ZAP Scanning Report Client Pages

performed on 2qa UAT

Sites: http://uat.sassieshop.com https://uat.sassieshop.com

Generated on Mon, 23 Jan 2023 10:03:23

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	4
Informational	5

Alerts

Name	Risk Level	Number of Instances
Cookie No HttpOnly Flag	Low	6
Cookie Without Secure Flag	Low	4
Cookie without SameSite Attribute	Low	6
X-Content-Type-Options Header Missing	Low	35
Content-Type Header Missing	Informational	1
Information Disclosure - Suspicious Comments	Informational	6
Modern Web Application	Informational	6
Re-examine Cache-control Directives	Informational	10
User Controllable HTML Element Attribute (Potential XSS)	Informational	10

Alert Detail

Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed accessible and can be transmitted to another site. If this is a session cookie then session hijacki
URL	https://uat.sassieshop.com/2_qa/index.norm.php
Method	GET
Attack	
Evidence	set-cookie: PHPSESSID
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php
Method	GET
Attack	
Evidence	set-cookie: testcookie

URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJITk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN2BvHzWWYcy
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZZ7YGzqBsZbUuwYqNErIlumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM2BQdXQk
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	
Instances	6
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed vi
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJITk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN2BvHzWWYcy
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZZ7YGzqBsZbUuwYqNErIlumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM2BQdXQk
Method	GET

Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	
Instances	4
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always b containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Tes
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://uat.sassieshop.com/2_qa/index.norm.php
Method	GET
Attack	
Evidence	set-cookie: PHPSESSID
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php
Method	GET
Attack	
Evidence	set-cookie: testcookie
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN 2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJlTk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN 2BvHzWWYcy
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZZ7YGzqBsZbUuwYqNErlIumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM 2BQdXQk
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST

Attack	
Evidence	
Instances	6
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows old body, potentially causing the response body to be interpreted and displayed as a content type o Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://uat.sassieshop.com/2_qa/custom/MSP/MSPlogo-big.gif
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/fetch/css/core.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/fetch/css/handheld.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/fetch/css/handheld.css?v=2
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/fetch/css/style.css?v=2
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/fetch/js/libs/dd_belatedpng.min.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/index.norm.php
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/sassiehelpers/common/css/CustomTheme.css.php?theme=bfe
Method	GET

Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/sassiehelpers/common/js/fixPretentiousPunctuation.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/sassiehelpers/common/js/gotoSite.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/sassiehelpers/common/js/shopperSignUp.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/sassiehelpers/common/js/shopperSignupProgressBar.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/sassiehelpers/common/tpl/en/shoppers/testcaster-style.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/ResetPassword.php
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJITk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN2BvHzWWYcy
Method	GET
Attack	
Evidence	
	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?

URL	EmsID=ZSMZZ7YGzqBsZbUuwYqNErIIumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM2BQdXQk
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/custom/2_qa/custom/MSP/MSPlogo-big.gif
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/favicon.ico
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/robots.txt
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/common/css/jquery-ui.datepicker.custom.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/common/css/sassieLoginHome.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/common/css/ShopperSignUp.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/common/css/ShopperSignUpProgressBar.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/common/sassielogo_text_lg.gif
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery-ui/jquery-ui.css
Method	GET
Attack	
Evidence	

URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery-ui/jquery-ui.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery-ui/jquery-ui.structure.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery-ui/jquery-ui.theme.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery-ui/jquery-ui.theme.ui-lightness.css
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/ResetPassword.php
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	
Instances	35
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it s If possible, ensure that the end user uses a standards-compliant and modern web browser that /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	Content-Type Header Missing
Description	The Content-Type header was either missing or empty.
URL	https://uat.sassieshop.com/favicon.ico
Method	GET
Attack	
Evidence	
Instances	1
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
CWE Id	345
WASC Id	12
Plugin Id	10019

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matc
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery-ui/jquery-ui.js
Method	GET
Attack	
Evidence	select
URL	https://uat.sassieshop.com/sassiehelpers/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	username
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	todo
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJITk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN2BvHzWWYcy
Method	GET
Attack	
Evidence	todo
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZZ7YGzqBsZbUuwYqNErIlumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM2BQdXQk
Method	GET
Attack	
Evidence	todo
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	

Evidence	todo
Instances	6
Solution	Remove all comments that return information that may help an attacker and fix any underlying p
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php
Method	GET
Attack	
Evidence	Go
URL	https://uat.sassieshop.com/2_qa/shoppers/ResetPassword.php
Method	GET
Attack	
Evidence	Send Reset Link
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	 NEXT
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJITk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN2BvHzWWYcy
Method	GET
Attack	
Evidence	 NEXT
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZZ7YGzqBsZbUuwYqNErIlumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM2BQdXQk
Method	GET
Attack	
Evidence	 NEXT
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	Go
Instances	6
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 intended, however, the resources should be reviewed to ensure that no sensitive content will be
URL	https://uat.sassieshop.com/2_qa/index.norm.php
Method	GET
Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php
Method	GET
Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/ResetPassword.php
Method	GET
Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZadfJxGCbYwXtlUT5X7woLDkwYWYwZDQ5Zjc2ZWUwYjE5ZGRmYmM0ODNkN2ByxSx70HQ8Zp
Method	GET
Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZSoPXWhbbSvqyJITk3M51XTE1ZGM0ZjQwMGQyYzNjMjc0Y2YzMjI5ZWJjMzcxN2BvHzWWYcy
Method	GET
Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php?EmsID=ZSMZZ7YGzqBsZbUuwYqNErIlumMxODI0ODU5NDBjZmIxMTk4MjhkMDJhOTZhNjllM2BQdXQk
Method	GET
Attack	
Evidence	private
URL	https://uat.sassieshop.com/robots.txt
Method	GET
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/ResetPassword.php
Method	POST

Attack	
Evidence	private
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	private
Instances	10
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

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 where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	

URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/LoginShopper.norm.php?mode=submit&relogin=0
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	
URL	https://uat.sassieshop.com/2_qa/shoppers/Signup.php
Method	POST
Attack	
Evidence	
Instances	10
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute
CWE Id	20
WASC Id	20
Plugin Id	10031