Web Application Scanning Detailed Scan

Export: soilgassafe.rti.org

November 2, 2022 at 20:22 (UTC)

achang@rti.org-4f032210

Table of Contents

Scan Summary

Vulnerability Breakdown

0	0	6	6
CRITICAL	HIGH	MEDIUM	LOW

Scan Details

NAME	soilgassafe.rti.org
STATUS	Completed
CREATE TIME	11/02/2022 at 03:38 PM UTC
START TIME	11/02/2022 at 03:38 PM UTC
END TIME	11/02/2022 at 04:23 PM UTC
TEMPLATE	Scan
SCANNER	Scanner
TARGET	https://soilgassafe.rti.org/
DESCRIPTION	-

Scan Notes

Severity	Scan Notes	Description

No tuning recommendations for this scan.

Scan Results

Vulnerabilities

Severity	Plugin Id	Name	Family	Instances
Medium	98056	Missing HTTP Strict Transport Security Policy	HTTP Security Header	1
Medium	98590	jQuery < 3.4.0 Prototype Pollution	Component Vulnerability	1
Medium	112373	Bootstrap < 3.4.0 Cross-Site Scripting	Component Vulnerability	1
Medium	112375	Bootstrap 3.x < 3.4.1 Cross-Site Scripting	Component Vulnerability	1
Medium	112383	jQuery 1.2.0 < 3.5.0 Cross-Site Scripting	Component Vulnerability	1
Medium	112435	jQuery 1.12.4 < 3.0.0 Cross-Site Scripting	Component Vulnerability	1
Low	112553	Missing 'Cache-Control' Header	HTTP Security Header	1
Low	98060	Missing 'X-Frame-Options' Header	HTTP Security Header	1
Low	115540	Cookie Without SameSite Flag Detected	Web Applications	1
Low	98618	HTTP Header Information Disclosure	HTTP Security Header	1
Low	112529	Missing 'X-Content-Type-Options' Header	HTTP Security Header	1
Low	112551	Missing Content Security Policy	HTTP Security Header	1

Missing HTTP Strict Transport Security Policy

VULNERABILITY MEDIUM PLUGIN ID 98056

Description

The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.

HTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.

Cyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures.

Scanner discovered that the affected application is using HTTPS however does not use the HSTS header.

Solution

Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.

One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in

which the client's browser will adhere to the header policy.

Depending on the environment and the application this time period could be from as low as minutes to as long as days.

See Also

https://tools.ietf.org/html/rfc6797

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

https://www.chromium.org/hsts

https://hstspreload.org/

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Medium
PLUGIN ID	98056

Risk Information

CVSSV3 BASE SCORE	6.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS BASE SCORE	5.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Reference Information

CWE	319, 523
WASC	Insufficient Transport Layer Protection
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A2, 2019-API7
CVE	-
BID	-

Missing HTTP Strict Transport Security Policy Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98056

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL https://soilgassafe.rti.org/.

HTTP Info

REQUEST MADE

GET https://soilgassafe.rti.org/

REQUEST HEADERS

Accept=*/*

Accept-Language=en-US,en;q=0.5

Upgrade-Insecure-Requests=1

User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36

RESPONSE HEADERS

HTTP/1.1 200 OK

Content-Type: text/html

Content-Encoding: gzip

Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT

Accept-Ranges: bytes

ETag: "0b9ad14cfeed81:0"

```
Vary: Accept-Encoding

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

---

jQuery < 3.4.0 Prototype Pollution

VULNERABILITY MEDIUM PLUGIN ID 98590

Description

According to its self-reported version number, jQuery is prior to 3.4.0. Therefore, it may be affected by a prototype pollution vulnerability due to 'extend' function that can be tricked into modifying the prototype of 'Object'.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to jQuery version 3.4.0 or later.

See Also

https://snyk.io/vuln/SNYK-JS-JQUERY-174006

https://snyk.io/blog/after-three-years-of-silence-a-new-jquery-prototype-pollution-vulnerability-emerges-once-again/

https://github.com/jquery/jquery/pull/4333

Plugin Details

PUBLICATION DATE	2019-04-25T00:00:00+00:00
MODIFICATION DATE	2022-10-26T00:00:00+00:00

FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	98590

Risk Information

CVSSV3 BASE SCORE	6.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	400
WASC	Denial of Service
OWASP	2013-A9, 2017-A9, 2021-A6, 2019-API7
CVE	CVE-2019-11358
BID	108023

jQuery < 3.4.0 Prototype Pollution Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98590

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Current Version: 2.1.4

Fixed Version: 3.4.0

Detected technology URL: https://soilgassafe.rti.org/
```

Bootstrap < 3.4.0 Cross-Site Scripting

VULNERABILITY MEDIUM PLUGIN ID 112373

Description

According to its self-reported version number, Bootstrap is prior to 3.4.0. Therefore, it may be affected by a Cross-Site Scripting (XSS) vulnerability via the data-target attribute.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Bootstrap version 3.4.0 or later.

See Also

https://github.com/twbs/bootstrap/issues/20184

Plugin Details

PUBLICATION DATE	2018-11-05T00:00:00+00:00
MODIFICATION DATE	2022-10-26T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium

PLUGIN ID	112373

Risk Information

CVSSV3 BASE SCORE	6.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2017-A9, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A7, 2019-API7
CVE	-
BID	-

Bootstrap < 3.4.0 Cross-Site Scripting Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 112373

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Current Version: 3.3.5

Fixed Version: 3.4.0

Detected technology URL: https://soilgassafe.rti.org/
```

Bootstrap 3.x < 3.4.1 Cross-Site Scripting

VULNERABILITY MEDIUM PLUGIN ID 112375

Description

According to its self-reported version number, Bootstrap is 3.x prior 3.4.1 or 4.x prior to 4.3.1. Therefore, it may be affected by a Cross-Site Scripting (XSS) vulnerability via data-template attribute for tooltip and popover plugins.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Bootstrap version 3.4.1 or later.

See Also

https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/

Plugin Details

PUBLICATION DATE	2019-02-15T00:00:00+00:00
MODIFICATION DATE	2022-10-26T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium

PLUGIN ID	112375

Risk Information

CVSSV3 BASE SCORE	6.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2017-A9, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A7, 2019-API7
CVE	CVE-2019-8331
BID	107375

Bootstrap 3.x < 3.4.1 Cross-Site Scripting Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 112375

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Current Version: 3.3.5

Fixed Version: 3.4.1

Detected technology URL: https://soilgassafe.rti.org/
```

jQuery 1.2.0 < 3.5.0 Cross-Site Scripting

VULNERABILITY MEDIUM PLUGIN ID 112383

Description

According to its self-reported version number, jQuery is at least 1.2.0 and prior to 3.5.0. Therefore, it may be affected by a cross-site scripting vulnerability via the regex operation in jQuery.htmlPrefilter.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to jQuery version 3.5.0 or later.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

https://github.com/jquery/jquery/commit/1d61fd9407e6fbe82fe55cb0b938307aa0791f77

Plugin Details

PUBLICATION DATE	2020-05-14T00:00:00+00:00
MODIFICATION DATE	2022-10-26T00:00:00+00:00
FAMILY	Component Vulnerability

SEVERITY	Medium
PLUGIN ID	112383

Risk Information

CVSSV3 BASE SCORE	6.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2017-A9, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A7, 2019-API7
CVE	CVE-2020-11022, CVE-2020-11023
BID	-

jQuery 1.2.0 < 3.5.0 Cross-Site Scripting Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 112383

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Current Version: 2.1.4

Fixed Version: 3.5.0

Detected technology URL: https://soilgassafe.rti.org/
```

jQuery 1.12.4 < 3.0.0 Cross-Site Scripting

VULNERABILITY MEDIUM PLUGIN ID 112435

Description

According to its self-reported version number, jQuery is at least 1.4.0 and prior to 1.12.0 or at least 1.12.4 and prior to 3.0.0-beta1. Therefore, it may be affected by a cross-site scripting vulnerability due to cross-domain ajax request performed without the dataType.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to jQuery version 3.0.0 or later.

See Also

https://github.com/jquery/jquery/issues/2432

https://github.com/jquery/jquery/pull/2588/commits/c254d308a7d3f1eac4d0b42837804cfffcba4bb2

Plugin Details

PUBLICATION DATE	2018-11-05T00:00:00+00:00
MODIFICATION DATE	2022-10-26T00:00:00+00:00

FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	112435

Risk Information

CVSSV3 BASE SCORE	6.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2017-A9, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A7, 2019-API7
CVE	CVE-2015-9251
BID	105658

jQuery 1.12.4 < 3.0.0 Cross-Site Scripting Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 112435

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Current Version: 2.1.4

Fixed Version: 3.0.0

Detected technology URL: https://soilgassafe.rti.org/
```

Missing 'X-Frame-Options' Header

VULNERABILITY LOW PLUGIN ID 98060

Description

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

The server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Solution

Configure your web server to include an `X-Frame-Options` header.

See Also

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

http://tools.ietf.org/html/rfc7034

https://www.owasp.org/index.php/Clickjacking

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98060

Risk Information

CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

Reference Information

CWE	346, 1021
WASC	Application Misconfiguration
OWASP	2021-A7, 2017-A6, 2021-A4, 2013-A5, 2010-A6, 2019-API7
CVE	-
BID	-

Missing 'X-Frame-Options' Header Instances (1)

VULNERABILITY LOW PLUGIN ID 98060

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Page https://soilgassafe.rti.org/ has no X-Frame-Option header defined
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

HTTP Header Information Disclosure

VULNERABILITY LOW PLUGIN ID 98618

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and technologies used by the web server.

Solution

Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

http://projects.webappsec.org/w/page/13246925/Fingerprinting

Plugin Details

PUBLICATION DATE	2019-06-12T00:00:00+00:00
MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98618

Risk Information

CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	200
WASC	Information Leakage
OWASP	2017-A6, 2021-A1, 2013-A5, 2010-A6, 2019-API7
CVE	-
BID	-

HTTP Header Information Disclosure Instances (1)

VULNERABILITY LOW PLUGIN ID 98618

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://soilgassafe.rti.org/:


- X-Powered-By: ASP.NET

- Server: Microsoft-IIS/10.0
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*

Accept-Language=en-US,en;q=0.5

Upgrade-Insecure-Requests=1

User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK

Content-Type: text/html

Content-Encoding: gzip

Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
```

```
Accept-Ranges: bytes

ETag: "0b9ad14cfeed81:0"

Vary: Accept-Encoding

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Missing 'X-Content-Type-Options' Header

VULNERABILITY LOW PLUGIN ID 112529

Description

The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.

The server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack.

Solution

Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto

Plugin Details

PUBLICATION DATE	2018-11-28T00:00:00+00:00
MODIFICATION DATE	2022-05-04T00:00:00+00:00
FAMILY	HTTP Security Header

SEVERITY	Low
PLUGIN ID	112529

Risk Information

CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	693
WASC	Application Misconfiguration
OWASP	2010-A6, 2013-A5, 2017-A6, 2019-API7
CVE	-
BID	-

Missing 'X-Content-Type-Options' Header Instances (1)

VULNERABILITY LOW PLUGIN ID 112529

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application response

HTTP Info

REQUEST MADE

GET https://soilgassafe.rti.org/

REQUEST HEADERS

Accept=*/*

Accept-Language=en-US,en;q=0.5

Upgrade-Insecure-Requests=1

User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36

RESPONSE HEADERS

HTTP/1.1 200 OK

Content-Type: text/html

Content-Encoding: gzip

Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT

Accept-Ranges: bytes

ETag: "0b9ad14cfeed81:0"

```
Vary: Accept-Encoding

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Missing Content Security Policy

VULNERABILITY LOW PLUGIN ID 112551

Description

Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load.

No CSP header has been detected on this host. This URL is flagged as a specific example.

Solution

Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

https://csp-evaluator.withgoogle.com/

https://content-security-policy.com/

https://developers.google.com/web/fundamentals/security/csp/

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

Plugin Details

PUBLICATION DATE	2019-02-14T00:00:00+00:00
MODIFICATION DATE	2022-07-18T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112551

Risk Information

CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	1021
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2019-API7
CVE	-
BID	-

Missing Content Security Policy Instances (1)

VULNERABILITY LOW PLUGIN ID 112551

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
https://soilgassafe.rti.org/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Missing 'Cache-Control' Header

VULNERABILITY LOW PLUGIN ID 112553

Description

The HTTP 'Cache-Control' header is used to specify directives for caching mechanisms.

The server did not return or returned an invalid 'Cache-Control' header which means page containing sensitive information (password, credit card, personal data, social security number, etc) could be stored on client side disk and then be exposed to unauthorised persons. This URL is flagged as a specific example.

Solution

Configure your web server to include a 'Cache-Control' header with appropriate directives. If page contains sensitive information 'Cache-Control' value should be 'no-store' and 'Pragma' header value should be 'no-cache'.

See Also

https://www.owasp.org/index.php/Testing_for_Browser_cache_weakness_(OTG-AUTHN-006)

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Pragma

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

Plugin Details

PUBLICATION DATE	2019-02-15T00:00:00+00:00

MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112553

Risk Information

CVSSV3 BASE SCORE	3.7
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	525
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2019-API7
CVE	-
BID	-

Missing 'Cache-Control' Header Instances (1)

VULNERABILITY LOW PLUGIN ID 112553

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
https://soilgassafe.rti.org/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Cookie Without SameSite Flag Detected

VULNERABILITY LOW PLUGIN ID 115540

Description

SameSite is an attribute which can be set on a cookie to instruct the web browser if this cookie can be sent along with cross-site requests to help prevent Cross-Site Request Forgery (CSRF) attacks.

The attribute has three possible values :

- Strict : the cookie will only be sent in a first-party context, thus preventing cross-site requests initiated from third-party websites to include it.

- Lax : the cookie is allowed to be sent in GET cross-site requests initiated by the top-level navigation from third-party websites. For example, following an hypertext link from the external website will make the request include the cookie.

- None : the cookie is explicitly set to be sent by the browser in any context.

The scanner identified the lack of SameSite attribute on cookies set by the application or a misconfiguration.

Solution

Web browsers default behavior may differ when processing cookies in a cross-site context, making the final decision to send the cookie in this context unpredictable. The SameSite attribute should be set in every cookie to enforce the

expected result by developers. When using the 'None' attribute value, ensure that the cookie is also set with the 'Secure' flag.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#samesite-cookie-attribute

https://web.dev/samesite-cookies-explained

https://blog.chromium.org/2019/10/developers-get-ready-for-new.html

Plugin Details

PUBLICATION DATE	2018-12-14T00:00:00+00:00
MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Low
PLUGIN ID	115540

Risk Information

CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	352
WASC	Cross-Site Request Forgery
OWASP	2010-A5, 2013-A8, 2021-A1, 2019-API7
CVE	-
BID	-

Cookie Without SameSite Flag Detected Instances (1)

VULNERABILITY LOW PLUGIN ID 115540

INSTANCE

https://soilgassafe.rti.org/

INPUT TYPE	cookie
INPUT NAME	BALANCE

Identification

PROOF

```
BALANCE=rd200o00000000000000000000ffffac18231fo80; Path=/; Secure; HttpOnly
```

OUTPUT

```
The scanner detected a cookie named 'BALANCE' which does not have the 'SameSite' attribute set.
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK

Content-Type: text/html

Content-Encoding: gzip

Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT

Accept-Ranges: bytes

ETag: "0b9ad14cfeed81:0"

Vary: Accept-Encoding

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Scan Information

VULNERABILITY INFO PLUGIN ID 98000

Description

Provides scan information and statistics of plugins run.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2017-03-31T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98000

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-

CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Scan Information Instances (1)

VULNERABILITY INFO PLUGIN ID 98000

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Engine Version 1.40.1-682

Scan ID 1b71e911-bd07-40ef-be3b-1db98e9ce7b6


Start Time 2022-11-02 11:38:33 -0400

Duration 00:44:59


Requests 9954

Crawler Requests 581

Requests/s 3.7712

Mean Response Time 1.3116s


Bandwidth Usage

- Data to Target 3.55 MB

- Data from Target 114 MB


Timeouts Encountered

Network Timeouts 9

Browser Timeouts 0
```

Browser Respawns 0

HTTP Protocols Detected

- HTTP
- HTTPs

Authentication Identified

- None

Plugins

- 426 have been included per scan policy
- 369 have been started based on target information collected

List of plugins is available in 'plugins.csv' attachment.

Settings used to conduct this scan are available in 'configuration.csv' attachment.

OS Detection

VULNERABILITY INFO PLUGIN ID 98003

Description

This is an informational notice that by investigating the response headers from the remote host, it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-03-01T00:00:00+00:00
MODIFICATION DATE	2018-03-01T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98003

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

OS Detection Instances (1)

VULNERABILITY INFO PLUGIN ID 98003

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Operating system has been guessed as 'Microsoft Windows 10' from https://soilgassafe.rti.org/ response contents.
```

Web Application Sitemap

VULNERABILITY INFO PLUGIN ID 98009

Description

Publishes the sitemap of the web application as seen by the scan.

The list of all URLs that have been detected during the scan are available as an attachment. For each URL in the sitemap, the following information is provided:

- The first time the URL is detected - The logic used to detect the URL. This information may be found by: crawling rendering the page by a specific plugin - The parent URL requested to detect the URL - If the URL has been requested at least once, information about the response - Whether or not the URL has been queued for audit - If the URL has not been queued for audit, the reason why the URL does not need an audit - Whether or not the URL has been effectively audited - If the URL has not been effectively audited, the reason that the scanner was unable to audit the URL

Reasons for not adding a URL to the audit queue are as follows:

- not_in_domain: The domain of the URL does not match main target URL - scope_configuration: The URL does not match scope include list scan settings - directory_depth: The number of directories in the URL path exceeds the scan configuration setting - exclude_file_extension: The URL file extension matched one entry of the file extension blacklist

setting - exclude_path_patterns: The URL matched one entry of the URL exclusion blacklist setting - redundant_path: The number of URLs to be audited with the same path and query string parameters has been reached - request_redirect_limit: The number of HTTP redirects allowed per scan configuration setting has been reached - queue_full: The number of URLs to audit has been reached

If a scan fails to audit a URL that has been queued for audit, reasons for the failure are as follows:

- timeout: The request timed out when trying to retrieve URL contents - filesize_exceeded: URL response exceeded file size limit defined in the scan configuration - scan_timelimit_reached: The URL couldn’t be audited before the scan time limit - user_abort: The user stopped the scan before the URL could be audited

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2020-11-03T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98009

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Web Application Sitemap Instances (1)

VULNERABILITY INFO PLUGIN ID 98009

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The scan has discovered 57 distinct URLs.


The following is a breakdown of which URLs were audited:


- 4 effectively audited

- 27 not queued due to file extension exclusions

- 18 not queued due to the URL not being in the target domain

- 8 not queued due to the URL containing a fragment which is a feature of browsers and not included in HTTP requests.

The page being referred to by the fragment shall still be audited by the scanner.


For URLs we received responses for, here is a distribution of the content type headers:


- 13 application/javascript

- 1 image/jpeg

- 3 image/svg+xml

- 9 text/css

- 2 text/css; charset=utf-8

- 1 text/html


Response times ranged between 0.003564s and 0.096116s.
```

You can access the complete list of URLs with the information collected by the scan as an attachment to this plugin.

Network Timeout Encountered

VULNERABILITY INFO PLUGIN ID 98019

Description

Provides a report of network timeouts encountered during the scan, showing URLs and the number of timeouts for each URL.

Note that assessment will stop on any URLs in timeout state, and timeouts may increase significantly the overall duration of the scan.

Solution

Check your web application logs and verify that it is functioning as expected and can handle significant amounts of traffic generated by the scanner.

Additionally, the scan policy may be edited to optimize the performance settings.

See Also

Plugin Details

PUBLICATION DATE	2017-09-25T00:00:00+00:00
MODIFICATION DATE	2017-09-25T00:00:00+00:00
FAMILY	General
SEVERITY	Info

PLUGIN ID	98019

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Network Timeout Encountered Instances (1)

VULNERABILITY INFO PLUGIN ID 98019

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
3 timeouts encountered for URL 'https://soilgassafe.rti.org/'

1 timeouts encountered for URL 'https://soilgassafe.rti.org/index.html'

2 timeouts encountered for URL 'https://soilgassafe.rti.org/www.rti.org'

3 timeouts encountered for URL 'https://soilgassafe.rti.org/www.Jacobs.com'
```

Allowed HTTP Methods

VULNERABILITY INFO PLUGIN ID 98047

Description

There are a number of HTTP methods that can be used on a webserver (`OPTIONS`, `HEAD`, `GET`, `POST`, `PUT`, `DELETE` etc.). Each of these methods perform a different function and each have an associated level of risk when their use is permitted on the webserver.

By sending an HTTP OPTIONS request and a direct HTTP request for each method, the scanner discovered the methods that are allowed by the server.

Solution

It is recommended that a whitelisting approach be taken to explicitly permit only the HTTP methods required by the application and block all others.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#limitexcept

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2021-07-13T00:00:00+00:00

FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98047

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Allowed HTTP Methods Instances (1)

VULNERABILITY INFO PLUGIN ID 98047

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The scanner was able to identify several HTTP methods that can be used for one or several URLs. The results are
available as attachments.
```

Interesting Response

VULNERABILITY INFO PLUGIN ID 98050

Description

The scanner identified some responses with a status code other than the usual 200 (OK), 301 (Moved Permanently), 302 (Found) and 404 (Not Found) codes. These codes can provide useful insights into the behavior of the web application and identify any unexpected responses to be addressed.

Solution

-

See Also

http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2021-06-14T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98050

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Interesting Response Instances (9)

VULNERABILITY INFO PLUGIN ID 98050

INSTANCE

https://soilgassafe.rti.org/www.rti.org

Identification

PROOF

```
HTTP/1.1 400 Bad Request
```

OUTPUT

```
A response has been received with a response code '400' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/www.rti.org'.
```

HTTP Info

REQUEST MADE

```
GET /www.rti.org HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Length: x
Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 02 Nov 2022 16:06:57 GMT
Connection: close
Content-Length: 374
```

INSTANCE

https://soilgassafe.rti.org/index.html

Identification

PROOF

```
HTTP/1.1 400 Bad Request
```

OUTPUT

A response has been received with a response code '400' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/index.html'.

HTTP Info

REQUEST MADE

```
GET /index.html HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
```

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip;q=1.0,deflate;q=0.6,identity;q=0.3'"

Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80

RESPONSE HEADERS

HTTP/1.1 400 Bad Request

Content-Type: text/html; charset=us-ascii

Server: Microsoft-HTTPAPI/2.0

Date: Wed, 02 Nov 2022 15:50:59 GMT

Connection: close

Content-Length: 311

INSTANCE

https://soilgassafe.rti.org/*~1*%5Ca.aspx?&aspxerrorpath=/

Identification

PROOF

HTTP/1.1 501 Not Implemented

OUTPUT

A response has been received with a response code '501' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP TRACE request made on the URL 'https://soilgassafe.rti.org/*~1*%5Ca.aspx?&aspxerrorpath=/'.

HTTP Info

REQUEST MADE

TRACE /*~1*%5Ca.aspx?&aspxerrorpath=/ HTTP/1.1

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80
```

RESPONSE HEADERS

```
HTTP/1.1 501 Not Implemented
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 02 Nov 2022 15:50:34 GMT
Content-Length: 1508
```

INSTANCE

https://soilgassafe.rti.org/Trace.axd

Identification

PROOF

```
HTTP/1.1 403 Forbidden
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/Trace.axd'.
```

HTTP Info

REQUEST MADE

```
GET /Trace.axd HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 403 Forbidden
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 02 Nov 2022 15:46:25 GMT
Content-Length: 2500
```

INSTANCE

https://soilgassafe.rti.org/images/

Identification

PROOF

```
HTTP/1.1 403 Forbidden
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this response is due to an abnormal behavior of the target.
```

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/images/'.

HTTP Info

REQUEST MADE

```
GET /images/ HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 02 Nov 2022 15:44:51 GMT
Content-Length: 1233
```

INSTANCE

https://soilgassafe.rti.org/assets/file:%2f%2f/etc/passwd

Identification

PROOF

```
HTTP/1.1 400 Bad Request
```

OUTPUT

A response has been received with a response code '400' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/assets/file:%2f%2f/etc/passwd'.

HTTP Info

REQUEST MADE

```
GET /assets/file:%2f%2f/etc/passwd HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 400 Bad Request
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 02 Nov 2022 15:43:06 GMT
Content-Length: 3490
```

INSTANCE

https%3A%2F%2Fsoilgassafe.rti.org%2Fcgi-bin%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2Fetc%2Fpasswd

Identification

PROOF

```
HTTP/1.1 400 Bad Request
```

OUTPUT

A response has been received with a response code '400' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd'.

HTTP Info

REQUEST MADE

```
GET /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Upgrade-Insecure-Requests: 1
Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
```

Date: Wed, 02 Nov 2022 15:39:34 GMT

Connection: close

Content-Length: 324

INSTANCE

https%3A%2F%2Fsoilgassafe.rti.org%2F..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwindows%5Cwin.ini

Identification

PROOF

HTTP/1.1 403 Forbidden

OUTPUT

A response has been received with a response code '403' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/..\..\..\..\..\..\..\..\..\windows\win.ini'.

HTTP Info

REQUEST MADE

GET /..\..\..\..\..\..\..\..\..\windows\win.ini HTTP/1.1

REQUEST HEADERS

Host: soilgassafe.rti.org

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36

Accept: */*

Accept-Language: en-US,en;q=0.5

```
Upgrade-Insecure-Requests: 1

Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 403 Forbidden

Content-Type: text/html; charset=us-ascii

Server: Microsoft-HTTPAPI/2.0

Date: Wed, 02 Nov 2022 15:39:33 GMT

Connection: close

Content-Length: 312
```

INSTANCE

https://soilgassafe.rti.org/

Identification

PROOF

```
HTTP/1.1 406 Not Acceptable
```

OUTPUT

```
A response has been received with a response code '406' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://soilgassafe.rti.org/'.
```

HTTP Info

REQUEST MADE

```
GET / HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36

Accept: C:/windows/win.ini

Accept-Language: en-US,en;q=0.5

Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80
```

RESPONSE HEADERS

```
HTTP/1.1 406 Not Acceptable

Content-Type: text/html

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:47 GMT

Content-Length: 1346
```

Technologies Detected

VULNERABILITY INFO PLUGIN ID 98059

Description

This is an informational plugin to inform the user what technologies the framework has detected on the target application, which can then be examined and checked for known vulnerable software versions

Solution

Only use components that do not have known vulnerabilities, only use components that when combined to not introduce a security vulnerability, and ensure that a misconfiguration does not cause any vulnerabilities

See Also

Plugin Details

PUBLICATION DATE	2017-12-06T00:00:00+00:00
MODIFICATION DATE	2017-12-11T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98059

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Technologies Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98059

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The framework has detected the following technologies in the target application:


- Bootstrap (v3.3.5)

- jQuery (v2.1.4)

- Modernizr (v2.6.2)

- ASP.NET (version unknown)

- IIS (v10.0)
```

Cookies Collected

VULNERABILITY INFO PLUGIN ID 98061

Description

The scanner collected the cookies returned by the application during the scan. The list includes the following information for each cookie:

- Name: name of the cookie

- Value: value of the cookie

- Domain: hosts to which the cookie will be sent

- Path: URL path which must exist in the requested resource before sending the cookie

- Expires: maximum lifetime of the cookie as an HTTP-date timestamp

- Max-Age: number of seconds until the cookie expires

- HttpOnly: cookie is set to be not accessible via JavaScript, XMLHttpRequest and Request APIs

- Secure: cookie will be sent to the server only when a request is made using HTTPS

- SameSite: cookie will be sent along with cross-site request according the defined policy

- URL: first URL discovered which set the cookie in its response

- Set-Method: method used by the application to set the cookie (Set-Cookie or JavaScript)

- Audited: cookie will be audited by plugins during the scan

- Reason Not Audited: reason given for the cookie not being audited during the scan

Solution

-

See Also

https://en.wikipedia.org/wiki/HTTP_cookie

https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

https://tools.ietf.org/html/rfc6265

Plugin Details

PUBLICATION DATE	2020-09-01T00:00:00+00:00
MODIFICATION DATE	2021-11-23T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98061

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-

WASC	-
OWASP	-
CVE	-
BID	-

Cookies Collected Instances (1)

VULNERABILITY INFO PLUGIN ID 98061

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The following cookies have been collected during the scan of the target:

- 1 cookie(s) specified via Set-Cookie

- 0 cookie(s) set via JavaScript code

The complete list of the cookies is available in attachment.
```

E-mail Address Disclosure

VULNERABILITY INFO PLUGIN ID 98078

Description

Email addresses are typically found on "Contact us" pages, however, they can also be found within scripts or code comments of the application. They are used to provide a legitimate means of contacting an organisation.

As one of the initial steps in information gathering, cyber-criminals will spider a website and using automated methods collect as many email addresses as possible, that they may then use in a social engineering attack.

Using the same automated methods, scanner was able to detect one or more email addresses that were stored within the affected page.

Solution

E-mail addresses should be presented in such a way that it is hard to process them automatically.

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2022-02-15T00:00:00+00:00
FAMILY	Data Exposure

SEVERITY	Info
PLUGIN ID	98078

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

E-mail Address Disclosure Instances (1)

VULNERABILITY INFO PLUGIN ID 98078

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Number of Email Addresses Collected: 2

Listed below are each email address and the number of URLs where the email address has been found:

madeline.collins@jacobs.com found on 2 URLs

soilgassafe@rti.org found on 2 URLs
```

Target Information

VULNERABILITY INFO PLUGIN ID 98136

Description

Publishes the target information of the starting url as evaluated by the scan.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-07-27T00:00:00+00:00
MODIFICATION DATE	2017-07-27T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98136

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-

CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Target Information Instances (1)

VULNERABILITY INFO PLUGIN ID 98136

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Access to URL 'https://soilgassafe.rti.org/' has been confirmed.



Target Information

------------------------


Domain Name : soilgassafe.rti.org

IP Address : 152.5.64.97



Response Information

---------------------------


Status Code : 200

Response Code : ok

Response Time : 0.061025s

Response Size : 38535 bytes

Content-Type : text/html
```

HTTP Info

REQUEST MADE

```
GET / HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "42aefd14cfeed81:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 02 Nov 2022 15:38:35 GMT
Content-Length: 13003
Set-Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80; path=/; Httponly; Secure
```

Screenshot

VULNERABILITY INFO PLUGIN ID 98138

Description

Screenshot of the target web page, see attached image. This screenshot should show you the target page we are launching the scan against. If the image is not of the intended target page, please check the provided url in the scan configuration.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-01-23T00:00:00+00:00
MODIFICATION DATE	2018-02-14T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98138

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Screenshot Instances (1)

VULNERABILITY INFO PLUGIN ID 98138

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
WAS Scanner has taken a screenshot of the page at url 'https://soilgassafe.rti.org/' with dimensions 1585x1200.


Please see the attachment for the screenshot image.
```

Missing Permissions Policy

VULNERABILITY INFO PLUGIN ID 98526

Description

Permissions Policy provides mechanisms to websites to restrict the use of browser features in its own frame and in iframes that it embeds.

Solution

Configure Permissions Policy on your website by adding 'Permissions-Policy' HTTP header.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/

Plugin Details

PUBLICATION DATE	2019-03-27T00:00:00+00:00
MODIFICATION DATE	2021-05-07T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98526

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Permissions Policy Instances (1)

VULNERABILITY INFO PLUGIN ID 98526

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://soilgassafe.rti.org/
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Missing Referrer Policy

VULNERABILITY INFO PLUGIN ID 98527

Description

Referrer Policy provides mechanisms to websites to restrict referrer information (sent in the referer header) that browsers will be allowed to add.

No Referrer Policy header or metatag configuration has been detected.

Solution

Configure Referrer Policy on your website by adding 'Referrer-Policy' HTTP header or meta tag referrer in HTML.

See Also

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

Plugin Details

PUBLICATION DATE	2019-04-02T00:00:00+00:00
MODIFICATION DATE	2019-04-02T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98527

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Referrer Policy Instances (1)

VULNERABILITY INFO PLUGIN ID 98527

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://soilgassafe.rti.org/
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

Missing 'Expect-CT' Header

VULNERABILITY INFO PLUGIN ID 98612

Description

The Expect-CT header allows sites to opt in to reporting and or enforcement of Certificate Transparency requirements, which prevents the use of misissued certificates for that site from going unnoticed. This URL is flagged as a specific example.

The Expect-CT will likely become obsolete in June 2021. Since May 2018 new certificates are expected to support SCTs by default. Certificates before March 2018 were allowed to have a lifetime of 39 months, those will all be expired in June 2021.

Solution

If your certificate supports SCT (Signed Certificate Timestamp) by default, the Expect-CT header is not required.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT

Plugin Details

PUBLICATION DATE	2019-05-29T00:00:00+00:00
MODIFICATION DATE	2021-06-16T00:00:00+00:00

FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98612

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	693
WASC	Application Misconfiguration
OWASP	-
CVE	-
BID	-

Missing 'Expect-CT' Header Instances (1)

VULNERABILITY INFO PLUGIN ID 98612

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The Expect-CT header was not detected on https://soilgassafe.rti.org/
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

SSL/TLS Certificate Information

VULNERABILITY INFO PLUGIN ID 112491

Description

This plugin displays information about the X.509 certificate extracted from the HTTPS connection.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-10-03T00:00:00+00:00
MODIFICATION DATE	2020-10-02T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112491

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-

CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Certificate Information Instances (1)

VULNERABILITY INFO PLUGIN ID 112491

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Certificate 1

--------------

Common Name: *.rti.org

Alternative Names: *.rti.org rti.org

Issuer: GlobalSign nv

Valid from: 2022-02-04 18:51:07 UTC

Valid until: 2023-03-08 18:51:07 UTC (expires in 4 months, 4 days)

Validity Period: 397 days

Key: RSA 2048-bit

Signature: sha256WithRSAEncryption


Certificate 2

--------------

Common Name: globalsign rsa ov ssl ca

Issuer: GlobalSign

Valid from: 2018-11-21 00:00:00 UTC

Valid until: 2028-11-21 00:00:00 UTC (expires in 6 years, 2 weeks, 4 days)

Validity Period: 3653 days

Key: RSA 2048-bit
```

Signature: sha256WithRSAEncryption

Certificate 3

Common Name: globalsign

Issuer: GlobalSign

Valid from: 2009-03-18 10:00:00 UTC

Valid until: 2029-03-18 10:00:00 UTC (expires in 6 years, 4 months, 2 weeks)

Validity Period: 7305 days

Key: RSA 2048-bit

Signature: sha256WithRSAEncryption

Missing 'X-XSS-Protection' Header

VULNERABILITY INFO PLUGIN ID 112526

Description

The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.

The server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.

If legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead.

Solution

Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages.

See Also

https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xxxsp

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Plugin Details

PUBLICATION DATE	2018-11-27T00:00:00+00:00
MODIFICATION DATE	2021-03-12T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	112526

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing 'X-XSS-Protection' Header Instances (1)

VULNERABILITY INFO PLUGIN ID 112526

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://soilgassafe.rti.org/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Language=en-US,en;q=0.5
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Wed, 02 Nov 2022 15:23:38 GMT
Accept-Ranges: bytes
ETag: "0b9ad14cfeed81:0"
Vary: Accept-Encoding
```

```
Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Wed, 02 Nov 2022 15:38:38 GMT

Content-Length: 9946

Set-Cookie: BALANCE=rd200o00000000000000000000ffffac18231fo80; path=/; Httponly; Secure
```

SSL/TLS Versions Supported

VULNERABILITY INFO PLUGIN ID 112530

Description

This plugin displays information about the SSL/TLS versions supported by remote server for HTTPS connection.

Solution

-

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2018-10-03T00:00:00+00:00
MODIFICATION DATE	2020-10-02T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112530

Risk Information

CVSSV3 BASE SCORE	-

CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Versions Supported Instances (1)

VULNERABILITY INFO PLUGIN ID 112530

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Protocol Supported
---------------------
SSL 2.0 No
SSL 3.0 No
TLS 1.0 No
TLS 1.1 No
TLS 1.2 Yes
TLS 1.3 No
```

SSL/TLS Server Cipher Suite Preference

VULNERABILITY INFO PLUGIN ID 112598

Description

The remote server is configured with a SSL/TLS cipher suite preference list used to determine the cipher suite during the negotiation with the client.

Solution

-

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

http://www.exploresecurity.com/testing-for-cipher-suite-preference/

Plugin Details

PUBLICATION DATE	2020-09-24T00:00:00+00:00
MODIFICATION DATE	2020-09-24T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112598

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Server Cipher Suite Preference Instances (1)

VULNERABILITY INFO PLUGIN ID 112598

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The scanner detected that the remote host is configured with cipher suite preference on the following protocol(s):


TLS v1.2

-------

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```

Allowed HTTP Versions

VULNERABILITY INFO PLUGIN ID 112613

Description

The Hypertext Transfer Protocol (HTTP) is the underlying protocol of the World Wide Web. Since its first release, HTTP has evolved to support modern web usages and currently exists in four versions:

- HTTP/0.9

- HTTP/1.0

- HTTP/1.1

- HTTP/2

The scanner identified the supported versions of the HTTP protocol on the target web application.

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP

Plugin Details

PUBLICATION DATE	2020-10-13T00:00:00+00:00

MODIFICATION DATE	2020-10-13T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	112613

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Allowed HTTP Versions Instances (1)

VULNERABILITY INFO PLUGIN ID 112613

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
The scanner detected the following HTTP versions on the target application :


- HTTP/1.1


The list of requests and responses observed is provided in attachment.
```

Security.txt File Not Detected

VULNERABILITY INFO PLUGIN ID 112723

Description

A Security.txt file has not been detected on the target.

When security risks in web services are discovered by independent security researchers, this file defines the channels to disclose them properly & enables 3rd party researchers to disclose issues securely in a manner defined by the organization.

Organizations should consider creating a security.txt file containing contact and other information in the defined format and place it under the .well-known directory of the server.

Solution

-

See Also

https://securitytxt.org/

https://tools.ietf.org/html/draft-foudil-securitytxt-11

Plugin Details

PUBLICATION DATE	2021-03-17T00:00:00+00:00
MODIFICATION DATE	2021-03-17T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	112723

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Security.txt File Not Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112723

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
No or a malformed security.txt was found at https://soilgassafe.rti.org/.well-known/security.txt
```

HTTP Info

REQUEST MADE

```
GET /.well-known/security.txt HTTP/1.1
```

REQUEST HEADERS

```
Host: soilgassafe.rti.org
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4158.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: BALANCE=rd200o00000000000000000000ffffac182320o80
```

RESPONSE HEADERS

```
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 02 Nov 2022 15:44:57 GMT
```

```
Content-Length: 1245
```

Out-of-Date JQuery Detected

VULNERABILITY INFO PLUGIN ID 113027

Description

An out-of-date version of JQuery has been detected. An outdated version could have vulnerabilities or missing security features.

Solution

Upgrade to the latest version of JQuery.

See Also

https://jquery.com/

https://blog.jquery.com/

https://github.com/jquery/jquery/tags

Plugin Details

PUBLICATION DATE	2021-10-25T00:00:00+00:00
MODIFICATION DATE	2021-10-27T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Info
PLUGIN ID	113027

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Out-of-Date JQuery Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 113027

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Technology jQuery has been detected with version 2.1.4. Latest version available is : 3.6.0
```

Out-of-Date Bootstrap Detected

VULNERABILITY INFO PLUGIN ID 113030

Description

An out-of-date version of Bootstrap has been detected. An outdated version could have vulnerabilities or missing security features.

Solution

Upgrade to the latest version of Bootstrap.

See Also

https://getbootstrap.com/

https://getbootstrap.com/docs/versions/

https://github.com/twbs/bootstrap/tags

Plugin Details

PUBLICATION DATE	2021-10-27T00:00:00+00:00
MODIFICATION DATE	2022-05-25T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Info
PLUGIN ID	113030

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Out-of-Date Bootstrap Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 113030

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Technology Bootstrap has been detected with version 3.3.5. Latest version available is : 5.2.0-beta1
```

Out-of-Date Modernizr Detected

VULNERABILITY INFO PLUGIN ID 113032

Description

An out-of-date version of Modernizr has been detected. An outdated version could have vulnerabilities or missing security features.

Solution

Upgrade to the latest version of Modernizr.

See Also

https://modernizr.com/

https://github.com/Modernizr/Modernizr/blob/master/CHANGELOG.md

https://github.com/Modernizr/Modernizr/tags

Plugin Details

PUBLICATION DATE	2021-10-27T00:00:00+00:00
MODIFICATION DATE	2022-05-25T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Info
PLUGIN ID	113032

Risk Information

CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Out-of-Date Modernizr Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 113032

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Technology Modernizr has been detected with version 2.6.2. Latest version available is : 3.12.0
```

SSL/TLS Certificate Contains Wildcard Entries

VULNERABILITY INFO PLUGIN ID 113045

Description

The remote server presents an SSL/TLS certificate with wildcard entries. The use of a wildcard character in a entry permits a certificate to cover a number of subdomains of a domain.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2021-11-10T00:00:00+00:00
MODIFICATION DATE	2021-11-10T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	113045

Risk Information

CVSSV3 BASE SCORE	-

CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Certificate Contains Wildcard Entries Instances (1)

VULNERABILITY INFO PLUGIN ID 113045

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
A wildcard symbol (*) has been detected in the following certificate entries:

Certificate Common Name: *.rti.org

Certificate Subject Alternative Names:

- *.rti.org
```

SSL/TLS Cipher Suites Supported

VULNERABILITY INFO PLUGIN ID 115491

Description

This plugin displays supported SSL/TLS cipher suites.

Solution

-

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2022-10-07T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	115491

Risk Information

CVSSV3 BASE SCORE	-

CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Cipher Suites Supported Instances (1)

VULNERABILITY INFO PLUGIN ID 115491

INSTANCE

https://soilgassafe.rti.org/

Identification

OUTPUT

```
Protocol Cipher Suite Name (RFC)

-----------------------------------

TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```