



### Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Scan Detail

Target	<a href="https://team2dojo.eastus.cloudapp.azure.com/">https://team2dojo.eastus.cloudapp.azure.com/</a>
Scan Type	Full Scan
Start Time	Jul 7, 2021, 5:30:30 PM GMT+2
Scan Duration	49 minutes
Requests	67758
Average Response Time	126ms
Maximum Response Time	15543ms



High



Medium



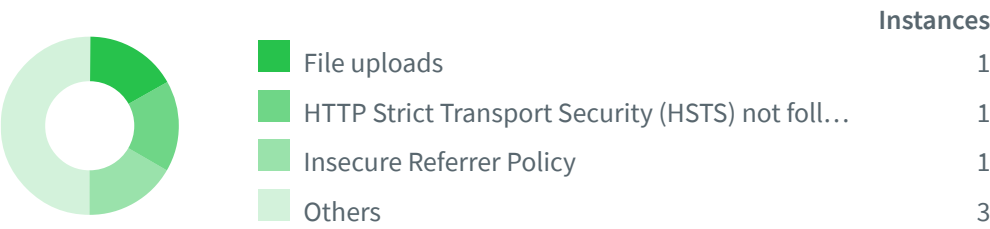
Low



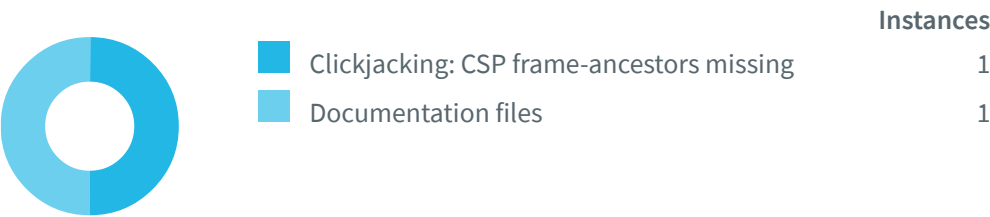
Informational

Severity	Vulnerabilities	Instances
High	1	1
Medium	4	4
Low	2	2
Informational	6	6
Total	13	13

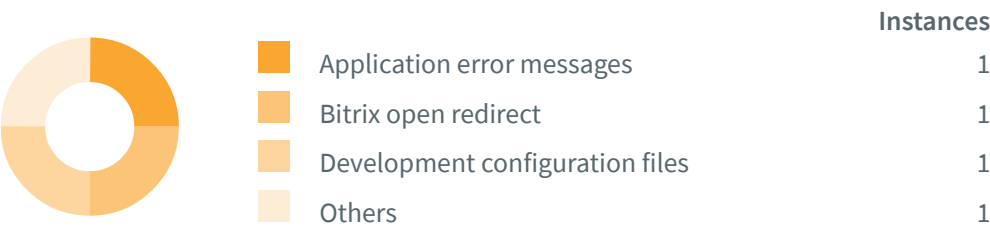
## Informational



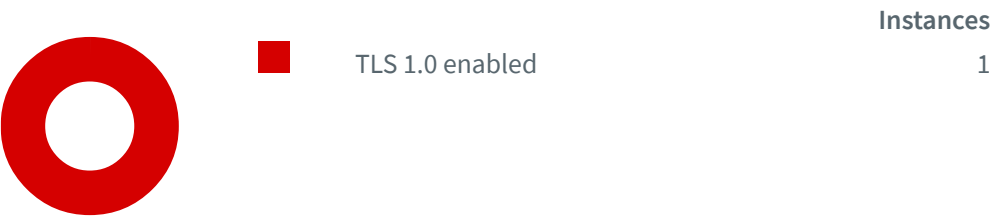
## Low Severity
















## Medium Severity



## High Severity



# Impacts

SEVERITY	IMPACT	
 High	<b>1</b>	TLS 1.0 enabled
 Medium	<b>1</b>	Application error messages
 Medium	<b>1</b>	Bitrix open redirect
 Medium	<b>1</b>	Development configuration files
 Medium	<b>1</b>	TLS 1.1 enabled
 Low	<b>1</b>	Clickjacking: CSP frame-ancestors missing
 Low	<b>1</b>	Documentation files
 Informational	<b>1</b>	File uploads
 Informational	<b>1</b>	HTTP Strict Transport Security (HSTS) not following best practices
 Informational	<b>1</b>	Insecure Referrer Policy
 Informational	<b>1</b>	Javascript Source map detected
 Informational	<b>1</b>	Outdated JavaScript libraries
 Informational	<b>1</b>	Possible server path disclosure (Unix)

# TLS 1.0 enabled

---

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

## Impact

---

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

---

<https://team2dojo.eastus.cloudapp.azure.com/>

Confidence: 100%

The SSL server (port: 443) encrypts traffic using TLSv1.0.

## Recommendation

---

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

## References

---

[RFC 8996: Deprecating TLS 1.0 and TLS 1.1](https://tools.ietf.org/html/rfc8996)

<https://tools.ietf.org/html/rfc8996>

[Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)

<https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>

[PCI 3.1 and TLS 1.2 \(Cloudflare Support\)](https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

<https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2>

# Application error messages

---

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).

## Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

### <https://team2dojo.eastus.cloudapp.azure.com/>

Application error messages:

- <https://team2dojo.eastus.cloudapp.azure.com/api/localUser/updateUser>  
**SyntaxError: Unexpected token**
- [https://team2dojo.eastus.cloudapp.azure.com/api/instructor\\_link](https://team2dojo.eastus.cloudapp.azure.com/api/instructor_link)  
**SyntaxError: Unexpected token**
- <https://team2dojo.eastus.cloudapp.azure.com/api/teams>  
**SyntaxError: Unexpected token**

## Request

```
POST /api/localUser/updateUser HTTP/1.1
Content-Type: application/json;charset=UTF-8
Referer: https://team2dojo.eastus.cloudapp.azure.com/
Cookie: connect.sid=s%3AuPNp2zgWAOL2BVleqbOQl_SvpzO-6itY.k9gxJRl7uCMwb1suM0GAHQqxP8wcxmsfocga8HvGloE
xsrftoken: QfA1eMW3WRrh_xgIOM5eDzwKpmdhkh89hcRive-tRY8AQzoyf3KiOWJEHwvxkiPzAPBOaTtxKTaaKL_UHYKgiA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 42
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: team2dojo.eastus.cloudapp.azure.com
Connection: Keep-alive

12345'"\"';|]*%00{%0d%0a<%00>%bf%27'🕒
```

## Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

## Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

Internal IP addresses

Secrets (passwords, keys, tokens...)  
Operating system distributions  
Software version numbers  
Missing security patches  
Application stack traces  
SQL statements  
Location of sensitive files (backups, temporary files...)  
Location of sensitive resources (databases, caches, code repositories...)

## References

---

### [PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

### [Improper Error Handling](#)

[https://www.owasp.org/index.php/Improper\\_Error\\_Handling](https://www.owasp.org/index.php/Improper_Error_Handling)

## Bitrix open redirect

---

Acunetix has detected that the web application is based on Bitrix. This version of Bitrix has an open redirect vulnerability.

Open redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

## Impact

---

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, spammers.

---

**<https://team2dojo.eastus.cloudapp.azure.com/>**

## Request

---

```
GET /bitrix/redirect.php?goto=https://team2dojo.eastus.cloudapp.azure.com%252F@bxss.me/ HTTP/1.1
Cookie:
connect.sid=s%3AUw2B32IN6tOeZg5NZHNVFCvcm_M_J4oh.UGeJi4hb7XN1hmZ92RXCAVFSRyQtxBNSnliI%2BR3VrvNY
xsrfToken: QfA1eMW3WRrh_xgIOM5eDzwKPmdhkh89hcRive-tRY8AQzoyf3KiOWJEHwvxkiPzAPBOaTtxKTaaKL_UHYKgiA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: team2dojo.eastus.cloudapp.azure.com
```

## Recommendation

---

Upgrade to the latest version of Bitrix

## References

---

### [Unvalidated Redirects and Forwards Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)

[https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated\\_Redirects\\_and\\_Forwards\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)

# Development configuration files

---

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

## Impact

---

These files may disclose sensitive information. This information can be used to launch further attacks.

---

### <https://team2dojo.eastus.cloudapp.azure.com/>

Development configuration files:

- <https://team2dojo.eastus.cloudapp.azure.com/public/jquery/package.json>

`package.json => Grunt configuration file. Grunt is a JavaScript task runner.`

- <https://team2dojo.eastus.cloudapp.azure.com/public/highlightjs/composer.json>

`composer.json => Composer configuration file. Composer is a dependency manager for PHP.`

- <https://team2dojo.eastus.cloudapp.azure.com/public/bootstrap/package.json>

`package.json => Grunt configuration file. Grunt is a JavaScript task runner.`

- <https://team2dojo.eastus.cloudapp.azure.com/public/angular/bower.json>

`bower.json => Bower manifest file. Bower is a package manager for the web.`

- <https://team2dojo.eastus.cloudapp.azure.com/public/angular-route/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

## Request

---

```
GET /public/jquery/package.json HTTP/1.1
Cookie: connect.sid=s%3AuPNp2zgWAOL2BVleqbOQl_SvpzO-6itY.k9gxJRl7uCMwb1suM0GAHQqxP8wcxmsfocga8HvGloE
xsrftoken: FGYS7REZQxTTttxyxE3Mxi6Df4gRy7wBVO3V0Ck6WxX4Aov1GZBUoKWI9AA5CnjK9_vjQXJ2YIpxxrKMHjRfmA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: team2dojo.eastus.cloudapp.azure.com
Connection: Keep-alive
```

## Recommendation

---

Remove or restrict access to all configuration files accessible from internet.

# TLS 1.1 enabled

---

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

## Impact

---

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

<https://team2dojo.eastus.cloudapp.azure.com/>

Confidence: 100%

The SSL server (port: 443) encrypts traffic using TLSv1.1.

## Recommendation

---

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

## References

---



[RFC 8996: Deprecating TLS 1.0 and TLS 1.1](https://tools.ietf.org/html/rfc8996)

<https://tools.ietf.org/html/rfc8996>

[Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)

<https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>

[PCI 3.1 and TLS 1.2 \(Cloudflare Support\)](https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

<https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2>

## Clickjacking: CSP frame-ancestors missing

---

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return a **frame-ancestors** directive in the Content-Security-Policy header which means that this website could be at risk of a clickjacking attack. The frame-ancestors directives can be used to indicate whether or not a browser should be allowed to render a page inside a frame. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

### Impact

---

The impact depends on the affected web application.

---

**<https://team2dojo.eastus.cloudapp.azure.com/>**

Paths without CSP frame-ancestors:

- <https://team2dojo.eastus.cloudapp.azure.com/public/index.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/trainingModules.html>
- <https://team2dojo.eastus.cloudapp.azure.com/public/locallogin.html>
- <https://team2dojo.eastus.cloudapp.azure.com/main>
- <https://team2dojo.eastus.cloudapp.azure.com/static/report.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/leaderboard.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/dashboard.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks.html>

- <https://team2dojo.eastus.cloudapp.azure.com/static/activity.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/authenticationByDefault.html>
- <https://team2dojo.eastus.cloudapp.azure.com/api/salt>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/checkBoundaries.html>
- <https://team2dojo.eastus.cloudapp.azure.com/public/>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/disableXmlExternalEntities.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/displayGenericErrorMessages.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/enforceSafeConfig.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/enforceSafeDeserialization.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/indirectObjectReferences.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/integrityVerification.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/inputAllowListing.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/keep3rdPartyUpToDate.html>

## Request

---

```
GET /public/index.html HTTP/1.1
Host: team2dojo.eastus.cloudapp.azure.com
Pragma: no-cache
Cache-Control: no-cache
upgrade-insecure-requests: 1
accept-language: en-US
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
```

## Recommendation

Configure your web server to include a CSP header with frame-ancestors directive and an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

## References

### [OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

[https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking\\_Defense\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

### [CSP: frame-ancestors](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors>

### [The X-Frame-Options response header](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

## Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

## Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

### <https://team2dojo.eastus.cloudapp.azure.com/>

Documentation files:

- <https://team2dojo.eastus.cloudapp.azure.com/public/open-iconic/readme.md>

File contents (first 100 characters):

```
[Open Iconic v1.1.1] (http://useiconic.com/open)
```

```
=====
```

```
### Open Iconic is the open source sibl ...
```

- <https://team2dojo.eastus.cloudapp.azure.com/public/jquery/readme.md>

File contents (first 100 characters):

```
# jQuery
```

```
> jQuery is a fast, small, and feature-rich JavaScript library.
```

For information on how to ...

- <https://team2dojo.eastus.cloudapp.azure.com/public/jquery/license.txt>

File contents (first 100 characters):

```
Copyright OpenJS Foundation and other contributors, https://openjsf.org/
```

```
Permission is hereby grant ...
```

- <https://team2dojo.eastus.cloudapp.azure.com/public/bootstrap/readme.md>

File contents (first 100 characters):

```
<p align="center">
<a href="https://getbootstrap.com/">
<img src="https://getbootstrap.com/doc ...
```

- <https://team2dojo.eastus.cloudapp.azure.com/public/angular/readme.md>

File contents (first 100 characters):

```
# packaged angular
```

```
This repo is for distribution on `npm` and `bower`. The source for this module i
...
```

- <https://team2dojo.eastus.cloudapp.azure.com/public/angular-route/readme.md>

File contents (first 100 characters):

```
# packaged angular-route
```

```
This repo is for distribution on `npm` and `bower`. The source for this mo ...
```

## Request

---

```
GET /public/open-iconic/readme.md HTTP/1.1
Cookie: connect.sid=s%3AuPNp2zgWAOL2BVleqbOQl_SvpzO-6itY.k9gxJRl7uCMwb1suM0GAHQqxP8wcxmsfocga8HvGloE
xsrftoken: FGYS7REZQxTTttxyxE3Mxi6Df4gRy7wBVO3V0Ck6WxX4Aov1GZBUoKWI9AA5CnjK9_vjQXJ2YIpxxrKMHjRfmA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: team2dojo.eastus.cloudapp.azure.com
Connection: Keep-alive
```

## Recommendation

---

Remove or restrict access to all documentation file accessible from internet.

# File uploads

---

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

## Impact

---

If the uploaded files are not safely checked an attacker may upload malicious files.

---

### <https://team2dojo.eastus.cloudapp.azure.com/>

Pages with file upload forms:

- <https://team2dojo.eastus.cloudapp.azure.com/static/report.html>

```
Form name: <empty>
Form action: <empty>
Form method: GET
Form file input: fileUpload [file]
```

## Request

---

```
GET /static/report.html HTTP/1.1
Host: team2dojo.eastus.cloudapp.azure.com
accept: application/json, text/plain, */*
accept-language: en-US
cookie: connect.sid=s%3AuPNp2zgWAOL2BVleqbOQl_SvpzO-6itY.k9gxJRl7uCMwb1suM0GAHQqxP8wcxmsfocga8HvGloE
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://team2dojo.eastus.cloudapp.azure.com/main
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
```

## Recommendation

---

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

# HTTP Strict Transport Security (HSTS) not following best practices

---

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

## Impact

---

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

---

### <https://team2dojo.eastus.cloudapp.azure.com/>

URLs where HSTS configuration is not according to best practices:

- <https://team2dojo.eastus.cloudapp.azure.com/public/index.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/trainingModules.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/public/locallogin.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/main> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/report.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/leaderboard.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/dashboard.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/activity.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/authenticationByDefault.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/api/salt> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/checkBoundaries.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/public/> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/disableXmlExternalEntities.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/displayGenericErrorMessages.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/enforceSafeConfig.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/enforceSafeDeserialization.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/indirectObjectReferences.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/integrityVerification.html> - No includeSubDomains directive
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/inputAllowListing.html> - No includeSubDomains directive

- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/keep3rdPartyUpToDate.html> - No includeSubDomains directive

## Request

---

```
GET /public/index.html HTTP/1.1
Host: team2dojo.eastus.cloudapp.azure.com
Pragma: no-cache
Cache-Control: no-cache
upgrade-insecure-requests: 1
accept-language: en-US
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
```

## Recommendation

---

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

## References

---

[hstspreload.org](https://hstspreload.org)

<https://hstspreload.org/>

[MDN: Strict-Transport-Security](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

# Insecure Referrer Policy

---

Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

## Impact

---

## **<https://team2dojo.eastus.cloudapp.azure.com/>**

URLs where Referrer Policy configuration is insecure:

- <https://team2dojo.eastus.cloudapp.azure.com/public/index.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/trainingModules.html>
- <https://team2dojo.eastus.cloudapp.azure.com/public/locallogin.html>
- <https://team2dojo.eastus.cloudapp.azure.com/main>
- <https://team2dojo.eastus.cloudapp.azure.com/static/report.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/leaderboard.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/dashboard.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/activity.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/authenticationByDefault.html>
- <https://team2dojo.eastus.cloudapp.azure.com/api/salt>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/checkBoundaries.html>
- <https://team2dojo.eastus.cloudapp.azure.com/public/>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/disableXmlExternalEntities.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/displayGenericErrorMessages.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/enforceSafeConfig.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/enforceSafeDeserialization.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/indirectObjectReferences.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/integrityVerification.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/inputAllowListing.html>
- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/keep3rdPartyUpToDate.html>



## Request

---

```
GET /public/index.html HTTP/1.1
Host: team2dojo.eastus.cloudapp.azure.com
Pragma: no-cache
Cache-Control: no-cache
upgrade-insecure-requests: 1
accept-language: en-US
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4298.0 Safari/537.36
```

## Recommendation

---

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

## References

---

### Referrer-Policy

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

# Javascript Source map detected

---

Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.

## Impact

---

Access to source maps may help an attacker to read and debug Javascript code. It simplifies finding client-side vulnerabilities

---

<https://team2dojo.eastus.cloudapp.azure.com/>

Confidence: 80%

URLs where links to SourceMaps were found:

- sourceMappingURL in JS body -  
`https://team2dojo.eastus.cloudapp.azure.com/public/bootstrap/dist/js/bootstrap.min.js`
- sourceMappingURL in JS body - `https://team2dojo.eastus.cloudapp.azure.com/public/angular-route/angular-route.min.js`
- sourceMappingURL in JS body - `https://team2dojo.eastus.cloudapp.azure.com/public/angular/angular.min.js`

## Request

---

```
GET /public/bootstrap/dist/js/bootstrap.min.js HTTP/1.1
Host: team2dojo.eastus.cloudapp.azure.com
Pragma: no-cache
Cache-Control: no-cache
accept-language: en-US
accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://team2dojo.eastus.cloudapp.azure.com/public/index.html
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
```

## Recommendation

---

According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information

## References

---

[Using sourcemaps on production without exposing the source code](https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89)

`https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89`

[SPA source code recovery by un-Webpacking source maps](https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d)

`https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d`

# Outdated JavaScript libraries

---

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

## Impact

Consult References for more information.

<https://team2dojo.eastus.cloudapp.azure.com/>

Confidence: 95%

- **bootstrap.js 4.6.0**
  - URL: <https://team2dojo.eastus.cloudapp.azure.com/public/bootstrap/dist/js/bootstrap.min.js>
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - <https://github.com/twbs/bootstrap/releases>

## Request

```
GET /public/bootstrap/dist/js/bootstrap.min.js HTTP/1.1
Host: team2dojo.eastus.cloudapp.azure.com
Pragma: no-cache
Cache-Control: no-cache
accept-language: en-US
accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://team2dojo.eastus.cloudapp.azure.com/public/index.html
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
```

## Recommendation

Upgrade to the latest version.

# Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

## Impact

Possible sensitive information disclosure.

### <https://team2dojo.eastus.cloudapp.azure.com/>

Pages with paths being disclosed:

- <https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/indirectObjectReferences.html>  
    >/var/www/myapp/files/docs/accounts.xls

## Request

```
GET /static/codeBlocks/indirectObjectReferences.html HTTP/1.1
Referer: https://team2dojo.eastus.cloudapp.azure.com/static/codeBlocks/codeBlocksDefinitions.json
Cookie: connect.sid=s%3AlQIU9CSXHujmvFCyFei2gZMd0-
jib35q.ZbGvuHjrRe7H5n7pwmPAoQgUMW9NIkgOgfO1%2BXIf3Cc
xsrftoken: aogMsnCanuuidyUhcgc9Ylj3qihlCdLwcYQojQoaHSkWlymRqfM4HSoXMKYOKWus5JHWlcfwMtUBTlinZpPVbA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/88.0.4298.0 Safari/537.36
Host: team2dojo.eastus.cloudapp.azure.com
Connection: Keep-alive
```

## Recommendation


Prevent this information from being displayed to the user.

## References

### [Full Path Disclosure](#)

[https://www.owasp.org/index.php/Full\\_Path\\_Disclosure](https://www.owasp.org/index.php/Full_Path_Disclosure)

## Coverage

 <https://team2dojo.eastus.cloudapp.azure.com>

 #fragments

 attacks

 blocks

 rules

 api

 activity

 heartbeat

 localUser

 updateUser

 Inputs


 application/json;charset=UTF-8

 profileInfo.curPassword, profileInfo.newPassword


 report

 status

 statusMessage

 teams

 user

 badges

 challengeCode

 team

 activity

 Inputs

 query


 challengeStats

 instructor\_link

 Inputs

 application/json;charset=UTF-8

 instructorId

 modules


 moduleStats

 reportUpload

 Inputs

 reportCSV

 salt

 teams

 Inputs

 application/json;charset=UTF-8

 name

 teamStats

 Inputs

 limit

 user

 users

 v1

 v2

 v3

 v4

 v5

 challenges

 descriptions

 :moduleId

 codeBlocks

 inputAllowListing

 public

 #fragments

 attacks

 blocks

 rules

 angular-route

 angular-route.min.js

 angular-route.min.js.map

 bower.json

 readme.md

 angular

 angular.min.js

 angular.min.js.map

 bower.json

 readme.md

 bootstrap

 dist

 css

 bootstrap.min.css

 js

 bootstrap.min.js

 bootstrap.min.js.map

 js

 src

 tools

 package.json

 readme.md

 canvas-confetti

 dist

 confetti.browser.js

 highlightjs

 styles

 darcula.css

 darkula.css

 composer.json

 highlight.pack.min.js

 jquery

 dist

 jquery.min.js

 src

 core

 data

 license.txt

 package.json

 readme.md

- open-iconic
  - font
    - css
      - open-iconic-bootstrap.min.css

- fonts
  - open-iconic.otf

- readme.md

- provider
  - local

- authFail.html

- index.html
  - #fragments
    - attacks
    - blocks
    - rules

- locallogin
  - Inputs
    - POST** loginCaptcha, password, username

- locallogin.html

- privacy

- providers


- static
  - codeBlocks
    - authenticationByDefault.html
    - checkBoundaries.html
    - codeBlocksDefinitions.json
    - disableXmlExternalEntities.html
    - displayGenericErrorMessages.html
    - enforceSafeConfig.html
    - enforceSafeDeserialization.html
    - indirectObjectReferences.html
    - inputAllowListing.html
    - integrityVerification.html
    - keep3rdPartyUpToDate.html



 loginBestPractices.html

 neutralizeOutput.html

 parameterizedCommands.html

 principleOfLeastPrivilege.html

 requestForgeryPrevention.html

 resourceSeparation.html

 safeMemoryManagement.html

 serverSideValidation.html

 useStrongDataEncryption.html

 activity.html

 activityCtrl.js

 challengesCtrl.js

 codeBlocks.html

 codeBlocksCtrl.js

 dashboard.html

 dashboardCtrl.js


 dataSvc.js

 leaderboard.html

 Inputs

 teamListChoice

 leaderboardCtrl.js

 main-app.js

 report.html

 Inputs

 fileUpload

 reportCtrl.js

 solutionCtrl.js

 submitCodeCtrl.js

 trainingModules.html

 trainingModulesCtrl.js

 activity

 api

 dashboard

 leaderboard

 logout

 main

 #fragments

 !

 !/

 !/activity

 !/codeBlocks/inputAllowListing

 !/dashboard

 !/leaderboard

 !/report

 !activity

 !codeBlocks/inputAllowListing

 !dashboard

 !leaderboard

 !report

 Inputs

 userTeamListChoice

 report