ZAP Scanning Report

Scan of staging.va.gov

Sites: https://brain.foresee.com https://static.idp.int.identitysandbox.gov https://idp.int.identitysandbox.gov https://sqa.eauth.va.gov https://staging-api.va.gov https://resource.digital.voice.va.gov https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://dap.digitalgov.gov https://staging.va.gov

Generated on Tue, 22 Mar 2022 11:26:37

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	7
Low	9
Informational	4

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	6
CSP: Wildcard Directive	Medium	9
CSP: script-src unsafe-inline	Medium	1
CSP: style-src unsafe-inline	Medium	14
Cross-Domain Misconfiguration	Medium	2
Missing Anti-clickjacking Header	Medium	2
Vulnerable JS Library	Medium	2
CSP: Notices	Low	3
Cookie No HttpOnly Flag	Low	54
Cookie Without Secure Flag	Low	46
Cookie with SameSite Attribute None	Low	31
Cookie without SameSite Attribute	Low	69
Cross-Domain JavaScript Source File Inclusion	Low	49
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	8
Timestamp Disclosure - Unix	Low	120
X-Content-Type-Options Header Missing	Low	34
Charset Mismatch (Header Versus Meta Charset)	Informational	2
Information Disclosure - Suspicious Comments	Informational	41
Loosely Scoped Cookie	Informational	41
Re-examine Cache-control Directives	Informational	20

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 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
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	<form method=POST action="https://sqa.pki.eauth.va.gov/pkmslogin.form?token=7c9892f8-a9e
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	<form method="post" action="https://staging-api.va.gov/v1/sessions/callback">
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	<form method="post" action="https://idp.int.identitysandbox.gov/api/saml/auth2022">
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	<form method="post" action="https://idp.int.identitysandbox.gov/api/saml/auth2022">
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	<form id="saml-form" action="https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login" accep
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	<form id="saml-form" action="https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login" accep
Instances	6
	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constru

Solution	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	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**CSP: Wildcard Directive**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d com; frame-src 'self' https://*.va.gov; frame-ancestors https://*.va.gov;
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d frame-src 'self' https://*.va.gov; frame-ancestors https://*.va.gov;
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d gstatic.com https://*.googletagmanager.com https://*.googleapis.com;
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d com https://*.googletagmanager.com https://*.googleapis.com;
	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.

URL	gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX 2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm46 2BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d https://*.va.gov;
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d https://*.va.gov;
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d https://*.va.gov;
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	block-all-mixed-content; default-src 'self' https://*.va.gov; script-src 'self' https://*.va.gov https://d https://*.va.gov;
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	frame-ancestors 'none'
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
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 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://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	

Evidence	frame-ancestors 'none'
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
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 Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attack from data theft to site defacement or distribution of malware. CSP provides a set of standard HT website owners to declare approved sources of content that browsers should be allowed to load types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java and video files.
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-550404eed2c86901d35ea3217ba https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
	https://idp.int.identitysandbox.gov/api/saml/auth2022? SAMLRequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpkcz0iaHR0cDovL3d3dy53My 0D%0AbWxkc2lnIyIgeG1sbnM6c2FtbD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmF 0AbiIgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpwcm90b2NvbCIgI 0AdGluYXRpb249Imh0dHBzOi8vaWRwLmludC5pZGVudGl0eXNhbmRib3guZ292L2FwaS9zYV 0AdGgyMDIyIiBGb3JjZUF1dGhuPSJmYWxzZSIgSUQ9IkZJTVJFUV9iMWZiYjgzZi0wMTdmLTF 0AOTNmNi04YjliNDUzNmRmYmYiIElzUGFzc2l2ZT0iZmFsc2UiIElzc3VlSW5zdGFudD0iMjAyM 0AMy0yMlQxNDoxNTozOFoiIFZlcnNpb249IjIuMCI%2BPHNhbWw6SXNzdWVyIEZvcm1hdD0ic 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0AYXV0aC52YS5nb3YvaXNhbS9zcHMvc2FtbDIwc3Avc2FtbDIwPC9zYW1sOklzc3VlcjxZHM6 0AbmF0dXJlIElkPSJ1dWlkYjFmYmI4NDEtMDE3Zi0xNDFlLTg4NGQtOGI5YjQ1MzZkZmJmIj48 0AU2lnbmVkSW5mbz48ZHM6Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBBbGdvcml0aG09Imh0dH 0Ad3cudzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyI%2BPC9kczpDYW5vbmljYWxpemF 0AaG9kPjxkczpTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZ 0ALzA0L3htbGRzaWctbW9yZSNyc2Etc2hhMjU2Ij48L2RzOlNpZ25hdHVyZU1ldGhvZD48ZHM6 0AZXJlbmNlIFVSST0iI0ZJTVJFUV9iMWZiYjgzZi0wMTdmLTFiNDgtOTNmNi04YjliNDUzNmRm 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AZy8yMDAwLzA5L3htbGRzaWcjZW52ZWxvcGVkLXNpZ25hdHVyZSI%2BPC9kczpUcmFuc2 0AOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMTAveG1sL 0AMTRuIyI%2BPHhjMTRuOkluY2x1c2l2ZU5hbWVzcGFjZXMgeG1sbnM6eGMxNG49Imh0dHA 0AdzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyIgUHJlZml4TGlzdD0ic2FtbHAgc2FtbCBk 0APC94YzE0bjpJbmNsdXNpdmVOYW1lc3BhY2VzPjwvZHM6VHJhbnNmb3JtPjwvZHM6VHJh 0Acz48ZHM6RGlnZXN0TWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwM 0AbWxlbmMjc2hhMjU2Ij48L2RzOkRpZ2VzdE1ldGhvZD48ZHM6RGlnZXN0VmFsdWU%2BTEq 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AUmVmZXJlbmNlPjwvZHM6U2lnbmVkSW5mbz48ZHM6U2lnbmF0dXJlVmFsdWU%2BUmNp 0AeEw5SEFlajluajQ1Q3RBeVUzYnQwWDhqOG1QMG1nbDlNS2pBYXBSaGVEVStSRHYzNn 0AUTIyUzlzMGV0RHlHNVVMWlkvV1JQTTNiUmtNVG5jTTZYa0dHMlFmRzJGVGhQeGtBMTd5 0AeXRSMUZNL3BRdE5HM0FYVWJiNFBlOWpEZmgwYTlsUXFYVG5ETXc0Z0s1SzVtT2JoRD

URL	0AcTBrb2tiNlEvZmlCMGs4VTdMdTVQeURqSktNblZ0L1dnbUo1MmY1R2NuRFZMbzQvcU5UU 0AUWpMY2dtWGxiMlA3ejE0WG9NK2tZS2w3SXZCamo1b2VDbjhNR01iYks3UGVaWGswVjM4 0ATWl4TnU3TXpsZHpPdCtiREUvZGdqOTYyWWxxcmpzRkZzZ2l4M1JKcUtDTXA3L2xMV1FX 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AVnhRVDNaanlaNXhPUk9xVXpoeFlZOEhiTFZIdHc2M2NYa0h2MHkxN1M2ZFN5QmVmM2tH 0AT25nS1BPcEdjMGRHNUN6bkREYWF4RTBKU0NSM1MwT016U1psMXV2eU45OFZXeEsyQ 0AT3duWmhaYm5qNDdQaDgyTFErM1B6UVJ3VVBUcGNmRkVESTdjZGJXeVcvV21VSVlLUG 0Aalp0MFRPREhFejlvOEQ1L1FOTHMyK1llM2k1dVVjbnZlYzdUY0krYVhHUWN5c1ZBVkExcD 0Ac1JucCsreWh5S0VnTy91cWRxM2RIb2ZHcC8rMTVhdTJKQnZHUVpPOU1sZ1U9PC9kczpT 0AcmVWYWx1ZT48ZHM6S2V5SW5mbz48ZHM6WDUwOURhdGE%2BPGRzOlg1MDlDZXJ0a 0D%0AeVRDQ0JyR2dBd0lCQWdJUURFQi9NckdESGkwTzcyME5lK1RBYnpBTkJna3Foa2lHC 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0AWURWUVFERXlCRWFXZHBRMlZ5ZENCVVRGTWdVbE5CSUZOSVFUSTFOaUF5TURJd0 0AeU1URXdNRGN3TURBd01EQmFGdzB5TWpFd01EY3lNelU1TlRsYU1ab3hDekFKQmdOVkJ 0ATVE0d0RBWURWUVFJRXdWVVpYaGhjekVTTUJBR0ExVUVCeE1KUVhKc2FXNW5kRzl1T 0AUVFLRXlOVkxsTXVJRVJsY0dGeWRHMWxiblFnYjJZZ1ZtVjBaWEpoYm5NZ1FXWm1ZV2x5 0AY0dBMVVFQXhNUVpHVjJMbVZoZFhSb0xuWmhMbWR2ZGpDQ0FpSXdEUVlKS29aSWh2 0ARGdnSVBBRENDQWdvQ2dnSUJBSzNUeG5OcVZYamZLN2VqcmprQXZ6cWoxbzdMNTdlV 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxb 0AVld3MVV2WS9QVGxDQlk3RzlTOVh1RXAzYTJQdGVKb2FGZTZKK3hQVWRpMUZtQTM1c 0AcU90RkZ2bVpNU1pYaHdpdmszQnpNMVdoMm16cDBDTXBwSzl5MkUvcjkyaHZMWlJVYStY 0AbTBJMGFEeDNaSERPT0E5bkc2WXVwNWZxNUt6Z28vdVFMK0QzN0JRQlRic2Q2NGNWa 0AZ1UrdS9yejczN0l4UU96aUpKRW9oMkZqYVE5Q2lVcEorVFRuQ21leXdUUDh6N1lmOG1RV 0AVExuR2Q2bVN6U2M3ZER1NmhEaUJRZlYzalkwWUhQTDAzUG1XMXJIbnlQMHZPWHZ5T 0AWWdCc2xLSWI2QXE1d0s1bTdlOHpHenJyakNBZXBNSmk3Q1AwK3VGTFhqWlJKa1V1ZkU 0AR2l1SVhlM0MvRnZKTmJsZkczSEc3WExKWTVBV1FGQjVzZnNBZGN5eFlENU1DS1kzTDd 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AY2Z2aFlkZVV6cWhPUmdsRndldTJtRG5LRDBBRUxaZkZHenR6c1pOQVB5VExPOHRkRSs 0AUHVUQnVaOXNKVERBNWMwQW1WMzZCdkZ6NXAwTEJWNVo1ZlRsWXVHWXlCZGdSS 0ARG5QaTVTdzJXcVhVMmcraUhBZ01CQUFHamdnTjBNSUlEY0RBZkJnTlZIU01FR0RBV2dC 0AcUtxRWpIbnF0Tm9QbUxMRmxYYTU5REFkQmdOVkhRNEVGZ1FVajFTZlc1YXVndFNrOTc 0AQ01VYWE4d0d3WURWUjBSQkJRd0VvSVFaR1YyTG1WaGRYUm9MblpoTG1kdmRqQU9C 0AOEVCQU1DQmFBd0hRWURWUjBsQkJZd0ZBWUlLd1lCQlFVSEF3RUdDQ3NHQVFVRkJ3 0AVkhSOEVnWWN3Z1lRd1FLQStvRHlHT21oMGRIQTZMeTlqY213ekxtUnBaMmxqWlhKMExt 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ASEE2THk5amNtdzBMbVJwWjJsalpYSjBMbU52YlM5RWFXZHBRMlZ5ZEZSTVUxSlRRVk5J 0ASXdNakJEUVRFdE5DNWpjbXd3UGdZRFZSMGdCRGN3TlRBekJnWm5nUXdCQWdJd0tUC 0ARkJRY0NBUlliYUhSMGNEb3ZMM2QzZHk1a2FXZHBZMlZ5ZEM1amIyMHZRMUJUTUg4R0 0AQndFQkJITXdjVEFrQmdnckJnRUZCUWN3QVlZWWFIUjBjRG92TDI5amMzQXVaR2xuYVd0 0AMjl0TUVrR0NDc0dBUVVGQnpBQ2hqMW9kSFJ3T2k4dlkyRmpaWEowY3k1a2FXZHBZMlZ5 0AMHZSR2xuYVVObGNuUlVURk5TVTBGVFNFRXlOVFl5TURJd1EwRXhMVEV1WTNKME1B 0AQi93UUNNQUF3Z2dGL0Jnb3JCZ0VFQWRaNUFnUUNCSUlCYndTQ0FXc0JhUUIzQUVhbF 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0AUFBQMkR6WGlPQVRDUUVXdGFvTkZMOE1FMmc3RWRaUnNsRWYydml5aldzTUFpRUF 0AcnpWaWFTUzB5RWJ4Zk1tQWp5T0ZXNUExWEFZWDRiUktzQWRnQlJvN0QxL1FGNW5GV 0Aa2Vzd2JKOHYzbm9oQ21nMysxSXNGNVFBQUFYeGRLRDBpQUFBRUF3QkhNRVVDSUFI 0AbG1ROVh6ZWYrYU82RXRTSlFhNTVQVWp5Qkc0a1QrMStBaUVBMGIzVG9YcWNnU01teE 0AWGd4WWVNTW4rSUh4dFlNLzE0TVRJNEFkZ0JCeU1xeDN5SkdTaERHb1RvSlFvZGVUak 0AdkhhUENRWXBZRzlnQUFBWHhkS0R6akFBQUVBd0JITUVVQ0lEQkpwY2ttSHhiOGpZaldu 0Aa0IvVGcyOHZubTg3Uno1WitWOUNPQWlFQWdQNyt1NXhpTTNrTzB0cjYrUlBOd2lrZEpmR 0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUDM3Vr 0AT1ViN2p3YUxOY1oyWHJ3NVRaWUdlWVAwV1c5aXhvSkRvdkdDcW5pOWoyMFhCemh5RI 0AKy9Pa0pqdVpTMFhIamJQQ3VWVHZQaTdORGhkU285WkpwZVdrblVUTDYwb3FYdkFsbGx 0ARWZKcU9aV3RHRUhxZXdWdTlvbU56Tkw0L2JQSWF0NStpNHdqQklSSk5POGhIOCtBWnI 0AbmtrU3NtNkUzeHFEVVlpR1dlc3ZTS2Fkc1ZxZGNxeDQ4Y2JxT0FGU2k4UDE1NWZGQXFN 0AWkJhUWV1VlBRcGZUNVc2R2FhV3VTWmZyeHNDeFlzbEFCdzYwbGJkbUJCbzZweVREUk 0ASFkwLzZtMDFHYnJ2WStuSCtpSWVKRGV0Sk9DTmRoMUJ2R3F6az08L2RzOlg1MDlDZXJ 0AZT48L2RzOlg1MDlEYXRhPjwvZHM6S2V5SW5mbz48L2RzOlNpZ25hdHVyZT48c2FtbHA6T 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM 0ATDoxLjE6bmFtZWlkLWZvcm1hdDplbWFpbEFkZHJlc3MiPjwvc2FtbHA6TmFtZUlEUG9saWN 0AYW1scDpSZXF1ZXN0ZWRBdXRobkNvbnRleHQgQ29tcGFyaXNvbj0ibWluaW11bSI%2BPH 0AaG5Db250ZXh0Q2xhc3NSZWY%2BaHR0cDovL2lkbWFuYWdlbWVudC5nb3YvbnMvYXNzd 0AbC8xPC9zYW1sOkF1dGhuQ29udGV4dENsYXNzUmVmPjxzYW1sOkF1dGhuQ29udGV4dE 0APmh0dHA6Ly9pZG1hbmFnZW1lbnQuZ292L25zL2Fzc3VyYW5jZS9hYWwvMjwvc2FtbDpBd 0AbnRleHRDbGFzc1JlZj48L3NhbWxwOlJlcXVlc3RlZEF1dGhuQ29udGV4dD48L3NhbWxwOkF 0AUmVxdWVzdD4%3D&RelayState=uuidecfd2e99-27cb-4b11-a466-8d9d064fbac1
Method	GET

Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self' https://sqa.eauth.va.gov; connect-src 'self' *.nr-data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: htt identitysandbox.gov; img-src 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscan https://s3.us-west-2.amazonaws.com; media-src 'self'; object-src 'none'; script-src 'self' js-agent. dap.digitalgov.gov *.google-analytics.com https://static.idp.int.identitysandbox.gov 'nonce-8d708c630e2929381e7f6b5e3807a2a8'; style-src 'self' https://static.idp.int.identitysandbox.gov 'self'
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-8d708c630e2929381e7f6b5e3807 https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-8d708c630e2929381e7f6b5e3807 https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'nonce-dotQsB9qLzvJcxrUJrjetg4157VqzYde' http://www.google-a uservoice.com https://dap.digitalgov.gov https://designsystem.digital.gov https://maps.googleapi usa.gov https://www.google-analytics.com https://www.googletagmanager.com https://tagmanag eval' https://optimize.google.com https://gateway.foresee.com https://resource.digital.voice.va.g kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov https://www.youtube.com https://*.ytimg.com https://cdn.botframework.com 'strict-dynamic'; style https://fonts.googleapis.com https://tagmanager.google.com https://optimize.google.com https:// https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s amazonaws.com https://s3-us-gov-west-1.amazonaws.com; frame-ancestors 'none'; manifest-sr frame-src https://dap.digitalgov.gov https://resource.digital.voice.va.gov https://www.googletagm https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://www.youtube.com; obje src 'self' blob:; img-src 'self' data: blob: https://*.gstatic.com https://api.mapbox.com https://www. https://www.googletagmanager.com https://*.va.gov https://optimize.google.com https://gateway foresee.com https://udc-neb.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amaz gov-west-1.amazonaws.com https://ok6static.oktacdn.com https://dvp-oauth-application-director amazonaws.com https://i.ytimg.com; connect-src 'self' http://localhost:4000 https://*.va.gov https https://events.mapbox.com https://www.google-analytics.com https://stats.g.doubleclick.net http https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://staging-va-gov-mainten west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://analytics.foresee.com https://survey.foreseeresults.com https://device.4seeresults.com https://health.foresee.com http https://resource.digital.voice.va.gov https://raw.githubusercontent.com wss://northamerica.direct https://northamerica.directline.botframework.com https://search.usa.gov https://udc-neb.kampyl uservoice.com https://www.googletagmanager.com https://www.youtube.com https://optimize.g digital.voice.va.gov https://nebula-cdn.kampyle.com blob:; media-src 'none'; font-src 'self' data: https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s amazonaws.com https://s3-us-gov-west-1.amazonaws.com; block-all-mixed-content ; form-actic va.gov https://vaww.vicbdc.ppd.vba.va.gov https://resource.digital.voice.va.gov; base-uri http://* va.gov https://optimize.google.com; report-uri /csp-report
URL	https://staging.va.gov/?next=loginModal&postLogin=true

Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'nonce-jQKemYml2FZIgeFLluTuoA8HhFBXe9aS' http://www.goog uservoice.com https://dap.digitalgov.gov https://designsystem.digital.gov https://maps.googleapi usa.gov https://www.google-analytics.com https://www.googletagmanager.com https://tagmanag eval' https://optimize.google.com https://gateway.foresee.com https://resource.digital.voice.va.g kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov https://www.youtube.com https://*.ytimg.com https://cdn.botframework.com 'strict-dynamic'; style https://fonts.googleapis.com https://tagmanager.google.com https://optimize.google.com https:// https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s amazonaws.com https://s3-us-gov-west-1.amazonaws.com; frame-ancestors 'none'; manifest-sr frame-src https://dap.digitalgov.gov https://resource.digital.voice.va.gov https://www.googletagm https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://www.youtube.com; obje src 'self' blob:; img-src 'self' data: blob: https://*.gstatic.com https://api.mapbox.com https://www. https://www.googletagmanager.com https://*.va.gov https://optimize.google.com https://gateway foresee.com https://udc-neb.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amaz gov-west-1.amazonaws.com https://ok6static.oktacdn.com https://dvp-oauth-application-director amazonaws.com https://i.ytimg.com; connect-src 'self' http://localhost:4000 https://*.va.gov https https://events.mapbox.com https://www.google-analytics.com https://stats.g.doubleclick.net http https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://staging-va-gov-mainten west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://analytics.foresee.com https://survey.foreseeresults.com https://device.4seeresults.com https://health.foresee.com http https://resource.digital.voice.va.gov https://raw.githubusercontent.com wss://northamerica.direct https://northamerica.directline.botframework.com https://search.usa.gov https://udc-neb.kampyl uservoice.com https://www.googletagmanager.com https://www.youtube.com https://optimize.g digital.voice.va.gov https://nebula-cdn.kampyle.com blob:; media-src 'none'; font-src 'self' data: https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s amazonaws.com https://s3-us-gov-west-1.amazonaws.com; block-all-mixed-content ; form-actic va.gov https://vaww.vicbdc.ppd.vba.va.gov https://resource.digital.voice.va.gov; base-uri http://* va.gov https://optimize.google.com; report-uri /csp-report
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'nonce-UrIdh9jDufBooyYfV5lePcFEhYYQQNhH' http://www.google uservoice.com https://dap.digitalgov.gov https://designsystem.digital.gov https://maps.googleapi usa.gov https://www.google-analytics.com https://www.googletagmanager.com https://tagmanag eval' https://optimize.google.com https://gateway.foresee.com https://resource.digital.voice.va.g kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov https://www.youtube.com https://*.ytimg.com https://cdn.botframework.com 'strict-dynamic'; style https://fonts.googleapis.com https://tagmanager.google.com https://optimize.google.com https:// https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s amazonaws.com https://s3-us-gov-west-1.amazonaws.com; frame-ancestors 'none'; manifest-sr frame-src https://dap.digitalgov.gov https://resource.digital.voice.va.gov https://www.googletagm https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://www.youtube.com; obje src 'self' blob:; img-src 'self' data: blob: https://*.gstatic.com https://api.mapbox.com https://www. https://www.googletagmanager.com https://*.va.gov https://optimize.google.com https://gateway foresee.com https://udc-neb.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amaz gov-west-1.amazonaws.com https://ok6static.oktacdn.com https://dvp-oauth-application-director amazonaws.com https://i.ytimg.com; connect-src 'self' http://localhost:4000 https://*.va.gov https https://events.mapbox.com https://www.google-analytics.com https://stats.g.doubleclick.net http https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://staging-va-gov-mainten west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://analytics.foresee.com https://survey.foreseeresults.com https://device.4seeresults.com https://health.foresee.com http https://resource.digital.voice.va.gov https://raw.githubusercontent.com wss://northamerica.direct https://northamerica.directline.botframework.com https://search.usa.gov https://udc-neb.kampyl uservoice.com https://www.googletagmanager.com https://www.youtube.com https://optimize.g digital.voice.va.gov https://nebula-cdn.kampyle.com blob:; media-src 'none'; font-src 'self' data: https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s amazonaws.com https://s3-us-gov-west-1.amazonaws.com; block-all-mixed-content ; form-actic va.gov https://vaww.vicbdc.ppd.vba.va.gov https://resource.digital.voice.va.gov; base-uri http://* va.gov https://optimize.google.com; report-uri /csp-report
URL	https://idp.int.identitysandbox.gov/
Method	POST

Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-550404eed2c86901d35ea3217ba https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-49ff00fa00163b0f690ee13a5547e https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-8a38082d38656eac12c9fc4950a9 https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self' https://sqa.eauth.va.gov; connect-src 'self' *.nr-data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: htt identitysandbox.gov; img-src 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscar https://s3.us-west-2.amazonaws.com; media-src 'self'; object-src 'none'; script-src 'self' js-agent. dap.digitalgov.gov *.google-analytics.com https://static.idp.int.identitysandbox.gov 'nonce-8d708c630e2929381e7f6b5e3807a2a8'; style-src 'self' https://static.idp.int.identitysandbox.gov 'self'
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-550404eed2c86901d35ea3217ba https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	frame-ancestors 'self'; default-src 'self'; child-src 'self'; form-action 'self'; block-all-mixed-content; data.net *.google-analytics.com us.acas.acuant.net; font-src 'self' data: https://static.idp.int.ident 'self' data: login.gov https://static.idp.int.identitysandbox.gov idscangoweb.acuant.com https://s3 com; media-src 'self'; object-src 'none'; script-src 'self' js-agent.newrelic.com *.nr-data.net dap.d analytics.com https://static.idp.int.identitysandbox.gov 'nonce-8d708c630e2929381e7f6b5e3807 https://static.idp.int.identitysandbox.gov 'unsafe-inline'; base-uri 'self'

URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	frame-ancestors 'none'
Instances	14
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
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://resource.digital.voice.va.gov/wdcvoice/5/onsite/embed.js
Method	GET
Attack	
Evidence	access-control-allow-origin: *
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	access-control-allow-origin: *
Instances	2
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?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https%3A%2F%2Fssoe-sp-staging.va.gov&cspKey=logingov3&appName=VA+gov+%28vagov%29&cspName=LOGIN.GOV&cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/ial/1&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/aal/2&AuthnContextComparison=minimum&ForceAuthn=false

Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https%3A%2F%2Fssoe-sp-staging.va.gov&cspKey=logingov3&appName=VA+gov+%28vagov%29&cspName=LOGIN.GOV&cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/ial/2&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/aal/2
Method	GET
Attack	
Evidence	
Instances	2
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 1.11.0 is vulnerable.
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	jquery-1.11.0.min.js
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	/*! jQuery UI - v1.10.4
Instances	2
Solution	Please upgrade to the latest version of jquery.
Reference	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

Low	CSP: Notices
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://staging.va.gov/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'nonce-dotQsB9qLzvJcxrUJrjetg4157VqzYde' http://www.google-analytics.com https://*.uservoice.com https://dap.digitalgov.gov https://designsystem.digital.gov https://maps.googleapis.com https://standards.usa.gov https://www.google-analytics.com https://www.googletagmanager.com https://tagmanager.google.com 'unsafe-eval' https://optimize.google.com https://gateway.foresee.com https://resource.digital.voice.va.gov https://nebula-cdn.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://www.youtube.com https://*.ytimg.com https://cdn.botframework.com 'strict-dynamic'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://tagmanager.google.com https://optimize.google.com https://fonts.googleapis.com https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com; frame-ancestors 'none'; manifest-src 'none'; default-src 'self'; frame-src https://dap.digitalgov.gov https://resource.digital.voice.va.gov https://www.googletagmanager.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://www.youtube.com; object-src 'self' blob:; worker-src 'self' blob:; img-src 'self' data: blob: https://*.gstatic.com https://api.mapbox.com https://www.google-analytics.com https://www.googletagmanager.com https://*.va.gov https://optimize.google.com https://gateway.foresee.com https://static.foresee.com https://udc-neb.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://ok6static.oktacdn.com https://dvp-oauth-application-directory-logos.s3-us-gov-west-1.amazonaws.com https://i.ytimg.com; connect-src 'self' http://localhost:4000 https://*.va.gov https://api.mapbox.com https://events.mapbox.com https://www.google-analytics.com https://stats.g.doubleclick.net http://*.vetsgov-internal https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://staging-va-gov-maintenance-windows.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://analytics.foresee.com https://brain.foresee.com https://survey.foreseeresults.com https://device.4seeresults.com https://health.foresee.com https://gateway.foresee.com https://resource.digital.voice.va.gov https://raw.githubusercontent.com wss://northamerica.directline.botframework.com https://northamerica.directline.botframework.com https://search.usa.gov https://udc-neb.kampyle.com; child-src https://*.uservoice.com https://www.googletagmanager.com https://www.youtube.com https://optimize.google.com https://resource.digital.voice.va.gov https://nebula-cdn.kampyle.com blob:; media-src 'none'; font-src 'self' data: https://fonts.gstatic.com https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com; block-all-mixed-content ; form-action 'self' https://vicbdc.vba.va.gov https://vaww.vicbdc.ppd.vba.va.gov https://resource.digital.voice.va.gov; base-uri http://*.vetsgov-internal https://*.va.gov https://optimize.google.com; report-uri /csp-report
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
	script-src 'self' 'unsafe-inline' 'nonce-jQKemYml2FZIgeFLluTuoA8HhFBXe9aS' http://www.google-analytics.com https://*.uservoice.com https://dap.digitalgov.gov https://designsystem.digital.gov https://maps.googleapis.com https://standards.usa.gov https://www.google-analytics.com https://www.googletagmanager.com https://tagmanager.google.com 'unsafe-eval' https://optimize.google.com https://gateway.foresee.com https://resource.digital.voice.va.gov https://nebula-cdn.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://www.youtube.com https://*.ytimg.com https://cdn.botframework.com 'strict-dynamic'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://tagmanager.google.com https://optimize.google.com https://fonts.googleapis.com https://gateway.foresee.com https://medallia.s3.

Evidence	amazonaws.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com; frame-ancestors 'none'; manifest-src 'none'; default-src 'self'; frame-src https://dap.digitalgov.gov https://resource.digital.voice.va.gov https://www.googletagmanager.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://www.youtube.com; object-src 'self' blob:; worker-src 'self' blob:; img-src 'self' data: blob: https://*.gstatic.com https://api.mapbox.com https://www.google-analytics.com https://www.googletagmanager.com https://*.va.gov https://optimize.google.com https://gateway.foresee.com https://static.foresee.com https://udc-neb.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://ok6static.oktacdn.com https://dvp-oauth-application-directory-logos.s3-us-gov-west-1.amazonaws.com https://i.ytimg.com; connect-src 'self' http://localhost:4000 https://*.va.gov https://api.mapbox.com https://events.mapbox.com https://www.google-analytics.com https://stats.g.doubleclick.net http://*.vetsgov-internal https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://staging-va-gov-maintenance-windows.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://analytics.foresee.com https://brain.foresee.com https://survey.foreseeresults.com https://device.4seeresults.com https://health.foresee.com https://gateway.foresee.com https://resource.digital.voice.va.gov https://raw.githubusercontent.com wss://northamerica.directline.botframework.com https://northamerica.directline.botframework.com https://search.usa.gov https://udc-neb.kampyle.com; child-src https://*.uservoice.com https://www.googletagmanager.com https://www.youtube.com https://optimize.google.com https://resource.digital.voice.va.gov https://nebula-cdn.kampyle.com blob:; media-src 'none'; font-src 'self' data: https://fonts.gstatic.com https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com; block-all-mixed-content ; form-action 'self' https://vicbdc.vba.va.gov https://vaww.vicbdc.ppd.vba.va.gov https://resource.digital.voice.va.gov; base-uri http://*.vetsgov-internal https://*.va.gov https://optimize.google.com; report-uri /csp-report
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'nonce-UrIdh9jDufBooyYfV5lePcFEhYYQQNhH' http://www.google-analytics.com https://*.uservoice.com https://dap.digitalgov.gov https://designsystem.digital.gov https://maps.googleapis.com https://standards.usa.gov https://www.google-analytics.com https://www.googletagmanager.com https://tagmanager.google.com 'unsafe-eval' https://optimize.google.com https://gateway.foresee.com https://resource.digital.voice.va.gov https://nebula-cdn.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://www.youtube.com https://*.ytimg.com https://cdn.botframework.com 'strict-dynamic'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com https://tagmanager.google.com https://optimize.google.com https://fonts.googleapis.com https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com; frame-ancestors 'none'; manifest-src 'none'; default-src 'self'; frame-src https://dap.digitalgov.gov https://resource.digital.voice.va.gov https://www.googletagmanager.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://www.youtube.com; object-src 'self' blob:; worker-src 'self' blob:; img-src 'self' data: blob: https://*.gstatic.com https://api.mapbox.com https://www.google-analytics.com https://www.googletagmanager.com https://*.va.gov https://optimize.google.com https://gateway.foresee.com https://static.foresee.com https://udc-neb.kampyle.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://ok6static.oktacdn.com https://dvp-oauth-application-directory-logos.s3-us-gov-west-1.amazonaws.com https://i.ytimg.com; connect-src 'self' http://localhost:4000 https://*.va.gov https://api.mapbox.com https://events.mapbox.com https://www.google-analytics.com https://stats.g.doubleclick.net http://*.vetsgov-internal https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com https://staging-va-gov-maintenance-windows.s3-us-gov-west-1.amazonaws.com https://s3-us-gov-west-1.amazonaws.com https://analytics.foresee.com https://brain.foresee.com https://survey.foreseeresults.com https://device.4seeresults.com https://health.foresee.com https://gateway.foresee.com https://resource.digital.voice.va.gov https://raw.githubusercontent.com wss://northamerica.directline.botframework.com https://northamerica.directline.botframework.com https://search.usa.gov https://udc-neb.kampyle.com; child-src https://*.uservoice.com https://www.googletagmanager.com https://www.youtube.com https://optimize.google.com https://resource.digital.voice.va.gov https://nebula-cdn.kampyle.com blob:; media-src 'none'; font-src 'self' data: https://fonts.gstatic.com https://gateway.foresee.com https://medallia.s3.amazonaws.com https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com

	https://s3-us-gov-west-1.amazonaws.com; block-all-mixed-content ; form-action 'self' https://vicbdc.vba.va.gov https://vaww.vicbdc.ppd.vba.va.gov https://resource.digital.voice.va.gov; base-uri http://*.vetsgov-internal https://*.va.gov https://optimize.google.com; report-uri /csp-report
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022?SAMLRequest=PHNhbWxwOkF1dGhuUr 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxI 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0D%0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUD 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022?SAMLRequest=PHNhbWxwOkF1dGhuUr 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxI 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0D%0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUD 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM

Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/embed.js
Method	GET
Attack	
Evidence	set-cookie: SERVERID
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01a80adf
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET

Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET

Attack	
Evidence	Set-Cookie: TS01c2ba4c
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://staging-api.va.gov/v0/user
Method	GET
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	

Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	Set-Cookie: TS014670a6
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	Set-Cookie: TS016f4012
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	Set-Cookie: TS016f4012
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	OPTIONS
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v0/user
Method	OPTIONS
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://idp.int.identitysandbox.gov/
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/
Method	POST
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB

URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	Set-Cookie: AWSALBCORS
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	Set-Cookie: TS01a556e5
URL	https://staging-api.va.gov/v1/sessions/callback

Method	POST
Attack	
Evidence	Set-Cookie: TS01de8f7b
Instances	54
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://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022?SAMLRequest=PHNhbWxwOkF1dGhuUr 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxI 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0D%0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUD 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/embed.js
Method	GET
Attack	
Evidence	set-cookie: SERVERID
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	

Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01a80adf
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679

URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01c2ba4c
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679

URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://staging-api.va.gov/v0/user
Method	GET
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	Set-Cookie: TS014670a6
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	Set-Cookie: TS016f4012
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	Set-Cookie: TS016f4012
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	OPTIONS
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v0/user

Method	OPTIONS
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://idp.int.identitysandbox.gov/
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	Set-Cookie: TS01a556e5
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST

Attack	
Evidence	Set-Cookie: TS01de8f7b
Instances	46
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always b
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 with SameSite Attribute None**
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie ca
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022?SAMLRequest=PHNhbWxwOkF1dGhuUr 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxI 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0D%0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUD 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM
Method	GET
Attack	
Evidence	
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	

URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva_widget.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap-formhelpers.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrapValidator.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/gov/va/accessva/common.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/isam-oauth/saml.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js

Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/scripts/login.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	
URL	https://idp.int.identitysandbox.gov/
Method	POST
Attack	
Evidence	

URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	
Instances	31
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	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022?SAMLRequest=PHNhbWxwOkF1dGhuUr 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxI 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0D%0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUD 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM
Method	GET

Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/embed.js
Method	GET
Attack	
Evidence	set-cookie: SERVERID
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01a80adf
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	

Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva.css
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva_widget.css
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap-formhelpers.min.css
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap.min.css
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrapValidator.min.css
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/js/gov/va/accessva/common.js
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer

URL	https://sqa.eauth.va.gov/accessva/resources/js/isam-oauth/saml.js
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	

Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	Set-Cookie: TS01c2ba4c
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	

Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/scripts/login.js
Method	GET
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://staging-api.va.gov/v0/user
Method	GET
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	Set-Cookie: TS014670a6
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	Set-Cookie: TS016f4012

URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	Set-Cookie: TS016f4012
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	OPTIONS
Attack	
Evidence	Set-Cookie: TS013da938
URL	https://staging-api.va.gov/v0/user
Method	OPTIONS
Attack	
Evidence	Set-Cookie: TS01de8f7b
URL	https://idp.int.identitysandbox.gov/
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	Set-Cookie: AWSALB
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login

Method	POST
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: __Secure-BIGipServer
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01a7b184
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	Set-Cookie: TS01b45679
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	Set-Cookie: TS01a556e5
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	Set-Cookie: TS01de8f7b
Instances	69
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	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET

Attack	
Evidence	<script src="https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=GSA&amp async" id="_fed_an_ua_tag"> //<![CDATA[//]]> </script>
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/assets/es5-shim.min-08adc386ca6471303e97607bac7d044722912858eb4b42af460a8583449fe021.js"></script>
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/assets/html5shiv-3481001ecf33e49ca9e98b5dbd99334cffcd0b1d9c27b554463e70735e9a17e3.js"></script>
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/assets/respond.min-aa35dd790d2b157f3ef06473825ac6c7a637739b7a8f2ab2ea6a365b439462cc.js"></script>
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/29-ed45901c.js"></script>
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.en.js"></scri
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.js"></script>
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.en.js"><
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.js"></sc
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/polyfill-9c10ccd9.js" nomodule="no
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7

Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/session-expire-session-0704b440.
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022? SAMLRequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpkcz0iaHR0cDovL3d3dy53My 0D%0AbWxkc2lnIyIgeG1sbnM6c2FtbD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmF 0AbiIgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpwcm90b2NvbCIgI 0AdGluYXRpb249Imh0dHBzOi8vaWRwLmludC5pZGVudGl0eXNhbmRib3guZ292L2FwaS9zYV 0AdGgyMDIyIiBGb3JjZUF1dGhuPSJmYWxzZSIgSUQ9IkZJTVJFUV9iMWZiYjgzZi0wMTdmLTF 0AOTNmNi04YjliNDUzNmRmYmYiIElzUGFzc2l2ZT0iZmFsc2UiIElzc3VlSW5zdGFudD0iMjAyM 0AMy0yMlQxNDoxNTozOFoiIFZlcnNpb249IjIuMCI%2BPHNhbWw6SXNzdWVyIEZvcm1hdD0id 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0AYXV0aC52YS5nb3YvaXNhbS9zcHMvc2FtbDIwc3Avc2FtbDIwPC9zYW1sOklzc3Vlcj48ZHM6 0AbmF0dXJlIElkPSJ1dWlkYjFmYmI4NDEtMDE3Zi0xNDFlLTg4NGQtOGI5YjQ1MzZkZmJmIj48 0AU2lnbmVkSW5mbz48Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBBbGdvcml0aG09Imh0dH 0Ad3cudzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyI%2BPC9kczpDYW5vbmljYWxpemF 0AaG9kPjxkczpTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZ 0ALzA0L3htbGRzaWctbW9yZSNyc2Etc2hhMjU2Ij48L2RzOlNpZ25hdHVyZU1ldGhvZD48ZHM6 0AZXJlbmNlIFVSST0iI0ZJTVJFUV9iMWZiYjgzZi0wMTdmLTFiNDgtOTNmNi04YjliNDUzNmRm 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AZy8yMDAwLzA5L3htbGRzaWcjZW52ZWxvcGVkLXNpZ25hdHVyZSI%2BPC9kczpUcmFuc2 0AOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMTAveG1sL 0AMTRuIyI%2BPHhjMTRuOkluY2x1c2l2ZU5hbWVzcGFjZXMgeG1sbnM6eGMxNG49Imh0dHA 0AdzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyIgUHJlZml4TGlzdD0ic2FtbHAgc2FtbCBk 0APC94YzE0bjpJbmNsdXNpdmVOYW1lc3BhY2VzPjwvZHM6VHJhbnNmb3JtPjwvZHM6VHJh 0Acz48ZHM6RGlnZXN0TWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwM 0AbWxlbmMjc2hhMjU2Ij48L2RzOkRpZ2VzdE1ldGhvZD48ZHM6RGlnZXN0VmFsdWU%2BTEq 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AUmVmZXJlbmNlPjwvZHM6U2lnbmVkSW5mbz48ZHM6U2lnbmF0dXJlVmFsdWU%2BUmNp 0AeEw5SEFlajluajQ1Q3RBeVUzYnQwWDhqOG1QMG1nbDlNS2pBYXBSaGVEVStSRHYzNn 0AUTIyUzIzMGV0RHlHNVVMWlkvV1JQTTNiUmtNVG5jTTZYa0dHMlFmRzJGVGhQeGtBMTd5 0AeXRSMUZNL3BRdE5HM0FYVWJiNFBlOWpEZmgwYTlsUXFYVG5ETXc0Z0s1SzVtT2JoRD 0AcTBrb2tiNlEvZmlCMGs4VTdMdTVQeURqSktNblZ0L1dnbUo1MmY1R2NuRFZMbzQvcU5UU 0AUWpMY2dtWGxiMlA3ejE0WG9NK2tZS2w3SXZCamo1b2VDbjhNR01iYks3UGVaWGswVjM4 0ATWl4TnU3TXpsZHpPdCtiREUvZGdqOTYyWWxxcmpzRkZzZ2l4M1JKcUtDTXA3L2xMV1FX 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AVnhRVDNaanlaNXhPUk9xVXpoeFlZOEhiTFZIdHc2M2NYa0h2MHkxN1M2ZFN5QmVmM2tH 0AT25nS1BPcEdjMGRHNUN6bkREYWF4RTBKU0NSM1MwT016U1psMXV2eU45OFZXeEsyC 0AT3duWmhaYm5qNDdQaDgyTFErM1B6UVJ3VVBUcGNmRkVESTdjZGJXeVcvV21VSVlLUG 0Aalp0MFRPREhFejlvOEQ1L1FOTHMyK1llM2k1dVVjbnZlYzdUY0krYVhHUWN5c1ZBVkExcD 0Ac1JucCsreWh5S0VnTy91cWRxM2RIb2ZHcC8rMTVhdTJKQnZHUVpPOU1sZ1U9PC9kczpT 0AcmVWYWx1ZT48ZHM6S2V5SW5mbz48ZHM6WDUwOURhdGE%2BPGRzOlg1MDlDZXJ0a 0D%0AeVRDQ0JyR2dBd0lCQWdJUURFQi9NckdESGkwTzcyME5lK1RBYnpBTkJna3Foa2lHC 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0AWURWUVFERXlCRWFXZHBRMlZ5ZENCVVRGTWdVbE5CSUZOSVFUSTFOaUF5TURJd0 0AeU1URXdNRGN3TURBd01EQmFGdzB5TWpFd01EY3lNelU1TlRsYU1Ib3hDekFKQmdOVk 0ATVE0d0RBWURWUVFJRXdWVVpYaGhjekVTTUJBR0ExVUVCeE1KUVhKc2FXNW5kRzl1T 0AUVFLRXlOVkxsTXVJRVJsY0dGeWRHMWxiblFnYjJZZ1ZtVjBaWEpoYm5NZ1FXWm1ZV2x5 0AY0dBMVVFQXhNUVpHVjJMbVZoZFhSb0xuWmhMbWR2ZGpDQ0FpSXdEUVlKS29aSWh2 0ARGdnSVBBRENDQWdvQ2dnSUJBSzNUeG5OcVZYamZLN2VqcmprQXZ6cWoxbzdMNTdlV 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxl 0AVld3MVV2WS9QVGxDQlk3RzlTOVh1RXAzYTJQdGVKb2FGZTZKK3hQVWRpMUZtQTM1c 0AcU90RkZ2bVpNU1pYaHdpdmszQnpNMVdoMm16cDBDTXBwSzl5MkUvcjkyaHZMWlJVYStY 0AbTBJMGFEeDNaSERPT0E5bkc2WXVwNWZxNUt6Z28vdVFMK0QzN0JRQlRic2Q2NGNWa 0AZ1UrdS9yejczN0l4UU96aUpKRW9oMkZqYVE5Q2lVcEorVFRuQ21leXdUUDh6N1lmOG1RV 0AVExuR2Q2bVN6U2M3ZER1NmhEaUJRZlYzalkwWUhQTDAzUG1XMXJlbnlQMHZPWHZ5T 0AWWdCc2xLSWI2QXE1d0s1bTdlOHpHenJyakNBZXBNSmk3Q1AwK3VGTFhqWlJKa1V1ZkU 0AR2l1SVhlM0MvRnZKTmJsZkczSEc3WExKWTVBV1FGQjVzZnNBZGN5eFlENU1DS1kzTDd 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AY2Z2aFlkZVV6cWhPUmdsRndldTJtRG5LRDBBRUxaZkZHenR6c1pOQVB5VExPOHRkRSs 0AUHVUQnVaOXNKVERBNWMwQW1WMzZCdkZ6NXAwTEJWNVo1ZlRsWXVHWXlCZGdSS 0ARG5QaTVTdzJXcVhVMmcraUhBZ01CQUFHamdnTjBNSUlEY0RBZkJnTlZIU01FR0RBV2dC 0AcUtxRWpIbnF0Tm9QbUxMRmxYYTU5REFkQmdOVkhRNEVGZ1FVajFTZlc1YXVndFNrOTc 0AQ01VYWE4d0d3WURWUjBSQkJRd0VvSVFaR1YyTG1WaGRYUm9MblpoTG1kdmRqQU9C 0AOEVCQU1DQmFBd0hRWURWUjBsQkJZd0ZBWUlLd1lCQlFVSEF3RUdDQ3NHQVFVRkJ3

	0AVkhSOEVnWWN3Z1lRd1FLQStvRHlHT21oMGRIQTZMeTlqY213ekxtUnBaMmxqWlhKMExt 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ASEE2THk5amNtdzBMbVJwWjJsalpYSjBMbU52YlM5RWFXZHBRMlZ5ZEZSTVUxSlRRVk5J 0ASXdNakJEUVRFdE5DNWpjbXd3UGdZRFZSMGdCRGN3TlRBekJnWm5nUXdCQWdJd0tUC 0ARkJRY0NBUlliYUhSMGNEb3ZMM2QzZHk1a2FXZHBZMlZ5ZEM1amIyMHZRMUJUTUg4R0 0AQndFQkJITXdjVEFrQmdnckJnRUZCUWN3QVlZWWFIUjBjRG92TDI5amMzQXVaR2xuYVd0 0AMjl0TUVrR0NDc0dBUVVGQnpBQ2hqMW9kSFJ3T2k4dlkyRmpaWEowY3k1a2FXZHBZMlZ5 0AMHZSR2xuYVVObGNuUlVURk5TVTBGVFNFRXlOVFl5TURJd1EwRXhMVEV1WTNKME1B 0AQi93UUNNQUF3Z2dGL0Jnb3JCZ0VFQWRaNUFnUUNCSUlCYndTQ0FXc0JhUUIzQUVhbF 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0AUFBQMkR6WGlPQVRDUUVXdGFvTkZMOE1FMmc3RWRaUnNsRWYydml5aldzTUFpRUFC 0AcnpWaWFTUzB5RWJ4Zk1tQWp5T0ZXNUExWEFZWDRiUktzQWRnQlJvN0QxL1FGNW5GV 0Aa2Vzd2JKOHYzbm9oQ21nMysxSXNGNVFBQUFYeGRLRDBpQUFBRUF3QkhNRVVDSUFI 0AbG1ROVh6ZWYrYU82RXRTSlFhNTVQVWp5Qkc0a1QrMStBaUVBMGIzVG9YcWNnU01teD 0AWGd4WWVNTW4rSUh4dFlNLzE0TVRJNEFkZ0JCeU1xeDN5SkdTaERHb1RvSlFvZGVUak 0AdkhhUENRWXBZRzlnQUFBWHhkS0R6akFBQUVBd0JITUVVQ0lEQkpwY2ttSHhiOGpZaldu 0Aa0IvVGcyOHZubTg3Uno1WitWOUNPQWlFQWdQNyt1NXhpTTNrTzB0cjYrUlBOd2lrZEpmR 0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUDM3V 0AT1ViN2p3YUxOY1oyWHJ3NVRaWUdlWVAwV1c5aXhvSkRvdkdDcW5pOWoyMFhCemh5RI 0AKy9Pa0pqdVpTMFhIamJQQ3VWVHZQaTdORGhkU285WkpwZVdrblVUTDYwb3FYdkFsbGx 0ARWZKcU9aV3RHRUhxZXdWdTlvbU56Tkw0L2JQSWF0NStpNHdqQklSSk5POGhlOCtBWnI 0AbmtrU3NtNkUzeHFEVVlpR1dlc3ZTS2Fkc1ZxZGNxeDQ4Y2JxT0FGU2k4UDE1NWZGQXFN 0AWkJhUWV1VlBRcGZUNVc2R2FhV3VTWmZyeHNDeFlzbEFCdzYwbGJkbUJCbzZweVREUk 0ASFkwLzZtMDFHYnJ2WStuSCtpSWVKRGV0Sk9DTmRoMUJ2R3F6az08L2RzOlg1MDlDZXJ 0AZT48L2RzOlg1MDlEYXRhPjwvZHM6S2V5SW5mbz48L2RzOlNpZ25hdHVyZT48c2FtbHA6T 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM 0ATDoxLjE6bmFtZWlkLWZvcm1hdDplbWFpbEFkZHJlc3MiPjwvc2FtbHA6TmFtZUlEUG9saWN 0AYW1scDpSZXF1ZXN0ZWRBdXRobkNvbnRleHQgQ29tcGFyaXNvbj0ibWluaW11bSI%2BPH 0AaG5Db250ZXh0Q2xhc3NSZWY%2BaHR0cDovL2lkbWFuYWdlbWVudC5nb3YvbnMvYXNzd 0AbC8xPC9zYW1sOkF1dGhuQ29udGV4dENsYXNzUmVmPjxzYW1sOkF1dGhuQ29udGV4dE 0APmh0dHA6Ly9pZG1hbmFnZW1lbnQuZ292L25zL2Fzc3VyYW5jZS9hYWwvMjwvc2FtbDpBd 0AbnRleHRDbGFzc1JlZj48L3NhbWxwOlJlcXVlc3RlZEF1dGhuQ29udGV4dD48L3NhbWxwOkF 0AUmVxdWVzdD4%3D&RelayState=uuidecfd2e99-27cb-4b11-a466-8d9d064fbac1
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/polyfill-9c10ccd9.js" nomodule="no
	https://idp.int.identitysandbox.gov/api/saml/auth2022? SAMLRequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpkcz0iaHR0cDovL3d3dy53My 0D%0AbWxkc2lnIyIgeG1sbnM6c2FtbD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmF 0AbiIgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpwcm90b2NvbCIgI 0AdGluYXRpb249Imh0dHBzOi8vaWRwLmludC5pZGVudGl0eXNhbmRib3guZ292L2FwaS9zYV 0AdGgyMDIyIiBGb3JjZUF1dGhuPSJmYWxzZSIgSUQ9IkZJTVJFUV9iMWZiYjgzZi0wMTdmLTF 0AOTNmNi04YjliNDUzNmRmYmYiIElzUGFzc2l2ZT0iZmFsc2UiIElzc3VlSW5zdGFudD0iMjAyM 0AMy0yMlQxNDoxNTozOFoiIFZlcnNpb249IjIuMCI%2BPHNhbWw6SXNzdWVyIEZvcm1hdD0ic 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0AYXV0aC52YS5nb3YvaXNhbS9zcHMvc2FtbDIwc3Avc2FtbDIwPC9zYW1sOklzc3Vlcj48ZHM6 0AbmF0dXJlIElkPSJ1dWlkYjFmYmI4NDEtMDE3Zi0xNDFlLTg4NGQtOGI5YjQ1MzZkZmJmIj48 0AU2lnbmVkSW5mbz48ZHM6Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBBbGdvcml0aG09Imh0dH 0Ad3cudzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyI%2BPC9kczpDYW5vbmljYWxpemF 0AaG9kPjxkczpTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZ 0ALzA0L3htbGRzaWctbW9yZSNyc2Etc2hhMjU2Ij48L2RzOlNpZ25hdHVyZU1ldGhvZD48ZHM6 0AZXJlbmNlIFVSST0iI0ZJTVJFUV9iMWZiYjgzZi0wMTdmLTFiNDgtOTNmNi04YjliNDUzNmRm 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AZy8yMDAwLzA5L3htbGRzaWcjZW52ZWxvcGVkLXNpZ25hdHVyZSI%2BPC9kczpUcmFuc2 0AOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMTAveG1sL 0AMTRuIyI%2BPHhjMTRuOkluY2x1c2l2ZU5hbWVzcGFjZXMgeG1sbnM6eGMxNG49Imh0dHA 0AdzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyIgUHJlZml4TGlzdD0ic2FtbHAgc2FtbCBk 0APC94YzE0bjpJbmNsdXNpdmVOYW1lc3BhY2VzPjwvZHM6VHJhbnNmb3JtPjwvZHM6VHJhl 0Acz48ZHM6RGlnZXN0TWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwM 0AbWxlbmMjc2hhMjU2Ij48L2RzOkRpZ2VzdE1ldGhvZD48ZHM6RGlnZXN0VmFsdWU%2BTEq 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AUmVmZXJlbmNlPjwvZHM6U2lnbmVkSW5mbz48ZHM6U2lnbmF0dXJlVmFsdWU%2BUmNp 0AeEw5SEFlajluajQ1Q3RBeVUzYnQwWDhqOG1QMG1nbDlNS2pBYXBSaGVEVStSRHYzNn 0AUTIyUzlzMGV0RHlHNVVMWlkvV1JQTTNiUmtNVG5jTTZYa0dHMlFmRzJGVGhQeGtBMTd5 0AeXRSMUZNL3BRdE5HM0FYVWJiNFBlOWpEZmgwYTlsUXFYVG5ETXc0Z0s1SzVtT2JoRD

URL	0AcTBrb2tiNlEvZmlCMGs4VTdMdTVQeURqSktNblZ0L1dnbUo1MmY1R2NuRFZMbzQvcU5UU 0AUWpMY2dtWGxiMlA3ejE0WG9NK2tZS2w3SXZCamo1b2VDbjhNR01iYks3UGVaWGswVjM4 0ATWl4TnU3TXpsZHpPdCtiREUvZGdqOTYyWWxxcmpzRkZzZ2l4M1JKcUtDTXA3L2xMV1FX 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AVnhRVDNaanlaNXhPUk9xVXpoeFlZOEhiTFZIdHc2M2NYa0h2MHkxN1M2ZFN5QmVmM2tH 0AT25nS1BPcEdjMGRHNUN6bkREYWF4RTBKU0NSM1MwT016U1psMXV2eU45OFZXeEsyQ 0AT3duWmhaYm5qNDdQaDgyTFErM1B6UVJ3VVBUcGNmRkVESTdjZGJXeVcvV21VSVlLUG 0Aalp0MFRPREhFejlvOEQ1L1FOTHMyK1llM2k1dVVjbnZlYzdUY0krYVhHUWN5c1ZBVkExcD 0Ac1JucCsreWh5S0VnTy91cWRxM2RIb2ZHcC8rMTVhdTJKQnZHUVpPOU1sZ1U9PC9kczpT 0AcmVWYWx1ZT48ZHM6S2V5SW5mbz48ZHM6WDUwOURhdGE%2BPGRzOlg1MDlDZXJ0a 0D%0AeVRDQ0JyR2dBd0lCQWdJUURFQi9NckdESGkwTzcyME5lK1RBYnpBTkJna3Foa2lHC 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0AWURWUVFERXlCRWFXZHBRMlZ5ZENCVVRGTWdVbE5CSUZOSVFUSTFOaUF5TURJd0 0AeU1URXdNRGN3TURBd01EQmFGdzB5TWpFd01EY3lNelU1TlRsYU1ib3hDekFKQmdOVkJ 0ATVE0d0RBWURWUVFJRXdWVVpYaGhjekVTTUJBR0ExVUVCeE1KUVhKc2FXNW5kRzl1T 0AUVFLRXlOVkxsTXVJRVJsY0dGeWRHMWxiblFnYjJZZ1ZtVjBaWEpoYm5NZ1FXWm1ZV2x5 0AY0dBMVVFQXhNUVpHVjJMbVZoZFhSb0xuWmhMbWR2ZGpDQ0FpSXdEUVlKS29aSWh2 0ARGdnSVBBRENDQWdvQ2dnSUJBSzNUeG5OcVZYamZLN2VqcmprQXZ6cWoxbzdMNTdlV 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxb 0AVld3MVV2WS9QVGxDQlk3RzlTOVh1RXAzYTJQdGVKb2FGZTZKK3hQVWRpMUZtQTM1c 0AcU90RkZ2bVpNU1pYaHdpdmszQnpNMVdoMm16cDBDTXBwSzl5MkUvcjkyaHZMWlJVYStY 0AbTBJMGFEeDNaSERPT0E5bkc2WXVwNWZxNUt6Z28vdVFMK0QzN0JRQlRic2Q2NGNWa 0AZ1UrdS9yejczN0l4UU96aUpKRW9oMkZqYVE5Q2lVcEorVFRuQ21leXdUUDh6N1lmOG1RV 0AVExuR2Q2bVN6U2M3ZER1NmhEaUJRZlYzalkwWUhQTDAzUG1XMXJIbnlQMHZPWHZ5T 0AWWdCc2xLSWI2QXE1d0s1bTdlOHpHenJyakNBZXBNSmk3Q1AwK3VGTFhqWlJKa1V1ZkU 0AR2l1SVhlM0MvRnZKTmJsZkczSEc3WExKWTVBV1FGQjVzZnNBZGN5eFlENU1DS1kzTDd 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AY2Z2aFlkZVV6cWhPUmdsRndldTJtRG5LRDBBRUxaZkZHenR6c1pOQVB5VExPOHRkRSs 0AUHVUQnVaOXNKVERBNWMwQW1WMzZCdkZ6NXAwTEJWNVo1ZlRsWXVHWXlCZGdSS 0ARG5QaTVTdzJXcVhVMmcraUhBZ01CQUFHamdnTjBNSUlEY0RBZkJnTlZIU01FR0RBV2dC 0AcUtxRWpIbnF0Tm9QbUxMRmxYYTU5REFkQmdOVkhRNEVGZ1FVajFTZlc1YXVndFNrOTc 0AQ01VYWE4d0d3WURWUjBSQkJRd0VvSVFaR1YyTG1WaGRYUm9MblpoTG1kdmRqQU9C 0AOEVCQU1DQmFBd0hRWURWUjBsQkJZd0ZBWUlLd1lCQlFVSEF3RUdDQ3NHQVFVRkJ3 0AVkhSOEVnWWN3Z1lRd1FLQStvRHlHT21oMGRIQTZMeTlqY213ekxtUnBaMmxqWlhKMExt 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ASEE2THk5amNtdzBMbVJwWjJsalpYSjBMbU52YlM5RWFXZHBRMlZ5ZEZSTVUxSlRRVk5J 0ASXdNakJEUVRFdE5DNWpjbXd3UGdZRFZSMGdCRGN3TlRBekJnWm5nUXdCQWdJd0tUC 0ARkJRY0NBUlliYUhSMGNEb3ZMM2QzZHk1a2FXZHBZMlZ5ZEM1amIyMHZRMUJUTUg4R0 0AQndFQkJITXdjVEFrQmdnckJnRUZCUWN3QVlZWWFIUjBjRG92TDI5amMzQXVaR2xuYVd0 0AMjl0TUVrR0NDc0dBUVVGQnpBQ2hqMW9kSFJ3T2k4dlkyRmpaWEowY3k1a2FXZHBZMlZ5 0AMHZSR2xuYVVObGNuUlVURk5TVTBGVFNFRXlOVFl5TURJd1EwRXhMVEV1WTNKME1B 0AQi93UUNNQUF3Z2dGL0Jnb3JCZ0VFQWRaNUFnUUNCSUlCYndTQ0FXc0JhUUIzQUVhbF 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0AUFBQMkR6WGlPQVRDUUVXdGFvTkZMOE1FMmc3RWRaUnNsRWYydml5aldzTUFpRUF 0AcnpWaWFTUzB5RWJ4Zk1tQWp5T0ZXNUExWEFZWDRiUktzQWRnQlJvN0QxL1FGNW5GV 0Aa2Vzd2JKOHYzbm9oQ21nMysxSXNGNVFBQUFYeGRLRDBpQUFBRUF3QkhNRVVDSUFI 0AbG1ROVh6ZWYrYU82RXRTSlFhNTVQVWp5Qkc0a1QrMStBaUVBMGIzVG9YcWNnU01teE 0AWGd4WWVNTW4rSUh4dFlNLzE0TVRJNEFkZ0JCeU1xeDN5SkdTaERHb1RvSlFvZGVUak 0AdkhhUENRWXBZRzlnQUFBWHhkS0R6akFBQUVBd0JITUVVQ0lEQkpwY2ttSHhiOGpZaldu 0Aa0IvVGcyOHZubTg3Uno1WitWOUNPQWlFQWdQNyt1NXhpTTNrTzB0cjYrUlBOd2lrZEpmR 0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUDM3Vr 0AT1ViN2p3YUxOY1oyWHJ3NVRaWUdlWVAwV1c5aXhvSkRvdkdDcW5pOWoyMFhCemh5RI 0AKy9Pa0pqdVpTMFhIamJQQ3VWVHZQaTdORGhkU285WkpwZVdrblVUTDYwb3FYdkFsbGx 0ARWZKcU9aV3RHRUhxZXdWdTlvbU56Tkw0L2JQSWF0NStpNHdqQklSSk5POGhIOCtBWnI 0AbmtrU3NtNkUzeHFEVVlpR1dlc3ZTS2Fkc1ZxZGNxeDQ4Y2JxT0FGU2k4UDE1NWZGQXFN 0AWkJhUWV1VlBRcGZUNVc2R2FhV3VTWmZyeHNDeFlzbEFCdzYwbGJkbUJCbzZweVREUk 0ASFkwLzZtMDFHYnJ2WStuSCtpSWVKRGV0Sk9DTmRoMUJ2R3F6az08L2RzOlg1MDlDZXJ 0AZT48L2RzOlg1MDlEYXRhPjwvZHM6S2V5SW5mbz48L2RzOlNpZ25hdHVyZT48c2FtbHA6T 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM 0ATDoxLjE6bmFtZWlkLWZvcm1hdDplbWFpbEFkZHJlc3MiPjwvc2FtbHA6TmFtZUlEUG9saWN 0AYW1scDpSZXF1ZXN0ZWRBdXRobkNvbnRleHQgQ29tcGFyaXNvbj0ibWluaW11bSI%2BPH 0AaG5Db250ZXh0Q2xhc3NSZWY%2BaHR0cDovL2lkbWFuYWdlbWVudC5nb3YvbnMvYXNzd 0AbC8xPC9zYW1sOkF1dGhuQ29udGV4dENsYXNzUmVmPjxzYW1sOkF1dGhuQ29udGV4dE 0APmh0dHA6Ly9pZG1hbmFnZW1lbnQuZ292L25zL2Fzc3VyYW5jZS9hYWwvMjwvc2FtbDpBd 0AbnRleHRDbGFzc1JlZj48L3NhbWxwOlJlcXVlc3RlZEF1dGhuQ29udGV4dD48L3NhbWxwOkF 0AUmVxdWVzdD4%3D&RelayState=uuidecfd2e99-27cb-4b11-a466-8d9d064fbac1
Method	GET

Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/saml-post-96dc0778.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/assets/es5-shim.min-08adc386ca6471303e97607bac7d044722912858eb4b42af460a8583449fe021.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/assets/html5shiv-3481001ecf33e49ca9e98b5dbd99334cffcd0b1d9c27b554463e70735e9a17e3.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/assets/respond.min-aa35dd790d2b157f3ef06473825ac6c7a637739b7a8f2ab2ea6a365b439462cc.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/29-ed45901c.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/30-1a6066ea.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.en.js"></scri
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.js"></script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/countdown_component-153bd7bd
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/countdown_component-153bd7bd
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator

Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.en.js"><</script>
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.js"></sc
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/one-time-code-input-f050e903.js">
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/polyfill-9c10ccd9.js" nomodule="n
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/session-timeout-ping-a1fe05f2.js">
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	<script async type="text/javascript" nonce="dotQsB9qLzvJcxrUJrjetg4157VqzYde" src="https://d /Universal-Federated-Analytics-Min.js?agency=VA" id="_fed_an_ua_tag"></script>
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	<script defer type="text/javascript" nonce="dotQsB9qLzvJcxrUJrjetg4157VqzYde" src="https://re gov/wdcvoice/5/onsite/embed.js" async></script>
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	<script nonce="dotQsB9qLzvJcxrUJrjetg4157VqzYde" nomodule data-entry-name="polyfills.js" gov-assets.s3-us-gov-west-1.amazonaws.com/generated/polyfills.entry.js"></script>
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	<script nonce="dotQsB9qLzvJcxrUJrjetg4157VqzYde" defer data-entry-name="static-pages.js" gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js"></script>
URL	https://staging.va.gov/
Method	GET
Attack	
	<script nonce="dotQsB9qLzvJcxrUJrjetg4157VqzYde" defer data-entry-name="vendor.js" src="h

Evidence	assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js"></script>
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	<script nonce="dotQsB9qLzvJcxrUJrjetg4157VqzYde" defer data-entry-name="web-component va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.entry.js"></script
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	<script async type="text/javascript" nonce="jQKemYml2FZIgeFLluTuoA8HhFBXe9aS" src="http /Universal-Federated-Analytics-Min.js?agency=VA" id="_fed_an_ua_tag"></script>
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	<script defer type="text/javascript" nonce="jQKemYml2FZIgeFLluTuoA8HhFBXe9aS" src="https va.gov/wdcvoice/5/onsite/embed.js" async></script>
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	<script nonce="jQKemYml2FZIgeFLluTuoA8HhFBXe9aS" nomodule data-entry-name="polyfills gov-assets.s3-us-gov-west-1.amazonaws.com/generated/polyfills.entry.js"></script>
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	<script nonce="jQKemYml2FZIgeFLluTuoA8HhFBXe9aS" defer data-entry-name="static-pages gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js"></script>
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	<script nonce="jQKemYml2FZIgeFLluTuoA8HhFBXe9aS" defer data-entry-name="vendor.js" sr assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js"></script>
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	<script nonce="jQKemYml2FZIgeFLluTuoA8HhFBXe9aS" defer data-entry-name="web-compon https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.en
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	<script async type="text/javascript" nonce="UrIdh9jDufBooyYfV5lePcFEhYYQQNhH" src="https /Universal-Federated-Analytics-Min.js?agency=VA" id="_fed_an_ua_tag"></script>
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
	<script defer type="text/javascript" nonce="UrIdh9jDufBooyYfV5lePcFEhYYQQNhH" src="https:

Evidence	gov/wdcvoice/5/onsite/embed.js" async></script>
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	<script nonce="UrIdh9jDufBooyYfV5lePcFEhYYQQNhH" defer data-entry-name="auth.js" src=" assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js"></script>
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	<script nonce="UrIdh9jDufBooyYfV5lePcFEhYYQQNhH" nomodule data-entry-name="polyfills.j gov-assets.s3-us-gov-west-1.amazonaws.com/generated/polyfills.entry.js"></script>
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	<script nonce="UrIdh9jDufBooyYfV5lePcFEhYYQQNhH" defer data-entry-name="vendor.js" src assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js"></script>
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	<script nonce="UrIdh9jDufBooyYfV5lePcFEhYYQQNhH" defer data-entry-name="web-compone https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/polyfill-9c10ccd9.js" nomodule="n
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/saml-post-96dc0778.js"></script>
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/polyfill-9c10ccd9.js" nomodule="n
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	<script src="https://static.idp.int.identitysandbox.gov/packs/js/saml-post-96dc0778.js"></script>
Instances	49
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be c the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP respor such information may facilitate attackers identifying other frameworks/components your web ap and the vulnerabilities such components may be subject to.
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022? SAMLRequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpkcz0iaHR0cDovL3d3dy53My 0D%0AbWxkc2lnIyIgeG1sbnM6c2FtbD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmF 0AbiIgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpwcm90b2NvbCIgI 0AdGluYXRpb249Imh0dHBzOi8vaWRwLmludC5pZGVudGl0eXNhbmRib3guZ292L2FwaS9zYV 0AdGgyMDIyIiBGb3JjZUF1dGhuPSJmYWxzZSIgSUQ9IkZJTVJFUV9iMWZiYjgzZi0wMTdmLTF 0AOTNmNi04YjliNDUzNmRmYmYiIElzUGFzc2l2ZT0iZmFsc2UiIElzc3VlSW5zdGFudD0iMjAyM 0AMy0yMlQxNDoxNTozOFoiIFZlcnNpb249IjIuMCI%2BPHNhbWw6SXNzdWVyIEZvcm1hdD0ic 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij5odHRwczov 0AYXV0aC52YS5nb3YvaXNhbS9zcHMvc2FtbDIwc3Avc2FtbDIwPC9zYW1sOklzc3Vlcj48ZHM6 0AbmF0dXJlIElkPSJ1dWlkYjFmYmI4NDEtMDE3Zi0xNDFlLTg4NGQtOGI5YjQ1MzZkZmJmIj48 0AU2lnbmVkSW5mbz48ZHM6Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBBbGdvcml0aG09Imh0dH 0Ad3cudzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyI%2BPC9kczpDYW5vbmljYWxpemF 0AaG9kPjxkczpTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZ 0ALzA0L3htbGRzaWctbW9yZSNyc2Etc2hhMjU2Ij48L2RzOlNpZ25hdHVyZU1ldGhvZD48ZHM6 0AZXJlbmNlIFVSST0iI0ZJTVJFUV9iMWZiYjgzZi0wMTdmLTFiNDgtOTNmNi04YjliNDUzNmRm 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AZy8yMDAwLzA5L3htbGRzaWcjZW52ZWxvcGVkLXNpZ25hdHVyZSI%2BPC9kczpUcmFuc2 0AOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMTAveG1sL 0AMTRuIyI%2BPHhjMTRuOkluY2x1c2l2ZU5hbWVzcGFjZXMgeG1sbnM6eGMxNG49Imh0dHA 0AdzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyIgUHJlZml4TGlzdD0ic2FtbHAgc2FtbCBk 0APC94YzE0bjpJbmNsdXNpdmVOYW1lc3BhY2VzPjwvZHM6VHJhbnNmb3JtPjwvZHM6VHJh 0Acz48ZHM6RGlnZXN0TWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwM 0AbWxlbmMjc2hhMjU2Ij48L2RzOkRpZ2VzdE1ldGhvZD48ZHM6RGlnZXN0VmFsdWU%2BTEc 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AUmVmZXJlbmNlPjwvZHM6U2lnbmVkSW5mbz48ZHM6U2lnbmF0dXJlVmFsdWU%2BUmNp 0AeEw5SEFlajluajQ1Q3RBeVUzYnQwWDhqOG1QMG1nbDlNS2pBYXBSaGVEVStSRHYzNn 0AUTIyUzIzMGV0RHlHNVVMWlkvV1JQTTNiUmtNVG5jTTZYa0dHMlFmRzJGVGhQeGtBMTd5 0AeXRSMUZNL3BRdE5HM0FYVWJiNFBlOWpEZmgwYTlsUXFYVG5ETXc0Z0s1SzVtT2JoRD 0AcTBrb2tiNlEvZmlCMGs4VTdMdTVQeURqSktNblZ0L1dnbUo1MmY1R2NuRFZMbzQvcU5UU 0AUWpMY2dtWGxiMlA3ejE0WG9NK2tZS2w3SXZCamo1b2VDbjhNR01iYks3UGVaWGswVjM 0ATWl4TnU3TXpsZHpPdCtiREUvZGdqOTYyWWxxcmpzRkZzZ2l4M1JKcUtDTXA3L2xMV1FX 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AVnhRVDNaanlaNXhPUk9xVXpoeFlZOEhiTFZIdHc2M2NYa0h2MHkxN1M2ZFN5QmVmM2tH 0AT25nS1BPcEdjMGRHNUN6bkREYWF4RTBKU0NSM1MwT016U1psMXV2eU45OFZXeEsyC 0AT3duWmhaYm5qNDdQaDgvTFErM1B6UVJ3VVBUcGNmRkVESTdjZGJXeVcvV21VSVlLUG 0Aalp0MFRPREhFejlvOEQ1L1FOTHMyK1llM2k1dVVjbnZIYzdUY0krYVhHUWN5c1ZBVkExcD 0Ac1JucCsreWh5S0VnTy91cWRxM2Rlb2ZHcC8rMTVhdTJKQnZHUVpPOU1sZ1U9PC9kczpT 0AcmVWYWx1ZT48ZHM6S2V5SW5mbz48ZHM6WDUwOURhdGE%2BPGRzOlg1MDlDZXJ0a 0D%0AeVRDQ0JyR2dBd0lCQWdJUURFQi9NckdESGkwTzcyME5IK1RBYnpBTkJna3Foa2lHC 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0AWURWUVFERXlCRWFXZHBRMlZ5ZENCVVRGTWdVbE5CSUZOSVFUSTFOaUF5TURJd(0AeU1URXdNRGN3TURBd01EQmFGdzB5TWpFd01EY3lNelU1TlRsYU1Ib3hDekFKQmdOVk 0ATVE0d0RBWURWUVFJRXdWVVpYaGhjekVTTUJBR0ExVUVCeE1KUVhKc2FXNW5kRzl1T 0AUVFLRXlOVkxsTXVJRVJsY0dGeWRHMWxiblFnYjJZZ1ZtVjBaWEpoYm5NZ1FXWm1ZV2x5 0AY0dBMVVFQXhNUVpHVjJMbVZoZFhSb0xuWmhMbWR2ZGpDQ0FpSXdEUVlKS29aSWh2 0ARGdnSVBBRENDQWdvQ2dnSUJBSzNUeG5OcVZYamZLN2VqcmprQXZ6cWoxbzdMNTdlV 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxI 0AVld3MVV2WS9QVGxDQlk3RzlTOVh1RXAzYTJQdGVKb2FGZTZKK3hQVWRpMUZtQTM1c 0AcU90RkZ2bVpNU1pYaHdpdmszQnpNMVdoMm16cDBDTXBwSzl5MkUvcjkyaHZMWlJVYStY 0AbTBJMGFEeDNaSERPT0E5bkc2WXVwNWZxNUt6Z28vdVFMK0QzN0JRQlRic2Q2NGNWa 0AZ1UrdS9yejczN0l4UU96aUpKRW9oMkZqYVE5Q2lVcEorVFRuQ21leXdUUDh6N1lmOG1RV 0AVExuR2Q2bVN6U2M3ZER1NmhEaUJRZlYzalkwWUhQTDAzUG1XMXJIbnlQMHZPWHZ5T 0AWWdCc2xLSWI2QXE1d0s1bTdlOHpHenJyakNBZXBNSmk3Q1AwK3VGTFhqWlJKa1V1ZkU 0AR2l1SVhlM0MvRnZKTmJsZkczSEc3WExKWTVBV1FGQjVzZnNBZGN5eFlENU1DS1kzTDd

	0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AY2Z2aFlkZVV6cWhPUmdsRndldTJtRG5LRDBBRUxaZkZHenR6c1pOQVB5VExPOHRkRSs 0AUHVUQnVaOXNKVERBNWMwQW1WMzZCdkZ6NXAwTEJWNVo1ZlRsWXVHWXlCZGdSS 0ARG5QaTVTdzJXcVhVMmcraUhBZ01CQUFHamdnTjBNSUlEY0RBZkJnTlZIU01FR0RBV2dC 0AcUtxRWpIbnF0Tm9QbUxMRmxYYTU5REFkQmdOVkhRNEVGZ1FVajFTZlc1YXVndFNrOTc 0AQ01VYWE4d0d3WURWUjBSQkJRd0VvSVFaR1YyTG1WaGRYUm9MblpoTG1kdmRqQU9C 0AOEVCQU1DQmFBd0hRWURWUjBsQkJZd0ZBWUlLd1lCQlFVSEF3RUdDQ3NHQVFVRkJ3 0AVkhSOEVnWWN3Z1lRd1FLQStvRHlHT21oMGRIQTZMeTlqY213ekxtUnBaMmxqWlhKMExt 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ASEE2THk5amNtdzBMbVJwWjJsalpYSjBMbU52YlM5RWFXZHBRMlZ5ZEZSTVUxSlRRVk5J 0ASXdNakJEUVRFdE5DNWpjbXd3UGdZRFZSMGdCRGN3TlRBekJnWm5nUXdCQWdJd0tUC 0ARkJRY0NBUlliYUhSMGNEb3ZMM2QzZHk1a2FXZHBZMlZ5ZEM1amIyMHZRMUJUTUg4R0 0AQndFQkJITXdjVEFrQmdnckJnRUZCUWN3QVlZWWFIUjBjRG92TDI5amMzQXVaR2xuYVd0 0AMjl0TUVrR0NDc0dBUVVGQnpBQ2hqMW9kSFJ3T2k4dlkyRmpaWEowY3k1a2FXZHBZMlZ5 0AMHZSR2xuYVVObGNuUlVURk5TVTBGVFNFRXlOVFl5TURJd1EwRXhMVEV1WTNKME1B 0AQi93UUNNQUF3Z2dGL0Jnb3JCZ0VFQWRaNUFnUUNCSUlCYndTQ0FXc0JhUUIzQUVhbF 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0AUFBQMkR6WGlPQVRDUUVXdGFvTkZMOE1FMmc3RWRaUnNsRWYydml5aldzTUFpRUF 0AcnpWaWFTUzB5RWJ4Zk1tQWp5T0ZXNUExWEFZWDRiUktzQWRnQlJvN0QxL1FGNW5GV 0Aa2Vzd2JKOHYzbm9oQ21nMysxSXNGNVFBQUFYeGRLRDBpQUFBRUF3QkhNRVVDSUFI 0AbG1ROVh6ZWYrYU82RXRTSlFhNTVQVWp5Qkc0a1QrMStBaUVBMGIzVG9YcWNnU01teD 0AWGd4WWVNTW4rSUh4dFlNLzE0TVRJNEFkZ0JCeU1xeDN5SkdTaERHb1RvSlFvZGVUak 0AdkhhUENRWXBZRzlnQUFBWHhkS0R6akFBQUVBd0JITUVVQ0lEQkpwY2ttSHhiOGpZaldu 0Aa0IvVGcyOHZubTg3Uno1WitWOUNPQWlFQWdQNyt1NXhpTTNrTzB0cjYrUlBOd2lrZEpmR 0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUDM3V 0AT1ViN2p3YUxOY1oyWHJ3NVRaWUdlWVAwV1c5aXhvSkRvdkdDcW5pOWoyMFhCemh5RI 0AKy9Pa0pqdVpTMFhIamJQQ3VWVHZQaTdORGhkU285WkpwZVdrblVUTDYwb3FYdkFsbGx 0ARWZKcU9aV3RHRUhxZXdWdTlvbU56Tkw0L2JQSWF0NStpNHdqQklSSk5POGhlOCtBWnI 0AbmtrU3NtNkUzeHFEVVlpR1dlc3ZTS2Fkc1ZxZGNxeDQ4Y2JxT0FGU2k4UDE1NWZGQXFN 0AWkJhUWV1VlBRcGZUNVc2R2FhV3VTWmZyeHNDeFlzbEFCdzYwbGJkbUJCbzZweVREUk 0ASFkwLzZtMDFHYnJ2WStuSCtpSWVKRGV0Sk9DTmRoMUJ2R3F6az08L2RzOlg1MDlDZXJ 0AZT48L2RzOlg1MDlEYXRhPjwvZHM6S2V5SW5mbz48L2RzOlNpZ25hdHVyZT48c2FtbHA6T 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM 0ATDoxLjE6bmFtZWlkLWZvcm1hdDplbWFpbEFkZHJlc3MiPjwvc2FtbHA6TmFtZUlEUG9saWN 0AYW1scDpSZXF1ZXN0ZWRBdXRobkNvbnRleHQgQ29tcGFyaXNvbj0ibWluaW11bSI%2BPH 0AaG5Db250ZXh0Q2xhc3NSZWY%2BaHR0cDovL2lkbWFuYWdlbWVudC5nb3YvbnMvYXNzd 0AbC8xPC9zYW1sOkF1dGhuQ29udGV4dENsYXNzUmVmPjxzYW1sOkF1dGhuQ29udGV4dE 0APmh0dHA6Ly9pZG1hbmFnZW1lbnQuZ292L25zL2Fzc3VyYW5jZS9hYWwvMjwvc2FtbDpBd 0AbnRleHRDbGFzc1JlZj48L3NhbWxwOlJlcXVlc3RlZEF1dGhuQ29udGV4dD48L3NhbWxwOkF 0AUmVxdWVzdD4%3D&RelayState=uuidecfd2e99-27cb-4b11-a466-8d9d064fbac1
Method	GET
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/users/two_factor_authentication
Method	GET
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/
Method	POST
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022

Method	POST
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	POST
Attack	
Evidence	X-Powered-By: Phusion Passenger(R)
Instances	8
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.a http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=GSA&subagency=TTS
Method	GET
Attack	
Evidence	20181010
URL	https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=GSA&subagency=TTS
Method	GET
Attack	
Evidence	33523145
URL	https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=VA
Method	GET
Attack	
Evidence	20181010
URL	https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=VA
Method	GET
Attack	
Evidence	33523145
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	46002776
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator

Method	GET
Attack	
Evidence	46002776
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	2147483000
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	2147483646
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	2147483647
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	99999990
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	99999998
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	99999999
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva.css
Method	GET
Attack	
Evidence	13622391
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva.css
Method	GET
Attack	
Evidence	42857143
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap-formhelpers.min.css
Method	GET
Attack	
Evidence	428571429
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET

Attack	
Evidence	0123456789
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	10000000
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	86400000
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	02252021
URL	https://staging-api.va.gov/v0/user
Method	GET
Attack	
Evidence	19800816
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	0123456789
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	1073741823
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	1073741824
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	1073741825
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	134217727
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js

Method	GET
Attack	
Evidence	134217728
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	2147483647
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	268435456
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	33554432
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	50123418
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	62914560
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	67108864
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	805306368
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	010101010
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	01012121
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET

Attack	
Evidence	010201010
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	01021030
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	01212121
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	0121212121
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	01231321
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	01232425
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	012324256
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	0123423232
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	0123456789
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	1073741823
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	

Evidence	1073741824
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	1073741825
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	134217727
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	134217728
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	2147483647
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	268435456
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	33554432
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	50123418
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	62914560
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	67108864
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	805306368

URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	00130856
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	00236113
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	00236114
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	00316183
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	04312294
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	06237894
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	06613116
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	06613117
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	09714598
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	09714602
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css

Method	GET
Attack	
Evidence	13670922
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	15074264
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	16464716
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	17852023
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	17983216
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	19177244
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	20623953
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	23004795
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	23205493
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	25339173
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET

Attack	
Evidence	27508006
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	32239492
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	32475606
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	32647608
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	38099726
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	38477624
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	43782037
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	43782038
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	44285278
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	44806278
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	

Evidence	45430875
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	50357616
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	57956202
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	62639628
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	67996622
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	68209638
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	83771396
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	0123456789
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	1073741823
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	1073741824
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	1073741825

URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	134217727
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	134217728
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	2147483647
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	268435456
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	33554432
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	62914560
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	67108864
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	805306368
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	0123456789
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	1073741823
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e

Method	GET
Attack	
Evidence	1073741824
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	1073741825
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	134217727
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	134217728
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	268435456
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	33554432
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	62914560
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	67108864
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET
Attack	
Evidence	805306368
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	19560932
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET

Attack	
Evidence	47871502
URL	https://static.idp.int.identitysandbox.gov/packs/js/29-ed45901c.js
Method	GET
Attack	
Evidence	0123456789
URL	https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.js
Method	GET
Attack	
Evidence	2146823252
Instances	120
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregat
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	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.
URL	https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=GSA&subagency=TTS
Method	GET
Attack	
Evidence	
URL	https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=VA
Method	GET
Attack	
Evidence	
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/embed.js
Method	GET
Attack	
Evidence	
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.css
Method	GET
Attack	

Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/bitter-bold.woff2
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/fa-solid-900.woff2
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/sourcesanspro-bold-webfont.woff2
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/sourcesanspro-regular-webfont.woff2
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.css
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/style.css
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.css

Method	GET
Attack	
Evidence	
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.entry.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/assets/application-f1ba59207acdfe21cd1ccba9a593337f182efe5d400b8c86ce5b7c72951bd440.css
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/assets/identity-style-guide/dist/assets/fonts/roboto-mono/roboto-mono-v5-latin-700-e6d54686857c5d34a85b527fc19fd2ff437bded88b72171651e9eace36f5e99c.woff2
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/assets/public-sans/PublicSans-Bold-0f085885a00b3aabf7d06531c6d5b28437491dcc3e034d5aa9d4b95f9c8df447.woff
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/assets/public-sans/PublicSans-Bold-9191c15dec4a2ea55d3e870cf678e011a5ce88ffa2840a4641bbe0ea53669468.woff2
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/assets/public-sans/PublicSans-Regular-03f263d0e3a5ddc6f6ff0d7d0fe3bc009468b04db10f25f89d56508ff2cc4c66.woff
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/assets/public-sans/PublicSans-Regular-ef3013af0f5807190388435430e1942d249f8e2c462c6db67406532d17c64aa6.woff2
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/29-ed45901c.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/30-1a6066ea.js
Method	GET

Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.en.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/countdown_component-153bd7bd.en.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/countdown_component-153bd7bd.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.en.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/one-time-code-input-f050e903.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/saml-post-96dc0778.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/session-expire-session-0704b440.js
Method	GET
Attack	
Evidence	
URL	https://static.idp.int.identitysandbox.gov/packs/js/session-timeout-ping-a1fe05f2.js
Method	GET
Attack	

Evidence	
Instances	34
Solution	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.
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	**Charset Mismatch (Header Versus Meta Charset)**
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https%3A%2F%2Fssoe-sp-staging.va.gov&cspKey=logingov3&appName=VA+gov+%28vagov%29&cspName=LOGIN.GOV&cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/ial/1&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/aal/2&AuthnContextComparison=minimum&ForceAuthn=false
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https%3A%2F%2Fssoe-sp-staging.va.gov&cspKey=logingov3&appName=VA+gov+%28vagov%29&cspName=LOGIN.GOV&cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/ial/2&AuthnContextClassRef=http://idmanagement.gov/ns/assurance/aal/2
Method	GET
Attack	
Evidence	
Instances	2
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matc

URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	from
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	query
URL	https://resource.digital.voice.va.gov/wdcvoice/5/onsite/generic1645720786527.js
Method	GET
Attack	
Evidence	user
URL	https://sqa.eauth.va.gov/accessva/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	from
URL	https://sqa.eauth.va.gov/accessva/resources/js/gov/va/accessva/common.js
Method	GET
Attack	
Evidence	from
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	db
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	username
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	bug
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	bugs
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	from
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js

Method	GET
Attack	
Evidence	later
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	select
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	TODO
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	user
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	where
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	user
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	user
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/auth.entry.js
Method	GET
Attack	
Evidence	bug
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/static-pages.entry.js
Method	GET
Attack	
Evidence	bug
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/vendor.entry.js
Method	GET
Attack	
Evidence	bug
URL	https://staging-va-gov-assets.s3-us-gov-west-1.amazonaws.com/generated/web-components.e
Method	GET

Attack	
Evidence	bugs
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	from
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	select
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	user
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	from
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	select
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	user
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	select
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	todo
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	user
URL	https://staging.va.gov/generated/7345.entry.js
Method	GET
Attack	

Evidence	query
URL	https://staging.va.gov/generated/7461.entry.js
Method	GET
Attack	
Evidence	from
URL	https://staging.va.gov/generated/announcements-widget.entry.js
Method	GET
Attack	
Evidence	from
URL	https://staging.va.gov/generated/facility-detail.entry.js
Method	GET
Attack	
Evidence	query
URL	https://static.idp.int.identitysandbox.gov/packs/js/29-ed45901c.js
Method	GET
Attack	
Evidence	select
URL	https://static.idp.int.identitysandbox.gov/packs/js/application-d24f19db.js
Method	GET
Attack	
Evidence	select
URL	https://static.idp.int.identitysandbox.gov/packs/js/form-validation-615952bb.js
Method	GET
Attack	
Evidence	from
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	from
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	from
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	FROM
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET

Attack	
Evidence	from
Instances	41
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	**Loosely Scoped Cookie**
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope.Th
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/broker?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva_widget.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/accessva_widget.css
Method	GET
Attack	

Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap-formhelpers.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap-formhelpers.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrap.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrapValidator.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/css/bootstrapValidator.min.css
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/bootstrap.min.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/gov/va/accessva/common.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/gov/va/accessva/common.js
Method	GET
Attack	
Evidence	

URL	https://sqa.eauth.va.gov/accessva/resources/js/isam-oauth/saml.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/isam-oauth/saml.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/isam-oauth/saml.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-1.11.0.min.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/resources/js/jquery-ui-1.10.4.js
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	

Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.in
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/scripts/login.js
Method	GET
Attack	
Evidence	
URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/keepalive
Method	HEAD
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20idp/saml20/login
Method	POST
Attack	
Evidence	

URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/login
Method	POST
Attack	
Evidence	
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	
Instances	41
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Tes http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
CWE Id	565
WASC Id	15
Plugin Id	90033

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and pro
URL	https://idp.int.identitysandbox.gov/?request_id=4240f52f-85bc-46af-9ab6-87f1bf9856e7
Method	GET
Attack	
Evidence	no-store
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022?SAMLRequest=PHNhbWxwOkF1dGhuUr 0Ac2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5lj5odHRwczov 0APjxkczpUcmFuc2Zvcm1zPjxkczpUcmFuc2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8vd3d3Lncz 0AcGRDTWJzYzJVdE9TdlhrN2V0ZmtWOWFOaFdRU2RiMVZyZz08L2RzOkRpZ2VzdFZhbHV 0AQVZDc0JoTmExbFJtL0dwSGQ2a0tYQmlLN2lsdm5ZTS9zSHNXcW1qVCs5ZWY4Y3BlZmo4 0AREJQTVFzd0NRWURWUVFHRXdKVlV6RVZNQk1HQTFVRUNoTU1SR2xuYVVObGNuUW 0ASWFkb0toOHcxV295dUUrYzg2V1JWUkhsZVc1eU50VkVzV0dhcERya2NOeDZXVCs4SFgxl 0AQjNBcERINXdiNlUvSnoyNlptN0xmTXZWOUtqV3VJRFo3Y2V3V0d6MFBCRjM3VGlxdHdQY 0AYVdkcFEyVnlkRlJNVTFKVFFWTklRVEkxTmpJd01qQkRRVEV0TkM1amNtd3dRS0Erb0R5R 0ATUxXaWlXbjA4MzBSTEVGMHZ2MUp1SVdyOHZ4dy9tMUhBQUFCZkYwb1BPZ0FBQVFEQ 0D%0AQW1QU3kxbXMrcjB3RFFZSktvWklodmNOQVFFTEJRQURnZ0VCQUZZRHJ1aTBzUD 0AUG9saWN5IEFsbG93Q3JlYXRlPSJmYWxzZSIgRm9ybWF0PSJ1cm46b2FzaXM6bmFtZXM
Method	GET
Attack	
Evidence	no-store
URL	https://idp.int.identitysandbox.gov/login/two_factor/authenticator
Method	GET
Attack	
Evidence	no-store
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https%3A%2F%2Fssoe-sp-staging.va.gov&A

Method	GET
Attack	
Evidence	no-cache
URL	https://sqa.eauth.va.gov/accessva/?cspSelectFor=https://ssoe-sp-staging.va.gov&AuthnContext
Method	GET
Attack	
Evidence	no-cache
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/accessva/widget_confirm_redirect_508?cancelJustCloses&appId=https
Method	GET
Attack	
Evidence	
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https%3A%2F%2Fssoe-sp-staging.va.gov&SSORequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sPSJ1cm46b2FzaX2BPHNhbWxwOk5hbWVJRFBvbGljeSBBbGxvd0NyZWF0ZT0idHJ1ZSIgRm9ybWF0PSJ1cm462BPC9zYW1scDpBdXRoblJlcXVlc3Q%2B&AuthnContext=PHNhbWxwOlJlcXVlc3RlZEF1dGhu
Method	GET
Attack	
Evidence	no-cache
URL	https://sqa.eauth.va.gov/isam/sps/auth?PartnerId=https://ssoe-sp-staging.va.gov
Method	GET
Attack	
Evidence	no-cache, no-store
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	no-cache, no-store
URL	https://sqa.eauth.va.gov/isam/sps/saml20sp/saml20/logininitial?ITFIM_WAYF_IDP=https://idp.i
Method	GET
Attack	
Evidence	no-cache, no-store
URL	https://staging-api.va.gov/v0/feature_toggles?&cookie_id=c3otfeviavlm3wn7vtly1
Method	GET
Attack	
Evidence	no-cache, no-store
URL	https://staging-api.va.gov/v0/user
Method	GET
Attack	
Evidence	

URL	https://staging-api.va.gov/v1/sessions/logingov/new
Method	GET
Attack	
Evidence	no-cache, no-store
URL	https://staging.va.gov/
Method	GET
Attack	
Evidence	public, no-cache
URL	https://staging.va.gov/?next=loginModal&postLogin=true
Method	GET
Attack	
Evidence	public, no-cache
URL	https://staging.va.gov/auth/login/callback?type=logingov
Method	GET
Attack	
Evidence	public, no-cache
URL	https://idp.int.identitysandbox.gov/api/saml/auth2022
Method	POST
Attack	
Evidence	no-store
URL	https://idp.int.identitysandbox.gov/api/saml/authpost2022
Method	POST
Attack	
Evidence	no-store
URL	https://staging-api.va.gov/v1/sessions/callback
Method	POST
Attack	
Evidence	no-cache, no-store
Instances	20
Solution	Whenever possible 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/Headers/Cache-Control
CWE Id	525
WASC Id	13
Plugin Id	10015