ZAP Security Report for PurpleBox APIs

Program Name: ZAP
Version: 2.13.0
Generated: Mon, 21 Aug 2023 05:45:26

Site Name: http://host.docker.internal:8000
Host: host.docker.internal
Port: 8000
SSL: Disabled

Alert 1 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
1. SQL Injection	40018	3	2	High (Medium)	SQL injection may be possible.
Instances Count	**CWE ID**	**WASC ID**	**Source ID**	**Solution**	**Solution Reference**
1	89	19	348	Do not trust client side input, even if there is client side validation in place.In general, type check all data on the server side.If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.If database Stored Procedures can be used, use them.Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!Do not create dynamic SQL queries using simple string concatenation.Escape all data received from the client.Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.Apply the principle of least privilege by using the least privileged database user possible.In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.Grant the minimum database access that is necessary for the application.	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
Instances info is	located in the	INSTANCES	APPENDIX		

Alert 2 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
2. A Server Error response code was returned by the server	100000	1	3	Low (High)	A response code of 500 was returned by the server.This may indicate that the application is failing to handle unexpected input correctly.Raised by the 'Alert on HTTP Response Code Error' script
Instances Count	CWE ID	WASC ID	Source ID	Solution	Solution Reference
35	388	20	1093		
Instances info is	located in the	INSTANCES	APPENDIX		

Alert 3 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
3. X-Content-Type-Options Header Missing	10021	1	2	Low (Medium)	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Instances Count	CWE ID	WASC ID	Source ID	Solution	Solution Reference
2	693	15	1	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspxhttps://owasp.org/www-community/Security_Headers
Instances info is	located in the	INSTANCES	APPENDIX		

Alert 4 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
4. A Client Error response code was returned by the server	100000	0	3	Informational (High)	A response code of 404 was returned by the server.This may indicate that the application is failing to handle unexpected input correctly.Raised by the 'Alert on HTTP Response Code Error' script
Instances Count	CWE ID	WASC ID	Source ID	Solution	Solution Reference
224	388	20	13		
Instances info is	located in the	INSTANCES	APPENDIX		

Alert 5 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
5. Authentication Request Identified	10111	0	3	Informational (High)	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
Instances Count	CWE ID	WASC ID	Source ID	Solution	Solution Reference
1	-1	-1	4	This is an informational alert rather than a vulnerability and so there is nothing to fix.	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
Instances info is	located in the	INSTANCES	APPENDIX		

Alert 6 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
6. Non-Storable Content	10049	0	2	Informational (Medium)	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
Instances Count	**CWE ID**	**WASC ID**	**Source ID**	**Solution**	**Solution Reference**
4	524	13	6	The content may be marked as storable by ensuring that the following conditions are satisfied:The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable)The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood)The "no-store" cache directive must not appear in the request or response header fieldsFor caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the responseFor caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives)In addition to the conditions above, at least one of the following conditions must also be satisfied by the response:It must contain an "Expires" header fieldIt must contain a "max-age" response directiveFor "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directiveIt must contain a "Cache Control Extension" that allows it to be cachedIt must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).	https://tools.ietf.org/html/rfc7234https://tools.ietf.org/html/rfc7231http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
Instances info is	located in the	INSTANCES	APPENDIX		

Alert 7 Summary

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
7. Storable and Cacheable Content	10049	0	2	Informational (Medium)	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Instances Count	**CWE ID**	**WASC ID**	**Source ID**	**Solution**	**Solution Reference**
2	524	13	1	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:Cache-Control: no-cache, no-store, must-revalidate, privatePragma: no-cacheExpires: 0This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.	https://tools.ietf.org/html/rfc7234https://tools.ietf.org/html/rfc7231http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
Instances info is	located in the	INSTANCES	APPENDIX		

Endpoint Access Summary

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/Account/IsTenantAvailable	Yes	Yes	Yes
/api/services/app/Account/SendPasswordResetCode	Yes	Yes	Yes
/api/services/app/Account/SendNewAccountPasswordResetCode	Yes	Yes	Yes
/api/services/app/Account/Register	Yes	Yes	Yes
/api/services/app/Account/ResetPassword	Yes	Yes	Yes
/api/services/app/Account/ResolveTenantId	Yes	Yes	Yes
/api/services/app/ClientAdviserRelationship/GetAllSelectedAdvisers	Yes	Yes	Yes
/api/services/app/ClientAdviserRelationship/GetAllSelectedClients	Yes	Yes	Yes
/api/services/app/ClientAdviserRelationship/GetAllSelectedClientsInList	Yes	Yes	Yes
/api/services/app/ClientAdviserRelationship/CreateRelationshipMap	Yes	Yes	No
/api/services/app/ClientAdviserRelationship/DeleteClientAllRelationships	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/GetSelectedClientAndFlexiformTemplate	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/CreateAccessMap	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/DeleteAccess	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/Get	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/GetAll	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/Create	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/Update	Yes	Yes	No
/api/services/app/ClientFlexiformTemplateAccess/Delete	Yes	Yes	No
/api/services/app/CoClient/Create	Yes	Yes	Yes
/api/services/app/CoClient/GetByPrimaryUserId	Yes	Yes	Yes
/api/services/app/CoClient/Get	Yes	Yes	Yes
/api/services/app/CoClient/GetAll	Yes	Yes	Yes
/api/services/app/CoClient/Update	Yes	Yes	Yes
/api/services/app/CoClient/Delete	Yes	Yes	Yes
/api/services/app/CommonLookup/GetEditionsForCombobox	Yes	Yes	Yes
/api/services/app/CommonLookup/GetDefaultEditionName	Yes	Yes	Yes
/api/services/app/Configuration/ChangeUiTheme	Yes	No	No
/api/services/app/Customisation/ChangeThemeColor	Yes	No	No
/api/services/app/Customisation/GetByTenant	Yes	Yes	Yes

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/Customisation/Get	Yes	Yes	Yes
/api/services/app/Customisation/GetAll	Yes	Yes	Yes
/api/services/app/Customisation/Create	Yes	Yes	Yes
/api/services/app/Customisation/Update	Yes	Yes	Yes
/api/services/app/Customisation/Delete	Yes	Yes	Yes
/api/services/app/DynamicFormMapping/Get	Yes	Yes	No
/api/services/app/DynamicFormMapping/GetById	Yes	Yes	No
/api/services/app/DynamicFormMapping/GetByName	Yes	Yes	No
/api/services/app/DynamicFormMapping/getBySrsDestIds	Yes	Yes	No
/api/services/app/DynamicFormMapping/Create	Yes	Yes	No
/api/services/app/DynamicFormMapping/Update	Yes	Yes	No
/api/services/app/DynamicFormMapping/UpdateStatus	Yes	Yes	No
/api/services/app/Edition/GetEditions	No	No	No
/api/services/app/Edition/GetEditionForEdit	No	No	No
/api/services/app/Edition/CreateEdition	No	No	No
/api/services/app/Edition/UpdateEdition	No	No	No
/api/services/app/Edition/DeleteEdition	No	No	No
/api/services/app/Edition/GetEditionComboboxItems	No	No	No
/api/services/app/Edition/GetTenantCount	Yes	Yes	Yes
/api/services/app/Flexiform/Get	Yes	Yes	No
/api/services/app/Flexiform/GetAllWithSubmitterNameAndTemplateName	Yes	Yes	No
/api/services/app/Flexiform/GetAllWithSubmitterNameAndTemplateNameShorterRequest	Yes	Yes	No
/api/services/app/Flexiform/GetByClientUserIdWithSubmitterNameAndTemplateName	Yes	Yes	Yes
/api/services/app/Flexiform/GetByFlexiformTemplateIdAndClientUserIdWithSubmitterNameAndTemplateName	Yes	Yes	No
/api/services/app/Flexiform/GetById	Yes	Yes	No
/api/services/app/Flexiform/GetByIdClientOnly	Yes	Yes	Yes
/api/services/app/Flexiform/GetByEmailAddress	Yes	Yes	No
/api/services/app/Flexiform/Create	Yes	Yes	Yes
/api/services/app/FlexiformTemplate/Get	Yes	Yes	No
/api/services/app/FlexiformTemplate/GetById	Yes	Yes	Yes
/api/services/app/FlexiformTemplate/GetByName	Yes	Yes	Yes
/api/services/app/FlexiformTemplate/GetListByNameContain	Yes	Yes	Yes

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/FlexiformTemplate/GetByStatus	Yes	Yes	Yes
/api/services/app/FlexiformTemplate/Create	Yes	Yes	No
/api/services/app/FlexiformTemplate/UpdateStatus	Yes	Yes	No
/api/services/app/Notification/PostMessageSendGridApi	Yes	Yes	Yes
/api/services/app/Notification/SendEmailByUserIds	Yes	Yes	Yes
/api/services/app/Notification/SendSubmissionUpdateEmail	Yes	Yes	Yes
/api/services/app/Notification/SendEmailWithSingleAttachment	Yes	Yes	Yes
/api/services/app/Notification/SendEmailWithAttachments	Yes	Yes	Yes
/api/services/app/Notification/SendSmtpEmailWithAttachments	Yes	Yes	Yes
/api/services/app/Role/Create	Yes	No	No
/api/services/app/Role/GetRolesAsync	Yes	No	No
/api/services/app/Role/Update	Yes	No	No
/api/services/app/Role/Delete	Yes	No	No
/api/services/app/Role/GetAllPermissions	Yes	No	No
/api/services/app/Role/GetRoleForEdit	Yes	No	No
/api/services/app/Role/Get	Yes	No	No
/api/services/app/Role/GetAll	Yes	No	No
/api/services/app/Session/GetCurrentLoginInformations	Yes	Yes	Yes
/api/services/app/SmtpConfigService/CreateSmtpConfig	Yes	Yes	Yes
/api/services/app/SmtpConfigService/GetByTenant	Yes	Yes	Yes
/api/services/app/SmtpConfigService/Get	Yes	Yes	Yes
/api/services/app/SmtpConfigService/GetAll	Yes	Yes	Yes
/api/services/app/SmtpConfigService/Create	Yes	Yes	Yes
/api/services/app/SmtpConfigService/Update	Yes	Yes	Yes
/api/services/app/SmtpConfigService/Delete	Yes	Yes	Yes
/api/services/app/Tenant/Create	No	No	No
/api/services/app/Tenant/GetTenantFeaturesForEdit	No	No	No
/api/services/app/Tenant/UpdateTenantFeatures	No	No	No
/api/services/app/Tenant/ResetTenantSpecificFeatures	No	No	No
/api/services/app/Tenant/Delete	No	No	No
/api/services/app/Tenant/Get	No	No	No
/api/services/app/Tenant/GetAll	No	No	No

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/Tenant/Update	Yes	Yes	Yes
/api/services/app/TenantBlobService/UploadFile	Yes	No	No
/api/services/app/TenantBlobService/ListAllFiles	Yes	No	No
/api/services/app/TenantBlobService/ListFilesInDirectory	Yes	No	No
/api/services/app/TenantBlobService/GetBlobAsync	Yes	No	No
/api/services/app/TenantMFASettings/GetByTenant	Yes	Yes	No
/api/services/app/TenantMFASettings/UpdateTenantConfig	Yes	Yes	No
/api/services/app/TenantMFASettings/Get	Yes	Yes	No
/api/services/app/TenantMFASettings/GetAll	Yes	Yes	No
/api/services/app/TenantMFASettings/Create	Yes	Yes	No
/api/services/app/TenantMFASettings/Update	Yes	Yes	No
/api/services/app/TenantMFASettings/Delete	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/GetByTenant	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/UpdateTenantConfig	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/Get	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/GetAll	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/Create	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/Update	Yes	Yes	No
/api/services/app/TenantXplanNoteEmail/Delete	Yes	Yes	No
/api/services/app/Timing/GetTimezones	Yes	Yes	Yes
/api/services/app/Timing/GetTimezoneComboboxItems	Yes	Yes	Yes
/api/TokenAuth/Authenticate	Yes	Yes	Yes
/api/TokenAuth/AuthenticateFlexiformSubmission	Yes	Yes	Yes
/api/TokenAuth/GetExternalAuthenticationProviders	Yes	Yes	Yes
/api/TokenAuth/ExternalAuthenticate	Yes	Yes	Yes
/api/TokenAuth/SendTwoFactorAuthCode	Yes	Yes	Yes
/api/TokenAuth/SendFlexiformSubmissionClientSecurityCode	Yes	Yes	Yes
/api/services/app/User/Create	Yes	Yes	No
/api/services/app/User/Update	Yes	Yes	No
/api/services/app/User/Delete	Yes	Yes	No
/api/services/app/User/GetRoles	Yes	Yes	No
/api/services/app/User/ChangeLanguage	Yes	Yes	No

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/User/ChangePassword	Yes	Yes	No
/api/services/app/User/ResetPassword	Yes	Yes	No
/api/services/app/User/Get	Yes	Yes	No
/api/services/app/User/GetAll	Yes	Yes	No
/api/services/app/UserContact/Create	Yes	Yes	Yes
/api/services/app/UserContact/GetByUserId	Yes	Yes	Yes
/api/services/app/UserContact/Get	Yes	Yes	Yes
/api/services/app/UserContact/GetAll	Yes	Yes	Yes
/api/services/app/UserContact/Update	Yes	Yes	Yes
/api/services/app/UserContact/Delete	Yes	Yes	Yes
/api/services/app/UserXplanDetail/GetByUserId	Yes	Yes	No
/api/services/app/UserXplanDetail/Create	Yes	Yes	No
/api/services/app/UserXplanDetail/Get	Yes	Yes	No
/api/services/app/UserXplanDetail/GetAll	Yes	Yes	No
/api/services/app/UserXplanDetail/Update	Yes	Yes	No
/api/services/app/UserXplanDetail/Delete	Yes	Yes	No
/api/services/app/XplanApiResourcefulService/GetResourcefulGoalsObjectivesAsync	Yes	Yes	Yes
/api/services/app/XplanApiResourcefulService/PostAUResourcefulGoalsObjectivesAsync	Yes	Yes	Yes
/api/services/app/XplanApiResourcefulService/PatchAUResourcefulGoalsObjectivesAsync	Yes	Yes	Yes
/api/services/app/XplanApiResourcefulService/DeleteAUResourcefulGoalsObjectivesAsync	Yes	Yes	Yes
/api/services/app/XplanApiResourcefulService/GetResourcefulRiskProfileAsync	Yes	Yes	Yes
/api/services/app/XplanApiResourcefulService/PostAUResourcefulRiskProfileAsync	Yes	Yes	Yes
/api/services/app/XplanApiResourcefulService/PatchAUResourcefulRiskProfileAsync	Yes	Yes	Yes
/api/services/app/XplanApiService/PostSuperannuationBeneficiaryV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperannuationBeneficiaryByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchSuperannuationBeneficiaryV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteSuperannuationBeneficiaryV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperannuationBeneficiaryOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperfundMemberListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostSuperfundMemberV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperfundMemberByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchSuperfundMemberV2Async	Yes	Yes	Yes

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/XplanApiService/DeleteSuperfundMemberV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperfundTrusteeListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostSuperfundTrusteeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperfundTrusteeByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchSuperfundTrusteeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteSuperfundTrusteeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperfundTrusteeOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetUserListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetUserByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetAddressListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostAddressV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetAddressByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchAddressV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteAddressV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetAddressOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetAssetListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostAssetV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetAssetByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchAssetV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteAssetV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetAssetOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetBeneficiaryListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostBeneficiaryV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetBeneficiaryByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchBeneficiaryV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteBeneficiaryV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetBeneficiaryOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetClientListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostClientV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetClientByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchClientV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteClientV2Async	Yes	Yes	Yes

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/XplanApiService/GetClientOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetContactListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostContactV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetContactByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchContactV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteContactV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetContactOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetContributionListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostContributionV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetContributionByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchContributionV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteContributionV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetContributionOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetDependantListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostDependantV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetDependantByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchDependantV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteDependantV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetDependantOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostDocumentNoteV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetDocumentNoteOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetEstatePlanningListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchEstatePlanningV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetEstatePlanningOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetExecutorListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostExecutorV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetExecutorByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchExecutorV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteExecutorV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetExpenseListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostExpenseV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetExpenseByIdV2Async	Yes	Yes	Yes

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/XplanApiService/PatchExpenseV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteExpenseV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetExpenseOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetGeneralListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostGeneralV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetGeneralByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetGeneralOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetGoalListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostGoalV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetGoalByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchGoalV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteGoalV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetGoalOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetIncomeListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostIncomeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetIncomeByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchIncomeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteIncomeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetIncomeOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetInsuranceListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetLiabilityListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostLiabilityV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetLiabilityByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchLiabilityV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteLiabilityV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetLiabilityOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetLifeListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostLifeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetLifeByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetLifeOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetMedicalListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostMedicalV2Async	Yes	Yes	Yes

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/XplanApiService/GetMedicalByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetMedicalOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetObjectiveListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostObjectiveV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetObjectiveByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchObjectiveV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteObjectiveV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetObjectiveOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetPortfolioListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetPowerOfAttorneyListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostPowerOfAttorneyV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetPowerOfAttorneyByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchPowerOfAttorneyV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeletePowerOfAttorneyV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetPowerOfAttorneyOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetRetirementIncomeListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostRetirementIncomeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetRetirementIncomeByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchRetirementIncomeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteRetirementIncomeV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetRetirementIncomeOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSessionListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteSessionV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperannuationListV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PostSuperannuationV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperannuationByIdV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/PatchSuperannuationV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/DeleteSuperannuationV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperannuationOptionsV2Async	Yes	Yes	Yes
/api/services/app/XplanApiService/GetSuperannuationBeneficiaryListV2Async	Yes	Yes	Yes
/api/services/app/XplanOAuth2TenantConfig/Create	Yes	Yes	No
/api/services/app/XplanOAuth2TenantConfig/GetByTenant	Yes	Yes	No

Endpoint Name	Client Access	Advisor Access	Admin Access
/api/services/app/XplanOAuth2TenantConfig/GetDoRealOAuth2XplanAppSiteUri	Yes	Yes	Yes
/api/services/app/XplanOAuth2TenantConfig/GetByTenantStatic	Yes	Yes	No
/api/services/app/XplanOAuth2TenantConfig/Get	Yes	Yes	Yes
/api/services/app/XplanOAuth2TenantConfig/GetAll	Yes	Yes	Yes
/api/services/app/XplanOAuth2TenantConfig/Update	Yes	Yes	Yes
/api/services/app/XplanOAuth2TenantConfig/Delete	Yes	Yes	Yes
/api/services/app/XplanOAuthLogin/GetByUserId	Yes	Yes	No
/api/services/app/XplanOAuthLogin/GetByUserIdStatic	Yes	Yes	No
/api/services/app/XplanOAuthLogin/Create	Yes	Yes	No
/api/services/app/XplanOAuthLogin/DoRealOAuth2GetAccessTokenByAuthorisationCode	Yes	Yes	No
/api/services/app/XplanOAuthLogin/DoRealOAuth2GetAccessTokenByRefreshToken	Yes	Yes	No
/api/services/app/XplanOAuthLogin/DoRealOAuth2GetAccessTokenByXplanRedirect	Yes	Yes	No
/api/services/app/XplanOAuthLogin/GetAll	Yes	Yes	No
/api/services/app/XplanOAuthLogin/Update	Yes	Yes	No
/api/services/app/XplanOAuthLogin/Delete	Yes	Yes	No
/api/services/app/XplanOAuthLogin/Get	No	No	No

Appendix: Instances for Alert 1

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
1. SQL Injection	40018	3	2	High (Medium)	
Instance: Method	Param	Attack	Instance: URI	Evidence	Other Info
GET	item	item' OR '1'='1' --	http://host.docker.internal:8000/sqlinjection?item=item%27+AND+%271%27%3D%271%27+--+		The page results were successfully manipulated using the boolean conditions [item' AND '1'='1' --] and [item' OR '1'='1' --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison Data was NOT returned for the original parameter. The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter

Appendix: Instances for Alert 2

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
2. A Server Error response code was returned by the server	100000	1	3	Low (High)	
Instance: Method	**Param**	**Attack**	**Instance: URI**	**Evidence**	**Other Info**
GET			http://host.docker.internal:8000/sqlinjection?item=%22%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%22%2F%3E%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E%3C%21--	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%23%7Bglobal.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29%7D	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%24%7B%40print%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%7D%5C	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%27%28	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%27%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B%24var%3D%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%3C%25%3D+global.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29%25%3E	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Fhost.docker.internal%3A22%27%29%22%2F%3E	HTTP/1.1 500	

GET			http://host.docker.internal:8000/sqlinjection?item=%3Cxsl%3Avalue-of+select%3D%22php%3Afunction%28%27exec%27%2C%27erroneous_command+2%3E%26amp%3B1%27%29%22%2F%3E	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E%3C%21--	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%3Cxsl%3Avariable+name%3D%22rtobject%22+select%3D%22runtime%3AgetRuntime%28%29%22%2F%3E%0A%3Cxsl%3Avariable+name%3D%22process%22+select%3D%22runtime%3Aexec%28%24rtobject%2C%27erroneous_command%27%29%22%2F%3E%0A%3Cxsl%3Avariable+name%3D%22waiting%22+select%3D%22process%3AwaitFor%28%24process%29%22%2F%3E%0A%3Cxsl%3Avalue-of+select%3D%22%24process%22%2F%3E	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%7B%7B%3D+global.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29+%7D%7D	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=%7B%7Brange.constructor%28%22return+eval%28%5C%22global.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29%5C%22%29%22%29%28%29%7D%7D	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=5%3BURL%3D%27https%3A%2F%2F5947544072267739403.owasp.org%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%22+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%26cat+%2Fetc%2Fpasswd%26%27	HTTP/1.1 500	

GET			http://host.docker.internal:8000/sqlinjection?item=item%27%26sleep+1.0%26%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%26timeout+%2FT+1.0%26%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%26type+%25SYSTEMROOT%25%5Cwin.ini%26%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%28	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%3Bcat+%2Fetc%2Fpasswd%3B%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%3Bget-help	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%3Bsleep+1.0%3B%27	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%3Bstart-sleep+-s+1.0	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%7Ctimeout+%2FT+1.0	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%27+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%29+%27+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item%29+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=item+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=system-property%28%27xsl%3Avendor%27%29%2F%3E	HTTP/1.1 500	
GET			http://host.docker.internal:8000/sqlinjection?item=URL%3D%27http%3A%2F%2F5947544072267739403.owasp.org%27	HTTP/1.1 500	

Appendix: Instances for Alert 3

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
3. X-Content-Type-Options Header Missing	10021	1	2	Low (Medium)	
Instance: Method	**Param**	**Attack**	**Instance: URI**	**Evidence**	**Other Info**
GET	x-content-type-options		http://host.docker.internal:8000/openapi.json		This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
GET	x-content-type-options		http://host.docker.internal:8000/sqlinjection?item=item		This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

Appendix: Instances for Alert 4

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
4. A Client Error response code was returned by the server	100000	0	3	Informational (High)	
Instance: Method	Param	Attack	Instance: URI	Evidence	Other Info
GET			http://host.docker.internal:8000	HTTP/1.1 404	
GET			http://host.docker.internal:8000/	HTTP/1.1 404	
GET			http://host.docker.internal:8000/._darcs	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.bzr	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.DS_Store	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.env	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.git/config	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.hg	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.htaccess	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.idea/WebServers.xml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.php_cs.cache	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.ssh/id_dsa	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.ssh/id_rsa	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.svn/entries	HTTP/1.1 404	
GET			http://host.docker.internal:8000/.svn/wc.db	HTTP/1.1 404	
GET			http://host.docker.internal:8000/4142749567617553565	HTTP/1.1 404	
GET			http://host.docker.internal:8000/_framework/blazor.boot.json	HTTP/1.1 404	
GET			http://host.docker.internal:8000/_wpeprivate/config.json	HTTP/1.1 404	
GET			http://host.docker.internal:8000/actuator/health	HTTP/1.1 404	
GET			http://host.docker.internal:8000/adminer.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/app/etc/local.xml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/BitKeeper	HTTP/1.1 404	
GET			http://host.docker.internal:8000/CHANGELOG.txt	HTTP/1.1 404	

GET			http://host.docker.internal:8000/composer.json	HTTP/1.1 404	
GET			http://host.docker.internal:8000/composer.lock	HTTP/1.1 404	
GET			http://host.docker.internal:8000/config/database.yml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/config/databases.yml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/core	HTTP/1.1 404	
GET			http://host.docker.internal:8000/CVS/root	HTTP/1.1 404	
GET			http://host.docker.internal:8000/DEADJOE	HTTP/1.1 404	
GET			http://host.docker.internal:8000/elmah.axd	HTTP/1.1 404	
GET			http://host.docker.internal:8000/filezilla.xml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/i.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/id_dsa	HTTP/1.1 404	
GET			http://host.docker.internal:8000/id_rsa	HTTP/1.1 404	
GET			http://host.docker.internal:8000/info.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/key.pem	HTTP/1.1 404	
GET			http://host.docker.internal:8000/lfm.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/login?class.module.classLoader.DefaultAssertionStatus=nonsense	HTTP/1.1 405	
GET			http://host.docker.internal:8000/login?client_id=client_id&client;_secret=client_secret&grant;_type=grant_type&password;=ZAP&scope;=scope&username;=username	HTTP/1.1 405	
GET			http://host.docker.internal:8000/myserver.key	HTTP/1.1 404	
GET			http://host.docker.internal:8000/phpinfo.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/privatekey.key	HTTP/1.1 404	
GET			http://host.docker.internal:8000/scan	HTTP/1.1 404	
GET			http://host.docker.internal:8000/scan/	HTTP/1.1 404	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D/	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22%27	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22%2Bresponse.write%28123%2C567*521%2C110%29%2B%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22%2F%3E%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E%3C%21--	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B%24var%3D%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22%3E%3C%21--%23EXEC+cmd%3D%22dir+%5C%22--%3E%3C	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%22%3E%3C%21--%23EXEC+cmd%3D%22ls+%2F%22--%3E%3C	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%23%7B%25x%28sleep+2%29%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%23%7Bglobal.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%23set%28%24engine%3D%22%22%29%0A%23set%28%24proc%3D%24engine.getClass%28%29.forName%28%22java.lang.Runtime%22%29.getRuntime%28%29.exec%28%22sleep+2%22%29%29%0A%23set%28%24null%3D%24proc.waitFor%28%29%29%0A%24%7Bnull%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%24%7B%40print%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%24%7B%40print%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%7D%5C	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%24%7B__import__%28%22subprocess%22%29.check_output%28%22sleep+2%22%2C+shell%3DTrue%29%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%27%28	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%27%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B%24var%3D%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%2Bresponse.write%28%7B0%7D*%7B1%7D%29%2B	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%2F%2F5947544072267739403.owasp.org	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3B	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3Bprint%28chr%28122%29.chr%2897%29.chr%28112%29.chr%2895%29.chr%28116%29.chr%28111%29.chr%28107%29.chr%28101%29.chr%28110%29%29%3B	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C%21--	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C%21--%23EXEC+cmd%3D%22dir+%5C%22--%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C%21--%23EXEC+cmd%3D%22ls+%2F%22--%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C%23assign+ex%3D%22freemarker.template.utility.Execute%22%3Fnew%28%29%3E+%24%7B+ex%28%22sleep+2%22%29+%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C%25%3D%25x%28sleep+2%29%25%3E	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3C%25%3D+global.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29%25%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Fhost.docker.internal%3A22%22%27%29%22%2F%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3Cxsl%3Avalue-of+select%3D%22php%3Afunction%28%27exec%27%2C%27erroneous_command+2%3E%26amp%3B1%27%29%22%2F%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E%3C%21--	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%3Cxsl%3Avariable+name%3D%22rtobject%22+select%3D%22runtime%3AgetRuntime%28%29%22%2F%3E%0A%3Cxsl%3Avariable+name%3D%22process%22+select%3D%22runtime%3Aexec%28%24rtobject%2C%27erroneous_command%27%29%22%2F%3E%0A%3Cxsl%3Avariable+name%3D%22waiting%22+select%3D%22process%3AwaitFor%28%24process%29%22%2F%3E%0A%3Cxsl%3Avalue-of+select%3D%22%24process%22%2F%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%5D%5D%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%7B%7B%22%22.__class__.__mro__%5B1%5D.__subclasses__%28%29%5B157%5D.__repr__.__globals__.get%28%22__builtins__%22%29.get%28%22__import__%22%29%28%22subprocess%22%29.check_output%28%22sleep+2%22%29%7D%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%7B%7B%3D+global.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29+%7D%7D	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%7B%7B__import__%28%22subprocess%22%29.check_output%28%22sleep+2%22%2C+shell%3DTrue%29%7D%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%7B%7Brange.constructor%28%22return+eval%28%5C%22global.process.mainModule.require%28%27child_process%27%29.execSync%28%27sleep+2%27%29.toString%28%29%5C%22%29%22%29%28%29%7D%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=%7Bsystem%28%22sleep+2%22%29%7D	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=5%3BURL%3D%27https%3A%2F%2F5947544072267739403.owasp.org%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=5947544072267739403.owasp.org	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=any%0ASet-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=any%0D%0ASet-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=any%0D%0ASet-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d%0D%0A	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=any%3F%0ASet-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=any%3F%0D%0ASet-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=any%3F%0D%0ASet-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d%0D%0A	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=cat+%2Fetc%2Fpasswd	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=get-help	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2F%5C594754407226 7739403.owasp.org	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2F5947544072267739 403.owasp.org	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2Fwww.google.com	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2Fwww.google.com% 2F	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2Fwww.google.com% 2Fsearch%3Fq%3DOWASP%2520ZAP	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2Fwww.google.com% 3A80%2F	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=http%3A%2F%2Fwww.google.com% 3A80%2Fsearch%3Fq%3DOWASP%2520ZAP	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=https%3A%2F%2F%5C59475440722 67739403.owasp.org	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=https%3A%2F%2F594754407226773 9403%252eowasp%252eorg	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=https%3A%2F%2F594754407226773 9403.owasp.org	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=ID	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=ID%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=ID%22%26cat+%2Fetc%2Fpasswd% 26%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=ID%22%26sleep+1.0%26%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=ID%22%26timeout+%2FT+1.0%26% 22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID %7D?ID=ID%22%26type+%25SYSTEMROOT %25%5Cwin.ini%26%22	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22%3Bcat+%2Fetc%2Fpasswd%3B%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22%3Bget-help	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22%3Bsleep+1.0%3B%22	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22%3Bstart-sleep+-s+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22%7Ctimeout+%2FT+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22+UNION+ALL+select+NULL+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%22+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%26cat+%2Fetc%2Fpasswd%26	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%26sleep+1.0%26	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%26timeout+%2FT+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%26type+%25SYSTEMROOT%25%5Cwin.ini	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%26cat+%2Fetc%2Fpasswd%26%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%26sleep+1.0%26%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%26timeout+%2FT+1.0%26%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%26type+%25SYSTEMROOT%25%5Cwin.ini%26%27	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%28	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%29+UNION+ALL+select+NULL+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%3Bcat+%2Fetc%2Fpasswd%3B%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%3Bget-help	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%3Bsleep+1.0%3B%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%3Bstart-sleep+-s+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%7Ctimeout+%2FT+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27+AND+%271%27%3D%271%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27+AND+%271%27%3D%272%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27+OR+%271%27%3D%271%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27+UNION+ALL+select+NULL+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%27+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%29+%27+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%29+UNION+ALL+select+NULL+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%29+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3B	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3Bcat+%2Fetc%2Fpasswd%3B	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3Bget-help	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3Bget-help+%23	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3Bsleep+1.0%3B	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3Bstart-sleep+-s+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%3Bstart-sleep+-s+1.0+%23	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%7Ctimeout+%2FT+1.0	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID%7Ctype+%25SYSTEMROOT%25%5Cwin.ini	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID&class.module.classLoader.DefaultAssertionStatus;=nonsense	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID+AND+1%3D1+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID+AND+1%3D2+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID+OR+1%3D1+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID+UNION+ALL+select+NULL+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID+WAITFOR+DELAY+%270%3A0%3A15%27+--+	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=response.write%28123%2C567*521%2C110%29	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=Set-cookie%3A+Tamper%3D44ec83a4-3086-4b63-80c3-d951281e100d	HTTP/1.1 401	
GET			LONG URI SEE APPENDIX ENTRY NO: 1	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=system-property%28%27xsl%3Avendor%27%29%2F%3E	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=type+%25SYSTEMROOT%25%5Cwin.ini	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=URL%3D%27http%3A%2F%2F5947544072267739403.owasp.org%27	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=www.google.com	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=www.google.com%2F	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=www.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=www.google.com%3A80%2F	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=www.google.com%3A80%2Fsearch%3Fq%3DOWASP%2520ZAP	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ZAP	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%0A	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ZAP+%251%21s%252%21s%253%21s%254%21s%255%21s%256%21s%257%21s%258%21s%259%21s%2510%21s%2511%21s%2512%21s%2513%21s%2514%21s%2515%21s%2516%21s%2517%21s%2518%21s%2519%21s%2520%21s%2521%21n%2522%21n%2523%21n%2524%21n%2525%21n%2526%21n%2527%21n%2528%21n%2529%21n%2530%21n%2531%21n%2532%21n%2533%21n%2534%21n%2535%21n%2536%21n%2537%21n%2538%21n%2539%21n%2540%21n%0A	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%23%7B7244*2766%7Dzj	HTTP/1.1 401	

GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%23set%28%24x%3D4824*3098%29%24%7Bx%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%24%7B8430*6502%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%3C%25%3D2086*2898%25%3Ezj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%3Cp+th%3Atext%3D%22%24%7B6307*2137%7D%22%3E%3C%2Fp%3Ezj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%237543*5471%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%403989*5344%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%40math+key%3D%226771%22+method%3D%22multiply%22+operand%3D%228243%22%2F%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%7B%3D1462*9637%7D%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%7B2344*8225%7D%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%7B48300%7Cadd%3A56680%7D%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B%7Bprint+%226462%22+%228272%22%7D%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj%7B1794*4485%7Dzj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=zj+5080*8308+zj	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/.env	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/.htaccess	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/8217313364316538587	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan/trace.axd	HTTP/1.1 401	
GET			http://host.docker.internal:8000/scan?class.module.classLoader.DefaultAssertionStatus=nonsense	HTTP/1.1 404	
GET			http://host.docker.internal:8000/server-info	HTTP/1.1 404	

GET			http://host.docker.internal:8000/server-status	HTTP/1.1 404	
GET			http://host.docker.internal:8000/server.key	HTTP/1.1 404	
GET			http://host.docker.internal:8000/sftp-config.json	HTTP/1.1 404	
GET			http://host.docker.internal:8000/signup?class.module.classLoader.DefaultAssertionStatus=nonsense	HTTP/1.1 405	
GET			http://host.docker.internal:8000/sitemanager.xml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/sites/default/files/.ht.sqlite	HTTP/1.1 404	
GET			http://host.docker.internal:8000/sites/default/private/files/backup_migrate/scheduled/test.txt	HTTP/1.1 404	
GET			http://host.docker.internal:8000/sqlinjection	HTTP/1.1 422	
GET			http://host.docker.internal:8000/sqlinjection/	HTTP/1.1 422	
GET			http://host.docker.internal:8000/sqlinjection?=	HTTP/1.1 422	
GET			http://host.docker.internal:8000/test.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/trace.axd	HTTP/1.1 404	
GET			http://host.docker.internal:8000/user	HTTP/1.1 401	
GET			http://host.docker.internal:8000/user/	HTTP/1.1 401	
GET			http://host.docker.internal:8000/user?class.module.classLoader.DefaultAssertionStatus=nonsense	HTTP/1.1 401	
GET			http://host.docker.internal:8000/vb_test.php	HTTP/1.1 404	
GET			http://host.docker.internal:8000/vim_settings.xml	HTTP/1.1 404	
GET			http://host.docker.internal:8000/winscp.ini	HTTP/1.1 404	
GET			http://host.docker.internal:8000/WS_FTP.ini	HTTP/1.1 404	
GET			http://host.docker.internal:8000?class.module.classLoader.DefaultAssertionStatus=nonsense	HTTP/1.1 404	
POST			http://host.docker.internal:8000	HTTP/1.1 404	
POST			http://host.docker.internal:8000/latest/meta-data/	HTTP/1.1 404	
POST			http://host.docker.internal:8000/login	HTTP/1.1 422	
POST			http://host.docker.internal:8000/login/	HTTP/1.1 422	
POST			http://host.docker.internal:8000/openapi.json	HTTP/1.1 405	
POST			http://host.docker.internal:8000/scan	HTTP/1.1 404	

POST			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID	HTTP/1.1 405	
POST			http://host.docker.internal:8000/signup	HTTP/1.1 401	
POST			http://host.docker.internal:8000/signup/	HTTP/1.1 401	
POST			http://host.docker.internal:8000/sqlinjection?item=item	HTTP/1.1 405	
POST			http://host.docker.internal:8000/user	HTTP/1.1 405	

Appendix: Instances for Alert 5

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
5. Authentication Request Identified	10111	0	3	Informational (High)	
Instance: Method	Param	Attack	Instance: URI	Evidence	Other Info
POST	username		http://host.docker.internal:8000/login	password	userParam=username userValue=username passwordParam=password

Appendix: Instances for Alert 6

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
6. Non-Storable Content	10049	0	2	Informational (Medium)	
Instance: Method	Param	Attack	Instance: URI	Evidence	Other Info
GET			http://host.docker.internal:8000/scan/%7BRFID%7D?ID=ID	401	
GET			http://host.docker.internal:8000/user	401	
POST			http://host.docker.internal:8000/login	422	
POST			http://host.docker.internal:8000/signup	401	

Appendix: Instances for Alert 7

Alert Name	Alert Ref.	Risk Level	Confidence Level	Risk (Confidence) Levels	Vulnerability Description
7. Storable and Cacheable Content	10049	0	2	Informational (Medium)	
Instance: Method	Param	Attack	Instance: URI	Evidence	Other Info
GET			http://host.docker.internal:8000/openapi.json		In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
GET			http://host.docker.internal:8000/sqlinjection?item=item		In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

Appendix: Long URIs

Entry No: 1

http://host.docker.internal:8000/scan/%7BRFID%7D?ID=sxHYSxPPNHLOVGfePmFxrMHfQXXsBxHZHKIGtYDFhmJPShleGgbfGmXiYOvqDmtVqViLxWsuWYVNNOPQCkuxxZjEPkPEaDRXqutgQuoriiYnrGhfUobrhkqXOuwPMPoGS
TJCqPMNbOlVGTJCFQHOnyStgEFHjJEUOTyUTBRZeqHfhNMOxHFGVkRqgnUjdcxMddykOtfyslcrZyckCVMPeMHTdoXnMxidNsUDcpqCVIPTjRcOCppqmCXOKOTbedPkORDGjuKKgoQWZMGyFZjnqFQGIhrjRKcrNyqdQjmbrpruJll
HfRVCBGHLPXZkbHAvfWxcYTxbjYJNpaWkcbIjIydhFvMDNYARhVLYkUrANTkgfxvGiIAbakHnrcvxdXGdWyxnxojYYNiXALUcoxKPBeTsEKYaXVcFOdbJSYvVlQcEvNMbFmgPBQUYufMguZdhhheaqekITSTSlanLcZqFbePNeIpKDfVK
jgRIootkRWQJQeIbcZXkESuJeHPXMJPBhHNoPwMUPwZEVpqFAbaQjWJKjXGhKTDfWuCdBxjXQHyZalbxNGladVAODEDxfumFNDDdsvOMUxNXPFWjjfXiQnKPesKsiFsIoWwLlIMjEuDgGHHHMbWIwpaNjMUrepoynPFTMXQlJlQS
WvqqoKOlvqyICCHXrKQAOUACLPxVoERxLhoGofyHfOQDHxDfwHaowUmusLFxnWCgWjKBGrrIPFNmTdjWKpLyoetuwGhtlfkuksKUIRnyneqmVxSoxjuaqIfXpDocHtmCgESKVRIHHDosbJZCXrqKcZjTSePmTevBAOxYlsuXuJhdHIpa
wBdjRtQtOZXlQcHYUSYEHFpyRZQdHdmgJpiZJtIbuEdQnHjIIcryTodmGYHhnpwpIkXWsNLqjgapWtvgWlkXWbCTKlpCUDKEZFNUQdZnvNNQCxUqUsoDiNFNpXEZoKuoQxaxHqSCqMgXONeFZIylPtKcIvCBCyESktChZeptxKnFnwh
AUrEeRJmePrscvcoDnnwDtdjDGLAcjYioUNRdXNDHrQYoOAOtQuAsOePnbgnZtmhGgJcgtDTbrwFLLuYFiZBKxrvIGVkodiFDGOfWplrBgaVaSTQFeMCHaJYbrKHiNjEfmhsVvuidvZJPpdRvavYrYBcPWDtuyOGDkLoTKBWsXRdPhQB
RwPGnhtpmEGbfvoWLakbuHsJWGIuRYHVfdjSFaDsluaZydHEYnLCBllLUZtBPTtAnUPgRGpSKhrOjwXJLmxvcIOWGLmPhnqStfVPJFNBpVLxxVHudMRoNKnIKHJTxOIijDfcXYUuwGxfPDGaRDCMWictSiXxhGrIDMcZhOtiESMhTiriW
oOJREuvaeGXoGuvJxQFMayEFTDHlaIsUykGCdHKCWjLBbwZIcfXyXrYmNtuJLcVMnSXOuhxfPOyoJsATbJAFZXoOXtMHQPfaqHUjtjXOiTOWMcXpCneuCyGlmCJPpdJooNcgboGDNwmxZlUTLyxfpOMdunQOjnhxrgyIVMeNldOTqF
aluETCdZLhaviirbFCqnRrrkrStjpfCtXHMLlqKopEIcEVKfXiUwAbpLvQYZitkIMVxIkZdTUJmskfveSLcLHkUKXUYyOsIHoiWGapJoTTrsCooVtxuRPLHMDefyvHKbRagtSDhpBjLIfkjIimoNmKLyjiIFwQMUbIAimwkoOGeXMqYShjcmeUbtQe
VSnBxdfupOARKuJnYVshXPByidtyUKYgZjMxCDvfwAXBBMsAoIhyqfePfQPGSZNGhNJoqnNcuaASsumsSlUqEvHgcfIBZmqyoEoeOLIwTWFUfLXCAKIIbxYgXAaovjhfCvZYBEULeZOGColpRTAUrCsyVWBGxdrWeByBJOegaoCBjBC
oslJduWNjAySuSJEMNDxaaCerNRNJpGLMxpfqJBsRfpAidnwUJPndZMJgLrJnhmuBVhnYxWqnJLQHKVoXMfaeKMcQkXtJPbgXiYORhTbMAHLcbTnNYigaUUXCtXaYMQlnhYZNGpHKgetHBYjVlGcTtRXxpEgTuwlEWGhvWlrlMgZH
wuAYNUpofoSAknIfIAEVutTkAWDdouFlJQeA