alerts

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12246
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	158
alertRef	10098

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12248
inputVector	
url	http://localhost:8884/?order_by=id&sort=DESC
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	159
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12248
inputVector	
url	http://localhost:8884/?order_by=id&sort=DESC

tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	160
alertRef	10021

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12246
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	161
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12248
inputVector	
url	http://localhost:8884/?order_by=id&sort=DESC
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	162
alertRef	10037

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express

pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12246
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	163
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12250
inputVector	
url	http://localhost:8884/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	164
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12250
inputVector	
url	http://localhost:8884/
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low

id	166
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12250
inputVector	
url	http://localhost:8884/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	167
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12253
inputVector	
url	http://localhost:8884/7
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	173
alertRef	10098

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12252
inputVector	
url	http://localhost:8884/13

tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	174
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12252
inputVector	
url	http://localhost:8884/13
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	175
alertRef	10021

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12253
inputVector	
url	http://localhost:8884/7
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	176
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express

pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12252
inputVector	
url	http://localhost:8884/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	177
alertRef	10037

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12253
inputVector	
url	http://localhost:8884/7
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	178
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	PUT
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12254
inputVector	
url	http://localhost:8884/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium

id	179
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	PUT
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12254
inputVector	
url	http://localhost:8884/13
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-cc
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	180
alertRef	10021

alert

sourceid	3
other	
method	PUT
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12254
inputVector	
url	http://localhost:8884/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	181
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	POST
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12255
inputVector	
url	http://localhost:8884/create

tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	182
alertRef	10098

alert

sourceid	3
other	
method	POST
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12255
inputVector	
url	http://localhost:8884/create
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	183
alertRef	10037

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	POST
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12256
inputVector	
url	http://localhost:8884/create
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	185
alertRef	10021

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	DELETE
evidence	Access-Control-Allow-Origin: *

pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12257
inputVector	
url	http://localhost:8884/14
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	187
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	DELETE
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12257
inputVector	
url	http://localhost:8884/14
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	188
alertRef	10021

alert

sourceid	3
other	
method	DELETE
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12257
inputVector	
url	http://localhost:8884/14
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low

id	189
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12258
inputVector	
url	http://localhost:8882/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	190
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12258
inputVector	
url	http://localhost:8882/
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	191
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12258
inputVector	
url	http://localhost:8882/

tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	192
alertRef	10037

alert

sourceid	3
other	userParam=email userValue=Otho93@gmail.com passwordParam=password referer=http://localhost:8882/
method	POST
evidence	password
pluginId	10111
cweid	-1
confidence	Low
wascid	-1
description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fiel
messageId	12260
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
alert	Authentication Request Identified
param	email
attack	
name	Authentication Request Identified
risk	Informational
id	193
alertRef	10111

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	POST
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12260
inputVector	
url	http://localhost:8882/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	194
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	POST
evidence	

pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12260
inputVector	
url	http://localhost:8882/
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	195
alertRef	10021

alert

sourceid	3
other	
method	POST
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12260
inputVector	
url	http://localhost:8882/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	196
alertRef	10037

alert

sourceid	3
other	userParam=email userValue=Kyle24@gmail.com passwordParam=password referer=http://localhost:8882/
method	POST
evidence	password
pluginId	10111
cweid	-1
confidence	Low
wascid	-1
description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fiel
messageId	12261
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
alert	Authentication Request Identified
param	email
attack	
name	Authentication Request Identified
risk	Informational

id	197
alertRef	10111

alert

sourceid	3
other	userParam=email userValue=Kyle24@gmail.com passwordParam=password referer=http://localhost:8881/login
method	POST
evidence	password
pluginId	10111
cweid	-1
confidence	High
wascid	-1
description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fiel
messageId	12262
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
alert	Authentication Request Identified
param	email
attack	
name	Authentication Request Identified
risk	Informational
id	201
alertRef	10111

alert

sourceid	3
other	json:token
method	POST
evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MjIsInByb2ZpbGUiOlt7ImlkIjoyMSwidXNlcl9pZCI6MjIsImZ1bGxfbmFtZSI6IkRvbmFsZCBHb
pluginId	10112
cweid	-1
confidence	Medium
wascid	-1
description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used i
messageId	12262
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
alert	Session Management Response Identified
param	token
attack	
name	Session Management Response Identified
risk	Informational
id	202
alertRef	10112

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	POST
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12262
inputVector	
url	http://localhost:8881/login

tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	203
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	POST
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12262
inputVector	
url	http://localhost:8881/login
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	204
alertRef	10021

alert

sourceid	3
other	
method	POST
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12262
inputVector	
url	http://localhost:8881/login
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	205
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *

pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12264
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	206
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12264
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	207
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12264
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low

id	208
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	PUT
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12265
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	209
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	PUT
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12265
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	210
alertRef	10021

alert

sourceid	3
other	
method	PUT
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12265
inputVector	
url	http://localhost:8882/13

tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	211
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	DELETE
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12266
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	212
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	DELETE
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12266
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	213
alertRef	10021

alert

sourceid	3
other	
method	DELETE
evidence	X-Powered-By: Express

pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12266
inputVector	
url	http://localhost:8882/13
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	214
alertRef	10037

alert

sourceid	3
other	
method	GET
evidence	HTTP/1.1 500 Internal Server Error
pluginId	90022
cweid	200
confidence	Medium
wascid	13
description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. T
messageId	12268
inputVector	
url	http://localhost:8883/
tags	{WSTG-v42-ERRH-02=https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/08-Testing_for_Error_Ha
reference	
solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier t
alert	Application Error Disclosure
param	
attack	
name	Application Error Disclosure
risk	Low
id	215
alertRef	90022

alert

sourceid	3
other	json:token
method	POST
evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MjIsInByb2ZpbGUiOlt7ImlkIjoyMSwidXNlcl9pZCI6MjIsImZ1bGxfbmFtZSI6IkRvbmFsZCBHb
pluginId	10112
cweid	-1
confidence	High
wascid	-1
description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used i
messageId	12262
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
alert	Session Management Response Identified
param	token
attack	
name	Session Management Response Identified
risk	Informational

id	216
alertRef	10112

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12268
inputVector	
url	http://localhost:8883/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	217
alertRef	10098

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12268
inputVector	
url	http://localhost:8883/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	219
alertRef	10037

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12267
inputVector	
url	http://localhost:8883/

tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	220
alertRef	10021

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12270
inputVector	
url	http://localhost:8883/5
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	222
alertRef	10098

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12270
inputVector	
url	http://localhost:8883/5
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	223
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *

pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12271
inputVector	
url	http://localhost:8883/4
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	224
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12271
inputVector	
url	http://localhost:8883/4
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	225
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12271
inputVector	
url	http://localhost:8883/4
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low

id	226
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12272
inputVector	
url	http://localhost:8883/6
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	227
alertRef	10098

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12272
inputVector	
url	http://localhost:8883/6
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	228
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12274
inputVector	
url	http://localhost:8883/3

tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	231
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12274
inputVector	
url	http://localhost:8883/3
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all w
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	232
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12274
inputVector	
url	http://localhost:8883/3
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	233
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *

pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12275
inputVector	
url	http://localhost:8883/9
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	234
alertRef	10098

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12275
inputVector	
url	http://localhost:8883/9
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	235
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12281
inputVector	
url	http://localhost:8883/1
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium

id	254
alertRef	10098

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12281
inputVector	
url	http://localhost:8883/1
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	255
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	POST
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12282
inputVector	
url	http://localhost:8883/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	257
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	POST
evidence	
pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12282
inputVector	
url	http://localhost:8883/

tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	258
alertRef	10021

alert

sourceid	3
other	
method	POST
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12282
inputVector	
url	http://localhost:8883/
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	259
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12287
inputVector	
url	http://localhost:8883/17
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium
id	275
alertRef	10098

alert

sourceid	3
other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concer
method	GET
evidence	

pluginId	10021
cweid	693
confidence	Medium
wascid	15
description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform
messageId	12287
inputVector	
url	http://localhost:8883/17
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, OWASP_2017_A06=https://owasp.org/www-project-top-ten/201
reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-co
solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all v
alert	X-Content-Type-Options Header Missing
param	x-content-type-options
attack	
name	X-Content-Type-Options Header Missing
risk	Low
id	276
alertRef	10021

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12287
inputVector	
url	http://localhost:8883/17
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	277
alertRef	10037

alert

sourceid	3
other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this
method	GET
evidence	Access-Control-Allow-Origin: *
pluginId	10098
cweid	264
confidence	Medium
wascid	14
description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
messageId	12288
inputVector	
url	http://localhost:8883/8
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, OWASP_2017_A05=https://owasp.org/www-project-top-ten/2017/
reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allo
alert	Cross-Domain Misconfiguration
param	
attack	
name	Cross-Domain Misconfiguration
risk	Medium

id	278
alertRef	10098

alert

sourceid	3
other	
method	GET
evidence	X-Powered-By: Express
pluginId	10037
cweid	200
confidence	Medium
wascid	13
description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate a
messageId	12288
inputVector	
url	http://localhost:8883/8
tags	{OWASP_2021_A01=https://owasp.org/Top10/A01_2021-Broken_Access_Control/, WSTG-v42-INFO-08=https://owasp.org/www-project-web-security
reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_A
solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
alert	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
param	
attack	
name	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
risk	Low
id	279
alertRef	10037

alert

sourceid	1
other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8
description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	12705
inputVector	json
url	http://localhost:8883/
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actu malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	payment_method
attack	<script>alert(1);</script>
name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	290
alertRef	40014

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low

wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	13623
inputVector	
url	http://localhost:8883/.hg
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	291
alertRef	40035

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	13625
inputVector	
url	http://localhost:8883/.bzr
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	292
alertRef	40035

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	13627
inputVector	
url	http://localhost:8883/._darcs
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	293
alertRef	40035

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	13629
inputVector	
url	http://localhost:8883/BitKeeper
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	294
alertRef	40035

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13632
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	295
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13638
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	296
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13641
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	297
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13643
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	298
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0

description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13655
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	299
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13657
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	300
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13659
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	301
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13671
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	302
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13675
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	303
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13682
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	304
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13685
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	305
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13693
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	306
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0

description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13698
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	307
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13704
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	308
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13713
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	309
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13715
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	310
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13721
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	311
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13733
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	312
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13735
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	313
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13738
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	314
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0

description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13744
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	315
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13746
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	316
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13751
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	317
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13754
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	318
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13755
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	319
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13761
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	320
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13764
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	321
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13766
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	322
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0

description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13771
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	323
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13777
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	324
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13779
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	325
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13782
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	326
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13789
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	327
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13790
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	328
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13796
inputVector	
url	http://localhost:8883/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	329
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	13798
inputVector	
url	http://localhost:8883
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	330
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13

description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	15087
inputVector	
url	http://localhost:8881/.hg
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	331
alertRef	40035

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	15089
inputVector	
url	http://localhost:8881/.bzr
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	332
alertRef	40035

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	15091
inputVector	
url	http://localhost:8881/._darcs
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	333
alertRef	40035

alert

sourceid	1
other	
method	GET
evidence	HTTP/1.1 200 OK
pluginId	40035
cweid	538
confidence	Low
wascid	13
description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by
messageId	15093
inputVector	
url	http://localhost:8881/BitKeeper
tags	{OWASP_2021_A05=https://owasp.org/Top10/A05_2021-Security_Misconfiguration/, WSTG-v42-CONF-05=https://owasp.org/www-project-web-secu
reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate autl
alert	Hidden File Found
param	
attack	
name	Hidden File Found
risk	Medium
id	334
alertRef	40035

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15117
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	335
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15119
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	336
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15121
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	337
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15123
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	338
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0

description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15125
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	339
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15127
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	340
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15129
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	341
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15131
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	342
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15133
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	343
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15135
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer

param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	344
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15137
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	345
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	15139
inputVector	
url	http://localhost:8881/login
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	346
alertRef	10104

alert

sourceid	1
other	The page results were successfully manipulated using the boolean conditions [Kyle24@gmail.com%] and [Kyle24@gmail.comXYZABCDEFGHIJ] The
method	POST
evidence	
pluginId	40018
cweid	89
confidence	Medium
wascid	19

description	SQL injection may be possible.
messageId	18433
inputVector	json
url	http://localhost:8882/
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-05=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user
alert	SQL Injection
param	email
attack	Kyle24@gmail.com%
name	SQL Injection
risk	High
id	347
alertRef	40018

alert

sourceid	1
other	The page results were successfully manipulated using the boolean conditions [Otho93@gmail.com%] and [Otho93@gmail.comXYZABCDEFGHIJ] The
method	POST
evidence	
pluginId	40018
cweid	89
confidence	Medium
wascid	19
description	SQL injection may be possible.
messageId	18434
inputVector	json
url	http://localhost:8882/
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-05=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user
alert	SQL Injection
param	email
attack	Otho93@gmail.com%
name	SQL Injection
risk	High
id	348
alertRef	40018

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25527
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	349
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25532
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	350
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25538
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	352
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25539
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg

solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	353
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25541
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	354
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25546
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	355
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0

confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25553
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	357
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25555
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	358
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25572
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	359
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25574
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	360
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25577
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	361
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25580
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg

solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	363
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25582
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	364
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25584
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	365
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0

confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25586
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	366
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25589
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	367
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25592
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	369
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25594
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	370
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25596
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	371
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25598
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg

solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	372
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25602
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	374
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25604
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	375
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0

confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25606
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	376
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25608
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	377
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25612
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	379
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25614
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	380
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25616
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	381
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25618
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg

solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	382
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25622
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	384
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25624
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	385
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0

confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25626
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	386
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25628
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	387
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25632
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	389
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25635
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	390
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25636
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	391
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25639
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg

solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	392
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25642
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	394
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25644
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	395
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0

confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25646
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	396
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25648
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	397
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25652
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	399
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25654
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	400
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25656
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	401
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25658
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg

solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	402
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25662
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	404
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25664
inputVector	
url	http://localhost:8882/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	405
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0

confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25666
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	406
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	25668
inputVector	
url	http://localhost:8882/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	407
alertRef	10104

alert

sourceid	1
other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8
description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	31694
inputVector	json
url	http://localhost:8884
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actu malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	title
attack	<script>alert(1);</script>

name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	409
alertRef	40014

alert

sourceid	1
other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8
description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	31704
inputVector	json
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actua malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	description
attack	<script>alert(1);</script>
name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	411
alertRef	40014

alert

sourceid	1
other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8
description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	31722
inputVector	json
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actua malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	course_content
attack	<script>alert(1);</script>
name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	413
alertRef	40014

alert

sourceid	1

other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8
description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	31744
inputVector	json
url	http://localhost:8884/
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actua malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	learning_outcomes
attack	<script>alert(1);</script>
name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	415
alertRef	40014

alert

sourceid	1
other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8
description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	31764
inputVector	json
url	http://localhost:8884/
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actua malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	course_inclusions
attack	<script>alert(1);</script>
name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	417
alertRef	40014

alert

sourceid	1
other	Raised with LOW confidence as the Content-Type is not HTML
method	GET
evidence	
pluginId	40014
cweid	79
confidence	Low
wascid	8

description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (respons
messageId	31782
inputVector	json
url	http://localhost:8884/?order_by=id&sort=DESC
tags	{OWASP_2021_A03=https://owasp.org/Top10/A03_2021-Injection/, WSTG-v42-INPV-02=https://owasp.org/www-project-web-security-testing-guide/v
reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakn encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to dete CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove th such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actu malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so ma perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved e
alert	Cross Site Scripting Weakness (Persistent in JSON Response)
param	author
attack	<script>alert(1);</script>
name	Cross Site Scripting Weakness (Persistent in JSON Response)
risk	Low
id	419
alertRef	40014

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45393
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	421
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45396
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational

id	422
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45399
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	423
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45404
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	424
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45405
inputVector	
url	http://localhost:8884/14

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	425
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45409
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	426
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45411
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	427
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45413
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	428
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45418
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
name	User Agent Fuzzer
risk	Informational
id	429
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45419
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational

id	430
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45421
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	431
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45424
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	432
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45426
inputVector	
url	http://localhost:8884

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	433
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45432
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	434
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45433
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	435
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45434
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	436
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45437
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	437
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45441
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational

id	438
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45442
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
name	User Agent Fuzzer
risk	Informational
id	439
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45446
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	440
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45448
inputVector	
url	http://localhost:8884/13

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	441
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45450
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	442
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45452
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	443
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45455
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational
id	444
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45457
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	445
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45459
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
name	User Agent Fuzzer
risk	Informational

id	446
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45463
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	447
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45464
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	448
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45465
inputVector	
url	http://localhost:8884

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	449
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45470
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	450
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45471
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	451
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45472
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	452
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45474
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	453
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45476
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational

id	454
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45479
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
name	User Agent Fuzzer
risk	Informational
id	455
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45481
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	456
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45485
inputVector	
url	http://localhost:8884/13

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	457
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45488
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	458
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45489
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	459
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45490
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational
id	460
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45492
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	461
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45495
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
name	User Agent Fuzzer
risk	Informational

id	462
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45499
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	463
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45500
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	464
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45501
inputVector	
url	http://localhost:8884/13

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	465
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45504
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	466
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45506
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	467
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45507
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	468
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45510
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
name	User Agent Fuzzer
risk	Informational
id	469
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45512
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational

id	470
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45514
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	471
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45516
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	472
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45518
inputVector	
url	http://localhost:8884

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	473
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45521
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	474
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45523
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	475
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45527
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	476
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45528
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	477
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45530
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational

id	478
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45531
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
name	User Agent Fuzzer
risk	Informational
id	479
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45533
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	480
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45536
inputVector	
url	http://localhost:8884

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	481
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45540
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	482
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45541
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational
id	483
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45542
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	484
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45544
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	485
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45547
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
name	User Agent Fuzzer
risk	Informational

id	486
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45549
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	487
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45551
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	488
alertRef	10104

alert

sourceid	1
other	
method	PUT
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45555
inputVector	
url	http://localhost:8884/13

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	489
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45556
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	490
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45557
inputVector	
url	http://localhost:8884/13
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	491
alertRef	10104

alert

sourceid	1
other	
method	POST
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45562
inputVector	
url	http://localhost:8884/create
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	492
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45563
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.
name	User Agent Fuzzer
risk	Informational
id	493
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45564
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational

id	494
alertRef	10104

alert

sourceid	1
other	
method	DELETE
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45565
inputVector	
url	http://localhost:8884/14
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	495
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45567
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	496
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45569
inputVector	
url	http://localhost:8884/13

tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	497
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45571
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
name	User Agent Fuzzer
risk	Informational
id	498
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45573
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	499
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	

pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45576
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	500
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45577
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
name	User Agent Fuzzer
risk	Informational
id	501
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45581
inputVector	
url	http://localhost:8884/
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational

id	502
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45582
inputVector	
url	http://localhost:8884/?order_by=id&sort=ASC
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	503
alertRef	10104

alert

sourceid	1
other	
method	GET
evidence	
pluginId	10104
cweid	0
confidence	Medium
wascid	0
description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode a
messageId	45583
inputVector	
url	http://localhost:8884
tags	{}
reference	https://owasp.org/wstg
solution	
alert	User Agent Fuzzer
param	Header User-Agent
attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
name	User Agent Fuzzer
risk	Informational
id	504
alertRef	10104