Compass Security

Bedrohungen Web-Applikationen

27. Juli 2005

Name des Dokumentes:	bedrohungen_web_applikationen_v2.0.doc
Version:	V 2.0
Autor(en):	Walter Sprenger, Compass Security AG
Lieferungsdatum:	27. Juli 2005
Klassifikation:	ÖFFENTLICH

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

Inhaltsverzeichnis

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

1 Angriffe auf Web Applikationen

1.1 Einleitung

Das OWASP[1] (Open Web Application Security Project) hat gute Richtlinien erarbeitet für die sichere Entwicklung von Web Applikationen. Dieses Dokument baut auf diesen Empfehlungen auf und ist durch die Erfahrungswerte von Compass Security ergänzt worden. In Kapitel 2 werden Security Bedrohungen und dazugehörige Gegenmassnahmen aufgezeigt. Dieses Kapitel ist das Herz dieses Dokumentes und kann als Raster für ein Security Konzept verwendet werden.

1.2 Compass Security

Compass Security Network Computing AG (CSNC) ist eine Schweizer Firma, die im Februar 1999 durch Walter Sprenger und Ivan Buetler gegründet wurde. Compass Security hat sich von seit Beginn an mit "Security Assessments" beschäftigt und bietet dieses Know-How in Form von Penetration Tests und Security Reviews an. Seit 2004 werden auch zunehmend forensische Untersuchungen durchgeführt. Das Know-How wird in der Zusammenarbeit mit der FH Rapperswil und der HSW (Hochschule für Wirtschaft) im Fach „Informatik Sicherheit“ laufend erweitert.

1.3 Zielpublikum dieses Dokuments

Dieses Dokument ist in einer technische gehaltenen Sprache verfasst und setzt Kenntnisse über die Protokolle wie HTTP, HTTPS unter Berücksichtigung von Sessions, Cookies, Cookie Attribute etc. voraus.

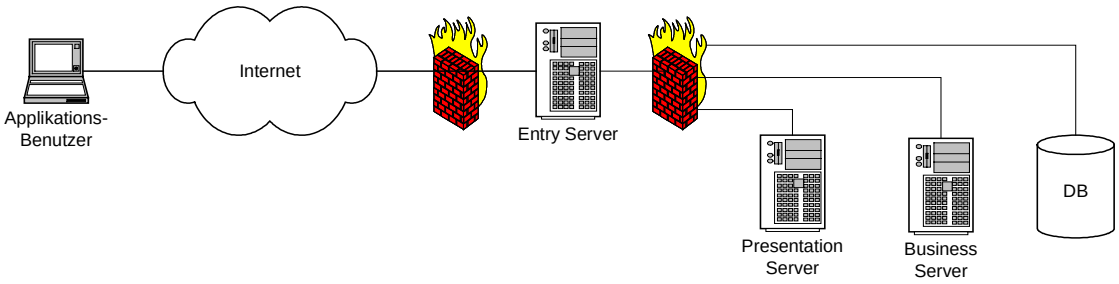
Das Zielpublikum dieser Checkliste sind Security Verantwortliche und Web Entwickler, damit diese eine Hilfestellung bei der Implementation von sicheren Webanwendungen haben.

[1] *OWASP: http://www.owasp.org/*

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

1.4 Bedeutung von Fachbegriffen



1.4.1 Entry Server

Ein Entry Server ist eine der Applikation vorgeschaltete Sicherheits-Komponente, welche eine Prüfung der Requests erlaubt. Beispiele für Entry Server sind: Reverse Proxy, Seclutions Airlock, IBM WebSeal, Tetrade SES, keyon TESS, AdNovum Easyweb

1.4.2 Presentation Server

Gemäss J2EE Standard ist der „Presentation Server“ eine Komponente, welche lediglich die Präsentation der Web Applikation durchführt, so wie dies in einer 3-Tier Architektur vorgesehen ist.

1.4.3 Business Server

Gemäss J2EE Standard ist der „Business Server“ eine Komponente, welche die Business Logik implementiert.

1.4.4 Phishing

Compass Security ist der Meinung, dass technisch gesehen lediglich ein Client Zertifikat als Schutz vor Phishing mit „Man in the Middle“ implementiert werden.

Challenge/Response Verfahren bei der Authentisierung erschweren Phishing Attacken, bei denen der Angreifer Teile der originalen Webseite durch gefälschte Seiten auf einem Fremdsystem anbietet.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

1.5 Web Application Security Lab

Die Ausbildung der Entwickler und Security Verantwortlichen von Webapplikationen ist sehr wichtig bei der Erstellung von sicheren Anwendungen. Der Compass „Application Security Lab“ Kurs geht in praktischer Form auf die Sicherheit von Webapplikationen ein. Während drei Tagen tauchen Sie in die Welt von Browser, Cookie, Sessions, Verschlüsselung und Entry Server ein. Ist es zum Beispiel möglich, dass ein Kunde des OnlineBanking auf Daten eines anderen Kunden zugreifen kann? Ist die Autorisierung, Datenisolierung und Session Handling sauber implementiert? Compass Security hat die grössten Fehler von Webapplikationen in einer **selbst entwickelten Webapplikation** eingebaut - die es während der Dauer des Kurses zu analysieren gilt. Viele praktische Übungen! Informationen dazu finden Sie unter folgendem Link:

http://www.csnc.ch/static/services/training/index.html

Die Kurse sind über ISACA Schweiz[2] erhältlich, oder direkt als Firmenkurs vor Ort.

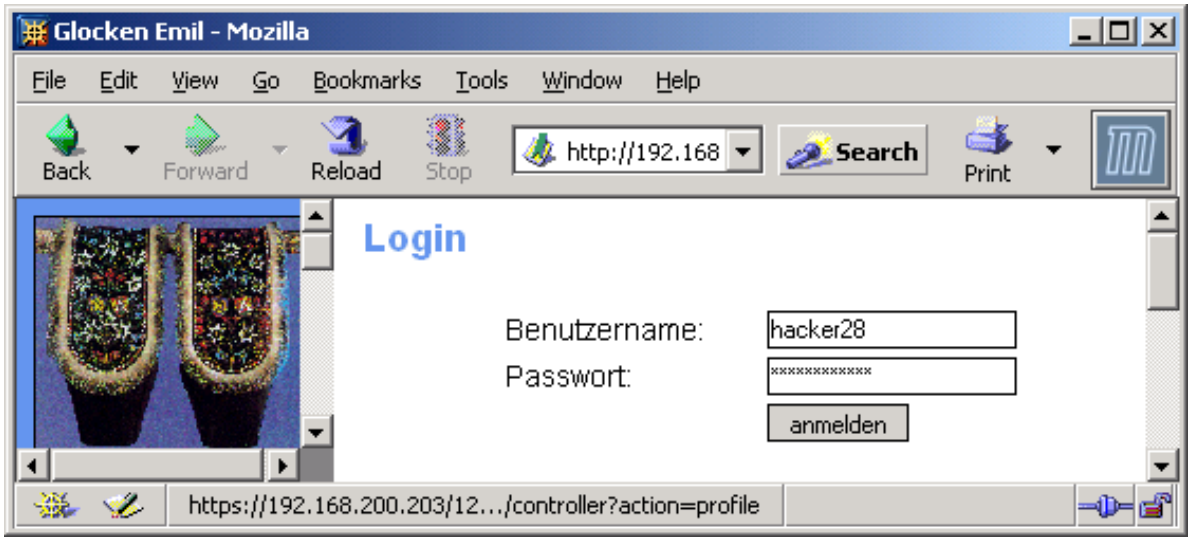


Abbildung: Lern Anwendung von Compass Security: SQL Injection

[2] *http://www.isaca.ch/*

2 Checkliste

Die folgende Checkliste zeigt Bedrohungen und Gegenmassnahmen auf, welche bei HTML basierten Anwendungen zu berücksichtigen sind.

2.1 Authentisierung

Nr.	Kategorie	Bedrohung	Gegenmassnahme
1	Authentisierung	Phishing mit kopierter Login Seite	• Challenge-Response Verfahren oder SSL Client Zertifikat
2	Authentisierung	Phishing mit Man in the Middle (Umleitung des Verkehrs über den Angreifer)	• SSL Client Zertifikat • Benutzer informieren
3	Authentisierung	Phishing durch Ausnützen von Redirection Schwächen (URL Redirection Attack)	• Redirect URL prüfen • nur auf die eigene Domain weiterleiten
4	Authentisierung	Benutzernamen Enumeration	• Fehlermeldung „Benutzername oder Passwort falsch“ anstatt „Benutzer ungültig“ oder „Passwort falsch“
5	Authentisierung	Benutzer aussperren	• Zeitverzögerung einbauen
6	Authentisierung	Schwache Passworte (Default Passworte, Policy beim Ändern des Passwortes)	• Starkes Passwort beim Passwort Wechsel erzwingen
7	Authentisierung	Schwächen in der Selbstregistrierung von Benutzern ausnützen	• Nur Gastrechte zuteilen • Autorisierung prüfen
8	Authentisierung	Umgehung der Authentisierung (z.B. Login mit Default oder Test Benutzername/ Passwort)	• Default und Testbenutzer löschen. • Entry Server muss prüfen, ob Benutzer authentisiert ist.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

2.2 Session Handling

Nr.	Kategorie	Bedrohung	Gegenmassnahme
9	Session Handling	Logout beendet nicht alle Sessions (Mit Back Button gelangt nachfolgender Benutzer wieder in authentisierte Bereiche)	• Logout Request mit POST absetzen. Server-seitig alle Sessions beenden und Cookies beim Benutzer löschen.
10	Session Handling	Session Prediction	• Generieren von eindeutigen und zufälligen, langen Session Identifikatoren
11	Session Handling	Session Fixation	• Nach einem erfolgreichen Login muss eine neue Session generiert werden falls zuvor schon eine erzeugt wurde • Session Identifikator darf nicht vom Client übernommen werden
12	Session Handling	Session Hijacking	• Verschlüsseln des Verkehrs • Zufällige Session Identifikatoren • Cookie Settings (secure Flag, HTTPOnly Flag) • Verhindern von CSS (Cross Site Scripting)
13	Session Handling	Session des Entry Servers, des Presentation Servers und des Business Servers müssen ein-eindeutig sein. Es darf keine Verwechslung geben da sonst ein Benutzer die Daten eines anderen Benutzers sieht.	• Sauberes Session Handling • Benutzerkontext muss auf jedem System eindeutig identifizierbar sein

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

2.3 Autorisierung

Nr.	Kategorie	Bedrohung	Gegenmassnahme
14	Autorisierung	Umgehung Autorisationprüfung auf Funktionen (mehr Rechte erlangen)	• Berechtigungen für Funktionen muss bei jedem Request server-seitig geprüft werden
15	Autorisierung	Umgehung Autorisationsprüfung auf Daten	• Berechtigungen für Daten muss bei jedem Request server-seitig geprüft werden

2.4 Input Validation

Nr.	Kategorie	Bedrohung	Gegenmassnahme
16	Eingabevalidierung	SQL Injection	• Technischer Datenbank User sollte minimale Rechte haben • Prepared Statements verwenden (Java Technik) • Eingabeprüfung
17	Eingabevalidierung	OS Command Injection	• Validieren der Eingaben • Keine direkten Betriebssystemaufrufe
18	Eingabevalidierung	LDAP Injection	• Validieren der Eingaben • Gefährliche Zeichen entfernen (z.B. Strichpunkt ;)
19	Eingabevalidierung	Cross Site Scripting (CSS / XSS)	• Validieren der Eingaben • Bei der Anzeige der Daten müssen diese HTML encodiert werden
20	Eingabevalidierung	Missbrauch von Mail-Funktionalität	• Empfänger müssen in der Applikation konfiguriert werden und dürfen nicht in den HTML Seiten definiert sein • SMTP Headers entfernen falls Mail an Kunde verschickt wird

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

Nr.	Kategorie	Bedrohung	Gegenmassnahme
21	Eingabevalidierung	Missbrauch von File Uploads (Upload in Applikationsverzeichnisse oder Modifikation von Webseiten, Upload von Viren, Upload falsch formatierter Dateien)	• Grösse beschränken • Dateitypen einschränken • Datei nicht auf Filesystem schreiben sondern direkt im Speicher verarbeiten • Wenn Datei auf Filesystem gespeichert wird: Einmalige Namen verwenden, Pfadinformationen entfernen und in Verzeichnis schreiben, das vom Internet her nicht erreichbar ist • Syntax der erwarteten Datei prüfen • Dateien auf Viren prüfen falls diese auf anderen Systemen verarbeitet werden (z.B. Excel, Word Dateien)
22	Eingabevalidierung	Codierungsschwächen ausnützen (z.B. doppelt codierte URLs werden vom Entry Server durchgelassen aber vom Backend Server interpretiert -> Directory Traversal)	• Request mit URL Encoding auf dem Entry Server einmal decodieren und dann Sicherheitsfunktionen anwenden. Falls doppeltes Encoding auftritt URL verwerfen
23	Eingabevalidierung / Konfiguration	Modifikation von Webseiten (Web-Authoring Funktionalität vorhanden oder Freitext Felder in z.B. Mitteilungsbrett)	• Validieren der Eingaben • Bei der Anzeige der Daten müssen diese HTML encodiert werden

2.5 Konfiguration

Nr.	Kategorie	Bedrohung	Gegenmassnahme
24	Konfiguration	Cross Site Tracing (XST)	• HTTP Methode TRACE und OPTIONS auf dem Webserver deaktivieren
25	Konfiguration	System Compromise (Zugriff auf einen Server: Authentisierung/EntryServer/Presentation/Business/Database)	• Server Software laufend auf dem aktuellsten Stand halten • Berechtigungen so restriktiv wie möglich (Prozess Benutzer darf nur Leserechte auf die Prozess Binaries und Konfigurationsdateien haben) • System mit Firewall voneinander trennen • Evtl. Chroot verwenden

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

Nr.	Kategorie	Bedrohung	Gegenmassnahme
26	Konfiguration	Administrationsinterfaces vom Internet her erreichbar	• Administrations-Interfaces dürfen nicht vom Internet erreicht werden können. Separaten Webserver auf anderem Port oder mindestens Einschränkung basierend auf IP-Adresse und starke Authentisierung
27	Konfiguration	Fehler und Funktionalität in Beispiel Seiten ausnützen	• Test, Beispiel und Demo Seiten entfernen
28	Konfiguration	Zugriff auf Dateien ausserhalb Web-Applikation (z.B. Zugriff auf Konfiguration oder Schlüsselmaterial aufgrund zu wenig restriktiver Berechtigungen)	• Restriktive Konfiguration von Webserver und Servlet-Engines. Zugriff nur auf benötigte Dateien/ Verzeichnisse zulassen.
29	Konfiguration	Zugriff auf Demo/Test-Umgebung und dadurch Zugriff auf produktive Daten	• Test-Umgebungen dürfen nur von bestimmten IP-Adressen erreicht werden können • In den Demo und Testumgebungen dürfen keine produktiven Daten vorkommen
30	Konfiguration	Zugriff auf Backup-Files auf dem produktiven Server	• Alle Dateien, welche für den Betrieb nicht direkt benötigt werden sollen entfernt werden
31	Konfiguration	Zugriff auf unverschlüsselte Passworte in Konfigurationsdateien	• Alle Passwort, welche auf den Systemen gespeichert werden, müssen verschlüsselt sein
32	Konfiguration	Zugriff auf Standard URL (z.B. /script /admin /backup /WEB-INF /snoop.jsp /test.html)	• Entfernen aller Standardverzeichnisse • Schützen der Verzeichnisse, damit nicht vom Internet zugegriffen werden kann • Sensitive Informationen aus den Verzeichnissen entfernen
33	Konfiguration	Daten respektive HTML Seiten werden im Cache des Browsers gespeichert und können durch einen nachfolgenden Benutzer eingesehen werden.	• Header setzen, welche den Browser anweisen die Seiten nicht zu speichern. „Pragma: no-cache“ „Cache-Control: no-cache, no-store“

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

2.6 Logging

Nr.	Kategorie	Bedrohung	Gegenmassnahme
34	Logging	Sensitive Informationen in Logfiles (z.B. Sessions oder Passwörter in Logfiles)	• Keine sensitiven Informationen in Logdateien schreiben • Logdateien schützen, dürfen nie vom Internet erreichbar sein
35	Logging	Angriffe werden nicht erkannt	• Applikationen sollen alle Anfragen und Tätigkeiten in Logdateien protokollieren • Die Logdateien müssen automatisch verarbeitet werden können (Parsen nach kritischen Einträgen)
36	Logging	Fehlende Logeinträge für forensische Untersuchungen (kein Nachweis was ein Benutzer gemacht hat)	• Alle Logdateien müssen miteinander korreliert werden können (vom Entry Server bis zur Datenbank)

2.7 Error Handling

Nr.	Kategorie	Bedrohung	Gegenmassnahme
37	Fehlerbehandlung	Fehlerbehandlung zu sprechend (Fehlermeldungen verraten interne Informationen oder geben dem Angreifer Hilfestellungen was auf dem Backend falsch läuft)	• Eigene Fehlerseiten erstellen und alle Standard-Fehlerseiten ersetzen
38	Fehlerbehandlung	Manipulationen am URL, an Form Feldern oder Cookie Werten	• Zugriffskontrolle bei allen Parametern durchführen • Wertebereiche prüfen

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch

2.8 Sonstiges

Nr.	Kategorie	Bedrohung	Gegenmassnahme
39	Schutz der Daten	Information Disclosure (Versionen, Produkte, Entwicklernamen, Source Code, Konfigurationen sichtbar)	• Keine versteckten Informationen in HTML/CSS Seiten • Nur benötigte Seiten/Servlets auf dem Server • Kein Zugriff auf Source Code / Class Files und Konfigurationsverzeichnisse • In allen Produkten Default Fehlermeldungen durch eigene Seiten ersetzen • Deaktivieren von Stack Traces
40	Verschlüsselung	Verkehr belauschbar weil nicht verschlüsselt	• Jeglichen Verkehr mit SSL verschlüsseln • Secure Flag beim Cookie setzen
41	Funktionalität	Belauschen von sensitiver Information welche per Email verschickt wird	• Keine sensitiven Informationen in Emails verschicken. (Text z.B. Neue Informationen in ihrem Online Banking Bereich)

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch www.csnc.ch