sr solutions

Dateiupload und Sicherheit

Warum zentrale Services sicherheitsrelevant sind

ILIAS Conference | 6. September 2024 | Graz

Übersicht über gängige Webdienst-Exploits

- Remote Code Execution: Exploiter können Befehle auf dem Server ausführen.
- File Inclusion: Schaden an Dateien durch unerwünschte Einbindung von Dateien.
- Cross-Site Scripting (XSS): Einschleichen von bösartigem JavaScript in Webseiten, um Angreifer Zugang zu Cookies und anderen sensiblen Daten zu gewinnen.
- SQL Injection: Manipulation von SQL-Abfragen zur Informationsteilung oder zum Datenbankangriff.

Remote Code Execution

- Beschreibung: Ein Exploit, der es ermöglicht, Befehle auf dem Server auszuführen.
- Schritte: Datei hochladen, die das Skript enthält; Ausnutzen einer Sicherheitslücke in der Webanwendung.
- Folgen: Virendiskussion, Datenverlust, Dienstunterbrechung.

File Inclusion

- Beschreibung: Ein Exploit, bei dem eine Datei unerwartet eingebunden wird.
- Schritte: Angreifer lädt schädliche PHP-Dateien hoch; Webanwendung liest und interpretiert die Datei als Teil einer Seite.
- Folgen: Offenlegung sensibler Informationen, Kompromittierung der Datenbank, Serverüberlastung.

Cross-Site Scripting (XSS)

- Beschreibung: Ein Exploit, bei dem bösartiges JavaScript in eine Webseite eingebettet wird.
- Schritte: Angreifer fügen schädliches Skript ein; Benutzer, die die manipulierte Seite besuchen, erhalten das Skript im Kontext ihrer Sitzung.
- Folgen: Cookie-Klauen, Session Hijacking, Persistenz von Schadsoftware auf dem System des Opfers.

SQL Injection

- Beschreibung: Ein Exploit, bei dem ein Angriff die eingehenden SQL-Abfragen manipuliert.
- Schritte: Angreifer fügt Schadcode in Eingabefeldern ein; Webanwendung interpretiert den Code als Teil einer SQL-Anweisung, was zu fehlerhaften Ergebnissen und möglicherweise sensiblen Informationen führt.
- Folgen: Datenbankkompromittierung, Offenlegung vertraulichen Datenmaterials, Beeinträchtigung der Integrität von Transaktionen.

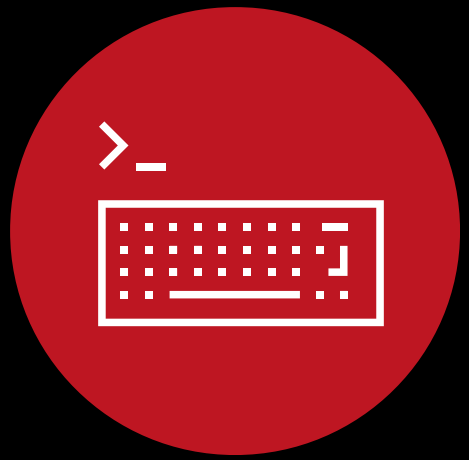
Live Hacks statt Life Hacks

- Technische Vorbedingungen
  - ILIAS 6 (nicht mehr supported)
  - Verschiedene Patches, um Security-Fixes wieder rückgängig zu machen
  - Patches, um zentrale Security-Mechanismen auszuschalten
  - Deaktivierter WebAccessChecker

- Rahmenbedingungen
  - Login muss möglich sein
  - Genügend Rechte in ILIAS, um verschiedene Objekte anlegen zu können

sr solutions

Live Hacks statt Life Hacks



sr solutions

Was hilft?

- Zentralisierung
- Security by Design

Danke für die Aufmerksamkeit

Fabian Schmid

fabian@sr.solutions

https://sr.solutions