ZAP by Checkmarx Scanning Report

Sites: https://s.gravatar.com https://localhost:7047 https://cdn.auth0.com https://household-manager-dev.eu.auth0.com https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://localhost:4200

Generated on Wed, 3 Dec 2025 22:43:48

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	7
Low	5
Informational	9

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
CSP: Failure to Define Directive with No Fallback	Medium	1
CSP: Wildcard Directive	Medium	3
CSP: script-src unsafe-eval	Medium	2
CSP: script-src unsafe-inline	Medium	3
CSP: style-src unsafe-inline	Medium	3
Cross-Domain Misconfiguration	Medium	6
Cookie with SameSite Attribute None	Low	10
Cookie without SameSite Attribute	Low	7
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1
Strict-Transport-Security Header Not Set	Low	44
Timestamp Disclosure - Unix	Low	3
Authentication Request Identified	Informational	1
Information Disclosure - Information in Browser sessionStorage	Informational	1
Information Disclosure - Suspicious Comments	Informational	7
Loosely Scoped Cookie	Informational	3
Modern Web Application	Informational	3

Re-examine Cache-control Directives	Informational	3
Retrieved from Cache	Informational	6
Session Management Response Identified	Informational	7
User Controllable HTML Element Attribute (Potential XSS)	Informational	1

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request t functionality using predictable URL/form actions in a repeatable way. The nature of the attack is site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privile is dramatically increased when the target site is vulnerable to XSS, because XSS can be used a
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	<form method="POST" class="cdbb334bd c1de237ad" data-form-primary="true" data-disable-h
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddleware _csrfToken] was found in the following HTML form: [Form 1: "password" "state" "username"].
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	<form method="post" data-provider="google" class="c24b23c67 cea6c6ee0 cfdfafa4e" data-form
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddleware _csrfToken] was found in the following HTML form: [Form 2: "connection" "state"].
Instances	2
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constru For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upo Note that this can be bypassed using XSS.

	Identify especially dangerous operations. When the user performs a dangerous operation, send Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This co
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Che https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/exc
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	frame-ancestors 'none'
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: Wildcard Directive
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer from data theft to site defacement or distribution of malware. CSP provides a set of standard HT covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	frame-ancestors 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove
URL	https://localhost:4200/
Method	GET

Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.c com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove
URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.c com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: script-src unsafe-eval**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://localhost:4200/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://cdn.auth0.com https://accounts.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts. googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs. cloudflare.com https://fonts.googleapis.com; img-src 'self' data: https:; font-src 'self' data: https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://accounts.google.com; frame-src 'self' https://*.auth0.com https://accounts.google.com; form-action 'self'; frame-ancestors 'self';
Other Info	script-src includes unsafe-eval.
URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL&state=WlBNQXRBQVZHNC5PdnFiY3RyRWp%2BRUE3RHIxZXpTSktpS184ZWdlU2FWcQ%3D%3D
Method	GET
Attack	
	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://cdn.auth0.com https://accounts.google.com; style-src

Evidence	'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; img-src 'self' data: https:; font-src 'self' data: https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://accounts.google.com; frame-src 'self' https://*.auth0.com https://accounts.google.com; form-action 'self'; frame-ancestors 'self';
Other Info	script-src includes unsafe-eval.
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer from data theft to site defacement or distribution of malware. CSP provides a set of standard HT covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	frame-ancestors 'none'
Other Info	script-src includes unsafe-inline.
URL	https://localhost:4200/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.c com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://
Other Info	script-src includes unsafe-inline.
URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.c com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://
Other Info	script-src includes unsafe-inline.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/

	https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: style-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer from data theft to site defacement or distribution of malware. CSP provides a set of standard HT covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	frame-ancestors 'none'
Other Info	style-src includes unsafe-inline.
URL	https://localhost:4200/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.c com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://
Other Info	style-src includes unsafe-inline.
URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.c com https://fonts.googleapis.com; style-src-elem 'self' 'unsafe-inline' https://cdn.jsdelivr.net https com https://fonts.gstatic.com; connect-src 'self' https://localhost:7047 https://*.auth0.com https://
Other Info	style-src includes unsafe-inline.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://cdn.jsdelivr.net/npm/primeicons@7.0.0/primeicons.css
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/css/all.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/fa-brands-400.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/fa-regular-400.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/fa-solid-900.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	6
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Low	**Cookie with SameSite Attribute None**
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie ca script inclusion, and timing attacks.
URL	https://household-manager-dev.eu.auth0.com/authorize/resume?state=-Z6hMuOXf-3cp7RTu-E
Method	GET
Attack	
Evidence	Set-Cookie: auth0
Other Info	
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3Dol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	GET
Attack	
Evidence	Set-Cookie: __cf_bm
Other Info	
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3Dol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	GET
Attack	
Evidence	Set-Cookie: auth0
Other Info	
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3Dol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	GET

Attack	
Evidence	Set-Cookie: did
Other Info	
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	
Evidence	Set-Cookie: __cf_bm
Other Info	
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	
Evidence	Set-Cookie: did
Other Info	
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	POST
Attack	
Evidence	Set-Cookie: __cf_bm
Other Info	
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	POST
Attack	
Evidence	Set-Cookie: did
Other Info	
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	POST
Attack	
Evidence	Set-Cookie: auth0
Other Info	
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	POST
Attack	
Evidence	Set-Cookie: did
Other Info	
Instances	10
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent inclusion, and timing attacks.
URL	https://household-manager-dev.eu.auth0.com/authorize/resume?state=-Z6hMuOXf-3cp7RTu-E
Method	GET
Attack	
Evidence	Set-Cookie: auth0_compat
Other Info	
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa 2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo 3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3D ol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	GET
Attack	
Evidence	Set-Cookie: auth0_compat
Other Info	
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa 2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo 3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3D ol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	GET
Attack	
Evidence	Set-Cookie: did_compat
Other Info	
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	
Evidence	Set-Cookie: did_compat
Other Info	
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	POST
Attack	
Evidence	Set-Cookie: did_compat
Other Info	
URL	https://household-manager-dev.eu.auth0.com/u/login? state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	POST
Attack	

Evidence	Set-Cookie: auth0_compat
Other Info	
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	POST
Attack	
Evidence	Set-Cookie: did_compat
Other Info	
Instances	7
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://cdn.auth0.com/ulp/react-components/1.167.0/css/main_wcag_compliant.cdn.min.css
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://localhost:4200/
Method	GET
Attack	
Evidence	
Other Info	

URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL&state=WlBNQXRBQVZHNC5PdnFiY3RyRWp%2BRUE3RHIxZXpTSktpS184ZWdlU2FWcQ%3D%3D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-2NXX5BKP.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-2YAKVAX7.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-36SWMQ43.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-5D37D4WT.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-5J7I2FSX.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-5ZWQ3G5T.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-63TWBEAA.js

Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-6OFTMVX3.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-D4UWGXTE.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-DDEYNCEU.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-EJPZGPHD.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-EOTRQMIW.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-EQDQRRRY.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-EZXEYWKO.js
Method	GET

Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-FRKX6X6L.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-ICEZ5I6T.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-IULR3N55.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-IYL72G7E.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-IZ3EFSN4.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-JAVVGEZK.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-JEMB5IYM.js
Method	GET
Attack	
Evidence	

Other Info	
URL	https://localhost:4200/chunk-JRDS5FVA.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-KAOVGVNL.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-MO3HL3BA.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-O6B6RT6D.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-ODZVSCRB.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-OYJ2YKV6.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-QK4QRAK4.js
Method	GET
Attack	
Evidence	
Other Info	

URL	https://localhost:4200/chunk-RGGDWMDT.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-RWFUFX63.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-TZRKD6GO.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-UC6CQNPC.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-UETVL4HX.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-UTH3N33H.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-UYVH4YCO.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-WSDJA326.js
Method	GET

Attack	
Evidence	
Other Info	
URL	https://localhost:4200/chunk-Z3ZMUM5H.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/main-5LZDPABA.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/polyfills-5CFQRCPP.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/scripts-TTWY4XDY.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/styles-GYOJ6G3O.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://s.gravatar.com/avatar/19f84906f4412abf6066aaa92fe9d6c1?s=480&r=pg&d=https%3A%2F%2Fcdn.auth0.com%2Favatars%2Fte.png
Method	GET
Attack	
Evidence	
Other Info	
Instances	44
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3Dol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY3D%3D
Method	GET
Attack	
Evidence	1764794516
Other Info	1764794516, which evaluates to: 2025-12-03 22:41:56.
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	
Evidence	1764794525
Other Info	1764794525, which evaluates to: 2025-12-03 22:42:05.
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	POST
Attack	
Evidence	1764794526
Other Info	1764794526, which evaluates to: 2025-12-03 22:42:06.
Instances	3
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregat
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Informational	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contai Detect" then this rule will change the authentication to match the request identified.
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	POST
Attack	
Evidence	password

Other Info	userParam=username userValue=test33@gmail.com passwordParam=password referer=https: state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	Information Disclosure - Information in Browser sessionStorage
Description	Information was stored in browser sessionStorage. This is not unusual or necessarily unsafe - this informational alert has been raised to help you get a better understanding of what this app is doing. For more details see the Client tabs - this information was set directly in the browser and will therefore not necessarily appear in this form in any HTTP(S) messages.
URL	https://localhost:4200/
Method	GET
Attack	
Evidence	
Other Info	The following data (key=value) was set: a0.spajs.txs. HAAmCfAQ0RmlG3zEHUPaY6NrvIbB85es={"nonce":" Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg==","code_verifier":"x6l4Qkqfq8D949EzOoTyiqON_e~GzcjgsRlqPjshblj","scope":"openid profile email offline_access","audience":"https://household-manager-api","redirect_uri":" https://localhost:4200/callback","state":" WlBNQXRBQVZHNC5PdnFiY3RyRWp+RUE3RHIxZXpTSktpS184ZWdlU2FWcQ==","appState":{"target":"/households","action":"login"},"response_type":"code"} Note that this alert will only be raised once for each URL + key.
Instances	1
Solution	This is an informational alert and no action is necessary.
Reference	
CWE Id	359
WASC Id	13
Plugin Id	120000

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://localhost:4200/chunk-63TWBEAA.js
Method	GET
Attack	
Evidence	Admin
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "//calendar.google.com","target","_blank"],[1,"alert","alert-info","mt-3","mb-0"],[1,"fas","fa-lightbulb","me-1"],["id","headingO", see evidence field for the suspicious comment/snippet.
URL	https://localhost:4200/chunk-D4UWGXTE.js
Method	GET
Attack	
Evidence	user

Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: " //householdmanager.com/email"]||e?.email))}login(e="/households"){this.auth0. loginWithRedirect({appState:{target:e,action:"login", see evidence field for the suspicious comment/snippet.
URL	https://localhost:4200/chunk-EJPZGPHD.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//g,"_")}; function G(o){return Pe(o)}var O=class extends Error{constructor(e){var t;super(e??" operation not supported"),this.nam", see evidence field for the suspicious comment/snippet.
URL	https://localhost:4200/chunk-IZ3EFSN4.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//www. w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' viewBox='0 0 17 17'><g>< /g><path d='M13.207 8.472l-7.854 7.854", see evidence field for the suspicious comment /snippet.
URL	https://localhost:4200/chunk-JAVVGEZK.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//").test(e)){let [,n]=e.split(/\/\/[^\/]+/);return n}return e}var HI=(()=>{class e extends Rn{_platformLocation; _baseHref="";_re", see evidence field for the suspicious comment/snippet.
URL	https://localhost:4200/chunk-OYJ2YKV6.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//i;function As(t,r){if(!l(Fi)||t.method==="GET"||t.method==="HEAD"||Ms.test(t.url))return r(t);let e=l(at). getToken(),n=l(Cs);r", see evidence field for the suspicious comment/snippet.
URL	https://localhost:4200/scripts-TTWY4XDY.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper. js.org/docs/v2/");let e=this._element;this._config.reference==="parent"?e=this._parent:ie (this._config.reference)?e=ae", see evidence field for the suspicious comment/snippet.
Instances	7
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	Loosely Scoped Cookie
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope.Th subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are tr parent, or any subdomain of the parent.
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa 2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo 3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3D ol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY 3D%3D
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: household-manager-dev.eu.auth0.com __cf_bm=H BxTwaIm0QmaiKHP2oKTVhYVi0mLLHcIN1Xx6Gka9
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	
Evidence	
Other Info	The origin domain used for comparison was: household-manager-dev.eu.auth0.com __cf_bm=9 aRrlIMQvmTcPsQ3jNRxUVO5uJc.EkZ4vX8v8waB0
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	POST
Attack	
Evidence	
Other Info	The origin domain used for comparison was: household-manager-dev.eu.auth0.com __cf_bm=a TfmV1djSWf9XokO9GuSURww_WTVw6OugFjji
Instances	3
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Reference	https://datatracker.ietf.org/doc/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Tes https://code.google.com/archive/p/browsersec/wikis/Part2.wiki
CWE Id	565
WASC Id	15
Plugin Id	90033

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZIcnNhbC1sb
Method	GET
Attack	
Evidence	<noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with J
URL	https://localhost:4200/
Method	GET
Attack	

Evidence	<script src="polyfills-5CFQRCPP.js" type="module"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL
Method	GET
Attack	
Evidence	<script src="polyfills-5CFQRCPP.js" type="module"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and pro that no sensitive content will be cached.
URL	https://household-manager-dev.eu.auth0.com/u/login?state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	no-store, max-age=0, no-transform
Other Info	
URL	https://localhost:4200/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://localhost:4200/callback?code=fWJVpA8OQ9GZiV24GjwlCmGCn1FubhLy-LAbVzUi1JjxL
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	Retrieved from Cache
Description	The content was retrieved from a shared cache. 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 caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdn.auth0.com/ulp/react-components/1.167.0/css/main_wcag_compliant.cdn.min.css
Method	GET
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://cdn.jsdelivr.net/npm/primeicons@7.0.0/primeicons.css
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/css/all.min.css
Method	GET
Attack	
Evidence	Age: 238117
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/fa-brands-400.woff2
Method	GET
Attack	
Evidence	Age: 495866
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/fa-regular-400.woff2
Method	GET
Attack	
Evidence	Age: 314634
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/fa-solid-900.woff2
Method	GET
Attack	
Evidence	Age: 327725
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	6

Solution	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, private Pragma: no-cache Expires: 0 This 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.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	525
WASC Id	
Plugin Id	10050

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other which has a Session Management Method set to "Auto-Detect" then this rule will change the ses
URL	https://household-manager-dev.eu.auth0.com/authorize/resume?state=-Z6hMuOXf-3cp7RTu-E
Method	GET
Attack	
Evidence	auth0
Other Info	cookie:auth0 cookie:auth0_compat
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa 2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo 3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3D ol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	GET
Attack	
Evidence	did
Other Info	cookie:did cookie:auth0 cookie:__cf_bm cookie:did_compat cookie:auth0_compat
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	OPTIONS
Attack	
Evidence	did
Other Info	cookie:did cookie:__cf_bm cookie:did_compat
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	POST
Attack	
Evidence	did
Other Info	cookie:did cookie:__cf_bm cookie:did_compat
	https://household-manager-dev.eu.auth0.com/u/login?

URL	state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	POST
Attack	
Evidence	did
Other Info	cookie:did cookie:auth0 cookie:did_compat cookie:auth0_compat
URL	https://household-manager-dev.eu.auth0.com/oauth/token
Method	GET
Attack	
Evidence	access_token
Other Info	json:access_token
URL	https://household-manager-dev.eu.auth0.com/authorize?client_id=HAAmCfAQ0RmlG3zEHUPa 2Fcallback&audience=https%3A%2F%2Fhousehold-manager-api&response_type=code&respo 3D&nonce=Qnp0blR6ZjRKQmV4WDNtbi5zbGw5YzlhSzNGNGxKS3MyclJ2WnJXaWF5cg%3D ol0iFxdZPB9zx3TUoVRZY8Uu5AbMM_7c&code_challenge_method=S256&auth0Client=eyJuY
Method	POST
Attack	
Evidence	auth0Client
Other Info	url:auth0Client
Instances	7
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify wh review by a security analyst to determine exploitability.
URL	https://household-manager-dev.eu.auth0.com/u/login? state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb
Method	GET
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb appears to include user input in: a(n) [input] tag [value] attribute The user input found was: state=hKFo2SBVRFB3LUpnaDJPRlhHVHotbm9icHF0Y0c2ajZfdGowa6Fur3VuaXZlcnNhbC1sb The user-controlled value was: hkfo2sbvrfb3lupnadjprlhhvhotbm9ichf0y0c2ajzfdgowa6fur3vuax
Instances	1
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031