Title

Session Cookie Not Marked as Secure

URLs

https://auth.deq.virginia.gov/
https://auth-test.deq.virginia.gov/

Vulnerability Details

Identified Cookie(s) ASP.NET_SessionId

Acunetix 360 identified a session cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack.

It is important to note that Acunetix 360 inferred from the its name that the cookie in question is session related.

Impact

This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to understand layer 2 and have gained access to a system between the victim and the web server.

Remedy

Mark all cookies used within the application as secure.

Title

Insecure HTTP Usage

URLs

http://auth.deq.virginia.gov/
http://auth-test.deq.virginia.gov/

Vulnerability Details

Acunetix 360 identified that the target website allows web browsers to access to the website over HTTP and doesn't redirect them to HTTPS.

HSTS is implemented in the target website however HTTP requests are not redirected to HTTPS. This decreases the value of HSTS implementation significantly.

For example visitors who haven't visited the HTTPS version of the website previously will not be able to take advantage of HSTS.

Impact

Users will not be able to take advantage of HSTS which almost renders the HSTS implementation useless. Not having HSTS will make MITM attacks easier for attackers.
If there is a client side redirect to HTTPS version of the website (via JavaScript or Meta tags) then you can ignore this vulnerability.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# redirect all HTTP to HTTPS
<VirtualHost *:80>
    ServerAlias *
    RewriteEngine On
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>
```

Title

Out-of-date Version (Bootstrap)

URLs

https://www.deq.virginia.gov/

Vulnerability Details

Impact

Remedy

Title

HTTP Strict Transport Security (HSTS) Policy Not Enabled

URLs

https://www.deq.virginia.gov/

Identified Version	3.3.6
Latest Version	3.4.1 (in this branch)
Overall Latest Version	5.3.3
Vulnerability Database	Result is based on 02/04/2025 15:00:00 vulnerability database content.
Retestable	

Vulnerability Details

Acunetix 360 identified that the target web site is using Bootstrap and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.
See known issues.

Remedy

Please upgrade your installation of Bootstrap to the latest stable version.

Title

Weak Ciphers Enabled

URLs

https://www.deq.virginia.gov/

List of Supported Weak Ciphers	• TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D) • TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C) • TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) • TLS_RSA_WITH_AES_128_CBC_SHA (0x002F) • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028) • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027) • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014) • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013) • TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009D) • TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009C)
Retestable	

Vulnerability Details

Acunetix 360 detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors. However, it is possible that the reported weak ciphers are not a concern in your specific environment due to factors such as **serverless architectures**, **managed services**, or **cloud-provider-controlled configurations** that do not allow modification of cipher settings.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

If your environment is serverless or managed by a cloud provider, you may consider **marking this vulnerability as a Accepted Risk**.

If further validation is needed, ensure that your **web server configuration** is reviewed and that only strong ciphers are enabled. Follow the configuration steps below to secure your communication.

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
```

```
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

4. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

   You may also use the `Disable-TlsCipherSuite` powershell command to disable certain ciphers.

```
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_AES_256_CBC_SHA"
```

   To get a formatted list of ciphers, you can use the following command.

```
Get-TlsCipherSuite | Format-Table Name
```

Remedy

Configure your web server to disallow using weak ciphers. Please consider following when selecting ciphers:

- Use at least 128 bit of encryption
- Anonymous Diffie-Hellman (ADH) suites do not provide authentication.
- Using CBC ciphers, Export ciphers, NULL cipher suites is insecure.
- RC4 is insecure.

General Information:

Scans last run: 2/7/25

Scans due to run: 3/7/25

Report pulled 3/3/25