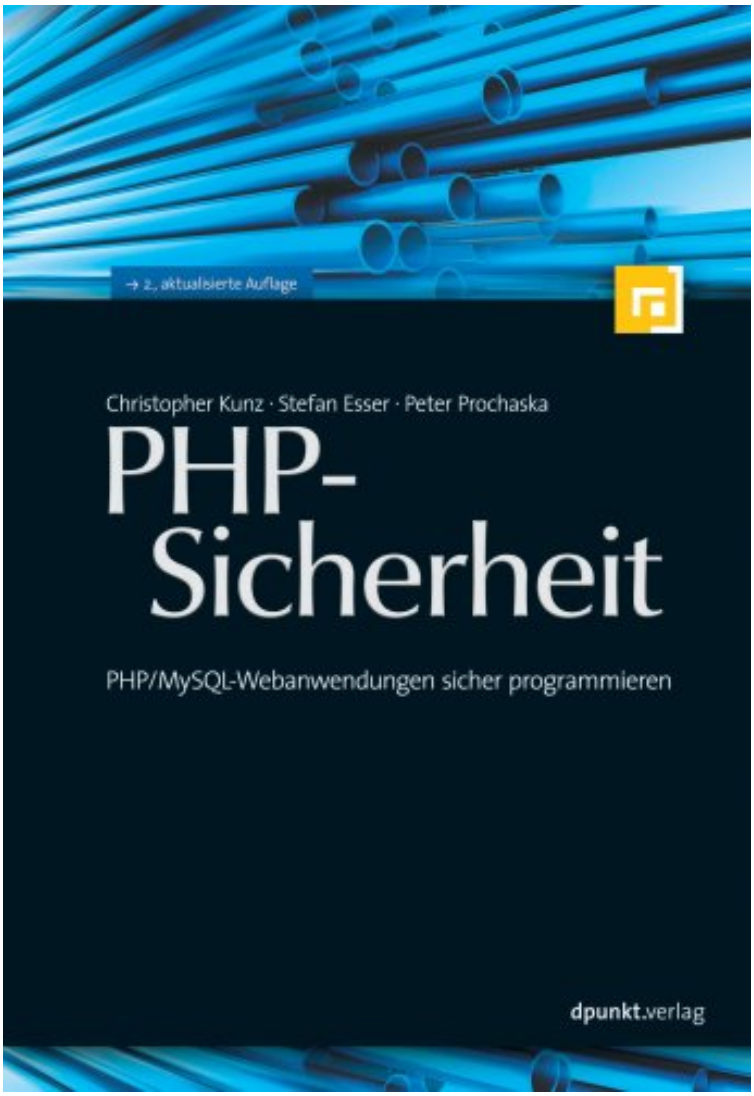
# PHP-Sicherheit: PHP/MySQL-Webanwendungen sicher programmieren

*Von Christopher Kunz, Peter Prochaska, Stefan Esser*
**Download PDF | ePub | DOC | audiobook | ebooks*






Produktinformation -Verkaufsrang: #437863 in BcherVerffentlicht am: 2007Einband: Taschenbuch321 Seiten | File size: 60.Mb

**Von Christopher Kunz, Peter Prochaska, Stefan Esser : PHP-Sicherheit: PHP/MySQL-Webanwendungen sicher programmieren** before purchasing it in order to gage whether or not it would be worth my time, and all praised PHP-Sicherheit: PHP/MySQL-Webanwendungen sicher programmieren:

KundenrezensionenHilfreichste Kundenrezensionen23 von 24 Kunden fanden die folgende Rezension hilfreich. PHP-Sicherheit 2. AuflageVon Pelle BoeseDie aktualisierte zweite Auflage des Buches von Christopher Kunz und Peter Prochaska, die ber 50 Seiten mehr als die erste Auflage bietet, ist eine lohnende - in meinen Augen sogar dringend

notwendige - Anschaffung fr PHP Entwickler und Systemadministratoren, aber auch fr Entwickler die mit anderen Sprachen im Web-Bereich arbeiten. Besonders die Kapitel ber Parametermanipulation, Cross-Site-Scripting und SQL-Injections sind, bis auf die Beispiele in PHP, sprachbergreifend.Die wichtigsten Neuerungen in der zweiten Auflage sind- PHP5: Neue Features und Konfiguration- Ein Kapitel ber die Vor- und Nachteile von ext/filter- Das Kapitel zum Hardening- bzw. Suhosin-Patch wurde komplett berarbeitet von Security-Guru Stefan Esser, der nun als Co-Autor mit ins Boot genommen wurde. Somit gleicht die Liste der Autoren des Buches nun der des Hardened-PHP Projektes.- mod_security 2.0: nderungen und Probleme- mod_parmguard als Whitelisting-Modul fr Apache- Neue XSS-Attacken, XSS-Filter und Attack APIDas Buch eignet sich fr den geneigten Leser als Nachschlagwerk beim Entwickeln oder um einfach mal die beschriebenen Angriffe und Konfigurationstipps auszuprobieren und nachzuvollziehen. Auch als Bettlektre ist es nicht zu verachten, da es sich sehr gut liest und mehr Flietext als Code enthlt. Das Hauptaugenmerk liegt hier auf der Vermittlung von professionellem Wissen aus dem Bereich Web-Security und nicht auf Code-Beispielen.Die Zielgruppe des Buches sind alle PHP-Entwickler, vom Anfnger bis zum Profi. Finden wird hier jeder etwas ihm bis dato unbekanntes. Ausserdem ist das Buch eine hervorragende Hilfe bei der Konfiguration von PHP sowie dem Hardening-Patch / Suhosin und diverser Erweiterungen und Module.Meiner Meinung nach ist dieses Buch die Referenz im PHP-Security-Bereich. Die vollstndige bersicht ber mgliche Attacken und Prventionsmglichkeiten gibt es - meines Erachtens nach - nirgends sonst in einem Buch vereint. Ein Must-Have, auch fr stolze Besitzer der ersten Auflage.6 von 6 Kunden fanden die folgende Rezension hilfreich. Von Grund auf sichere PHP-Anwendungen erstellenVon Lars H. KorteDas Buch sollte mir einen kleinen Einblick in die Welt der PHP-Sicherheit geben. Ich war neugierig, was es fr Mglichkeiten gibt, in PHP-Anwendungen einzubrechen und wie ich meine Anwendungen gegen "bse Buben und Mdels" schtzen kann.Ich muss sagen, dass ich bei weitem nicht gedacht htte, wie viele Angriffsmglichkeiten und Schwachstellen es heutzutage geben kann (Session Fixation, Cross-Site Request Forgery, SQL-Injection, uvm.). Das Buch hat mir sehr geholfen, meinen Horizont in dieser Hinsicht zu erweitern.Es werden eine Menge Angriffsmglichkeiten erklrt und ein mglicher Schutz dagegen erlutert. Bei einigen Angriffsarten waren mir die Gedankengnge der Autoren ab und zu leider etwas zu abstrus bzw. zu theoretisch erklrt und nur schwer nachvollziehbar. Bei einigen Angriffen wurde gezeigt, welchen Code man braucht, um zu "hacken" und bei anderen wurde leider nur theoretisch beschrieben, wie "Schadcode" eingeschleust werden kann. Hier htte ich gerne auch noch ein handfestes Praxis-Beispiel gesehen, da in mir leider nicht so viel kriminelle Energie schlummert, als dass ich mir sowas selbst ausdenken knnte :-)Die Anschaffung des Buches hat fr mich zu 100% gelohnt und ich kann es ohne schlechtes Gewissen wrmstens weiterempfehlen!3 von 3 Kunden fanden die folgende Rezension hilfreich. DAS Buch zum Thema SicherheitVon Michael KarlIch habe mir das Buch mit Hoffnung auf eine umfassende Lektre zum Thema Sicherheit mit PHP Mysql Anwendungen gekauft. Diese Hoffnungen - und Erwartungen - wurden vollstndig erfllt.Das Buch richtet sich sowohl an Anfnger wie auch an Profis, da der Schreibstil klar und eindeutig und sehr leicht verstndlich ist.Der Inhalt verfolgt eine klare Linie. Die Autoren fhren den Leser somit durch das komplette Thema ohne sich in Details aufzuhngen, oder wichtiges zu vergessen. Zudem hngt sich das Buch nicht an irgendwelchen Codebeispielen auf, sondern zeigt nur die wichtigen Codeschnipsel.Ich lege dieses Buch jedem PHP Entwickler nahe, da man das Thema Security nicht verachten darf! Die ca. 300 Seiten sind komplett mit Wissen gefllt und nicht wie so oft mit unwichtigen Details vollgestopft.Ein Buch mit viel Praxis, von dem man was lernen kann...

Produktbeschreibung2007 Ill., graph. Darst. PHP 5.0; Datensicherung; DDC-Notation 005.133 [DDC22ger]; Sachgruppe(n) 004 Informatik kart. 24 cm Heidelberg XV, 321 S. [Varia/Modern 004 Informatik ]

RezensionAbsolute Sicherheit gibt es nicht. Aber bekannte Fehler lassen sich vermeiden. Diese Grundregel gilt auch fr PHP -- Paranoia hilft nicht weiter, aber Nachlssigkeit ist Selbstverschulden -- Christopher Kunz, Peter Prochaska und Stefan Esser schlieen mit der 2., aktualisierten und erweiterten Auflage ihres PHP-Sicherheit-Buchs fr viele engagierte PHP-Programmierer eine Wissenslcke und zeigen praktisch und leicht umsetzbar, wie sich PHP-basierte Webanwendungen gezielt absichern lassen, woher Gefahren drohen und welche Regeln zu beachten sind. Fr viele Hobby- aber auch Profi-Webentwickler stand und steht bei PHP die einfache Umsetzung bei gleichzeitig ungeschlagener Leistungsfhigkeit im Vordergrund. Fragen zur Sicherheit ergaben sich erst im Laufe der Zeit, vor allem durch die groe Verbreitung. Wie nun also "nachtrglich" Sicherheit "einbauen"? Was kann denn eigentlich passieren? Und was gilt es bei zuknftigen PHP/MySQL-Projekten zu beachten? Kunz, Prochaska und Esser haben die 320 Seiten ihres PHP-Buchs auf den neusten Stand gebracht und die Version 5.2.0 angepasst und um Themen wie die PHP-Erweiterungen zur Filterung von Eingabedaten erweitert. Damit bieten sie Einstieg, bersicht und konkrete Lsungen und richten sich sowohl an Entwickler und Administratoren, die nachtrglich bestehende PHP-Projekte sicherheitsrelevant berarbeiteten als auch an Programmierer, die neue Anwendungen vorneweg "hrten" wollen. Dabei setzen sie fr PHP/MySQL relevante Administratorenkenntnisse und natrlich praktisches Wissen rund um datenbankbasierte PHP-Anwendungen voraus. Die Themen umfassen nach einer Einleitung zu Begriffen, Quellen und Hintergrnden etwa die Informationsgewinnung, Parametermanipulation, Cross-Site Scripting, SQL-Injection, Autorisierung und Authentisierung, Sessions, Upload-Formulare, Variablenfilter mit ext/filter, PHP intern und PHP-

Hardening bis hin zu Webserver-Filter fr Apache. Die Kapitel beginnen meist mit einer Starterklrung, es folgen Beispiele, Lsungen und am Ende ein Fazit. Im Anhang dann noch eine Checkliste, eine Liste aller Schwachstellen mit Gefahrenpotenzial-Bewertung sowie ein Glossar und ein Stichwortverzeichnis. Kunz und Prochaska zitieren in PHP-Sicherheit Security-Guru Bruce Schneier mit den Worten "Security is a process, not a product." -- das Motto passt auf ihr Buch wie gegossen, denn sie vermitteln Sicherheit nicht als Hindernis oder Erschwernis, sondern als Teil des PHP-Datenbank-Ganzen. Ein "Must-have" fr alle PHP-Programmierer, die sich und ihre Arbeit ernst nehmen. --Wolfgang TreKurzbeschreibungPHP gilt mittlerweile als die beliebteste Skriptsprache fr Webanwendungen. Leider werden Sicherheitsaspekte bei der PHP-Entwicklung oft vernachlssigt. Dies fhrt leicht zu massiven Sicherheitsproblemen und ist dann fr kompromittierte Server und verunstaltete Webseiten verantwortlich. Wie man solche Risiken erkennen und abwehren kann, zeigt dieses Buch.An nachvollziehbaren Beispielen lernen die Leser alle wichtigen Gefahren kennen, u.a.:- SQL-Injection- Cross-Site Scripting- Angriffe gegen Sessions- Angriffe auf Upload-Formulare- Cross-Site Request Forgery- HTTP Response SplittingDarauf aufbauend vermitteln die Autoren effiziente Vorbeugungs- und Gegenmanahmen, z.B.: - Sichere Konfiguration von PHP- Filterung von Web-Angriffen- Richtige berprfung von Variablen- Blacklist-/Whitelist-Prfungen- Absichern von PHP mit SuhosinDie Leser lernen, welche Fehler sie bei der Umsetzung ihrer Ideen in PHP vermeiden sollten. Auerdem knnen sie anhand der im Buch genannten "Best Practices" ihren eigenen Programmierstil kritisch berprfen und schnell in die Fehlersuche einsteigen. Die Checkliste im Anhang bietet eine Anleitung fr Code Audits und fr die Absicherung von Projekten.Die dritte Auflage wurde grndlich berarbeitet, aktualisiert und an aktuelle Neuerungen in der PHP-Welt angepasst.Stimmen zur ersten Auflage:Dieser Titel bietet eine grndliche Abhandlung, die jeder gelesen haben sollte, bevor er PHP-Skripte auf ffentlichen Webservern installiert. Selbst erfahrene PHP-Programmierer finden hier noch wertvolle Hinweise und konkrete Lsungen. Linux-MagazinEine lohnende Investition fr jeden, der sich ernsthaft mit der Entwicklung von PHP-Anwendungen beschftigt. phpforumKlappentextPHP gilt mittlerweile als die beliebteste Skriptsprache fr Webanwendungen. Leider werden Sicherheitsaspekte bei der PHP-Entwicklung oft vernachlssigt. Dies fhrt leicht zu massiven Sicherheitsproblemen und ist dann fr kompromittierte Server und verunstaltete Webseiten verantwortlich. Wie man solche Risiken erkennen und abwehren kann, zeigt dieses Buch. An nachvollziehbaren Beispielen lernen die Leser alle wichtigen Gefahren kennen, u.a.: - SQL-Injection - Cross-Site Scripting - Angriffe gegen Sessions - Angriffe auf Upload-Formulare - Cross-Site Request Forgery - HTTP Response Splitting Darauf aufbauend vermitteln die Autoren effiziente Vorbeugungs- und Gegenmanahmen, z.B.: - Sichere Konfiguration von PHP - Filterung mit mod_security - Richtige berprfung von Variablen - Blacklist-/Whitelist-Prfungen - Prepared Statements / Stored Procedures - Captchas Die Leser lernen, welche Fehler sie bei der Umsetzung ihrer Ideen in PHP vermeiden sollten. Auerdem knnen sie anhand der im Buch genannten "Best Practices" ihren eigenen Programmierstil kritisch berprfen und schnell in die Fehlersuche einsteigen. Die Checkliste im Anhang bietet eine Anleitung fr Code Audits und fr die Absicherung von Projekten, sowohl bei neu konzipierten als auch bei bereits fertig gestellten Programmen. Vorausgesetzt werden Erfahrungen mit datenbankbasierten PHP-Anwendungen sowie grundlegende Kenntnisse in der Administration von Unix- bzw. Windows-Systemen.