ZAP by Checkmarx bwapp.scan

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
User Controllable HTML Element Attribute (Potential XSS)	Informational	4

Alert Detail

High	**SQL Injection - SQLite**
Description	SQL injection may be possible.
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	case randomblob(1000000) when not null then 1 else 1 end
Evidence	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.
Other Info	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
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

CWE Id	89
WASC Id	19
Plugin Id	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. * The victim is on the same local network as 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">
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">
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">
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">
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">
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">
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	352
WASC Id	9
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 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
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=A
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=M;O=D
Method	GET
Attack	
Evidence	Parent Directory
Other Info	
URL	https://bwapp.hakhub.net/stylesheets/?C=N;O=A
Method	GET
Attack	

Evidence	Parent Directory
Other 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	550
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/
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/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/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	
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 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=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	
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	
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	693
WASC Id	15

Plugin Id	10038

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>

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

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

Info	Web server identified: Apache 2
URL	https://bwapp.hakhub.net/stylesheets/?C=D;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=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	548
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	538
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

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	
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 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=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/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	
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	

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	55
Solution	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/jquery-1.4.4.min.js
Method	GET
Attack	
Evidence	jquery-1.4.4.min.js
Other Info	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/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/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
WASC Id	

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	10037

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/

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/
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=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/documents/?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/documents/?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/documents/?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/documents/?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/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	

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/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 or server error responses.
URL	https://bwapp.hakhub.net/images/favicon_drupal.ico
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/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.

URL	https://bwapp.hakhub.net/js/?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/js/?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/js/?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/js/?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/js/html5.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/jquery-1.4.4.min.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/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	693
WASC Id	15
Plugin Id	10021

Informational	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	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
Other Info	userParam=login userValue=oBDvlHECSqNnVCOH 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=PIyvKOnyOgyzHQff 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**
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	345
WASC Id	12
Plugin Id	10019

Informational	**GET for POST**

Description	A request that was originally observed as a POST was also accepted as a GET. This issue doe however, it may facilitate simplification of other attacks. For example if the original POST is subj may 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=PIyvKOnyOgyzHQff&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=oUlBxWFxUhZuzznA&login=yGDySAbKAjYAIKWC&mail_activation=&pas HTTP/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_c
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	10058

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	598
WASC Id	13
Plugin Id	10024

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://bwapp.hakhub.net/js/jquery-1.4.4.min.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "/*"}}, ajax:function(a){var b=c.extend(true,{},c.ajaxSettings,a),d,e,f,h=b.type.toUpperCase(),l=qb.test(h);b.url=b.url.replace(ub", see evidence field for the suspicious comment/snippet.
URL	https://bwapp.hakhub.net/js/json2.js
Method	GET
Attack	
Evidence	from
Other Info	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.
URL	https://bwapp.hakhub.net/js/xss_ajax_1.js
Method	GET
Attack	
Evidence	user
Other Info	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.
Instances	3

Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[615](615)
WASC Id	13
Plugin Id	[10027](10027)

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	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](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	
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
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=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=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/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	
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	
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	
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, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

	https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
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

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	10112

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

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://bwapp.hakhub.net/
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/
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/
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/
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/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

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
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/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	
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	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	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	[10031]()

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 https://bwapp.hakhub.net 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).