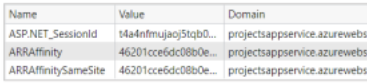
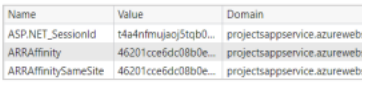
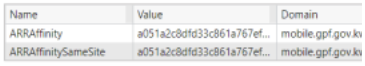
Please confirm if you finished the recommendations that related to your system.

Unencrypted __VIEWSTATE Parameter	Open Web.Config and add the following line under the <system.web> element: <machineKey validation="AES"/>	https://www.acunetix.com/vulnerabilities/web/unencrypted-__viewstate-parameter/	https://projectsappservice.azurewebsites.net/New/Login.asp
Vulnerable Javascript Library	Upgrade to the latest stable version of Javascript library.	https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://www.securityfocus.com/bid/108023 https://access.redhat.com/security/cve/CVE-2019-11358	https://projectsappservice.azurewebsites.net/New/vendor/b
Web Server Error Page Information Disclosure	Modify the web server to not disclose detailed information about the underlying web server or use a custom error page instead.	https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-3.0/h0hfz6fc(v=vs.85) https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/ https://www.owasp.org/index.php/Improper_Error_Handling	https://projectsappservice.azurewebsites.net/ Example: https://projectsappservice.azurewebsites.net:443/ Example: https://projectsappservice.azurewebsites.net:443/' Example: https://projectsappservice.azurewebsites.net:443/'
Insecure Inline Frame (iframe)	Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.	https://www.acunetix.com/vulnerabilities/web/insecure-inline-frame-iframe/ https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe	https://projectsappservice.azurewebsites.net/assets/vendor
Login Page Password-Guessing Attack	It is recommended to implement some type of account lockout after a defined number of incorrect password attempts. Also it is recommended to: - Use a strong CAPTCHA like Google reCAPTCHA for more security. - Use multifactor authentication method for accessing the accounts.	https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks	https://projectsappservice.azurewebsites.net/New/Login.asp
HTTP OPTIONS Method Enabled	It is recommended to disable OPTIONS method on the web server.	https://www.valencynetworks.com/kb/how-to-disable-options-method-vulnerability.html	https://projectsappservice.azurewebsites.net/
Web Server Allows Password Auto-Completion	Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.	https://portswigger.net/kb/issues/00500800_password-field-with-autocomplete-enabled	https://projectsappservice.azurewebsites.net/New/Login.asp
Possible Sensitive Directories	Restrict access to these directories or remove them and any unwanted directories from the website.	https://www.acunetix.com/websitesecurity/webserver-security/ https://www.technology.pitt.edu/security/disclosure-sensitive-information	https://projectsappservice.azurewebsites.net/ Example URLs: https://projectsappservice.azurewebsites.net:443/asse form/docs/_layouts/
Server Information Header Exposed	The server should be configured to remove unwanted HTTP response headers from the response.	https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/	https://projectsappservice.azurewebsites.net/ https://mobile.gpf.gov.kw/api/
X-Powered-By Header Exposed	The server configuration should be changed	https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/	https://projectsappservice.azurewebsites.net/

	to remove this header.		
ASP.NET Version Disclosure	Apply the following changes to the web.config file to prevent ASP.NET version disclosure:	http://msdn.microsoft.com/en-us/library/system.web.configuration.httpruntimesection.enableversionheader.aspx https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/version-disclosure-aspnet/	https://projectsappservice.azurewebsites.net/
Clickjacking: X-Frame-Options Header Missing	Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive	https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options https://www.owasp.org/index.php/Clickjacking https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-frame-options-header/	https://projectsappservice.azurewebsites.net/
Missing HTTP Security Headers (X-XSS-Protection)	We recommend setting the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block"	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection	https://projectsappservice.azurewebsites.net/
Missing HTTP Security Headers (X-Content-Type-Options)	We recommend setting the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options	https://projectsappservice.azurewebsites.net/
Missing HTTP Security Headers (Content-Security-Policy)	It is recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP https://hacks.mozilla.org/2016/02/implementing-content-security-policy/	https://projectsappservice.azurewebsites.net/
Missing HTTP Security Headers (Referrer-Policy)	- You should use POST rather than GET wherever possible, to avoid passing sensitive data to other locations via URLs. - You should always use HTTPS for your sites. - You should consider removing any third-party content (e.g. social networking widgets embedded in) from secure areas of your website, like password reset pages, payment forms, login areas, etc. - The Referrer-Policy header on your server to control what information is sent through the Referrer header	https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy	https://projectsappservice.azurewebsites.net/
Missing HTTP Security Headers (Feature-Policy)	We recommend using the Feature-Policy header to control and restrict what APIs the site	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy	https://projectsappservice.azurewebsites.net/

	can access or modify the browser's default behavior for certain features.		
Cookie(s) without Secure Flag Set	If possible, you should set the Secure flag for this cookie.	https://portswigger.net/kb/issues/00500200_ssl-cookie-without-secure-flag-set	https://projectsappservice.azurewebsites.net/New/Login.asp URL: https://projectsappservice.azurewebsites.net:443/New/Logir Parameter: ASP.NET_SessionId  Name Value Domain ASP.NET_SessionId t4a4nfmujaoj5tqb0... projectsappservice.azurewebs ARRAffinity 46201cce6dc08b0e... projectsappservice.azurewebs ARRAffinitySameSite 46201cce6dc08b0e... projectsappservice.azurewebs
Cookie(s) without SameSite Flag Set	The server can set a same-site cookie by adding the SameSite=... attribute to the Set-Cookie header: Set-Cookie: key=value; SameSite=strict There are two possible values for the same-site attribute: • Lax • Strict In the strict mode, the cookie is not sent with any cross-site usage even if the user follows a link to another website. Lax cookies are only sent with a top-level get request. If the cookie contains sensitive information, then the server should ensure that the cookie has the SameSite flag set. If set, it can help in preventing Cross-Site Request Forgery (CSRF) attacks	https://www.tenable.com/plugins/was/115540 https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/samesite-cookie-not-implemented/	https://projectsappservice.azurewebsites.net/New/Login.asp https://mobile.gpf.gov.kw/api/ URL: https://projectsappservice.azurewebsites.net:443/New/Logi Parameter: ARRAffinity, ARRAffinitySameSite  Name Value Domain ASP.NET_SessionId t4a4nfmujaoj5tqb0... projectsappservice.azureweb ARRAffinity 46201cce6dc08b0e... projectsappservice.azureweb ARRAffinitySameSite 46201cce6dc08b0e... projectsappservice.azureweb URL: https://mobile.gpf.gov.kw:443/api/ Parameter: ARRAffinity, ARRAffinitySameSite  Name Value Domain ARRAffinity a051a2c8dfd33c861a767ef... mobile.gpf.gov.kv ARRAffinitySameSite a051a2c8dfd33c861a767ef... mobile.gpf.gov.kv