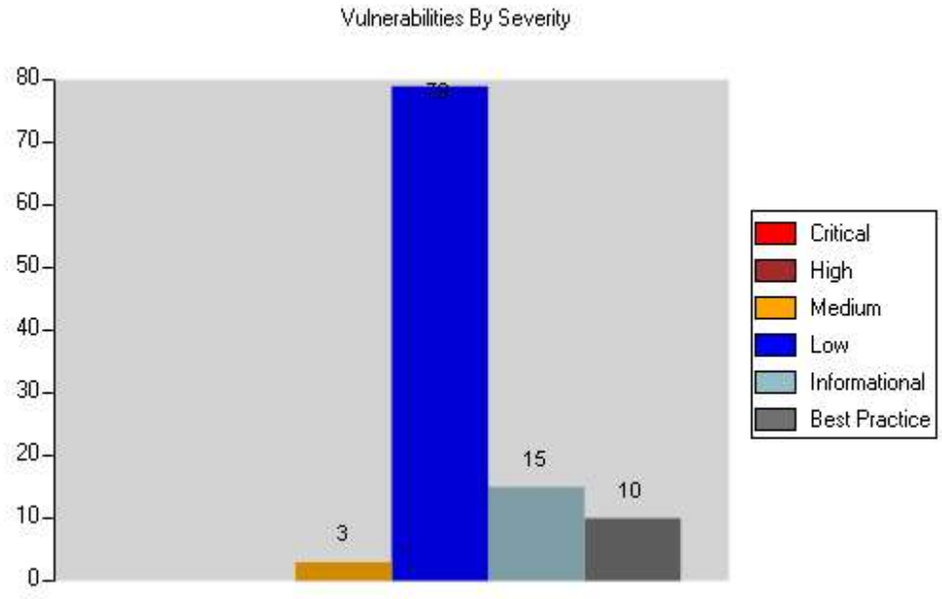
Micro Focus WebInspect

Vulnerability (Legacy)

Web Application Assessment Report

Scan Name:	CX-MarketPlace - 7-18-2019		
Policy:	OWASP Top 10 2017 - (OWASP 2017)	**Crawl Sessions:**	52
Scan Date:	7/18/2019 3:54:42 PM	**Vulnerabilities:**	82
Scan Version:	19.1.0.311	**Scan Duration:**	3 hours : 1 Minute
Scan Type:	Site	**Client:**	FF

Server: https://mot.deltadentalins.com:443



Medium **Cookie Security: Cookie not Sent Over SSL**

Summary:

This policy states that any area of the website or web application that contains sensitive information or access to privileged functionality such as remote site administration requires that all cookies are sent via SSL during an SSL session. The URL: https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA has failed this policy. If a cookie is marked with the "secure" attribute, it will only be transmitted if the communications channel with the host is a secure one. Currently this means that secure cookies will only be sent to HTTPS (HTTP over SSL) servers. If secure is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

Fix:

For Development:
This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your development environment.

For Security Operations:

IIS 4.0 and 5.0 Fix Information:
http://support.microsoft.com/default.aspx?scid=kb;en-us;274149

Remediation for IIS 6.x:
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0d49cbc8-10e1-4fa8-ba61-c34e524a3ae6.mspx?mfr=true
http://msdn2.microsoft.com/en-us/library/ms998310.aspx

Require SSL for an Authentication Cookie (IIS 7):
http://technet.microsoft.com/en-us/library/cc771633(WS.10).aspx

AnonymousIdentificationSection Class [IIS 7]:
http://msdn.microsoft.com/en-us/library/ms689482.aspx

Use the following links to remediate this issue on an Apache server:
http://search.cpan.org/~jkrasnoo/ApacheCookieEncrypted-0.03/Encrypted.pm
http://hc.apache.org/httpclient-3.x/apidocs/org/apache/commons/httpclient/class-use/Cookie.html

For QA:
This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your testing environment.

Reference:

General Information:
The Unofficial Cookie FAQ

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%
2FQ; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-
b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 22:55:18 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2661286922.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/

<!DOCTYPE html>
<html lang="en">
<head>
  ...TRUNCATED...
```

File Names:
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Medium

Insecure Deployment: OpenSSL

Summary:

WebInspect has detected an SSL/TLS man-in-the-middle (MitM) vulnerability caused by a specially crafted SSL handshake message. Also known as OpenSSL ChangeCipherSpec (CCS) injection vulnerability, this bug is known to manifest in the OpenSSL implementation of the secure socket layer for versions earlier than 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h. A ChangeCipherSpec message signals peers to switch to a symmetric encryption during SSL handshake process after negotiating a master key to use for symmetric encryption. However, vulnerable versions of OpenSSL allow a CCS message before the master key is negotiated resulting in a zero length master key.

Execution:

To verify the vulnerability, determine the version of the OpenSSL library deployed on the application servers. The version information can be obtained by running the command openssl version. Note that the client needs to be directly connected to the server in order to test for the vulnerability. If a proxy server is present in the environment, it is recommended to test both the proxy and the application server for the vulnerability.

Implication:

Man-in-the-middle attackers may use this vulnerability to hijack and intercept secure SSL/TLS communication by issuing an early CCS message to client and server when both are using vulnerable instance of OpenSSL. This may allow the attacker to compromise the confidentiality of sensitive session data.

Fix:

Upgrade to latest OpenSSL version.

- OpenSSL 0.9.8 SSL/TLS users should upgrade to 0.9.8za or later.
- OpenSSL 1.0.0 SSL/TLS users should upgrade to 1.0.0m or later.
- OpenSSL 1.0.1 SSL/TLS users should upgrade to 1.0.1h or later.

Additionally, users should check for the possibility of an indirect dependency on the OpenSSL library via third party software. Upgrade any such instances according to vendor recommendations.

Reference:

- https://www.openssl.org/news/secadv_20140605.txt
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224

Attack Request:

GET /shopping/js/html5shiv-40bd440d29.min.js HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/shopping/delta/get-a-quote?issuerCode=DELTA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000; TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a4562a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b36261d1; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBilT3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+ZojyfeefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrUlfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9zwR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2Iqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:53 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 12 Jul 2019 22:07:28 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 2730
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie: TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a4562a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b36261d1; Path=/

/**
* @preserve HTML5 Shiv 3.7.3 | @afarkas @jdalton @jon_neal @rem | MIT/GPL2 Licensed
*/

!function(a,b){function c(a,b){var c=a.createElement("p"),d=a.getElementsByTagName("head")[0]
||a.documentElement;return c.innerHTML="x<style>"+b+"</style>",d.insertBefore(c.lastChild,d.firstChild)}function d(){var
a=t.elements;return"string"==typeof a?a.split(" "):a}function e(a,b){var c=t.elements;"string"!=typeof c&&(c=c.join("
")),"string"!=typeof a&&(a=a.join(" ")),t.elements=c+" "+a,j(b)}function f(a){var b=s[a[q]];return b||(b={},r++,a[q]=r,s[r]
=b),b}function g(a,c,d){if(c||(c=b),l)return c.createElement(a);d||(d=f(c));var e;return e=d.cache[a]?d.cache[a].cloneNode
():p.test(a)?(d.cache[a]=d.createElem(a)).cloneNode():d.createElem(a),!e.canHaveChildren||o.test(a)||e.tagUrn?
e:d.frag.appendChild(e)}function h(a,c){if(a||(a=b),l)return a.createDocumentFragment();c=c||f(a);for(var
e=c.frag.cloneNode(),g=0,h=d(),i=h.length;i>g;g++)e.createElement(h[g]);return e}function i(a,b){b.cache||(b.cache=
{},b.createElem=a.createElement,b.createFrag=a.createDocumentFragment,b.frag=b.createFrag()),a.createElement=function
(c){return t.shivMethods?g(c,a,b):b.createElem(c)},a.createDocumentFragment=Function("h,f","return function(){var
n=f.cloneNode(),c=n.createElement;h.shivMethods&&("+d().join().replace(/[\w\-:]+/g,function(a){return b.createElem
(a),b.frag.createElement(a),'c("'+a+'")'})+");return n}")(t,b.frag)}function j(a){a||(a=b);var d=f(a);return!
t.shivCSS||k||d.hasCSS||(d.hasCSS=!!c(a,"article,aside,dialog,figcaption,figure,footer,header,hgroup,main,nav,section
{display:block}mark{background:#FF0;color:#000}template{display:none}")),l||i(a,d),a}var k,l,m="3.7.3",n=a.html5||
{},o=/^<|^(?:button|map|select|textarea|object|iframe|option|optgroup)$/i,p=/^
(?:a|b|code|div|fieldset|h1|h2|h3|h4|h5|h6|i|label|li|ol|p|q|span|strong|style|table|tbody|td|th|tr|ul)
$/i,q="_html5shiv",r=0,s={};!function(){try{var a=b.createElement("a");a.innerHTML="<xyz></xyz>",k="hidden"in
a,l=1==a.childNodes.length||function(){b.createElement("a");var a=b.createDocumentFragment
();return"undefined"==typeof a.cloneNode||"undefined"==typeof a.createDoc
umentFragment||"undefined"==typeof a.createElement}()}catch(c){k=!0,l=!0}}();var t={elements:n.elements||"abbr article
aside audio bdi canvas data datalist details dialog figcaption figure footer header hgroup main mark meter nav output picture
progress section summary template time video",version:m,shivCSS:n.shivCSS!==!
1,supportsUnknownElements:l,shivMethods:n.shivMethods!==!
1,type:"default",shivDocument:j,createElement:g,createDocumentFragment:h,addElements:e};a.html5=t,j
(b),"object"==typeof module&&module.exports&&(module.exports=t)}("undefined"!=typeof window?window:this,document);

File Names:

- https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js

Medium

Insecure Transport: Weak SSL Protocol

Summary:

Fortify WebInspect has detected support for Transport Layer Security Protocol (TLS) 1.1 protocol on the target server. NIST publication 800-52 revision 1 recommends all web applications to prefer Transport Layer Security Protocol version 1.2 (TLS 1.2) and mandates government agencies to develop a migration plan for TLS1.2 by January 2015. TLS1.1 mandates a combination of MD5 and SHA1 for the hash function, which leads to conclusion that strength of TLS1.1 depends largely on the strength of SHA1. MD5 is generally known to be weak. SHA1 use is being phased out. NIST Special Publication 800-131A deprecated the use of SHA-1 in digital signature starting January 2014.

Execution:

The list of supported SSL/TLS protocols can be obtained by running the server analyzer tool from Fortify Security Toolkit supplied with Fortify WebInspect against the target server.

Implication:

Weak TLS/SSL protocols may exhibit any or all of the following properties:

- No protection against man-in-the-middle (MitM) attacks
- Same key used for authentication and encryption
- Weak message authentication control
- No protection against TCP connection closing

These properties can allow an attacker to intercept, modify and tamper with sensitive data.

Fix:

Have a migration plan in place for all sites to exclusively use TLS1.2 and above. Disable support for the TLS 1.1 protocol on the server. Instead, TLSv1.2 and above should be used.

- For Apache, modify the following lines in the server configuration
- SSL Protocol ALL –SSLv2 -SSLv3 -TLSv1 –TLSv1.1
- For Nginx, modify the following lines in server configuration:
- SSL_Protocols TLSv1.2

- For IIS, please refer to Microsoft Knowledge Base Articles:

- https://technet.microsoft.com/library/security/3009008

For other servers, please refer to vendor specific documentation.

Reference:

NIST Special Publication 800-131A
NIST Special Publication 800-52r1

Attack Request:

GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%
2FQ; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-
b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 22:55:18 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2661286922.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/


```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <meta http-equiv="X-UA-Compatible" content="IE=edge" />
   <title>Get A Quote</title>

   <!-- Page-hiding snippet (recommended)  -->
   <style>.async-hide { opacity: 0 !important} </style>
   <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
      h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
      (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
   })(window,document.documentElement,'async-hide','dataLayer',4000,
```

```
        {'GTM-NPRVDTC':true});</script>
    <!-- Modified Analytics tracking code with Optimize plugin -->
    <script type="text/javascript">
        (function(i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r;
            i[r] = i[r] || function() {
                    (i[r].q = i[r].q || []).push(arguments)
                }, i[r].l = 1 * new Date();
            a = s.createElement(o), m = s.getElementsByTagName(o)[0];
            a.async = 1;
            a.src = g;
            m.parentNode.insertBefore(a, m)
        })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
        ga('create', 'UA-9398012-1', 'auto');
        ga('require', 'GTM-NPRVDTC', 'auto');
        var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
        ga('set', 'dimension9', dnt);
        ga('send', 'pageview');
    </script>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-00239ae0e5.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
            <header class="shopping-header-title">

                                        <a class="back-arrow-link" id="shoppingBack"
href="https://mot.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                                    <div class="main-content">
                                        <h1 class="shopping-header-content">
                                                Get a Quote
                                        </h1>
                                    </div>
                                    </header>


<main role="main" class="main-content container page-control get-a-quote">
  <div class="main-container-inner">
    <div class="top-heading-section">
        <div class="error-container global-margin">
        </div>
      <div class="summary grey-text">
        We need a little more information to give you a quote.
      </div>
    </div>
    <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
      <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
         <label for="zip"   >What

...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Low

Cookie Security: HTTPOnly not Set

Summary:

The web application does not utilize HTTP only cookies. This is a new security feature introduced by Microsoft in IE 6 SP1 to mitigate the possibility of a successful Cross-Site scripting attack by not allowing cookies with the HTTP only attribute to be accessed via client-side scripts. Recommendations include adopting a development policy that includes the utilization of HTTP

only cookies, and performing other actions such as ensuring proper filtration of user-supplied data, utilizing client-side validation of user supplied data, and encoding all user supplied data to prevent inserted scripts being sent to end users in a format that can be executed.

Reference:

References:
https://social.msdn.microsoft.com/Search/en-US?query=HTTPOnly%20Cookie&emptyWatermark=true&ac=5

Attack Request:

GET /enroll/js/zippopupsingle-17eac51cc4.js HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache

Cookie: ADRUM_BT=R:116|i:2050|g:f9e47ca0-5b58-468d-bba5-6621489693799858|e:-nan|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000; TS01d1e64c=01729bd698f45abe959d34b69c298df56a4295206a537fb63d31b5acd0749beed29aa3abe0416dcf85ba6b4069ff2fd72f2e1361088d78011c76db0d186db3cfd260ee536bdc47e52830c81ee6789a68b4cc4f5aeaca82b72ae7119c410a1a1959dd60def8; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1563490501836%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1563490776381%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA~1563490790452%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA%26planEffectiveDate%3D8%2F15%2F2019~1563490797421; TS018e8e3c=01729bd698350341c79702fd652cb89a27951cd890404ef3a01486cadec575fb339b19b25b0078f2d62bd04be799146b98d1079c79f323bed30d0f5710ec9c493c25e09027; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18096%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1564095295%7C9%7CMCAAMB-1564095295%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1563497695s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBilT3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+ZojyfeefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrUlfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9zwR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy; _gid=GA1.2.1908194059.1563490494; _gat=1; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true; s_sq=deltadentalcaddinsstage%3D%2526c.%2526a.%2526activitymap.%2526page%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fshopping%25252Fdelta%25252Fplan-options%25252F11048636%25253FissuerCode%25253DDELTA%252526planEffectiveDate%25253D8%25252F15%25252F2019%2526link%253DBuy%252520Plan%2526region%253DbuyPlan%2526.activitymap%2526.a%2526.c%2526pid%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fshopping%25252Fdelta%25252Fplan-options%25252F11048636%25253FissuerCode%25253DDELTA%252526planEffectiveDate%25253D8%25252F15%25252F2019%2526oid%253DBuy%252520Plan%2526oidt%253D3%2526ot%253DSUBMIT%2526oi%253D59; ADRUM=s=1563490798933&r=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3F-223145629;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:59:59 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 15 Jul 2019 17:49:58 GMT
Accept-Ranges: bytes

Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 327
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS018e8e3c=01729bd698350341c79702fd652cb89a27951cd890404ef3a01486cadec575fb339b19b25b0078f2d62bd04be799146b98d1079c79f323bed30d0f5710ec9c493c25e09027; Path=/

"use strict";
// Zipcode change notification ...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/js/zippopupsingle-17eac51cc4.js
- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/enroll/js/ddAnalyticsHooks-d23401eeab.js
- https://mot.deltadentalins.com:443/enroll/js/ddWebAnalytics-144c7eb39b.js
- https://mot.deltadentalins.com:443/enroll/js/validation-b8bdcabe8c.js
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/js/jquery-3b5470c70d.mask.min.js
- https://mot.deltadentalins.com:443/shopping/js/planDetails-31a18623f9.js
- https://mot.deltadentalins.com:443/enroll/js/es5-shim-136920ce3d.min.js
- https://mot.deltadentalins.com:443/shopping/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/shopping/js/es5-shim-136920ce3d.min.js
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/shopping/js/common-972ff0042e.js
- https://mot.deltadentalins.com:443/enroll/js/payment-2f2f93c856.js
- https://mot.deltadentalins.com:443/enroll/js/common-e61e276d1a.js
- https://mot.deltadentalins.com:443/enroll/delta/dependents
- https://mot.deltadentalins.com:443/enroll/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/enroll/js/additional-methods-d95f4f840a.min.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-36917469dc.validate.min.js
- https://mot.deltadentalins.com:443/enroll/delta/review
- https://mot.deltadentalins.com:443/enroll/js/receipt-29d5b827f2.js
- https://mot.deltadentalins.com:443/shopping/js/ddAnalyticsHooks-d23401eeab.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/11048636?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/js/jquery-ab3696dee1.payment.js
- https://mot.deltadentalins.com:443/enroll/delta/receipt
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/enroll/js/personal-info-5e7db54b46.js
- https://mot.deltadentalins.com:443/shopping/js/planOptions-d79e83ab18.js
- https://mot.deltadentalins.com:443/enroll/js/dependents-58d3246a95.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-24ae1ca673.validate.min.js
- https://mot.deltadentalins.com:443/enroll/js/review-83be065106.js
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/shopping/js/additional-methods-0a2ac4c9f1.min.js

- https://mot.deltadentalins.com:443/shopping/js/ddWebAnalytics-144c7eb39b.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/js/feedback-d3abf5fee6.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-3b5470c70d.mask.min.js
- https://mot.deltadentalins.com:443/shopping/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/shopping/js/getAQuote-ad773bf537.js
- https://mot.deltadentalins.com:443/shopping/js/validation-041e807db4.js
- https://mot.deltadentalins.com:443/enroll/js/mot-adrum-05508bc7fe.js

---

Low **Web Server Misconfiguration: Server Error Message**

Summary:

A server error response was detected. The server could be experiencing errors due to a misbehaving application, a misconfiguration, or a malicious value sent during the auditing process. While error responses in and of themselves are not dangerous, per se, the error responses give attackers insight into how the application handles error conditions. Errors that can be remotely triggered by an attacker can also potentially lead to a denial of service attack or other more severe vulnerability. Recommendations include designing and adding consistent error handling mechanisms which are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Implication:

The server has issued a 500 error response. While the body content of the error page may not expose any information about the technical error, the fact that an error occurred is confirmed by the 500 status code. Knowing whether certain inputs trigger a server error can aid or inform an attacker of potential vulnerabilities.

Fix:

For Security Operations:

Server error messages, such as "File Protected Against Access", often reveal more information than intended. For instance, an attacker who receives this message can be relatively certain that file exists, which might give him the information he needs to pursue other leads, or to perform an actual exploit. The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any server error message that is presented.

- Uniform Error Codes: Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- Informational Error Messages: Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- Proper Error Handling: Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

Removing Detailed Error Messages

Find instructions for turning off detailed error messaging in IIS at this link:

http://support.microsoft.com/kb/294807

For Development:

From a development perspective, the best method of preventing problems from arising from server error messages is to adopt secure programming techniques that prevent problems that might arise from an attacker discovering too much information

about the architecture and design of your web application. The following recommendations can be used as a basis for that.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad. Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.
- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

For QA:

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker? Inconsistent methods of dealing with errors gives an attacker a very powerful way of gathering information about your web application.

Reference:

Apache:
Security Tips for Server Configuration
Protecting Confidential Documents at Your Site
Securing Apache - Access Control

Microsoft:
How to set required NTFS permissions and user rights for an IIS 5.0 Web server
Default permissions and user rights for IIS 6.0
Description of Microsoft Internet Information Services (IIS) 5.0 and 6.0 status codes

Attack Request:

```
GET /enroll/delta/PRbjx^bx^bxeeibbbfdeRP/etc/passwd HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/dependents
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=19.1.0.311
X-Scan-Memo: Category="Audit.Attack"; SID="92936476ECEA1BDD668312D20BB7F778";
PSID="A356F523E100A47B16D1CBF1D86793C8"; SessionType="AuditAttack"; CrawlType="None";
AttackType="UrlComponentManipulation"; OriginatingEngineID="04922161-c0f3-47ba-8adf-397348373fed";
AttackSequence="1"; AttackParamDesc=""; AttackParamIndex="-1"; AttackParamSubIndex="0"; CheckId="11362";
Engine="Struts+Class+Loader+Manipulation"; SmartMode="NonServerSpecificOnly"; AttackString="";
AttackStringProps="Attack"; ThreadId="366"; ThreadType="AuditorStateRequestor";
X-RequestManager-Memo: sc="1"; ID="67fb38ed-882e-4522-8fbf-47f98a6b04ae";
X-Request-Memo: ID="25a90807-4524-4f4c-bc1b-b937f5cd7aea"; sc="1"; tid="366";

Cookie: ADRUM_BT=R:54|i:2050|g:f9e47ca0-5b58-468d-bba5-6621489693799865|e:2522|n:MOT_a5878d08-57da-4244-b352
-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-
L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000;
TS01d1e64c=01729bd698f45abe959d34b69c298df56a4295206a537fb63d31b5acd0749beed29aa3abe0416dcf85ba6b4069ff2f
d72f2e1361088d78011c76db0d186db3cfd260ee536bdc47e52830c81ee6789a68b4cc4f5aeaca82b72ae7119c410a1a1959dd60d
ef8; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%
3DDELTA~1563490501836%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%
3FissuerCode%3DDELTA~1563490776381%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-
options%2F11048636%3FissuerCode%3DDELTA~1563490790452%7Chttps%3A%2F%2Fmot.deltadentalins.com%
2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA%26planEffectiveDate%3D8%2F15%
2F2019~1563490797421%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fpersonal-
info~1563490807979%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fdependents~1563490931761;
TS018e8e3c=01729bd69889a85abdca332e028460aa553817c5f0404ef3a01486cadec575fb339b19b25b47badd9e28d1f0098f3c
b68cbeaf64981b777ca04f47843b6249450c73b46563; _ga=GA1.2.1222917316.1517435630;
AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18096%7CMCMID%
7C22137510049759883710112622098244936722%7CMCAAMLH-1564095295%7C9%7CMCAAMB-1564095295%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1563497695s%7CNONE%7CvVersion%
```

7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDC
bTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrUlfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/
EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9zwR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6ow
P5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy; _gid=GA1.2.1908194059.1563490494; _gat=1;
AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true; s_sq=deltadentalcaddinsstage%3D%2526c.%2526a.%
2526activitymap.%2526page%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%
25252Fdependents%2526link%253DNext%2526region%253Ddependent_form%2526.activitymap%2526.a%2526.c%
2526pid%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Fdependents%
2526oid%253DNext%2526oidt%253D3%2526ot%253DSUBMIT%2526oi%253D77; ADRUM=s=1563490933512&r=https%
3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fdependents%
3F0;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 500 Internal Server Error
Date: Thu, 18 Jul 2019 23:...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxeeibbbfdeRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxcabffaaceiRP/etc/passwd
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxcahggeiabcRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/PRbjx^bx^bxcfjbijfcgeRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxdhdjgccbgiRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxhhdccgfjhRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/enroll/delta/dependents
- https://mot.deltadentalins.com:443/enroll/delta/receipt
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxicafbfccaRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/delta/review
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=%60
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/?class.classLoader.resources.context.
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/11048636?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxdahfbhcfecRP/etc/passwd
- https://mot.deltadentalins.com:443/enroll/delta/PRbjx^bx^bxdcccbibhjdRP/etc/passwd

Low

Setting Manipulation: Character Set

Summary:

A vulnerability was detected in your web application that allows a user to control the HTML character encoding used to parse the HTTP response of a given request. Attackers can exploit this vulnerability to evade certain validation mechanisms used for Cross-site Scripting.
The response character encoding is used by a web browser to decide how to interpret the characters in the body of the HTTP response. The most common encoding used by web applications today is UTF-8. The character set (charset) declaration is usually done through a header in the HTTP response or using the HTML <meta> tag. Such declarations should be controlled by the application only. If this declaration is controlled through user input, then an attacker can use this feature to modify the charset that will be used by the browser and modify the interpretation of the contents of the response. This can allow for Cross-site Scripting attacks that would otherwise not have succeeded while using UTF-8 encoding.

Execution:

This vulnerability is detected by modifying an input parameter value in an HTTP request to a different charset. The headers and the HTML <meta> tag of the corresponding HTTP response are then observed to confirm a successful manipulation of the response charset.

Implication:

A successful exploitation of this vulnerability could increase the probability of a successful Cross-site Scripting attack by evading existing server-side input validation routines.
For example:

```
+ADw-script+AD4-alert(document.location)+ADw-/script+AD4
```

The above string means nothing in most encoding types, and therefore is "safe", but when a victim views this under utf-7 encoding, it will be interpreted as valid html tag and hence, the script will be executed.

Fix:

The ideal solution would be to control charset declarations from the application and never through user-supplied input. If a particular feature of the application demands such a capability, then it is advisable to use a white list of allowed charsets and validate that proper input validation routines are in place for all the values in the white list.

Reference:

Browser Security Handbook
Computer Security Research - Secunia
Maia Mailguard 'charset' Parameter HTML Injection Vulnerability
OWASP Encoding Project

Attack Request:

```
GET /enroll/locale-based/en/US/client-data.json HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: mot.deltadentalins.com
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=19.1.0.311
X-Scan-Memo: Category="Audit.Attack"; SID="A1B2831D48AEB160706F05608CB6FA65";
PSID="B66DADE92E491B58991ECDD11E4DA434"; SessionType="AuditAttack"; CrawlType="None";
AttackType="CookieParamManipulation"; OriginatingEngineID="29fad754-9640-4489-b6cf-91c822ecbd39";
AttackSequence="0"; AttackParamDesc="AMCVS_E9D70FA75B3A18E80A495C49%2540AdobeOrg"; AttackParamIndex="13";
AttackParamSubIndex="0"; CheckId="11550"; Engine="User+Controlled+Charset"; SmartMode="NonServerSpecificOnly";
AttackString="%2522%253e%253cmeta%2520charset%253dutf-8%2520id%253dPRfxbdxaxhcchibhcabcaabfgaicRP%252f%
253e"; AttackStringProps="Attack"; ThreadId="471"; ThreadType="Task";
X-RequestManager-Memo: sid="555"; smi="0"; sc="1"; ID="441f7496-6c32-495f-a051-0c5088a2a595";
X-Request-Memo: ID="48855071-1d92-49a3-8d4a-6fe7dbc9bab1"; sc="1"; tid="99";
Cookie:  connect.sid=s%3A-j2JDU8Smn1cRBxsDzijeJTW0is1CKX1.pH9jaNUXS5cinUOihAadVwrLG5%2F0xMY%2F2m%
2BrskID5WI; mot-ddins=2694841354.64288.0000;
TS01d1e64c=01729bd698a3d723bcacdac8f911ae5452a84db64202c56ba4a0677a9eea0ca3ef98dfb0b476cb46bcec616a97431e
d6ccaa4369cd551b09bb6fd0c7f61f4edf7bd70eb33e1946b715e4bdc3d5e773be940d1901b9357a5e28e410c7a2d9e85a3ca5d73
a39;
TS018e8e3c=01729bd6980de97bb3b0f73540ed437a2ef46afdaa1e5545c368fbe99a53e9f964934609055d5026b7785612434b6
3981e3cf4a4d484580e4009e7f62e38af9e8e11c548c3; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=%22%3e%
3cmeta%20charset%3dutf-8%20id%3dPRfxbdxaxhcchibhcabcaabfgaicRP%2f%
3e;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0;TS0132dfbe=01729bd698d5842dd76
4413ce7ceff50789fb93b13ab2bc6c07f7df35ecfc9f5d187d11dd0d33898eb1b7af18a6de85405de00a19b
```

Attack Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Content-Length: 247

<html><...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json

---

Low **Cache Management: Insecure Policy**

Summary:

WebInspect has detected a potentially unsafe cache control policy for secure content. While content transmitted over an SSL/TLS channel is expected to guarantee confidentiality, administrators must ensure that caching of sensitive content is disabled unless absolutely needed. The misconception that secure content caching is disabled by default by user-agents could

cause the application to fail the organization's cache policy. An unsafe specification such as Cache-Control: public instructs the browser to persistently cache the content on the hard drive. Cache-Control with no-store in the value must be set to prevent browsers from persisting content. Browsers and intermediate proxies will still persists with the no-cache directive. However, they will revalidate the content with the server before serving content from cache. The private directive prevents intermediate proxies from caching content and can be used in addition to no-store. Missing Cache-Control policy header results in browsers caching content regardless of whether it is served over HTTP or HTTPS.

- Cache-Control: no-store

Execution:

Send a request to https://mot.deltadentalins.com:443/enroll/delta/dependents and inspect the Cache-Control header value.

Implication:

Insecure caching policies could lead to content spoofing or information theft.

SSL provides secure encrypted channel to transfer information from source to user. The information served over SSL is considered sensitive and trusted to be only available to the requestor. However, caching this content on disk in temporary internet files or on an intermediate proxy server can compromise that trust by exposing it to anyone who has access to the temporary storage or proxy cache. Content served over SSL should have cache disabled.

Fix:

Set the Cache-Control directive to private and no-store.

private
This directive allows the server to prevent a shared cache from caching responses that are intended for a single user. You can use this mechanism to ensure that privileged information is not accidentally leaked to unauthorized users. The directive may still allow caching of responses by non-shared caches.

no-cache
For sensitive resources requiring user authentication, servers can send the no-cache directive to prevent caches from serving a cached response without first requiring the user-agent to validate the user identity. This directive can be specified with or without field names. When no field names are included, this directive applies to the entire request or response.
When one or more field names are specified in the no-cache directive, the response is cached but the specified fields must be excluded. If the response must include the specified field, then the cache must ensure that the request triggers a revalidation with the origin server.
Example: Cache-Control: no-cache="Set-Cookie"
This directive can be used to prevent sensitive information leakage by requiring the server to confirm the user identity before serving the protected information. While content is not served using the browser's history or back button, a user with disk access can retrieve the content.

no-store
To completely disable the caching of requests or responses, the server must specify the no-store directive in the Cache-Control header. This directive applies to the entire request and response regardless of whether the directive is sent in the request or the response.

Reference:

Server Configuration:
IIS
Apache

HTTP 1.1 Specification:
HTTP Header Field Definitions

OWASP:
Browser Cache FAQ

HTTP Caching:
Tutorial

Attack Request:

GET /enroll/delta/dependents HTTP/1.1
Accept: */*
Ref...TRUNCATED...

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 23:02:08 GMT
X...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/delta/dependents

- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/shopping/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/enroll/delta/receipt
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/11048636?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/enroll/delta/review
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA

Low

Web Server Misconfiguration: Insecure Content-Type Setting

Summary:

Almost all browsers are designed to use a mime sniffing technique to guess the content type of the HTTP response instead of adhering to the Content-Type specified by the application in specific cases or ignoring the content when no mime type is specified. Inconsistencies introduced by the mime sniffing techniques could allow attackers to conduct Cross-Site Scripting attacks or steal sensitive user data. WebInspect has determined that the application fails to instruct the browser to strictly enforce the Content-Type specification supplied in the response.

Web server misconfiguration can cause an application to send HTTP responses with the missing Content-Type header or specify a mime type that does not match up accurately with the response content. When a browser receives such a response, it attempts to programmatically determine the mime type based on the content returned in the response. The mime type derived by the browser, however, might not accurately match the one intended by the application developer. Such inconsistencies have historically allowed attackers to conduct Cross-Site Scripting or data theft using Cascading Style Sheets (CSS) by letting them bypass server-side filters using mime type checking and yet have the malicious payload with misleading mime type specification executed on the client-side due to the browser mime sniffing policies.

Microsoft Internet Explorer (IE) introduced the X-Content-Type-Options: nosniff specification that application developers can include in all responses to ensure that mime sniffing does not occur on the client-side. This protection mechanism is limited to Microsoft Internet Explorer versions 9 and above.

Execution:

. Build a test page that includes a reference to an external JavaScript or CSS resource

. Configure the server to return the external resource with an incorrect mime type specification

. Visit the test page using an old version of Microsoft's Internet Explorer (version IE 8) browser

. Interpretation of the external content as JavaScript or CSS by the browser despite the misleading mime type specification indicates a potential for compromise.

Implication:

By failing to dictate the suitable browser interpretation of the response content, application developers can expose their users to Cross-Site Scripting or information stealing attacks.

Fix:

Configure the web server to always send the X-Content-Type-Options: nosniff specification in the response headers. In addition, ensure that following safety precautions are also put in place:

. Verify that the web server configuration will send the accurate mime type information in the Content-Type header of each HTTP response

. Configure the server to send a default Content-Type of text-plain or application/octet-stream to tackle failure scenarios

. Ensure that appropriate Character Set is specified in the Content-Type header

. Configure the server to send Content-Disposition: attachment; filename=name; for content without an explicit content type specification.

Reference:

Microsoft Internet Explorer:
MIME-Handling Change: X-Content-Type-Options: nosniff
MIME-Handling Changes in Internet Explorer

OWASP:
OWASP Testing Guide Appendix D: Encoded Injection
List of Useful HTTP Headers

CSS Data Theft:
CVE-2010-0654

Attack Request:

GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2Iqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3...TRUNCATED...

File Names:
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Low

Insecure Transport: HSTS not Set

Summary:

Http Strict Transport Security (HSTS) policy enables web applications to enforce web browsers to restrict communication with the server over an encrypted SSL/TLS connection for a set period. Policy is declared via special Strict Transport Security response header. Encrypted connection protects sensitive user and session data from attackers eavesdropping on network connection.
Consider following attack scenarios:

- Users often omit the URI scheme i.e. https:// when typing a URL in location bar to access a website. Also third party websites can link to the site using the “http” scheme instead of ""https”. This could result in an initial connection to a HTTPS-enabled site over an unencrypted channel. An eavesdropping attacker can hijack this unencrypted connection and replace the intended use of HTTPS protocol with HTTP in an attack known as SSLStrip, granting unauthorized access to

all subsequent traffic.
- Websites often transfer non-sensitive resources such as help documents over an unencrypted HTTP connection. Any cookies without a secure flag are sent along with such requests potentially disclosing sensitive user and session data to eavesdropper.
- Man-in-the-Middle attacks that exploit user tendencies to override invalid certification warnings, e.g. SSLSniff.

For web sites configured with an accurate HSTS policy, browsers automatically upgrade any HTTP connections to HTTPS. Furthermore, browsers prevent users from overriding any host certificate warnings. HSTS offers an effective defense against above attack scenarios.

Execution:

Access location https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js and notice the absence of the Strict Transport Security header in the HTTP response.

Implication:

A successful MiTM attack such as SSLStrip or SSLsniff can lead to the compromise of sensitive user data such as financial information, Social Security Number, personal information etc. as well as grant unauthorized access to user accounts enabling attackers to perform privileged actions on client's behalf.

Fix:

Configure the web application under test to include Strict Transport Security header in every response generated by an HTTPS -enabled site. Any HTTP version of site on the same domain should permanently redirect to the secure encrypted site. Header should not be added to HTTP response as browsers will ignore it.

It is important to note that this header does not prevent from above mentioned attack scenarios during the very first connection to the site or any connections established after the set period has expired. To prevent such a scenario, the site must be added to the pre-loaded HSTS hosts list embedded in both Google Chrome and Mozilla Firefox browsers.

Reference:

http://tools.ietf.org/html/rfc6797

Attack Request:

GET /shopping/js/html5shiv-40bd440d29.min.js HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/shopping/delta/get-a-quote?issuerCode=DELTA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000; TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a4562a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b36261d1; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBilT3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+ZojyfeefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrUlfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9zwR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:53 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 12 Jul 2019 22:07:28 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public

Content-Length: 2730
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/

/**
* @preserve HTML5 Shiv 3.7.3 | @afarkas @jdalton @jon_neal @rem | MIT/GPL2 Licensed
*/

!function(a,b){function c(a,b){var c=a.createElement("p"),d=a.getElementsByTagName("head")[0]
||a.documentElement;return c.innerHTML="x<style>"+b+"</style>",d.insertBefore(c.lastChild,d.firstChild)}function d(){var
a=t.elements;return"string"==typeof a?a.split(" "):a}function e(a,b){var c=t.elements;"string"!=typeof c&&(c=c.join("
")),"string"!=typeof a&&(a=a.join(" ")),t.elements=c+" "+a,j(b)}function f(a){var b=s[a[q]];return b||(b={},r++,a[q]=r,s[r]
=b),b}function g(a,c,d){if(c||(c=b),l)return c.createElement(a);d||(d=f(c));var e;return e=d.cache[a]?d.cache[a].cloneNode
():p.test(a)?(d.cache[a]=d.createElem(a)).cloneNode():d.createElem(a),!e.canHaveChildren||o.test(a)||e.tagUrn?
e:d.frag.appendChild(e)}function h(a,c){if(a||(a=b),l)return a.createDocumentFragment();c=c||f(a);for(var
e=c.frag.cloneNode(),g=0,h=d(),i=h.length;i>g;g++)e.createElement(h[g]);return e}function i(a,b){b.cache||(b.cache=
{},b.createElem=a.createElement,b.createFrag=a.createDocumentFragment,b.frag=b.createFrag()),a.createElement=function
(c){return t.shivMethods?g(c,a,b):b.createElem(c)},a.createDocumentFragment=Function("h,f","return function(){var
n=f.cloneNode(),c=n.createElement;h.shivMethods&&("+d().join().replace(/[\w\-:]+/g,function(a){return b.createElem
(a),b.frag.createElement(a),'c("'+a+'")'})+");return n}")(t,b.frag)}function j(a){a||(a=b);var d=f(a);return!
t.shivCSS||k||d.hasCSS||(d.hasCSS=!!c(a,"article,aside,dialog,figcaption,figure,footer,header,hgroup,main,nav,section
{display:block}mark{background:#FF0;color:#000}template{display:none}")),l||i(a,d),a}var k,l,m="3.7.3",n=a.html5||
{},o=/^<|^(?:button|map|select|textarea|object|iframe|option|optgroup)$/i,p=/^
(?:a|b|code|div|fieldset|h1|h2|h3|h4|h5|h6|i|label|li|ol|p|q|span|strong|style|table|tbody|td|th|tr|ul)
$/i,q="_html5shiv",r=0,s={};!function(){try{var a=b.createElement("a");a.innerHTML="<xyz></xyz>",k="hidden"in
a,l=1==a.childNodes.length||function(){b.createElement("a");var a=b.createDocumentFragment
();return"undefined"==typeof a.cloneNode||"undefined"==typeof a.createDoc
umentFragment||"undefined"==typeof a.createElement}()}catch(c){k=!0,l=!0}}();var t={elements:n.elements||"abbr article
aside audio bdi canvas data datalist details dialog figcaption figure footer header hgroup main mark meter nav output picture
progress section summary template time video",version:m,shivCSS:n.shivCSS!==!
1,supportsUnknownElements:l,shivMethods:n.shivMethods!==!
1,type:"default",shivDocument:j,createElement:g,createDocumentFragment:h,addElements:e};a.html5=t,j
(b),"object"==typeof module&&module.exports&&(module.exports=t)}("undefined"!=typeof window?window:this,document);

File Names:

- https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js

---

Low

HTML5: Cross-Site Scripting Protection

Summary:

X-XSS-Protection HTTP response header enables developers and security architects to manage browser protection against reflected cross-site scripting. The mechanism is also known as the XSS Auditor in Chrome and the XSS filter in Internet Explorer. In modern browsers, the Content-Security-Policy header can provide better protection against XSS and setting X-XSS-Protection might be redundant. However, this header can reduce the risk of reflected XSS attacks in earlier browsers that do not support CSP.

This header can be set to one of three possible values: `0`, `1`, or `1`; `mode=block` . A value of `0` disables the protection. A value of `1` is the default behaviour in modern browsers that enables the protection in filter or replacement mode. For example, IE replaces JavaScript keywords such as <script> with <scr#pt> to render injected string ineffective. The value of `1` ; `mode=block` instructs browsers to block the response from rendering in the browser. Reports of multiple exploits that leverage false positives from default behaviour that filters or replaces JavaScript injection string within the response r eturned from server. Therefore, the current recommendation is to set the header in block mode.

Execution:

Click the response tab for the highlighted request. The response header X-XSS-Protection is either missing or set to `1`.

By default, WebInspect flags only one instance of this vulnerability per host because it is typical to set this header at the host level in a server configuration.

Perform the following steps to flag all instances of this issue:

- Create a new policy with the selection of checks that you want to include in a rescan. We recommend using the Blank or Passive policy as a base.
- Select this check and unselect the check input, “FlagAtHost”,from standard description window.
- Save the policy.
- Rescan with this new custom policy.

Implication:

Attackers may leverage zero day reflective XSS against a site. If the header is not set in block mode, an attacker can use browser-specific filter bypass bugs to succeed in launching a reflected XSS against the site.

Fix:

Add a configuration setting or a line of code that adds a response header or tag to set X-XSS-Protection with the value '`1; mode=block`'

Reference:

Fortify Taxonomy: Software Security Errors
OWASP Secure Headers Project
CWE ID 554
Chromium Bugs

Attack Request:

GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBilT3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+ZojyfeefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrUlfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9zwR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2Iqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Informational **Cache Management: Headers**

Summary:

The web server sent a Vary header, which indicates that server-driven negotiation was done to determine which content should be delivered. This may indicate that different content is available based on the headers in the HTTP request. Scan configuration recommendations include viewing the HTTP response to determine what criteria is used to negotiate content, and appending custom headers and values according to the negotiate criteria being used.

Fix:

For Development:
Verify your application does not display different content based on headers, and if necessary, re-scan with appropriate headers to ensure good coverage.

For Security Operations:

Evaluate if content negotiation is truly being used, and disable if it is unnecessary. Re-scan with appropriate headers to ensure good coverage.

For QA:
This requires a server or application configuration change. Contact Security Operations for assistance with the server.

Reference:

W3C RFC 2616 Header Field Definitions
http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.44

Attack Request:

```
GET /shopping/images/icons/ HTTP/1.1
Referer: https://mot.deltadentalins.com/shopping/images/icons/clock-f8cd172ffb.png
Accept: */*
Pragma: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: mot.deltadentalins.com
Connection: Keep-Alive
X-WIPP: AscVersion=19.1.0.311
X-Scan-Memo: Category="Audit.Attack"; SID="8822ECB852D0D0AE145480285488D589";
PSID="0FD1574D39F631640030ADE0BF3DE978"; SessionType="PathTruncation"; CrawlType="None"; AttackType="None";
OriginatingEngineID="398bfe9e-1b77-4458-9691-603eea06e341"; AttackSequence="0"; AttackParamDesc="";
AttackParamIndex="0"; AttackParamSubIndex="0"; CheckId="0"; Engine="Path+Truncation";
SmartMode="NonServerSpecificOnly"; ThreadId="389"; ThreadType="AuditDBReaderSessionDrivenAudit";
X-RequestManager-Memo: sid="559"; smi="0"; sc="1"; ID="c3c2746a-2588-4a0a-a6a4-fa8b9a703a9b";
X-Request-Memo: ID="6cfb7e5d-d85e-4b1b-9f70-92c0930e1274"; sc="1"; tid="474";
Cookie: CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0;mot-
ddins=2694841354.64288.0000;TS01d1e64c=01729bd6989930ceab3c5e207764f6beb9de16a42868049e1fa1ed6f97f5ad43405
380895eb09b6c06e1e9ec1ed9579962ab30157f2e2da9d2e1340ef79d4fda86654d424f3188a4780ceba62a2896a7acf423c170c93
75eccc4471dd49cb294e4f802d071;connect.sid=s%
3ASG8JA30nKEUxRUK6A431uKL8pvP8r7JD.5uTEsblBBRIRTTy7jr35yPxBMIVKb6aGE5KpCUbKfJQ
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 23:11:00 GMT
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Cache-Control: max-age=86400, public
Content-Length: 3326
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1
Set-Cookie:
TS01d1e64c=01729bd6989930ceab3c5e207764f6beb9de16a42868049e1fa1ed6f97f5ad43405380895eb09b6c06e1e9ec1ed957
9962ab30157f2e2da9d2e1340ef79d4fda86654d424f3188a4780ceba62a2896a7acf423c170c9375eccc4471dd49cb294e4f802d0
71; Path=/

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /shopping/images/icons</title>
 </head>
 <body>
<h1>Index of /shopping/images/icons</h1>
<ul><li><a href="/shopping/images/"> Parent Directory</a></li>
<li><a href="aarp_pdf-1e13b95df2.png"> aarp_pdf-1e13b95df2.png</a></li>
<li><a href="aarp_pdf-2724aafd15.svg"> aarp_pdf-2724aafd15.svg</a></li>
<li><a href="braces-47511bd1a1.png"> braces-47511bd1a1.png</a></li>
<li><a href="braces-f4fd630410.svg"> braces-f4fd630410.svg</a></li>
<li><a href="brush-82b87cf7ab.svg"> brush-82b87cf7ab.svg</a></li>
<li><a href="brush-ba05f1104b.png"> brush-ba05f1104b.png</a></li>
<li><a href="calculator-6d97df8aa6.png"> calculator-6d97df8aa6.png</a></li>
<li><a href="calculator-ca7ee66fab.svg"> calculator-ca7ee66fab.svg</a></li>
<li><a href="calculator_latest-230a48c854.svg"> calculator_latest-230a48c854.svg</a></li>
<li><a href="calculator_latest-be277ef023.png"> calculator_latest-be277ef023.png</a></li>
<li><a href="calendar-37dc5bc978.svg"> calendar-37dc5bc978.svg</a></li>
<li><a href="calendar-7e009bbc32.png"> calendar-7e009bbc32.png</a></li>
<li><a href="calendar_latest-e860c7958a.png"> calendar_latest-e860c7958a.png</a></li>
<li><a href="calendar_latest-fe027f360b.svg"> calendar_latest-fe027f360b.svg</a></li>
<li><a href="chair-4a3b8ba6c2.svg"> chair-4a3b8ba6c2.svg</a></li>
<li><a href="chair-8527691212.png"> chair-8527691212.png</a></li>
```

 clock-e203df31b0.svg
 clock-f8cd172ffb.png
 facility-394b391d27.png
 facility-8fe2e04150.svg
 facility_latest-48820af60d.png
 facility_latest-9d57e5a0b6.svg
 facility_small-03950f9ee4.svg
 facility_small-ecb73ea11f.png
 implant-029de84ae9.svg
 implant-8f623af0b3.png
 map-c3684cb1da.png
 map-fe6af3080a.svg
 map_small-b0729c84c5.png
 map_small-db06f3871c.svg
 pdf-965d4c4ee6.png
 pdf-e93ab74a24.svg
 pdf_latest-43f9177ddd.svg
 pdf_latest-fd41e22b02.png
 shinny-0f3e28f6cb.svg
 shinny-e1cc8d3a9b.png
 wallet-593f9444d2.png
 wallet-c6feffae08.svg
 wallet_latest-431461ea7e.svg
 wallet_latest-cad3a0c375.png
 woman-4f35c20f39.png
 woman-d5b7908c6a.svg

</body></html>

File Names:

- https://mot.deltadentalins.com:443/shopping/images/icons/
- https://mot.deltadentalins.com:443/shopping/downloads/delta/
- https://mot.deltadentalins.com:443/enroll/locale-based/en/
- https://mot.deltadentalins.com:443/shopping/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/locale-based/
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote
- https://mot.deltadentalins.com:443/enroll/downloads/
- https://mot.deltadentalins.com:443/enroll/js/additional-methods-d95f4f840a.min.js
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/
- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/enroll/images/
- https://mot.deltadentalins.com:443/enroll/styles/
- https://mot.deltadentalins.com:443/shopping/downloads/

Informational

Insecure Deployment: Known Technology Fingerprint

Summary:

WebInspect has determined that the target server supports the following TLS_RSA ciphers:

- **TLS_RSA_WITH_AES_256_CBC_SHA (0x35)**
- **TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)**
- **TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)**
- **TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)**
- **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)**
- **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)**

While TLS_RSA itself is not vulnerable, several implementations of TLS_RSA cipher have been shown to be vulnerable to ROBOT Attack (Return Of Bleichenbacher's Oracle Threat). Bleichenbacher's is an adaptive chosen-ciphertext attack on the RSA PKCS#1v1.5 encryption standard. The vulnerability in the implementation of the RSA PKCS#1v1.5 algorithm allows an attacker to steal the private session key from a secure SSL/TLS session. The attacker can then use the key to compromise and decrypt recorded SSL/TLS sessions, leading to information disclosure and impersonation attacks.

Execution:

A list of ciphers supported by this server can be obtained by running ServerAnalyzer tool from the WebInspect toolkit. Note the presence of "TLS_RSA" ciphers in the list of supported ciphers.

Implication:

If a vulnerable version of the TLS_RSA exists on the server, the server may be vulnerable to ROBOT Attack which would allow an attacker to successfully decrypt a previously recorded SSL/TLS session, leading to information disclosure and impersonation attacks.

Fix:

Please refer to your vendor's documentation to check if the TLS_RSA version in use is vulnerable to ROBOT attack. If necessary please apply the required patch from the vendor to protect against this vulnerability.

Reference:

The ROBOT Attack
Return Of Bleichenbacher's Oracle Threat

Attack Request:

GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%
2FQ; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-
b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 22:55:18 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2661286922.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/


```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <meta http-equiv="X-UA-Compatible" content="IE=edge" />
   <title>Get A Quote</title>

   <!-- Page-hiding snippet (recommended)  -->
   <style>.async-hide { opacity: 0 !important} </style>
   <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
      h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
      (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
   })(window,document.documentElement,'async-hide','dataLayer',4000,
         {'GTM-NPRVDTC':true});</script>
   <!-- Modified Analytics tracking code with Optimize plugin -->
```

```
    <script type="text/javascript">
      (function(i, s, o, g, r, a, m) {
        i['GoogleAnalyticsObject'] = r;
        i[r] = i[r] || function() {
                (i[r].q = i[r].q || []).push(arguments)
              }, i[r].l = 1 * new Date();
        a = s.createElement(o), m = s.getElementsByTagName(o)[0];
        a.async = 1;
        a.src = g;
        m.parentNode.insertBefore(a, m)
      })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
      ga('create', 'UA-9398012-1', 'auto');
      ga('require', 'GTM-NPRVDTC', 'auto');
      var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
      ga('set', 'dimension9', dnt);
      ga('send', 'pageview');
    </script>

      <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
      <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


      <link rel="stylesheet" type="text/css" href="/shopping/styles/style-00239ae0e5.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
          <header class="shopping-header-title">

                                    <a class="back-arrow-link" id="shoppingBack"
href="https://mot.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                                <div class="main-content">
                                    <h1 class="shopping-header-content">
                                        Get a Quote
                                    </h1>
                                </div>
                                </header>


<main role="main" class="main-content container page-control get-a-quote">
  <div class="main-container-inner">
    <div class="top-heading-section">
      <div class="error-container global-margin">
      </div>
     <div class="summary grey-text">
      We need a little more information to give you a quote.
     </div>
    </div>
    <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
     <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
       <label for="zip"   >What

...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Informational

HTML5: Missing Content Security Policy

Summary:

Content Security Policy (CSP) is an HTTP response security header that developers and security architects can leverage to whitelist domains from which the site is allowed to load resources. This header provides an in-depth security protection from critical vulnerabilities such as cross-site scripting and clickjacking. Additionally, CSP restricts execution of inline JavaScript, dynamic JavaScript code evaluation from strings, and framing of the site from external domains. While CSP is not a replacement for input validation, it can help to significantly reduce the risk of XSS from unknown weaknesses. The CSP frame-

ancestors directive is equivalent to X-Frame-Options and restricts the domain that are allowed to frame the site's content.

Execution:

Access link https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA through a proxy and notice the missing CSP header in the response. By default, WebInspect flags only one instance of this vulnerability per host because it is typical to set this header at the host level in a server configuration.

Perform the following steps to flag all instances of this issue:

- Create a new policy with the selection of checks that you want to include in a rescan. We recommend using the Blank or Passive policy as a base.
- Select this check and uncheck the "FlagAtHost" check input from standard description.
- Save the policy.
- Rescan with this new custom policy.

Implication:

Security architects and developers can leverage CSP to significantly reduce the risk of XSS and clickjacking attacks. CSP headers can restrict leakage of information to external domains by restricting which domains the site is allowed to load contents from when rendered in browser .

Fix:

Define a CSP policy suitable for your site. The policy can be set either with an HTTP response header or <meta /> tag.

For example:
```
Content-Security-Policy: default-src https://example.net; child-src 'none';
```
Or
```
<meta http-equiv="Content-Security-Policy" content="default-src https://cdn.example.net;
child-src 'none'; object-src 'none'">
```

Content-Security-Policy 2 is the recommended standard. Content-Security-Policy 3 is in draft. The following is a snapshot of modern browser support for the CSP header:

- Edge: Versions 15-18; supported with a nonce bug. Version 75 and later; fully supported.
- Chrome: Versions 36-38; missing the plugin-types, child-src, frame-ancestors, base-uri, and form-action directives. Version 39; missing the plugin-types, child-src, base-uri, and form-action directives. Version 40 and later; fully supported.
- Firefox: Versions 31-34; missing the plugin-types, child-src, frame-ancestors, base-uri, and form-action directives. Version 35; missing the plugin-types, child-src, frame-ancestors, and form-action directives. Versions 36-44; missing the plugin-types and child-src directives. Version 45 and later; missing the plugin-types directive.

Furthermore, the report-uri directive can be configured to receive reports of attempts to violate the policy. These reports can be used as an early indication of security issues in the site as well as to optimize the policy.

Reference:

Content Security Policy Level 3
OWASP Content Security Policy
MDN web docs
Content Security Policy (CSP) Quick Reference Guide

Attack Request:

GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%
2FQ; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-
b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 22:55:18 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2661286922.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/

<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <meta http-equiv="X-UA-Compatible" content="IE=edge" />
   <title>Get A Quote</title>

   <!-- Page-hiding snippet (recommended)  -->
   <style>.async-hide { opacity: 0 !important} </style>
   <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
      h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
      (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
   })(window,document.documentElement,'async-hide','dataLayer',4000,
         {'GTM-NPRVDTC':true});</script>
   <!-- Modified Analytics tracking code with Optimize plugin -->
   <script type="text/javascript">
      (function(i, s, o, g, r, a, m) {
         i['GoogleAnalyticsObject'] = r;
         i[r] = i[r] || function() {
                  (i[r].q = i[r].q || []).push(arguments)
               }, i[r].l = 1 * new Date();
         a = s.createElement(o), m = s.getElementsByTagName(o)[0];
         a.async = 1;
         a.src = g;
         m.parentNode.insertBefore(a, m)
      })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
      ga('create', 'UA-9398012-1', 'auto');
      ga('require', 'GTM-NPRVDTC', 'auto');
      var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
      ga('set', 'dimension9', dnt);
      ga('send', 'pageview');
   </script>

      <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
      <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

   <script>window['adrum-start-time'] = new Date().getTime();</script>
   <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


      <link rel="stylesheet" type="text/css" href="/shopping/styles/style-00239ae0e5.css">


   <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
         <header class="shopping-header-title">

                                          <a class="back-arrow-link" id="shoppingBack"
href="https://mot.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
```

back to previous page

<h1 class="shopping-header-content">
Get a Quote
</h1>

</header>

<main role="main" class="main-content container page-control get-a-quote">

We need a little more information to give you a quote.

<form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
<input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
<label for="zip" >What

...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Best Practice

Privacy Violation: Autocomplete

Summary:

Most recent browsers have features that will save form field content entered by users and then automatically complete form entry the next time the fields are encountered. This feature is enabled by default and could leak sensitive information since it is stored on the hard drive of the user. The risk of this issue is greatly increased if users are accessing the application from a shared environment. Recommendations include setting autocomplete to "off" on all your forms.

Reference:

Microsoft:
Autocomplete Security

Attack Request:

GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2Iqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 22:55:18 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2661286922.64288.0000; path=/; Httponly; Secure
Set-Cookie: TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a4562a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b36261d1; Path=/

...TRUNCATED...="zip" >What's your ZIP code?</label>
<input id="zip" class="form-input quote_address_zip zip" type="text" name="zip" placeholder="ZIP code" />

<div class="inline-error-con...TRUNCATED... class="hidden" >Month</label>
<input id="app0_dob_month" class="form-input month min_applicant_age" type="text" name="app0_dob_month" placeholder="mm" maxlength = "2" />

<label for="app0y" class="hidden" >day</label>
<input id="app0_dob_day" class="form-input day min_applicant_age" type="text" name="app0_dob_day" placeholder="dd" maxlength = "2" />

<label for="app0" class="hidden" >Year</label>
<input id="app0_dob_year" class="form-input year min_applicant_age" type="text" name="app0_dob_year" placeholder="yyyy" maxlength = "4" />

</field...TRUNCATED... how many people need coverage?</label>
<input id="noofcovered" class="form-input quote_add_people noofcovered" type="text" name="noofcovered" value="1" />

<button id="minusButton" t...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/delta/payment

Best Practice

Weak Cryptographic Hash

Summary:

A string of hexadecimal digits matching the length of a cryptographic hash from the MD family was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are multiple hashing algorithms in the MD family. By far the most commonly used algorithm is MD5, though MD4 and MD2 are still used with various public key and digital certificate systems. There are known attacks against MD5, MD4, and MD2. These hashes are also susceptible to Rainbow table attacks unless the input is properly salted. As such the MD family of cryptographic hashing functions should not be considered secure and should only be used in certain situations.

Implication:

Hashes produced by the MD family should only be used for short-lived uses where the hash and/or hashed data is not highly security sensitive, or for uses where uniqueness is not a critical requirement. MD Hashes should not be used for any type of long term application such as verifying the integrity of a file or for password storage.

Fix:

For Development:
The application should only use cryptographically secure hashing algorithms, such as SHA-224, SHA-256, SHA-384, or SHA-512. Hashes representing sensitive data should be salted to reduce the effectiveness of rainbow tables.

For Security Operations:
Implement a security policy that precludes the use of MD5, MD4, or MD2 for cryptographic functionality.

For QA:
Make sure that the application is not relying on MD5, MD4, or MD2 for cryptographic functionality.

Reference:

MD5
http://en.wikipedia.org/wiki/MD5
Cryptographic Salting
http://en.wikipedia.org/wiki/Salt_%28cryptography%29

Attack Request:

GET /enroll/js/mot-adrum-05508bc7fe.js HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache

Cookie: ADRUM_BT=R:116|i:2050|g:f9e47ca0-5b58-468d-bba5-6621489693799858|e:-nan|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000; TS01d1e64c=01729bd698f45abe959d34b69c298df56a4295206a537fb63d31b5acd0749beed29aa3abe0416dcf85ba6b4069ff2fd72f2e1361088d78011c76db0d186db3cfd260ee536bdc47e52830c81ee6789a68b4cc4f5aeaca82b72ae7119c410a1a1959dd60def8; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1563490501836%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1563490776381%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA~1563490790452%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA%26planEffectiveDate%3D8%2F15%2F2019~1563490797421; TS018e8e3c=01729bd698350341c79702fd652cb89a27951cd890404ef3a01486cadec575fb339b19b25b0078f2d62bd04be799146b98d1079c79f323bed30d0f5710ec9c493c25e09027; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18096%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1564095295%7C9%7CMCAAMB-1564095295%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1563497695s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBilT3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+ZojyfeefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrUlfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9zwR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy; _gid=GA1.2.1908194059.1563490494; _gat=1; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true; s_sq=deltadentalcaddinsstage%3D%2526c.%2526a.%2526activitymap.%2526page%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fshopping%25252Fdelta%25252Fplan-options%25252F11048636%25253FissuerCode%25253DDELTA%252526planEffectiveDate%25253D8%25252F15%25252F2019%2526link%253DBuy%252520Plan%2526region%253DbuyPlan%2526.activitymap%2526.a%2526.c%2526pid%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fshopping%25252Fdelta%25252Fplan-options%25252F11048636%25253FissuerCode%25253DDELTA%252526planEffectiveDate%25253D8%25252F15%25252F2019%2526oid%253DBuy%252520Plan%2526oidt%253D3%2526ot%253DSUBMIT%2526oi%253D59; ADRUM=s=1563490798933&r=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3F-223145629;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 23:00:01 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 15 Jul 2019 17:49:58 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 37915
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: application/javascript

Set-Cookie:
TS018e8e3c=01729bd698350341c79702fd652cb89a27951cd890404ef3a01486cadec575fb339b19b25b0078f2d62bd04be799146b98d1079c79f323bed30d0f5710ec9c493c25e09027; Path=/

;/* Version 28b707b4ae597aaa6317446ec323ad71 v:4.2.8.0,
c:3b331bdb5ca9c18ce583f6d2bad57b4289fa...TRUNCATED...cs.com":"http://cdn.appdynamics.com")+"/adrum-ext.
28b707b4ae597aaa6317446ec323ad71.js";a.adrumXdUrl="https://cdn.appdynamics.com/adrum-xd.
28b707b4ae597aaa6317446ec323ad71.html";a.agentVer="4.2.8.0";a.sendImageBeacon="fal...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/shopping/js/mot-adrum-05508bc7fe.js

Best Practice

Weak Cryptographic Hash

Summary:

A string of hexadecmial digits matching the length of a cryptographic SHA-0 or SHA-1 hash was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are known attacks against SHA-0 and SHA-1. While not broken, SHA-0 and SHA-1 are considered weak. Various organizations, such as NIST in the United States, no longer recommend SHA-0 or SHA-1 and these algorithms should only be used in certain situations.

Implication:

The SHA-0 and SHA-1 cryptographic hashing functions are considered weak. You should consider upgrading to a strong hash unless the hash is used for short-lived uses, where the hash and/or hashed data is not highly security sensitive, or for uses where uniqueness is not a critical requirement.

Fix:

For Development:
Consider upgrading to a secure hashing algorithms, such as SHA-224, SHA-256, SHA-384, or SHA-512. Hashes representing sensitive data that is stored for long periods of time should be salted to reduce the effectiveness of rainbow tables.

For Security Operations:
Implement a security policy that precludes the use of SHA-0 and SHA-1 for cryptographic functionality.

For QA:
Make sure that the application is not relying on SHA-0 and SHA-1 for cryptographic functionality.

Reference:

SHA Hash Functions
http://en.wikipedia.org/wiki/SHA_hash_functions
New Cryptoanalytic Results Against SHA-1
http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html
NIST Approved Secure Hashing Algorithms
http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html
Cryptographic Salting
http://en.wikipedia.org/wiki/Salt_%28cryptography%29

Attack Request:

GET /shopping/js/mot-adrum-05508bc7fe.js HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/shopping/delta/get-a-quote?issuerCode=DELTA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000; TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a4562a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b36261d1; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBilT3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6

QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:54 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 12 Jul 2019 22:07:28 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 37915
Keep-Alive: timeout=5, max=91
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/

ion 28b707b4ae597aaa6317446ec323ad71 v:4.2.8.0, c:3b331bdb5ca9c18ce583f6d2bad57b4289faab2d, b:5824 n:31-
4.2.8.next-build */(function(){new f...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/enroll/js/mot-adrum-05508bc7fe.js

Best Practice

Exposure of POST Parameters in GET Request

Summary:

Some web frameworks collapse the POST and GET parameters into a single collection. This is a flawed design pattern from a security standpoint. If a page accepts POST parameters as GET parameters an attacker would be able to effect change on websites through Cross-Site Request Forgery or leverage this design flaw with other vulnerabilities to attack the system hosting the web application.

Execution:

Using a Web Proxy tool, browse to https://mot.deltadentalins.com:443/enroll/delta/personal-info?
planType=PPO&planCode=Prem00002&planId=11048636&planName=Delta+Dental+PPO+Individual+-
+Premium+Plan&annualCost=64.92&enrollmentFee=10&planState=CA&planZip=95630&coverageType=Self&issuerCode=DEL
TA&coverageStartDate=2019-08-15&noOfCovered=1&planDetailsBaseUrl=%2Fshopping%2Fdelta%2Fplan-options%
2F11048636%3FissuerCode%3DDELTA&a_dob=12%2F12%2F1981. Once accessed add each POST parameter to the GET parameters list and re-request the page. If the same page appears while requesting ~FullUrl~ with an HTTP GET request with all POST parameters in the Url, then this page is vulnerable to this design flaw.

Implication:

Allowing POST data parameters to be passed through GET parameters as well can open the web application to Cross-Site Request Forgery attacks.

Fix:

For Developers:
POST variables and GET variables should be distinct and no attempt to collapse to two collections should occur.

For QA:
Follow the instructions listed in the Execution to reproduce the issue, and forward to development.

For Security Operations:
If using a web-framework, communicate to developers using the web-framework that POST variables and GET variables should be distinct and no attempt to collapse the two collections should occur.

Reference:

CWE 352 - Cross-Site Request Forgery
http://cwe.mitre.org/data/definitions/352.html

Attack Request:

GET /enroll/delta/personal-info?
planType=PPO&planCode=Prem00002&planId=11048636&planName=Delta+Dental+PPO+Individual+-
+Premium+Plan&annualCost=64.92&enrollmentFee=10&planState=CA&planZip=95630&coverageType=Self&issuerCode=DEL

TA&coverageStartDate=2019-08-15&noOfCovered=1&planDetailsBaseUrl=%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA&a_dob=12%2F12%2F1981 HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/shopping/delta/plan-options/11048636?issuerCode=DELTA&planEffectiveDate=8/15/2019
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=19.1.0.311
X-Scan-Memo: Category="Audit.Attack"; SID="DA84688CCC5C0F8BD6286FF66D932AD1"; PSID="8607DD441A2187680892C00BBF2B24C5"; SessionType="AuditAttack"; CrawlType="None"; AttackType="Other"; OriginatingEngineID="8ca14a29-1566-423d-b9f8-f46aa279ec29"; AttackSequence="0"; AttackParamDesc=""; AttackParamIndex="0"; AttackParamSubIndex="0"; CheckId="10655"; Engine="Form+Accepts+GET+Variables"; SmartMode="NonServerSpecificOnly"; ThreadId="51"; ThreadType="Task";
X-RequestManager-Memo: sid="557"; smi="0"; sc="1"; ID="f86c319c-8edc-4d47-b33d-2c7153815170";
X-Request-Memo: ID="0bdf0862-1a55-4118-a146-8036cc63563c"; sc="1"; tid="532"; r Cookie: ADRUM_BT=R:116|i:2050|g:f031f0ba-7ad4-439a-aee7-407db0f93db89860|e:22|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AYjcDujss4QCrdkmA1pyzGT8BrLTEJ2Xm.nINI2wwkAkjgDJi2pCs87u1qmccYLnZi%2Bwb3rMVwkoo; mot-ddins=2661286922.64288.0000;
TS01d1e64c=01729bd69865454884891e2dc8fe9d54f4f83ff7a33c1a85aacebf5c8c88c8fa099705b97ea39980d97a14c08de0e9f29f130c82bb5ac2c3df8f784ce10200f41ff3eba9c3cf2ce4c5f1a030b80680c2cd0b5fd596fc287ce9cbf1bf857de5e54c5a7a8b14;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0;TS0132dfbe=01729bd698f589f758b38a246162792d92ba94e0e080cca867a58cd1abc761b51e0dbdd522626a4b0c26e4751c4d3c1998bf8f0845;TS018e8e3c=01729bd698a0e0c3a05ab56f2be8370ac5acefd5de0b86638666f5411877ac2bc862fa29cfa7a05830c84a4fde01ae4cdca11e6f4152e26e787a3095b82e7f24ffa58dc854

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 23:16:08 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Content-Length: 31031
Set-Cookie: ADRUM_BT=R:116|i:2050|g:f9e47ca0-5b58-468d-bba5-6621489693799971|e:46|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 23:16:38 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Set-Cookie: TS018e8e3c=01729bd698b7c89742566bdc2d17738d40468524cc0b86638666f5411877ac2bc862fa29cf19384709a78214a9bb38fa9f365a90a0e0efa4a4c0248c4417948b50c98e6fd2; Path=/

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <title>Personal Info | Enrollment | Delta Dental Insurance Company</title>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-deltadentalofcalifornia&libraries=places"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/enroll/js/html5shiv-40bd440d29.min.js" async></script>

        <link rel="stylesheet" type="text/css" href="/enroll/styles/style-09346f3cb5.css">

        <script type="text/javascript" src="/enroll/js/zippopupsingle-17eac51cc4.js"> </script>

    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
    <script type="text/javascript">
        (function(i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r;
            i[r] = i[r] || function() {
                    (i[r].q = i[r].q || []).push(arguments)
                }, i[r].l = 1 * new Date();
```

```
        a = s.createElement(o), m = s.getElementsByTagName(o)[0];
        a.async = 1;
        a.src = g;
        m.parentNode.insertBefore(a, m)
      })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
      ga('create', 'UA-9398012-1', 'auto');
      var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
      ga('set', 'dimension9', dnt);
      ga('send', 'pageview');


    </script>
</head>
<body>
  <!--BEGIN QUALTRICS SITE INTERCEPT-->
    <script type='text/javascript'>
    (function(){var g=function(e,h,f,g){
    this.get=function(a){for(var a=a+"=",c=document.cookie.split(";"),b=0,e=c.length;b<e;b++){for(var d=c[b];"
"==d.charAt(0);)d=d.substring(1,d.length);if(0==d.indexOf(a))return d.substring(a.length,d.length)}return null};
    this.set=function(a,c){var b="",b=new Date;b.setTime(b.getTime()+6048E5);b="; expires="+b.toGMTString
();document.cookie=a+"="+c+b+"; path=/; "};
    this.check=function(){var a=this.get(f);if(a)a=a.split(":");else if(100!=e)"v"==h&&(e=Math.random()>=e/100?0:100),a=
[h,e,0],this.set(f,a.join(":"));else return!0;var c=a[1];if(100==c)return!0;switch(a[0]){case "v":return!1;case "r":return c=a
[2]%Math.floor(100/c),a[2]++,this.set(f,a.join(":")),!c}return!0};
    this.go=function(){if(this.check()){var a=document.createElement("script");a.type="text/javascript";a.src=g+ "&t=" +
(new Date()).getTime();document.body&&document.body.appendChild(a)}};
    this.start=function(){var a=this;window.addEventListener?window.addEventListener("load",function(){a.go()},!
1):window.attachEvent&&window.attachEvent("onload",function(){a.go()})};
    try{(new g(100,"r","QSI_S_ZN_bpjF3HlqMikXKbr","https://znbpjf3hlqmikxkbr-
deltadental.siteintercept.qualtrics.com/WRSiteInterceptEngine/?
Q_ZID=ZN_bpjF3HlqMikXKbr&Q_LOC="+encodeURIComponent(window.location.href))).start()}catch(i){}})();
    </script><div id='ZN_bpjF3HlqMikXKbr'><!--DO NOT REMOVE-CONTENTS PLACED HERE--></div>
  <!--END SITE INTERCEPT-->




  <!-- Code Type - Tag - Page -->
    <!--
    Start of DoubleClick Floodlight Tag: Please do not remove
    Activity name of this tag: 2018 First Enrollment Step
    URL of the webpage where the t

...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/enroll/delta/personal-info?planType=PPO&planCode=Prem00002&planId

Best Practice

Web Server Misconfiguration: Insecure Content-Type Setting

Summary:

The Content-Type HTTP response header or the HTML meta tag provides a mechanism for the server to specify an appropriate character encoding for the response content to be rendered in the web browser. Proper specification of the character encoding through the charset parameter in the Content-Type field reduces the likelihood of misinterpretation of the characters in the response content and ensure reliable rendering of the web page.Failure to ensure enforcement of the desired character encoding could result in client-side attacks like Cross-Site Scripting.

Execution:

Verify the character set specification on every HTTP response. Character sets can be specified in the HTTP header or in an HTML meta tag. In the case of an XML response, the character set can be specified along with the XML Declaration.

Implication:

In the absence of the character set specification, a user-agent might default to a non-standard character set, or could derive an incorrect character set based on certain characters in the response content. In some cases, both these approaches can cause the response to be incorrectly rendered. This may enable other attacks such as Cross-site Scripting.

Fix:

Ensure that a suitable character set is specified for every response generated by the web application. This can be done either

by,

- Modifying the code of the web application, which would require all pages to be modified.
- Adding Content-Type header to the server configuration (**recommended**). This ensures that the header is added to all the responses with minimal development effort.

Reference:

DoD Application Security and Development STIG
http://iase.disa.mil/stigs/app_security/app_sec/app_sec.html

UTF-7 encoding used to create XSS attack
http://www.securityfocus.com/archive/1/420001

Attack Request:

```
GET /enroll/locale-based/en/US/client-data.json HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache

Cookie: ADRUM_BT=R:116|i:2050|g:f9e47ca0-5b58-468d-bba5-6621489693799858|e:-nan|s:f|n:MOT_a5878d08-57da-4244-
b352-7b663d9a2a7d; connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-
L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%2FQ; mot-ddins=2661286922.64288.0000;
TS01d1e64c=01729bd698f45abe959d34b69c298df56a4295206a537fb63d31b5acd0749beed29aa3abe0416dcf85ba6b4069ff2f
d72f2e1361088d78011c76db0d186db3cfd260ee536bdc47e52830c81ee6789a68b4cc4f5aeaca82b72ae7119c410a1a1959dd60d
ef8; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%
3DDELTA~1563490501836%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%
3FissuerCode%3DDELTA~1563490776381%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-
options%2F11048636%3FissuerCode%3DDELTA~1563490790452%7Chttps%3A%2F%2Fmot.deltadentalins.com%
2Fshopping%2Fdelta%2Fplan-options%2F11048636%3FissuerCode%3DDELTA%26planEffectiveDate%3D8%2F15%
2F2019~1563490797421;
TS018e8e3c=01729bd698350341c79702fd652cb89a27951cd890404ef3a01486cadec575fb339b19b25b0078f2d62bd04be7991
46b98d1079c79f323bed30d0f5710ec9c493c25e09027; _ga=GA1.2.1222917316.1517435630;
AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18096%7CMCMID%
7C22137510049759883710112622098244936722%7CMCAAMLH-1564095295%7C9%7CMCAAMB-1564095295%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1563497695s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4
jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;
_gid=GA1.2.1908194059.1563490494; _gat=1; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true;
s_sq=deltadentalcaddinsstage%3D%2526c.%2526a.%2526activitymap.%2526page%253Dhttps%25253A%25252F%
25252Fmot.deltadentalins.com%25252Fshopping%25252Fdelta%25252Fplan-options%25252F11048636%
25253FissuerCode%25253DDELTA%252526planEffectiveDate%25253D8%25252F15%25252F2019%2526link%253DBuy%
252520Plan%2526region%253DbuyPlan%2526.activitymap%2526.a%2526.c%2526pid%253Dhttps%25253A%25252F%
25252Fmot.deltadentalins.com%25252Fshopping%25252Fdelta%25252Fplan-options%25252F11048636%
25253FissuerCode%25253DDELTA%252526planEffectiveDate%25253D8%25252F15%25252F2019%2526oid%253DBuy%
252520Plan%2526oidt%253D3%2526ot%253DSUBMIT%2526oi%253D59; ADRUM=s=1563490798933&r=https%3A%2F%
2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F11048636%3F-
223145629;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 23:00:01 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 15 Jul 2019 17:49:57 GMT
Accept-Ranges: bytes
Content-Length: 4763
Cache-Control: max-age=86400, public
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
```

Content-Type: application/json
Set-Cookie: TS018e8e3c=01729bd698350341c79702fd6...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/shopping/locale-based/en/US/client-data.json

Best Practice

Insecure Transport: Missing Perfect Forward Secrecy

Summary:

Perfect Forward Secrecy (PFS) assures the secrecy of encrypted communications into the future in case SSL/TLS private key is compromised. PFS is a function of key-exchange protocols used for the establishment of shared secret between the client and the server [1]. On a non-forward secrecy server, both the authentication of the server and the encryption is done using long-term private key. Hence, compromised long-term private key can jeopardize all communications. PFS mitigates this by achieving authentication using a long-term private key and session data encryption using a short-term private key. PFS is commonly achieved using Diffie-Hellman in ephemeral-static mode (DHE) or Elliptic Curve Diffie-Hellman key agreement scheme with ephemeral keys (ECDHE) [2, 3, 4]. For every TLS session established with DHE- or ECDHE- as key exchange algorithm in cipher suite, the server is required to use a new Diffie-Hellman public/private key for the generation of the TLS master secret [8]. The server signs this Diffie-Hellman public key using the long-term private key to guarantee authenticity. The long-term private key is not used for the encryption of session contents. While a stolen ephemeral private key could allow an attacker to decipher encrypted communication, the compromise is confined to the specific session for which the ephemeral key was generated. It is recommended that ephemeral keys are not logged.

WebInspect has determined that mot.deltadentalins.com:443 target server configuration contains following issues:
1. Target server supports ECDHE PFS cipher suites but it also uses 6 other cipher suites which do not support PFS:

- **TLS_RSA_WITH_AES_256_CBC_SHA (0x35)**
- **TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)**
- **TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)**
- **TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)**
- **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)**
- **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)**

Execution:

A list of supported ciphers by this server can be obtained by running ServerAnalyzer tool from WebInspect toolkit. Notice the absence of "DHE" and "ECDHE" in the list of supported cipher-suite names.

Implication:

A stolen long-term private key can be used by an attacker to decrypt past intercepted communication putting user data at risk where data is still relevant. This shortcoming in SSL/TLS was accentuated in the wake of Heartbleed [4] vulnerability, a vulnerability in Openssl library[4], that allowed attackers to steal server's private keys among other sensitive data.

Fix:

1. PFS is enabled by turning on Diffie-Hellman Ephemeral (DHE) or Elliptic-Curve-Diffie-Hellman Ephemeral (ECDHE) based cipher suites on the server [2]. e.g.

- For Apache – Modify SSLCipherSuite parameter in server configuration to add ECDHE or DHE key exchange algorithm.
- For nginx – Modify ssl_ciphers in server configuration to add ECDHE or DHE key exchange algorithm.
- For IIS please refer to following knowledge base articles:

- http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx
- http://support.microsoft.com/kb/245030

2. Make sure that all other cipher suites which do not provide PFS are disabled on the server.

Reference:

http://en.wikipedia.org/wiki/Forward_secrecy
Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.
Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.
Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.
http://tools.ietf.org/html/rfc4492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
http://www.openssl.org/
http://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange
http://nginx.org/en/docs/http/ngx_http_ssl_module.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mot.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C18086%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1563209151%7C9%
7CMCAAMB-1563209151%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1562611551s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=vS5x5GCkr6lsGnCgcTFPMMyjj8KCe9Dx1zMmzwqb+ZUlNwlk4Heol3Q/VQp/jtjuuUVfUBUqW7fGE7n/AcvKCvhGrBil
T3CuHJ3BTqckmcgrAp11mK3fW7rwNmv0dukhOxKjzNOLsRLDbYp4ipgZcXtmTUu8OeRz5YCXGY4UDU1kb5q/3YRfrz+7WAmYk6
QjTTrUaOSEOJWaINfe5VCZZ+HE0NyFh7KewalzGVF+Op+nAxWy2SOrpgoGaHoTC3dfmzqojx6przuo/2C/BN1QWbqH8OR+Zojyf
eefyGqAlQwxFZQiqiIXHZQrVaTbj2jIoueqgHETC+UvDCbTXnKY8jz8pUnXjdqfGdMBqtIQvXDzzXbSxrKoPuNdYn3SyPlsp+jEAVDvrU
lfjRz2bhyd6H9QOMXiJ3lEjsvvIYO6LMUv+yDNEZKpB9/EbnMGXujJUtd13xAOTJ2IoUeaHTpQduKMbXQJKVcZ8mkKGEVLsBpCX9z
wR4jbVPh6VDZglvwx6l6jJV/Pmcp8tv7tqx0aRkF2lqi6owP5q0liXoo/pee1vk3qltMQ1OPBzru9Wnsy;CustomCookie=WebInspect15
0223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 18 Jul 2019 22:54:48 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16397
Set-Cookie: connect.sid=s%3Ayb0oRDcaiBcGHxw47rV8Jhl3-L44WCQz.ZkGU3MFz1nNEoVTQtNB3cgtyM8CrbexczgRY4jR8Z%
2FQ; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|i:6573|g:601f5f15-de87-436e-9e80-0046f231b0ed9478|e:-nan|s:f|n:MOT_a5878d08-57da-4244-
b352-7b663d9a2a7d; Path=/; Expires=Thu, 18 Jul 2019 22:55:18 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2661286922.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd6988b6bafa28d0d653de2a7eb724e4c3d0e3f2eaabe3fba1119fe5df7d4b6780e8b5bf44a42a9ee9b32a456
2a3b8bb033d920bb55b5386d14449db48da6dfe7b30ccb1911b50da8fb76cb7b79816bdc7dec98fde290daf1a1efa6277f40b3626
1d1; Path=/

<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <meta http-equiv="X-UA-Compatible" content="IE=edge" />
   <title>Get A Quote</title>

   <!-- Page-hiding snippet (recommended)  -->
   <style>.async-hide { opacity: 0 !important} </style>
   <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
      h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
      (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
   })(window,document.documentElement,'async-hide','dataLayer',4000,
         {'GTM-NPRVDTC':true});</script>
   <!-- Modified Analytics tracking code with Optimize plugin -->
   <script type="text/javascript">
      (function(i, s, o, g, r, a, m) {
         i['GoogleAnalyticsObject'] = r;
         i[r] = i[r] || function() {
                  (i[r].q = i[r].q || []).push(arguments)
               }, i[r].l = 1 * new Date();
         a = s.createElement(o), m = s.getElementsByTagName(o)[0];
         a.async = 1;
         a.src = g;
         m.parentNode.insertBefore(a, m)
      })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
      ga('create', 'UA-9398012-1', 'auto');
      ga('require', 'GTM-NPRVDTC', 'auto');
      var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
      ga('set', 'dimension9', dnt);
```

```
        ga('send', 'pageview');
    </script>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-00239ae0e5.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
            <header class="shopping-header-title">

                                        <a class="back-arrow-link" id="shoppingBack"
href="https://mot.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                                    <div class="main-content">
                                        <h1 class="shopping-header-content">
                                                Get a Quote
                                        </h1>
                                    </div>
                                    </header>


<main role="main" class="main-content container page-control get-a-quote">
  <div class="main-container-inner">
    <div class="top-heading-section">
        <div class="error-container global-margin">
        </div>
      <div class="summary grey-text">
        We need a little more information to give you a quote.
      </div>
    </div>
    <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
      <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
          <label for="zip"   >What

...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA