netsparker

5/18/2023 2:45:32 PM (UTC+07:00)

Detailed Scan Report

https://uigradients.com/

Scan Time	: 5/17/2023 7:27:17 PM (UTC+07:00)
Scan Duration	: 00:00:03:46
Total Requests	: 982
Average Speed	: 4.3 r/s

Risk Level:
MEDIUM

39 IDENTIFIED	**16** CONFIRMED	**0** CRITICAL
0 HIGH	2 MEDIUM	11 LOW
	9 BEST PRACTICE	17 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	2
Low	11
Best Practice	9
Information	17
TOTAL	**39**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	3
Best Practice	1
Information	11
TOTAL	**16**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://uigradients.com/	
	Weak Ciphers Enabled	GET	https://uigradients.com/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://uigradients.com/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://uigradients.com/static/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://uigradients.com/static/css/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://uigradients.com/static/images/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://uigradients.com/static/js/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://uigradients.com/static/js/index.html	
	Missing X-Frame-Options Header	GET	https://uigradients.com/	
	Missing X-Frame-Options Header	GET	https://uigradients.com/static/js/	
	Cookie Not Marked as HttpOnly	GET	https://uigradients.com/	
	Cookie Not Marked as Secure	GET	https://uigradients.com/	
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://uigradients.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Content Security Policy (CSP) Not Implemented	GET	https://uigradients.com/	
	Expect-CT Not Enabled	GET	https://uigradients.com/	
	Missing X-XSS-Protection Header	GET	https://uigradients.com/	
	Missing X-XSS-Protection Header	GET	https://uigradients.com/static/css/app.33da80d69744798940b135da93bc7b98.css	
	Missing X-XSS-Protection Header	GET	https://uigradients.com/static/js/	
	Missing X-XSS-Protection Header	GET	https://uigradients.com/static/js/app.53b91acd33d920dc4ee4.js	
	Referrer-Policy Not Implemented	GET	https://uigradients.com/static/js/	
	SameSite Cookie Not Implemented	GET	https://uigradients.com/	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://uigradients.com/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://uigradients.com/static/js/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://uigradients.com/static/js/	
	default-src Used in Content Security Policy (CSP)	GET	https://uigradients.com/static/js/	
	Disabled X-XSS-Protection Header	POST	https://uigradients.com/	
	Missing object-src in CSP Declaration	GET	https://uigradients.com/static/js/	
	Out-of-date Version (Vue.js)	GET	https://uigradients.com/static/js/app.53b91acd33d920dc4ee4.js	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Forbidden Resource	POST	https://uigradients.com/	
	Forbidden Resource	GET	https://uigradients.com/	
	Forbidden Resource	POST	https://uigradients.com/static/	
	Forbidden Resource	GET	https://uigradients.com/static/	
	Forbidden Resource	POST	https://uigradients.com/static/css/	
	Forbidden Resource	GET	https://uigradients.com/static/css/	
	Forbidden Resource	GET	https://uigradients.com/static/images/	
	Forbidden Resource	POST	https://uigradients.com/static/images/	
	Forbidden Resource	POST	https://uigradients.com/static/js/	
	Forbidden Resource	GET	https://uigradients.com/static/js/	
	Forbidden Resource	POST	https://uigradients.com/static/js/index.html	

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM | 1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

1.1. https://uigradients.com/

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 311.0156 **Total Bytes Received** : 2869 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdbe24fef6baf-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E800:77B3:267EF8E:39138D8:6464C85C
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fRAOiR7Uey5NjuEEQFdvo%2FM
a1j5u%2F8APZ%2BBbX6iY2NU7l5tUyi5p89IiG7YIeLY9dpAssFZcMK1yKLCIkUXvk2td4rNh9ot52HljFyv70F9%2BoTbN%2F6bsSj
pR09aqN08z%2BKQ%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:28:56 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:28:12 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name
…
```

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.

```
# load module
LoadModule headers_module modules/mod_headers.so
```

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

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

- Wikipedia - HTTP Strict Transport Security
- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
- HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

2. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker 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.

Impact

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

Vulnerabilities

2.1. https://uigradients.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received** : 27 **Body Length** : 0 **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

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"
```

3. 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
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

3. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

3.1. https://uigradients.com/

CONFIRMED

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect

the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

4. Cookie Not Marked as Secure

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

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

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), 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 steal the cookie.

Vulnerabilities

4.1. https://uigradients.com/

CONFIRMED

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

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.)*

Remedy

Mark all cookies used within the application 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 be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- Netsparker - Security Cookies - Secure Flag
- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	614
CAPEC	102
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

5. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW 1 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 are considered non-compliant by PCI since 30 June 2018.

Impact

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

Vulnerabilities

5.1. https://uigradients.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received** : 27 **Body Length** : 0 **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

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 +TLSv1.2
```

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

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on 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.**
    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".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- How to Disable TLS v1.0
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- 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)
- Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

6. Misconfigured Access-Control-Allow-Origin Header

LOW | 6

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Vulnerabilities

6.1. https://uigradients.com/

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

6.2. https://uigradients.com/static/

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET /static/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1183.9285 **Total Bytes Received** : 10228 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Server: cloudflare
access-control-allow-origin: *
x-github-request-id: 44A6:7CDB:3EC9128:5B0AEAB:6464C85C
Transfer-Encoding: chunked
CF-RAY: 7c8bdbe2bc6f4733-SIN
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=upULwh1qC3ErE2JVaHDu92OxI
ZjgdFHR8mRo5CZZk5Lg%2BoxvvCYSesGwOFqG5dx2EXNoEMOvHI1tRzskzgi%2FHTNVJDbPE1phIIfvWP3hL2onZ4fEPDe1bZjyKBBe
9GNlNiY%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: MISS
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
Date: Wed, 17 May 2023 12:28:13 GMT
Content-Encoding:

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
      .logo { display: inline-block; margin-top: 35px; }

…
```

6.3. https://uigradients.com/static/css/

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET /static/css/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 298.9831 **Total Bytes Received** : 10209 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3075:6689223:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Ytn2wyK2t1YavGppCH%2BTAHq
W04c7HHiHGUn22BhP%2BCk0AHVntUH5FMSS%2FW6vbhuIHNDmNkfc0R1ht9v6pR1aTxTKhMKw30ylzRFiMbnhWOdpJMu90b8dClaGfB
5Q2WGmGag%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe6c8bd3daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT
vary: Accept-Encoding

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
        .logo { display: inline-block; margin-top: 35px; }
        .logo-img-2x {
…
```

6.4. https://uigradients.com/static/images/

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET /static/images/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 310.9776 **Total Bytes Received** : 10238 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Server: cloudflare
access-control-allow-origin: *
x-github-request-id: E800:77B3:267EFAE:3913902:6464C85C
Transfer-Encoding: chunked
CF-RAY: 7c8bdbe49a4c6baf-SIN
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=1r2GYOsqHOgRiMVYNhQQkvrOz
fP646qYbb%2BqyYMbSGW%2BlD4FFOq992OeA0bE54W2l8yl8xveDlnie6bb92jysADyEkOAqdoqnfzia9eSobIu%2Bh1MNwt2X%2Bw%
2BwVWDE%2B8O%2BLU%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: MISS
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
Date: Wed, 17 May 2023 12:28:13 GMT
Content-Encoding:

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
      .logo { display: inline-block; margin-top:
…
```

6.5. https://uigradients.com/static/js/

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 **Total Bytes Received** : 10213 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT
vary: Accept-Encoding

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
        .logo { display: inline-block; margin-top: 35px; }
        .logo-img-
…
```

6.6. https://uigradients.com/static/js/index.html

Access-Control-Allow-Origin

- *

Certainty

Request

```
GET /static/js/index.html HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
Referer: https://uigradients.com/static/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 295.9787 **Total Bytes Received** : 10242 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Server: cloudflare
access-control-allow-origin: *
x-github-request-id: 4402:55BD:2432A38:36C7FC6:6464C85F
Transfer-Encoding: chunked
CF-RAY: 7c8bdc1ff9454020-SIN
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=cnqL8lNWVw%2By7BQ5ykRAhsp
82TX29xQwuzKQLvkfFflDOqoMRjGj9sM2vIn8nGhYiMGz%2BEsh%2BvD3%2ByPvS7oXrxUByndxH%2FGKX5%2FHAsdxyK%2BmyT%2Fw
y3%2FgnCgx3TaHn9X8O8k%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: MISS
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
Date: Wed, 17 May 2023 12:28:22 GMT
Content-Encoding:

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
      .logo { display: inline-block; margin-
…
```

Remedy

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.
Apache

- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in `httpd.conf` or `apache.conf`), or within a `.htaccess` file.

```
Header set Access-Control-Allow-Origin "domain"
```

IIS6

1. Open Internet Information Service (IIS) Manager
2. Right click the site you want to enable CORS for and go to Properties
3. Change to the HTTP Headers tab
4. In the Custom HTTP headers section, click Add
5. Enter Access-Control-Allow-Origin as the header name
6. Enter `domain` as the header value

IIS7

- Merge the following xml into the web.config file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webserver>
    <httpprotocol>
      <customheaders>
        <add name="Access-Control-Allow-Origin" value="domain" />
      </customheaders>
    </httpprotocol>
  </system.webserver>
</configuration>
```

ASP.NET

- If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:

```
Response.AppendHeader("Access-Control-Allow-Origin", "domain");
```

External References

- Cross-Origin Resource Sharing
- HTTP access control (CORS)
- Using CORS

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

7. Missing X-Frame-Options Header

LOW | 2

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

7.1. https://uigradients.com/

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

7.2. https://uigradients.com/static/js/

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 **Total Bytes Received** : 10213 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT
vary: Accept-Encoding

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
        .logo { display: inline-block; margin-top: 35px; }
        .logo-img-
…
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *`URL`* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	693
CAPEC	103
ISO27001	A.14.2.5

8. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

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.

Vulnerabilities

8.1. https://uigradients.com/

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

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) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

9. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

9.1. https://uigradients.com/

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

10. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE 1 | CONFIRMED 1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

10.1. https://uigradients.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 27 **Body Length :** 0 **Is Compressed :** No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

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 +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1.1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on 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.**
    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 1.1\
```

    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".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00
- Google Security Blog: Modernizing Transport Security
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- 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

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

11. Missing X-XSS-Protection Header

BEST PRACTICE | 4

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.

Vulnerabilities

11.1. https://uigradients.com/

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

11.2. https://uigradients.com/static/css/app.33da80d69744798940b135da93bc7b98.css

Certainty

Request

```
GET /static/css/app.33da80d69744798940b135da93bc7b98.css HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
Referer: https://uigradients.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 65.9978 **Total Bytes Received** : 12384 **Body Length** : 11488 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdbe8da813daa-SIN
Age: 63
Cache-Control: max-age=600
etag: W/"5b11b904-2ce0"
access-control-allow-origin: *
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: HIT
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=SiL9Lmm3TlYsr4GE9BGYbGDTi
f5iU3TSMpYSZvTWmZxy87DK00qjWymSP1TRjP9jcA5XodNUadu1rAR3Brx%2F6SCghTUzdTnNUNj%2FMEnxI4dIDT8xu%2BZ2VzuY%2
F5FSE5PKfkc%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:37:10 GMT
vary: Accept-Encoding
x-github-request-id: 4864:614D:5AB8B:7AB01:6412B388
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/css; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:28:13 GMT
Content-Encoding:

.mono{font-family:monospace}.tal{text-align:left}.tar{text-align:right}.tac{text-align:center}.ml10{mar
gin-left:10px}.noselect{-webkit-touch-callout:none;-webkit-user-select:none;-moz-user-select:none;-ms-u
ser-select:none;user-select:none}.hide-text{margin:-1px;padding:0;width:1px;height:1px;overflow:hidden;
clip:rect(0 0 0 0);clip:rect(0,0,0,0);position:absolute}.bg-red{background-color:red}body{margin:0;padd
ing:0;background-color:#fff;font-family:-apple-system,BlinkMacSystemFont,Segoe UI,Roboto,Helvetica Neu
e,Ubuntu,Arial,sans-serif;color:#2c3e50}@keyframes a{0%{opacity:1}to{opacity:0;transform:translate3d(0,
-100%,0)}}.fadeup-leave{opacity:1}.fadeup-leave-active{animation:a .5s}.fadeup-leave-to{opacity:0}.fade
-enter-active,.fade-leave-active{transition:opacity .5s}.fade-enter,.fade-leave-to{opacity:0}.spinner,.
spinner:after{border-radius:50%;width:30px;height:30px}.spinner{font-size:10px;position:relative;text-i
ndent:-9999em;border-top:5px solid rgba(0,0,0,.1);border-right:5px solid rgba(0,0,0,.1);border-bottom:5
px solid rgba(0,0,0,.1);border-left:5px solid #ff512f;transform:translateZ(
…
```

11.3. https://uigradients.com/static/js/

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 **Total Bytes Received** : 10213 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT
vary: Accept-Encoding

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
        .logo { display: inline-block; margin-top: 35px; }
        .logo-img-
…
```

11.4. https://uigradients.com/static/js/app.53b91acd33d920dc4ee4.js

Certainty

Request

```
GET /static/js/app.53b91acd33d920dc4ee4.js HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
Referer: https://uigradients.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 107.9934 **Total Bytes Received** : 214696 **Body Length** : 213762 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdbe47fbf3fa6-SIN
Age: 463
Cache-Control: max-age=600
etag: W/"5b11b904-34302"
access-control-allow-origin: *
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=QuN0b0RtuWGzJq5v9B4ZDs7Tp
nZIe5x%2FWfqwpAaEji4eAuB500IRF3E4Pc%2B1LfqJkbloGTta2FN35cyPEZNcRGhxPVeaian5V0XfhQUJyF4X7t8L3OUCeAjejZl1
xeHbQAE%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: HIT
Connection: keep-alive
expires: Wed, 17 May 2023 12:30:28 GMT
vary: Accept-Encoding
x-github-request-id: BD86:73C9:2492590:3026B15:63FFC073
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: application/javascript; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: MISS
Date: Wed, 17 May 2023 12:28:12 GMT
Content-Encoding:

!function(e){function t(r){if(n[r])return n[r].exports;var o=n[r]={i:r,l:!1,exports:{}};return e[r].cal
l(o.exports,o,o.exports,t),o.l=!0,o.exports}var n={};t.m=e,t.c=n,t.d=function(e,n,r){t.o(e,n)||Object.d
efineProperty(e,n,{configurable:!1,enumerable:!0,get:r})},t.n=function(e){var n=e&&e.__esModule?functio
n(){return e.default}:function(){return e};return t.d(n,"a",n),n},t.o=function(e,t){return Object.proto
type.hasOwnProperty.call(e,t)},t.p="/",t(t.s=48)}([function(e,t,n){"use strict";function r(e,t,n,r,o,i,
a,s){e=e||{};var c=typeof e.default;"object"!==c&&"function"!==c||(e=e.default);var l="function"==typeo
f e?e.options:e;t&&(l.render=t,l.staticRenderFns=n,l._compiled=!0),r&&(l.functional=!0),i&&(l._scopeId=
i);var u;if(a?(u=function(e){e=e||this.$vnode&&this.$vnode.ssrContext||this.parent&&this.parent.$vnode&
&this.parent.$vnode.ssrContext,e||"undefined"==typeof __VUE_SSR_CONTEXT__||(e=__VUE_SSR_CONTEXT__),o&&
o.call(this,e),e&&e._registeredComponents&&e._registeredComponents.add(a)},l._ssrRegister=u):o&&(u=s?fu
nction(){o.call(this,this.$root.$opti
…
```

Remedy

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

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

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

SANS Top 25	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5

12. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

12.1. https://uigradients.com/static/js/

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 **Total Bytes Received** : 10213 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT
vary: Accept-Encoding

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
        .logo { display: inline-block; margin-top: 35px; }
        .logo-img-
…
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	200
ISO27001	A.14.2.5

13. SameSite Cookie Not Implemented

BEST PRACTICE | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

13.1. https://uigradients.com/

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Certainty

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1299.8656 **Total Bytes Received** : 2867 **Body Length** : 1973 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdacc2ba2a07e-SIN
Cache-Control: max-age=600
access-control-allow-origin: *
x-github-request-id: E60E:7B97:3C9A130:5D4E1E5:6464C830
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dz8I02GAbKqOYSGiVl2o9b5pw
4SEUiVCgfjjGueFBlfn3yCkWeLSo3DeUD96k%2BVgjjfoVo7qpv8wcZUZtMkOqvTh0B4oYg6UZ6%2B%2FczYBSGh%2F%2F0qn2Unqgs
lumCW1llLKkxI%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
expires: Wed, 17 May 2023 12:31:16 GMT
vary: Accept-Encoding
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: HIT
Date: Wed, 17 May 2023 12:27:29 GMT
Content-Encoding:

<!DOCTYPE html><html><head><meta charset=utf-8><title>uiGradients - Beautiful colored gradients</title>
<meta name=description content="A handpicked collection of beautiful color gradients for designers and
 developers"><meta property=og:type content=website><meta property=og:site_name content=uiGradients><me
ta property=og:url content=http://uigradients.com><meta property=og:title content="uiGradients - Beauti
ful colored gradients"><meta property=og:description content="uiGradients is a handpicked collection of
 beautiful color gradients for designers and developers."><meta property=og:image content=http://uigrad
ients.com/static/images/uigradients.jpg><meta name=twitter:card content=summary_large_image><meta name=
twitter:creator content=@_ighosh><meta name=twitter:title content="Handpicked beautiful color gradient
s"><meta name=twitter:description content="uiGradients is a handpicked collection of beautiful color gr
adients for designers and developers."><meta name=twitter:image content=http://uigradients.com/static/i
mages/uigradients.jpg><meta name=twitter:image:width content=1200><meta name=t
…
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...` attribute to the `Set-Cookie` header. There are three possible values for the `SameSite` attribute:

- Lax: In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None` must also specify the `Secure` attribute to transfer them via a secure context. Setting a `SameSite=None` cookie without the `Secure` attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- Security Cookies - SameSite Attribute - Netsparker
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute
- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

14. An Unsafe Content Security Policy (CSP) Directive in Use

INFORMATION 1

Netsparker detected that one of following CSP directives is used:

- unsafe-eval
- unsafe-inline

By using `unsafe-eval`, you allow the use of string evaluation functions like `eval`.

By using `unsafe-inline`, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.

Vulnerabilities

14.1. https://uigradients.com/static/js/

Unsafe Directive Used In Csp

- unsafe-inline

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 Total Bytes Received : 10213 Body Length : 9339 Is Compressed : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT

…
HuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZZTRqC3MR%2BJ4%3
D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=
…
```

Remedy

If possible remove `unsafe-eval` and `unsafe-inline` from your CSP directives.

External References

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

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

15. data: Used in a Content Security Policy (CSP) Directive

INFORMATION 1

Netsparker detected `data:` use in a CSP directive.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using `data:` protocol.

Vulnerabilities

15.1. https://uigradients.com/static/js/

Data Directive Used

- data:

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 Total Bytes Received : 10213 Body Length : 9339 Is Compressed : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT

…
5n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","m
ax_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-
…
```

Remedy

Remove `data:` sources from your CSP directives.

External References

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

CLASSIFICATION

ISO27001	A.14.2.5

16. default-src Used in Content Security Policy (CSP)

INFORMATION 1

Netsparker detected that you used *default-src* in CSP directive. It is important to know that *default-src* cannot be used as a fallback for the functions below:

```
base-uri

form-action

frame-ancestors

plugin-types

report-uri

sandbox
```

Vulnerabilities

16.1. https://uigradients.com/static/js/

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 **Total Bytes Received** : 10213 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT

…
OLh88NZbYC6k12hlfuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX
5NsUdW%2FxV%2FhZZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN

…
```

External References

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

CLASSIFICATION

OWASP Proactive Controls	C9
ISO27001	A.14.2.5

17. Disabled X-XSS-Protection Header

INFORMATION 1

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

Internet Explorer's built-in cross-site scripting protection can be disabled by using the following HTTP Header : `X-XSS-Protection: 0`

Impact

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

Vulnerabilities

17.1. https://uigradients.com/

Header

- x-xss-protection: 0

Certainty

Request

```
POST / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451; _gat=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 892.4304 **Total Bytes Received** : 55744 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0a5096a4488-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=kknZ0XFykNHkxA2Qmy0XqVFeK
d9RbD%2FBIdT1CAE6P4HO9Zpqm%2BMcT%2Bg2HyQZid8o7UZWNKCVcqGKW2mswYyuGedYa2ZkyCXlqC3tYKqxVHozwiU6WRTH8bTOaV
eAVnrzfR4%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:28 G
…
 cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0a5096a4488-SIN
x-content-type-options: nosniff
x-xss-protection: 0

Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=kknZ0XFykNHkxA2Qmy0XqVFeK
d9RbD%2FBIdT1CAE6P4HO9Zpqm%2BMcT%2Bg2HyQZid8o7UZWNKCVcqGKW2mswYyuGedYa2ZkyCXlqC3tYKqxVHozwiU6WRT
…
```

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
- X-XSS-Protection HTTP Header
  ```

- Internet Explorer 8 XSS Filter

CLASSIFICATION

SANS Top 25	693
WASC	15
OWASP Proactive Controls	C9
ISO27001	A.14.1.2

18. Forbidden Resource

INFORMATION 11 CONFIRMED 11

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.

Vulnerabilities

18.1. https://uigradients.com/

CONFIRMED

Request

```
POST / HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451; _gat=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 892.4304 Total Bytes Received : 55744 Body Length : 54879 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0a5096a4488-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=knZ0XFykNHkxA2Qmy0XqVFeK
d9RbD%2FBIdT1CAE6P4HO9Zpqm%2BMcT%2Bg2HyQZid8o7UZWNKCVcqGKW2mswYyuGedYa2ZkyCXlqC3tYKqxVHozwiU6WRTH8bTOaV
eAVnrzfR4%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:28 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0a5096a4488-SIN
x-content-type-options: n
…
```

18.2. https://uigradients.com/

CONFIRMED

Method	Parameter	Value
GET	Accept	../../../../../../../../../../../../etc/passwd{{

Request

```
GET / HTTP/1.1
Host: uigradients.com
Accept: ../../../../../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 833.2679 **Total Bytes Received** : 55744 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0b56f9e87ef-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=PIev21LXMv17W4LZEiibAI1dL
oni5rzIswgW5zNNOwkyX5IOaovoLIVTlyMQrDGkkOvzbRsAHnmNne80IZ3kGT%2B%2B7J%2F61l6yWOltAOyn2kZAAL4bEOHrNyto3l
TSanLqMao%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:30 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0b56f9e87ef-SIN
x-content-type-options: n
…
```

18.3. https://uigradients.com/static/

CONFIRMED

Request

```
POST /static/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 633.837 Total Bytes Received : 55742 Body Length : 54879 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0eeaafe4649-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jgPB8otl7mZc8YhH5kEbv1hAm
fZvNpYlaR9QpoSDN17dtfeaVYTygBdJ9ji9P2n7PWFuVSXnZEi%2Frgnt9jf1tiY2fW6imhZ%2BybgoOnazIPgA7fLsDMnbY9NAvpje
Lonyvxk%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:39 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0eeaafe4649-SIN
x-content-type-options: n
…
```

18.4. https://uigradients.com/static/

CONFIRMED

Method	Parameter	Value
GET	Accept	../../../../../../../../../../../../etc/passwd{{

Request

```
GET /static/ HTTP/1.1
Host: uigradients.com
Accept: ../../../../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 450.7169 **Total Bytes Received** : 55746 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0f1aa403f9e-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wfVTPRv5%2BlqPFFMXKzKb3xT
6BgC8Xgh8o8tVCHUoGfGP9d%2FAno2%2F08c8V1S7Ggt1EWouBYsMsri3pTgR2eHTOUgLYMJhCc5NqXOsIwq96xoOwrGzqhEKQIVkeq
2Xy%2Bjnbdc%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:40 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be0f1aa403f9e-SIN
x-content-type-options: n
…
```

18.5. https://uigradients.com/static/css/

CONFIRMED

Request

```
POST /static/css/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 434.3467 Total Bytes Received : 55746 Body Length : 54879 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1ab4dda406a-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=21VyjY3dO4e4B4STM8MCH%2BL
Gx3dk7HY%2F7ev3rnRUpwq0baCEEeWnJ2qXbzvjm1j5QqtetXl0VL%2B7uu%2F3f2pmratNbQK92NihtmFhm9HSoQHCOJrSC5GaAB1k
NZH2HYwFIMc%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:32:09 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1ab4dda406a-SIN
x-content-type-options: n
…
```

18.6. https://uigradients.com/static/css/

CONFIRMED

Method	Parameter	Value
GET	Accept	../../../../../../../../../../../../etc/passwd{{

Request

```
GET /static/css/ HTTP/1.1
Host: uigradients.com
Accept: ../../../../../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 613.593 **Total Bytes Received** : 55740 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1abbd6e40aa-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=FB6g5csgzohJRGrvXK96pA7Tw
ccW6kbgA%2BDBaGjRRHGRR2d5yEW37ydYM9U3YjjEJFnh9bGwmxMIQz1JFj4ughNRkrsA1XlHJL9MYw63v152t11Fol7Itoj7JPPJMT
UQDKg%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:32:10 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1abbd6e40aa-SIN
x-content-type-options: n
…
```

18.7. https://uigradients.com/static/images/

CONFIRMED

Method	Parameter	Value
GET	Accept	../../../../../../../../../../../../etc/passwd{{

Request

```
GET /static/images/ HTTP/1.1
Host: uigradients.com
Accept: ../../../../../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 690.1376 **Total Bytes Received** : 55746 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be17b1f1d3d8d-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=7Dg9Bz9FXIhUKwROVQeoFWod
X%2FvUEvqpif3%2BozLtE8aU5pTaK0l6cFeHLRxBL2bDzU22fjvQPywlMFuPqasacTMQ%2BZCOL37CYGB1CED6GpUIgCwi6P5%2BaBp
bhQURjuBqkF8%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:32:02 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be17b1f1d3d8d-SIN
x-content-type-options: n
…
```

18.8. https://uigradients.com/static/images/

CONFIRMED

Request

```
POST /static/images/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 434.8771 **Total Bytes Received** : 55746 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1879bd2409e-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=R1qtrDqxz9W73QAxfYp72lqxe
0QmH81MW2%2FRbWEjl0tZ0jOCWOViJTH82OZr7mrW6c15rnMe22nwJHWCYMq2EIeoHgfMVnbQuyRLZQ%2FkmK7NMH2uAbQ07%2BPGQd
b3%2F4ksYOg%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:32:04 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1879bd2409e-SIN
x-content-type-options: n
…
```

18.9. https://uigradients.com/static/js/

CONFIRMED

Request

```
POST /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 614.674 Total Bytes Received : 55746 Body Length : 54879 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1386b0fa060-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=smfvSaUcbKINiZ2uwx%2BoeZ4
6%2FRZNe1FC2w31z4Wp6iaQdhdWGWw%2FxC9o287Uc%2Bgmxc44KIsEnBCo11TaTKCVCwND0VJmN1MFUjF1iDbB9xZiYEXZJB7miqjd
eFNUU2DwD48%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:51 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1386b0fa060-SIN
x-content-type-options: n
…
```

18.10. https://uigradients.com/static/js/

CONFIRMED

Method	Parameter	Value
GET	Accept	../../../../../../../../../../../../etc/passwd{{

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: ../../../../../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 688.259 **Total Bytes Received** : 55750 **Body Length** : 54879 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be145ba63a036-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=PUQrjBLRXkqrNCUtRm7FloLTw
MlcMxiWkB%2FUARuE%2FF6KjnITSLsrYLCU%2F3oxdk8e0M9MEqrWLSbtqbM%2F%2BvviVw7%2FktIkoxIctgyC8rr6Bn8dkko77nBA
gtM79Chyadx09XE%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:31:53 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be145ba63a036-SIN
x-content-type-options: n
…
```

18.11. https://uigradients.com/static/js/index.html

CONFIRMED

Request

```
POST /static/js/index.html HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
Referer: https://uigradients.com/static/js/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 703.4771 Total Bytes Received : 55754 Body Length : 54879 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1ef8bd49f7d-SIN
x-content-type-options: nosniff
x-xss-protection: 0
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=%2FzpCuOM9aiQcH%2BK71J2qg
rdD1FC7S6aiMyxvhxyQ7a7jkHHGdTWvArXLKGa9YissLxoZx7YKvi88e0Td0A0dZZpWDbxQhn%2BzR%2FfIaj57N5%2BzuXqH%2BK7x
e%2BhQaKcFh%2Bk0hiE%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
x-frame-options: deny
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Content-Type: text/html; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:;
Date: Wed, 17 May 2023 12:32:20 GHTTP/1.1 403 Forbidden

Server: cloudflare
Cache-Control: no-cache
CF-Cache-Status: DYNAMIC
strict-transport-security: max-age=31536000
Transfer-Encoding: chunked
CF-RAY: 7c8be1ef8bd49f7d-SIN
x-content-type-options: n
…
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

19. Missing object-src in CSP Declaration

INFORMATION 1

Netsparker detected that `object-src` is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.

Vulnerabilities

19.1. https://uigradients.com/static/js/

Certainty

Request

```
GET /static/js/ HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 312.9744 **Total Bytes Received** : 10213 **Body Length** : 9339 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
x-proxy-cache: MISS
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
x-github-request-id: CEB8:1AF3:45D3059:66891FC:6464C85C
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Zd2z2FdGpOLh88NZbYC6k12hl
fuUINKuAHO7VBeQHuyTVUkgwwVh8nrICXh7i2V15n0mc0ECUt%2F1oyCEj1ld2VrVNN%2BNrIXBCJSbY3z4dswX5NsUdW%2FxV%2FhZ
ZTRqC3MR%2BJ4%3D"}],"group":"cf-nel","max_age":604800}
content-security-policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'sel
f'
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
access-control-allow-origin: *
CF-RAY: 7c8bdbe3add63daa-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 17 May 2023 12:28:13 GMT
vary: Accept-Encoding

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline';
 img-src data:; connect-src 'self'">
    <title>Page not found &middot; GitHub Pages</title>
    <style type="text/css" media="screen">
      body {
        background-color: #f1f1f1;
        margin: 0;
        font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      }

      .container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

      a { color: #4183c4; text-decoration: none; }
      a:hover { text-decoration: underline; }

      h1 { width: 800px; position:relative; left: -100px; letter-spacing: -1px; line-height: 60px; font
-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }
      p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

      ul { list-style: none; margin: 25px 0; padding: 0; }
      li { display: table-cell; font-weight: bold; width: 1%; }
```

```
        .logo { display: inline-block; margin-top: 35px; }
        .logo-img-
…
```

Remedy

Set `object-src` to `'none'` in CSP declaration:

```
Content-Security-Policy: object-src 'none';
```

CLASSIFICATION

SANS Top 25	16
WASC	15
OWASP Proactive Controls	C9
ISO27001	A.14.2.5

20. Out-of-date Version (Vue.js)

INFORMATION 1

Netsparker identified that the target web site is using Vue.js and detected that it is out of date.

Impact

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

Vulnerabilities

20.1. https://uigradients.com/static/js/app.53b91acd33d920dc4ee4.js

Identified Version

- 2.5.16

Latest Version

- 2.7.14 (in this branch)

Vulnerability Database

- Result is based on 05/16/2023 22:00:00 vulnerability database content.

Certainty

Request

```
GET /static/js/app.53b91acd33d920dc4ee4.js HTTP/1.1
Host: uigradients.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.342310680.1684326451; _gid=GA1.2.605287410.1684326451
Referer: https://uigradients.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 107.9934 **Total Bytes Received** : 214696 **Body Length** : 213762 **Is Compressed** : No

```
HTTP/1.1 200 OK
CF-RAY: 7c8bdbe47fbf3fa6-SIN
Age: 463
Cache-Control: max-age=600
etag: W/"5b11b904-34302"
access-control-allow-origin: *
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=QuN0b0RtuWGzJq5v9B4ZDs7Tp
nZIe5x%2FWfqwpAaEji4eAuB500IRF3E4Pc%2B1LfqJkbloGTta2FN35cyPEZNcRGhxPVeaian5V0XfhQUJyF4X7t8L3OUCeAjejZl1
xeHbQAE%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Server: cloudflare
CF-Cache-Status: HIT
Connection: keep-alive
expires: Wed, 17 May 2023 12:30:28 GMT
vary: Accept-Encoding
x-github-request-id: BD86:73C9:2492590:3026B15:63FFC073
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
last-modified: Fri, 01 Jun 2018 21:22:12 GMT
Content-Type: application/javascript; charset=utf-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
x-origin-cache: HIT
x-proxy-cache: MISS
Date: Wed, 17 May 2023 12:28:12 GMT
Con
…
'<a href="\n"/>':'<div a="\n"/>',Cc.innerHTML.indexOf("&#10;")>0}function ai(e){if(e.outerHTML)return
 e.outerHTML;var t=document.createElement("div");return t.appendChild(e.cloneNode(!0)),t.innerHTML}/*!
 * Vue.js v2.5.16
 * (c) 2014-2018 Evan You
 * Released under the MIT License.
 */
var si=Object.freeze({}),ci=Object.prototype.toString,li=h("slot,component",!0),ui=h("key,ref,slot,slot
-scope,is"),fi=Object.prototype
…
```

Remedy

Please upgrade your installation of Vue.js to the latest stable version.

Remedy References

- Downloading Vue.js

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,

		File Upload, Header Analyzer, Heartbleed, HSTS, HTML Content, HTTP Header Injection, HTTP Methods, HTTP Status, HTTP.sys (CVE-2015-1635), IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content, JavaScript Libraries, Local File Inclusion, Login Page Identifier, Mixed Content, Open Redirection, Referrer Policy, Reflected File Download, Remote File Inclusion, Remote File Inclusion (Out of Band), Reverse Proxy Detection, RoR Code Execution, Server-Side Request Forgery (DNS), Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	:	Heuristic
Detected URL Rewrite Rule(s)	:	None
Excluded URL Patterns	:	(log|sign)\-?(out|off) exit endsession gtm\.js WebResource\.axd

	ScriptResource\.axd
Authentication	: None
Scheduled	: No
Additional Website(s)	: None

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com