ZAP by Checkmarx Scanning Report

Sites: http://edge.microsoft.com https://telem-edge.smartscreen.microsoft.com https://data-edge.smartscreen.microsoft.com https://nav-edge.smartscreen.microsoft.com https://www.bing.com https://copilot.microsoft.com https://firefox-settings-attachments.cdn.mozilla.net https://firefox.settings.services.mozilla.com https://cdnjs.cloudflare.com https://cdn.jsdelivr.net https://content-signature-2.cdn.mozilla.net http://127.0.0.1:8000

Generated on Mon, 10 Nov 2025 23:04:54

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	7
Low	11
Informational	6

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	22
CSP: Wildcard Directive	Medium	22
CSP: script-src unsafe-eval	Medium	22
CSP: script-src unsafe-inline	Medium	22
CSP: style-src unsafe-inline	Medium	22
Content Security Policy (CSP) Header Not Set	Medium	1
Cross-Domain Misconfiguration	Medium	7
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Cookie No HttpOnly Flag	Low	23
Cookie Without Secure Flag	Low	4
Cookie with SameSite Attribute None	Low	1
Cookie without SameSite Attribute	Low	5
Cross-Domain JavaScript Source File Inclusion	Low	18

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	22
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1
Strict-Transport-Security Header Not Set	Low	14
Timestamp Disclosure - Unix	Low	10
X-Content-Type-Options Header Missing	Low	27
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	18
Re-examine Cache-control Directives	Informational	11
Retrieved from Cache	Informational	30
Session Management Response Identified	Informational	22

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/1
Method	GET

Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other	The directive(s): frame-ancestors, form-action is/are among the directives that do not

Info	fallback to default-src.
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	22
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: Wildcard Directive**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.

Evidence	cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/13

Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com

	https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET

Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
Instances	22
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: script-src unsafe-eval**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on

	that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.

URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net

Evidence	https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-eval.
Instances	22

Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com

	https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/3
Method	GET

Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';

Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	script-src includes unsafe-inline.
Instances	22
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.

URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.

Evidence	cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/7

Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com

	https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://fonts.googleapis.com; font-src 'self' https://cdnjs.cloudflare.com https://fonts.gstatic.com; img-src 'self' data: https:; connect-src 'self';
Other Info	style-src includes unsafe-inline.
Instances	22
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	[693](693)
WASC Id	15
Plugin Id	[10055](10055)

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer Scripting (XSS) and data injection attacks. These attacks are used for everything from data thef CSP provides a set of standard HTTP headers that allow website owners to declare approved s allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, image ActiveX, audio and video files.
URL	http://edge.microsoft.com/browsernetworktime/time/1/current?cup2key=2:b6cJvuCodGdc7GF_4RhBmovfeB9BgEpzu373S72haPI&cup2hreq=e3b0c44298fc1c149afbf4c8
Method	GET

Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Cont
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css
Method	GET
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js

Method	GET
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Method	GET
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=mfcdm-origins-list&bucket=main&_expected=0
Method	GET
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	7
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Low	Big Redirect Detected (Potential Sensitive Information Leak)
Description	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 27 [http://127.0.0.1:8000/login]. Predicted response size: 327. Response Body Length: 354.
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 30 [http://127.0.0.1:8000/register]. Predicted response size: 330. Response Body Length: 366.
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 30 [http://127.0.0.1:8000/register]. Predicted response size: 330. Response Body Length: 366.
Instances	3
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other	

Info	
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/3

Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET

Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _C_Auth
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: MUID
Other Info	
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	23
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004

WASC Id	13
Plugin Id	10010

Low	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _C_Auth
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _EDGE_S
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _EDGE_V
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: MUIDB
Other Info	
Instances	4
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cookie with SameSite Attribute None**
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://copilot.microsoft.com/c/api/user/eligibility

Method	GET
Attack	
Evidence	Set-Cookie: MUID
Other Info	
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _C_Auth
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _C_ETH
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _EDGE_S
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: _EDGE_V
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: MUIDB
Other	

Info	
Instances	5
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/11

Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other	

Info	
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
Instances	18
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	

CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	

URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/7
Method	GET

Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	

Evidence	X-Powered-By: PHP/8.4.14
Other Info	
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.4.14
Other Info	
Instances	22
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10037

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2025-12-18-09-14-51.chain
Method	GET
Attack	
Evidence	AmazonS3
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2025-12-18-09-14-51.chain
Method	GET
Attack	

Evidence	
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/a66d82fe-d400-401d-a950-5bd20efea1f7
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/c3d257f6-ff88-4ba3-ba4a-6b55611db0b8
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/d02cc572-8a59-4b0b-b04b-ff196ad7aa69
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e340b04e-37c1-4917-b1bd-0012bb9f385e
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e8a9706c-8f9e-45f8-8117-809b038fbd35
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f06715b2-b762-430c-ab6b-075d215700aa
Method	GET

Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f572130f-3b65-45d6-8cb9-64d549ee2188
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3
Method	POST
Attack	
Evidence	
Other Info	
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3
Method	POST
Attack	
Evidence	
Other Info	
URL	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
Method	POST
Attack	
Evidence	
Other Info	
URL	https://telem-edge.smartscreen.microsoft.com/api/browser/edge/telemetry/3
Method	POST
Attack	
Evidence	
Other Info	
Instances	14
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	1762786937
Other Info	1762786937, which evaluates to: 2025-11-10 23:02:17.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/a66d82fe-d400-401d-a950-5bd20efea1f7
Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/c3d257f6-ff88-4ba3-ba4a-6b55611db0b8
Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/d02cc572-8a59-4b0b-b04b-ff196ad7aa69
Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e340b04e-37c1-4917-b1bd-0012bb9f385e
Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e8a9706c-8f9e-45f8-8117-809b038fbd35

Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f06715b2-b762-430c-ab6b-075d215700aa
Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f572130f-3b65-45d6-8cb9-64d549ee2188
Method	GET
Attack	
Evidence	1758071408
Other Info	1758071408, which evaluates to: 2025-09-17 09:10:08.
URL	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json
Method	GET
Attack	
Evidence	1762786937
Other Info	1762786937, which evaluates to: 2025-11-10 23:02:17.
URL	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json
Method	GET
Attack	
Evidence	1762786940
Other Info	1762786940, which evaluates to: 2025-11-10 23:02:20.
Instances	10
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
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 MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://127.0.0.1:8000/images/community_photo.jpg

Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/events/coastal_cleanup.jpg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/events/computer.png
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/events/feeding-program.png
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/events/reforestation.jpg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/Onehelp-white-logo.svg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg-11-logo.svg
Method	GET

Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg-16-logo.svg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg-17-logo.svg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg-2-logo.svg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg-3-logo.svg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg-4-logo.svg
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/images/sdg_logo.svg
Method	GET

Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2025-12-18-09-14-51.chain
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/a66d82fe-d400-401d-a950-5bd20efea1f7
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/c3d257f6-ff88-4ba3-ba4a-6b55611db0b8
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists

URL	/d02cc572-8a59-4b0b-b04b-ff196ad7aa69
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e340b04e-37c1-4917-b1bd-0012bb9f385e
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e8a9706c-8f9e-45f8-8117-809b038fbd35
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f06715b2-b762-430c-ab6b-075d215700aa
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f572130f-3b65-45d6-8cb9-64d549ee2188
Method	GET
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json
Method	GET
Attack	
Evidence	
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 concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3
Method	POST
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3
Method	POST
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
Method	POST
Attack	
Evidence	
Other Info	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 concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	27
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 web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Authentication Request Identified**
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 fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=http://127.0.0.1:8000/login csrfToken=_token

Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper.js.org")");let t=this._element;"parent"===this._config.reference?t=this._parent:o(this._config.reference)?t=r(this._conf", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	<a class="page-link" href="#" tabindex="-1">Previous</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> <

Evidence	/a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/7
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/login
Method	GET

Attack	
Evidence	<a href="#" style="color: #2C7A6E; font-weight: 600; text-decoration: none;">Forgot your password?</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	<a href="#" class="social-icon" aria-label="Facebook"> <i class="fab fa-facebook-f"></i> </a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	18
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/a66d82fe-d400-401d-a950-5bd20efea1f7
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/c3d257f6-ff88-4ba3-ba4a-6b55611db0b8
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/d02cc572-8a59-4b0b-b04b-ff196ad7aa69
Method	GET

Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e340b04e-37c1-4917-b1bd-0012bb9f385e
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e8a9706c-8f9e-45f8-8117-809b038fbd35
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f06715b2-b762-430c-ab6b-075d215700aa
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f572130f-3b65-45d6-8cb9-64d549ee2188
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Method	GET
Attack	
Evidence	max-age=3600
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=mfcdm-origins-list&bucket=main&_expected=0
Method	GET
Attack	
Evidence	max-age=3600
Other Info	
URL	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json

Method	GET
Attack	
Evidence	
Other Info	
Instances	11
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	Retrieved from Cache
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/a66d82fe-d400-401d-a950-5bd20efea1f7
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/c3d257f6-ff88-4ba3-ba4a-6b55611db0b8
Method	GET
Attack	
Evidence	HIT

Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/d02cc572-8a59-4b0b-b04b-ff196ad7aa69
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e340b04e-37c1-4917-b1bd-0012bb9f385e
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/e8a9706c-8f9e-45f8-8117-809b038fbd35
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f06715b2-b762-430c-ab6b-075d215700aa
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/f572130f-3b65-45d6-8cb9-64d549ee2188
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000638
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	

Evidence	Age: 1000641
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000643
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000645
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000650
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000652
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000659
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 1000662
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988285

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988294
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988302
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988312
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988320
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988332
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988367
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988387
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988430
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 988435
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2025-12-18-09-14-51.chain
Method	GET
Attack	
Evidence	Age: 706
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Method	GET
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=mfcdm-origins-list&bucket=main&_expected=0
Method	GET
Attack	
Evidence	Age: 0
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	30
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html

CWE Id	525
WASC Id	
Plugin Id	10050

Informational	Session Management Response Identified
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 in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/about
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/1
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/10
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/11
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN

URL	http://127.0.0.1:8000/events/12
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/13
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/2
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/3
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/4
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/5
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/6
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/7

Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/8
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/events/9
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/register
Method	GET
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	MUIDB
Other Info	cookie:MUIDB cookie:MUID cookie:_EDGE_S
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/register/organization
Method	POST
Attack	

Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/register/volunteer
Method	POST
Attack	
Evidence	laravel-session
Other Info	cookie:laravel-session cookie:XSRF-TOKEN
Instances	22
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112