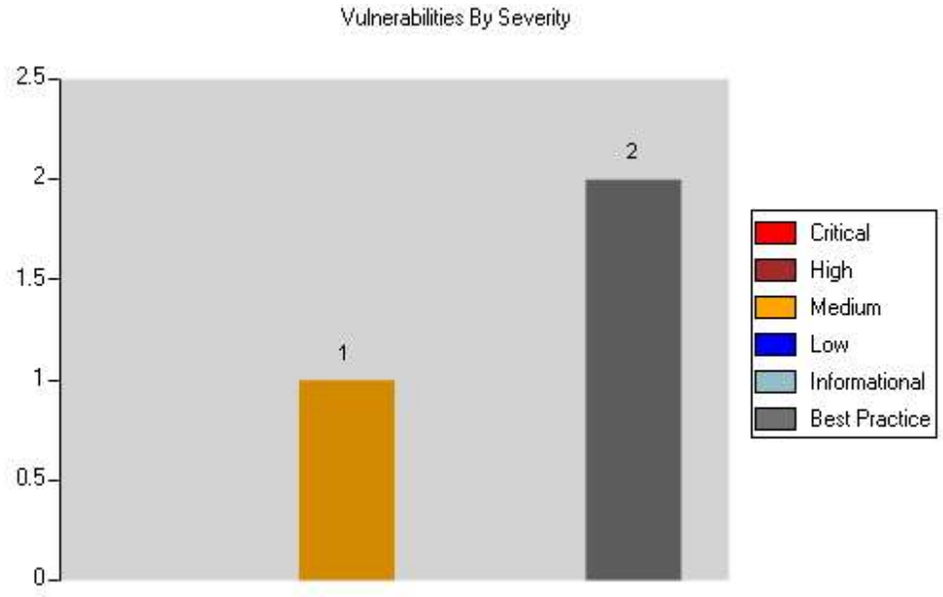
Micro Focus WebInspect

Vulnerability (Legacy)

Web Application Assessment Report

Scan Name:	https://mot3.deltadentalins.com/find-a-dentist/alpha/		
Policy:	SOAP	**Crawl Sessions:**	0
Scan Date:	2/11/2019 2:55:30 PM	**Vulnerabilities:**	1
Scan Version:	18.20.178.0	**Scan Duration:**	1 Minute : 49 seconds
Scan Type:	Site	**Client:**	FF

Server: https://mot3.deltadentalins.com:443



Medium

Cookie Security: Persistent Cookie

Summary:

Cookies are small bits of data that are sent by the web application but stored locally in the browser. This lets the application use the cookie to pass information between pages and store variable information. The web application controls what information is stored in a cookie and how it is used. Typical types of information stored in cookies are session Identifiers, personalization and customization information, and in rare cases even usernames to enable automated logins. There are two different types of cookies: *session cookies*and *persistent cookies*. Session cookies only live in the browser's memory, and are not stored anywhere. Persistent cookies, however, are stored on the browser's hard drive. This can cause security and privacy issues depending on the information stored in the cookie and how it is accessed.

Execution:

All cookies are set by the server via the Set-Cookie HTTP Header. A browser knows to store that cookie as a persistent cookie when it finds the keyword 'Expires=' followed by a date in the future. If there is no 'Expires=' tag, or if the specified date has already passed, then the browser will keep the cookie in memory only as a session cookie.

To view the persistent cookie set on this page, view the **HTTP response** and examine the Set-Cookie header. You should see the 'Expires=' tag with a future date specified.

Implication:

Persistent cookies are stored on the browsing clients hard drive even when that client is no longer browsing the Web site that set the client. Depending on what information is stored in the cookie, this could lead to security and privacy violations. The Office of Management and Budget has decreed that no federal websites shall use persistent cookies except in very specific situations.

Fix:

From a coding perspective, the only distinction between a session cookie and a persistent cookie is the 'Expires=' tag that specifies when a persistent cookie should expire. If a cookie has no 'Expires=' tag, then it is automatically interpreted as a session cookie. Removing the expiration date from the code that sets the cookie will change it to a session cookie.

Reference:

White House Office of Management and Budget:
Memorandum M-00-13Privacy Policies and Data Collection on Federal Web Sites

Microsoft Knowledgebase Article:
Description of Persistent and Per-Session Cookies in Internet Explorer.

Attack Request:

GET /find-a-dentist/alpha/ HTTP/1.1
Host: mot3.deltadentalins.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Crawl.EventMacro.Workflow"; SID="0D1282C59C9580A6A9A6D5E8BB433AB8";
SessionType="NamedMacro"; CrawlType="None";
X-RequestManager-Memo: sid="499"; smi="0"; Category="EventMacro.Named"; MacroName="Workflow1";
X-Request-Memo: ID="d187c270-6ba6-4b3d-90ec-a0eabf797098"; tid="158";
Pragma: no-cache
Cookie: CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5

Attack Response:

HTTP/1.1 200 OK
Date: Mon, 11 Feb 2019 22:55:40 GMT
Set-Cookie:
SMIDENTITY=RwxcvjUjFV+x7jLHq8Sp45i1ntx90xqvjJ/8JrBIVJ6sBSnsKJ7pObiJjItTXmAsybHwgOMYlR1vBmVrmksDnVOiUL99xS4q/VAPpmFm2yQuJCWFuKsXVc8EDzZ1+b7Yhncia+U3mEYpFPtkwvu6K5uLJ74P5RG4G6b5tDvG77wMMefTO4QlnB6DVBS1KJ4guGHy5HlThWOvspYEIlialbTsgJGdW/bUl4+8u7oEE1IHxJdwS0tkOjrkjqcboQY+ZCvWrKV+fQ5FJJYCn6CYC324yTbIzzhdMVMQEv4BdXTywr+PtYOT6a3iwMrc+YGKZFxSsdgkmrplMVdD39CQdTKwN0g1mrnY4zmjjrNamYefrELtupl9L6PDyB7QqfB1mHaw8gtmPA1qoGlVtOBlxqFpuPaeyi/31XInS6FYwTbzIDjVi3hwsKN+llzIA/B5TbigXUwg9has7fWhWF1OqfQm16Q6XzGBFha0u+u60Y6F4PzbA+lQgLczIjAdtxafICw7uEoBrrz0H8VsafX16H14dwcq0Jn4mi5up50FMRvV30FrJaozNE6kpDpk5XhR; expires=Wed, 10 Feb 2021 22:55:40 GMT; path=/; domain=.deltadentalins.com; secure; HTTP...TRUNCATED...

File Names:

- https://mot3.deltadentalins.com:443/find-a-dentist/alpha/

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 /find-a-dentist/alpha/js/mot-adrum.js HTTP/1.1
Host: mot3.deltadentalins.com

User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://mot3.deltadentalins.com/find-a-dentist/alpha/
Pragma: no-cache
Cookie:
SMIDENTITY=RwxcvjUjFV+x7jLHq8Sp45i1ntx90xqvjJ/8JrBIVJ6sBSnsKJ7pObiJjItTXmAsybHwgOMYlR1vBmVrmksDnVOiUL99xS4q/VAPpmFm2yQuJCWFuKsXVc8EDzZ1+b7Yhncia+U3mEYpFPtkwvu6K5uLJ74P5RG4G6b5tDvG77wMMefTO4QlnB6DVBS1KJ4guGHy5HlThWOvspYEIlialbTsgJGdW/bUl4+8u7oEE1IHxJdwS0tkOjrkjqcboQY+ZCvWrKV+fQ5FJJYCn6CYC324yTbIzzhdMVMQEv4BdXTywr+PtYOT6a3iwMrc+YGKZFxSsdgkmrplMVdD39CQdTKwN0g1mrnY4zmjjrNamYefrELtupl9L6PDyB7QqfB1mHaw8gtmPA1qoGlVtOBlxqFpuPaeyi/31XInS6FYwTbzIDjVi3hwsKN+llzIA/B5TbigXUwg9has7fWhWF1OqfQm16Q6XzGBFha0u+u60Y6F4PzbA+lQgLczIjAdtxafICw7uEoBrrz0H8VsafX16H14dwcq0Jn4mi5up50FMRvV30FrJaozNE6kpDpk5XhR;
TS01460762=01729bd698544df55c9dd98a415502142b01ad8c08cc5bcd22c4f3d3a9cf099f5be8f98486cccf697e231820655f94c159fff5ddb0c33b784b0c91dd24fe5851dcb6cb0052;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
Connection: keep-alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Crawl.EventMacro.Workflow"; SID="425C70661FE907B36686E71BC2DF4665";
SessionType="NamedMacro"; CrawlType="None";
X-RequestManager-Memo: sid="499"; smi="0"; Category="EventMacro.Named"; MacroName="Workflow1";
X-Request-Memo: ID="85aa68a4-ab3d-4199-aaa3-43ef69ba2174"; tid="81";

Attack Response:

HTTP/1.1 200 OK
Date: Mon, 11 Feb 2019 22:55:41 GMT
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Last-Modified: Tue, 15 Jan 2019 00:13:43 GMT
Content-Type: application/javascript; charset=UTF-8
Content-Length: 37915
Via: 1.1 mot3.deltadentalins.com
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Set-Cookie:
TS01460762=01729bd698544df55c9dd98a415502142b01ad8c08cc5bcd22c4f3d3a9cf099f5be8f98486cccf697e231820655f94c159fff5ddb0c33b784b0c91dd24fe5851dcb6cb0052; Path=/; Domain=.mot3.deltadentalins.com

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

File Names:

- https://mot3.deltadentalins.com:443/find-a-dentist/alpha/js/mot-adrum.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 /find-a-dentist/alpha/js/mot-adrum.js HTTP/1.1
Host: mot3.deltadentalins.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://mot3.deltadentalins.com/find-a-dentist/alpha/
Pragma: no-cache
Cookie:
SMIDENTITY=RwxcvjUjFV+x7jLHq8Sp45i1ntx90xqvjJ/8JrBIVJ6sBSnsKJ7pObiJjItTXmAsybHwgOMYlR1vBmVrmksDnVOiUL99xS4q/VAPpmFm2yQuJCWFuKsXVc8EDzZ1+b7Yhncia+U3mEYpFPtkwvu6K5uLJ74P5RG4G6b5tDvG77wMMefTO4QlnB6DVBS1KJ4guGHy5HlThWOvspYEIlialbTsgJGdW/bUl4+8u7oEE1IHxJdwS0tkOjrkjqcboQY+ZCvWrKV+fQ5FJJYCn6CYC324yTbIzzhdMVMQEv4BdXTywr+PtYOT6a3iwMrc+YGKZFxSsdgkmrplMVdD39CQdTKwN0g1mrnY4zmjjrNamYefrELtupl9L6PDyB7QqfB1mHaw8gtmPA1qoGlVtOBlxqFpuPaeyi/31XInS6FYwTbzIDjVi3hwsKN+llzIA/B5TbigXUwg9has7fWhWF1OqfQm16Q6XzGBFha0u+u60Y6F4PzbA+lQgLczIjAdtxafICw7uEoBrrz0H8VsafX16H14dwcq0Jn4mi5up50FMRvV30FrJaozNE6kpDpk5XhR;
TS01460762=01729bd698544df55c9dd98a415502142b01ad8c08cc5bcd22c4f3d3a9cf099f5be8f98486cccf697e231820655f94c159fff5ddb0c33b784b0c91dd24fe5851dcb6cb0052;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
Connection: keep-alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Crawl.EventMacro.Workflow"; SID="425C70661FE907B36686E71BC2DF4665";
SessionType="NamedMacro"; CrawlType="None";
X-RequestManager-Memo: sid="499"; smi="0"; Category="EventMacro.Named"; MacroName="Workflow1";
X-Request-Memo: ID="85aa68a4-ab3d-4199-aaa3-43ef69ba2174"; tid="81";

Attack Response:

HTTP/1.1 200 OK
Date: Mon, 11 Feb 2019 22:55:41 GMT
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Last-Modified: Tue, 15 Jan 2019 00:13:43 GMT
Content-Type: application/javascript; charset=UTF-8
Content-Length: 37915
Via: 1.1 mot3.deltadentalins.com
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Set-Cookie:
TS01460762=01729bd698544df55c9dd98a415502142b01ad8c08cc5bcd22c4f3d3a9cf099f5be8f98486cccf697e231820655f94c159fff5ddb0c33b784b0c91dd24fe5851dcb6cb0052; Path=/; Domain=.mot3.deltadentalins.com

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://mot3.deltadentalins.com:443/find-a-dentist/alpha/js/mot-adrum.js