WordPress Security

WordCamp Cologne MMXV

Über mich

- Name: Jon Ziemlich
- Geboren: 07.08.1992
- www.ziemlich-webdesign.de
- Spezialisiert auf:
  - PHP Entwicklung
  - WordPress Plugin Entwicklung
  - Internetsecurity

Übersicht

- PHP Theorie
- Überblick über die gängigen Angriffsmethoden
- Demonstration eines Angriffes auf WordPress
- Wie werden Schwachstellen gefunden?
- Wie kann ich mich vor Angriffen schützen?

PHP Theorie

- Kommunikation mit PHP Script (WordPress) über HTTP(S)
- HTTP-Anfragemethode: **GET**
- HTTP-Anfragemethode: **POST**

HTTP-Anfragemethode: GET

- Übertragung **in der Url**
  - index.php?page=12&action=update
  - (mit Rewrite z.B.) www.seite.de/12/update
- z.B. **Abruf in PHP mit $_GET[]**
  - $_GET[„page"] = „12“;
  - $_GET[”action“] = „update“;

HTTP-Anfragemethode: POST

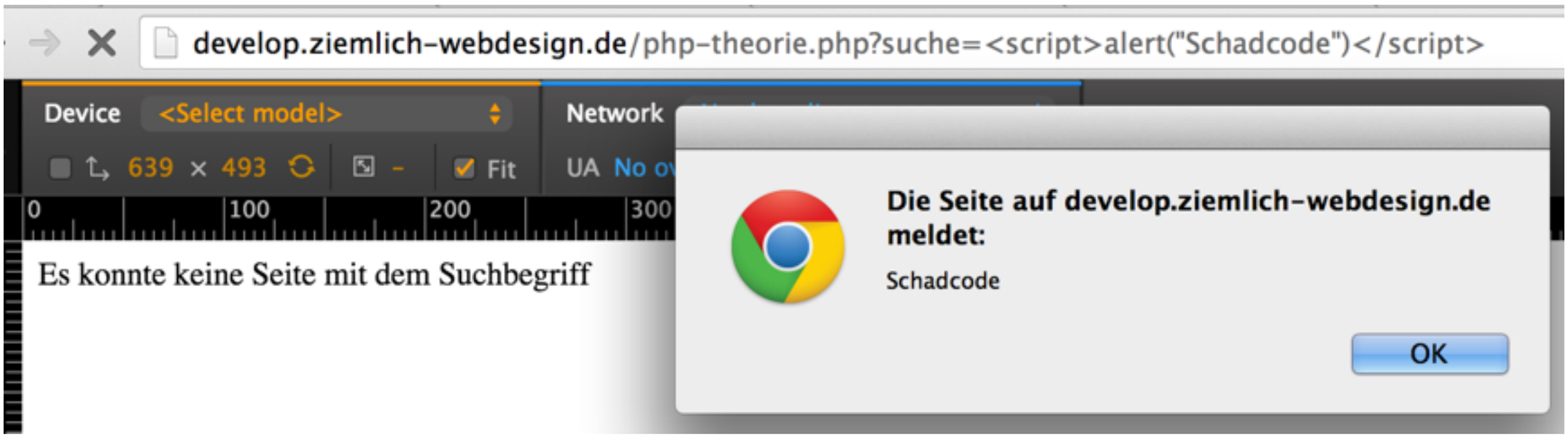
- Kann sowohl **Strings als auch Dateien** übertragen
- Übertragung über bspw. **HTML Formular oder AJAX**
  - <form action="" method=„post“>
  - <input type=„text“ value=„12“ name=„page“>
- z.B. **Abruf in PHP mit $_POST[]**
  - $_POST[„page"] = „12“;

Beispiel einer PHP Sicherheitslücke

- GET und POST bieten Angriffsmöglichkeiten, da der Input vom Client (Browser) bestimmt wird!

```php
<?php

/* Unsere GET Variable php-theorie.php?suche=Seite */
$suchbegriff = $_GET["suche"];

/* Array als Bsp. für Datenbankeinträge */
$meineseiten = array("Seite1","Seite2");


/* Überprüft, ob Suchbegriff in Array existiert */
if(!in_array($suchbegriff,$meineseiten)){

    /* String Ausgabe und Sicherheitslücke */
    echo "Es konnte keine Seite mit dem Suchbegriff " . $suchbegriff . " gefunden werden!";

}

?>
```

Output


develop.ziemlich-webdesign.de/php-theorie.php?suche=<script>alert("Schadcode")</script>
Device
<Select model>
Network
639 × 493
Fit
UA
0
100
200
300
Es konnte keine Seite mit dem Suchbegriff
Die Seite auf develop.ziemlich-webdesign.de meldet:
Schadcode
OK

Beispiel einer PHP Sicherheitslücke

- Schliessen der Lücke mit bspw. **htmlspecialchars()**

```php
<?php

/* Unsere GET Variable php-theorie.php?suche=Seite */
$suchbegriff = $_GET["suche"];

/* Array als Bsp. für Datenbankeinträge */
$meineseiten = array("Seite1","Seite2");


/* Überprüft, ob Suchbegriff in Array existiert */
if(!in_array($suchbegriff,$meineseiten)){

    /* String Ausgabe und Sicherheitslücke */
    echo "Es konnte keine Seite mit dem Suchbegriff " . htmlspecialchars($suchbegriff) . " gefunden werden!";

}

?>
```

Output


develop.ziemlich-webdesign.de/php-theorie.php?suche=<script>alert()</script>
Es konnte keine Seite mit dem Suchbegriff <script>alert()</script> gefunden werden!

Überblick über die gängigen Angriffsmethoden

- XSS (Cross-Site-Scripting)
- SQL-Injection
- Brute Force Attacken
- HTTP Sniffer

XSS (Cross-Site-Scripting)

- **Einbindung von schädlichem Code in eine vertrauenswürdige Seite**

- In Wordpress kann durch eine XSS Schwachstelle **die komplette Seite übernommen** werden

- z.B. index.php?seite=<script src=„schadscript.js“></script>

SQL-Injection

- **Einbindung von unerwünschten SQL Befehlen**

- In Wordpress kann durch eine SQL-Injection auf **die komplette Datenbank** zugegriffen und diese verändert werden

- z.B. mysql_Query(„SELECT * FROM benutzer WHERE id = „$_GET[„id“]“);

Brute-Force Attacke

- **Angriff auf ein Passwort durch wiederholtes Ausprobieren beliebiger Kombinationen**

- Läuft automatisiert ab

- **Prävention:** Ein sicheres und langes Passwort mit Sonderzeichen wählen

Live Hacking

Cross-Site-Request-Forgery (CSRF)

Wie werden Schwachstellen gefunden?

- Programme wie **WPScan** beinhalten eine Datenbank mit Schwachstellen und scannen eine Seite nach diesen ab

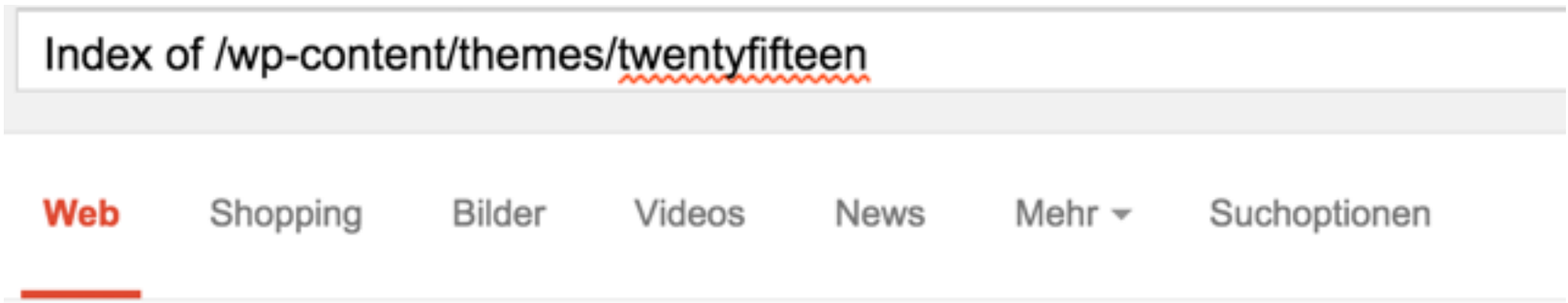
- **Google** ermöglicht die Suche nach Themes / Plugins bei denen bereits Schwachstellen bekannt sind

WPScan

```
[+] URL: [redacted]
[+] Started: Tue Jun  2 16:58:57 2015

[+] robots.txt available under: 'http:/[redacted]robots.txt'
[!] The WordPress 'http:[redacted]readme.html' file exists exposing a version number
[+] Interesting header: SERVER: nginx
[+] Interesting header: X-POWERED-BY: PHP/5.6.0-1
[+] XML-RPC Interface available under: http:/[redacted]xmlrpc.php

[+] WordPress version 3.5.1 identified from advanced fingerprinting
[!] 17 vulnerabilities identified from the version number

[!] Title: Wordpress 3.4 - 3.5.1 /wp-admin/users.php Malformed s Parameter Path Disclosure
    Reference: https://wpvulndb.com/vulnerabilities/5978
    Reference: http://osvdb.org/95060
[i] Fixed in: 3.5.2

[!] Title: WordPress 3.4-3.5.1 DoS in class-phpass.php
    Reference: https://wpvulndb.com/vulnerabilities/5979
    Reference: https://secunia.com/advisories/53676
[i] Fixed in: 3.5.2

[!] Title: WordPress 3.5.1 Multiple XSS
    Reference: https://wpvulndb.com/vulnerabilities/5980
    Reference: http://osvdb.org/94790
```

Google Suche

- falsch konfiguriertes Directory Listing



Ungefähr 105.000 Ergebnisse (0,49 Sekunden)

Tipp: Begrenzen Sie die Suche auf **deutschsprachige** Ergebnisse. Sie können Ihre Suchsprache in den Einstellungen ändern.

Index of /content/wp-content/themes/twentyfifteen
[redacted]**content/wp-content/themes/twentyfifte...** ▾ Diese Seite übersetzen
Index of /content/**wp-content/themes/twentyfifteen**. Parent Directory · 404.php · archive.php · author-bio.php · comments.php · content-link.php · content-none.php ...

Index of [redacted]/wp-content/themes/twentyfifteen
[redacted]/.../**wp-content/themes/twentyfi...** - Diese Seite übersetzen
Index of /~cafrica/**wp-content/themes/twentyfifteen**. Parent Directory · 404.php · archive.php · author-bio.php · comments.php · content-link.php · content-none.

HTTP Sniffing

- Abfangen der POST und GET Anfragen in einem Netzwerk
- https:// für sensible Daten (Login)
- Nicht überall einloggen!

Wie kann ich mich vor Angriffen schützen?

- **Es gibt keinen 100%igen Schutz**

- **Immer WordPress, Themes und Plugins updaten !**

- Bei fremden Links und auch bei Links der eigenen Domain immer vorsichtig sein!

- Mitarbeiterschulungen

- Sichere Passwörter wählen

Vielen Dank für eure Aufmerksamkeit

Vielen Dank für eure Aufmerksamkeit

Jon Ziemlich

mail@ziemlich-webdesign.de
www.ziemlich-webdesign.de