Course Alert Report

Site: http://localhost:8884

Generated on Sat, 30 Mar 2024 11:57:48

ZAP Version: 2.14.0

ZAP is supported by the [Crash Override Open Source Fellowship]()

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	0
Low	5
Informational	2
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
SQL Injection	High	2
Application Error Disclosure	Low	4
Cross Site Scripting Weakness (Persistent in JSON Response)	Low	6
Private IP Disclosure	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	8
X-Content-Type-Options Header Missing	Low	4
Information Disclosure - Suspicious Comments	Informational	1
User Agent Fuzzer	Informational	72

Alert Detail

High	SQL Injection
Description	SQL injection may be possible.
URL	http://localhost:8884/27
Method	GET
Attack	*/* AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [*/* AND 1=1 --] and [*/* AND 1=2 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter

URL	http://localhost:8884/27
Method	GET
Attack	0b4619da-3cd3-4fbc-9040-fc350ba4f92f AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [0b4619da-3cd3-4fbc-9040-fc350ba4f92f AND 1=1 --] and [0b4619da-3cd3-4fbc-9040-fc350ba4f92f AND 1=2 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter
Instances	2
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Low	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://localhost:8884/create
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8884/favicon.ico

Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8884/robots.txt
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8884/sitemap.xml
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
Instances	4
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	90022

Low	**Cross Site Scripting Weakness (Persistent in JSON Response)**
Description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (response).
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	<script>alert(1);</script>
Evidence	

Other Info	Raised with LOW confidence as the Content-Type is not HTML
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML
Instances	6
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

	Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40014

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://localhost:8884
Method	GET
Attack	
Evidence	10.0.0.1
	10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5

Other Info	10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790
URL	http://localhost:8884/
Method	GET
Attack	
Evidence	10.0.0.1
	10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5

Other Info	10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	
Evidence	192.168.1.17:51790
	192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790

Other Info	192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 192.168.1.17:51790 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
Instances	3
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

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://localhost:8884
Method	GET
Attack	
Evidence	X-Powered-By: Express

Other Info	
URL	http://localhost:8884/
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8884/28
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8884/7
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8884/create
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8884/favicon.ico
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8884/robots.txt
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8884/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	

Instances	8
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/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

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://localhost:8884
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://localhost:8884/
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://localhost:8884/28
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://localhost:8884/7
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.
Instances	4

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	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 12 times, the first in the element starting with: "<!--","rating":3,"total_enrollments":5,"status":1,"created_at":"2024-03-30T11:52:59.000Z","updated_at":"2024-03-30T11:52:59.000Z", 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	200
WASC Id	13
Plugin Id	10027

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	http://localhost:8884/28
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8884/28
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:8884/28

Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8884/28
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:8884/28
Method	DELETE
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	http://localhost:8884/28
Method	DELETE
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	http://localhost:8884/28
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8884/28
Method	DELETE
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8884/28
Method	DELETE
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:8884/28
Method	DELETE

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	http://localhost:8884/28
Method	DELETE
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	http://localhost:8884/28
Method	DELETE
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET

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	http://localhost:8884
Method	GET
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	http://localhost:8884
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:8884
Method	GET
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	http://localhost:8884
Method	GET
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	http://localhost:8884
Method	GET

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
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	http://localhost:8884/27
Method	GET
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	http://localhost:8884/27
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	GET
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	http://localhost:8884/27
Method	GET
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	http://localhost:8884/27
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
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	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
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	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
Other Info	
URL	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
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	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
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	http://localhost:8884/?order_by=id&sort=DESC
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://localhost:8884/create
Method	POST
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	http://localhost:8884/create
Method	POST
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	http://localhost:8884/create
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:8884/create
Method	POST
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	http://localhost:8884/create
Method	POST
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	http://localhost:8884/create
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
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	http://localhost:8884/27
Method	PUT
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	http://localhost:8884/27
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:8884/27
Method	PUT
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	http://localhost:8884/27
Method	PUT
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	http://localhost:8884/27
Method	PUT
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	72
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	

Plugin Id	10104