

## Sicherheit von Webanwendungen

Hintergrund 25.01.2007 12:33 Uhr – Christiane Rütten, Tobias Glemser

**Besonders anfällig für Angriffe auf Webserver sind mit PHP oder anderen Skriptsprachen geschriebene Webanwendungen. Wer jedoch die gängigen Sicherheitslücken und Angriffstechniken kennt, kann den Attacken die Stirn bieten.**

Unterthema: Das PHP-Dilemma

Unterthema: Die wichtigsten

Sicherheitsoptionen in der php.ini

Die Sicherheit von Webanwendungen geht keineswegs nur die Betreiber von Online-Shops und Banking-Portalen an. Vielmehr sind zunehmend auch kleinere oder privat betriebene Websites das Ziel böswilliger Angreifer aus dem Internet. Nicht unbedingt, weil es da Geld oder geheime Daten zu holen gäbe, sondern um den gekaperten Server für eigene Zwecke zu missbrauchen. Dort kann man dann raubkopierte Software archivieren und tauschen, verteilte Denial-of-Service-Angriffe vorbereiten oder Spam-Mails verschicken. Oder der Angreifer manipuliert die Webseiten, um Besucher mit Dialern oder Spyware zu infizieren.

### INHALTSVERZEICHNIS

1. Sicherheit von Webanwendungen
  2. Remote Code Execution
  3. Weiße Weste
  4. Das PHP-Dilemma
  5. Die wichtigsten Sicherheitsoptionen in der php.ini
- » Auf einer Seite lesen





### Dienste

[Security Consultant](#)[Emailcheck](#)[Netzwerkcheck](#)[Browsercheck](#)[Anti-Virus](#)[Krypto-Kampagne](#)

Anzeige

### Alerts!

[alle Alert-Meldungen »](#)

-  **Grub2 BootHole**
-  **Magento Commerce 2 / Open Source 2 (alle Plattformen)**
-  **Cisco-Produkte**
-  **WordPress wpDiscuz**

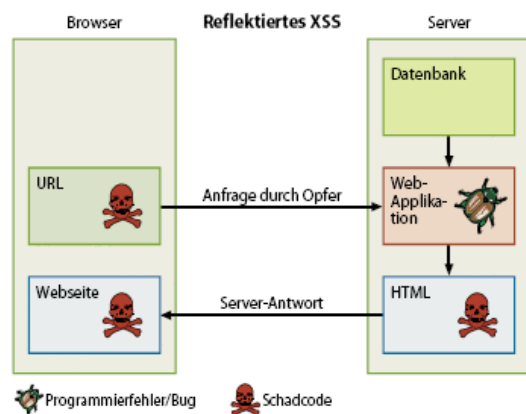
### Online-Konferenz: IT-Sicherheitstag



Wer seinen Server selbst administriert, also beispielsweise einen "Root-Server" betreibt, muss sich natürlich darum kümmern, diesen aktuell zu halten und auftretende Sicherheitslücken zu schließen. Doch auch wer nur ein bisschen Webspace angemietet hat, um seinen Freunden die selbst geschossenen Fotos zu zeigen, ist möglicherweise angreifbar. Ob Bildgalerie, Blog oder Gästebuch – jegliche Art von dynamischem Inhalt, sei er in PHP, Perl, Ruby oder sonst einer Sprache programmiert, ist ein potenzielles Einfallstor.

## Cross Site Scripting

Die verbreitetste Angriffsform ist das sogenannte Cross Site Scripting (XSS). Dabei versucht ein Angreifer, die Webanwendung so zu manipulieren, dass sie schädlichen Skriptcode in die beim Besucher angezeigte Seite einbettet. Der Browser verarbeitet dann den eingeschmuggelten Code, als wäre es ein legitimer Inhalt der Webseite – mit den entsprechenden Sicherheitsfreigaben. Mit dem eingebetteten Schadcode kann ein Angreifer dann beispielsweise falsche Informationen als Inhalte der angegriffenen Webseite verkaufen, um Passwörter oder Kontodaten zu erbeuten (Phishing).



Die fehlerhafte Webapplikation bettet den Schadcode aus der URL in ihre Ausgabe ein und "reflektiert" ihn zum Anwender zurück.

Man unterscheidet drei Haupttypen von XSS, und zwar je nachdem, auf welchem Weg der Schadcode in die im Browser angezeigte Webseite gelangt. Am häufigsten ist das sogenannte reflektierte XSS anzutreffen. Hierzu muss der Angreifer das Opfer dazu bringen, eine präparierte URL anzuklicken. In Variablenparametern dieser URL versteckt er dabei Code, den die fehlerhafte Anwendung auf Serverseite übernimmt und als vermeintlichen Usernamen, E-Mail-Adresse oder Suchausdruck in die Webseite einbettet. Fast alle von der Hacker-Gruppe Electrical



## Neue Cyberangriffe - Wie können Unternehmen sich schützen - Kritische Infrastrukturen & Industrie 4.0 im Fokus

Der IT-Sicherheitstag findet dieses Jahr zum ersten Mal online statt und ist eine Mischung aus Konferenz und Plattform zum Erfahrungsaustausch und Netzwerken. Neben der Notwendigkeit von Cyberabwehrmaßnahmen werden auch verschiedene Konzepte und Vorgehensweisen zur Sicherung der unternehmensinternen IT- und Prozessnetze dargelegt.

### Anzeige

Corona & Phishing: Bieten Sie Hackern die Stirn!  
Zero Trust: Null Vertrauen, aber voll zufrieden  
Container- und Serverless-Umgebungen absichern  
Risk-based Vulnerability Management – jetzt!  
SAP Cloud Platform: Merkmale und Fallbeispiele  
Wie KI den Alltag von Netzwerkadmins erleichtert  
So schützen Sie Ihre Mitarbeiter überall!  
Zeit zu handeln: Jetzt auf S/4HANA umsteigen  
Webcast: So wird Ihr RZ zukunftssicher!  
In 5 Schritten zur modernen IT-Infrastruktur

Ordered Freedom auf der Website Phishmarkt gezeigten Beispiele bei Webpräsenzen von Banken und Institutionen sind aktuell und von diesem Typ [4].

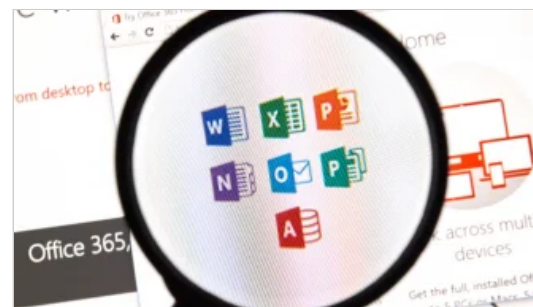
Ebenfalls weit verbreitet ist das persistente oder beständige XSS. Ähnlich dem reflektierten XSS spielt der Server den Schadcode aus der URL als Webinhalt an den Browser zurück, doch diesmal mit einem Zwischenstopp in der Serverdatenbank. Dadurch liefert der Server den Schadcode unter Umständen auch an Anwender aus, die nicht auf einen manipulierten Link geklickt haben – man denke etwa an Forenbeiträge mit eingebettetem JavaScript-Code. Bei diesem Typ ist es in der Regel der Angreifer, der einmalig auf einen manipulierten Link klickt, um den Schadcode auf dem Server abzuladen.

Bei reflektiertem und persistentem XSS läuft der fehlerhafte Programmcode, der den Schadcode letztlich einbettet, auf dem Server. Wenn sich im Gegensatz dazu der gesamte Angriff vom Klicken einer manipulierten URL bis zum Einbetten des Schadcodes in die Webseite auf dem Rechner des Anwenders abspielt, spricht man von lokalem XSS. Dieser dritte Haupttyp tritt insbesondere bei Web-2.0-Anwendungen auf, die einen erheblichen Teil der Applikationsfunktionen als Java- oder JavaScript-Code in den Browser des Anwenders verlagern.

Landet der Schadcode zunächst einmal in der Serverdatenbank, müssen Opfer gar nicht erst auf einen manipulierten Link klicken.

Das baumartige Document Object Model (DOM), das im Webbrowser die komplette Webseite repräsentiert, spielt dabei eine besondere Rolle, daher auch die Bezeichnung "DOM-basiertes XSS". Über Zugriffe auf den DOM-Baum kann eine

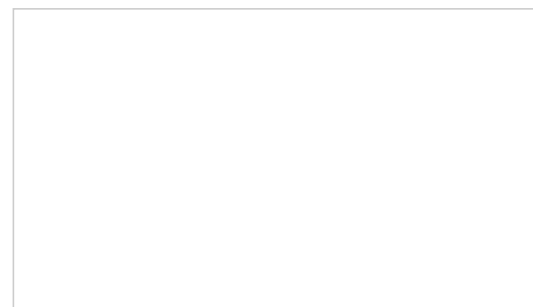
## Artikel



### Microsoft und Emotet: Makroschutz in Office 365 nur für Konzerne

Angeblich kann man das Ausführen der gefährlichen Emotet-Makros mit Gruppenrichtlinien firmenweit abschalten. Doch dieser Schutz hat riesige Lücken, die nur den wenigsten bekannt sind.

Hintergrund 52



### Best of Backdoor-Fails

Hintertüren in Hard- und Software haben fast immer auch Nebenwirkungen - manchmal sogar spektakuläre.

Hintergrund 156

Besonders bei Web-2.0-Anwendungen kann sich der gesamte Angriff auf dem Nutzerrechner abspielen. Der Server liefert nur das fehlerhafte Skript an den Browser, aber nicht den Schadcode.

Prinzip entfällt dabei der Umweg über den Server, der lediglich HTML und den fehlerhaften Applikationscode übermittelt.

Applikation unter anderem dynamische Änderungen an der dargestellten Webseite vornehmen, etwa für interaktive Webanwendungen. Bei DOM-basiertem XSS kopiert ein fehlerhaftes browserseitiges Anwendungsskript den Schadcode direkt aus der URL per DOM-Zugriff in die angezeigte Webseite. Im



Forum bei heise online: [Serversicherheit](#)

TEILE DIESEN BEITRAG



<https://heise.de/-270870>

Drucken

Anzeige

## Rückblick: Die größten Hacks der vergangenen 10 Jahre

Von Stuxnet über Heartbleed bis zum Yahoo-Hack: Das haben Hacker von 2010 bis 2019 "geleistet".


Lesetipp

## Neueste Forenbeiträge

### Re: Lock Error "Error 5: Zugriff verweigert"

Googeln nach <windows ereignis 225> liefert u.a. in einem Treffer eine anschauliche Anleitung, um den Verursacher zu finden, der das Auswerfen...


Forum: Desinfect

 von Kybfels; vor 49 Minuten

### Features der 64bit- Desinfect-Software für 32bit - Systeme

Hallo allerseits, es gibt in der Praxis viele 32bit-Systeme, u.a. auch durch die 10Zoll-Mini-Laptop-Klasse. Kann man nicht die 32bit- Version...

Forum: Desinfect

 von desinfektanwender; vor 7 Stunden

**Re: Desinfect installation auf SSD (mit Schreibzugriff)?**

Ja schon klar aber die Frage war ja nicht ob der Stick beschreibbar ist sondern ob man die SSD schreibbar machen könnte. Das das nicht...

Forum: Desinfect



von BR0KK; vor 8 Stunden

NEWS UND ARTIKEL

News  
7-Tage-News  
News-Archiv  
Hintergrund-Artikel  
Alert-Meldungen

SERVICE

Newsletter  
Tools  
Foren  
RSS  
mobil

DIENSTE

Security Consulter  
Netzwerkcheck  
Anti-Virus  
Emailcheck  
Browsercheck  
Krypto-Kampagne