

my findings

Site: https://bwapp.hakhub.net

Generated on Sat, 19 Apr 2025 18:18:50

ZAP Version: 2.16.1

ZAP by Checkmarx

## **Summary of Alerts**

Risk Level	Number of Alerts
High	1
Medium	7
Low	7
Informational	10

## Alerts

Name	Risk Level	Number of Instances
SQL Injection - SQLite	High	1
Absence of Anti-CSRF Tokens	Medium	6
Application Error Disclosure	Medium	45
Content Security Policy (CSP) Header Not Set	Medium	58
Directory Browsing	Medium	51
Hidden File Found	Medium	1
Missing Anti-clickjacking Header	Medium	55
Vulnerable JS Library	Medium	1
Cookie No HttpOnly Flag	Low	3
Cookie Without Secure Flag	Low	3
Cookie without SameSite Attribute	Low	3
Private IP Disclosure	Low	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	12
Timestamp Disclosure - Unix	Low	1
X-Content-Type-Options Header Missing	Low	102
Authentication Request Identified	Informational	11
Content-Type Header Missing	Informational	1
GET for POST	Informational	4
Information Disclosure - Sensitive Information in URL	Informational	3

Information Disclosure - Suspicious Comments	Informational	3
Modern Web Application	Informational	1
Re-examine Cache-control Directives	Informational	53
Session Management Response Identified	Informational	11
User Agent Fuzzer	Informational	48
<u>User Controllable HTML Element Attribute</u> ( <u>Potential XSS</u> )	Informational	4

## **Alert Detail**

Description  SQL injection may be possible.  https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password_ZAP&password_conf=ZAP&secret=ZAP  Method  GET  Attack  case randomblob(1000000) when not null then 1 else 1 end  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  Instances  1  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!	High	SQL Injection - SQLite
Method  GET  Attack  Case randomblob(1000000) when not null then 1 else 1 end  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  Instances  1  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!	Description	SQL injection may be possible.
Attack  case randomblob(1000000) when not null then 1 else 1 end  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000)] when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  Instances  1  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!	URL	
The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  Instances  1  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!	Method	GET
Pridence  Intervalue [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  Instances  1  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!	Attack	case randomblob(1000000) when not null then 1 else 1 end
Other Info  null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took [1,314] milliseconds.  Instances  1  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!	Evidence	null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took
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!		null then 1 else 1 end ], which caused the request to take [714] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [814] milliseconds, when the original unmodified query with value [ZAP] took
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!	Instances	1
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.	Solution	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.
Reference https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.	Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL Injection Prevention Cheat Sheet.

CWE Id	89
WASC Id	19
Plugin Id	40024
Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form.  A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.  CSRF attacks are effective in a number of situations, including:  * The victim has an active session on the target site.  * The victim is authenticated via HTTP auth on the target site.  CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://bwapp.hakhub.net
Method	GET
Attack	
Evidence	<form action="/login.php" method="POST"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "login" "password" ].
URL	https://bwapp.hakhub.net/login.php
Method	GET
Attack	
Evidence	<form action="/login.php" method="POST"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "login" "password" ].
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	<form action="/user_new.php" method="POST"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "email" "login" "mail_activation" "password" "password_conf" "secret" ].
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP

Method	GET
Attack	
Evidence	<form action="/user_new.php" method="POST"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "email" "login" "mail_activation" "password" "password_conf" "secret" ].
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	<form action="/login.php" method="POST"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "login" "password" ].
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	<form action="/user_new.php" method="POST"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "email" "login" "mail_activation" "password" "password_conf" "secret" ].
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.  For example, use anti-CSRF packages such as the OWASP CSRFGuard.  Phase: Implementation  Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.  Phase: Architecture and Design  Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).  Note that this can be bypassed using XSS.  Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.  Note that this can be bypassed using XSS.  Use the ESAPI Session Management control.  This control includes a component for CSRF.  Do not use the GET method for any request that triggers a state change.  Phase: Implementation

	Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross- Site Request Forgery Prevention Cheat Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	<u>352</u>
WASC Id	9
Plugin Id	10202

Plugin Id	10202
Medium	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	https://bwapp.hakhub.net/documents/
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=A

Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=S;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=S;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=D;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=D;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=A
Method	GET
Attack	

Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=D;O=A
Method	GET
Attack	
Evidence	Parent Directory

Other	
Info	
URL	https://bwapp.hakhub.net/js/?C=D;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=M;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=M;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=N;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=N;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=S;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/?C=S;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	

URL	https://bwapp.hakhub.net/passwords/
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=D;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=D;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=A
Method	GET

Attack	
Evidence	Parent Directory
Other	Parent Directory
Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=D
URL Method	https://bwapp.hakhub.net/stylesheets/?C=D;O=D  GET
Method	
Method Attack	GET
Method Attack Evidence Other	GET
Method Attack Evidence Other Info	Parent Directory
Method Attack Evidence Other Info URL	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A
Method Attack Evidence Other Info URL Method	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A
Method Attack Evidence Other Info URL Method Attack	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A  GET
Method Attack Evidence Other Info URL Method Attack Evidence Other	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A  GET
Method Attack Evidence Other Info URL Method Attack Evidence Other Info	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  Parent Directory
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A  GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=D
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL Method	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A  GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=D
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack Attack	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=D GET
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M;O=D GET
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M:O=A GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M:O=D GET  Parent Directory
Method Attack Evidence Other Info URL Method Attack URL URL Method Attack URL URL URL	Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M:O=A GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M:O=D GET  Parent Directory  https://bwapp.hakhub.net/stylesheets/?C=M:O=D GET

Evidence	Parent Directory
Other	T drone Birectory
Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
Instances	45
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	<u>550</u>
WASC Id	13
Plugin Id	90022
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	https://bwapp.hakhub.net
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/admin/
URL Method	https://bwapp.hakhub.net/admin/ GET

Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=D
Method	GET
Attack	
Evidence	
Other	

Info  URL  https://bwapp.hakhub.net/documents/?C=S:O=A  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/documents/?C=S:O=D  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/icons  Method  GET
Attack Evidence Other Info  URL https://bwapp.hakhub.net/documents/?C=S:O=D  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/icons
Evidence Other Info  URL https://bwapp.hakhub.net/documents/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/icons
Other Info  URL https://bwapp.hakhub.net/documents/?C=S:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/ioons
Info  URL https://bwapp.hakhub.net/documents/?C=S;O=D  Method GET  Attack Evidence  Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence  Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Evidence Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/icons
Other Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/icons
Info  URL https://bwapp.hakhub.net/DTD/xhtml1-transitional.dtd  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Evidence  Other Info  URL https://bwapp.hakhub.net/icons
Other Info  URL https://bwapp.hakhub.net/icons
URL <a href="https://bwapp.hakhub.net/icons">https://bwapp.hakhub.net/icons</a>
Method GET
Attack
Evidence
Other Info
URL <a href="https://bwapp.hakhub.net/images/">https://bwapp.hakhub.net/images/</a>
Method GET
Attack
Evidence
Other Info
URL <a href="https://bwapp.hakhub.net/images/?C=D;O=A">https://bwapp.hakhub.net/images/?C=D;O=A</a>
Method GET
Attack
Evidence
Other Info
URL <a href="https://bwapp.hakhub.net/images/?C=D;O=D">https://bwapp.hakhub.net/images/?C=D;O=D</a>
Method GET
Attack
Evidence
Other Info
URL <a href="https://bwapp.hakhub.net/images/?C=M;O=A">https://bwapp.hakhub.net/images/?C=M;O=A</a>

Madhada	OFT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/info.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/
Method	GET

Attack	
Evidence	
Other	
Info	
URL	https://bwapp.hakhub.net/js/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=M;O=A
Method	GET
Attack	
Evidence	
Other	
Info	
URL	https://bwapp.hakhub.net/js/?C=M;O=D
	https://bwapp.hakhub.net/js/?C=M;O=D GET
URL Method Attack	
URL Method Attack Evidence	
URL Method Attack	
URL Method Attack Evidence Other	
URL Method Attack Evidence Other Info	GET
URL  Method  Attack  Evidence  Other Info  URL	GET  https://bwapp.hakhub.net/js/?C=N;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence	GET  https://bwapp.hakhub.net/js/?C=N;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	GET  https://bwapp.hakhub.net/js/?C=N;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	GET  https://bwapp.hakhub.net/js/?C=N;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/js/?C=N;O=A GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  URL  Method  Attack  URL  URL  URL  URL  URL  URL  URL	https://bwapp.hakhub.net/js/?C=N;O=A GET  https://bwapp.hakhub.net/js/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence	https://bwapp.hakhub.net/js/?C=N;O=A GET  https://bwapp.hakhub.net/js/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Attack  Evidence  Other Info  URL  Method  Attack	https://bwapp.hakhub.net/js/?C=N;O=A GET  https://bwapp.hakhub.net/js/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL	https://bwapp.hakhub.net/js/?C=N;O=A GET  https://bwapp.hakhub.net/js/?C=N;O=D
URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/js/?C=N:O=A GET  https://bwapp.hakhub.net/js/?C=N:O=D GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  URL  URL  URL  URL  URL  URL  UR	https://bwapp.hakhub.net/js/?C=N:O=A GET  https://bwapp.hakhub.net/js/?C=N:O=D GET  https://bwapp.hakhub.net/js/?C=S:O=A

Other	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	

URL	https://bwapp.hakhub.net/passwords/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=A
Method	GET

Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
IIIIO	
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=A
	https://bwapp.hakhub.net/stylesheets/?C=N;O=A  GET
URL	
URL Method	
URL Method Attack	
URL Method Attack Evidence Other	
URL Method Attack Evidence Other Info	GET
URL  Method  Attack  Evidence  Other Info  URL	GET  https://bwapp.hakhub.net/stylesheets/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method	GET  https://bwapp.hakhub.net/stylesheets/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	GET  https://bwapp.hakhub.net/stylesheets/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	GET  https://bwapp.hakhub.net/stylesheets/?C=N;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=N;O=D  GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  URL  URL  URL  URL  URL  UR	https://bwapp.hakhub.net/stylesheets/?C=N;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=S;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  Method  Method  Attack  Evidence  Other Info  URL  Method	https://bwapp.hakhub.net/stylesheets/?C=N;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=S;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	https://bwapp.hakhub.net/stylesheets/?C=N;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=S;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Other Info  URL  Method  Attack  Evidence  Other	https://bwapp.hakhub.net/stylesheets/?C=N;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=S;O=A
URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=N:O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=S:O=A  GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  URL  URL  URL  URL	https://bwapp.hakhub.net/stylesheets/?C=N:O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=S:O=A  GET  https://bwapp.hakhub.net/stylesheets/?C=S:O=D

Evidence	
Other Info	
URL	https://bwapp.hakhub.net/training.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	
Other Info	
Instances	58
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP /Introducing Content Security Policy https://cheatsheetseries.owasp.org/cheatsheets/Content Security Policy Cheat Sheet.html  https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	<u>693</u>
WASC Id	15

Plugin Id	<u>10038</u>
Medium	Directory Browsing
Description	It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.
URL	https://bwapp.hakhub.net/documents/
Method	GET
Attack	https://bwapp.hakhub.net/documents/
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/fonts/
Method	GET
Attack	https://bwapp.hakhub.net/fonts/
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/images/
Method	GET
Attack	https://bwapp.hakhub.net/images/
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/js/
Method	GET
Attack	https://bwapp.hakhub.net/js/
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/passwords/
Method	GET
Attack	https://bwapp.hakhub.net/passwords/
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	https://bwapp.hakhub.net/stylesheets/
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/documents/
Method	GET
Attack	

Evidence	<title>Index of /documents</title>
Other	
Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=D;O=A
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=D;O=D
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=M;O=A
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=M;O=D
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=N;O=A
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=N;O=D
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=S;O=A
Method	GET
Attack	
Evidence	<title>Index of /documents</title>

Othern	Waltana and dan Chada Annala O
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/documents/?C=S;O=D
Method	GET
Attack	
Evidence	<title>Index of /documents</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/images/
Method	GET
Attack	
Evidence	<title>Index of /images</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/images/?C=D;O=A
Method	GET
Attack	
Evidence	<title>Index of /images</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/images/?C=D;O=D
Method	GET
Attack	
Evidence	<title>Index of /images</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/images/?C=M;O=A
Method	GET
Attack	
Evidence	<title>Index of /images</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/images/?C=M;O=D
Method	GET
Attack	
Evidence	<title>Index of /images</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/images/?C=N;O=A
Method	GET
Attack	
Evidence	<title>Index of /images</title>
Other Info	Web server identified: Apache 2

Attack Evidence other Info Web server identified: Apache 2 Hittps://bwapp.hakhub.net/images/7C=S.O=A Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/images/7C=S.O=D Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/images/7C=S.O=D Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/is/ Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/  Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/ Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=D.O=A Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=D.O=A Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=D.O=D Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=D.O=D  Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=D.O=D  Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=D.O=D  Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=M.O=A  Method GET Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=M.O=A  Method GET  Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=M.O=A  Method GET  Attack Evidence other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/s/7C=M.O=D  Method GET	URL	https://bwapp.hakhub.net/images/?C=N;O=D
Evidence <title>index of /images</title> Other info Other info Other info Other info Other info URL https://bwapp.hakhub.net/images/7C=S.O=A  Method GET Attack Evidence <title>index of /images</title> Other info Web server identified: Apache 2 IURL https://bwapp.hakhub.net/images/7C=S.O=D  Method GET Attack Evidence <title>info Other info Web server identified: Apache 2 IURL https://bwapp.hakhub.net/is/S Other info Other info Web server identified: Apache 2 IURL https://bwapp.hakhub.net/js/ Method GET  Attack Evidence &lt;title&gt;info Other info Other info Other info Web server identified: Apache 2 IURL https://bwapp.hakhub.net/js/C=D.O=A  Method GET Attack Evidence &lt;title&gt;info Other info Web server identified: Apache 2 IURL https://bwapp.hakhub.net/js/7C=D.O=A  Method GET  Attack Evidence &lt;title&gt;info Other info Other&lt;/td&gt;&lt;td&gt;Method&lt;/td&gt;&lt;td&gt;GET&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Other Info  URL  https://bwapp.hakhub.net/images/?C=S:O=A  Method  Attack  Evidence  ctitle&gt;Index of /images</title> Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/images/?C=S:O=D  Method  GET  Attack  Evidence  ctitle>Index of /images  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/is/  Evidence  ctitle>Index of /images  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/is/  Evidence  ctitle>Index of /js  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=A  Method  GET  Attack  Evidence  ctitle>Index of /js  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  ctitle>Index of /js  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  ctitle>Index of /js  Other Info  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  ctitle>Index of /js  Other Info  Web server identified: Apache 2  Info  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence  ctitle>Index of /js  Other Info  Web server identified: Apache 2  Info  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence  ctitle>Index of /js  Other Info  Web server identified: Apache 2  Info  URL  https://bwapp.hakhub.net/js/?C=M:O=D  URL  https://bwapp.hakhub.net/js/?C=M:O=D  URL  https://bwapp.hakhub.net/js/?C=M:O=D	Attack	
Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/images/?C=S;O=A  Method GET  Attack  Evidence <title>Index of /images</title> Other Info  URL https://bwapp.hakhub.net/images/?C=S;O=D  Method GET  Attack  Evidence <title>Index of /images</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/  Method GET  Attack  Evidence <title>Index of /ijs</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/  Method GET  Attack  Evidence <title>Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=D:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=M:O=D  URL https://bwapp.hakhub.net/is/?C=M:O=D  URL https://bwapp.hakhub.net/is/?C=M:O=D&lt;/td&gt;&lt;td&gt;Evidence&lt;/td&gt;&lt;td&gt;&lt;title&gt;Index of /images</title>		
Method GET  Attack Evidence <title>Index of /images</title> Other Info  Method GET  Attack Evidence <title>Intps://bwapp.hakhub.net/images/?C=S;O=D  Method GET  Attack Evidence &lt;title&gt;Info Other Info Other Inf&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Web server identified: Apache 2&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Attack Evidence &lt;title&gt;Index of /images</title> Other Info  URL https://bwapp.hakhub.net/images/7C=S:O=D  Method GET  Attack Evidence <title>Info  Other Info  URL https://bwapp.hakhub.net/images/7C=S:O=D  Method GET  Attack Evidence &lt;title&gt;Info  Other Info  URL https://bwapp.hakhub.net/is/  Method GET  Attack Evidence &lt;title&gt;Info  Other Info  Other Info  URL https://bwapp.hakhub.net/is/  Evidence &lt;title&gt;Info  Other Info  URL https://bwapp.hakhub.net/is/?C=D:O=A  Method GET  Attack Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=D:O=A  Method GET  Attack Evidence &lt;title&gt;Info  Other Info  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack Evidence &lt;title&gt;Info  Other Info  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack Evidence &lt;title&gt;Index of /js</title> Other Info  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack Evidence <title>Info  Other Info  Web server identified: Apache 2  Info  URL https://bwapp.hakhub.net/is/?C=M:O=A  Method GET  Attack Evidence &lt;title&gt;Info  Other Info  Web server identified: Apache 2  Info  Other Info  Web server identified: Apache 2&lt;/td&gt;&lt;td&gt;URL&lt;/td&gt;&lt;td&gt;https://bwapp.hakhub.net/images/?C=S;O=A&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Evidence &lt;title&gt;Index of /images</title> Other Info  Web server identified: Apache 2  Web server identified: Apache 2  Method GET  Attack  Evidence <title>Index of /images</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/ Method GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL web server identified: Apache 2  URL https://bwapp.hakhub.net/js/7C=D:O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=D:O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=D:O=D  Method GET  Attack  Evidence <title>Info  URL https://bwapp.hakhub.net/js/7C=D:O=D  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/js/7C=D:O=D  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/js/7C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/js/7C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/js/7C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/js/7C=M:O=D  URL https://bwapp.hakhub.net/js/7C=M:O=D&lt;/td&gt;&lt;td&gt;Method&lt;/td&gt;&lt;td&gt;GET&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  Attack  Evidence  other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=D:O=A  Method  GET  Attack  Evidence  other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=D:O=D  Method  GET  Attack  Evidence  other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=M:O=A  Method  GET  Attack  Evidence  other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=M:O=A  Method  GET  Attack  Evidence  other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=M:O=A  Method  GET  Attack  Evidence  other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=M:O=D&lt;/td&gt;&lt;td&gt;Attack&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Info  Web server identified: Apache 2  URL  Attack  Evidence  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/  Method  GET  Attack  Evidence  Attack  Evidence  Attack  Evidence  Attack  Evidence  Other Info  Web server identified: Apache 2  URL  Attack  Evidence  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/7C=D:O=A  Method  GET  Attack  Evidence  Attack  Attack&lt;/td&gt;&lt;td&gt;Evidence&lt;/td&gt;&lt;td&gt;&lt;title&gt;Index of /images</title>		
Method GET  Attack  Evidence <titite>Index of /images  Other Info  URL https://bwapp.hakhub.net/js/  Method GET  Attack  Evidence <titite>index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=A  Method GET  Attack  Evidence <titite>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=A  Method GET  Attack  Evidence <titite>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=D  Method GET  Attack  Evidence <titite>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=D  Method GET  Attack  Evidence <titite>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence <titite>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M:O=D</titite></titite></titite></titite></titite></titite></titite>		Web server identified: Apache 2
Attack  Evidence <title>Index of /images</title> Other Info  URL https://bwapp.hakhub.net/is/  Method GET  Attack  Evidence <title>Info  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=D:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=D:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack  Evidence &lt;title&gt;Info  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack  Evidence &lt;title&gt;Info  Other Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=D:O=D  Method GET  Attack  Evidence &lt;title&gt;Info  Other Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Info  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/is/?C=M:O=D&lt;/td&gt;&lt;td&gt;URL&lt;/td&gt;&lt;td&gt;https://bwapp.hakhub.net/images/?C=S;O=D&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Evidence &lt;title&gt;Info Other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/ Method GET Attack Evidence &lt;title&gt;Info Web server identified: Apache 2 Other Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/?C=D:O=A Method GET Attack Evidence &lt;title&gt;Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/?C=D:O=A  Method GET Attack Evidence &lt;title&gt;Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/?C=D:O=D  Method GET Attack Evidence &lt;title&gt;Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/?C=D:O=D  Method GET Attack Evidence &lt;title&gt;Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack Evidence &lt;title&gt;Info Web server identified: Apache 2 URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET Attack Evidence &lt;title&gt;Info Web server identified: Apache 2&lt;/td&gt;&lt;td&gt;Method&lt;/td&gt;&lt;td&gt;GET&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/  Method GET  Attack  Evidence &lt;titite&gt;Index of /js&lt;/titite&gt;  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=A  Method GET  Attack  Evidence &lt;titite&gt;Index of /js&lt;/titte&gt;  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method GET  Attack  Evidence &lt;titite&gt;Index of /js&lt;/titte&gt;  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence &lt;titite&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence &lt;titite&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=D&lt;/td&gt;&lt;td&gt;Attack&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/is/  Attack  Evidence  Attile&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/is/?C=D:O=A  Method  GET  Attack  Evidence  &lt;tittle&gt;Index of /js&lt;/tittle&gt;  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/is/?C=D:O=A  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  &lt;tittle&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  &lt;tittle&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence  &lt;tittle&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence  &lt;tittle&gt;Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=D&lt;/td&gt;&lt;td&gt;Evidence&lt;/td&gt;&lt;td&gt;&lt;title&gt;Index of /images</title>		
Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=D:O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=D:O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=D:O=D  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=D:O=D  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/7C=M:O=A  Method GET  Attack  Evidence <title>Index of /js</title> URL https://bwapp.hakhub.net/js/7C=M:O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/7C=M:O=D		Web server identified: Apache 2
Attack Evidence <title>Index of /js</title> Other Info Other Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=A  Method GET Attack Evidence <title>Index of /js</title> Other Info URL https://bwapp.hakhub.net/js/?C=D:O=D  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=D  Method GET Attack Evidence <title>Index of /js</title> Other Info URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack Evidence <title>Index of /js</title> URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack Evidence <title>Info URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack Evidence &lt;title&gt;Index of /js</title> Other Info URL https://bwapp.hakhub.net/js/?C=M:O=D	URL	https://bwapp.hakhub.net/js/
Evidence <a href="https://bwapp.hakhub.net/js/?C=D:O=A"></a>	Method	GET
Other Info  URL  https://bwapp.hakhub.net/js/?C=D:O=A  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence <tititle>Index of /js</tititle> Other Info  URL  https://bwapp.hakhub.net/js/?C=D:O=D  URL  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence <tititle>Index of /js  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=D</tititle>	Attack	
Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=A  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL  Method  GET  Attack  Evidence <title>Index of /js</title> Other Info  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence <title>Index of /js</title> Other Info  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=D  URL  https://bwapp.hakhub.net/js/?C=M:O=D	Evidence	<title>Index of /js</title>
Method GET  Attack  Evidence <titile>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D;O=D  Method GET  Attack  Evidence <titile>Index of /js  Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence <titile>Index of /js  URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence <titile>Index of /js  Other Info  Web server identified: Apache 2  INTERIT ATTACK  INTERIT ATTACK  INTERIT ATTACK  Evidence <titile>Index of /js  Other Info  Web server identified: Apache 2  INTERIT ATTACK  INTERIT AND INTERIT A</titile></titile></titile></titile></titile>		Web server identified: Apache 2
Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D:O=D  Method GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence <title>Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack  Evidence &lt;title&gt;Index of /js</title> Other Info  Web server identified: Apache 2	URL	https://bwapp.hakhub.net/js/?C=D;O=A
Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=D;O=D  Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Index of /js</title> URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	Method	GET
Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=D:O=D  Method  GET  Attack  Evidence  Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence <title>Index of /js</title> URL  https://bwapp.hakhub.net/js/?C=M:O=A  Method  GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M:O=D	Attack	
URL https://bwapp.hakhub.net/js/?C=D;O=D  Method GET  Attack Evidence <title>Index of /js</title> Other Info  URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack Evidence &lt;title&gt;Index of /js</title> Other Info  Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	Evidence	<title>Index of /js</title>
Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=A		Web server identified: Apache 2
Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	URL	https://bwapp.hakhub.net/js/?C=D;O=D
Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	Method	GET
Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M;O=A  Method  GET  Attack  Evidence <title>Index of /js</title> Other Info  Web server identified: Apache 2  URL  https://bwapp.hakhub.net/js/?C=M;O=D	Attack	
URL https://bwapp.hakhub.net/js/?C=M;O=A  Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	Evidence	<title>Index of /js</title>
Method GET  Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D		Web server identified: Apache 2
Attack  Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	URL	https://bwapp.hakhub.net/js/?C=M;O=A
Evidence <title>Index of /js</title> Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	Method	GET
Other Info Web server identified: Apache 2  URL https://bwapp.hakhub.net/js/?C=M;O=D	Attack	
URL https://bwapp.hakhub.net/js/?C=M;O=D		<title>Index of /js</title>
		Web server identified: Apache 2
Method GET	URL	https://bwapp.hakhub.net/js/?C=M;O=D
	Method	GET

Attack	
Evidence	<title>Index of /js</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/js/?C=N;O=A
Method	GET
Attack	
Evidence	<title>Index of /js</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/js/?C=N;O=D
Method	GET
Attack	
Evidence	<title>Index of /js</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/js/?C=S;O=A
Method	GET
Attack	
Evidence	<title>Index of /js</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/js/?C=S;O=D
Method	GET
Attack	
Evidence	<title>Index of /js</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/
URL Method	https://bwapp.hakhub.net/passwords/ GET
Method	
Method Attack	GET
Method Attack Evidence Other	GET <title>Index of /passwords</title>
Method Attack Evidence Other Info	<pre>GET  <title>Index of /passwords</title> Web server identified: Apache 2</pre>
Method Attack Evidence Other Info URL	<pre>GET  <title>Index of /passwords</title>  Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D;O=A</pre>
Method Attack Evidence Other Info URL Method	<pre>GET  <title>Index of /passwords</title>  Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D;O=A</pre>
Method Attack Evidence Other Info URL Method Attack	<pre>GET  <title>Index of /passwords</title> Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D;O=A GET</pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other	<pre>GET  <title>Index of /passwords</title> Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D;O=A GET  <title>Index of /passwords</title></pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info	<pre>GET  <title>Index of /passwords</title> Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D:O=A GET  <title>Index of /passwords</title> Web server identified: Apache 2</pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL URL URL URL URL URL	GET <title>Index of /passwords</title> Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D;O=A  GET <title>Index of /passwords</title> Web server identified: Apache 2  https://bwapp.hakhub.net/passwords/?C=D;O=D

Evidonos	stitles lader of Indeasuarde stitles
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/?C=M;O=A
Method	GET
Attack	
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/?C=M;O=D
Method	GET
Attack	
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/?C=N;O=A
Method	GET
Attack	
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/?C=N;O=D
Method	GET
Attack	
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/?C=S;O=A
Method	GET
Attack	
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/passwords/?C=S;O=D
Method	GET
Attack	
Evidence	<title>Index of /passwords</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other	

lufa	Wah samunidantifiad. Anasha 2
Info URL	Web server identified: Apache 2 <a href="https://bwapp.hakhub.net/stvlesheets/?C=D:O=A">https://bwapp.hakhub.net/stvlesheets/?C=D:O=A</a>
Method	GET
Attack	GET
Evidence	stitles Index of /ots/pophestes //titles
Other	<title>Index of /stylesheets</title>
Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=D
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=D
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=A
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=D
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=A
Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=D

Method	GET
Attack	
Evidence	<title>Index of /stylesheets</title>
Other Info	Web server identified: Apache 2
Instances	51
Solution	Configure the web server to disable directory browsing.
Reference	https://cwe.mitre.org/data/definitions/548.html
CWE Id	<u>548</u>
WASC Id	16
Plugin Id	10033
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	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	phpinfo
Instances	1
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	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html https://www.php.net/manual/en/function.phpinfo.php
CWE Id	<u>538</u>
WASC Id	13
Plugin Id	40035
Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://bwapp.hakhub.net
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/admin/
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://bwapp.hakhub.net/documents/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=S;O=A

NA d	OFT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=A
Method	GET

Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=D
Method	GET
Attack	
Evidence	
Other	
Info	
	https://bwapp.hakhub.net/info.php
Info	https://bwapp.hakhub.net/info.php GET
Info URL	
Info URL Method	
Info URL Method Attack	
Info URL Method Attack Evidence Other	
Info URL Method Attack Evidence Other Info	GET
Info URL Method Attack Evidence Other Info URL	GET  https://bwapp.hakhub.net/js/
Info URL Method Attack Evidence Other Info URL Method	GET  https://bwapp.hakhub.net/js/
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	GET  https://bwapp.hakhub.net/js/
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	GET  https://bwapp.hakhub.net/js/
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info	https://bwapp.hakhub.net/js/ GET
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL	https://bwapp.hakhub.net/js/ GET  https://bwapp.hakhub.net/js/?C=D;O=A
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  Method  Method  Method  URL  Method	https://bwapp.hakhub.net/js/ GET  https://bwapp.hakhub.net/js/?C=D;O=A
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack	https://bwapp.hakhub.net/js/ GET  https://bwapp.hakhub.net/js/?C=D;O=A
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Other Info URL  Method Attack Evidence Other	https://bwapp.hakhub.net/js/ GET  https://bwapp.hakhub.net/js/?C=D;O=A
Info URL  Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL Method Attack Evidence Other Info	https://bwapp.hakhub.net/js/ GET  https://bwapp.hakhub.net/js/?C=D:O=A GET
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack URL  URL	https://bwapp.hakhub.net/js/ GET  https://bwapp.hakhub.net/js/?C=D:O=A GET  https://bwapp.hakhub.net/js/?C=D:O=D

URL https://bwapp.hakhub.net/js/?C=M:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=M:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php	Other Info	
Method GET  Attack  Evidence Other Info URL https://bwapp.hakhub.net/is/?C=M.O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=N.O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=N.O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=N.O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=S.O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=S.O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/login.php  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/login.php		https://bwapp.hakhub.net/is/?C=M:O=A
Attack Evidence Other Info  URL Attack Evidence Other Info  Other Info  URL Attack Evidence Other Info  Ot		
Evidence Other Info URL https://bwapp.hakhub.net/is/?C=M:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=N:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=N:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=N:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/is/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/login.php Method GET Attack		
Info URL https://bwapp.hakhub.net/js/?C=M:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jojin.php Method GET Attack  Evidence Other Info URL https://bwapp.hakhub.net/login.php Method GET Attack		
URL https://bwapp.hakhub.net/js/?C=M:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack	Other	
Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack	Info	
Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=A  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jojin.php Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/login.php Method GET Attack		
Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/login.php Method GET Attack		GET
Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack		
Info URL https://bwapp.hakhub.net/js/?C=N:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/login.php  Method GET  Attack		
Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/7C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/7C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/2C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/2C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/2C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack		
Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	URL	https://bwapp.hakhub.net/js/?C=N;O=A
Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Method	GET
Other Info  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/jogin.php  URL https://bwapp.hakhub.net/login.php  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Attack	
Info  URL  https://bwapp.hakhub.net/js/?C=N:O=D  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=S:O=A  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=S:O=D  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/js/?C=S:O=D  Method  GET  Attack  Evidence  Other Info  URL  https://bwapp.hakhub.net/login.php  URL  https://bwapp.hakhub.net/login.php  Method  GET  Attack	Evidence	
Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=A  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack		
Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=A  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	URL	https://bwapp.hakhub.net/js/?C=N;O=D
Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Method	GET
Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Attack	
Info  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Evidence	
Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack		
Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	URL	https://bwapp.hakhub.net/js/?C=S;O=A
Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack  Attack	Method	GET
Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Attack	
Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Evidence	
Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack		
Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	URL	https://bwapp.hakhub.net/js/?C=S;O=D
Evidence Other Info URL https://bwapp.hakhub.net/login.php Method GET Attack	Method	GET
Other Info  URL https://bwapp.hakhub.net/login.php  Method GET  Attack	Attack	
URL <a href="https://bwapp.hakhub.net/login.php">https://bwapp.hakhub.net/login.php</a> Method GET  Attack	Evidence	
Method GET Attack		
Attack	URL	https://bwapp.hakhub.net/login.php
	Method	GET
Evidence	Attack	
	Evidence	
Other Info		

URL	https://bwapp.hakhub.net/passwords/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=A
Method	GET

Attack	
Evidence	
Other	
Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	
Evidence	
Other	
Info	
Info URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=A
	https://bwapp.hakhub.net/stylesheets/?C=D;O=A GET
URL	
URL Method	
URL Method Attack	
URL Method Attack Evidence Other	
URL  Method  Attack  Evidence  Other Info	GET
URL  Method  Attack  Evidence  Other Info  URL	GET  https://bwapp.hakhub.net/stylesheets/?C=D;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method	GET  https://bwapp.hakhub.net/stylesheets/?C=D;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	GET  https://bwapp.hakhub.net/stylesheets/?C=D;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	GET  https://bwapp.hakhub.net/stylesheets/?C=D;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=D;O=D  GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  URL  Method  Attack  URL  URL  URL  URL  URL  URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Method  Method  Method	https://bwapp.hakhub.net/stylesheets/?C=D;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Attack  Evidence  Other Info  URL  Method  Attack	https://bwapp.hakhub.net/stylesheets/?C=D;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=D;O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=D:O=D GET  https://bwapp.hakhub.net/stylesheets/?C=M:O=A GET
URL  Method  Attack  Evidence  Other Info  URL	https://bwapp.hakhub.net/stylesheets/?C=D:O=D  GET  https://bwapp.hakhub.net/stylesheets/?C=M:O=A  GET  https://bwapp.hakhub.net/stylesheets/?C=M:O=D

Evidence	
Other	
Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/training.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	

URL https://bwapp.hakhub.net/login.php  Method POST  Attack Evidence Other Info  URL https://bwapp.hakhub.net/user.new.php  Method POST  Attack Evidence Other Info  Instances S5  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  Solution If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/guetry-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4968 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://www.pinchub.com/query/jquery/issues/2432 https://wesearch.insecurites.org/query/issues/2432 https://wesearch.insecurites.org/query/issues/2432 https://github.com/query/jquery-Cve-2015-7056 https://wd.nist.gov/vuln/detall/CVE-2019-2516 https://github.com/query/jquery-Cve-20-7666 https://bus.puery-com/cve-10/2016/01/08/jquery-2-2-and-1-12-released/ https://wilnbs.jquery-com/cve-10/2016/01/08/jquery-2-2-and-1-12-released/ https://wilnbs.jquery-com/cve-10/2016/01/08/jquery-2-2-and-1-12-released/ https://wilnbs.jquery-com/cve-10/2016/01/09/query-3-3-0-released/ https://wilnd.ist.gov/vuln/detall/CVE-2019-3681  Instances 1  Solution Upgrade to the latest version of the affected library.  MASC Id  WASC Id	Othor	
Method POST  Attack Evidence Other Info URL https://bwapp.hakhub.net/user_new.php  Method POST  Attack Evidence Other Info Instances  55  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  Solution  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  WaSC Id 15 Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/is/guery-1.4.4.min.js  Method GET  Attack  Evidence   jquery-1.4.4.min.js The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://jbub.com/divers/inscovrelabs.org/jquery/issel/ribub.com/jquery/jquery/issues/2422 https://jbub.com/divers/inscovrelabs.org/jquery/issel/ribub.com/jquery/jquery/issues/122 https://invd.nist.gov/vuln/detailCVE-2019-11358 CVE-2020-11029 CVE-2015-9251 thtps://jridub.com/jquery/issel/sues/inscovrelabs.org/jquery/issel/ribub.com/jqu	Other Info	
Attack Evidence Other Info  URL bttps://bwapp.hakhub.net/user_new.php  Method POST Attack Evidence Other Info  Instances  55  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilia.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE id 1021 WASC Id 15 Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/[query-1.4.4.min.js]  Attack  Evidence  [query-1.4.4.min.js] The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-14969 CVE-2020-11023 http://wod.nist.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://md.nist.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2019-11358 https://glitub.com/query/guery.com/picket/1290 https://wod.nist.gov/vuln/detail/CVE-2019-11358 https://glitub.com/advisories/GHSA-rmsg-73gg-498 https://youg.juery.com/picket/11974 /destil/CVE-2019-1019-1019-1019-1019-1019-1019-1019	URL	https://bwapp.hakhub.net/login.php
Evidence Other Info URL https://bwapp.hakhub.net/user_new.php  Method POST Attack Evidence Other Info Instances  55 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY, Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  WASC Id 15 Plugin Id 10020  Medium Vulnerable JS Library Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/iguery-1.4.4.min.js  Method GET Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE: 2011-14969 CVE-2020-11023 http://www.nis.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://www.nis.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2012-1023 https://www.nis.gov/vuln/detail/CVE-2019-11358 cVE-2020-7656 CVE-2012-6708 https://jdhub.com/query/iguery.com/civles/1974 https://jdhub.com/query/iguery.com/civ	Method	POST
Other Info  URL https://bwapp.hakhub.net/user_new.php  Method POST  Attack  Evidence Other Info  Instances 55  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g., it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  WASC Id 15  Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/fquery-1.4.4.min.js  Method GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://md.nist.gov/uni/detail/CVE-2019-11358 https://glithub.com/query/jsuery.com/yideal/CVE-2012-8708 https://glithub.com/query/jsuery.com/yideal/CVE-2012-8708 https://glithub.com/query/jsuery.com/yideal/CVE-2012-8708 https://glithub.com/query/jsuery.com/yideal/CVE-2012-8708 https://glithub.com/query/jsuery.com/yideal/CVE-2013-9755 https://glithub.com/query/jsuery.com/yideal/CVE-2019-9755 https://glithub.com/query/jsuery.com/yideal/CVE-2019-9755 https://glithub.com/query/jsuery.com/yideal/CVE-2019-9755 https://glithub.com/query/jsuery.com/yideal/CVE-2019-9755 https://glithub.com/query/jsuery.com/yideal/CVE-2019-9775-97-1128-1128-977-1128-1128-978-979-977-1128-1128-979-979-979-979-979-979-979-979-979-97	Attack	
Info  URL  Method  POST  Attack  Evidence  Other Info  Instances  55  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  Solution  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policys 'frame-ancestors' directive.  Reference  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id  1021  WASC Id  15  Plugin Id  10020  Medium  Vulnerable JS Library  Description  The identified library appears to be vulnerable.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  iquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://rivsd-nist.gov/vuln/detail/CVE-2019-11358 https://jwitub.com/jquery/jquery/sissuss/2432 http://irsearch.insecurelabs.org/jquery/sissuss/2432 https://jgithub.com/jquery/jquery/csers/inses/index/insecurelassed/ https://md.nist.gov/vuln/detail/CVE-2019-11358 https://jgithub.com/jquery/jquery/csers/inses/GHSA-rmay-73gg-4p98 https://md.nist.gov/vuln/detail/CVE-2019-11358 https://jgithub.com/jquery/jquery/com/sissuss/162 https://md.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/inses/1618-https://md.nist.gov/vuln/detail/CVE-2019-1358 https://jgithub.com/jquery/jquery/com/sissuss/162 https://md.nist.gov/vuln/detail/CVE-2019-1358 https://jgithub.com/jquery/jquery/com/sissuss/162 https://md.nist.gov/vuln/detail/CVE-2019-1358 https://jgithub.com/jquery/jquery/com/sissuss/162 https://md.nist.gov/vuln/detail/CVE-2019-1358 https://jgithub.com/jquery/jquery-2-3-0-released/ https://md.nist.gov/vuln/detail/CVE-2019-1358 https://jgithub.com/jquery/jquery-2-3-0-released/ https://md.nist.gov/vuln/det	Evidence	
Method POST  Attack  Evidence Other Info  Instances 55  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  Solution If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy 'frame-ancestors' directive.'  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  WASC Id 15  Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2012-6708 https://work.inst.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://jglubu.com/iguery/jquery/com/sizes/162 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://jub.com/iguery/jquery/com/sizes/162 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://jub.com/iguery/jquery/com/sizes/162 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://jub.com/iguery/jquery/com/sizes/162 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://jub.com/iguery/jquery/com/sizes/162 https://work.inst.gov/vuln/detail/CVE-2019-67656 https://jub.com/iguery/guery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub.com/jquery/jquery/com/sizes/162 https://jub		
Attack Evidence Other Info Instances 55 Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021 WASC Id 15 Plugin Id 10020  Medium Vulnerable JS Library Description The identified library appears to be vulnerable.  URL https://dbwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2012-6708 https://work.inst.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://work.inst.gov/vuln/detail/CVE-2019-6756 https://work.inst.gov/vuln/detail/CVE-2019-6756 https://jchub.com/apuery/jquery/com/suses/162 https://mvd.nist.gov/vuln/detail/CVE-2019-6756 https://jchub.com/apuery/jquery/com/suses/162 https://mvd.nist.gov/vuln/detail/CVE-2019-6756 https://jchub.com/apuery/jquery/com/suses/162 https://mvd.nist.gov/vuln/detail/CVE-2019-6756 https://jchub.com/apuery/jquery/com/suses/162 https://mvd.nist.gov/vuln/detail/CVE-2019-6756 https://jchub.com/apuery/jquery/com/suses/162 https://jchub.com/apuery/jquery/co	URL	https://bwapp.hakhub.net/user_new.php
Evidence Other Info Instances Other Info Instances  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  Solution  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id  1021  WASC Id 15 Plugin Id 10020  Medium  Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  Attack Evidence  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-1	Method	POST
Other Info	Attack	
Instances  55  Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  Solution  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id  1021  WASC Id  15  Plugin Id  10020  Medium  Vulnerable JS Library  Description  The identified library appears to be vulnerable.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nyd.nist.gov/vuln/detail/CVE-2019-11358 CVE-2020-7656 CVE-2019-11358 https://nyd.nist.gov/vuln/detail/CVE-2019-7656 https://github.com/jquery/jquery/ses/dail/CVE-2019-7656 https://github.com/jquery/jquery-com/suses/423 https://github.com/jquery/jquery-ca-2-and-1-12-released/ https://bugs.jquery.com/suses/ds18-14-14-18-14-1	Evidence	
Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  WASC Id 15  Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/is/iguery-1.4.4.min.js  Method GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 CVE-2019-1358 CVE-2020-7656 CVE-2019-1358 https://ipsearch.insecurelabs.org/jquery/tes/lb https://ipsidub.com/jquery/jquery/suery/suery/suery/suery/ses/detail/cVE-2015-9251 https://github.com/jquery/jquery/suery/sick/11974 https://jgithub.com/jquery/jquery/suery/sick/11974 https://jgithub.com/jquery/jquery/sick/11974 https://jgithub.com/jquery/jquery/sick/11974 https://jgithub.com/jquery/jquery/sick/11974 https://jgithub.com/jquery/jquery/com/inst-gov/vuln/detail/CVE-2020-7656 https://jougi-jquery.com/inst-gov/vuln/detail/CVE-2015-9251 https://jgithub.com/advisories/GHSA-rmxy-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://jougi-jquery.com/inst-gov/vuln/detail/CVE-2015-9251 https://jgithub.com/advisories/GHSA-q4m3-2/7h-f7xw https://jgithub.com/jquery/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecrelabs.org/jquery/sesarch.insecre		
headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.  Reference	Instances	55
FRAMESET) then you'll want to use SANEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's 'frame-ancestors' directive.  Reference https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  CWE Id 1021  WASC Id 15  Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2014-6708 https://jcsearch.insecurelabs.org/jquery/jtest https://jrd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://pud-nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/921 http://blog.jquery.com/ticket/11974 https://bugs.jquery.com/ticket/921 http://blog.jquery.com/ticket/1290 https://research.insecurelabs.org/jquery/com/ticket/1290 https://research.insecurelabs.org/jquery/com/ticket/1290 https://research.insecurelabs.org/jquery/com/ticket/1290 https://research.insecurelabs.org/jquery/com/ticket/1290 https://research.insecurelabs.org/jquery/com/ticket/921 http://blog.jquery.com/com/ticket/921 http://blog.jquery.com/com/ticket/921 https://blog.jquery.com/com/ticket/921 https://github.com/advisories/GHSA-a-4m3-2/7h-f7xw https://github.com/jquery/com/mit/53d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/com/2019/dh/ticket/dts/CVE-2011-4969  Instances 1  Solution Upgrade to the latest version of the affected library.  Reference https://owasp.org/Top10/A06 2021-Vul		
CWE Id 1021  WASC Id 15  Plugin Id 10020  Medium Vulnerable JS Library  Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://mvd.nist.gov/vuln/detail/CVE-2012-6708 https://jmvd.nist.gov/vuln/detail/CVE-2012-6708 https://jrude.pisues/2432 http://research.insecurelabs.org/jquery/ses/739g-4p98 https://jbudy.jquery.com/ticket/11974  Other Info  Other Info  Other Info  Other Info  Info  Other Info	Solution	FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security
Medium  Vulnerable JS Library  Description  The identified library appears to be vulnerable.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://jnvd.nist.gov/vuln/detail/CVE-2012-6708 https://jrude.nist.gov/vuln/detail/CVE-2012-6708 https://jrude.nist.gov/vuln/detail/CVE-2019-11358 https://jthub.com/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://jvud.nist.gov/vuln/detail/CVE-2019-11358 https://jthub.com/jquery/jquery.com/icket/11974 https://jthub.com/jquery/jquery.com/icket/13921 https://jnvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/icket/13921 https://jnvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/icket/13921 https://jouery.com/com/jquery-2-2-and-11-2-released/ http://bugs.jquery.com/icket/1390 https://research.insecurelabs.org/jquery/rest/ https://jblog.jquery.com/icket/1390 https://research.insecurelabs.org/jquery/rest/ https://jglthub.com/jquery/3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2010-7656 https://jquery/com/icket/1390 https://research.insecurelabs.org/jquery/rest/ https://jquery/com/icket/1390 https://rosearch.insecurelabs.org/jquery/rest/ https://jquery/com/advisories/GHSA-q4m3-27h-f7xw https://github.com/jquery/jquery/com/itr/53d591-aea698e578d658se9722cd0808619b1 https://jblog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1  Solution  Upgrade to the latest version of the affected library.  Reference  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/	Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
Plugin Id   Medium   Vulnerable JS Library	CWE Id	<u>1021</u>
Description The identified library appears to be vulnerable.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://presearch.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/itcket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1 Solution Upgrade to the latest version of the affected library. Reference https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/		
Description  The identified library appears to be vulnerable.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://jqthub.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bug.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://hod.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/icket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://bugs.jquery.com/icket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://hod.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1  Solution  Upgrade to the latest version of the affected library.  Reference  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/  CWE Id  1395	WASC Id	15
URL     https://bwapp.hakhub.net/js/jquery-1.4.4.min.js       Method     GET       Attack     Evidence       The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/icket/11974 https://github.com/ajquery/jquery/com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969       Instances     1       Solution     Upgrade to the latest version of the affected library.       Reference     https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/       CWE Id     1395		
Method GET  Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://jqithub.com/jquery/jguery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances 1  Solution Upgrade to the latest version of the affected library.  Reference https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/  CWE Id 1395	Plugin Id	10020
Attack  Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jguery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2013-11358 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://bugs.jquery.com/2019/04/10/jquery-3-4-0-released/ https://research.insecurelabs.org/jquery/test/ https://slog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/slog-mit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1  Solution  Upgrade to the latest version of the affected library.  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/  CWE Id  1395	Plugin Id  Medium	10020 Vulnerable JS Library
Evidence jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://presearch.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1  Solution  Upgrade to the latest version of the affected library.  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/  CWE Id  1395	Plugin Id  Medium  Description	Vulnerable JS Library The identified library appears to be vulnerable.
The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/icket/9521 https://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1  Solution  Upgrade to the latest version of the affected library.  Reference  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/  CWE Id  1395	Plugin Id  Medium  Description  URL	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js
CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jssues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  Instances  1  Solution  Upgrade to the latest version of the affected library.  Reference  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/  CWE Id  1395	Plugin Id  Medium  Description  URL  Method	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js
Solution Upgrade to the latest version of the affected library.  Reference <a href="https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/">https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/</a> CWE Id <a href="https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/">1395</a>	Plugin Id  Medium  Description  URL  Method  Attack	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET
Reference <a href="https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/">https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/</a> CWE Id <a href="https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/">1395</a>	Plugin Id  Medium  Description  URL  Method  Attack  Evidence	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://jethub.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/icket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-
CWE ld <u>1395</u>	Plugin Id  Medium  Description  URL  Method  Attack  Evidence  Other Info	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://github.com/jquery/issues/2432 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969
_	Plugin Id  Medium  Description  URL  Method  Attack  Evidence  Other Info	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/detail/CVE-2019-11358 https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/com/com/com/com/com/com/com/com/com/
WASC Id	Plugin Id  Medium  Description  URL  Method  Attack  Evidence  Other Info	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 https://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/9521 https://lolog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://bugs.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  1 Upgrade to the latest version of the affected library.
	Plugin Id  Medium  Description  URL  Method  Attack  Evidence  Other Info  Instances  Solution  Reference	Vulnerable JS Library  The identified library appears to be vulnerable.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET  jquery-1.4.4.min.js  The identified library jquery, version 1.4.4 is vulnerable. CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/query/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-and-1-12-released/ http://bugs.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969  1 Upgrade to the latest version of the affected library. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Plugin Id	10003
Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	Set-Cookie: security_level
Other Info	
Instances	3
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010
Low	Cookie Without Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	Set-Cookie: PHPSESSID
Other	

Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	Set-Cookie: security_level
Other	
Info	
Instances	3
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4- Web Application Security Testing/06-Session Management Testing/02- Testing for Cookies Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011
Low	Cookie without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	Set-Cookie: security_level
Other Info	
Instances	3
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

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	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	172.19.0.6
Other Info	172.19.0.6 172.19.0.1 172.19.0.6 172.19.0.1
Instances	1
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	497
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	https://bwapp.hakhub.net
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/admin/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other	

Info	
URL	https://bwapp.hakhub.net/login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/training.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	

URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Other Info	
Instances	12
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	497
WASC Id	13
Plugin Id	<u>10037</u>
Low	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server Unix
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	1745097697
Other Info	1745097697, which evaluates to: 2025-04-19 17:21:37.
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096
Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://bwapp.hakhub.net
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/admin/

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/bWAPP_intro.pdf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/Iron_Man.pdf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/Terminator_Salvation.pdf
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/The Amazing Spider-Man.pdf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/The Cabin in the Woods.pdf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/The Dark Knight Rises.pdf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/documents/The Incredible Hulk.pdf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/fonts/architectsdaughter.ttf
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/icons/back.gif
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/icons/blank.gif
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/icons/image2.gif
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/icons/layout.gif
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/icons/text.gif
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/icons/unknown.gif
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=N;O=D
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/bee_1.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/bg 1.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/bg_2.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/bg_3.jpg
Method	GET
Attack	
Evidence	

	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/blogger.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/captcha.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/cc.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/evil_bee.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/facebook.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/favicon.ico
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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
URL	or server error responses.  https://bwapp.hakhub.net/images/favicon_drupal.ico
Method	GET
Attack	GLI
Evidence	
LVIGETICE	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/free_tickets.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/linkedin.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/mk.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/mme.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/netsparker.gif
Method	GET
Attack	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/netsparker.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/nsa.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/owasp.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/sb_1.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/twitter.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/images/zap.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	https://bwapp.hakhub.net/info.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/js/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/js/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/js/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/js/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/js/?C=M;O=D
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.

Wethod GET  Attack Evidence  Cher Inic 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 acutal content type. At "High" threshold this scan rule will not alert on client or server arror responses.  URL https://bwapp.hakhub.net/js/?C=N.O=D  Method GET  Attack Evidence  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 acutal content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S.O=A  Method GET  Attack Evidence  Other Info away from their acutal content type. At "High" threshold this scan rule will not alert on client or server or responses.  URL https://bwapp.hakhub.net/js/?C=S.O=D  Method GET  Attack Evidence  Other Info away from their acutal content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S.O=D  Method GET  Attack Evidence  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 acutal content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  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 acutal content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  This issue still applies to error type pages (401, 403, 500, etc.) a	LIRI	
Attack Evidence  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 servere error responses.  URL  Method  GET  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  Method  GET  Attack Evidence  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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing 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  Method  GET  Attack Evidence  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  Method  GET  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 the	OILL	https://bwapp.hakhub.net/js/?C=N;O=A
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=N:O=D  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/furny-1.4.4.min.js  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often	Method	GET
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  Method  GET  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/?C=S:O=A  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/?C=S:O=D  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/?tml5.js  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/fuurey-1.4.4.min.js  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in	Attack	
Other Info area yr from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=N-O=D  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S:O=A  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S:O=D  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/ftuney-1.4.4.min.js  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.	Evidence	
Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/?C=S:O=A  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/?C=S:O=D  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/?C=S:O=D  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/fuguery-1.4.4.min.js  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/fuguery-1.4.4.min.js  This issue still applies to error type pages (401, 403, 500, etc.) as those pages ar		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
Attack Evidence  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 allert on client or server error responses.  URL  https://bwapp.hakhub.net/js/?C=S:O=A  Method  GET  Attack Evidence  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 allert on client or server error responses.  URL  https://bwapp.hakhub.net/js/?C=S:O=D  GET  Attack Evidence  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 allert on client or server error responses.  URL  https://bwapp.hakhub.net/js/html5.js  Method  GET  Attack Evidence  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 and you from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses.  URL  https://bwapp.hakhub.net/js/html5.js  GET  Attack Evidence  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 and you from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses.  URL  https://bwapp.hakhub.net/js/query-1.4.4.min.js  GET  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often st	URL	https://bwapp.hakhub.net/js/?C=N;O=D
Cither Info Other Info	Method	GET
Other Info Other Info Other Info Other Info Other Info Other Info Info Other Info Info Other Info Info Other Info Info Info Info Info Info Info Info	Attack	
Other Info away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/?C=S:O=A  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/?C=S:O=D  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/is/ntml5.js  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack Evidence  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 no	Evidence	
Method  Attack  Evidence  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 are often still on away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/?C=S:O=D  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/html5.js  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/is/iquery-1.4.4.min.js  Method  GET  Attack  Evidence  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.  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 affected by injection issues, in which case there is still concern for browsers sniffing pages 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 of the pages aff		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
Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/?C=S:O=D  GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/html5.js  Method  GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack Evidence  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 affected by injection issues, in which case there is still concern for browsers sniffing pages laffected 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 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 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 aler	URL	https://bwapp.hakhub.net/js/?C=S;O=A
Cher Info away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/7C=S:O=D  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/7C=S:O=D  Other away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack Evidence  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 affected by injection issues, in which case there is still concern for browsers sniffing pages life of the 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 life of the 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 life of the 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 life of the pages (401, 403, 500, etc.) as those pages are often still affected by injection	Method	GET
Other Info	Attack	
Other Info affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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 of the affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still a	Evidence	
Method GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/html5.js  Method  GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages info  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		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
Attack Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/html5.js  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages info  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	URL	https://bwapp.hakhub.net/js/?C=S;O=D
Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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 in the 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 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	Method	GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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 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 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	Attack	
Other Info adjected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/html5.js  Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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 of the pages away from their actual content type. At "High" threshold this scan rule will not alert on client or elient or server under the 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	, mao	
Method GET  Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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		
Attack  Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  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	Evidence Other	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
Evidence  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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	Evidence Other Info	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.
Other Info  Other Info  Other Info  Other Info  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method  GET  Attack  Evidence  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	Evidence Other Info URL	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js
Other Info adjected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  URL https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  Method GET  Attack  Evidence  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	Evidence  Other Info  URL  Method	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js
Method  Attack  Evidence  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	Evidence  Other Info  URL  Method  Attack	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js
Attack  Evidence  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	Evidence  Other Info  URL  Method  Attack  Evidence  Other	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js  GET  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
Evidence  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	Other Info  URL  Method  Attack  Evidence  Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js  GET  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.
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	Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js  GET  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js
Other 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	Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js  GET  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js
	Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/html5.js  GET  This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js

URL	https://bwapp.hakhub.net/js/json2.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/js/xss_ajax_1.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/login.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=M;O=A

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/heroes.xml

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/web.config.bak
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/passwords/wp-config.bak
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/robots.txt
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=A
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=A
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/stylesheet.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/stylesheet_low_resolution.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/stylesheets/stylesheet_normal_resolution.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/training.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	102
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	<u>693</u>
WASC Id	15
Plugin Id	10021
Informational	Authentication Request Identified

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	https://bwapp.hakhub.net/user_new.php
Method	POST

Attack	
Evidence	password
Other Info	userParam=email userValue=gAtmtngVyWehtJmoxtEoFlem passwordParam=password referer=https://bwapp.hakhub.net/user_new.php
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=oUlBxWFxUhZuzznA passwordParam=password referer=https://bwapp.hakhub.net/user_new.php
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=pFmRetaWJjhPbsjs passwordParam=password referer=https://bwapp.hakhub.net/user_new.php
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=yFXgqNry passwordParam=password referer=https://bwapp.hakhub.net/user_new.php
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://bwapp.hakhub.net/user_new.php
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	password
LVIGGIOG	userParam=login userValue=oBDvlHECSqNnVCOH passwordParam=password
Other Info	referer=https://bwapp.hakhub.net/login.php
Other	
Other Info	referer=https://bwapp.hakhub.net/login.php
Other Info URL	referer=https://bwapp.hakhub.net/login.php  https://bwapp.hakhub.net/login.php

Evidence	password
Other Info	userParam=login userValue=PlyvKOnyOgyzHQff passwordParam=password referer=https://bwapp.hakhub.net/login.php
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=login userValue=qUZHyovV passwordParam=password referer=https://bwapp.hakhub.net/login.php
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=login userValue=yEFPLQCYHYQYtTjq passwordParam=password referer=https://bwapp.hakhub.net/login.php
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=login userValue=ZAP passwordParam=password referer=https://bwapp.hakhub.net/login.php
Instances	11
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111
Informational	Content-Type Header Missing

Informational	Content-Type Header Missing
Description	The Content-Type header was either missing or empty.
URL	https://bwapp.hakhub.net/fonts/architectsdaughter.ttf
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
CWE Id	<u>345</u>
WASC Id	12
Plugin Id	10019
Solution  Reference  CWE Id  WASC Id	Ensure each page is setting the specific and appropriate content-type value for the content being delivered. <a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> 345 12

**GET for POST** 

Informational

Description	A request that was originally observed as a POST was also accepted as a GET. This issue does however, it may facilitate simplification of other attacks. For example if the original POST is subjumy indicate that a simplified (GET based) XSS may also be possible.
URL	https://bwapp.hakhub.net/login.php
Method	GET
Attack	
Evidence	GET https://bwapp.hakhub.net/login.php?form=submit&login=PlyvKOnyOgyzHQff&password=&
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	GET https://bwapp.hakhub.net/user_new.php? action=create&email=oUIBxWFxUhZuzznA&login=yGDySAbKAjYAIKWC&mail_activation=&pasHTTP/1.1
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	GET https://bwapp.hakhub.net/user_new.php? action=create&email=pFmRetaWJjhPbsjs&login=kjUsarKgPoNhiVUs&password=&password_cd
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	GET https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP HTTP/1
Other Info	
Instances	4
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	<u>10058</u>
Informational	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for

Informational	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	zaproxy@example.com

Other Info	The URL contains email address(es).
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail activation=&password=ZAP&password conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	password
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass password
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	password_conf
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass password_conf
Instances	3
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	<u>598</u>
WASC Id	13
Plugin Id	10024
Informational	Information Disclosure - Suspicious Comments

The response appears to contain suspicious comments which may help an attacker.  https://bwapp.hakhub.net/js/jquery-1.4.4.min.js  GET
GET CONTROL OF THE CO
sername
The following pattern was used: \bUSERNAME\b and was detected in likely comment: "/*"}}, ujax:function(a){var b=c.extend(true,{},c.ajaxSettings,a),d,e,f,h=b.type.toUpperCase(),l=qb.est(h);b.url=b.url.replace(ub", see evidence field for the suspicious comment/snippet.
ttps://bwapp.hakhub.net/js/json2.js
GET CONTROL OF THE CO
rom
The following pattern was used: \bFROM\b and was detected in likely comment: "// Produce a string from holder[key].", see evidence field for the suspicious comment/snippet.
uttps://bwapp.hakhub.net/js/xss_ajax_1.js
BET
ser
The following pattern was used: \bUSER\b and was detected in likely comment: "// Retrieves the movie title typed by the user on the form", see evidence field for the suspicious comment/snippet.

Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<u>615</u>
WASC Id	13
Plugin Id	<u>10027</u>

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	
Evidence	<a name="module_apache2handler">apache2handler</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://bwapp.hakhub.net/admin/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	

URL	https://bwapp.hakhub.net/documents/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/documents/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/
Method	GET

Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
LIDI	
URL	https://bwapp.hakhub.net/images/?C=N;O=D
Method	https://bwapp.hakhub.net/images/?C=N;O=D  GET
Method	
Method Attack	
Method Attack Evidence Other	
Method Attack Evidence Other Info	GET
Method Attack Evidence Other Info URL	GET  https://bwapp.hakhub.net/images/?C=S;O=A

Evidence	
Other Info	
URL	https://bwapp.hakhub.net/images/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/info.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=D;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=M;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/js/?C=M;O=D
Method	GET
Attack	
Evidence	
Other	

URL https://bwapp.hakhub.net/js/7C=N:O=A  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/js/7C=N:O=D  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/js/7C=S:O=A  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/js/7C=S:O=D  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/js/7C=S:O=D  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/passwords/ Evidence Other Info  URL https://hwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/passwords/7C=D:O=A  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/passwords/7C=D:O=A  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/passwords/7C=D:O=D  Method GET  Attack Evidence Other Info  URL https://hwapp.hakhub.net/passwords/7C=D:O=D  Method GET  Attack Evidence Other Info	Info	
Method Attack Evidence Other Info URL Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/ Evidence Other Info URL https://bwapp.hakhub.net/jasswords/ GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/ GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/?C=D:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/?C=D:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/jasswords/?C=D:O=D Method GET Attack Evidence Other Info		https://bwapp.hakhub.net/js/?C=N;O=A
Evidence Other Info URL https://bwapp.hakhub.net/js/?C=N:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/ Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/ Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info	Method	
Other Info  URL https://bwapp.hakhub.net/js/7C=N:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/7C=S:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/7C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/ Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/ Evidence Other Info  URL https://bwapp.hakhub.net/passwords/7C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/7C=D:O=D  Method GET  Attack Evidence Other Info	Attack	
Info URL https://bwapp.hakhub.net/js/7C=N:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/7C=S:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/7C=S:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/7C=S:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Evidence	
Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/7C=S:O=A  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/7C=S:O=D  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/7C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/7C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/7C=D:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/7C=D:O=D  Method GET  Attack Evidence Other Info		
Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/ Evidence Other Info URL https://bwapp.hakhub.net/passwords/ Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/ GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D	URL	https://bwapp.hakhub.net/js/?C=N;O=D
Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/ Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/ Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D Method GET Attack Evidence Other Info	Method	GET
Other Info  URL https://bwapp.hakhub.net/js/?C=S:Q=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:Q=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:Q=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:Q=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:Q=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:Q=D  Method GET  Attack Evidence Other Info	Attack	
Info URL https://bwapp.hakhub.net/js/?C=S;O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/  Wethod GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Evidence	
Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  Other Info  Other Info  Other Info		
Attack Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S;O=D  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  Other Info  Other Info	URL	https://bwapp.hakhub.net/js/?C=S;O=A
Evidence Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/ Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack  Evidence  Other Info  Other Info  Other Info  Other Info  Other Info	Attack	
Info  URL https://bwapp.hakhub.net/js/?C=S:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  Other Info	Evidence	
Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack  Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack  Evidence Other Info  Other Info  Other Info  Other Info		
Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/ Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  Other Info  Other Info	URL	https://bwapp.hakhub.net/js/?C=S;O=D
Evidence Other Info  URL https://bwapp.hakhub.net/passwords/ Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Attack	
Info  URL https://bwapp.hakhub.net/passwords/  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Evidence	
Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info		
Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack Evidence Other Info	URL	https://bwapp.hakhub.net/passwords/
Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=A  Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=A  Method GET  Attack  Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack  Evidence  Other Info  Other Info  Other Info	Attack	
Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=A  Method GET  Attack Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack Evidence  Other Info  Other Info	Evidence	
Method GET  Attack Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D:O=D  Method GET  Attack Evidence Other Info		
Attack Evidence  Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack Evidence Other Info	URL	https://bwapp.hakhub.net/passwords/?C=D;O=A
Evidence Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack  Evidence  Other Info	Attack	
Info  URL https://bwapp.hakhub.net/passwords/?C=D;O=D  Method GET  Attack  Evidence  Other Info		
Method GET  Attack  Evidence  Other Info		
Attack Evidence Other Info	URL	https://bwapp.hakhub.net/passwords/?C=D;O=D
Evidence Other Info	Method	GET
Other Info		
Info	Evidence	
URL <a href="https://bwapp.hakhub.net/passwords/?C=M:O=A">https://bwapp.hakhub.net/passwords/?C=M:O=A</a>		
	URL	https://bwapp.hakhub.net/passwords/?C=M;O=A

Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=M;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/passwords/heroes.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET

Attack	
Evidence	
Other	
Info	
URL	https://bwapp.hakhub.net/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=A
Method	GET
Attack	
Evidence	
Other Info	
IIIIO	
URL	https://bwapp.hakhub.net/stylesheets/?C=D;O=D
	https://bwapp.hakhub.net/stylesheets/?C=D;O=D GET
URL	
URL Method Attack Evidence	
URL Method Attack	
URL Method Attack Evidence Other	
URL Method Attack Evidence Other Info	GET
URL  Method  Attack  Evidence  Other Info  URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  URL  Method  Attack  URL  URL  URL  URL  URL  URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method	https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=D
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Attack  Evidence  Other Info  URL  Method  Attack	https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=D
URL  Method  Attack  Evidence  Other Info  URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A GET  https://bwapp.hakhub.net/stylesheets/?C=M;O=D
URL  Method  Attack  Evidence  Other Info	https://bwapp.hakhub.net/stylesheets/?C=M:O=A GET  https://bwapp.hakhub.net/stylesheets/?C=M:O=D GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  URL  URL  URL	https://bwapp.hakhub.net/stylesheets/?C=M:O=A GET  https://bwapp.hakhub.net/stylesheets/?C=M:O=D GET  https://bwapp.hakhub.net/stylesheets/?C=N:O=A

Other	
Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=S:O=A
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=S;O=D
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/training.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP
Method	GET
Attack	
Evidence	
Other Info	
Instances	53
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, maxage, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet. html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

	https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	<u>525</u>
WASC Id	13
Plugin Id	<u>10015</u>

Plugin Id	10015
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	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	2eev20f2ihtr3v9d030omal1g1
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	4s8sg3ohg0jbcsnfanqhr6eac2
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	9bab782nl5a1d8mribfg7itcq1
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	b4jo64vkoqpo0accla1hb8cf02
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	ipedivc918t5d6d66f7asl20p1
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	jjicq8ltpcbl5dr8pqorof6mp1

041	
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	iibgv5obm2or76t8v5qh1ao1a1
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	
Evidence	n6vpfsc2c3d4s7adl46fmkghp3
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	4s8sg3ohg0jbcsnfanqhr6eac2
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	9bab782nl5a1d8mribfg7itcq1
Other Info	cookie:PHPSESSID
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	
Evidence	jjicq8ltpcbl5dr8pqorof6mp1
Other Info	cookie:PHPSESSID
Instances	11
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	<u>10112</u>
Informational	User Agent Fuzzer

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	https://bwapp.hakhub.net/
Method	GET

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
https://bwapp.hakhub.net/
GET
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
https://bwapp.hakhub.net/
GET
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
https://bwapp.hakhub.net/
GET
Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
https://bwapp.hakhub.net/
GET
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
https://bwapp.hakhub.net/
GET
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
https://bwapp.hakhub.net/
GET
GET  Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0

Evidence	
Other Info	
URL	https://bwapp.hakhub.net/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/
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	https://bwapp.hakhub.net/
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	https://bwapp.hakhub.net/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
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	https://bwapp.hakhub.net/phpinfo.php
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	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other	
Info	
URL	https://bwapp.hakhub.net/phpinfo.php
	https://bwapp.hakhub.net/phpinfo.php  GET
URL	

Evidence	
Other Info	
URL	https://bwapp.hakhub.net/phpinfo.php
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	https://bwapp.hakhub.net/phpinfo.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
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	https://bwapp.hakhub.net/portal.php
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	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/portal.php
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	https://bwapp.hakhub.net/portal.php
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	https://bwapp.hakhub.net/portal.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

Other	
Info URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	iviozilia/4.0 (compatible, iviole 6.0, vviildows ivi 5.1)
Other	
Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
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	https://bwapp.hakhub.net/login.php
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	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other	

Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/login.php
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	https://bwapp.hakhub.net/login.php
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	https://bwapp.hakhub.net/login.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	48
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	10101
Plugin Id	<u>10104</u>
Informational	User Controllable HTML Element Attribute (Potential XSS)

In	formational	User Controllable HTML Element Attribute (Potential XSS)
De	escription	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	https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP

Method	GET
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: https://bwapp.hakhub.net/user_new.php?action=create&email=zaproxy@example.com&login=ZAP&mail_activation=&password=ZAP&password_conf=ZAP&secret=ZAP appears to include user input in: a(n) [button] tag [value] attribute The user input found was: action=create The user-controlled value was: create
URL	https://bwapp.hakhub.net/login.php
Method	POST
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: https://bwapp.hakhub.net/login.php appears to include user input in: a(n) [button] tag [type] attribute The user input found was: form=submit The user-controlled value was: submit
URL	https://bwapp.hakhub.net/login.php
Method	POST
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: https://bwapp.hakhub.net/login.php appears to include user input in: a(n) [button] tag [value] attribute The user input found was: form=submit The user-controlled value was: submit
URL	https://bwapp.hakhub.net/user_new.php
Method	POST
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: https://bwapp.hakhub.net/user_new.php appears to include user input in: a(n) [button] tag [value] attribute The user input found was: action=create The user-controlled value was: create
Instances	4
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input Validation Cheat Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	<u>10031</u>

#### MAUNDU ERICK NZIOKA

## Ericknzioka83@gmail.com

Answers of Task B Practical section: Active Scanning and Vulnerability Analysis:

Have Attached A detailed OWASP ZAP report which have scanned the <a href="https://bwapp.hakhub.net">https://bwapp.hakhub.net</a> site.

## Three Vulnerabilities detected during the scan;

### 1. SQL Injection - SQLite

Risk Level: High

URL: https://bwapp.hakhub.net/user\_new.php?action=create&...

What it is-SQL Injection occurs when unsanitized input is included directly in SQL queries. This is the most critical vulnerability found, with 1 instance detected. SQL injection allows attackers to manipulate database queries by inserting malicious SQL code.

Why it's important- This vulnerability allows attackers to execute arbitrary SQL commands against the backend database. If exploited, an attacker could potentially read, modify, or delete data, or even gain administrative access to the system.

#### 2. Absence of Anti-CSRF Tokens

Risk Level: Medium

URL: Multiple forms, including https://bwapp.hakhub.net/login.php and user new.php

What it is- Cross-Site Request Forgery (CSRF) exploits the trust a site has in a user's browser. If the application doesn't include anti-CSRF tokens in forms, attackers can trick users into submitting unintended requests.

Why it's important- Without protection, attackers can perform unauthorized actions on behalf of authenticated users (e.g., changing passwords) simply by tricking them into visiting malicious pages.

# 3. Application Error Disclosure

Risk Level: Medium

URL: Multiple, such as https://bwapp.hakhub.net/documents/

What it is-The application exposes detailed error or warning messages, often revealing the file path or internal implementation details.

**Why it's important-** This kind of information can help attackers understand the structure of the application, find exploitable components, and plan further attacks such as Local File Inclusion (LFI) or Remote Code Execution (RCE).