

Webanwendungsbericht

Dieser Bericht umfasst wichtige Sicherheitsinformationen zu Ihrer Webanwendung.

Sicherheitsbericht

Dieser Bericht wurde mit IBM Application Security Analyzer - dynamische Sicherheitsregeln erstellt; Version: 12395

Bitte beachten Sie:

Dieser Übersichtsbericht wurde mit dem Free Plan von Application Security Analyzer erstellt. Wenn Sie den vollen Service erwerben, haben Sie Zugriff auf einen vollständigen Bericht mit detaillierten Beschreibungen der gefundenen Probleme und Lösungen zu deren Behebung.

Inhaltsverzeichnis

Einführung

- Allgemeine Informationen
- Anmeldeeinstellungen

Zusammenfassung

- Problemtypen
- Sicherheitsrisiken
- WASC-Klassifizierung für Sicherheitsrisiken

Probleme nach Problemtyp sortiert

- Unverschlüsselte Anmeldeanforderung ①
- Cross-Site Request Forgery ②
- Sitzungs-ID nicht aktualisiert ①
- Unzulängliche Kontosperrung ①
- Auf SRI-Unterstützung (Subresource Integrity) prüfen ②
- Header "Content-Security-Policy" fehlt ⑤
- Header "X-Content-Type-Options" fehlt ⑤
- Header "X-XSS-Protection" fehlt ⑤

Anwendungsdaten

- Besuchte URLs
- Fehlgeschlagene Anforderungen

Einführung

Dieser Bericht enthält die Ergebnisse eines Sicherheitsscans einer Webanwendung, der von IBM Security AppScan Standard durchgeführt wurde.

Probleme mit hohem Schweregrad:	1
Probleme mit mittlerem Schweregrad:	4
Probleme mit niedrigem Schweregrad:	17
Gesamtzahl der in diesem Bericht aufgeführten Sicherheitsprobleme:	22
Gesamtzahl der in diesem Scan erkannten Sicherheitsprobleme:	22

Allgemeine Informationen

Scandateiname: chatsnap.eu-de.mybluemix.net

Testrichtlinie: Default (Staging)

Host chatsnap.eu-de.mybluemix.net

Port 0

Betriebssystem: Unbekannt

Web-Server: Unbekannt

Anwendungsserver: Beliebig

Anmeldeeinstellungen

Anmeldeverfahren: Automatisch

Gleichzeitige Anmeldungen: Aktiviert

JavaScript-Ausführung: Inaktiviert

Erkennung aktiver Sitzungen: Aktiviert

Muster zur Erkennung aktiver Sitzungen: >Sign Out<

Überwachte oder Sitzungs-ID-Cookies: connect.sid
io

Überwachte oder Sitzungs-ID-Parameter: sid









Anmeldesequenz: http://chatsnap.eu-de.mybluemix.net/
http://chatsnap.eu-de.mybluemix.net/login
http://chatsnap.eu-de.mybluemix.net/chat
http://chatsnap.eu-de.mybluemix.net/login
http://chatsnap.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=polling&t=L-wyyNq&sid=Taa-9CdkKjM6KNawAAAF
http://chatsnap.eu-de.mybluemix.net/socket.io/?

EIO=3&transport=polling&t=L-wyyQH.0&sid=Taa-9CdkKjM6KNawAAAF

Zusammenfassung







Problemtypen 8







TOC

Problemtyp	Anzahl der Probleme
H Unverschlüsselte Anmeldeanforderung	1 
M Cross-Site Request Forgery	2 
M Sitzungs-ID nicht aktualisiert	1 
M Unzulängliche Kontosperrung	1 
N Auf SRI-Unterstützung (Subresource Integrity) prüfen	2 
N Header "Content-Security-Policy" fehlt	5 
N Header "X-Content-Type-Options" fehlt	5 
N Header "X-XSS-Protection" fehlt	5 

Sicherheitsrisiken 6

TOC

Risiko	Anzahl der Probleme
H Benutzeranmeldedaten wie Benutzername und Kennwort können gestohlen werden, wenn diese unverschlüsselt versendet werden	1 
M Es kann möglich sein, Kundensitzungen und Cookies zu manipulieren oder zu stehlen, um damit die Identität eines legitimen Benutzers vorzutäuschen, sodass Hacker unter dieser falschen Identität Benutzerdaten anzeigen oder ändern und Transaktionen ausführen können.	3 
M Es könnte möglich sein, Benutzerberechtigungen zu eskalieren und Administratorberechtigungen über die Webanwendung zu erhalten	1 
N Wenn der Server des anderen Anbieters beeinträchtigt ist, ändert sich der Inhalt/das Verhalten der Site.	2 
N Es ist möglich, sensible Informationen zur Webanwendung, wie Benutzernamen, Kennwörter, Systemnamen und/oder sensible Dateispeicherorte abzurufen	15 
N Es ist möglich, einen naiven Benutzer zu überreden, sensible Daten wie Benutzername, Kennwort, Kreditkartennummer, Sozialversicherungsnummer usw. preiszugeben	15 

Risiko	Anzahl der Probleme	
Brute-Force-Angriff	1	
Cross-Site Request Forgery	2	
Informationsleck	15	
Remote File Inclusion	2	
Sitzungsfixierung	1	
Unzureichender Transportebenschutz	1	

Anwendungsdaten

Besuchte URLs 29

TOC

URL
http://chatsnap.eu-de.mybluemix.net/
http://chatsnap.eu-de.mybluemix.net/js/modernizr-2.6.2.min.js
http://chatsnap.eu-de.mybluemix.net/js/jquery.placeholder.min.js
http://chatsnap.eu-de.mybluemix.net/js/jquery.waypoints.min.js
http://chatsnap.eu-de.mybluemix.net/js/bootstrap.min.js
http://chatsnap.eu-de.mybluemix.net/js/main-boot.js
http://chatsnap.eu-de.mybluemix.net/js/delivery.js
http://chatsnap.eu-de.mybluemix.net/js/main.js
http://chatsnap.eu-de.mybluemix.net/js/jquery.min.js
http://chatsnap.eu-de.mybluemix.net/js/moment.js
http://chatsnap.eu-de.mybluemix.net/socket.io/socket.io.js
http://chatsnap.eu-de.mybluemix.net/login
http://chatsnap.eu-de.mybluemix.net/chat
http://chatsnap.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=L-wz2f7&sid=Ni0lzuCjfPVnm6OFAAAG
http://chatsnap.eu-de.mybluemix.net/logout
http://chatsnap.eu-de.mybluemix.net/js/modernizr-2.6.2.min.js
http://chatsnap.eu-de.mybluemix.net/js/main-boot.js
http://chatsnap.eu-de.mybluemix.net/js/jquery.placeholder.min.js
http://chatsnap.eu-de.mybluemix.net/js/jquery.waypoints.min.js
http://chatsnap.eu-de.mybluemix.net/js/jquery.min.js
http://chatsnap.eu-de.mybluemix.net/js/bootstrap.min.js
http://chatsnap.eu-de.mybluemix.net/js/main.js
http://chatsnap.eu-de.mybluemix.net/socket.io/socket.io.js
http://chatsnap.eu-de.mybluemix.net/js/moment.js
http://chatsnap.eu-de.mybluemix.net/js/delivery.js
http://chatsnap.eu-de.mybluemix.net/chat
http://chatsnap.eu-de.mybluemix.net/register
http://chatsnap.eu-de.mybluemix.net/login
http://chatsnap.eu-de.mybluemix.net/login

URL	Grund
http://chatsnap.eu-de.mybluemix.net/.navbar-collapse	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/.container-fluid	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/.navbar-collapse	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/.container-fluid	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/.navbar-collapse	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/.container-fluid	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/profile?file=	Antwortstatus '404' - Nicht gefunden
http://chatsnap.eu-de.mybluemix.net/downloadFile?username=	Zeitlimit