PEPPERSHOP

Direkt externer Login vom PepperShop

Anleitung

Datum
12. Oktober 2016

Version
3.3

PEPPERSHOP

Inhaltsverzeichnis

PepperShop wird von Glarotech entwickelt und vertrieben. Seit 1998 ist das innovative Unternehmen im Internet tätig und auf E-Commerce spezialisiert. Sie als Kunde profitieren vom direkten Draht zu den Herstellern der Produkte.

glarotech

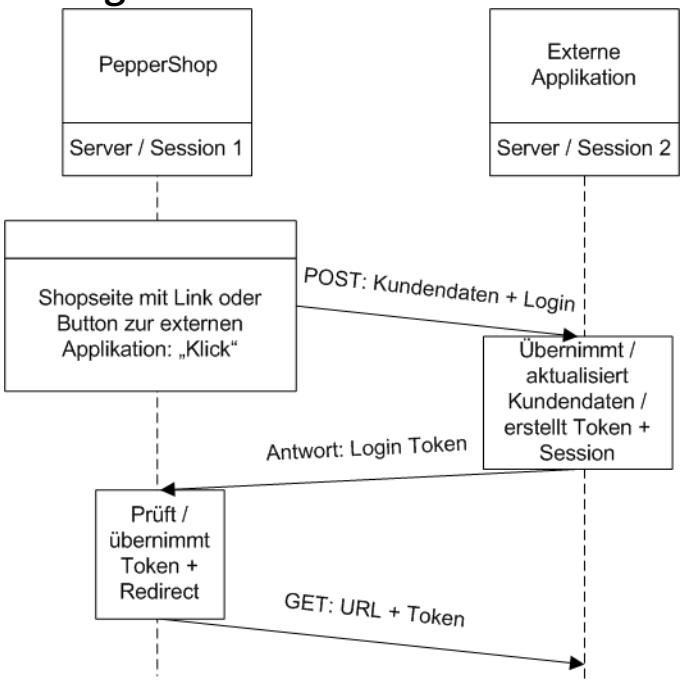
Glarotech GmbH
Toggenburgerstrasse 156
CH-9500 Wil

info@glarotech.ch
Tel. +41 (0)71 923 08 58
www.glarotech.ch

Direkt externer Login vom PepperShop

Mit diesem Webservice kann der Shop einen angemeldeten Kunden bei einer externen Applikation anmelden(SSO), wenn diese den Webservice wie folgt beschrieben implementiert .

1. Ablauf Visualisierung



2. Ablauf Beschreibung

```
                  Shopsystem                          externe Applikation
                  ----------                          -------------------
                      |
[0.)]       angemeldeter Benutzer
              klickt auf Button
                      |                HTTPS-POST
 1.)          ..ruft diese Datei auf ---------------> Sendet aktuelle Kundendaten
                                                      an externe Applikation (UTF-8)
                                                                |
 2.)                                                  Erstellt / aktualisiert internes
                                        (Antwort)       Kundenkonto und erstellt eine
 3.)            übernimmt Token     <---------------     Session und einen Token
                (+Fehlerhandling)
                      |
 4.)           Erstellt URL zu
              externer Applikation      GET-Redirect
 5.)      mit Token als GET-Parameter --------------> Benutzer wird zu externer Appli-
                                                      kation redirected und ist dort
                                                           nun angemeldet.
```

3. Vereinbarung zur Verwendung dieses Webservices

- SSL/TLS muss in einer kompatiblen Form auf beiden Systemen vorhanden sein, optional mit Zertifikaten
- Wenn der IP-Check verwendet wird, muss der externe Server eine fixe IPv4 Adresse haben
- Die Kundendaten werden vom Shop UTF-8 encodiert via HTTPS-POST Call angeliefert (bitte TLS verwenden)
- Als Antwort auf den HTTPS-POST Call darf ausschliesslich der Token retourniert werden
- Der generierte (Session-)Token darf nur DEXLO_TOKEN_MAXLENGTH lang sein (Default = 32 Zeichen)

- Der generierte (Session-)Token darf nur aus folgenden Zeichen bestehen: `a-zA-Z0-9_-`
- Für den HTTPS-POST Call kann optional eine HTTP-Basic Authentication verwendet werden (in diesem Fall muss ein Benutzername + Passwort vereinbart werden und die Redirection-URL muss an einem anderen Ort liegen, denn diese verwendet keine Authentication mehr!)
- Info: Der Shop muss Kunden-Nr. vergeben oder er überliefert sonst die interne k_ID (Tabelle 'kunde')

4. Beispiel Server (externe Applikation) in PHP

```php
<?php
// ---------------------------------------------------------------------
// TESTSERVER EXAMPLE
// ---------------------------------------------------------------------
define(DEXLO_TOKEN_NAME,'token'); // (Name of token must comply to shop-side-script!)
if (!empty($_POST) && isset($_POST['DEXLO_HTTP_POST_CALL']) && $_POST['DEXLO_HTTP_POST_CALL'] == true) {
    // Create a new customer record or update an existing record
    // Creating a new session for this customer record
    // Generating an identification token, which satisfies the conditions described in uniqid()
    echo uniqid()."\n";
}
else if (!empty($_GET) && isset($_GET[DEXLO_TOKEN_NAME])) {
    // Checking the token and assigning the Session
    echo "Logged in to external application, your Token = ".$_GET[DEXLO_TOKEN_NAME];
}
exit;
```

5. Kommunikation und übertragene POST-Werte

Folgende Parameter werden im HTTP-POST Call UTF-8 encodiert übermittelt:

Label	*Format*	*Beschreibung*
customer_number	AN255	Kunden Identifikation
language	AN2	Sprachcode: ISO-639-1, z.B. 'de'
salutation	AN24	Lokalisierte Anrede
given_name	AN128	Vorname
surname	AN128	Nachname
company	AN128	Firma
division	AN128	Abteilung
street	AN128	Strasse
house_nr	AN128	Hausnummer
p_o_box	AN16	Postfach
zip	AN32	Postleitzahl
city	AN128	Ort
country	AN3	Ländercode: ISO-3166-2, z.B. 'CH'
telephone	AN32	Telefonnummer
fax	AN32	FAX Nummer
mobile	AN32	Handynummer
email	AN128	E-Mail Adresse
login*	AN255	Eindeutiger Benutzername
is_guest*	AN5: 'true' oder 'false'	Handelt es sich um ein Gastkonto?

password_hash*	AN255	BCRYPT Hash, 10 Rounds *(=default)*
additional_field_label_*{X}**	AN255	Kundenzusatzfeld 1-10 Beschriftung
additional_field_value_*{X}**	AN255	Kundenzusatzfeld 1-10 Wert
DEXLO_HTTP_POST_CALL	AN4: 'true' (konstanter String)	Call-Identifizierung / Info-Wert

* Optional (Übermittlung muss im Shop freigeschaltet werden: `{shop_dir}/shop/direct_extern_login.php`)

Formatlegende : N = nummerisch, AN = alphanummerisch, Zahl dahinter = Maximale Zeichenlänge

Passwort Hash : Es werden Blowfish basierte BCRYPT Hashes erzeugt. Die Konfiguration ist aber vom jeweiligen System und der Konfiguration im Shop abhängig. Dieses Feld ist übrigens optional!

Zusatzfeld Daten : In einem PepperShop gibt es standardmässig 10 Zusatzfelder, welche in der Administration (Kundenattribute) entweder zum Kunden oder zur Bestellung gemapped werden können. Je nach angepasstem Shopsystem können auch mehr Felder vorhanden sein. Für jedes dieser Felder gibt es ein Wertepaar, welches übertragen wird. Tabelle: *{X}* wird durch eine Zahl er setzt. Die übermittelten Labels sind in der jeweiligen Kundensprache lokalisiert.

Nun folgen zwei Kapitel, welche Beispielhaft eine HTTP(S)-Kommunikation des HTTPS-POST Calls und der Antwort der externen Applikation abbilden:

5.1 Anfrage

Shop sendet HTTPS-POST-Call an externe Applikation mit Kundendaten (Beispielanzeige):

```
POST /path_to_shop/shop/direct_extern_login.php HTTP/1.1
Host: www.yourdomain.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 324
Connection: close

customer_number=KD_1&amp;language=de&amp;salutation=Herr&amp;given_name=Jos
%C3%A9&amp;surname=Fontanil&amp;company=Glarotech+GmbH&amp;division=Software+
Engineering&amp;street=Toggenburgerstrasse&amp;house_nr=156&amp;p_o_box=&amp;
zip=9500&amp;city=Wil&amp;country=CH&amp;telephone=071+923+08+58&amp;fax=071+
923+08+59&amp;mobile=&amp;email=fontajos
%40peppershop.com&amp;DEXLO_HTTP_POST_CALL=1
```

5.2 Antwort

Externe Applikation liefert Session-Token in Antwort zurück (Beispielanzeige):

```
HTTP/1.1 200 OK
Date: Wed, 25 Jun 2014 11:46:22 GMT
Content-Length: 14
Connection: close
Content-Type: text/html

53aab68e252e9
```

6. Shop-seitige Dienste-Konfiguration

Es wird ein PepperShop Professional oder Enterprise benötigt, mindestens in der Version 5.0.

Die Konfiguration wird in der Datei `{shop_verzeichnis}/shop/direct_extern_login.php` umgesetzt. Es gibt explizit Informationsblocks und einen Abschnitt mit Steuerungskonstanten.

Einbindung im Shop als Link:

```
<a href="{pps_webroot}shop/direct_extern_login.php">Login bei externem Service</a>
```

Einbindung als hidden Server-To-Server Element:

Dieser Webservice wurde zum Zeitpunkt der Implementierung dafür ausgelegt, dass er mit der Einbindungsvariante als Link funktioniert. Zusätzlich lässt er sich aber auch als reiner Server-To-Server Call verwenden. Dazu muss man vor der Einbindung der Datei eine Steuerungskonstante definieren. Details, siehe folgendes Beispiel:

```
define('DEXLO_USED_BY_INCLUDE',true);
ob_start();
include_once('direct_extern_login.php');
$ext_login_errors = trim(ob_get_contents());
ob_end_clean();
if ($ext_login_errors != '') {
    // Errorhandling
}
if (defined('DEXLO_RECEIVED_TOKEN') && DEXLO_RECEIVED_TOKEN != '') {
    $token = DEXLO_RECEIVED_TOKEN;
    // Weitere Verarbeitung des Tokens...
}
```

7. History

24.11.2014:	fjo	v.3.2	Möglichkeit die Source-IP anzugeben
14.11.2014:	fjo	v.3.1	Server-To-Server Hidden Call
31.10.2014:	fjo	v.3.0	Support für SSL-Zertifikate
17.10.2014:	fjo	v.2.0	Login, Passwort-Hashes und Kundenzusatzfelder optional übertragbar
16.07.2014:	fjo	v.1.1	Strukturelle Verbesserungen, Dokumentation überarbeitet
10.07.2014:	fjo	v.1.0	Erste Version