Webanwendungsbericht

Dieser Bericht umfasst wichtige Sicherheitsinformationen zu Ihrer Webanwendung.

Sicherheitsbericht

Dieser Bericht wurde mit IBM Application Security Analyzer - dynamische Sicherheitsregeln erstellt; Version: 16137

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

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

Probleme mit mittlerem Schweregrad:	1
Probleme mit niedrigem Schweregrad:	22
Probleme mit dem Schweregrad 'Nur zur Information':	3
Gesamtzahl der in diesem Bericht aufgeführten Sicherheitsprobleme:	26
Gesamtzahl der in diesem Scan erkannten Sicherheitsprobleme:	26

Allgemeine Informationen

Scandateiname: hsrtcloudchat.eu-de.mybluemix.net

Testrichtlinie: Default (Production)

Host	hsrtcloudchat.eu-de.mybluemix.net
Port	443
Betriebssystem:	Unbekannt
Web-Server:	Unbekannt
Anwendungsserver:	Beliebig

Host	hsrtcloudchat.eu-de.mybluemix.net
Port	443
Betriebssystem:	Unbekannt
Web-Server:	Unbekannt
Anwendungsserver:	Beliebig

Anmeldeeinstellungen

Anmeldeverfahren:	Aufgezeichnete Anmeldung
Gleichzeitige Anmeldungen:	Aktiviert
JavaScript-Ausführung:	Inaktiviert
Erkennung aktiver Sitzungen:	Aktiviert
Muster zur Erkennung aktiver Sitzungen:	`ok`
Überwachte oder Sitzungs-ID-Cookies:	`io`
Überwachte oder Sitzungs-ID-Parameter:	`sid`

Anmeldesequenz:

```
https://hsrtcloudchat.eu-de.mybluemix.net/
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=polling&t=MTR5wk_
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=polling&t=MTR5wnY&sid=XiOWx0dKfCNS1RO3AAAK
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=websocket&sid=XiOWx0dKfCNS1RO3AAAK
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=polling&t=MTR5-rG&sid=XiOWx0dKfCNS1RO3AAAK
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=polling&t=MTR6Afi&sid=RZG4TmO3ZW5GRpvKAAAM
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?
EIO=3&transport=polling&t=MTR6Dzi&sid=RZG4TmO3ZW5GRpvKAAAM
```

Zusammenfassung

Problemtypen 11

TOC

	Problemtyp	Anzahl der Probleme
M	Fehlendes sicheres Attribut in verschlüsseltem Sitzungs-Cookie (SSL)	1
N	Allzu tolerante CORS-Zugriffsrichtlinie	1
N	Auf SRI-Unterstützung (Subresource Integrity) prüfen	1
N	Header "Content-Security-Policy" fehlt oder unsicher	4
N	Header "X-Content-Type-Options" fehlt oder unsicher	4
N	Header "X-XSS-Protection" fehlt oder unsicher	4
N	HSTS-Header (HTTP Strict-Transport-Security) fehlt oder unsicher	4
N	HTML-Attribut 'autocomplete' wird für das Feld 'password' nicht inaktiviert	1
N	Verschlüsselung nicht erzwungen	3
N	Offenlegung sensibler HTML-Kommentare	1
N	SHA-1-Cipher-Suites wurden erkannt	2

Sicherheitsrisiken 7

TOC

	Risiko	Anzahl der Probleme
M	Benutzer- und Sitzungsdaten (Cookies)können gestohlen werden, wenn diese unverschlüsselt versendet werden	1
N	Es ist möglich, sensible Informationen zur Webanwendung, wie Benutzernamen, Kennwörter, Systemnamen und/oder sensible Dateispeicherorte abzurufen	18
N	Es ist möglich, einen naiven Benutzer zu überreden, sensible Daten wie Benutzername, Kennwort, Kreditkartennummer, Sozialversicherungsnummer usw. preiszugeben	17
N	Wenn der Server des anderen Anbieters beeinträchtigt ist, ändert sich der Inhalt/das Verhalten der Site.	1
N	Es kann möglich sein, die Authentifizierungsverfahren der Webanwendung zu umgehen	1
N	Sensible Daten wie Kreditkartennummern, Sozialversicherungsnummern usw. können gestohlen werden, wenn diese unverschlüsselt versendet werden	3
N	Es kann möglich sein, Kundensitzungen und Cookies zu manipulieren	2

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.

WASC-Klassifizierung für Sicherheitsrisiken

TOC

Risiko	Anzahl der Probleme
Fehlerhafte Serverkonfiguration	2
Informationsleck	23
Remote File Inclusion	1

Anwendungsdaten

Besuchte URLs 20

TOC

URL
https://hsrtcloudchat.eu-de.mybluemix.net/
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/socket.io.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io-stream.js
https://hsrtcloudchat.eu-de.mybluemix.net/client.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTR72ht
https://hsrtcloudchat.eu-de.mybluemix.net/client.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/socket.io.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io-stream.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTR73-Z
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTR74Hn&sid=bha6WC5SdXnvBY1aAAAZ
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTR72kG&sid=D9sZCT0VZAbEvg0TAAAY
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTR7SRL
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTR7STg&sid=ne4Tv1B3VgwjZyBtAAAc
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTRKxul
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/socket.io.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io-stream.js
https://hsrtcloudchat.eu-de.mybluemix.net/client.js
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTRKxxA&sid=qy1GQp7e67mI84gVAAYL
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTRL1WX&sid=qy1GQp7e67mI84gVAAYL
https://hsrtcloudchat.eu-de.mybluemix.net/socket.io/?EIO=3&transport=polling&t=MTRL24G&sid=qy1GQp7e67mI84gVAAYL

Fehlgeschlagene Anforderungen 0

TOC

URL	Grund