



# ZAP Scanning Report

**Site:** <http://localhost>

**Generated on** **Tue, 11 Nov 2025 21:59:35**

**ZAP Version:** 2.16.1

**ZAP by** [Checkmarx](#)

## Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	7
Low	4
Informational	6
False Positives:	0

## Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

## Alerts

Name	Risk Level	Number of Instances
<a href="#">CSP: Failure to Define Directive with No Fallback</a>	Medium	6
<a href="#">CSP: Wildcard Directive</a>	Medium	6
<a href="#">CSP: script-src unsafe-inline</a>	Medium	6
<a href="#">CSP: style-src unsafe-inline</a>	Medium	6
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	2
<a href="#">Directory Browsing</a>	Medium	1
<a href="#">Hidden File Found</a>	Medium	2
<a href="#">Big Redirect Detected (Potential Sensitive Information Leak)</a>	Low	1
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	8
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	6

<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	9
<a href="#">Authentication Request Identified</a>	Informational	1
<a href="#">GET for POST</a>	Informational	2
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	2
<a href="#">Session Management Response Identified</a>	Informational	2
<a href="#">User Agent Fuzzer</a>	Informational	48
<a href="#">User Controllable HTML Element Attribute (Potential XSS)</a>	Informational	8

## 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	<a href="http://localhost/SYSTEMINTEG/">http://localhost/SYSTEMINTEG/</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	<a href="http://localhost/SYSTEMINTEG/index.php">http://localhost/SYSTEMINTEG/index.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	



Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	<a href="http://localhost/SYSTEMINTEGRATION/views/register.php">http://localhost/SYSTEMINTEGRATION/views/register.php</a>
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://web.dev/articles/csp#resource-options">https://web.dev/articles/csp#resource-options</a>
CWE Id	<a href="https://cwe.mitre.org/cgi-bin/cwe.cgi?cwe=693">693</a>
WASC Id	15
Plugin Id	<a href="https://www.pluginid.com/plugin/10055">10055</a>

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	<a href="http://localhost/SYSTEMINTEGRATION/">http://localhost/SYSTEMINTEGRATION/</a>

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	<a href="http://localhost/SYSTEMINTEGRITY/index.php">http://localhost/SYSTEMINTEGRITY/index.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	<a href="http://localhost/SYSTEMINTEGRITY/views/login.php">http://localhost/SYSTEMINTEGRITY/views/login.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Content-Security-Policy
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://web.dev/articles/csp#resource-options">https://web.dev/articles/csp#resource-options</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>

Medium	<b>CSP: script-src unsafe-inline</b>
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	<a href="http://localhost/SYSTEMINTEGRITY/">http://localhost/SYSTEMINTEGRITY/</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	<a href="http://localhost/SYSTEMINTEGRITY/index.php">http://localhost/SYSTEMINTEGRITY/index.php</a>

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.

URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	script-src includes unsafe-inline.
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://web.dev/articles/csp#resource-options">https://web.dev/articles/csp#resource-options</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>

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	<a href="http://localhost/SYSTEMINTEG/">http://localhost/SYSTEMINTEG/</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
URL	<a href="http://localhost/SYSTEMINTEG/index.php">http://localhost/SYSTEMINTEG/index.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	GET
Parameter	Content-Security-Policy
Attack	



Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; img-src 'self' data: https: https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; font-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; connect-src 'self' https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://oauth2.googleapis.com https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-src 'self' https://accounts.google.com https://apis.google.com https://*.gstatic.com https://*.google.com; frame-ancestors 'self';
Other Info	style-src includes unsafe-inline.
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://web.dev/articles/csp#resource-options">https://web.dev/articles/csp#resource-options</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>

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 certain types of attacks, including 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	<a href="http://localhost/robots.txt">http://localhost/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost/sitemap.xml">http://localhost/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	2

Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP">https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a> <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a> <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>

Medium	Directory Browsing
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
URL	<a href="http://localhost/SYSTEMINTEG/views/">http://localhost/SYSTEMINTEG/views/</a>
Method	GET
Parameter	
Attack	http://localhost/SYSTEMINTEG/views/
Evidence	Parent Directory
Other Info	
Instances	1
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	<a href="https://httpd.apache.org/docs/current/mod/core.html#options">https://httpd.apache.org/docs/current/mod/core.html#options</a>
CWE Id	<a href="#">548</a>
WASC Id	48
Plugin Id	<a href="#">0</a>

Medium	Hidden File Found
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	<a href="http://localhost/server-info">http://localhost/server-info</a>
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	apache_server_info
URL	<a href="http://localhost/server-status">http://localhost/server-status</a>
Method	GET
Parameter	

Attack	
Evidence	HTTP/1.1 200 OK
Other Info	apache_server_status
Instances	2
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	<a href="https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html">https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html</a> <a href="https://httpd.apache.org/docs/current/mod/mod_status.html">https://httpd.apache.org/docs/current/mod/mod_status.html</a>
CWE Id	<a href="#">538</a>
WASC Id	13
Plugin Id	<a href="#">40035</a>

<b>Low</b>	<b>Big Redirect Detected (Potential Sensitive Information Leak)</b>
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	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 29 [http://localhost/SYSTEMINTEG/]. Predicted response size: 329. Response Body Length: 336.
Instances	1
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	<a href="#">201</a>
WASC Id	13
Plugin Id	<a href="#">10044</a>

<b>Low</b>	<b>Cross-Domain JavaScript Source File Inclusion</b>
Description	The page includes one or more script files from a third-party domain.
URL	<a href="http://localhost/SYSTEMINTEG/">http://localhost/SYSTEMINTEG/</a>
Method	GET
Parameter	<a href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js">https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js</a>
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	

URL	<a href="http://localhost/SYSTEMINTEG/index.php">http://localhost/SYSTEMINTEG/index.php</a>
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	GET
Parameter	https://accounts.google.com/gsi/client
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client" async defer></script>
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	https://accounts.google.com/gsi/client
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client" async defer></script>
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js
Attack	

Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
URL	<a href="http://localhost/SYSTEMINTEGRATION/views/register.php">http://localhost/SYSTEMINTEGRATION/views/register.php</a>
Method	POST
Parameter	https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js"></script>
Other Info	
Instances	8
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	<a href="#">829</a>
WASC Id	15
Plugin Id	<a href="#">10017</a>

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	<a href="http://localhost/SYSTEMINTEGRATION/">http://localhost/SYSTEMINTEGRATION/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEGRATION/index.php">http://localhost/SYSTEMINTEGRATION/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEGRATION/views/login.php">http://localhost/SYSTEMINTEGRATION/views/login.php</a>
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a> <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10037</a>

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	<a href="http://localhost/robots.txt">http://localhost/robots.txt</a>
Method	GET
Parameter	
Attack	

Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/sitemap.xml">http://localhost/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/">http://localhost/SYSTEMINTEG/</a>
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/index.php">http://localhost/SYSTEMINTEG/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	

Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	<a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a> <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)</a> <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10036</a>

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	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	username
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=http://localhost/SYSTEMINTEG/views/login.php csrfToken=csrf_token
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/</a>
CWE Id	

WASC Id	
Plugin Id	<a href="#">10111</a>

Informational	GET for POST
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	GET <a href="http://localhost/SYSTEMINTEG/views/login.php?csrf_token=201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44&amp;password=ZAP&amp;username=ZAP">http://localhost/SYSTEMINTEG/views/login.php?csrf_token=201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44&amp;password=ZAP&amp;username=ZAP</a> HTTP/1.1
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	
Attack	
Evidence	GET <a href="http://localhost/SYSTEMINTEG/views/register.php?address=688%20Zaproxy%20Ridge&amp;clinic_address=&amp;clinic_name=ZAP&amp;confirm_password=ZAP&amp;csrf_token=201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44&amp;date_of_birth=2025-11-11&amp;email=zaproxy@example.com&amp;full_name=ZAP&amp;gender=Male&amp;home_address=&amp;medical_license=ZAP&amp;password=ZAP&amp;phone=9999999999&amp;profile_photo=test_file.txt&amp;role=patient&amp;specialization=General%20Medicine&amp;username=ZAP">http://localhost/SYSTEMINTEG/views/register.php?address=688%20Zaproxy%20Ridge&amp;clinic_address=&amp;clinic_name=ZAP&amp;confirm_password=ZAP&amp;csrf_token=201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44&amp;date_of_birth=2025-11-11&amp;email=zaproxy@example.com&amp;full_name=ZAP&amp;gender=Male&amp;home_address=&amp;medical_license=ZAP&amp;password=ZAP&amp;phone=9999999999&amp;profile_photo=test_file.txt&amp;role=patient&amp;specialization=General%20Medicine&amp;username=ZAP</a> HTTP/1.1
Other Info	
Instances	2
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	<a href="#">16</a>
WASC Id	20
Plugin Id	<a href="#">10058</a>

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	GET
Parameter	
Attack	
Evidence	Admin

Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "<!-- Clinic Admin Specific Fields -->", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	
Attack	
Evidence	Admin
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "<!-- Clinic Admin Specific Fields -->", see evidence field for the suspicious comment/snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<a href="#">615</a>
WASC Id	13
Plugin Id	<a href="#">10027</a>

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	<a href="http://localhost/SYSTEMINTEG/">http://localhost/SYSTEMINTEG/</a>
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	PHPSESSID
Other Info	cookie:PHPSESSID
URL	<a href="http://localhost/SYSTEMINTEG/">http://localhost/SYSTEMINTEG/</a>
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	PHPSESSID
Other Info	cookie:PHPSESSID
Instances	2
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10112</a>

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	

URL	<a href="http://localhost/SYSTEMINTEG">http://localhost/SYSTEMINTEG</a>
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	

Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views">http://localhost/SYSTEMINTEG/views</a>
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	

URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	48
Solution	
Reference	<a href="https://owasp.org/wstg">https://owasp.org/wstg</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10104</a>

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>
Method	POST
Parameter	csrf_token
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: <a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was: csrf_token=201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44 The user-controlled value was: 201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44
URL	<a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a>

Method	POST
Parameter	csrf_token
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/login.php">http://localhost/SYSTEMINTEG/views/login.php</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was:    csrf_token=71fb7e80f63cbc0e5d24c23d7a9bae75fdb81cf6d4d53e8c05c220a67bed9e3c The user-controlled value was:    71fb7e80f63cbc0e5d24c23d7a9bae75fdb81cf6d4d53e8c05c220a67bed9e3c</p>
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	csrf_token
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was:    csrf_token=201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44 The user-controlled value was:    201f1cbdf9c692c7ad8405010f9be067b3f6e04f93e10eb4768aab0525a01b44</p>
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	csrf_token
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was:    csrf_token=71fb7e80f63cbc0e5d24c23d7a9bae75fdb81cf6d4d53e8c05c220a67bed9e3c The user-controlled value was:    71fb7e80f63cbc0e5d24c23d7a9bae75fdb81cf6d4d53e8c05c220a67bed9e3c</p>
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	gender
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a> appears to include user input in: a(n) [option] tag [value] attribute The user input found was: gender=Male The user-controlled value was: male</p>

URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	role
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a> appears to include user input in: a(n) [div] tag [id] attribute The user input found was: role=patient The user-controlled value was: patientfields</p>
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	role
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a> appears to include user input in: a(n) [option] tag [value] attribute The user input found was: role=patient The user-controlled value was: patient</p>
URL	<a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a>
Method	POST
Parameter	specialization
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:  <a href="http://localhost/SYSTEMINTEG/views/register.php">http://localhost/SYSTEMINTEG/views/register.php</a> appears to include user input in: a(n) [option] tag [value] attribute The user input found was: specialization=General Medicine The user-controlled value was: general medicine</p>
Instances	8
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a>
CWE Id	<a href="#">20</a>
WASC Id	20
Plugin Id	<a href="#">10031</a>

## Sequence Details

With the associated active scan results.