به نام خدا

هر کس به زبانی صفت حمد تو گوید

راهنما و معرفی سیستم وبسرویس پرداخت واسطه نگارش شخصی

Payment WebService System

طراحی و برنامه نویسی : رضا شیخله

تکنولوژی :

Php5 , MySQL ,SOAP,Html,Css

Base on Yii framework(MVC)

ارائه شده در

www.rezaworkshop.ir

زمستان 1391

معرفی :

وبسرویس پرداخت واسط ، یک رابط تراکنشهای آنلاین بانکی هست که این امکان را به وجود می آورد تا بتوان درگاههای متعددی را به بانک مورد دلخواه متصل نمود و بصورت امن ترانشهایی را از وبسایتهای متعدد (با توجه به درگاه مورد نظر) به بانک منتقل کند .

مورد استفاده این وبسرویس بصورت شخصی و تک کاربره میباشد ، و برای حل مشکل عدم توانایی استفاده از یک درگاه بانکی برای چندین وبسایت با آی پی های مختلف ساخته شده است ، هر چند میتوان به هر فرد دل خواه نیز درگاه ارائه داد اما امکاناتی چون بخش رجیستر و لاگین ، تیکت و ... برای سیستم در نظر گرفته نشده لذا برای موارد تجاری استفاده از این اسکریپت پیشنهاد نمیشود هر چند ممانعت و محدودیتی ندارد .

الزامات :

برای اجرای اسکریپت باید از php 5.2+ استفاده کرد هرچند استفاده از php 5.3+ پیشنهاد میشود .

برای دیتابیس از MySQL5 استفاده شود در ضمن فعال بودن انجین InnoDB الزامی است . همچنین باید روی پی اچ پی SOAPسرور فعال باشد که در 99 درصد مواقع فعال هست .

منابع سخت افزاری مورد نیاز با توجه به تعدد تراکنشهای روزانه محاسبه میشود ، بطور مثال برای 2000 تراکنش روزانه (هر یک دقیقه یک تراکنش) سروری با رم 1 و سی پی یو متوسط جوابگو خواهد بود .

اگر مورد استفاده شما برای حداکثر 20 سایت استفاده میکنید سیستم برروی هاست اشتراکی با کیفیت بالا هم به خوبی کار میکند .

امکانات :

با نصب این سیستم ، شما قادر خواهید بود به تعداد متعدد درگاه برای سایتهای خود ایجاد کنید و تراکنشها را بصورت مستقیم به بانک بفرستید ، تمامی تراکنشها از طریق پنل قابل پیگیری میباشد . همچنین این امکان تعبیه شده که بصورت امکان گزارشگیری با فرمت اکسل بصورت ماهانه و سالانه برای تراکنشهای یک درگاه یا کل تراکنشها اقدام کنید .

نمونه فرمت گزارشگیری در عکس زیر نمایان است

	A	B	C	D	E	F	G	H	I
1	TransID	GatewayID	au	Price (toman)	ip	date	bank	bank_au	status
2	15	2	15e2418fc16	2500	[redacted]	1391/10/13 (01:55)	parsian	[redacted]987	OK
3	14	2	14sseedfsffr	2500	[redacted]	1391/10/12 (04:32)	parsian	[redacted]9786	OK
4	13	2	13defrgttgtvv	2500	[redacted]	1391/10/12 (04:32)	parsian	[redacted]5548	OK
5	12	2	12ervegt5tvt5	2500	[redacted]	1391/10/12 (04:32)	parsian	[redacted]9657	--
6	11	2	11vtvt88yyybyb	2500	[redacted]	1391/10/12 (04:32)	parsian	[redacted]8756	--
7	10	2	10vttvtyyhy	2500	[redacted]	1391/10/12 (04:32)	parsian	[redacted]3852	--

همچنین قابلیتهای پیشرفته ای برای جلوگیری از نفوذ احتمالی صورت گرفته که میتوان به سیستم قفل آی پی هوشمند اشاره کرد .

فارغ از این تمامی خطاهای سیستمی ، اعم از اتصال به وبسرویس با آی پی نامشخص ، اتصال با پین غیر صحیح ، لاگینهای ناموفق ، خطاهای احتمالی ارتباط با بانک و ... در سیستم لاگ میشود و مدیر میتواند آنهارا بررسی کند .

پیغام	عنوان	آی پی
آی پی کاربر به جهت تعدد لاگینهای ناموفق به مدت 8 دقیقه مسدود	لاگین ناموفق	[redacted]
عدم انجام دسترسی به کاربر برای لاگین به جهت مغایرت با آی پی شده اختصاصی مدیر .	لاگین با آی پی مغایر مدیر	[redacted]
آی پی فروشنده مطابقت ندارد	خطای برگشتی بانک	[redacted]

امنیت سیستم :

سیستم در مقابل حملات معمول کاملا مصون هست به طور مثال برای جلوگیری از حملات CSRF سیستم از ست کردن رشته رندم متغییر در فرمها استفاده میکند که فقط فرمهای داخل سیستمی را امن میشناسد . همچنین برای جلوگیری از XSS تمامی رشته های ارسالی از سمت مشتری پاکسازی و ایمن میشود .

برای جلوگیری از سرقت جلسات (session hijack) ، هر جلسه با توجه به SESSID در داخل دیتابیس ذخیره میشود .

برای جلوگیری از session fixation رشته هایی در هم (hash) در کوکی کاربر ذخیره میشود و در هر درخواست صحت آن بررسی میشود پس حتی اگر شخص هکر هم SESSID را در اختیار داشته باشد عملاً نفوذ به سیستم منتفی خواهد بود .

برای جلوگیری از حملات Remote file inclusion چون از فریم ورک استفاده شده و براساس معماری MVC و قوانین اسم گذاری فایلها براساس کلاس موجود همچنین autoload هوشمند ، بطور قطع سیستم در مقابل نفوذ RFI مصون است .

برای جلوگیری از کرک هش پسورد ، آلگوریتم هش برروی دور 4000 دور هست (قابل توجه کرکرهای محترم)

برای جلوگیری از تذریق به دیتابیس (sql injection) سیستم تمامی ورودی هارا بررسی میکند و هر پارامتر را با توجه به نوع مورد نیاز validate میکند ، جدای از این برای ارتباط با دیتابیس از PDO استفاده شده که حتی اگر validate هم انجام نشود در مقابل حملات sql inject مصون است .

برای جلوگیری از حملات brute force اسکریپت مجهز به سیستم قفل لاگین هست .

درحقیقت تنها بخشی که هکر /کرکر میتواند تست نفوذ انجام دهد در این بخش هست ، و در مقابل سیستم تمهیدات مناسبی اتخاذ میکند .

مدیر میتواند دسترسی به بخش مدیریت سیستم را به یک آی پی خاص محدود کند ، (که البته پیشنهاد نمیشود) فارغ از این آی پی تمامی درخواست لاگین هاییکه فرستاده میشود منتفی است .

البته این امکان همیشه وجود ندارد که آی پی شخص مدیر همیشه یک آی پی باشد پس این امکان بصورت پیشفرض غیرفعال است .

مدیر میتواند تعدد لاگین های ناموفق را مدیریت کند ، و آی پی های متخلف را مسد ود کند ، بطور مثال تعیین کند اگر شخص قصد لاگین داشت و سه بار نام کاربری یا کلمه عبور را اشتباه وارد کرد سیستم آی پی وی را به مدت n دقیقه مسدود کنند . همچنین اطلاعات به ایمیل مدیر ارسال شود .

جدای از این اگر آی پی مشخصی همیشه قصد مزاحمت و تست داشت ، مدیر می تواند دسترسی آی پی را به قسمت لاگین برای همیشه مسدود کند .

حال با این تفاسیر اگر باز هم هکر از طریق پیداکردن رمز عبور مدیر به سیستم لاگین کرد ، اطلاعات لاگین وی به ایمیل مدیر ارسال میشود .

در سیستم امکانی برای دسترسی به سرور /هاست وجود ندارد و فقط هکر میتواند خرابکاری هایی جزئی انجام دهد(مثلا غیرفعال کردن درگاهها) .

امنیت در بخش وبسرویس :

به ازای هر درگاهی که میخواهید برای سایتی استفاده کنید باید آی پی سایت مذکور را وارد کنید ، سیستم به شما یک پین میدهد که بوسیله آن میتوانید از وبسایت مذکورد به وبسرویس وصل شوید و پرداخت انجام بدید .

سایتهایی که به وبسرویس وصل میشوند در صورت عدم تطابقت آی پی یا عدم وجود پین ، آی پی آنها در سیستم لاگ میشود تا مدیر تمهیدات لازم را انجام دهد .

مدیر میتواند دسترسی به وبسرویس را برای آی پی های مختلف مسدود کند ، همچنین اگر درگاهی درخواستهای پرداخت متوالی فرستاد اما پرداختی انجام نداد ، مدیر میتواند درگاه مورد نظر را غیرفعال کند .

استفاده از وبسرویس :

برای استفاده یک سایت از وبسرویس مدیر باید قبلا یک درگاه با توجه به آی پی واقعی سایت بسازد و پین مربوطه را در اختیار سایت قرار دهد .

اگر چنانچه آی پی واقعی سایت مذکور را نمیدانید کافیست از آن سایت یک درخواست به وبسرویس بفرستید و متد realIp را درخواست کنید .

(در دستورات زیر به جای example.ir آدرس وبسرویس خود را جایگزاری کنید .)

```php
<?php
    $client = new SoapClient("http://example.ir/index.php/payment/wsdl");
    echo $client->realIp();
?>
```

ساخت درگاه :

برای ساخت درگاه ، از منوی سمت راست برروی درگاهها کلیک کنید سپس گزینه افزودن درگاه را بزنید .

برای ساخت درگاه شما باید یک اسم برای درگاه انتخاب کنید ، همچنین آی پی سایت استفاده کننده که طبق متد بالا میتوان ید آی پی سایت استفاده کننده را مشخص کنید ، همچنین بخش ایمیلهای گزارش که میتوانید چندیدن ایمیل را وارد کنید ، ایمیلهای گزارش برای ارسال گزارش تراکنشهای موفق به آن ایمیل هستند .

بعد از ساخت درگاه سیستم یک پین یکتا مخصوص آن درگاه میسازد که باید برای اتصال به وبسرویس از آن سایت مورد استفاده قرار گیرد .

راهنمای اتصال به وبسرویس :

اکنون که درگاهی ساختید همه چیز برای اتصال به وبسرویس مهیاست .

وبسایتی که میخواهد به وبسرویس وصل شود باید پین مربوط به خود را وارد کند .

جهت اتصال به وبسرویس باید از SOAP استفاده شود اگر چنانچه SOAP فعال نبود میتوانید کتابخانه NU_SOAP را در برنامه تان include کنید و از آن استفاده کنید .

انجام عملیات یک تراکنش موفق نیازمند ارسال یک درخواست به وبسرویس و دریافت au هست سپس مشتری را به لینک مناسب میفرستید تا سیستم مشتری را به درگاه بانک هدایت کند ، بعد از بازگشت مشتری به سایت شما باید صحت تراکنش انجام شده را با استفاده از au از وبسرویس درخواست کنید و درصورت صحت تراکنش اقدامات لازم را انجام دهید .

پس نتیجه انجام یک تراکنش موفق نیازمند دو بار اتصال به وبسرویس است که مرحله اول را request و مرحله دوم verify هست .

در مرحله اول شما باید مقادیر پین (که رشته پین اختصاصی درگاه شماست) ، مبلغ (که مبلغ پرداختی مشتری است به تومان) ، آدرس کال بک (که آدرس برگشتی به سایت شماست بعد از عملیات پرداخت) ، شناسه فاکتور مشتری (که شناسه مربوط به فاکتور مشتری در سایت شماست البته الزامی نیست وارد کردنش اما اگر وارد کنید بعنوان پارامتر get توسط وبسرویس به آدرس کال بک اضافه میشود) ، توضیحات (که توضیحاتی در مورد خرید هست که البته الزامی نیست ، اگر وارد کنید بعد از پرداخت صحیح تراکنش تمامی اطلاعات به ایمیل وارد شده در قسمت درگاه فرستاده میشود)

نمونه کد :

(در دستورات زیر به جای example.ir آدرس وبسرویس خود را جایگزاری کنید .)

```php
$client = new SoapClient("http://example.ir/index.php/payment/wsdl", array("encoding"=>"UTF-8"));

$pin = "8091cd8b645" ;
$price = 3500 ; // تومان
$callback = "http://rezaonline.net/callback.php";
$order_id = 123456;
$description = "تراکنش سایت رضا";

$au = $client->request($pin , $price , $callback , $order_id , urlencode($description) );
if(strlen($au) >=8)
    header("location: http://example.ir/index.php/paymentgateway/?au={$au}");
else
    echo "خطایی رخ داد : شماره خطا " . $au;
```

بعد از ارسال این اطلاعات به وبسرویس ، وبسرویس یک رشته بعنوان au برمیگرداند که شناسه پیگیری تراکنش مورد نظر شماست .

پیشنهاد میکنم قبل از فرستادن مشتری به درگاه خرید ، این رشته را ذخیره کنید .

رشته au اگر بیش از 8 کاراکتر باشد صحیح است در غیر اینصورت au یک عدد منفی است که بعنوان کد خطای سیستم شناخته میشود .

لیست کد خطاها در پایان این بخش هست .

بعد از فرستادن مشتری به درگاه ، سیستم مشتری را به بانک منتقل میکند تا پرداخت خود را انجام دهد بعداز برگشت سیستم مشتری را به آدرس کال بک شما میفرستید بطور مثال برای اطلاعات بالا مشتری به آدرس

http://rezaonline.net/callback.php?order_id=123456&au=ab458e25au

برگشت داده میشود ، در این مرحله شما باید اطلاعات تراکنش را از دیتابیس خود با استفاده از order_id (یا au اگر ثبت کرده بودید) واکشی کنید و مبلغ تراکنش را که باید پرداخت شده باشد مشخص کنید .

سپس یک بار دیگر از وبسرویس صحت این تراکنش را درخواست کنید . مقادیر ارسالی به وبسرویس باید پین ، مبلغ و au تراکنش باشد .

مثال :

```php
$order_id = (int) $_GET["order_id"];
$price = 3500 ; // SELECT `price` FROM `order_tbl` WHERE `id`={$order_id}
$pin = "8091cd8b645" ;
$au = $_GET["au"];

$client = new SoapClient("http://example.ir/index.php/payment/wsdl", array("encoding"=>"UTF-8"));

$result = $client->verify($pin,$au,$price);

if( ! empty($result) and $result == 1)
    echo "پرداخت موفقیت آمیز بوده است .";
else
    echo "خطایی رخ داد : شماره خطا " . $result;
```

اگر پاسخ برگشتی موجود و عدد 1 بود پس تراکنش با موفقیت انجام شده در غیر اینصورت عدد برگشتی یک عدد منفی است که کد خطای برگشتی است .

کدهای خطا به شرح زیر است .

شناسه خطا	توضیحات
-1	پین نامعتبر است
-2	آی پی نامعتبر است
-3	مبلغ از کف تعریف شده کمتر است
-4	مبلغ از سقف تعریف شده بیشتر است
-5	مبلغ نامعتبر است
-6	ارتباط با بانک برقرار نشد
-7	درگاه غیرفعال است
-8	آی پی شما مسدود است
-9	خطای ناشناخته رخ داده است
-10	آدرس کال باک خالی یا نامعتبر است
-11	چنین تراکنشی یافت نشد
-12	تراکنش انجام نشده است
-13	تراکنش انجام شده اما مبلغ نادرست است (مبلغ مطابقت ندارد)

همانطور که در بالا گفته شد چنانچه برروی سایت درخواست کننده SOAP فعال نبود میتوانید کلاس NU_SOAP را استفاده کنید ، در این صورت دستورات اتصال به وبسرویس باید بصورت زیر انجام شود .

قسمت اول request

```
include_once("nusoap.php");
$client = new nusoap_client("http://example.ir/index.php/payment/wsdl", "wsdl");

$pin = "8091cd8b645" ;
$price = 3500 ; // تومان
$callback = "http://rezaonline.net/callback.php";
$order_id = 123456;
$description = "تراکنش سایت رضا";

$au = $client->call("request",array($pin , $price , $callback , $order_id , urlencode($description)));
if(strlen($au) >=8)
    header("location: http://example.ir/index.php/paymentgateway/?au={$au}");
else
    echo "خطایی رخ داد : شماره خطا " . $au;
```

قسمت دوم verify

```
$order_id = (int) $_GET["order_id"];
$price = 3500 ; // SELECT `price` FROM `order_tbl` WHERE `id`={$order_id}
$pin = "8091cd8b645" ;
$au = $_GET["au"];

include_once("nusoap.php");
$client = new nusoap_client("http://example.ir/index.php/payment/wsdl", "wsdl");

$result = $client->call("verify" , array($pin,$au,$price));

if( ! empty($result) and $result == 1)
    echo "پرداخت موفقیت آمیز بوده است .";
else
    echo "خطایی رخ داد : شماره خطا " . $result;
```

سوالات متداول :

آیا اسکریپت کد شده است ؟

خیر اسکریپت بصورت اپن سورس ارائه میشود (دقت کنید که اپن سورس به معنی رایگان نیست !)

آیا محدودیتی در تعداد درگاهها و تراکنشها لحاظ شده ؟

خیر ، هیچ محدودیتی لحاظ نشده .

آیا میتوان از این وبسرویس بعنوان خدمات تجاری استفاده کرد ، مثل سایتهای زرین پال ، پارس پال و ... ؟

این سیستم با هدف استفاده شخصی ساخته شده و فاقد امکاناتی چون عضویت ، پشتیبانی ، تیکت و ... میباشد ! در کل وظیفه اسکریپت مدیریت تراکنشها و ارائه درگاه است .

برای خدمات تجاری هم میتواند مورد استفاده قرار گیرد ، اما پیشنهاد نمیشود (گرچه محدودیتی ندارد)

بطور کلی موارد استفاده این وبسرویس در چه مواقع است ؟

1. برای مواقعی که شما یک درگاه بانکی دارید و تعداد زیادی وبسایت در سرورهای مختلف با آی پی ها مختلف ، نمیتوانید برای تمامی وبسایتها از درگاه بانک استفاده کنید (به دلیل محدودیت تعدد آی پی) لذا میتوانید به جای گرفتن درگاههای متعدد و پر هزینه ، از این وبسرویس بعنوان واسط استفاده کنید .
2. برای مواقعی که لازم هست ارتباط با بانک فقط از طریق سرور و آی پی ایران باشد لذا میتوانید این وبسرویس را برروی یک هاست ایران نصب کنید و به بانک مرتبط کنید و از تمامی وبسایتهای خود به این وبسرویس متصل شوید و پرداخت انجام دهید .
3. برای مواردی که نباید برای خرید مستقیم به درگاه بانک وصل شد (به دلایلی که خودتان میدانید) ، لذا میتوانید از این وبسرویس بعنوان واسطه استفاده کنید و فروش خود را با خیال راحت انجام دهید .

آیا انتقال به درگاه بصورت مستقیم هست یا غیرمستقیم ؟

انتقال به درگاه بانکی بصورت مستقیم انجام میشود ، در حقیقت مشتری در پرداخت مستقیم با بانک یا بواسطه این اسکریپت هیچ تفاوتی احساس نمیکند .

دوستانی که قصد تهیه و استفاده از این سیستم رو دارند میتوانند از طریق وبسایت http://rezaworkshop.ir اقدام کنند .

با تشکر رضا شیخله

دی 1391

info@rezaonline.net