640168)	Severity	Confirmed Vulnerability - Level 2
Unique #	**0a16b72a-b89e-44f5-b353-1831d744237e**		
Group	Information Disclosure	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-1004		
OWASP	A5 Security Misconfiguration		
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION		

CVSS V3 Base 4.3 **CVSS V3 Temporal**4.1 **CVSS V3 Attack Vector** Network

Details

Threat

The cookie does not contain the "HTTPOnly" attribute.

Impact

Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s) **_gat_gtag_UA_228606560_1**

Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.ayabank.com/

Payloads

#1 Request

```
GET https://www.ayabank.com/digital-services/card-services/simple-pay
Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
_gat_gtag_UA_228606560_1=1; expires=Thu Jul 6 04:40:52 2023; path=/; domain=ayabank.com
Cookies set via JavaScript do not have an associated HTTP response header.
```

LOW 150123 Cookie Does Not Contain The "HTTPOnly" Attribute

URL: https://www.ayabank.com/

Finding #	**1849892**(73640172)	Severity	Confirmed Vulnerability - Level 2
Unique #	**19f6141d-20c9-491b-b905-d8f420b4e074**		
Group	Information Disclosure	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-1004		
OWASP	A5 Security Misconfiguration		
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION		

CVSS V3 Base	4.3	CVSS V3 Temporal	4.1	CVSS V3 Attack Vector	Network

Details

Threat

The cookie does not contain the "HTTPOnly" attribute.

Impact

Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s)	**XSRF-TOKEN**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

```
GET https://www.ayabank.com/
Host: www.ayabank.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
XSRF-TOKEN=
200 OK
Date: Thu, 06 Jul 2023 04:36:16 GMT
Server: Apache
Cache-Control: no-cache, private Content-
Encoding: gzip
Vary: Accept-Encoding,User-Agent Set-
Cookie: XSRF-
TOKEN=eyJpdiI6IitUY1UxekpZcDc3K28vY0VhSkYrYUE9PSIsInZhbHVlIjoia0I0Z29HaTVDQmM3Yk11cEFtWms5eWx6VGswTHp1MmlOSFpMbmJjbkhORE45a0ZiekpTNWo4Z1l1d243ckhlU0J
expires=Thu, 06-Jul-2023 06:36:16 GMT; Max-Age=7200; path=/; samesite=lax


aya_bank_session=eyJpdiI6IjNJSmJldmpNdmlNbnBHa0JFaUZQQWc9PSIsInZhbHVlIjoiUE9sT0hldWVJZGhMVnhkbk8zRUVEQithUHNYTWxOdCtBRFF3OWc0V0pJQlByTlV2ZTd6SzdXVEhCe
expires=Thu, 06-Jul-2023 06:36:16 GMT; Max-Age=7200; path=/; httponly; samesite=lax
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block Upgrade:
h2,h2c
Connection: Upgrade, Keep-Alive Access-
Control-Allow-Origin: * Access-Control-
Allow-Methods: GET Keep-Alive:
timeout=20, max=100 Transfer-Encoding:
chunked
Content-Type: text/html; charset=UTF-8
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

Information Gathered (39)

Scan Diagnostics (29)

INFO 150042 Server Returns HTTP 5XX Error Code During Scanning (1)

INFO 150042 Server Returns HTTP 5XX Error Code During Scanning

Finding #	**1034141**(73639739)	Severity	Information Gathered - Level 3
Unique #	**4638f87a-f616-4dee-849a-7afeeef9c1b4**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-209, CWE-550		
OWASP	A5 Security Misconfiguration		
WASC	WASC-14 SERVER MISCONFIGURATION		

Details

Threat

During the WAS scan, links with HTTP 5xx response code were observed and these are listed in the Results section.

The HTTP 5xx message indicates a server error. The list of supported 5xx response code is as below:

500 - Internal
Server Error 501 -
Not Implemented
502 - Bad Gateway

503 - Service
Unavailable 504 -
Gateway Timeout

505 - HTTP Version Not Supported

Impact

The presence of a HTTP 5xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depending on responses to detect many vulnerabilities if the link does not respond with an expected response then vulnerabilities present on such links may not be detected.

Solution

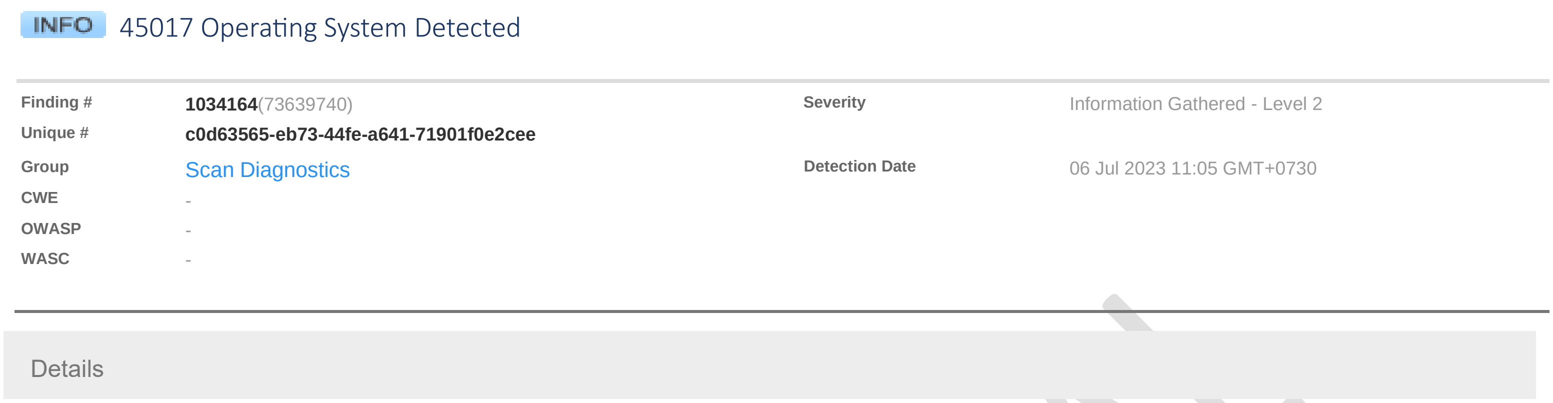
Review each link to determine why the server encountered an error when responding to the link. Review and investigate the results of QID 150528 which lists 4xx errors and QID 150019 which lists unexpected response codes.

Results

https://www.ayabank.com/report_download https://www.ayabank.com/about-aya/news-room/corporate-news/year
https://www.ayabank.com/about-aya/news-room/corporate-news/Asia_Money_2019_Awards_Best_Bank_for_SMEs_%22_Best_Bank_for_CSR Asia_Money_2019_Best_Bank_for_SMEs

https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%25E2%2580%2599s_10th_Homage_Ceremony
https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%25E2%2580%2599s_Family_Celebrating_10th_Kathina_Civara_Dana_Ceremony
https://www.ayabank.com/about-aya/news-room/corporate-news/Publication_of_Report_on_Myanmar%25E2%2580%2599s_Business_Transparency_2019_Pwint_Thit_Sa

INFO *45017 Operating System Detected (1)*



INFO 45017 Operating System Detected

Finding #	1034164(73639740)	Severity	Information Gathered - Level 2
Unique #	c0d63565-eb73-44fe-a641-71901f0e2cee		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Thrat

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/ IP stacks have subtle differences that can be seen in their responses to specially crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

2) Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

3) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

4) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

5) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

Impact

Not Applicable

Solution

Not applicable.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	169.60.37.100
Port	-
Result	EulerOS_/_Ubuntu_/_Fedora_/_Tiny_Core_Linux_/_Linux_3.x_/_IBM_/_FortiSOAR TCP/IP_Fingerprint U5933:443

Info List

Info #1

INFO 150375 PII Fields Found (1)

INFO 150375 PII Fields Found

Finding #	**1034149**(73639747)	Severity	Information Gathered - Level 2
Unique #	**af5c987a-eeed-47db-9766-8807f98e5af3**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-359		
OWASP	A2 Cryptographic Failures		
WASC	WASC-13 INFORMATION LEAKAGE		

Details

Threat

Personally Identifiable Information (PII) is found on the form(s) on the Web Application.

Impact

Improper handling of the PII can lead to loss of reputation for the organization and the individuals whose personal information is stored. Attackers can use this information for more focused attacks in the future.

Solution

Please review all the PII fields below in the report and if required, PII should be obtained by lawful and fair means.

Results

Parent URI: https://www.ayabank.com/personal-banking/royal-banking

PII fields Found:
Email

Parent URI: https://www.ayabank.com/about-aya/news-room/reports

PII fields Found:
Email

Parent URI: https://www.ayabank.com/enquiry

PII fields Found:
Email
Phone

INFO 6 DNS Host Name (1)

INFO 6 DNS Host Name

Finding #	**1034163**(73639729)	**Severity**	Information Gathered - Level 1
Unique #	**6f04abb8-7b7d-4a15-8e59-faec5be9f197**		
Group	Scan Diagnostics	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	169.60.37.100
Port	-
Result	#table IP_address Host_name 169.60.37.100 hs24.name.tools

INFO *38116 SSL Server Information Retrieval* (1)

INFO 38116 SSL Server Information Retrieval

Finding #	1034167(73639763)	Severity	Information Gathered - Level 1
Unique #	0f27af67-55a9-4f32-ba83-60d50d3bf2c2		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported
SSL ciphers.

Note: If a cipher is included in this list, it means that it was possible to establish a SSL connection using that cipher. There is some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though Low-grade cipher will be listed here QID 38140 will not be reported.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA CHACHA20/POLY1305(256) HIGH TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _ TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) TLS13-AES-128-CCM-SHA256 N/A N/A AEAD AESCCM(128) MEDIUM

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
DHE-RSA-AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	DH	AEAD	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	DH	AEAD	TLSv1.2
ECDHE-RSA-AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	ECDH	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	ECDH	AEAD	TLSv1.2
ECDHE-RSA-CHACHA20-POLY1305	RSA	CHACHA20/ POLY1305(256)	HIGH	ECDH	AEAD	TLSv1.2

Info #2

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(128)	MEDIUM	N/A	AEAD	TLSv1.3
TLS13-AES-256-GCM-SHA384	N/A	AESGCM(256)	HIGH	N/A	AEAD	TLSv1.3
TLS13-CHACHA20-POLY1305-	N/A	CHACHA20/ POLY1305(256)	HIGH	N/A	AEAD	TLSv1.3
TLS13-AES-128-CCM-SHA256	N/A	AESCCM(128)	MEDIUM	N/A	AEAD	TLSv1.3

INFO **38291 SSL Session Caching Information** (1)

INFO 38291 SSL Session Caching Information

Finding #	**1034162**(73639760)	Severity	Information Gathered - Level 1
Unique #	**a4462cca-eca8-4c78-b0d7-e47020a3701c**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	TLSv1.2 session caching is enabled on the target. TLSv1.3 session caching is enabled on the target.

INFO *38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance* (1)

INFO 38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

Finding #	**1034166**(73639762)	Severity	Information Gathered - Level 1
Unique #	**9307f05f-27ab-4a9f-8197-79f91a32b06c**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

INFO *38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods* *(1)*

INFO 38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

Finding #	**1034168**(73639764)	Severity	Information Gathered - Level 1
Unique #	**845482a0-ca4a-432a-8131-f3ec04ebb01d**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	#table cols="7" CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ _ DHE-RSA AES256-GCM-SHA384 DHE _ 2048 yes 110 low DHE-RSA-AES128-GCM-SHA256 DHE _ 2048 yes 110 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE 448 yes 224 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE x25519 256 yes 128 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp384r1 384 yes low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low E RSA-CHACHA20-POLY1305 ECDHE x448 448 yes 224 low ECDHE-RSA-CHACHA20-POLY1305 ECDHE x25519 256 yes 128 low ECDHE-RSA-CHACH POLY1305 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-CHACHA20-POL ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE x448 448 yes 224 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE x25 256 yes 128 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp256r1 256 y low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low TLSv1.3 _ _ _ _ _ _ TLS13-AES-128-GCM-SHA256 ECDHE x25519 256 yes low TLS13-AES-128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low TLS13-AES-128-GCM-SHA256 ECDHE x448 448 yes 224 low TLS13-AES-128-G SHA256 ECDHE secp521r1 521 yes 260 low TLS13-AES-128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low TLS13-AES-256-GCM-SHA384 ECDHE x25519 256 yes 128 low TLS13-AES-256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low TLS13-AES-256-GCM-SHA384 ECDHE

x448 448 yes 224 lo TLS13-AES-256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low TLS13-AES-256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low TLS13-CHACHA2 POLY1305-SHA256 ECDHE x25519 256 yes 128 low TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp256r1 256 yes 128 low TLS13-CHACHA20- POLY1305-SHA256 ECDHE x448 448 yes 224 low TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp521r1 521 yes 260 low TLS13-CHACHA20-POLY SHA256 ECDHE secp384r1 384 yes 192 low TLS13-AES-128-CCM-SHA256 ECDHE x25519 256 yes 128 low TLS13-AES-128-CCM-SHA256 ECDHE secp256r1 256 yes 128 low TLS13-AES-128-CCM-SHA256 ECDHE x448 448 yes 224 low TLS13-AES-128-CCM-SHA256 ECDHE secp521r1 521 yes 260 TLS13-AES-128-CCM-SHA256 ECDHE secp384r1 384 yes 192 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	2048	yes	110	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low

Info List

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low

INFO 38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

INFO 38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

Finding #	**1034169**(73639765)	Severity	Information Gathered - Level 1
Unique #	**b9cfa030-5610-428b-93cc-de090beee728**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of detected SSL/TLS protocol properties.

Impact

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non- AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution

N/A

SSL Data

Flags	-

VULNERABILITY ASSESSMENT REPORT

Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Heartbeat no Cipher_priority_controlled_by client OCSP_stapling no SCT_extensi TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by client OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	yes	TLSv1.2
Heartbeat	no	TLSv1.2
Cipher priority controlled by	client	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2
Heartbeat	no	TLSv1.3
Cipher priority controlled by	client	TLSv1.3
OCSP stapling	no	TLSv1.3
SCT extension	no	TLSv1.3

INFO **38718 Secure Sockets Layer (SSL) Certificate Transparency Information** (1)

INFO 38718 Secure Sockets Layer (SSL) Certificate Transparency Information

Finding #	**1034161**(73639759)	**Severity**	Information Gathered - Level 1
Unique #	**04468347-0c9f-4626-8e73-c7807a58ca07**		
Group	Scan Diagnostics	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	#table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=*.ayabank.com,O=Ayeyarwady_Bank_Limited,L=Yangon,C=MM _ _ _ Certificate (unknown) (unknown) eecdd064d5db1acec55cb79db4cd13a23287467cbcecdec351485946711fb59b Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 73d99e891b4c9678a0207d479de6b2c61cd0515e71192a8c6b80107ac17772b5 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate n (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT

Info List

Info #1

Certificate Fingerprint:D90041DF8A12813735228A3BF55E7D13BC53EF0E5A8799FE9D72B2C79DCA7F2F

INFO 42350 TLS Secure Renegotiation Extension Support Information (1)

INFO 42350 TLS Secure Renegotiation Extension Support Information

Finding #	**1034165**(73639761)	Severity	Information Gathered - Level 1
Unique #	7c24c9fe-bd80-4c9b-9720-b0c1704ae32b		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

INFO *45038 Host Scan Time - Scanner* *(1)*

INFO 45038 Host Scan Time- Scanner

Finding #	**1034153**(73639751)	Severity	Information Gathered - Level 1
Unique #	**3f66128d-0287-466e-a072-2ccbbd702f7e**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact

N/A

Solution

N/A

Results

Scan duration: 6764 seconds

Start time: Thu, Jul 06 2023, 04:35:09 GMT

End time: Thu, Jul 06 2023, 06:27:53 GMT

INFO *86002 SSL Certificate - Information* *(1)*

INFO 86002 SSL Certificate- Information

Finding #	**1034160**(73639758)	**Severity**	Information Gathered - Level 1
Unique #	**90289b09-10b0-4ac3-9106-9358f7442c79**		
Group	Scan Diagnostics	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL certificate information is provided in the Results section.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	www.ayabank.com
IP	169.60.37.100
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _06:31:cd:78:80:1b:d7:26:27:5a:71:0c:8d:37:8a:4e_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_TLS_RSA_SHA256_2020_CA1 (0)SUBJECT_NAME _ countryName MM _localityName Yangon _organizationName Ayeyarwady_Bank_Limited _commonName *.ayabank.com (0)Valid_From Mar_15_00:00:00_2023_GMT (0)Valid_Till Apr_5_23:59:59_2024_GMT (0)Public_Key_Algorithm rsaEncrypti (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:a1:2f:57:da:62:a3:5b:bc:a3:69:7b:20:6b:37: (0) _9d:15:4d:3f:72:e8:f9:4e:d8:5b:ad:36:35:be:69: (0) _3e:da:83:01:0a:82:97:c8:20:66:16:18:9b:57:f7: (0) _f1:cc:40:bd:92:e6:44:73:6e:d1:04:82:d0:ef:e7: (0) _48:69:60:23:c0:fa:e3:91:3b:75:bd:4f:11:c7:9c: (0) _0c:05:16:5b:e0:99:fd:b0:6e:1c:79:e8:5c:0e:ce: (0) _a7:2f:f5:79:f1:0d:49:ec:f6:b2:bd:05:39:f6:77: (0) _3a:13:74:4f:a8:b4:26:fb:32:e0:cf:29:e0:ad:4e: (0) _e7:a0:14:a7:e4:f0:4d:a9:5b:8f:6f:ce:26:bc:c4: (0) _5a:04:78:e8:9d:df:cc:07:eb:ca:fb:48:e4:f8:4c: (0) _00:37:22:1a:e8:3c:80:98:cc:7b:a1:fe:45:1e: (0) _75:de:46:2b:b6:1f:27:b5:c8:ef:4b:17:9d:11:e0: (0) _0e:d3:08:bc:1f:09:f9:d5:61:b8:a5:7c:f2:76:29: (0) _7b:27:e7:25:a3:cd:ea:ca:1f:ee:47:93:01:42:7f: (0) _2c:87:be:78:0f:93:4c:96:5e:7d:e4:aa:1b:64:ef: (0) _8d:6e:f5:e1:16:b7:08:ed:2d:82:f2:44:a8:63:a1: (0) _5b:56:28:63:01:aa:1d:4d:ac:a1:f3:fc:f1:6c:9f: (0) _f3:1f (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier

```
_keyid:B7:6B:A2:EA:A8:AA:84:8C:79:EA:B4:DA:0F:98:B2:C5:95:76:B9:F4 (0)X509v3_Subject_Key_Identifier _58:C1:F1:83:7E:F2:11:32:ED:
8E:E7:B8:22:C3:DB:E5:AC:06:E2:76 (0)X509v3_Subject_Alternative_Name _DNS:*.ayabank.com,_DNS:ayabank.com (0)X509v3_Key_Usage critical (0)
_Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication
(0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl (0) (0) _Full_Name: (0) _URI:ht
crl4.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.2 (0) _CPS:_http://www.digicert.com/CPS
(0)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (0) _CA_Issuers_-_URI:http://cacerts.digicert.com/
DigiCertTLSRSASHA2562020CA1-1.crt (0)X509v3_Basic_Constraints _CA:FALSE (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0)
_Version_:_v1_(0x0) (0) _Log_ID_:_EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2: (0) _32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B (0)
_Timestamp_:_Mar_15_04:37:28.707_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:79:49:AC:D6:C6:D6:8E:
65:C6:A1:BB:67: (0) _30:F3:7C:F4:38:B1:7E:1A:5F:C4:61:78:8E:0C:47:C7: (0) _0F:3B:A4:26:02:21:00:C4:49:05:AE:F3:F0:09:97:7F: (0) _B2:34:24:34:3A:CD
52:AA:EC:F6:C4:08:E5:1A:48:82: (0) _A7:69:82:D6:2F:F1:8E (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_73:D9:9E:89:1B:4
96:78:A0:20:7D:47:9D:E6:B2:C6: (0) _1C:D0:51:5E:71:19:2A:8C:6B:80:10:7A:C1:77:72:B5 (0) _Timestamp_:_Mar_15_04:37:28.769_2023_GMT (0)
_Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:46:02:21:00:AC:46:B1:33:7A:CF:46:45:AA:04:AA: (0) _14:D5:DB:C7:74:E2:1F:40:B7:DA:E4
7C:44:79:99: (0) _81:EC:27:F3:5C:02:21:00:BB:02:30:99:3E:91:17:6E: (0) _2B:14:70:BC:69:25:DB:1F:69:D0:F6:CA:69:BF:6E:7E: (0) _D6:C5:10:23:02:18:38
(0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2
81:D9:BB:BF:AB:39:D8:84:73 (0) _Timestamp_:_Mar_15_04:37:28.724_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0)
_30:44:02:20:73:BE:74:3B:F0:04:C1:AD:52:B5:01:45: (0) _5B:3D:DF:01:40:AA:2D:C1:04:73:00:7B:20:FE:00:C9: (0) _F9:49:E2:CA:02:20:6E:47:D8:C4:37:BD
4E:A6:06:D9: (0) _A3:BB:42:67:BD:F7:F3:67:84:90:9C:5F:D7:2E:74:8A: (0) _91:DA:18:6A:BE:5B (0)Signature (256_octets) (0) 55:7b:68:f7:3a:06:a9:5c:
32:7d:a1:46:93:b1:cf:bc (0) 35:f0:26:9b:bc:44:f5:2a:6f:61:a5:2b:ea:cc:e0:86 (0) 53:da:50:e1:36:3e:48:ea:13:aa:8c:d2:44:a0:6f:52 (0) 14:41:3e:44:99:d6:34:76:
7f:f7:83:cf:42:e1:f1 (0) 04:fa:ed:55:26:77:eb:5a:fa:ef:a0:50:c8:9c:f5:46 (0) 8c:f1:82:7a:c1:42:35:40:1b:c3:42:27:22:14:c9:60 (0)
d3:69:51:5a:b4:97:7f:d9:80:bf:a7:a7:60:ac:08:59 (0) 18:fc:9b:7c:4d:3a:9c:17:85:ef:ef:eb:d4:e2:1a:3f (0) 51:49:87:72:81:9e:28:76:ab:97:fb:62:ce:44:de:c2 (0)
93:55:17:4b:62:b3:20:52:2d:16:90:85:83:65:56:88 (0) a3:d2:17:2e:77:39:da:d3:42:8d:7e:e6:60:a7:31:d5 (0) cb:da:2a:51:73:18:1c:38:43:9c:30:b0:12:e1:ea:aa
6d:c5:d4:68:43:ad:c1:9d:94:0b:b5:92:1c:b4:58:af (0) eb:fa:5f:b8:2a:e5:75:86:32:a4:a6:87:8a:89:1b:f0 (0) ad:e7:49:ae:d4:a0:68:1e:72:3b:d9:37:51:e7:7d:be (0)
70:ec:b2:00:1a:bf:b6:13:f2:80:5f:cc:b4:0a:e9:9f (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _06:d8:d9:04:d5:58:43:46:f6:8a:2f:a7:54:22:7e:c4
(1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName
www.digicert.com _commonName DigiCert_Global_Root_CA (1)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _commonName
```

```
DigiCert_TLS_RSA_SHA256_2020_CA1 (1)Valid_From Apr_14_00:00:00_2021_GMT (1)Valid_Till Apr_13_23:59:59_2031_GMT (1)Public_Key_Algorithm
rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulus: (1) _00:c1:4b:b3:65:47:70:bc:dd:4f:58:db:ec:9c:ed: (1) _c3:66
31:13:54:ad:4a:66:46:1f:2c:0a:ec: (1) _64:07:e5:2e:dc:dc:b9:0a:20:ed:df:e3:c4:d0:9e: (1) _9a:a9:7a:1d:82:88:e5:11:56:db:1e:9f:58:c2:51: (1) _e7:2c:34:0d:
2e:d2:92:e1:56:cb:f1:79:5f:b3:bb: (1) _87:ca:25:03:7b:9a:52:41:66:10:60:4f:57:13:49: (1) _f0:e8:37:67:83:df:e7:d3:4b:67:4c:22:51:a6:df: (1) _0e:99:10:ed:
57:51:74:26:e2:7d:c7:ca:62:2e:13: (1) _1b:7f:23:88:25:53:6f:c1:34:58:00:8b:84:ff:f8: (1) _be:a7:58:49:22:7b:96:ad:a2:88:9b:15:bc:a0:7c: (1) _df:e9:51:a8:d5:
37:e2:36:b4:82:4b:62:b5: (1) _49:9a:ec:c7:67:d6:e3:3e:f5:e3:d6:12:5e:44:f1: (1) _bf:71:42:7d:58:84:03:80:b1:81:01:fa:f9:ca:32: (1) _bb:b4:8e:27:87:27:c5:2b
74:d4:a8:d6:97:de:c3: (1) _64:f9:ca:ce:53:a2:56:bc:78:17:8e:49:03:29:ae: (1) _fb:49:4f:a4:15:b9:ce:f2:5c:19:57:6d:6b:79:a7: (1) _2b:a2:27:20:13:b5:d0:3d:
40:d3:21:30:07:93:ea: (1) _99:f5 (1) _Exponent:_65537_(0x10001) (1)X509v3_EXTENSIONS _ (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathle
(1)X509v3_Subject_Key_Identifier _B7:6B:A2:EA:A8:AA:84:8C:79:EA:B4:DA:0F:98:B2:C5:95:76:B9:F4 (1)X509v3_Authority_Key_Identifier _keyid:03:DE:
50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign
(1)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)Authority_Information_Access _OCSP_-_URI:ht
ocsp.digicert.com (1) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertGlobalRootCA.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1)
_URI:http://crl3.digicert.com/DigiCertGlobalRootCA.crl (1)X509v3_Certificate_Policies _Policy:_2.16.840.1.114412.2.1 (1) _Policy:_2.23.140.1.1 (1)
_Policy:_2.23.140.1.2.1 (1) _Policy:_2.23.140.1.2.2 (1) _Policy:_2.23.140.1.2.3 (1)Signature (256_octets) (1) 80:32:ce:5e:0b:dd:6e:5a:0d:0a:af:e1:d6:84:cb:
8e:fa:85:70:ed:da:5d:b3:0c:f7:2b:75:40:fe:85:0a (1) fa:f3:31:78:b7:70:4b:1a:89:58:ba:80:bd:f3:6b:1d (1) e9:7e:cf:0b:ba:58:9c:59:d4:90:d3:fd:6c:fd:d0:98 (1)
6d:b7:71:82:5b:cf:6d:0b:5a:09:d0:7b:de:c4:43:d8 (1) 2a:a4:de:9e:41:26:5f:bb:8f:99:cb:dd:ae:e1:a8:6f (1) 9f:87:fe:74:b7:1f:1b:20:ab:b1:4f:c6:f5:67:5d:5d (1) 9
3c:e9:ff:69:f7:61:6c:d6:d9:f3:fd:36:c6:ab:03 (1) 88:76:d2:4b:2e:75:86:e3:fc:d8:55:7d:26:c2:11:77 (1) df:3e:02:b6:7c:f3:ab:7b:7a:86:36:6f:b8:f7:d8:93 (1) 71:cf
73:30:fa:7b:ab:ed:2a:59:c8:42:84:3b (1) 11:17:1a:52:f3:c9:0e:14:7d:a2:5b:72:67:ba:71:ed (1) 57:47:66:c5:b8:02:4a:65:34:5e:8b:d0:2a:3c:20:9c (1)
51:99:4c:e7:52:9e:f7:6b:11:2b:0d:92:7e:1d:e8:8a (1) eb:36:16:43:87:ea:2a:63:bf:75:3f:eb:de:c4:03:bb (1) 0a:3c:f7:30:ef:eb:af:4c:fc:8b:36:10:73:3e:f3:a4
```

Info List

Info #1

Certificate Fingerprint:D90041DF8A12813735228A3BF55E7D13BC53EF0E5A8799FE9D72B2C79DCA7F2F

Info #2

Certificate Fingerprint:52274C57CE4DEE3B49DB7A7FF708C040F771898B3BE88725A86FB4430182FE14

INFO **150009 Links Crawled** (1)

VULNERABILITY ASSESSMENT REPORT

INFO 150009 Links Crawled

Finding #	**1034157**(73639755)	Severity	Information Gathered - Level 1
Unique #	**3dfa7377-9d25-4b15-a3ad-36b806b74d5c**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled, and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 934.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

https://www.ayabank.com/
https://www.ayabank.com/?s=discovery
https://www.ayabank.com/about-aya
https://www.ayabank.com/about-aya/governance
https://www.ayabank.com/about-aya/governance/compliance
https://www.ayabank.com/about-aya/governance/compliance/aml-cft https://www.ayabank.com/about-aya/governance/corporate-governance https://www.ayabank.com/about-aya/governance/risk-management
https://www.ayabank.com/about-aya/governance/risk-management/managing-risk
https://www.ayabank.com/about-aya/governance/risk-management/risk-governance
https://www.ayabank.com/about-aya/governance/risk-management/risk-management-control
https://www.ayabank.com/about-aya/governance/risk-management/risk-management-framework
https://www.ayabank.com/about-aya/message-from-chairman
https://www.ayabank.com/about-aya/news-room https://www.ayabank.com/about-aya/news-room/corporate-

news
https://www.ayabank.com/about-aya/news-room/corporate-news/2020_Best_Bank_for_SMEs_Award from_AsiaMoney https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Bank_Offering_Apprenticeship_Opportunity https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Bank_PCL_Foreign_Currency_Online_Trading
https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%25E2%2580%2599s_10th_Homage_Ceremony
https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%25E2%2580%2599s_Family_Celebrating_10th_Kathina_Civara_Dana_Ceremony
https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%E2%80%99s_10th_Homage_Ceremony
https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%E2%80%99s_Family_Celebrating_10th_Kathina_Civara_Dana_Ceremony
https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_SOMPO_General_Insurance_Awareness_and_Sale_Marketing_Training https://www.ayabank.com/about-aya/news-room/corporate-news/Achievement_of_Silver_Award_for_Myanmar_Employer_Awards_2019
https://www.ayabank.com/about-aya/news-room/corporate-news/Asia_Money_2019_Awards_Best_Bank_for_SMEs_%22_Best_Bank_for_CSR Asia_Money_2019_Best_Bank_for_SMEs
https://www.ayabank.com/about-aya/news-room/corporate-news/Asia_Money_2019_Awards_Best_Bank_for_SMEs_&_Best_Bank_for_CSR Asia_Money_2019_Best_Bank_for_SMEs
https://www.ayabank.com/about-aya/news-room/corporate-news/Completion_of_Basic_Banking_Operations_Training_No8
https://www.ayabank.com/about-aya/news-room/corporate-news/First_Bank_in_Myanmar_for_achieving_EDGE_Certificate_for_Gender_Equality
https://www.ayabank.com/about-aya/news-room/corporate-news/Green_Energy_Exhibition_Banking_Partner
https://www.ayabank.com/about-aya/news-room/corporate-news/MOU_between_Mandalay_Smart_Pay_and_AYA_Bank
https://www.ayabank.com/about-aya/news-room/corporate-news/Memorandum_of_Understanding_Signing_Ceremony_between_AYA_Bank_and_Smart_Myanmar https://www.ayabank.com/about-aya/news-room/corporate-news/Pioneering_Green_Financing_for_Electric_Vehicles
https://www.ayabank.com/about-aya/news-room/corporate-news/Publication_of_Report_on_Myanmar%25E2%2580%2599s_Business_Transparency_2019_Pwint_Thit_Sa
https://www.ayabank.com/about-aya/news-room/corporate-news/Publication_of_Report_on_Myanmar%E2%80%99s_Business_Transparency_2019_Pwint_Thit_Sa https://www.ayabank.com/about-aya/news-room/corporate-news/Siam_Commercial_Bank_PCL_and_AYA_Sign_MOU
https://www.ayabank.com/about-aya/news-room/corporate-news/The_opening_of_the_261_branch_of_AYA_Bank https://www.ayabank.com/about-aya/news-room/corporate-news/Top_Income_Tax_Payer

https://www.ayabank.com/about-aya/news-room/corporate-news/Workshop_for_Certified_Branch_Managers_Program https://www.ayabank.com/about-aya/news-room/corporate-news/year
https://www.ayabank.com/about-aya/news-room/corporate-news/year/2019
https://www.ayabank.com/about-aya/news-room/corporate-news/year/2020
https://www.ayabank.com/about-aya/news-room/corporate-news/year/2023
https://www.ayabank.com/about-aya/news-room/corporate-news?page=1
https://www.ayabank.com/about-aya/news-room/corporate-news?page=2
https://www.ayabank.com/about-aya/news-room/corporate-news?page=3
https://www.ayabank.com/about-aya/news-room/reports https://www.ayabank.com/about-aya/who-we- https://www.ayabank.com/about-aya/who-we-/leadership https://www.ayabank.com/about-aya/who-we-are https://www.ayabank.com/about-aya/who-we-are/corporate-profile
https://www.ayabank.com/about-aya/who-we-are/corporate-profile/ayabank-profile https://www.ayabank.com/about-aya/who-we-are/corporate-profile/ayabank-profile/business-practices https://www.ayabank.com/about-aya/who-we-are/corporate-profile/ayabank-profile/shareholding-information https://www.ayabank.com/about-aya/who-we-are/corporate-profile/mission-corporate-value-brand-promise https://www.ayabank.com/about-aya/who-we-are/leadership
https://www.ayabank.com/about-aya/who-we-are/leadership/meet-our-leaders https://www.ayabank.com/about-aya/who-we-are/leadership/meet-our-leaders/contact-to-board https://www.ayabank.com/about-aya/who-we-are/our-strategies
https://www.ayabank.com/about-aya/who-we-are/our-strategies/corporate-strategy https://www.ayabank.com/about-aya/who-we-are/our-strategies/stakeholder-management https://www.ayabank.com/account-saving
https://www.ayabank.com/account-saving/current-deposit
https://www.ayabank.com/business https://www.ayabank.com/business-banking https://www.ayabank.com/business-banking/account-saving
https://www.ayabank.com/business-banking/borrowing
https://www.ayabank.com/business-banking/insurance
https://www.ayabank.com/business-banking/remittance
https://www.ayabank.com/business-banking/trade
https://www.ayabank.com/business/account-saving
https://www.ayabank.com/business/account-saving/call-deposit
https://www.ayabank.com/business/account-saving/current-deposit
https://www.ayabank.com/business/account-saving/fixed-deposit
https://www.ayabank.com/business/account-saving/saving-deposit
https://www.ayabank.com/business/borrowing
https://www.ayabank.com/business/borrowing/corporate-business-loan
https://www.ayabank.com/business/borrowing/hire-purchase
https://www.ayabank.com/business/borrowing/sme
https://www.ayabank.com/business/cash-management
https://www.ayabank.com/business/insurance
https://www.ayabank.com/business/insurance/car-ear
https://www.ayabank.com/business/insurance/domestic-inland-transit
https://www.ayabank.com/business/insurance/domestic-marine-cargo
https://www.ayabank.com/business/insurance/group-life
https://www.ayabank.com/business/insurance/industrial-all-risk
https://www.ayabank.com/business/insurance/oversea-marine-cargo
https://www.ayabank.com/business/remittance-payments
https://www.ayabank.com/business/remittance-payments/images
https://www.ayabank.com/business/remittance-payments/images/get_start_bg.jpg
https://www.ayabank.com/business/remittance-payments/international-payments
https://www.ayabank.com/business/remittance-payments/local-payments
https://www.ayabank.com/business/trade https://www.ayabank.com/business/trade/trade-financing https://www.ayabank.com/business/trade/trade-services
https://www.ayabank.com/digital-services
https://www.ayabank.com/digital-services/atm https://www.ayabank.com/digital-services/card-services https://www.ayabank.com/digital-services/card-services/card-privilege https://www.ayabank.com/digital-services/card-services/credit-card
https://www.ayabank.com/digital-services/card-services/debit-card
https://www.ayabank.com/digital-services/card-services/images
https://www.ayabank.com/digital-services/card-services/images/JBC_UPI_card.png https://www.ayabank.com/digital-services/card-services/images/MPU_JCB_card.png https://www.ayabank.com/digital-services/card-services/images/prepaid https://www.ayabank.com/digital-services/card-services/images/prepaid/card_block_termination.png https://www.ayabank.com/digital-services/card-services/images/prepaid/statement_inquiry.png https://www.ayabank.com/digital-services/card-services/images/simplepay
https://www.ayabank.com/digital-services/card-services/images/simplepay/how_to_apply_bg.jpg https://www.ayabank.com/digital-services/card-services/merchant-services https://www.ayabank.com/digital-services/card-services/merchant-services/ecommerce https://www.ayabank.com/digital-services/card-services/merchant-services/images
https://www.ayabank.com/digital-services/card-services/merchant-services/images/MPU_ecommerce_registration.jpg
https://www.ayabank.com/digital-services/card-services/merchant-services/images/how_to_apply_bg.jpg
https://www.ayabank.com/digital-services/card-services/merchant-services/images/how_to_apply_mobile_bg.jpg
https://www.ayabank.com/digital-services/card-services/merchant-services/pos
https://www.ayabank.com/digital-services/card-services/prepaid-card https://www.ayabank.com/digital-services/card-services/reset-pin https://www.ayabank.com/digital-services/card-services/simple-pay
https://www.ayabank.com/digital-services/guideline https://www.ayabank.com/digital-services/guideline/digital-secure https://www.ayabank.com/digital-services/guideline/digital-secure/images
https://www.ayabank.com/digital-services/guideline/digital-secure/images/MPU_ecommerce_registration.jpg

https://www.ayabank.com/digital-services/guideline/digital-secure/images/how_to_apply_bg.jpg https://www.ayabank.com/digital-services/guideline/digital-secure/images/how_to_apply_mobile_bg.jpg https://www.ayabank.com/digital-services/guideline/digital-secure/sms-alert https://www.ayabank.com/digital-services/guideline/frequently-used-digital https://www.ayabank.com/digital-services/online-payment-services
https://www.ayabank.com/digital-services/online-payment-services/corporate-internet-banking
https://www.ayabank.com/digital-services/online-payment-services/images https://www.ayabank.com/digital-services/online-payment-services/images/get_start_bg.jpg https://www.ayabank.com/digital-services/online-payment-services/internet-banking https://www.ayabank.com/digital-services/online-payment-services/mobile-banking https://www.ayabank.com/digital-services/wallet-solution
https://www.ayabank.com/digital-services/wallet-solution/aya-pay
https://www.ayabank.com/enquiry
https://www.ayabank.com/enquiry_form_submit
https://www.ayabank.com/fonts/boxicons/boxicons.svg?
https://www.ayabank.com/images/Background.png
https://www.ayabank.com/images/IB_KV.jpg
https://www.ayabank.com/images/MPU_ecommerce_registration_2.jpg
https://www.ayabank.com/images/MobileBanking_KV.jpg
https://www.ayabank.com/images/POS/KV.jpg
https://www.ayabank.com/images/about-aya/aml-cft/KV.webp
https://www.ayabank.com/images/about-aya/ayabank-profile/BG.webp
https://www.ayabank.com/images/about-aya/ayabank-profile/KV.webp
https://www.ayabank.com/images/about-aya/ayabank-profile/a_driver_growth.webp https://www.ayabank.com/images/about-aya/ayabank-profile/business_practices.webp https://www.ayabank.com/images/about-aya/ayabank-profile/consumer_financial_protection.webp https://www.ayabank.com/images/about-aya/ayabank-profile/financial_inclusion.webp
https://www.ayabank.com/images/about-aya/ayabank-profile/financial_inclusion_red.webp https://www.ayabank.com/images/about-aya/ayabank-profile/full_service_bank.webp https://www.ayabank.com/images/about-aya/ayabank-profile/responsible_lending.webp
https://www.ayabank.com/images/about-aya/ayabank-profile/share_holding_information.webp
https://www.ayabank.com/images/about-aya/ayabank-profile/transparent_marketing.webp https://www.ayabank.com/images/about-aya/chairman-message/KV.webp https://www.ayabank.com/images/about-aya/corporate-governance/KV.webp
https://www.ayabank.com/images/about-aya/corporate-profile/mission-promise/KV.webp https://www.ayabank.com/images/about-aya/corporate-profile/mission-promise/our_brand_promise.webp https://www.ayabank.com/images/about-aya/corporate-strategy/KV.webp https://www.ayabank.com/images/about-aya/corporate-strategy/credit_infra.webp
https://www.ayabank.com/images/about-aya/corporate-strategy/digitalization.webp https://www.ayabank.com/images/about-aya/corporate-strategy/innovation.webp https://www.ayabank.com/images/about-aya/corporate-strategy/our_key_enablers_bg.webp
https://www.ayabank.com/images/about-aya/corporate-strategy/sale_productivity.webp https://www.ayabank.com/images/about-aya/meet-our-leaders/KV.webp https://www.ayabank.com/images/about-aya/report/KV.webp
https://www.ayabank.com/images/about-aya/risk-management/KV.webp
https://www.ayabank.com/images/about-aya/risk-management/compliance_KV.webp
https://www.ayabank.com/images/about-aya/risk-management/managing_risk_KV.webp
https://www.ayabank.com/images/about-aya/risk-management/risk_governane_KV.webp
https://www.ayabank.com/images/about-aya/risk-management/risk_mgmt_ctl_KV.webp
https://www.ayabank.com/images/about-aya/risk-management/risk_mgmt_framework_KV.webp
https://www.ayabank.com/images/about-aya/stakeholder-management/KV.webp
https://www.ayabank.com/images/acc_saving/aya-loyal-saving/KV.jpg
https://www.ayabank.com/images/acc_saving/aya-maximizer-saving/KV.jpg
https://www.ayabank.com/images/acc_saving/aya-regular-saving/KV.jpg
https://www.ayabank.com/images/acc_saving/aya-su-buu/KV.jpg
https://www.ayabank.com/images/acc_saving/call_deposit/KV.jpg
https://www.ayabank.com/images/acc_saving/current_deposit/KV.jpg
https://www.ayabank.com/images/acc_saving/fixed-deposit/KV.jpg
https://www.ayabank.com/images/acc_saving/new_business_call/KV.jpg
https://www.ayabank.com/images/acc_saving/new_business_curr_acc/KV.jpg
https://www.ayabank.com/images/acc_saving/ngwe-toe-shwe-o/KV.jpg
https://www.ayabank.com/images/acc_saving/premium_call_deposit/KV.jpg
https://www.ayabank.com/images/acc_saving/regular_curr_acc/KV.jpg
https://www.ayabank.com/images/acc_saving/retail_fca_curr_acc/KV.jpg
https://www.ayabank.com/images/acc_saving/saving-deposit/KV.jpg
https://www.ayabank.com/images/acc_saving/seafarer/KV.jpg
https://www.ayabank.com/images/atm/KV.jpg
https://www.ayabank.com/images/ayaicon.png
https://www.ayabank.com/images/ayapay/KV.webp
https://www.ayabank.com/images/ayapay/agent.png
https://www.ayabank.com/images/ayapay/explore_bg.png
https://www.ayabank.com/images/ayapay/merchant.png
https://www.ayabank.com/images/borrowing/hire_purchase/auto_loan/Available-Brands.jpg
https://www.ayabank.com/images/borrowing/hire_purchase/auto_loan/KV.jpg
https://www.ayabank.com/images/borrowing/hire_purchase/auto_loan/eligibility_calculate_laptop_bg.png
https://www.ayabank.com/images/borrowing/hire_purchase/auto_loan/income_document_bg_4.png
https://www.ayabank.com/images/borrowing/hire_purchase/c2c_auto_loan/KV.jpg
https://www.ayabank.com/images/borrowing/hire_purchase/construction_loan/KV.jpg
https://www.ayabank.com/images/borrowing/hire_purchase/education_loan/KV.jpg
https://www.ayabank.com/images/borrowing/hire_purchase/home_loan/KV.jpg https://www.ayabank.com/images/business/account-saving/call-deposit/KV.jpg https://www.ayabank.com/images/business/account-saving/current-deposit/KV.jpg https://www.ayabank.com/images/business/account-saving/fixed-deposit/KV.jpg https://www.ayabank.com/images/business/account-saving/saving-deposit/KV.jpg
https://www.ayabank.com/images/business/borrowing/corporate-business-loan/KV.jpg

https://www.ayabank.com/images/business/borrowing/hire-purchase/KV.jpg
https://www.ayabank.com/images/business/borrowing/sme/KV.jpg
https://www.ayabank.com/images/business/borrowing/sme/testimonial_border_2.png
https://www.ayabank.com/images/business/cash-management/KV.jpg
https://www.ayabank.com/images/business/insurance/IAR/KV_bg.png
https://www.ayabank.com/images/business/insurance/car-ear/KV_bg.png
https://www.ayabank.com/images/business/insurance/domestic-inland-transit/KV_bg.png
https://www.ayabank.com/images/business/insurance/domestic-marine-cargo/KV_bg.png
https://www.ayabank.com/images/business/insurance/oversea-marine-cargo/KV_bg.png
https://www.ayabank.com/images/business/remittance/international-payments/KV.jpg
https://www.ayabank.com/images/business/remittance/local-payments/KV.jpg
https://www.ayabank.com/images/business/remittance/local-payments/create_payment_order_bg.png
https://www.ayabank.com/images/business/trade/trade-financing/KV.jpg
https://www.ayabank.com/images/business/trade/trade-financing/margin-financing.png
https://www.ayabank.com/images/business/trade/trade-services/KV.jpg
https://www.ayabank.com/images/business/trade/trade-services/letter-of-credit.png
https://www.ayabank.com/images/business/trade/trade-services/performance-based-guarantee.png
https://www.ayabank.com/images/corporate_internet_banking/KV.jpg
https://www.ayabank.com/images/corporate_internet_banking/basic.jpg
https://www.ayabank.com/images/corporate_internet_banking/basic_plus.jpg
https://www.ayabank.com/images/credit_KV.jpg
https://www.ayabank.com/images/debit_KV2.jpg
https://www.ayabank.com/images/digital_secure/KV.jpg
https://www.ayabank.com/images/dropdown_arrow.png
https://www.ayabank.com/images/ecommerce/KV.jpg
https://www.ayabank.com/images/frequently/KV.jpg
https://www.ayabank.com/images/get_start_bg.jpg https://www.ayabank.com/images/hand-with-card%20MPU-JCB.png https://www.ayabank.com/images/home/KV_slider_2.webp
https://www.ayabank.com/images/how_to_apply.jpg
https://www.ayabank.com/images/how_to_apply_bg.jpg
https://www.ayabank.com/images/insurance/PA/KV_bg.png
https://www.ayabank.com/images/insurance/aya-go/KV_bg.png
https://www.ayabank.com/images/insurance/aya-joy/KV_bg.png
https://www.ayabank.com/images/insurance/fire/KV_bg.png
https://www.ayabank.com/images/insurance/health/KV_bg.png
https://www.ayabank.com/images/insurance/life/KV_bg.png
https://www.ayabank.com/images/insurance/motor/KV_bg.png
https://www.ayabank.com/images/internet_banking/SMS%20OTP%20with%20do%20not%20share.jpg
https://www.ayabank.com/images/internet_banking/i-Banking%20-%20Bill%20Payment.png
https://www.ayabank.com/images/internet_banking/i-Banking%20-%20Get%20Your%20Statement.png
https://www.ayabank.com/images/internet_banking/i-Banking%20-%20Mobile%20TopUp.png
https://www.ayabank.com/images/jcb_credit_banner_2.jpg
https://www.ayabank.com/images/more_support.png
https://www.ayabank.com/images/new_home/KV_slider_2.webp
https://www.ayabank.com/images/new_home/KV_slider_3.webp
https://www.ayabank.com/images/new_home/KV_slider_4.webp
https://www.ayabank.com/images/new_home/KV_slider_5.webp
https://www.ayabank.com/images/new_home/atm_branch_fx_counter.webp
https://www.ayabank.com/images/new_home/award_accolades_bg.webp
https://www.ayabank.com/images/new_home/ayapay_wallet.webp
https://www.ayabank.com/images/new_home/business.webp
https://www.ayabank.com/images/new_home/desk_poster.webp
https://www.ayabank.com/images/new_home/mbanking.webp
https://www.ayabank.com/images/new_home/personal_borrowing_plan.webp
https://www.ayabank.com/images/news_image/view_all_news.webp https://www.ayabank.com/images/other-services/foreign-currency-exchange/KV.jpg https://www.ayabank.com/images/other-services/safe-deposit/KV.jpg https://www.ayabank.com/images/premium-banking/KV.jpg
https://www.ayabank.com/images/premium-banking/bg.jpg
https://www.ayabank.com/images/premium-banking/explore_membership_bg.jpg
https://www.ayabank.com/images/premium-banking/intro-bg.jpg
https://www.ayabank.com/images/premium-banking/novotel_branch_bg.jpg
https://www.ayabank.com/images/premium-banking/package_B_bottom_bg.png
https://www.ayabank.com/images/premium-banking/package_C_bottom_bg.png
https://www.ayabank.com/images/premium-banking/package_bottom_bg.png
https://www.ayabank.com/images/premium-banking/plan_section_bottom_bg.png
https://www.ayabank.com/images/prepaid/KV.jpg
https://www.ayabank.com/images/prepaid/card_block_termination.png
https://www.ayabank.com/images/prepaid/how_to_apply_bg.jpg
https://www.ayabank.com/images/prepaid/statement_inquiry.png
https://www.ayabank.com/images/remittance/inter/KV.jpg
https://www.ayabank.com/images/remittance/local/KV.jpg
https://www.ayabank.com/images/remittance/payment/KV.jpg
https://www.ayabank.com/images/simple_pay_installment.png
https://www.ayabank.com/images/simplepay/KV.jpg
https://www.ayabank.com/images/simplepay/contact_center_bg.png
https://www.ayabank.com/images/simplepay/how_to_apply_bg.jpg
https://www.ayabank.com/images/sms/KV.jpg https://www.ayabank.com/personal-banking
https://www.ayabank.com/personal-banking/account-saving https://www.ayabank.com/personal-banking/account-saving/call-deposit https://www.ayabank.com/personal-banking/account-saving/call-deposit/new-business-call
https://www.ayabank.com/personal-banking/account-saving/call-deposit/premium-call-deposit
https://www.ayabank.com/personal-banking/account-saving/current-deposit

https://www.ayabank.com/personal-banking/account-saving/current-deposit/new-business-current-account
https://www.ayabank.com/personal-banking/account-saving/current-deposit/regular-current-account
https://www.ayabank.com/personal-banking/account-saving/current-deposit/retail-fca-current
https://www.ayabank.com/personal-banking/account-saving/current-deposit/seafarer-acount
https://www.ayabank.com/personal-banking/account-saving/fixed-deposit https://www.ayabank.com/personal-banking/account-saving/saving-deposit https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-loyal-saving https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-maximizer-saving

INFO *150010 External Links Discovered* *(1)*

INFO 150010 External Links Discovered

Finding #	**1034156**(73639754)	Severity	Information Gathered - Level 1
Unique #	**520ab456-c916-41e3-a8bb-d6038d8967e2**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact

N/A

Solution

N/A

Results

```
Number of links: 73
https://prepaidcard.ayabank.com/
https://www.google-analytics.com/analytics.js
https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1758528169&t=pageview&_s=1&dl=https%3A%2F%2Fwww.ayabank.com%2Fdigital-services%2Fcard-services%2Fsimple-pay&ul=en-
us&de=UTF-8&dt=Simple%20Pay%20%E2%80%93%20AYA%20Bank&sd=32-
bit&sr=240x320&vp=1024x768&je=1&fl=10.3%20r183&_u=YEBAAUQAAAAAACAAI~&jid=1306466345&gjid=434993267&cid=1461755228.1688618393&tid=UA-228606560-1&_gid=91976293


https://cardpin.ayabank.com/
https://www.google.com/maps/d/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI&ehbc=2E312F
https://www.google.com/maps/d/u/0/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI%22ehbc=2E312F
https://www.google.com/maps/d/u/0/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI&ehbc=2E312F
https://www.linkedin.com/company/ayabank/
https://fonts.gstatic.com/
https://fonts.gstatic.com/s/nunito/v25/XRXI3I6Li01BKofiOc5wtlZ2di8HDLshdTQ3iazbXWjgeg.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmScMnk-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSdSn0-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSdSnk-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSdgnk-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSe1mU-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSeMmU-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSfSmU-NKQRDA8i1P4w.woff
https://fonts.gstatic.com/s/sora/v11/xMQOuFFYT72X5wkB_18qmnndmSfSnk-NKQRDA8i1P4w.woff
https://fonts.googleapis.com/
https://fonts.googleapis.com/css2?family=Nunito%22display=swap
https://fonts.googleapis.com/css2?family=Nunito&display=swap
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800%22display=swap
```

https://appgallery.huawei.com/app/C101771299
https://www.facebook.com/ayabank/
https://homecalc.ayabank.com/
https://creditcard.ayabank.com/
https://www.ayapay.com/
https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j101&tid=UA-228606560-1&cid=1461755228.1688618393&jid=1306466345&gjid=434993267&_gid=919762931.1688618393&_u=YEBAAUAAAAAAACAAI~&z=17

https://www.googletagmanager.com/a?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&e=gtm.js&eid=1&h=Ag&tr=5rep.5zone&ti=1rep.1zone&z=0
https://www.googletagmanager.com/a?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&es=1&e=gtag.config&eid=2&h=Ag&epr=1UA&z=0
https://www.googletagmanager.com/a?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&es=1&e=gtm.init&eid=0&h=Ag&z=0 https://www.googletagmanager.com/a?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&es=1&e=gtm.init_consent&eid=-1&h=Ag&dl=www.ayabank.com%2Fpersonal- banking%2Froyal-banking&tdp=UA-228606560-1;;0;0;0&z=0
https://www.googletagmanager.com/a?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&es=1&e=gtm.js&eid=1&h=Ag&tr=1rep.1zone&ti=1rep.1zone&z=0
https://www.googletagmanager.com/a?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&es=1&e=gtm.load&eid=4&u=Ag&h=Ag&z=0
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1
https://www.googletagmanager.com/td?id=UA-228606560-1&v=3&t=t&pid=1465219280&cv=1&rv=36s0&tc=2&es=1&e=gtm.init_consent&eid=-1&h=Ag&dl=www.ayabank.com%2Fpersonal-banking%2Froyal-banking&tdp=UA-228606560-1;;0;0;0&z=0
https://card.ayabank.com/
https://simplepay.ayabank.com/
https://corporate.ayaibanking.com/customer/portal
https://ibankapp.ayabank.com/
https://autocalc.ayabank.com/
https://play.google.com/store/apps/details?id=com.ayaplus.subscriber
https://www.ayaibanking.com/ibLogin.aspx

```
https://apps.apple.com/us/app/aya-pay-wallet/id1485836756
https://saltnpixel.com/AYABank/AYABANK_Contact_Us_Hotline.html
https://saltnpixel.com/AYABank/AYABank_Awards.html
https://saltnpixel.com/AYABank/AYABank_Career_Opportunities.html
https://saltnpixel.com/AYABank/AYABank_CorporateMilestone.html
https://saltnpixel.com/AYABank/AYABank_Employee_Development.html
https://saltnpixel.com/AYABank/AYABank_Sustainability.html
https://saltnpixel.com/AYABank/AYABank_UNGC_Commitment.html
https://saltnpixel.com/AYABank/AYABank_WhyUs.html
https://twitter.com/aya_bank
http://localhost/ayab/file/royal-banking/Royal_Banking_E_booklet.pdf
http://bit.ly/ayambankingandriod
http://bit.ly/ayambankingios
http://saltnpixel.com/AYABank/AYABank_CorporateGoal.html
tel:+95%201%202317777
tel:+95%201%20392070
tel:+95%201%20392462
tel:+95%201%20392526
tel:+95%209%20450215345
tel:+95%209%20453448814
tel:+95%209%20453448815
tel:+95%209%20453448817
tel:+95%209%2045448816
tel:+95%209%20458588953
tel:+9512317777
tel:+95925888993
tel:+959258889937
tel:+959258889973
tel:012317777
tel:9512317777
```

INFO *150020 Links Rejected By Crawl Scope or Exclusion List (1)*

INFO 150020 Links Rejected By Crawl Scope or Exclusion List

Finding #	**1034132**(73639730)	**Severity**	Information Gathered - Level 1
Unique #	**4e5da560-33dd-43e5-bcbf-e3634fe3c0bc**		
Group	Scan Diagnostics	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact

Links listed here were neither crawled or tested by the Web application scanning engine.

Solution

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

```
Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)


External links discovered:
https://prepaidcard.ayabank.com/
https://www.google-analytics.com/analytics.js
https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1758528169&t=pageview&_s=1&dl=https%3A%2F%2Fwww.ayabank.com%2Fdigital-services%2Fcard-services%2Fsimple-pay&ul=en-
us&de=UTF-8&dt=Simple%20Pay%20%E2%80%93%20AYA%20Bank&sd=32-
bit&sr=240x320&vp=1024x768&je=1&fl=10.3%20r183&_u=YEBAAUQAAAAAACAAI~&jid=1306466345&gjid=434993267&cid=1461755228.1688618393&tid=UA-228606560-1&_gid=91976293


https://cardpin.ayabank.com/
https://www.google.com/maps/d/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI&ehbc=2E312F
https://www.google.com/maps/d/u/0/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI%22ehbc=2E312F
https://www.google.com/maps/d/u/0/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI&ehbc=2E312F
https://www.linkedin.com/company/ayabank/
https://fonts.gstatic.com/
https://fonts.gstatic.com/s/nunito/v25/XRXI3I6Li01BKofiOc5wtlZ2di8HDLshdTQ3iazbXWjgeg.woff

IP based excluded links:
```

Links blocked by user:
https://www.ayabank.com/file/cib/FAQ-Corporate_Internet_Banking.pdf
https://www.ayabank.com/file/business/borrowing/AYA_SME_FAQ.pdf
https://www.ayabank.com/file/business/borrowing/AYA_Micro_Loan_FAQ.pdf
https://www.ayabank.com/file/personal/borrowing/hire_purchase/home_loan/Home_Loan_English.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2015_2016.pdf
https://www.ayabank.com/report_files/annual_general_meeting_notice/FY2019_2020_AGM_Notice_Myanmar_Version.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2013_2014.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2017_2018.pdf
https://www.ayabank.com/report_files/annual_report/IFRS_Financial_Statement_2021_2022_Summary.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2014_2015.pdf

INFO *150021 Scan Diagnostics* *(1)*

INFO 150021 Scan Diagnostics

Finding #	**1034134**(73639732)	Severity	Information Gathered - Level 1
Unique #	**dd1340be-1e3d-4681-b547-085842408e65**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

```
Loaded 0 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://www.ayabank.com/ fetched. Status code:200, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 1 minute (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 69 requests, 8 seconds. Completed 69 requests of 70 estimated requests (98.5714%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 4 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Collected 499 links overall in 0 hours 15 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 229) + files:(0 x 399) + directories:(9 x 146) + paths:(0 x 545) = total (1314)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 545 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 1305 requests, 25 seconds. Completed 1305 requests of 1314 estimated requests (99.3151%). All tests completed.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 543 inputs)
WS enumeration: 11 vulnsigs tests, completed 1920 requests, 33 seconds. Completed 1920 requests of 5973 estimated requests (32.1447%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (112 tests, 1 inputs)
Batch #1 URI parameter manipulation (no auth): 112 vulnsigs tests, completed 111 requests, 3 seconds. Completed 111 requests of 112 estimated requests (99.1071%). All tests completed.
Batch #1 Form parameter manipulation (no auth): estimated time < 1 minute (112 tests, 11 inputs)
Batch #1 Form parameter manipulation (no auth): 112 vulnsigs tests, completed 999 requests, 439 seconds. Completed 999 requests of 1232 estimated requests (81.0877%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 1 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #1 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 11 inputs)
Batch #1 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 172 requests, 87 seconds. Completed 172 requests of 264 estimated requests (65.1515%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 1 inputs)
```

VULNERABILITY ASSESSMENT REPORT

```
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 14 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests (no auth): estimated time < 1 minute (14 tests, 11 inputs)
Batch #1 Form field time-based tests (no auth): 14 vulnsigs tests, completed 126 requests, 65 seconds. Completed 126 requests of 154 estimated requests (81.8182%). All tests completed.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 1 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 11 inputs)
Batch #1 Form field time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 11 estimated requests (81.8182%). All tests completed.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (112 tests, 1 inputs)
Batch #2 URI parameter manipulation (no auth): 112 vulnsigs tests, completed 111 requests, 4 seconds. Completed 111 requests of 112 estimated requests (99.1071%). All tests completed.
Batch #2 Form parameter manipulation (no auth): estimated time < 10 minutes (112 tests, 10 inputs)
Batch #2 Form parameter manipulation (no auth): 112 vulnsigs tests, completed 1132 requests, 48 seconds. Completed 1132 requests of 1120 estimated requests (101.071%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 1 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #2 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 10 inputs)
Batch #2 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 160 requests, 7 seconds. Completed 160 requests of 240 estimated requests (66.6667%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 1 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 14 estimated requests (100%). All tests completed.
Batch #2 Form field time-based tests (no auth): estimated time < 1 minute (14 tests, 10 inputs)
Batch #2 Form field time-based tests (no auth): 14 vulnsigs tests, completed 140 requests, 6 seconds. Completed 140 requests of 140 estimated requests (100%). All tests completed.
Batch #2 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 1 inputs)
Batch #2 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #2 Form field time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 10 inputs)
Batch #2 Form field time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 10 requests, 0 seconds. Completed 10 requests of 10 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 2 hours (119 tests, 1 inputs)
Batch #4 WebCgiOob: 119 vulnsigs tests, completed 1178 requests, 140 seconds. Completed 1178 requests of 71395 estimated requests (1.64998%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 150 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 1200 requests, 2637 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (38 tests, 0 inputs)
Batch #4 HTTP call manipulation: 38 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 2 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 4 requests, 10 seconds. Completed 4 requests of 4 estimated requests (100%). All tests completed.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 10 minutes (1 tests, 405 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 405 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 30 minutes (47 tests, 3 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 8088 requests, 236 seconds. Completed 8088 requests of 8088 estimated requests (100%). XSS optimization removed 4698 links. All tests completed.
Batch #4 Header manipulation: estimated time < 30 minutes (47 tests, 186 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 11715 requests, 324 seconds. Completed 11715 requests of 24180 estimated requests (48.4491%). XSS optimization removed 5394 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 100 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 100 requests, 3 seconds. Completed 100 requests of 100 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 4 requests, 21 seconds. Completed 4 requests of 4 estimated requests (100%). All tests completed.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 12 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 229) + files:(0 x 399) + directories:(4 x 146) + paths:(11 x 545) = total (6579)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (15 tests, 545 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 5991 requests, 106 seconds. Completed 5991 requests of 6579 estimated requests (91.0625%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 229) + files:(0 x 399) + directories:(1 x 146) + paths:(0 x 545) = total (146)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 545 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 16 requests, 20 seconds. Completed 16 requests of 146 estimated requests (10.9589%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 229) + files:(0 x 399) + directories:(16 x 146) + paths:(0 x 545) = total (2336)
Batch #5 Time based path manipulation: estimated time < 10 minutes (16 tests, 419 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 64 requests, 960 seconds. Completed 64 requests of 2336 estimated requests (2.73973%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 229) + files:(18 x 399) + directories:(143 x 146) + paths:(18 x 545) = total (38786)
Batch #5 Path manipulation: estimated time < 30 minutes (183 tests, 545 inputs)
Batch #5 Path manipulation: 183 vulnsigs tests, completed 22799 requests, 428 seconds. Completed 22799 requests of 38786 estimated requests (58.7815%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 2 hours (319 tests, 1 inputs)
Batch #5 WebCgiGeneric: 319 vulnsigs tests, completed 1182 requests, 81 seconds. Completed 1182 requests of 216910 estimated requests (0.544926%). All tests completed.
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 2 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 5 seconds. Completed 0 requests of 4 estimated requests (0%). All tests completed.
Duration of Crawl Time: 934.00 (seconds)
Duration of Test Phase: 5827.00 (seconds)
Total Scan Time: 6761.00 (seconds)


Total requests made: 61665
Average server response time: 0.10 seconds


Average browser load time: 0.11 seconds
```

INFO *150028 Cookies Collected (1)*

INFO 150028 Cookies Collected

Finding #	**1034138**(73639736)	Severity	Information Gathered - Level 1
Unique #	**7f3f2416-6d9f-4f60-8fb7-3c57b6eb95e7**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were set by the web application during the crawl phase.

Impact

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

```
Total cookies: 4
XSRF-
TOKEN=eyJpdiI6IitUY1UxekpZcDc3K28vY0VhSkYrYUE9PSIsInZhbHVlIjoia0I0Z29HaTVDQmM3Yk11cEFtWms5eWx6VGswTHp1MmlOSFpMbmJjbkhORE45a0ZiekpTNWo4Z1l1d243ckhlU0J
expires=Thu, 06-Jul-2023 06:36:16 GMT; SameSite=lax; path=/ First set at URL: https://www.ayabank.com/


aya_bank_session=eyJpdiI6IjNJSmJldmpNdmlNbnBHa0JFaUZQQWc9PSIsInZhbHVlIjoiUE9sT0hldWVJZGhMVnhkbk8zRUVEQithUHNYTWxOdCtBRFF3OWc0V0pJQlByTlV2ZTd6SzdXVEhCeF
HttpOnly; expires=Thu, 06-Jul-2023 06:36:16 GMT; SameSite=lax; path=/ First set at URL: https://www.ayabank.com/
NID=511=vKrwzgR4lkKta8p0VUOnRM6HEg2rIrTWhzm0f3n1zA8HMmSPjPRCRcrEKWUTmm-Yd-1FZR7RX2lxIAz_YAiwH4hdn30-
qhAe7xec7FrK0Q_6MBMKnaexAv04_DiLQ9wNsSg35DUQJyuYpHYw7hhFrsBmNSHDwJufH0-s419_z3M; secure; HttpOnly; expires=Fri, 05-Jan-2024 04:38:50 GMT; domain=.google.com; path=/
First set at URL: https://www.google.com/maps/d/u/0/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI&ehbc=2E312F
_gat_gtag_UA_228606560_1=1; expires=Thu, 06-Jul-2023 04:40:52 GMT; domain=ayabank.com; path=/ First set at URL: https://www.ayabank.com/digital-services/card-services/simple-pay
```

INFO *150041 Links Rejected* *(1)*

INFO 150041 Links Rejected

Finding #	**1034144**(73639742)	**Severity**	Information Gathered - Level 1
Unique #	**6b43daa1-28f5-4880-b441-f79468d802cc**		
Group	Scan Diagnostics	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This has an informative nature. The links listed below were not crawled by the Web application scanning engine because they were intentionally prohibited by a blacklist or whitelist configuration setting. The list is provided to verify that links have been correctly blocked by blacklist and whitelist filters.

Impact

Links listed here were neither crawled or tested by the Web application scanning engine, and that should be in sync with the intended behavior.

Solution

No action is required.

Results

```
https://www.ayabank.com/file/cib/FAQ-Corporate_Internet_Banking.pdf
https://www.ayabank.com/file/business/borrowing/AYA_SME_FAQ.pdf
https://www.ayabank.com/file/business/borrowing/AYA_Micro_Loan_FAQ.pdf
https://www.ayabank.com/file/personal/borrowing/hire_purchase/home_loan/Home_Loan_English.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2015_2016.pdf
https://www.ayabank.com/report_files/annual_general_meeting_notice/FY2019_2020_AGM_Notice_Myanmar_Version.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2013_2014.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2017_2018.pdf
https://www.ayabank.com/report_files/annual_report/IFRS_Financial_Statement_2021_2022_Summary.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2014_2015.pdf
https://www.ayabank.com/report_files/annual_general_meeting_notice/FY2018_2019_AGM_Notice_English_Version.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2021_2022.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2019_2020.pdf
https://www.ayabank.com/report_files/annual_general_meeting_notice/FY2019_2020_AGM_Notice_English_Version.pdf
https://www.ayabank.com/report_files/annual_report/IFRS_Financial_Statement_Sept_30_2020_Summary.pdf
https://www.ayabank.com/report_files/annual_general_meeting_minutes/FY2018_2019_AGM_minutes_English_Version.pdf
https://www.ayabank.com/report_files/annual_general_meeting_notice/FY2018_2019_AGM_Notice_Myanmar_Version.pdf
https://www.ayabank.com/report_files/annual_general_meeting_minutes/FY2019_2020_AGM_minutes_English_Version.pdf
https://www.ayabank.com/report_files/annual_general_meeting_minutes/FY2019_2020_AGM_minutes_Myanmar_Version.pdf
https://www.ayabank.com/report_files/annual_general_meeting_minutes/FY2018_2019_AGM_minutes_Myanmar_Version.pdf
https://www.ayabank.com/report_files/annual_report/annual_report_FY_2016_2017.pdf
https://www.ayabank.com/file/iBanking/iBanking_User_Guide.pdf
https://www.ayabank.com/file/personal/borrowing/hire_purchase/edu_loan/Education_Loan_English.pdf
```

```
https://www.ayabank.com/file/personal/borrowing/hire_purchase/edu_loan/Partner%20Institutions.pdf
https://www.ayabank.com/file/personal/borrowing/hire_purchase/edu_loan/Partner%2520Institutions.pdf
https://www.ayabank.com/file/personal/borrowing/hire_purchase/auto_loan/Auto_Loan_English.pdf
https://www.ayabank.com/file/mBanking/mBanking_User_Guide.pdf
https://www.ayabank.com/file/business/remittance/Foreign%20Currency%20Funds%20Transfer%20Application%20Form.pdf
https://www.ayabank.com/file/business/remittance/Foreign%2520Currency%2520Funds%2520Transfer%2520Application%2520Form.pdf
https://www.ayabank.com/file/cardservices/AYA%20CREDIT%20CARD%20AGREEMENT%20(English%20Version%202.0).docx
https://www.ayabank.com/file/cardservices/Membership%20Guide.docx
https://www.ayabank.com/file/cardservices/AYA%2520CREDIT%2520CARD%2520AGREEMENT%2520(English%2520Version%25202.0).docx
https://www.ayabank.com/file/cardservices/Membership%2520Guide.docx
https://www.ayabank.com/blog_images/file/Online_Trading_by_AYA_Bank_PCL_5July23.pdf
```

INFO *150054 Email Addresses Collected (1)*

INFO 150054 Email Addresses Collected

Finding #	**1034147**(73639745)	Severity	Information Gathered - Level 1
Unique #	**980a0d8b-b5de-492c-87ee-5dba70267282**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-359		
OWASP	-		
WASC	-		

Details

Threat

The email addresses listed in the Results section were collected from the returned HTML content during the crawl phase.

Impact

Email addresses may help a malicious user with brute force and phishing attacks.

Solution

Review the email list to see if they are all email addresses you want to expose.

Results

```
Number of emails: 7
ibdteam@ayabank.com first seen at https://www.ayabank.com/business/remittance-payments/international-payments
info@ayabank.com first seen at https://www.ayabank.com/
mchecommerce@ayabank.com first seen at https://www.ayabank.com/digital-services/card-services/merchant-services/ecommerce
mchpayment@ayabank.com first seen at https://www.ayabank.com/digital-services/card-services/merchant-services/ecommerce
mchsupport.card@ayabank.com first seen at https://www.ayabank.com/digital-services/card-services/merchant-services/pos
support.card@ayabank.com first seen at https://www.ayabank.com/digital-services/card-services/prepaid-card
you@emailaddress.com first seen at https://www.ayabank.com/personal-banking/royal-banking
```

INFO *150082 Protection against Clickjacking* *(1)*

INFO 150082 Protection against Clickjacking

Finding #	**1034129**(73639727)	Severity	Information Gathered - Level 1
Unique #	**8b44e062-8be6-4bee-a38d-243ff60fcdfd**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The URLs listed have protection against Clickjacking. The protection is implemented via the X-Frame-Options response header.

Impact

X-Frame-Options header is used to prevent framing of the page.

Solution

N/A

Results

https://www.ayabank.com/
https://www.ayabank.com/about-aya/governance/corporate-governance
https://www.ayabank.com/business/account-saving/call-deposit
https://www.ayabank.com/business/insurance/oversea-marine-cargo
https://www.ayabank.com/business/remittance-payments/local-payments https://www.ayabank.com/personal-banking/account-saving/saving-deposit https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving https://www.ayabank.com/personal-banking/insurance/life/universal
https://www.ayabank.com/personal-banking/insurance/travel/aya-go https://www.ayabank.com/privacy-notice-cookie-policy

INFO *150104 Form Contains Email Address Field* *(1)*

INFO 150104 Form Contains Email Address Field

Finding #	**1034143**(73639741)	Severity	Information Gathered - Level 1
Unique #	**03b220e0-7646-4e63-b43a-0b737414fae9**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The HTML form contains a field that collects an email address.

Impact

In some web apps, forms that collect email addresses also generate messages to back-end systems whenever the form is submitted. If no rate limiting or CAPTCHA is applied to form submissions, then vulnerability tests against this form may produce a significant number of messages. If too many messages are generated, then it may produce a Denial-of-Service situation.

Solution

Review the form to determine if it produces an email message each time it is submitted. If so, consider excluding this form from being tested or disable the messaging during the web application scan. Forms that generate messages can be abused by malicious users to create Denial of Service attacks. Apply rate limiting to the form in order to throttle the number of times it may be submitted by a user or by an IP address; or apply a CAPTCHA to it to reduce the chance of automated tools being used against the form.

Results

https://www.ayabank.com/personal-banking/royal-banking
https://www.ayabank.com/about-aya/news-room/reports
https://www.ayabank.com/enquiry

INFO *150148 AJAX Links Crawled* *(1)*

INFO 150148 AJAX Links Crawled

Finding #	**1034133**(73639731)	Severity	Information Gathered - Level 1
Unique #	**1f2aadd8-945a-424d-8114-ad9a9850659a**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique AJAX links crawled by the scanner appears in the Results section. The link may be either a URL with fragment (#) or a Selenium script. To open a URL with fragment, open it in browser. To open a Selenium script, use Qualys Browser Recorder Chrome extension. The number of AJAX links reported is limited to 1000.

Impact

N/A

Solution

N/A

Results

Number of ajax links: 1
https://www.ayabank.com/#success

Smart Scan Optimizations - All Optimizations disabled.

INFO *150152 Forms Crawled (1)*

INFO 150152 Forms Crawled

Finding #	**1034136**(73639734)	Severity	Information Gathered - Level 1
Unique #	**a5c53eba-4a3e-41f6-825d-f6fcd2be2409**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact

N/A

Solution

N/A

Results

```
Total internal forms seen (this count includes duplicate forms): 146

Crawled forms (Total: 4)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115
Form #:1 Action URI:https://www.ayabank.com/ (found at: https://www.ayabank.com/)
Form Fields: s

Form #:2 Action URI:https://www.ayabank.com/personal-banking/royal-banking (found at: https://www.ayabank.com/personal-banking/royal-banking)
Form Fields: _token, report_file, subscribe_flag, report_down_email
```

Form #:3 Action URI:https://www.ayabank.com/report_download (found at: https://www.ayabank.com/about-aya/news-room/reports)
Form Fields: _token, report_down_email, report_file, subscribe_flag

Form #:4 Action URI:https://www.ayabank.com/enquiry_form_submit (found at: https://www.ayabank.com/enquiry)
Form Fields: _token, name_txt, phone_txt, email_txt, division_select, company_txt, comment_question_txt, product_check, sub_prod_check[], tnc_check

NOTE: Forms with exactly the same form fields were considered identical even if they had different action URI. Only one such form is crawled, the other forms with exactly the same form fields are considered duplicate and are not crawled. If they are different forms and each of them should be crawled then change the scan settings accordingly.

The following forms were not crawled as their fields matched Form #1 above:
Form Action URI: https://www.ayabank.com/privacy-notice-cookie-policy
Form Action URI: https://www.ayabank.com/business/account-saving/call-deposit
Form Action URI: https://www.ayabank.com/business/remittance-payments/local-payments
Form Action URI: https://www.ayabank.com/about-aya/governance/corporate-governance
Form Action URI: https://www.ayabank.com/personal-banking/insurance/life/universal
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving
Form Action URI: https://www.ayabank.com/business/insurance/oversea-marine-cargo
Form Action URI: https://www.ayabank.com/personal-banking/insurance/travel/aya-go
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/saving-deposit
Form Action URI: https://www.ayabank.com/business/insurance/industrial-all-risk
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/call-deposit
Form Action URI: https://www.ayabank.com/personal-banking/remittance/international
Form Action URI: https://www.ayabank.com/business/borrowing/corporate-business-loan
Form Action URI: https://www.ayabank.com/business/trade/trade-financing
Form Action URI: https://www.ayabank.com/personal-banking/insurance/life
Form Action URI: https://www.ayabank.com/digital-services/online-payment-services/corporate-internet-banking
Form Action URI: https://www.ayabank.com/digital-services/wallet-solution/aya-pay
Form Action URI: https://www.ayabank.com/business/borrowing/sme
Form Action URI: https://www.ayabank.com/personal-banking/insurance/life/one-health-solution-individual-plan

```
Form Action URI: https://www.ayabank.com/business/cash-management
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/fixed-deposit
Form Action URI: https://www.ayabank.com/digital-services/guideline/digital-secure
Form Action URI: https://www.ayabank.com/digital-services/guideline/frequently-used-digital
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/our-strategies/corporate-strategy
Form Action URI: https://www.ayabank.com/business/borrowing/hire-purchase
Form Action URI: https://www.ayabank.com/personal-banking/borrowing/hire-purchase/c2c-auto-loan
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-su-buu
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/corporate-profile/mission-corporate-value-brand-promise
Form Action URI: https://www.ayabank.com/personal-banking/borrowing/hire-purchase/home-loan
Form Action URI: https://www.ayabank.com/personal-banking/remittance/local
Form Action URI: https://www.ayabank.com/personal-banking/borrowing/hire-purchase/construction-loan
Form Action URI: https://www.ayabank.com/personal-banking/royal-banking
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/our-strategies/stakeholder-management
Form Action URI: https://www.ayabank.com/about-aya/news-room/reports
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/current-deposit/new-business-current-account
Form Action URI: https://www.ayabank.com/digital-services/atm
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-maximizer-saving
Form Action URI: https://www.ayabank.com/digital-services/online-payment-services/internet-banking
Form Action URI: https://www.ayabank.com/personal-banking/insurance/life/short-term
Form Action URI: https://www.ayabank.com/business/trade/trade-services
Form Action URI: https://www.ayabank.com/personal-banking/insurance/health
Form Action URI: https://www.ayabank.com/business/account-saving/fixed-deposit
Form Action URI: https://www.ayabank.com/digital-services/card-services/debit-card
Form Action URI: https://www.ayabank.com/personal-banking/other-services/safe-deposit
Form Action URI: https://www.ayabank.com/personal-banking/other-services
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/leadership/meet-our-leaders
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/current-deposit/regular-current-account
Form Action URI: https://www.ayabank.com/personal-banking/borrowing/hire-purchase/education-loan
Form Action URI: https://www.ayabank.com/personal-banking/borrowing/hire-purchase/auto-loan
Form Action URI: https://www.ayabank.com/business/insurance/group-life
Form Action URI: https://www.ayabank.com/digital-services/online-payment-services/mobile-banking
Form Action URI: https://www.ayabank.com/business/remittance-payments/international-payments
Form Action URI: https://www.ayabank.com/business/insurance/domestic-marine-cargo
Form Action URI: https://www.ayabank.com/personal-banking/insurance
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Green_Energy_Exhibition_Banking_Partner
Form Action URI: https://www.ayabank.com/about-aya/message-from-chairman
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/corporate-profile/ayabank-profile
Form Action URI: https://www.ayabank.com/personal-banking/insurance/life/education
Form Action URI: https://www.ayabank.com/personal-banking/remittance/payment
Form Action URI: https://www.ayabank.com/digital-services/card-services/simple-pay
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/call-deposit/new-business-call
Form Action URI: https://www.ayabank.com/digital-services/online-payment-services
Form Action URI: https://www.ayabank.com/personal-banking/insurance/travel/aya-joy
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/current-deposit/retail-fca-current
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/current-deposit/seafarer-acount
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/call-deposit/premium-call-deposit
Form Action URI: https://www.ayabank.com/business/insurance/domestic-inland-transit
Form Action URI: https://www.ayabank.com/about-aya/governance/compliance
Form Action URI: https://www.ayabank.com/personal-banking/insurance/motor
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-loyal-saving
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/current-deposit
Form Action URI: https://www.ayabank.com/personal-banking/insurance/personal-accident
Form Action URI: https://www.ayabank.com/personal-banking/insurance/fire
Form Action URI: https://www.ayabank.com/personal-banking/account-saving/saving-deposit/ngwe-toe-mae-shwe-o
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news
Form Action URI: https://www.ayabank.com/personal-banking/other-services/foreign-currency-exchange-service
Form Action URI: https://www.ayabank.com/digital-services/card-services/prepaid-card
Form Action URI: https://www.ayabank.com/business/insurance/car-ear
Form Action URI: https://www.ayabank.com/digital-services/card-services/credit-card
Form Action URI: https://www.ayabank.com/business/account-saving/saving-deposit
Form Action URI: https://www.ayabank.com/business/account-saving/current-deposit
Form Action URI: https://www.ayabank.com/digital-services/card-services/merchant-services/ecommerce
Form Action URI: https://www.ayabank.com/digital-services/card-services/merchant-services/pos
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Workshop_for_Certified_Branch_Managers_Program
Form Action URI: https://www.ayabank.com/about-aya/governance/compliance/aml-cft
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Bank_PCL_Foreign_Currency_Online_Trading
Form Action URI: https://www.ayabank.com/about-aya/governance/risk-management
Form Action URI: https://www.ayabank.com/business-banking
Form Action URI: https://www.ayabank.com/business-banking/account-saving
Form Action URI: https://www.ayabank.com/business-banking/remittance
Form Action URI: https://www.ayabank.com/about-aya/governance
Form Action URI: https://www.ayabank.com/about-aya
Form Action URI: https://www.ayabank.com/personal-banking
Form Action URI: https://www.ayabank.com/personal-banking/account-saving
Form Action URI: https://www.ayabank.com/business-banking/insurance
Form Action URI: https://www.ayabank.com/personal-banking/insurance/travel
Form Action URI: https://www.ayabank.com/personal-banking/remittance
Form Action URI: https://www.ayabank.com/business-banking/borrowing
Form Action URI: https://www.ayabank.com/enquiry
Form Action URI: https://www.ayabank.com/business-banking/trade
Form Action URI: https://www.ayabank.com/digital-services
Form Action URI: https://www.ayabank.com/digital-services/wallet-solution
```

Form Action URI: https://www.ayabank.com/digital-services/guideline
Form Action URI: https://www.ayabank.com/digital-services/guideline/digital-secure/sms-alert

```
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/our-strategies
Form Action URI: https://www.ayabank.com/about-aya/who-we-are
Form Action URI: https://www.ayabank.com/personal-banking/borrowing/hire-purchase
Form Action URI: https://www.ayabank.com/personal-banking/borrowing
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/corporate-profile
Form Action URI: https://www.ayabank.com/about-aya/news-room
Form Action URI: https://www.ayabank.com/digital-services/card-services
Form Action URI: https://www.ayabank.com/digital-services/card-services/reset-pin
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/leadership
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/leadership/meet-our-leaders/contact-to-board
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/year/2023
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Bank_Offering_Apprenticeship_Opportunity
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/year/2019
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/year/2020
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/corporate-profile/ayabank-profile/business-practices
Form Action URI: https://www.ayabank.com/about-aya/who-we-are/corporate-profile/ayabank-profile/shareholding-information
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Top_Income_Tax_Payer
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Completion_of_Basic_Banking_Operations_Training_No8
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/2020_Best_Bank_for_SMEs_Award    from_AsiaMoney
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/MOU_between_Mandalay_Smart_Pay_and_AYA_Bank
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Pioneering_Green_Financing_for_Electric_Vehicles
Form Action URI: https://www.ayabank.com/digital-services/card-services/merchant-services
Form Action URI: https://www.ayabank.com/about-aya/governance/risk-management/managing-risk
Form Action URI: https://www.ayabank.com/about-aya/governance/risk-management/risk-management-framework
Form Action URI: https://www.ayabank.com/about-aya/governance/risk-management/risk-management-control
Form Action URI: https://www.ayabank.com/about-aya/governance/risk-management/risk-governance
Form Action URI: https://www.ayabank.com/#success
Form Action URI: https://www.ayabank.com/digital-services/card-services/card-privilege
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%E2%80%99s_10th_Homage_Ceremony
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Achievement_of_Silver_Award_for_Myanmar_Employer_Awards_2019
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Memorandum_of_Understanding_Signing_Ceremony_between_AYA_Bank_and_Smart_Myanmar
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Publication_of_Report_on_Myanmar%E2%80%99s_Business_Transparency_2019_Pwint_Thit_Sa
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_Financial_Group%E2%80%99s_Family_Celebrating_10th_Kathina_Civara_Dana_Ceremony
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/First_Bank_in_Myanmar_for_achieving_EDGE_Certificate_for_Gender_Equality
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/
Asia_Money_2019_Awards_Best_Bank_for_SMEs_&_Best_Bank_for_CSR    Asia_Money_2019_Best_Bank_for_SMEs
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/Siam_Commercial_Bank_PCL_and_AYA_Sign_MOU
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/The_opening_of_the_261_branch_of_AYA_Bank
Form Action URI: https://www.ayabank.com/about-aya/news-room/corporate-news/AYA_SOMPO_General_Insurance_Awareness_and_Sale_Marketing_Training
```

INFO *150176 In-scope JavaScript Libraries Detected (1)*

INFO 150176 In-scope JavaScript Libraries Detected

Finding #	1034146(73639744)	Severity	Information Gathered - Level 1
Unique #	f74c0a9e-afda-44b3-9dc1-6f3c75d21631		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-200		
OWASP	-		
WASC	-		

Details

Threat

WAS will report "in-scope" JavaScript libraries discovered by the scanner during crawling and are provided in the Results section. In-scope means, links that are considered to be "in-scope" per the configuration set up for the Web Application. The discovered libraries are reported only once, based on the page on which they were first detected.

Each library is reported along with other information such as the URL of page on which it was first found, the version, and the URL of the .js file.

Impact

When including third-party JavaScript libraries, the application must effectively trust those libraries added. Without sufficient protection mechanisms, the functionality may be malicious in nature (i.e. either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source).

Solution

Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered. Ensure libraries and dependencies, are consuming trusted repositories. If you have a higher risk profile, consider hosting an internal known-good repository that's vetted.

Results

```
Number of unique JS libraries: 3
Javascript library : Bootstrap
Version : 5.1.3
Script uri : https://www.ayabank.com/js/bootstrap.js
Found on the following page(only first page is reported):
https://www.ayabank.com/


================================================================


Javascript library : jQuery
Version : 3.5.1
Script uri : https://www.ayabank.com/js/jquery.js
Found on the following page(only first page is reported):
 https://www.ayabank.com/

==============================================================

Javascript library : moment
Version : 2.29.1
Script uri : https://www.ayabank.com/js/moment.min.js
Found on the following page(only first page is reported):
https://www.ayabank.com/

==============================================================
```

INFO *150247 Web Server and Technologies Detected (1)*

INFO 150247 Web Server and Technologies Detected

Finding #	**1034148**(73639746)	Severity	Information Gathered - Level 1
Unique #	**b4e8a108-2b64-4470-8261-6b59641c2f2b**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-200		
OWASP	-		
WASC	-		

Details

Threat

Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

Impact

An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

Solution

Ensure that your web servers do not reveal any sensitive information about your technology stack and system details.

Please review the issues reported below:

Results

```
Number of technologies detected: 2
Technology name: Apache
Matched Components:
header match:
 Server:Apache
Matched links: reporting only first 3 links
https://www.ayabank.com/
https://www.ayabank.com/?s=discovery
https://www.ayabank.com/privacy-notice-cookie-policy


Technology name: Bootstrap
```

```
Matched Components:
script tag match:
 <script rel="modulepreload" src="https://www.ayabank.com/js/bootstrap.js" as="script"></script>
 <script src="https://www.ayabank.com/js/bootstrap.js"></script>
Matched links: reporting only first 3 links
https://www.ayabank.com/
https://www.ayabank.com/?s=discovery
https://www.ayabank.com/privacy-notice-cookie-policy
```

INFO *150528 Server Returns HTTP 4XX Error Code During Scanning (1)*

INFO 150528 Server Returns HTTP 4XX Error Code During Scanning

Finding #	1034130(73639728)	Severity	Information Gathered - Level 1
Unique #	3bdb77c5-2e5b-40b7-9130-0118598dc034		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad
Request 401 -
Unauthorized

403
Forbidden
404 - Not
Found

405 - Method Not
Allowed

407 - Proxy Authentication
Required 408 - Request
Timeout

413 - Payload Too
Large 414 - URI Too
Long

Impact

The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

Results

```
Number of links with 4xx response code: 37
(Only first 50 such links are listed)

404 https://www.ayabank.com/about-aya/who-we-
404 https://www.ayabank.com/about-aya/who-we-/leadership
404 https://www.ayabank.com/account-saving
404 https://www.ayabank.com/account-saving/current-deposit
404 https://www.ayabank.com/business
404 https://www.ayabank.com/business/account-saving
404 https://www.ayabank.com/business/borrowing
404 https://www.ayabank.com/business/insurance
404 https://www.ayabank.com/business/remittance-payments
404 https://www.ayabank.com/business/remittance-payments/images
404 https://www.ayabank.com/business/remittance-payments/images/get_start_bg.jpg
404 https://www.ayabank.com/business/trade
404 https://www.ayabank.com/digital-services/card-services/images
404 https://www.ayabank.com/digital-services/card-services/images/JBC_UPI_card.png
404 https://www.ayabank.com/digital-services/card-services/images/MPU_JCB_card.png
404 https://www.ayabank.com/digital-services/card-services/images/prepaid
404 https://www.ayabank.com/digital-services/card-services/images/prepaid/card_block_termination.png
404 https://www.ayabank.com/digital-services/card-services/images/prepaid/statement_inquiry.png
404 https://www.ayabank.com/digital-services/card-services/images/simplepay
404 https://www.ayabank.com/digital-services/card-services/images/simplepay/how_to_apply_bg.jpg
404 https://www.ayabank.com/digital-services/card-services/merchant-services/images
404 https://www.ayabank.com/digital-services/card-services/merchant-services/images/MPU_ecommerce_registration.jpg
404 https://www.ayabank.com/digital-services/card-services/merchant-services/images/how_to_apply_bg.jpg
404 https://www.ayabank.com/digital-services/card-services/merchant-services/images/how_to_apply_mobile_bg.jpg
404 https://www.ayabank.com/digital-services/guideline/digital-secure/images
404 https://www.ayabank.com/digital-services/guideline/digital-secure/images/MPU_ecommerce_registration.jpg
404 https://www.ayabank.com/digital-services/guideline/digital-secure/images/how_to_apply_bg.jpg
404 https://www.ayabank.com/digital-services/guideline/digital-secure/images/how_to_apply_mobile_bg.jpg
404 https://www.ayabank.com/digital-services/online-payment-services/images
```

```
404 https://www.ayabank.com/digital-services/online-payment-services/images/get_start_bg.jpg
405 https://www.ayabank.com/enquiry_form_submit
404 https://www.ayabank.com/personal-banking/other-services/images
404 https://www.ayabank.com/personal-banking/other-services/images/MPU_ecommerce_registration.jpg
404 https://www.ayabank.com/personal-banking/other-services/images/how_to_apply_bg.jpg
404 https://www.ayabank.com/personal-banking/other-services/images/how_to_apply_mobile_bg.jpg
405 https://www.ayabank.com/report_download
404 https://www.ayabank.com/sms-alert
```

INFO *150546 First Link Crawled Response Code Information (1)*

INFO 150546 First Link Crawled Response Code Information

Finding #	**1034139**(73639737)	Severity	Information Gathered - Level 1
Unique #	**13a1d873-cb3e-4a4c-811a-cde5fcfd560b**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 *(if present) for additional details.*

Results

```
Base URI: https://www.ayabank.com/
Response Code: 200
Response Header:
 Date: Thu, 06 Jul 2023 04:36:19 GMT
 Server: Apache
 Cache-Control: no-cache, private Content-
 Encoding: gzip
 Vary: Accept-Encoding,User-Agent Set-
 Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; Max-Age=7200; path=/; samesite=lax
 Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/
 Set-Cookie:
aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
HttpOnly; expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/


aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
expires=Thu, 06-Jul-2023 06: 36:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
 X-Content-Type-Options: nosniff
 Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
 Policy: strict-origin-when-cross-origin
```

```
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block Access-
Control-Allow-Origin: *
Access-Control-Allow-Methods: GET Keep-
Alive: timeout=20, max=86 Connection:
Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


Response Body:
<!DOCTYPE html><html lang="en"><head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="icon" href="https://www.ayabank.com/images/ayaicon.png" sizes="192x192">
<link rel="apple-touch-icon" href="https://www.ayabank.com/images/ayaicon.png" sizes="180x180">
<meta name="msapplication-TileImage" content="https://www.ayabank.com/images/ayaicon.png">
<meta name="description" content="AYA Bank is a leading p
...
```

INFO *150621 List of JavaScript Links* *(1)*

INFO 150621 List of JavaScript Links

Finding #	**1034145**(73639743)	Severity	Information Gathered - Level 1
Unique #	**1baa4df1-7fe8-462c-be7d-990ba6d2f6a3**		
Group	Scan Diagnostics	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This QID reports all the JavaScript links that are in-scope of this scan.

Impact

JavaScript links may pose security risks such as XSS, CSRF.

Solution

Verify JavaScript links are intentional and required for your web application.

Review any third-party scripts that are hosted on your local server instead of using CDN. Update all the JavaScript libraries with latest version as applicable.

Results

```
JavaScript Links were found while crawling.
Total Number of Links: 12
https://www.ayabank.com/js/popper.js
https://www.ayabank.com/js/helpers.js
https://www.ayabank.com/js/jquery.js
https://www.ayabank.com/js/menu.js
https://www.ayabank.com/js/moment.min.js
https://www.ayabank.com/js/bootstrap.js
https://www.ayabank.com/js/util.js
https://www.ayabank.com/js/main.js
https://www.ayabank.com/js/moment.js
https://www.ayabank.com/js/swiper-bundle.min.js
https://www.ayabank.com/js/bootstrap.min.js
https://www.ayabank.com/js/frequently_used.js
```

Security Weaknesses *(10)*

INFO **150089 Links to non-routable resources discovered in externally facing content** **(1)**

INFO 150089 Links to non-routable resources discovered in externally facing conten t

Finding #	**1034137**(73639735)	Severity	Information Gathered - Level 3
Unique #	**2b72bb3a-1d6e-447c-9c3f-5dafc29e6083**		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Links pointing to non-routable IPs (see RFC 1918 - Address Allocation for Private Internets) were discovered on the externally facing content. These links were present on the target Web application but were not crawled.

Impact

Such links could be either result of bad link resolution during porting QA web application to production, or due to injected malicious content to access for example customer's network equipment.

Solution

Review the links and ensure only valid links are served by the web application.

Results

total links pointing to internal resources: 1
http://localhost/ayab/file/royal-banking/Royal_Banking_E_booklet.pdf discovered on external page: https://www.ayabank.com/personal-banking/royal-banking

INFO *150261 Subresource Integrity (SRI) Not Implemented* *(1)*

INFO 150261 Subresource Integrity (SRI) Not Implemented

Finding #	1034155(73639753)	Severity	Information Gathered - Level 3
Unique #	35842961-6a4d-440d-8cb0-68106318f430		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-693		
OWASP	-		
WASC	-		

Details

Threat

The integrity attribute is missing in script and/or link elements. Subresource Integrity (SRI) is a standard browser security feature that verifies the value of the integrity attribute in

Impact

Absence of SRI checks mean it is impossible to verify that the third-party resources are delivered without any unexpected manipulation.

Solution

All script and link elements that load external content should include the integrity attribute to ensure that the content is trustworthy.

More information:

[Subresource Integrity article by Mozilla]

[OWASP Third-Party JavaScript Management Cheat Sheet]

Results

Externally loaded Javascript and CSS resources without integrity checks:

```
Parent link : https://www.ayabank.com/
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
 https://www.google-analytics.com/analytics.js
 https://www.googletagmanager.com/gtag/js?id=UA-228606560-1


Parent link : https://www.ayabank.com/?s=discovery
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
 https://www.google-analytics.com/analytics.js
 https://www.googletagmanager.com/gtag/js?id=UA-228606560-1


Parent link : https://www.ayabank.com/privacy-notice-cookie-policy
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
 https://www.google-analytics.com/analytics.js
 https://www.googletagmanager.com/gtag/js?id=UA-228606560-1


Parent link : https://www.ayabank.com/business/account-saving/call-deposit
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
 https://www.google-analytics.com/analytics.js
 https://www.googletagmanager.com/gtag/js?id=UA-228606560-1


Parent link : https://www.ayabank.com/business/remittance-payments/local-payments
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
 https://www.google-analytics.com/analytics.js
 https://www.googletagmanager.com/gtag/js?id=UA-228606560-1


Parent link : https://www.ayabank.com/about-aya/governance/corporate-governance
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
 https://www.google-analytics.com/analytics.js
 https://www.googletagmanager.com/gtag/js?id=UA-228606560-1


Parent link : https://www.ayabank.com/personal-banking/insurance/life/universal
Found following resource links without integrity checks (only first 10 links are reported)
 https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
```

https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/business/insurance/oversea-marine-cargo
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/personal-banking/insurance/travel/aya-go
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/personal-banking/account-saving/saving-deposit
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/business/insurance/industrial-all-risk
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/personal-banking/account-saving/call-deposit
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/personal-banking/remittance/international
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/business/borrowing/corporate-business-loan
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/business/trade/trade-financing
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/personal-banking/insurance/life
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/digital-services/online-payment-services/corporate-internet-banking
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/digital-services/wallet-solution/aya-pay
Found following resource links without integrity checks (only first 10 links are reported)

https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1

Parent link : https://www.ayabank.com/business/borrowing/sme
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Sora:wght@100;200;300;400;500;600;700;800&display=swap
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=UA-228606560-1
Please check there may be more pages with subresource links without integrity checks.

INFO *150206 Content-Security-Policy Not Implemented (1)*

INFO 150206 Content-Security-Policy Not Implemented

Finding #	**1034159**(73639757)	Severity	Information Gathered - Level 2
Unique #	**06de6ddb-7d58-419f-8c56-054ad9aff3a6**		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:

- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

```
Content-Security-Policy: Header missing
Response headers on link: GET https://www.ayabank.com/ response code: 200
Date: Thu, 06 Jul 2023 04:36:19 GMT
Server: Apache
Cache-Control: no-cache, private Content-
Encoding: gzip
Vary: Accept-Encoding,User-Agent Set-
Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/
Set-Cookie:
aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
HttpOnly; expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/


aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
expires=Thu, 06-Jul-2023 06: 36:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block
```

```
Access-Control-Allow-Origin: * Access-
Control-Allow-Methods: GET Keep-Alive:
timeout=20, max=86 Connection: Keep-
Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Header missing on the following link(s):
(Only first 50 such pages are listed)

```
GET https://www.ayabank.com/ response code: 200
GET https://www.ayabank.com/?s=discovery response code: 200
GET https://www.ayabank.com/privacy-notice-cookie-policy response code: 200
GET https://www.ayabank.com/business/account-saving/call-deposit response code: 200
GET https://www.ayabank.com/public/blog_images/Green-Energy-Exhibition-Banking-Partner.webp response code: 200
GET https://www.ayabank.com/business/remittance-payments/local-payments response code: 200
GET https://www.ayabank.com/about-aya/governance/corporate-governance response code: 200
GET https://www.ayabank.com/public/blog_images/Workshop-for-Certified-Branch-Managers-Program.webp response code: 200
GET https://www.ayabank.com/css/core.min.css response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life/universal response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving response code: 200
GET https://www.ayabank.com/business/insurance/oversea-marine-cargo response code: 200
GET https://www.ayabank.com/personal-banking/insurance/travel/aya-go response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit response code: 200
GET https://www.ayabank.com/business/insurance/industrial-all-risk response code: 200
GET https://www.ayabank.com/images/ayaicon.png response code: 200
GET https://www.ayabank.com/css/header.css response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/call-deposit response code: 200
GET https://www.ayabank.com/personal-banking/remittance/international response code: 200
GET https://www.ayabank.com/js/popper.js response code: 200
GET https://www.ayabank.com/business/borrowing/corporate-business-loan response code: 200
GET https://www.ayabank.com/business/trade/trade-financing response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life response code: 200
GET https://www.ayabank.com/digital-services/online-payment-services/corporate-internet-banking response code: 200
GET https://www.ayabank.com/sms-alert response code: 404
GET https://www.ayabank.com/digital-services/wallet-solution/aya-pay response code: 200
GET https://www.ayabank.com/business/borrowing/sme response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life/one-health-solution-individual-plan response code: 200
GET https://www.ayabank.com/business/cash-management response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/fixed-deposit response code: 200
GET https://www.ayabank.com/digital-services/guideline/digital-secure response code: 200
GET https://www.ayabank.com/digital-services/guideline/frequently-used-digital response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/our-strategies/corporate-strategy response code: 200
GET https://www.ayabank.com/business/borrowing/hire-purchase response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/c2c-auto-loan response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-su-buu response code: 200
GET https://www.ayabank.com/js/helpers.js response code: 200
GET https://www.ayabank.com/js/jquery.js response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/corporate-profile/mission-corporate-value-brand-promise response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/home-loan response code: 200
GET https://www.ayabank.com/personal-banking/remittance/local response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/construction-loan response code: 200
GET https://www.ayabank.com/personal-banking/royal-banking response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/our-strategies/stakeholder-management response code: 200
GET https://www.ayabank.com/about-aya/news-room/reports response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/current-deposit/new-business-current-account response code: 200
GET https://www.ayabank.com/digital-services/atm response code: 200
POST https://www.ayabank.com/report_download response code: 500
GET https://www.ayabank.com/css/landing_new.css response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-maximizer-saving response code: 200
```

INFO *150248 Missing header: Permissions-Policy* *(1)*

INFO 150248 Missing header: Permissions-Policy

Finding #	**1034150**(73639748)	**Severity**	Information Gathered - Level 2
Unique #	**3b063857-9135-4d8f-a737-9e3e7b0569fc**		
Group	Security Weaknesses	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	CWE-284		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The Permissions-Policy response header is not present.

Impact

Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application. A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies

Not defining policy for unused and risky policy-controlled features may leave application vulnerable.

Solution

It is recommended to define policy for policy-controlled features to make application more secure.

References:

Permissions-Policy W3C
Working Draft Policy
Controlled Features

Results

```
Permissions-Policy: Header missing
Response headers on link: GET https://www.ayabank.com/ response code: 200
Date: Thu, 06 Jul 2023 04:36:19 GMT
Server: Apache
Cache-Control: no-cache, private Content-
Encoding: gzip
Vary: Accept-Encoding,User-Agent Set-
Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/
Set-Cookie:
aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
HttpOnly; expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/


aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
expires=Thu, 06-Jul-2023 06: 36:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block Access-
Control-Allow-Origin: *
Access-Control-Allow-Methods: GET Keep-
Alive: timeout=20, max=86 Connection:
Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8


Header missing on the following link(s):
(Only first 50 such pages are listed)


GET https://www.ayabank.com/ response code: 200
GET https://www.ayabank.com/?s=discovery response code: 200
GET https://www.ayabank.com/privacy-notice-cookie-policy response code: 200
GET https://www.ayabank.com/business/account-saving/call-deposit response code: 200
GET https://www.ayabank.com/public/blog_images/Green-Energy-Exhibition-Banking-Partner.webp response code: 200
GET https://www.ayabank.com/business/remittance-payments/local-payments response code: 200
GET https://www.ayabank.com/about-aya/governance/corporate-governance response code: 200
GET https://www.ayabank.com/public/blog_images/Workshop-for-Certified-Branch-Managers-Program.webp response code: 200
GET https://www.ayabank.com/css/core.min.css response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life/universal response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving response code: 200
GET https://www.ayabank.com/business/insurance/oversea-marine-cargo response code: 200
GET https://www.ayabank.com/personal-banking/insurance/travel/aya-go response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit response code: 200
GET https://www.ayabank.com/business/insurance/industrial-all-risk response code: 200
GET https://www.ayabank.com/images/ayaicon.png response code: 200
GET https://www.ayabank.com/css/header.css response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/call-deposit response code: 200
GET https://www.ayabank.com/personal-banking/remittance/international response code: 200
GET https://www.ayabank.com/js/popper.js response code: 200
GET https://www.ayabank.com/business/borrowing/corporate-business-loan response code: 200
GET https://www.ayabank.com/business/trade/trade-financing response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life response code: 200
GET https://www.ayabank.com/digital-services/online-payment-services/corporate-internet-banking response code: 200
GET https://www.ayabank.com/sms-alert response code: 404
GET https://www.ayabank.com/digital-services/wallet-solution/aya-pay response code: 200
GET https://www.ayabank.com/business/borrowing/sme response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life/one-health-solution-individual-plan response code: 200
GET https://www.ayabank.com/business/cash-management response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/fixed-deposit response code: 200
GET https://www.ayabank.com/digital-services/guideline/digital-secure response code: 200
GET https://www.ayabank.com/digital-services/guideline/frequently-used-digital response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/our-strategies/corporate-strategy response code: 200
GET https://www.ayabank.com/business/borrowing/hire-purchase response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/c2c-auto-loan response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-su-buu response code: 200
GET https://www.ayabank.com/js/helpers.js response code: 200
GET https://www.ayabank.com/js/jquery.js response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/corporate-profile/mission-corporate-value-brand-promise response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/home-loan response code: 200
GET https://www.ayabank.com/personal-banking/remittance/local response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/construction-loan response code: 200
GET https://www.ayabank.com/personal-banking/royal-banking response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/our-strategies/stakeholder-management response code: 200
GET https://www.ayabank.com/about-aya/news-room/reports response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/current-deposit/new-business-current-account response code: 200
GET https://www.ayabank.com/digital-services/atm response code: 200
POST https://www.ayabank.com/report_download response code: 500
GET https://www.ayabank.com/css/landing_new.css response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-maximizer-saving response code: 200
```

INFO *150249 Misconfigured Header: Cache-Control (1)*

INFO 150249 Misconfigured Header: Cache-Control

Finding #	**1034151**(73639749)	Severity	Information Gathered - Level 2
Unique #	**204e0c4e-bf4a-4ab5-8ecb-86f2003f2e99**		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-525		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Cache-Control header present but directives may not configure to adequately safeguard sensitive information.

For Example:

Cache-Control directive set to public.

max-age value is greater than 86400.

Impact

If directive is set to public, the resource can be stored by any cache.

If max-age value is greater than 86400 for sensitive information may lead to information leakage.

Solution

Please check that resources with sensitive information are not configured with Cache-Control public directive.

Also please make sure that max-age directive value set properly to not cache sensitive information for longer period than needed.

References:

Mozilla Documentation Cache-Control

Results

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/public/blog_images/Green-Energy-Exhibition-Banking-Partner.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/public/blog_images/Workshop-for-Certified-Branch-Managers-Program.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/core.min.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/ayaicon.png response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/header.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/popper.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/helpers.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/jquery.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/landing_new.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.

```
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/fonts/boxicons.min.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/menu.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/fonts/Sora-Regular.ttf response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/style.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/moment.min.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/bootstrap.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/util.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/fonts/Pyidaungsu-1.8_Regular.ttf response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/main.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/public/blog_images/AYA-Bank-PCLs-Foreign-Currency-Online-Trading.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/fonts/boxicons/boxicons.svg? response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/fonts/boxicons/boxicons.ttf response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/dropdown_arrow.png response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/atm_branch_fx_counter.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/award_accolades_bg.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/ayapay_wallet.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/business.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/mbanking.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/desk_poster.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/news_image/view_all_news.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/new_home/personal_borrowing_plan.webp response code: 200
```

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/home/KV_slider_2.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/banner.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/js/moment.js response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/core.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/fonts/boxicons.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/business/acc-sav.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/business/account-saving/call-deposit/KV.jpg response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/business/remittance/local-payments.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/business/remittance/local-payments/KV.jpg response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/about-aya/corporate-governance.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/about-aya/corporate-governance/KV.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/slide_tab.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/pb_insurance.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/insurance/life/KV_bg.png response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/personal_banking/borrowing/hire_purchase/auto_loan.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/acc_saving/aya-regular-saving/KV.jpg response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/css/business/insurance.css response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/business/insurance/oversea-marine-cargo/KV_bg.png response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/insurance/aya-go/KV_bg.png response code: 200

Cache-Control: Header misconfigured. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:max-age=31536000 on the link: GET https://www.ayabank.com/images/acc_saving/saving-deposit/KV.jpg response code: 200

INFO *150262 Missing header: Feature-Policy (1)*

INFO 150262 Missing header: Feature-Policy

Finding #	**1034154**(73639752)	**Severity**	Information Gathered - Level 2
Unique #	**dec01fee-1f3c-495b-99b8-4e1da6173b03**		
Group	Security Weaknesses	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:

- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

```
Feature-Policy: Header missing
Response headers on link: GET https://www.ayabank.com/ response code: 200
Date: Thu, 06 Jul 2023 04:36:19 GMT
Server: Apache
Cache-Control: no-cache, private Content-
Encoding: gzip
Vary: Accept-Encoding,User-Agent Set-
Cookie: XSRF-
```

VULNERABILITY ASSESSMENT REPORT

```
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImZwNlJMbXlNWUM1eVRGVnBJbjJwdnc9PSIsInZhbHVlIjoiK3crcHN4UmVaa2tCV05OcjZFeWorN0dTeTZhTnVOaTZIanBPN0lBaXhodlYyOGhMN0pxdEJrT2dLL3JvTmZ6S09
expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/
Set-Cookie:
aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
HttpOnly; expires=Thu, 06-Jul-2023 06:36:20 GMT; domain=www.ayabank.com; SameSite=lax; path=/


aya_bank_session=eyJpdiI6InZGdEtrRGR2WStOUklRWjRlbXdBZ3c9PSIsInZhbHVlIjoiTXVCVGNXSkEwSU92Vkc1MVRpLzJhcmFkaUQ2cnZCaCtUb0oxTmlrQXBUUTVJYlY4VExwcG1QNXBx
expires=Thu, 06-Jul-2023 06: 36:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload Referrer-
Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block Access-
Control-Allow-Origin: *
Access-Control-Allow-Methods: GET Keep-
Alive: timeout=20, max=86 Connection:
Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Header missing on the following link(s):
(Only first 50 such pages are listed)

```
GET https://www.ayabank.com/ response code: 200
GET https://www.ayabank.com/?s=discovery response code: 200
GET https://www.ayabank.com/privacy-notice-cookie-policy response code: 200
GET https://www.ayabank.com/business/account-saving/call-deposit response code: 200
GET https://www.ayabank.com/public/blog_images/Green-Energy-Exhibition-Banking-Partner.webp response code: 200
GET https://www.ayabank.com/business/remittance-payments/local-payments response code: 200
GET https://www.ayabank.com/about-aya/governance/corporate-governance response code: 200
GET https://www.ayabank.com/public/blog_images/Workshop-for-Certified-Branch-Managers-Program.webp response code: 200
GET https://www.ayabank.com/css/core.min.css response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life/universal response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-regular-saving response code: 200
GET https://www.ayabank.com/business/insurance/oversea-marine-cargo response code: 200
GET https://www.ayabank.com/personal-banking/insurance/travel/aya-go response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit response code: 200
GET https://www.ayabank.com/business/insurance/industrial-all-risk response code: 200
GET https://www.ayabank.com/images/ayaicon.png response code: 200
GET https://www.ayabank.com/css/header.css response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/call-deposit response code: 200
GET https://www.ayabank.com/personal-banking/remittance/international response code: 200
GET https://www.ayabank.com/js/popper.js response code: 200
GET https://www.ayabank.com/business/borrowing/corporate-business-loan response code: 200
GET https://www.ayabank.com/business/trade/trade-financing response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life response code: 200
GET https://www.ayabank.com/digital-services/online-payment-services/corporate-internet-banking response code: 200
GET https://www.ayabank.com/sms-alert response code: 404
GET https://www.ayabank.com/digital-services/wallet-solution/aya-pay response code: 200
GET https://www.ayabank.com/business/borrowing/sme response code: 200
GET https://www.ayabank.com/personal-banking/insurance/life/one-health-solution-individual-plan response code: 200
GET https://www.ayabank.com/business/cash-management response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/fixed-deposit response code: 200
GET https://www.ayabank.com/digital-services/guideline/digital-secure response code: 200
GET https://www.ayabank.com/digital-services/guideline/frequently-used-digital response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/our-strategies/corporate-strategy response code: 200
GET https://www.ayabank.com/business/borrowing/hire-purchase response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/c2c-auto-loan response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-su-buu response code: 200
GET https://www.ayabank.com/js/helpers.js response code: 200
GET https://www.ayabank.com/js/jquery.js response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/corporate-profile/mission-corporate-value-brand-promise response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/home-loan response code: 200
GET https://www.ayabank.com/personal-banking/remittance/local response code: 200
GET https://www.ayabank.com/personal-banking/borrowing/hire-purchase/construction-loan response code: 200
GET https://www.ayabank.com/personal-banking/royal-banking response code: 200
GET https://www.ayabank.com/about-aya/who-we-are/our-strategies/stakeholder-management response code: 200
GET https://www.ayabank.com/about-aya/news-room/reports response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/current-deposit/new-business-current-account response code: 200
GET https://www.ayabank.com/digital-services/atm response code: 200
POST https://www.ayabank.com/report_download response code: 500
GET https://www.ayabank.com/css/landing_new.css response code: 200
GET https://www.ayabank.com/personal-banking/account-saving/saving-deposit/aya-maximizer-saving response code: 200
```

INFO *150101 Third-party Cookies Collected (1)*

INFO 150101 Third-party Cookies Collected

Finding #	**1034140**(73639738)	Severity	Information Gathered - Level 1
Unique #	**92bfb071-70de-4939-b9b4-5f0e592db2e4**		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were received from third-party web application(s) during the crawl phase.

Impact

Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

Solution

Review cookie values to ensure that sensitive information such as passwords are not present within them.

Results

```
Total cookies: 2
NID=511=vKrwzgR4lkKta8p0VUOnRM6HEg2rIrTWhzm0f3n1zA8HMmSPjPRCRcrEKWUTmm-Yd-1FZR7RX2lxIAz_YAiwH4hdn30-
qhAe7xec7FrK0Q_6MBMKnaexAv04_DiLQ9wNsSg35DUQJyuYpHYw7hhFrsBmNSHDwJufH0-s419_z3M; secure; HttpOnly; expires=Fri, 05-Jan-2024 04:38:50 GMT; domain=.google.com; path=/
First set at URL: https://www.google.com/maps/d/u/0/embed?mid=1TGQGlYgz_Y9HdOAuF7esdoZWtnSC9LI&ehbc=2E312F
_gat_gtag_UA_228606560_1=1; expires=Thu, 06-Jul-2023 04:40:52 GMT; domain=ayabank.com; path=/ First set at URL: https://www.ayabank.com/digital-services/card-services/simple-pay
```

INFO *150126 Links With High Resource Consumption* *(1)*

INFO 150126 Links With High Resource Consumption

Finding #	1034152(73639750)	Severity	Information Gathered - Level 1
Unique #	d1c12221-298f-4640-a7cd-786475156220		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact

The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution

Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

Results

```
688266.800000 bytes/sec https://www.ayabank.com/images/new_home/atm_branch_fx_counter.webp
802247.000000 bytes/sec https://www.ayabank.com/fonts/Sora-Regular.ttf
1822855.600000 bytes/sec https://www.ayabank.com/fonts/Pyidaungsu-1.8_Regular.ttf
2753258.800000 bytes/sec https://www.ayabank.com/images/corporate_internet_banking/KV.jpg
2816134.500000 bytes/sec https://www.ayabank.com/images/digital_secure/KV.jpg
2969636.800000 bytes/sec https://www.ayabank.com/fonts/boxicons/boxicons.woff
3011309.300000 bytes/sec https://www.ayabank.com/fonts/boxicons/boxicons.ttf
3486430.900000 bytes/sec https://www.ayabank.com/images/acc_saving/call_deposit/KV.jpg
3527875.300000 bytes/sec https://www.ayabank.com/images/business/remittance/local-payments/KV.jpg
```

```
4112527.900000 bytes/sec https://www.ayabank.com/images/corporate_internet_banking/basic.jpg
```

INFO *150142 Virtual Host Discovered* *(1)*

INFO 150142 Virtual Host Discovered

Finding #	**1034158**(73639756)	**Severity**	Information Gathered - Level 1
Unique #	**498c54d2-0986-4ae1-8ea5-7784ca702698**		
Group	Security Weaknesses	**Detection Date**	06 Jul 2023 11:05 GMT+0730
CWE	CWE-200		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Web server is responding differently when the HOST header is manipulated, and various common virtual hosts are tested. This could indicate the presence of Virtual Host. Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The extra virtual hosts discovered by the Web application scanner during HOST header manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures. If the Web application fails to apply security controls to other domains hosted on the same server, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Results

Virtual host discovered:

Detected based on: HTTP Response code
Virtual Host: mail.ayabank.com
URI: https://www.ayabank.com/

INFO *150277 Cookie without SameSite attribute* (1)

INFO 150277 Cookie without SameSite attribute

Finding #	**1034135**(73639733)	Severity	Information Gathered - Level 1
Unique #	**4aeceaa6-38ce-4785-a160-0facf2c6361e**		
Group	Security Weaknesses	Detection Date	06 Jul 2023 11:05 GMT+0730
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The cookies listed in the Results section are missing the SameSite attribute.

Impact

The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution

Consider adding the SameSite attribute to the cookie(s) listed.

More information:

DZone article

OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 1
_gat_gtag_UA_228606560_1=1; expires=Thu Jul 6 04:40:52 2023; path=/; domain=ayabank.com | First set at URL: https://www.ayabank.com/digital-services/card-services/simple-pay

Finding Summary List

Number of records: 48

Status	QID	Type	Title	Group	Last Detected	Age	Patch	Severity	Web Application	URL
New	151025	Qualys	Vulnerable JavaScript Library Detected - Moment.js	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 3	Coporate Website	https://www.ayabank.com/
-	150261	Qualys	Subresource Integrity (SRI) Not Implemented	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 3	Coporate Website	
-	150042	Qualys	Server Returns HTTP 5XX Error Code During Scanning	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 3	Coporate Website	
-	150089	Qualys	Links to non-routable resources discovered in externally facing content	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 3	Coporate Website	
New	150051	Qualys	Open Redirect	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 3	Coporate Website	https://www.ayabank.com/enquiry_form_submit
New	150162	Qualys	Use of JavaScript Library with Known Vulnerability	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 3	Coporate Website	https://www.ayabank.com/
New	150123	Qualys	Cookie Does Not Contain The "HTTPOnly" Attribute	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 2	Coporate Website	https://www.ayabank.com/digital-services/card-services/simple-pay
-	45017	Qualys	Operating System Detected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
-	150206	Qualys	Content-Security-Policy Not Implemented	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
-	150262	Qualys	Missing header: Feature-Policy	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
-	150249	Qualys	Misconfigured Header: Cache-Control	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
-	150248	Qualys	Missing header: Permissions-Policy	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
-	150375	Qualys	PII Fields Found	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
-	45017	Qualys	Operating System Detected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 2	Coporate Website	
New	150122	Qualys	Cookie Does Not Contain The "secure" Attribute	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 2	Coporate Website	https://www.ayabank.com/digital-services/card-services/simple-pay

New	150122	Qualys	Cookie Does Not Contain The "secure" Attribute	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 2	Coporate Website	https://www.ayabank.com/
New	150123	Qualys	Cookie Does Not Contain The "HTTPOnly" Attribute	Information Disclosure	06 Jul 2023 11:05AM GMT+0630	6		Confirmed Vulnerability - Level 2	Coporate Website	https://www.ayabank.com/
-	150082	Qualys	Protection against Clickjacking	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	
-	150528	Qualys	Server Returns HTTP 4XX Error Code During Scanning	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	
-	6	Qualys	DNS Host Name	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	
-	150020	Qualys	Links Rejected By Crawl Scope or Exclusion List	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	
-	150148	Qualys	AJAX Links Crawled	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	
-	150021	Qualys	Scan Diagnostics	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	
-	150277	Qualys	Cookie without SameSite attribute	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website	

-	150152	Qualys	Forms Crawled	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150028	Qualys	Cookies Collected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150546	Qualys	First Link Crawled Response Code Information	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150101	Qualys	Third-party Cookies Collected	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150104	Qualys	Form Contains Email Address Field	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150041	Qualys	Links Rejected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150621	Qualys	List of JavaScript Links	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150176	Qualys	In-scope JavaScript Libraries Detected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150054	Qualys	Email Addresses Collected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150247	Qualys	Web Server and Technologies Detected	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website

-	150126	Qualys	Links With High Resource Consumption	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	45038	Qualys	Host Scan Time - Scanner	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150010	Qualys	External Links Discovered	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150009	Qualys	Links Crawled	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	150142	Qualys	Virtual Host Discovered	Security Weaknesses	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	86002	Qualys	SSL Certificate - Information	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	38718	Qualys	Secure Sockets Layer (SSL) Certificate Transparency Information	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	38291	Qualys	SSL Session Caching Information	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	6	Qualys	DNS Host Name	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	42350	Qualys	TLS Secure Renegotiation Extension Support Information	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	38597	Qualys	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	38116	Qualys	SSL Server Information Retrieval	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	38704	Qualys	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website
-	38706	Qualys	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties	Scan Diagnostics	06 Jul 2023 11:05AM GMT+0630	6		Information Gathered - Level 1	Coporate Website

VULNERABILITY ASSESSMENT REPORT