netsparker®
web application security scanner

NETSPARKER SCAN REPORT SUMMARY

TARGET URL	https://dare2compete.com/
SCAN DATE	29-10-2021 12:24:52
REPORT DATE	29-10-2021 13:26:41
SCAN DURATION	00:50:51
NETSPARKER VERSION	4.8.1.14104-master-a24f36a

Total Requests
40317

Average Speed
13.21 req/sec.

15
Identified

6
Confirmed

0
Critical

10
Informational

SCAN SETTINGS

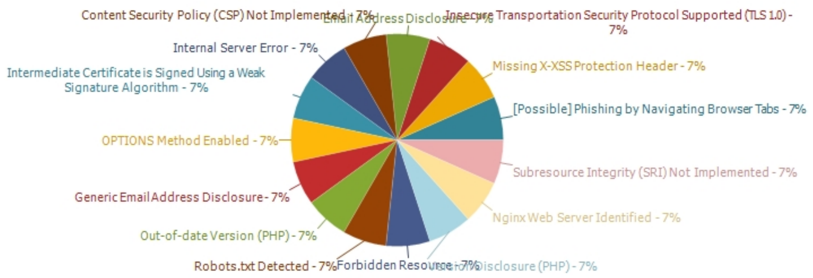
ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Server-Side Request Forgery (Pattern Based), Cross-Origin Resource Sharing (CORS), HTTP Methods, Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)
URL REWRITE MODE	Heuristic

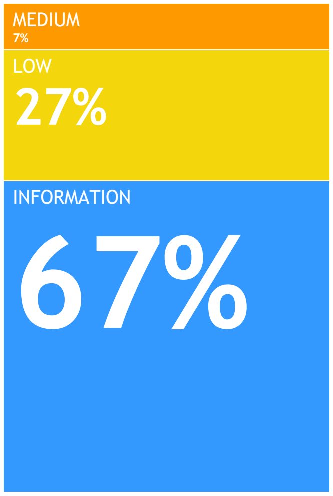
DETECTED URL REWRITE RULES	/blog/{param1}
	/competition/{param1}
	/{param1}

Authentication

Scheduled

VULNERABILITIES





VULNERABILITY SUMMARY

URL	Parameter	Method	Vulnerability	Confirmed
https://dare2compete.com/		GET	Insecure Transportation Security Protocol Supported (TLS 1.0)	Yes
		GET	Intermediate Certificate is Signed Using a Weak Signature Algorithm	Yes
		GET	Nginx Web Server Identified	No
		GET	Subresource Integrity (SRI) Not Implemented	No
		GET	Content Security Policy (CSP) Not Implemented	No
https://dare2compete.com/11-es5.c123e7c50d3edfa9754b.js		GET	Email Address Disclosure	No
https://dare2compete.com/21-es5.6d91eb490c866d544cb2.js		GET	Generic Email Address Disclosure	No
https://dare2compete.com/amp		GET	[Possible] Phishing by Navigating Browser Tabs	No
https://dare2compete.com/api/images/600/600/		OPTIONS	OPTIONS Method Enabled	Yes
https://dare2compete.com/api/images/600/600/c%3a%5cboot.ini		GET	Internal Server Error	Yes
https://dare2compete.com/etc/passwd		GET	Forbidden Resource	Yes
https://dare2compete.com/http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,payment,oppstatus,eligible		GET	Out-of-date Version (PHP)	No
		GET	Version Disclosure (PHP)	No
https://dare2compete.com/robots.txt		GET	Robots.txt Detected	Yes
https://dare2compete.com/runtime-es2015.d0e31b794685186052f7.js		GET	Missing X-XSS Protection Header	No

1. Out-of-date Version (PHP)

1 TOTAL
MEDIUM

Netsparker identified you are using an out-of-date version of PHP.

Impact

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

Remedy

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

Remedy References

- Downloading PHP

Known Vulnerabilities in this Version

PHP Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.

External References

- CVE-2021-21706

PHP Improper Input Validation Vulnerability

In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function with FILTER_VALIDATE_URL parameter, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision.

External References

- CVE-2021-21705

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server could cause crashes in various database functions, such as getAttribute(), execute(), fetch() and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption.

External References

- CVE-2021-21704

Classification

OWASP 2013-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310

1.1. https://dare2compete.com/http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,payment,oppstatus,eligible

https://dare2compete.com/http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,paymen...

Identified Version

7.4.19 (contains 3 medium vulnerabilities)

Latest Version

8.0.12

Vulnerability Database

Result is based on 27-10-2021 vulnerability database content.

Certainty

Request

```
GET /http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,payment,oppstatus,eligible HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Referer: https://dare2compete.com/amp
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 404 Not Found
X-Amz-Cf-Pop: BOM52-C1
Server: nginx
X-Amz-Cf-Id: g4aOFnop7gXxBpLr64V4WYgKMNuqYRYcTibEuWERR8sMJ-h3ct3-aA==
X-Powered-By: PHP/7.4.19

Connection: keep-alive
Via: 1.1 1ad884bdec2db9559f6147db99ff9e97.cloudfront.net (CloudFront)
X-Cache: Error from cloudfront
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 29 Oct 2021 07:13:28 GMT
Vary: Accept-Encoding

File not found.
```

2. Internal Server Error

1 TOTAL

LOW

CONFIRMED

1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

Classification

2.1. https://dare2compete.com/api/images/600/600/c%3a%5cboot.ini Confirmed

https://dare2compete.com/api/images/600/600/c%3a%5cboot.ini

Parameters

Parameter	Type	Value
URI-BASED	Full URL	c%3a%5cboot.ini

Request

```
GET /api/images/600/600/c%3a%5cboot.ini HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 500 Internal Server Error

X-Amz-Cf-Pop: BOM52-C1
Server: nginx
X-Amz-Cf-Id: I2E2x9B1tnzyn3xVcFkr_aKQy9Yfj0oNO4jV-9TuoL-nNOmBFBozGw==
Expires: -1
Connection: keep-alive
Via: 1.1 a2bc696ee5c3bea07f5d64c35f5db098.cloudfront
…
```

3. Version Disclosure (PHP)

1 TOTAL

LOW

Netsparker identified a version disclosure (PHP) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of PHP.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the `SERVER` header of its HTTP response.

Classification

CWE-205 CAPEC-170 WASC-45 HIPAA-164.306(A), 164.308(A)

3.1. https://dare2compete.com/http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,payment,oppstatus,eligible

https://dare2compete.com/http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,paymen...

Extracted Version

7.4.19

Certainty

Request

```
GET /http%3a%2f%2fr87.com%2fn%3f.php?filters=,all,open,all&types=teamsize,payment,oppstatus,eligible HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Referer: https://dare2compete.com/amp
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 404 Not Found
X-Amz-Cf-Pop: BOM52-C1
Server: nginx
X-Amz-Cf-Id: g4aOFnop7gXxBpLr64V4WYgKMNuqYRYcTibEuWERR8sMJ-h3ct3-aA==
X-Powered-By: PHP/7.4.19

Connection: keep-alive
Via: 1.1 1ad884bdec2db9559f6147db99ff9e97.cloudfront.net (CloudFront)
X-Cache: Error from cloudfront
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 29 Oct 2021 07:13:28 GMT
Vary: Accept-Encoding

File not found.
```

4. Insecure Transportation Security Protocol Supported (TLS 1.0)

1 TOTAL

LOW

CONFIRMED

1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

  ```
  SSLProtocol +TLSv1.1 +TLSv1.2
  ```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1`.

  ```
  ssl_protocols TLSv1.1 TLSv1.2;
  ```

- For Microsoft IIS, you should make some changes on the system registry.
  1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
     ```

  3. Locate a key named `Server` or create if it doesn't exist.
  4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".

External References

- How to disable TLS v1.0
- OWASP - Insecure Configuration Management
- OWASP - Insufficient Transport Layer Protection
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS
- Browser Exploit Against SSL/TLS Attack (BEAST)

Classification

OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-327 CAPEC-217 WASC-4

4.1. https://dare2compete.com/ Confirmed

https://dare2compete.com/

Request

```
[NETSPARKER] SSL Connection
```

Response

```
[NETSPARKER] SSL Connection
```

5. [Possible] Phishing by Navigating Browser Tabs

1 TOTAL

LOW

Opened windows through normal hrefs with target="_blank" can modify window.opener.location and replace the parent webpage with something else, even on a different origin.

While this doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab.

Impact

If the links lack of rel="noopener noreferrer" attribute, third party site can change the URL of source tab using window.opener.location.assign and trick the user as if he is still in a trusted page and lead him to enter his secret information or credentials to this malicious copy.

Remedy

To prevent pages from abusing window.opener, use *rel=noopener*. This ensures window.opener is null in Chrome 49 and Opera 36.

For older browsers and in Firefox, you could use *rel=noreferrer* which also disables the Referer HTTP header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Target="_blank" - the most underestimated vulnerability ever
- Blankshield & reverse tabnabbing attacks

Classification

OWASP 2013-A5

5.1. https://dare2compete.com/amp

https://dare2compete.com/amp

External Links

```
https://reliancetup.in/
```

Certainty

🟥

Request

```
GET /amp HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Referer: https://dare2compete.com/76-es5.f1b3219e400eb4b008bf.js
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
…
</amp-img>
</a>
</li>
<li>

<a href="https://reliancetup.in/" target="_blank">
<amp-img
alt="service-banner"
src="https://dare2compete.co
…
```

6. Forbidden Resource

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification

OWASP-PC-C8

6.1. https://dare2compete.com/etc/passwd Confirmed

https://dare2compete.com/etc/passwd

Parameters

Parameter	Type	Value
URI-BASED	Full URL	/etc/passwd

Request

```
GET /etc/passwd HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 403 Forbidden

Server: awselb/2.0
X-Amz-Cf-Id: hJiMrcBneHooV96_qH2F2ro2i0vc42bxdnOT3tgx_CBQphh5V-FduQ==
Connection: keep-alive
Via: 1.1 bd2d90f72f6306ec273a5dae120fe042.cloudfront.net (CloudFront)
Content-Length: 520
X-Cache: Error from cloudfront
Content-Type: text/html
X-Amz-Cf-Pop: BOM51-C2
Date: Fri, 29 Oct 2021 06:55:32 GMT

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

7. Email Address Disclosure

1 TOTAL
INFORMATION

Netsparker identified an email address disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- Wikipedia - Email Spam

Classification

CWE-200 CAPEC-118 WASC-13 OWASP-PC-C7

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Base: 5.3 (Medium)
Temporal: 5.3 (Medium)
Environmental: 5.3 (Medium)

7.1. https://dare2compete.com/11-es5.c123e7c50d3edfa9754b.js

https://dare2compete.com/11-es5.c123e7c50d3edfa9754b.js

Certainty

Request

```
GET /11-es5.c123e7c50d3edfa9754b.js HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Accept: */*
Referer: https://dare2compete.com/p/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
…
xt"](56,"You may also try changing your internet - mobile hotspot, wifi etc. "),r["\u0275\u0275elementEnd"](),r["\u0275\u0275elementStart"](57,"li"),r["\u0275\u0275text"](58,"Please shoot an email to support@dare2compete.com with a screenshot of the
page where you are facing a problem and your registered email id. Please note that we won't be helping you make decisions and any email asking us to take decisions will not b
…
```

8. Robots.txt Detected

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected a `Robots.txt` file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.

`Robots.txt` is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag` can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag` you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag` resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf` or an `.htaccess` file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
 # Don't index PDF files.
 Header set X-Robots-Tag "noindex, nofollow"
</Files>

<Files ~ "\.(png|jpe?g|gif)$">
 #Don't index image files.
 Header set X-Robots-Tag "noindex"
</Files>
```

External References

- [Controlling Crawling and Indexing]
- [X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag]

Classification

OWASP-PC-C7

8.1. https://dare2compete.com/robots.txt Confirmed

https://dare2compete.com/robots.txt

Interesting Robots.txt Entries

- Disallow: /p/*
- Disallow: /

Request

```
GET /robots.txt HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
…
a: 1.1 f282fe8093ec9f703de053518375c0f2.cloudfront.net (CloudFront)
Last-Modified: Tue, 26 Oct 2021 07:43:18 GMT
Content-Type: text/plain
Date: Fri, 29 Oct 2021 06:55:14 GMT
Content-Encoding:

User-agent: *
Disallow: /p/*

User-agent: Balihoo
Disallow: /

User-agent: BotRightHere
Disallow: /

User-agent: WebZip
Disallow: /

User-agent: larbin
Disallow: /

User-agent: b2w/0.1
Disallow: /

User-agent: Copernic
Disallow: /

User-agent: psbot
Disallow: /

User-agent: Python-urllib
Disallow: /

User-agent: NetMechanic
Disallow: /

User-agent: URL_Spider_Pro
Disallow: /

User-agent: CherryPicker
Disallow: /

User-agent: EmailCollector
Disallow: /

User-agent: EmailSiphon
Disallow: /

User-agent: WebBandit
Disallow: /

User-agent: EmailWolf
Disallow: /

User-agent: ExtractorPro
Disallow: /

User-agent: CopyRightCheck
Disallow: /

User-agent: Crescent
Disallow: /

User-agent: SiteSnagger
Disallow: /

User-agent: ProWebWalker
Disallow: /

User-agent: CheeseBot
Disallow: /

User-agent: LNSpiderguy
Disallow: /

User-agent: Alexibot
Disallow: /

User-agent: Teleport
Disallow: /

User-agent: TeleportPro
Disallow: /

User-agent: MIIxpc
Disallow: /

User-agent: Telesoft
Disallow: /

User-agent: Website Quester
Disallow: /

User-agent: WebZip
Disallow: /

User-agent: moget/2.1
Disallow: /

User-agent: WebZip/4.0
Disallow: /

User-agent: WebStripper
Disallow: /

User-agent: WebSauger
Disallow: /

User-agent: WebCopier
Disallow: /

User-agent: NetAnts
Disallow: /

User-agent: Mister PiX
Disallow: /

User-agent: WebAuto
Disallow: /

User-agent: TheNomad
Disallow: /

User-agent: WWW-Collector-E
Disallow: /

User-agent: RMA
Disallow: /

User-agent: libWeb/clsHTTP
Disallow: /

User-agent: asterias
Disallow: /

User-agent: httplib
Disallow: /

User-agent: turingos
Disallow: /

User-agent: spanner
Disallow: /

User-agent: InfoNaviRobot
Disallow: /

User-agent: Harvest/1.5
Disallow: /

User-agent: Bullseye/1.0
Disallow: /

User-agent: Mozilla/4.0 (compatible; BullsEye; Windows 95)
Disallow: /

User-agent: Crescent Internet ToolPak HTTP OLE Control v.1.0
Disallow: /

User-agent: CherryPickerSE/1.0
Disallow: /

User-agent: CherryPickerElite/1.0
Disallow: /
```

```
User-agent: WebBandit/3.50
Disallow: /

User-agent: NICErsPRO
Disallow: /

User-agent: Microsoft URL Control - 5.01.4511
Disallow: /

User-agent: DittoSpyder
Disallow: /

User-agent: Foobot
Disallow: /

User-agent: SpankBot
Disallow: /

User-agent: BotALot
Disallow: /

User-agent: lwp-trivial/1.34
Disallow: /

User-agent: lwp-trivial
Disallow: /

User-agent: BunnySlippers
Disallow: /

User-agent: Microsoft URL Control - 6.00.8169
Disallow: /

User-agent: URLy Warning
Disallow: /

User-agent: Wget/1.6
Disallow: /

User-agent: Wget/1.5.3
Disallow: /

User-agent: Wget
Disallow: /

User-agent: LinkWalker
Disallow: /

User-agent: cosmos
Disallow: /

User-agent: moget
Disallow: /

User-agent: hloader
Disallow: /

User-agent: humanlinks
Disallow: /

User-agent: LinkextractorPro
Disallow: /

User-agent: Offline Explorer
Disallow: /

User-agent: Mata Hari
Disallow: /

User-agent: LexiBot
Disallow: /

User-agent: Web Image Collector
Disallow: /

User-agent: The Intraformant
Disallow: /

User-agent: True_Robot/1.0
Disallow: /

User-agent: True_Robot
Disallow: /

User-agent: BlowFish/1.0
Disallow: /

User-agent: JennyBot
Disallow: /

User-agent: MIIxpc/4.2
Disallow: /

User-agent: BuiltBotTough
Disallow: /

User-agent: ProPowerBot/2.14
Disallow: /

User-agent: BackDoorBot/1.0
Disallow: /

User-agent: toCrawl/UrlDispatcher
Disallow: /

User-agent: WebEnhancer
Disallow: /

User-agent: suzuran
Disallow: /

User-agent: TightTwatBot
Disallow: /

User-agent: VCI WebViewer VCI WebViewer Win32
Disallow: /

User-agent: VCI
Disallow: /

User-agent: Szukacz/1.4
Disallow: /

User-agent: QueryN Metasearch
Disallow: /

User-agent: Openfind data gatherer
Disallow: /

User-agent: Openfind
Disallow: /

User-agent: Xenu's Link Sleuth 1.1c
Disallow: /

User-agent: Xenu's
Disallow: /

User-agent: Zeus
Disallow: /

User-agent: RepoMonkey Bait & Tackle/v1.01
Disallow: /

User-agent: RepoMonkey
Disallow: /

User-agent: Microsoft URL Control
Disallow: /

User-agent: Openbot
Disallow: /

User-agent: URL Control
Disallow: /

User-agent: Zeus Link Scout
Disallow: /

User-agent: Zeus 32297 Webster Pro V2.9 Win32
Disallow: /

User-agent: Webster Pro
Disallow: /

User-agent: EroCrawler
Disallow: /

User-agent: LinkScan/8.1a Unix
Disallow: /
```

```
User-agent: Keyword Density/0.9
Disallow: /

User-agent: Kenjin Spider
Disallow: /

User-agent: Iron33/1.0.2
Disallow: /

User-agent: Bookmark search tool
Disallow: /

User-agent: GetRight/4.2
Disallow: /

User-agent: FairAd Client
Disallow: /

User-agent: Gaisbot
Disallow: /

User-agent: Aqua_Products
Disallow: /

User-agent: Radiation Retriever 1.1
Disallow: /

User-agent: Flaming AttackBot
Disallow: /

User-agent: Oracle Ultra Search
Disallow: /

User-agent: MSIECrawler
Disallow: /

User-agent: PerMan
Disallow: /

User-agent: searchpreview
Disallow: /

User-agent: TurnitinBot
Disallow: /

User-agent: wget
Disallow: /

User-agent: ExtractorPro
Disallow: /

User-agent: WebZIP/4.21
Disallow: /

User-agent: WebZIP/5.0
Disallow: /

User-agent: HTTrack 3.0
Disallow: /

User-agent: TurnitinBot/1.5
Disallow: /

User-agent: WebCopier v3.2a
Disallow: /

User-agent: WebCapture 2.0
Disallow: /

User-agent: WebCopier v.2.2
Disallow: /

User-agent: Spinn3r
Disallow: /

User-agent: Tailrank
Disallow: /

User-agent: 008
Disallow: /
```

9. Intermediate Certificate is Signed Using a Weak Signature Algorithm

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected that an intermediate certificate in the certificate chain is signed using a weak signature algorithm.

The weak signature algorithm is known to be cryptographically weak and vulnerable to collision attacks.

External References

- MD5 considered harmful today - Creating a rogue CA certificate
- MS Security Advisory : Research proves feasibility of collision attacks against MD5
- OWASP - Insecure Configuration Management
- OWASP - Insufficient Transport Layer Protection
- When Will We See Collisions for SHA-1?
- Gradually sunsetting SHA-1
- Why Google is Hurrying the Web to Kill SHA-1
- SHA1 Deprecation: What You Need to Know

Classification

OWASP 2013-A6 CAPEC-459 WASC-4

9.1. https://dare2compete.com/ Confirmed

https://dare2compete.com/

Weakly Signed Certificates

```
sha1RSA - OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US
```

Request

```
[NETSPARKER] SSL Connection
```

Response

```
[NETSPARKER] SSL Connection
```

10. Generic Email Address Disclosure

1 TOTAL
INFORMATION

Netsparker identified a generic email address disclosure.

Impact

Generic email addresses discovered within the application.

Remedy

This is reported for informational purposes only.

You can use submission forms for this purpose to avoid automated email address harvesting tools.

External References

- Wikipedia - Email Spam

Classification

CWE-200 CAPEC-118 WASC-13 OWASP-PC-C7

10.1. https://dare2compete.com/21-es5.6d91eb490c866d544cb2.js

https://dare2compete.com/21-es5.6d91eb490c866d544cb2.js

Email Address(es)

sales@dare2compete.com

Certainty

Request

```
GET /21-es5.6d91eb490c866d544cb2.js HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Accept: */*
Referer: https://dare2compete.com/p/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
…
Start"](14,"li"),E["\u0275\u0275elementStart"](15,"a",316),E["\u0275\u0275elementStart"](16,"em",188),E["\u0275\u0275text"](17,"mail_outline"),E["\u0275\u0275elementEnd"](),E["\u0275\u0275text"](18," sales@dare2compete.com
"),E["\u0275\u0275elementEnd"](),E["\u0275\u0275elementEnd"](),E["\u0275\u0275elementStart"](19,"li"),E["\u0275\u0275elementStart"](20,"a",317),E["\u0275\u0275elementStart"](21,"em",188),E["\u0275\u0
…
rt"],[3,"themeColor","competition","currentUser","userLoggedIn","adBannerImages"],["class","bg step5",4,"ngIf"],[1,"bg","step5"],[1,"left_sect"],["class","no material-icons",4,"ngIf"],["href","mailTo:sales@dare2compete.com","taget","_blank",1,""],
["href","tel:9311777388"],[1,"right_sect"],["class","alert-message red-text",4,"ngIf"],["class","alert-message green-text",4,"ngIf"],[1,"no","material-icons"],["serviceForm","
…
```

11. OPTIONS Method Enabled

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected that `OPTIONS` method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Remedy

Disable `OPTIONS` method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

Classification

OWASP 2013-A5 CWE-16 CAPEC-107 WASC-14

11.1. https://dare2compete.com/api/images/600/600/ Confirmed

https://dare2compete.com/api/images/600/600/

Allowed methods

```
GET,HEAD
```

Request

```
OPTIONS /api/images/600/600/ HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
Content-Length: 0
```

Response

```
HTTP/1.1 200 OK
X-Cache: Miss from cloudfront
Cache-Control: private, must-revalidate
Allow: GET,HEAD
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: nginx
X-Amz-Cf-Id: 5KU5VV6_9lNbeZEHz0rShCAZhjNRxJRUf5KWS1-kYis2YmggTb5tcw==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Expires: -1
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding,Accept-Encoding
X-Amz-Cf-Pop: BOM52-C1
Via: 1.1 3358dcc05ba3775a502a9bcaf450ebf7.cloudfront.net (CloudFront)
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Date: Fri, 29 Oct 2021 07:12:55 GMT
```

12. Nginx Web Server Identified

1 TOTAL
INFORMATION

Netsparker identified a web server (Nginx) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification

OWASP-PC-C7

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C
Base: 5.3 (Medium)
Temporal: 5.1 (Medium)
Environmental: 5.1 (Medium)

12.1. https://dare2compete.com/

https://dare2compete.com/

Certainty

Request

```
GET / HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
X-Cache: Miss from cloudfront
ETag: W/"6177b196-25e5"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: nginx
X-Amz-Cf-Id: A3lOpFuYpU55-9kMNZzshtF5HT62RGkVAgMinMWHChiMINtiTCZYVQ==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Vary: Ac
…
```

13. Missing X-XSS Protection Header

1 TOTAL
INFORMATION

Netsparker detected a missing `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- `X-XSS-Protection: 1; mode=block`

External References

- [MSDN - Internet Explorer 8 Security Features]()
- [Internet Explorer 8 XSS Filter]()

Classification

[HIPAA-164.308(A)]() [OWASP-PC-C9]()

13.1. https://dare2compete.com/runtime-es2015.d0e31b794685186052f7.js

https://dare2compete.com/runtime-es2015.d0e31b794685186052f7.js

Certainty

Request

```
GET /runtime-es2015.d0e31b794685186052f7.js HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Referer: https://dare2compete.com/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
X-Amz-Cf-Pop: BOM51-C2
Server: nginx
X-Cache: Miss from cloudfront
Connection: keep-alive
Via: 1.1 533b573ebd801568db32d414dde39561.cloudfront.net (CloudFront)
X-Amz-Cf-Id: 0zwmxCYA-Jym3MsAnjIxZBjZ615nB6IpAyr9n25HDbdyTMvLj2yG3w==
Pragma: public
Last-Modified: Tue, 26 Oct 2021 07:43:18 GMT
Vary: Accept-Encoding,Accept-Encoding
Content-Type: application/javascript
Transfer-Encoding: chunked
Content-Encoding: 
Date: Fri, 29 Oct 2021 06:55:14 GMT
ETag: W/"6177b196-156f"
Cache-Control: max-age=31536000, public

!function(e){function c(c){for(var b,r,t=c[0],n=c[1],o=c[2],i=0,l=[];i<t.length;i++)r=t[i],Object.prototype.hasOwnProperty.call(f,r)&&f[r]&&l.push(f[r][0]),f[r]=0;for(b in n)Object.prototype.hasOwnProperty.call(n,b)&&
(e[b]=n[b]);for(u&&u(c);l.length;)l.shift()();return d.push.apply(d,o||[]),a()}function a(){for(var e,c=0;c<d.length;c++){for(var a=d[c],b=!0,t=1;t<a.length;t++)0!==f[a[t]]&&(b=!1);b&&(d.splice(c--,1),e=r(r.s=a[0]))}return e}var b={},f={37:0},d=
[];function r(c){if(b[c])return b[c].exports;var a=b[c]={i:c,l:!1,exports:{}};return e[c].call(a.exports,a,a.exports,r),a.l=!0,a.exports}r.e=function(e){var c=[],a=f[e];if(0!==a)if(a)c.push(a[2]);else{var b=new Promise(function(c,b){a=f[e]=
[c,b]});c.push(a[2]=b);var d,t=document.createElement("script");t.charset="utf-8",t.timeout=120,r.nc&&t.setAttribute("nonce",r.nc),t.src=function(e){return r.p+""+({3:"common"}[e]||e)+"-es2015."+
{0:"7ba6437d79b00349c05c",1:"2efbcc1ba1f1e6fb7978",2:"9fba369c41e92326c131",3:"302291cdcf5fcede5982",4:"89ca653dbe96e22f9f92",5:"2c6819b6329bdfa90a9a",6:"690e868b4e959b87d5b9",7:"3c21048037d7c277b496",8:"359f28584992192b5441",9:"35912aa1eebae00ce562
",10:"236884ca3f3c2ac9ba97",11:"c123e7c50d3edfa9754b",12:"c1b272e412d48ea50f10",13:"f95ccc4afe0c243b5a43",14:"ea5cbd8fedeb3bf89202",15:"207c8e7d071441ffebcc",16:"ef59031c8c035fd0bf31",17:"1f9e55622ebebbfc5e43",18:"14c0097262886715a921",19:"ca0a36bda
a717b5794a6",20:"0cca001e40720ecd70dc",21:"6d91eb490c866d544
…
```

14. Subresource Integrity (SRI) Not Implemented

1 TOTAL
INFORMATION

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Remedy

Using Subresource Integrity is simply to add *integrity* attribute to the *script* tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384** or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

Classification

14.1. https://dare2compete.com/

https://dare2compete.com/

Identified Sub Resource(s)

- https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js?client=ca-pub-5688792921429060
- https://www.googletagmanager.com/gtag/js?id=G-V3K94FPJNR

Certainty

Request

```
GET / HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```

…
#ffffff, #e9f9ff);*/
}

/*new loader*/
.loading-loader {
height: 64px;
width: 64px;
margin: 0px auto;
position: relative;
}
</style>
<script defer="" src="https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js?client=ca-pub-5688792921429060" crossorigin="anonymous"></script>
<link rel="stylesheet" href="styles.b99ac06b8cf8f879ce6e.css"></head>

<body id="s_menu" style="margin: 0px; padding: 0px;">
<div class="home-loader-screen position
…
e(o)[0];
a.async = 1;
a.src = g;
m.parentNode.insertBefore(a, m)
})(window, document, 'script', 'https://www.google-analytics.com/analytics.js', 'ga');
</script>


<script defer="" src="https://www.googletagmanager.com/gtag/js?id=G-V3K94FPJNR"></script>
<script defer="">
window.dataLayer = window.dataLayer || [];

function gtag() {
dataLayer.push(arguments);
}

gtag('js', new Date());
</script>

<!-- <script defer>
(function
…
```

15. Content Security Policy (CSP) Not Implemented

1 TOTAL
INFORMATION

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:** Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:** Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src** : Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
  - child-src
  - connect-src
  - font-src
  - img-src
  - manifest-src
  - media-src
  - object-src
  - script-src
  - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
```

```
Content-Security-Policy: script-src https://example.com:*;
```

```
Content-Security-Policy: script-src https;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)

Classification

OWASP-PC-C9

15.1. https://dare2compete.com/

https://dare2compete.com/

Certainty

Request

```
GET / HTTP/1.1
Host: dare2compete.com
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
X-Cache: Miss from cloudfront
ETag: W/"6177b196-25e5"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: nginx
X-Amz-Cf-Id: A3lOpFuYpU55-9kMNZzshtF5HT62RGkVAgMinMWHChiMINtiTCZYVQ==
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Amz-Cf-Pop: BOM51-C2
Via: 1.1 f282fe8093ec9f703de053518375c0f2.cloudfront.net (CloudFront)
Last-Modified: Tue, 26 Oct 2021 07:43:18 GMT
Content-Type: text/html
Date: Fri, 29 Oct 2021 06:55:00 GMT
Content-Encoding:

<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=0"/>
<!-- <link async rel="preconnect" href="//fonts.googleapis.com/">-->
<link async="" rel="preconnect" href="//d8it4huxumps7.cloudfront.net/">
<!-- <link async rel="preconnect" href="//connect.facebook.net"> -->
<!-- <link async rel="preconnect" href="//apis.google.com"> -->
<!-- <link async rel="preconnect" href="//www.facebook.com"> -->
<!-- <link async rel="preconnect" href="//www.clarity.ms"> -->


<link rel="preload" href="https://d8it4huxumps7.cloudfront.net/font/fontawesome-webfont.woff2" as="font" type="font/woff2" crossorigin=""/>
<link rel="preload" href="https://fonts.gstatic.com/s/materialicons/v48/flUhRq6tzZclQEJ-Vdg-IuiaDsNcIhQ8tQ.woff2" as="font" type="font/woff2" crossorigin=""/>
<link rel="preload" href="https://fonts.gstatic.com/s/inter/v3/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7W0Q5nw.woff2" as="font" type="font/woff2" crossorigin=""/>
<link rel="preload" href="https://fonts.gstatic.com/s/inter/v3/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7W0Q5nw.woff2" as="font" type="font/woff2" crossorigin=""/>
<!-- <link rel="preload" href="https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ
…
```