

# 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

- Allgemeine Informationen
- Anmeldeeinstellungen

## Zusammenfassung

- Problemtypen
- Sicherheitsrisiken
- WASC-Klassifizierung für Sicherheitsrisiken

## Probleme nach Problemtyp sortiert

- Fehlendes sicheres Attribut in verschlüsseltem Sitzungs-Cookie (SSL) ①
- Allzu tolerante CORS-Zugriffsrichtlinie ①
- Auf SRI-Unterstützung (Subresource Integrity) prüfen ①
- Header "Content-Security-Policy" fehlt oder unsicher ③
- Header "X-Content-Type-Options" fehlt oder unsicher ②
- Header "X-XSS-Protection" fehlt oder unsicher ②
- HSTS-Header (HTTP Strict-Transport-Security) fehlt oder unsicher ②
- Im Cache speicherbare SSL-Seite gefunden ①
- Verschlüsselung nicht erzwungen ①
- Weitergabe von Informationen über die Oracle-Protokolldatei ②
- SHA-1-Cipher-Suites wurden erkannt ①

## 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 mittlerem Schweregrad:	1
Probleme mit niedrigem Schweregrad:	15
Probleme mit dem Schweregrad 'Nur zur Information':	1
Gesamtzahl der in diesem Bericht aufgeführten Sicherheitsprobleme:	17
Gesamtzahl der in diesem Scan erkannten Sicherheitsprobleme:	17

## Allgemeine Informationen

**Scandateiname:** objective-euler.mybluemix.net

**Testtrichtlinie:** Default (Production)

**Host** objective-euler.mybluemix.net

**Port** 443

**Betriebssystem:** Unbekannt

**Web-Server:** Unbekannt

**Anwendungsserver:** Beliebig

**Host** objective-euler.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:

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

35

[illegible]

37

[illegible]

[illegible]



[illegible]

EIO=3&transport=polling&t=MTLQTIT&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTIh.0&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTIh&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTIv.0&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTIv&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTJ6.0&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTJ6&sid=cAKYeuRqSnuApl4cAAAB  
https://objective-euler.mybluemix.net/socket.io/?  
EIO=3&transport=polling&t=MTLQTLV&sid=cAKYeuRqSnuApl4cAAAB

# 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	3
N Header "X-Content-Type-Options" fehlt oder unsicher	2
N Header "X-XSS-Protection" fehlt oder unsicher	2
N HSTS-Header (HTTP Strict-Transport-Security) fehlt oder unsicher	2
N Im Cache speicherbare SSL-Seite gefunden	1
N Verschlüsselung nicht erzwungen	1
N Weitergabe von Informationen über die Oracle-Protokolldatei	2
N SHA-1-Cipher-Suites wurden erkannt	1



## Sicherheitsrisiken 6

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	13
N Es ist möglich, einen naiven Benutzer zu überreden, sensible Daten wie Benutzername, Kennwort, Kreditkartennummer, Sozialversicherungsnummer usw. preiszugeben	10
N Wenn der Server des anderen Anbieters beeinträchtigt ist, ändert sich der Inhalt/das Verhalten der Site.	1
N Sensible Daten wie Kreditkartennummern, Sozialversicherungsnummern usw. können gestohlen werden, wenn diese unverschlüsselt versendet werden	1
N 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	1

## WASC-Klassifizierung für Sicherheitsrisiken

TOC

Risiko	Anzahl der Probleme	
Fehlerhafte Serverkonfiguration	1	
Informationsleck	15	
Remote File Inclusion	1	

# Anwendungsdaten

## Besuchte URLs 25

TOC

URL
<a href="https://objective-euler.mybluemix.net/">https://objective-euler.mybluemix.net/</a>
<a href="https://objective-euler.mybluemix.net/socket.io/socket.io.js">https://objective-euler.mybluemix.net/socket.io/socket.io.js</a>
<a href="https://objective-euler.mybluemix.net/jquery_min.js">https://objective-euler.mybluemix.net/jquery_min.js</a>
<a href="https://objective-euler.mybluemix.net/bootstrap.min.js">https://objective-euler.mybluemix.net/bootstrap.min.js</a>
<a href="https://objective-euler.mybluemix.net/jquery.cssemoticons.min.js">https://objective-euler.mybluemix.net/jquery.cssemoticons.min.js</a>
<a href="https://objective-euler.mybluemix.net/main.js">https://objective-euler.mybluemix.net/main.js</a>
<a href="https://objective-euler.mybluemix.net/slider.less">https://objective-euler.mybluemix.net/slider.less</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTpeU">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTpeU</a>
<a href="https://objective-euler.mybluemix.net/bootstrap.min.js">https://objective-euler.mybluemix.net/bootstrap.min.js</a>
<a href="https://objective-euler.mybluemix.net/socket.io/socket.io.js">https://objective-euler.mybluemix.net/socket.io/socket.io.js</a>
<a href="https://objective-euler.mybluemix.net/jquery_min.js">https://objective-euler.mybluemix.net/jquery_min.js</a>
<a href="https://objective-euler.mybluemix.net/main.js">https://objective-euler.mybluemix.net/main.js</a>
<a href="https://objective-euler.mybluemix.net/jquery.cssemoticons.min.js">https://objective-euler.mybluemix.net/jquery.cssemoticons.min.js</a>
<a href="https://objective-euler.mybluemix.net/slider.less">https://objective-euler.mybluemix.net/slider.less</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTqv0">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTqv0</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTr1S&amp;sid=tvUm0KZ59KYVskOxAAAAI">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTr1S&amp;sid=tvUm0KZ59KYVskOxAAAAI</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTqvZ&amp;sid=tvUm0KZ59KYVskOxAAAAI">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLTqvZ&amp;sid=tvUm0KZ59KYVskOxAAAAI</a>
<a href="https://objective-euler.mybluemix.net/slider.less">https://objective-euler.mybluemix.net/slider.less</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLU0H_">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLU0H_</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLU0JQ&amp;sid=neRrPJmaUucXd9J0AAAL">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLU0JQ&amp;sid=neRrPJmaUucXd9J0AAAL</a>
<a href="https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLU0TC&amp;sid=neRrPJmaUucXd9J0AAAL">https://objective-euler.mybluemix.net/socket.io/?EIO=3&amp;transport=polling&amp;t=MTLU0TC&amp;sid=neRrPJmaUucXd9J0AAAL</a>
<a href="https://objective-euler.mybluemix.net/jquery_min.js">https://objective-euler.mybluemix.net/jquery_min.js</a>
<a href="https://objective-euler.mybluemix.net/bootstrap.min.js">https://objective-euler.mybluemix.net/bootstrap.min.js</a>
<a href="https://objective-euler.mybluemix.net/jquery.cssemoticons.min.js">https://objective-euler.mybluemix.net/jquery.cssemoticons.min.js</a>
<a href="https://objective-euler.mybluemix.net/main.js">https://objective-euler.mybluemix.net/main.js</a>

## Fehlgeschlagene Anforderungen 0

TOC

URL	Grund
-----	-------