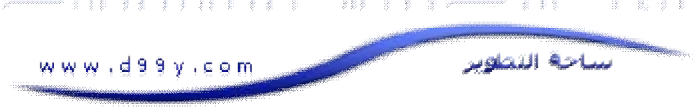
بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركاته



اهلاً وسهلاً بكم احبّتي 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 الانماط 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 الفلترة هو نقطة تكوّن ثغرات الـ XSS وذلك لان المستخدم يمكنه ادراج اكواد html , java script والخ من ملحقات لغة html وينفذ هذا المدخل في الصفحة ، وهذا يعني تخطيه صلاحياته في الطباعه ، 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 ثابته - مخزّنه! Persistent - stored

ثانياً / ثغرات XSS غير ثابته - غير مخزّنه! Non persistent - Reflected

ثغرات XSS الثابته هي اخطر من النوع الغير ثابت ، وذلك لان ثغرات XSS الثابته ، مايدخله الزائر ثابت بالصفحه ، اي مايدخله مثلاً يخزّن بقاعدة بيانات السكربت ، وبذلك عند دخول موضوع يحتوي على امكانية التفاعل بالردود ، في حالة لم يكون السكربت محمي بالتأكيد اي شخص يقوم بالدخول الى الموضوع سيشاهد اعمال المخترق في الصفحة . .

بعكس ثغرات الـ XSS الغير ثابته ، 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 ثابته , وذلك لان ادخالك لن يخزّن في قاعدة بيانات الموقع اي في حالة الطلب يظهر لك لا اكثر ..

"وللمعلوميه " ثغرات XSS الثابته البعض يُطلق عليها HTML Injection لكي يوضّح انها ثغرة XSS مُخزّنه وخطيرة ولكن التسمية ليست صحيحه فعلياً لكي تخصص لنوع معيّن وذلك لان النوعين تقوم على اساس حقن الاكواد . .

خطورة الثغرة كبيرة جداً في النوع الثابت ، وذلك لانه يمكن للمخترق اولاً اختراق متصفحي الموقع وهذا يعني القدرة على اختراق مُدير 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 الثغره ، جميع اللغات المتخصصه في برمجة تطبيقات الويب مثل PHP , Perl , ASP 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 الزوّار ، لذلك هنا نقول ان ثغرات XSS خطيرة جداً ولا يستهان ابداً بها . .

اعيد واكرر مره اخرى ان عدم فلترة المُخرجات 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 احبّتي اعضاء ساحة التطوير في درس استغلال واكتشاف ثغرة! XSS

بعد المقدمة تعلّمنا سابقاً ، ماهي 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 تعلّمنا طرق الاستغلال والاكتشاف. .

وذكرت لكم في ان لكل ثغرة لابد من برمجة سكربت نقوم بالتطبيق عليه في بيئة السيرفر المحلي ، وكذلك نقوم بترقيعه والتأكد من سلامة الترقيع ، وطبعاً سكربت الـ XSS تم برمجته وفقاً للانواع المذكورة سابقاً ثابت وغير ثابت اي مُخزّن وغير مُخزّن ، وطبعاً لابد ان اذكّر ان طُرق الاستغلال طُرحت لكي نختبر الحماية في المستقبل للثغرة ، وكذلك نكون في علم بطرق الاستغلال التي قد يستغلها المُخترق. .

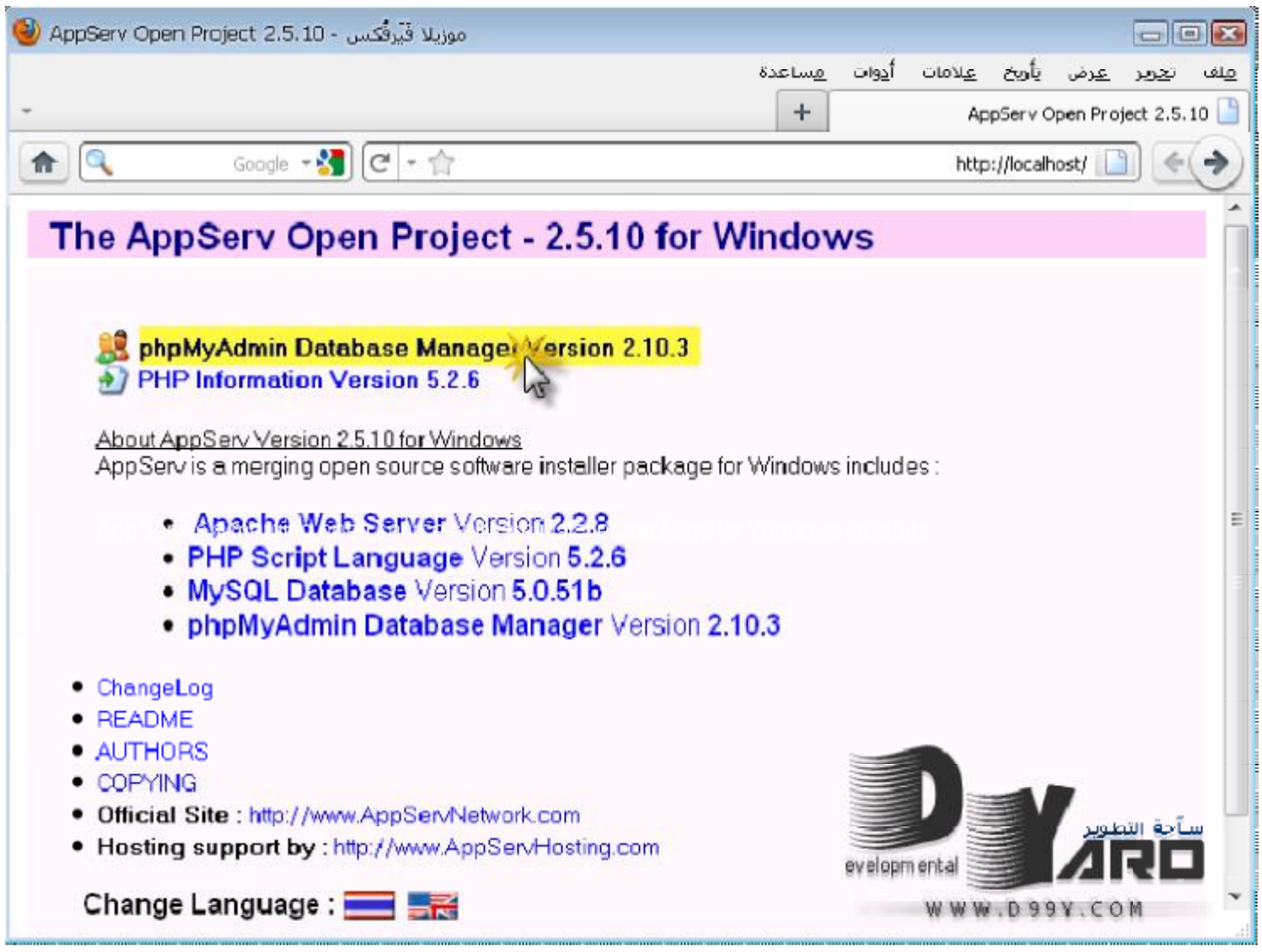
اولاً تحميل السكربت. .

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

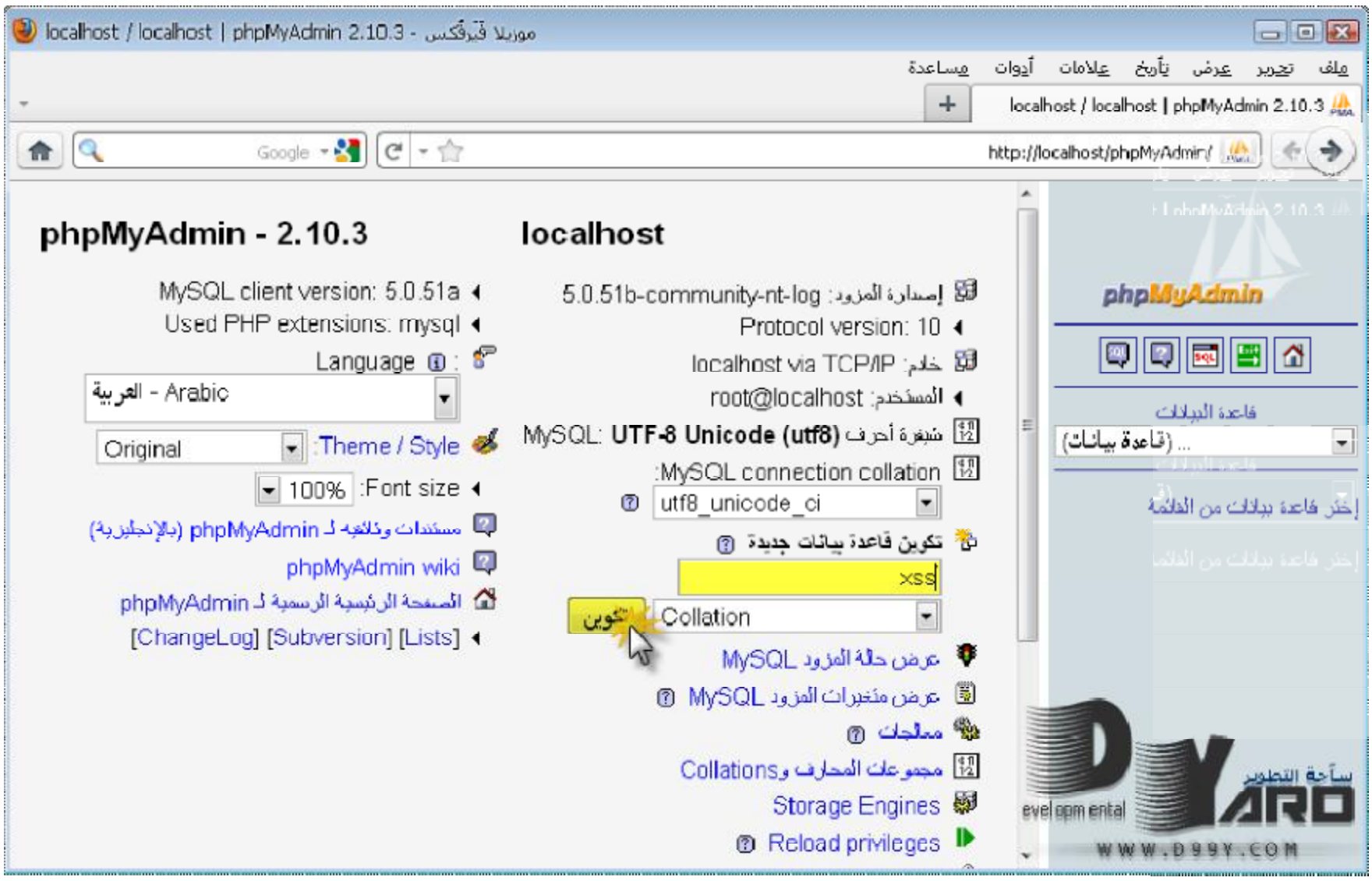
قبل الدخول في شرح تنصيب السكربت , التعليق موجود على جميع الصفحات . .

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

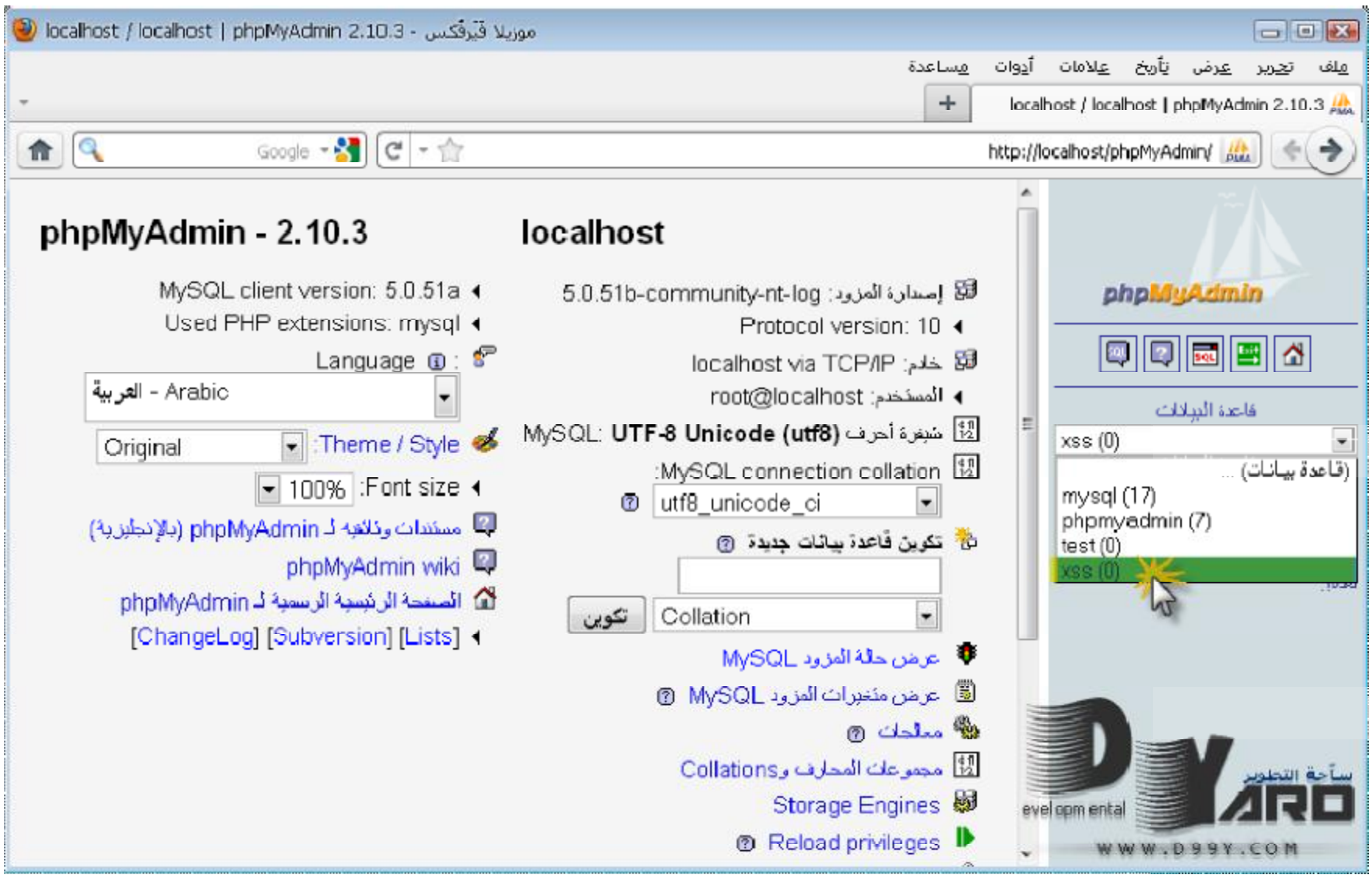
اتمنى وصلت المعلومه ، الان نقوم سريعاً بالدخول الى طريقة التنصيب . .



نقوم بالدخول الى! phpMyAdmin

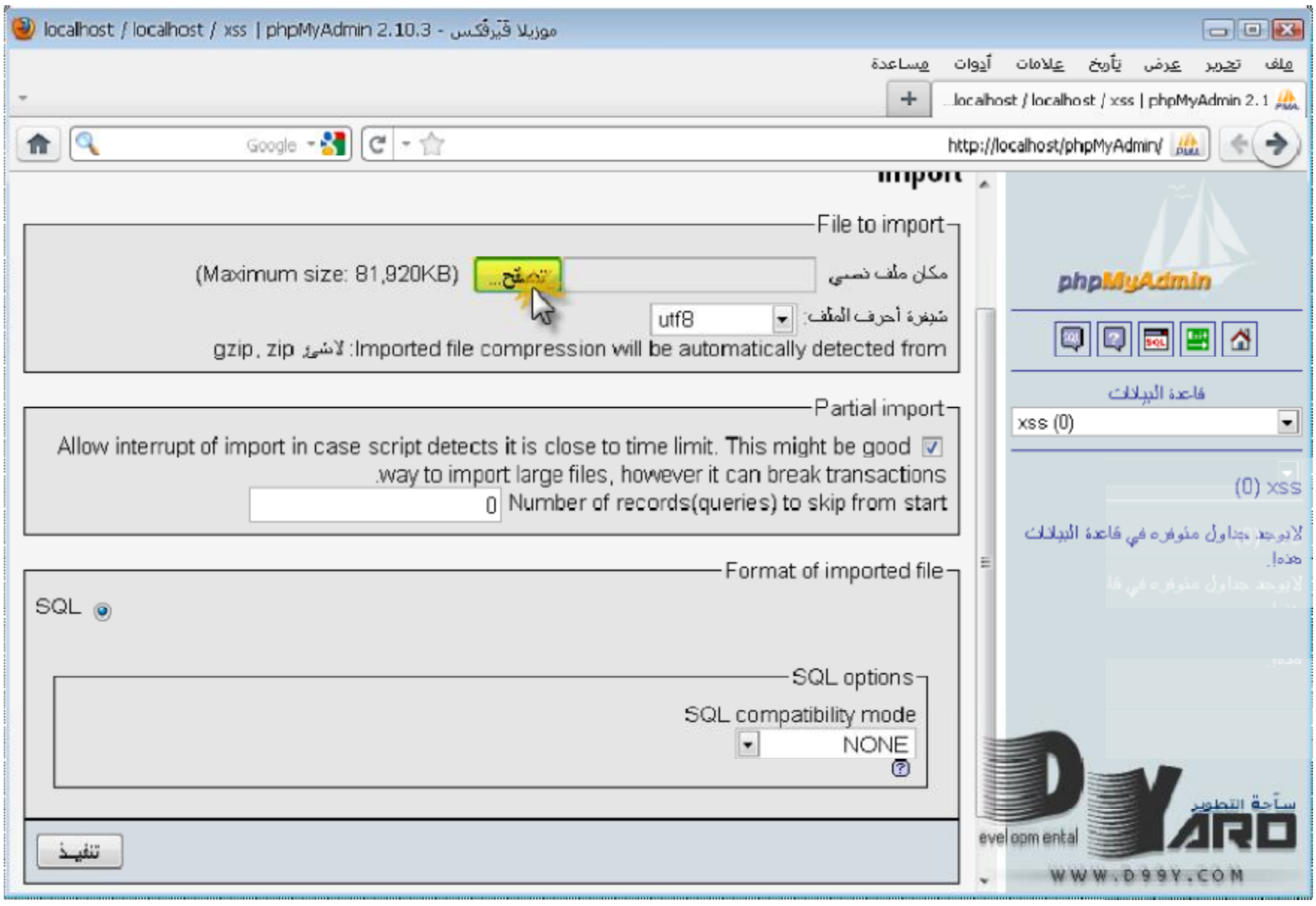


نقوم بعمل قاعدة بيانات جديده باسم! xss



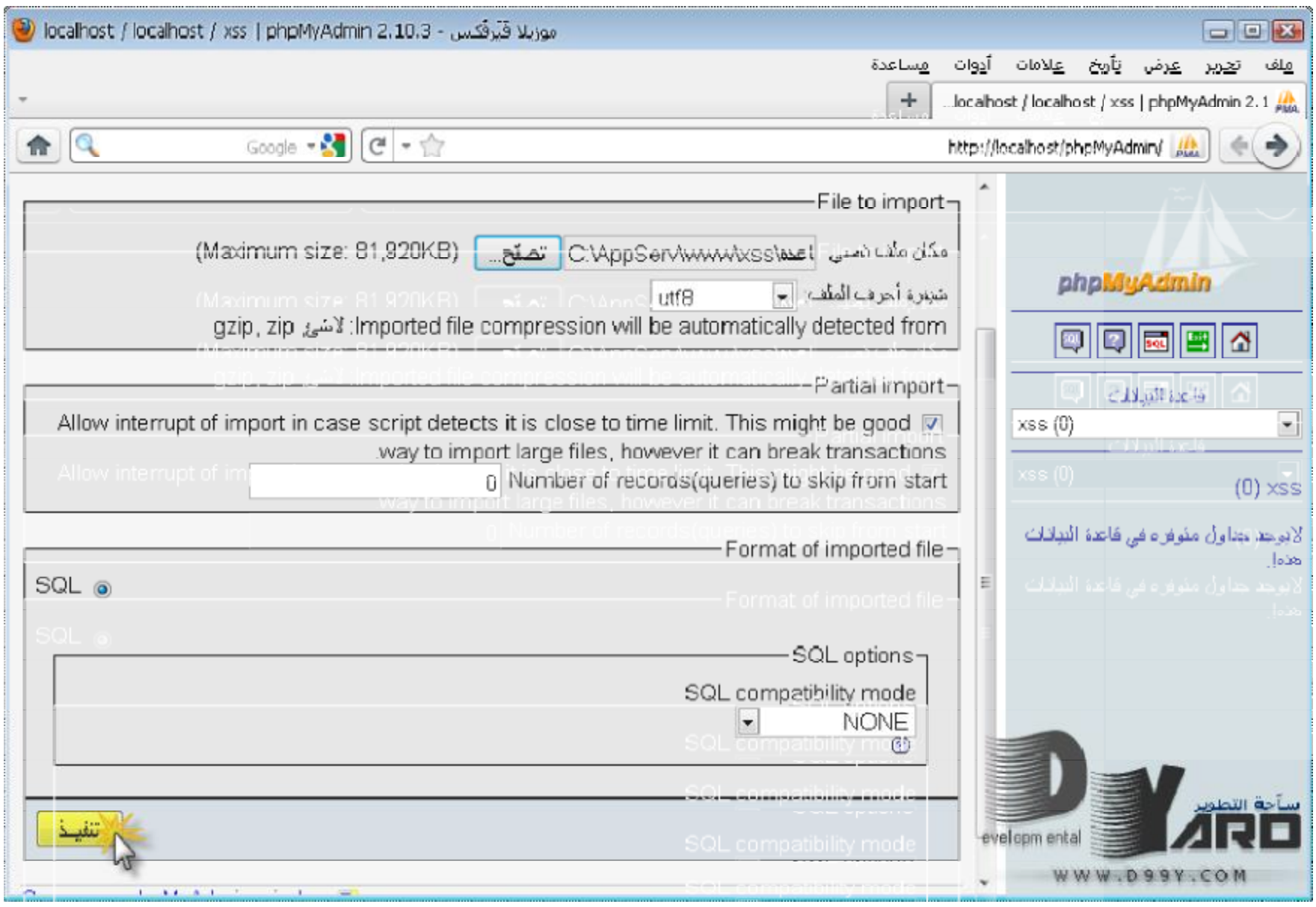
بعد التكوين نقوم باختيار القاعده من القائمة . .

نقوم بالضغط على import لاستيراد قاعدة البيانات . .

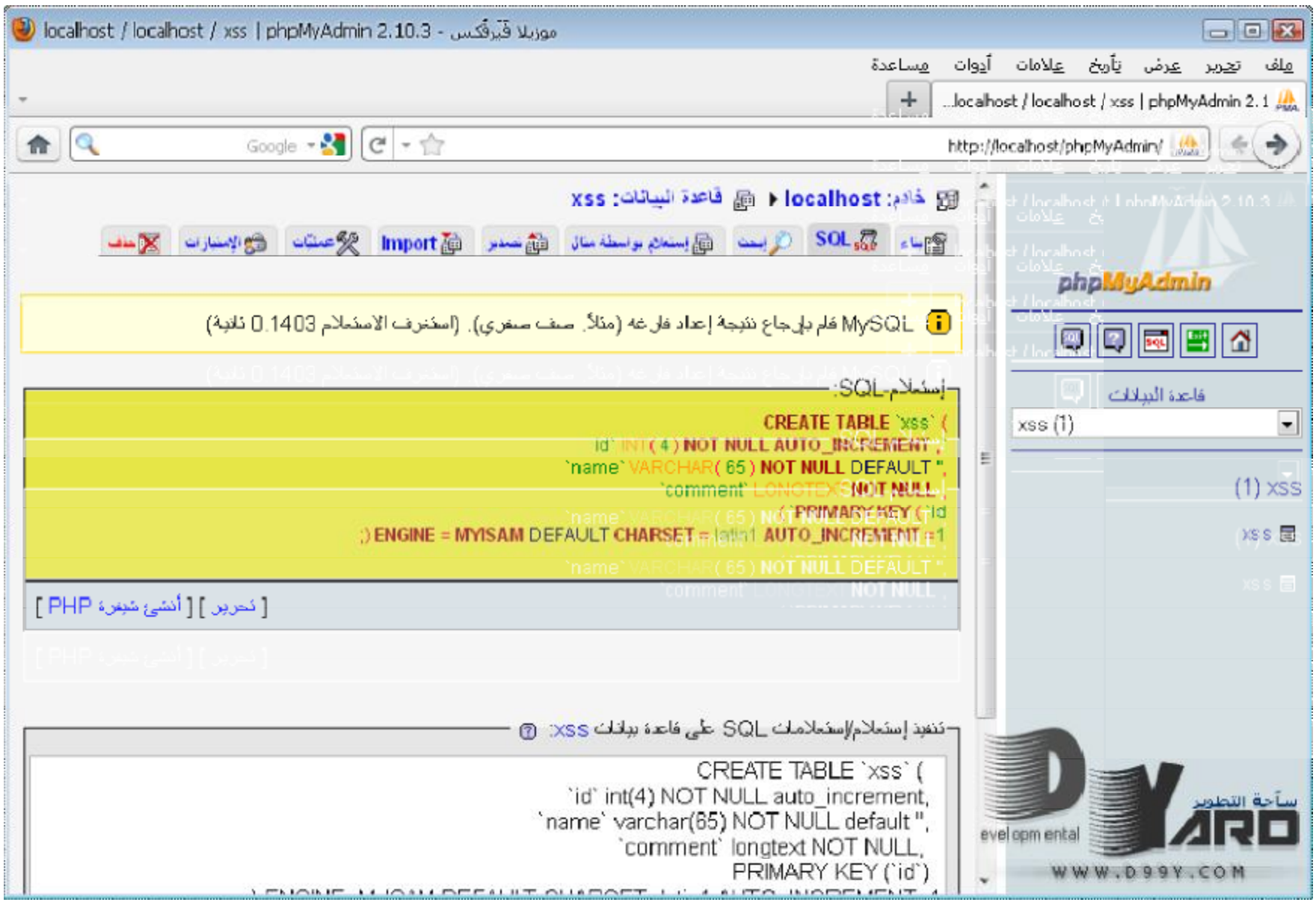


نقوم بالضغط على زر الاستعراض. .

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



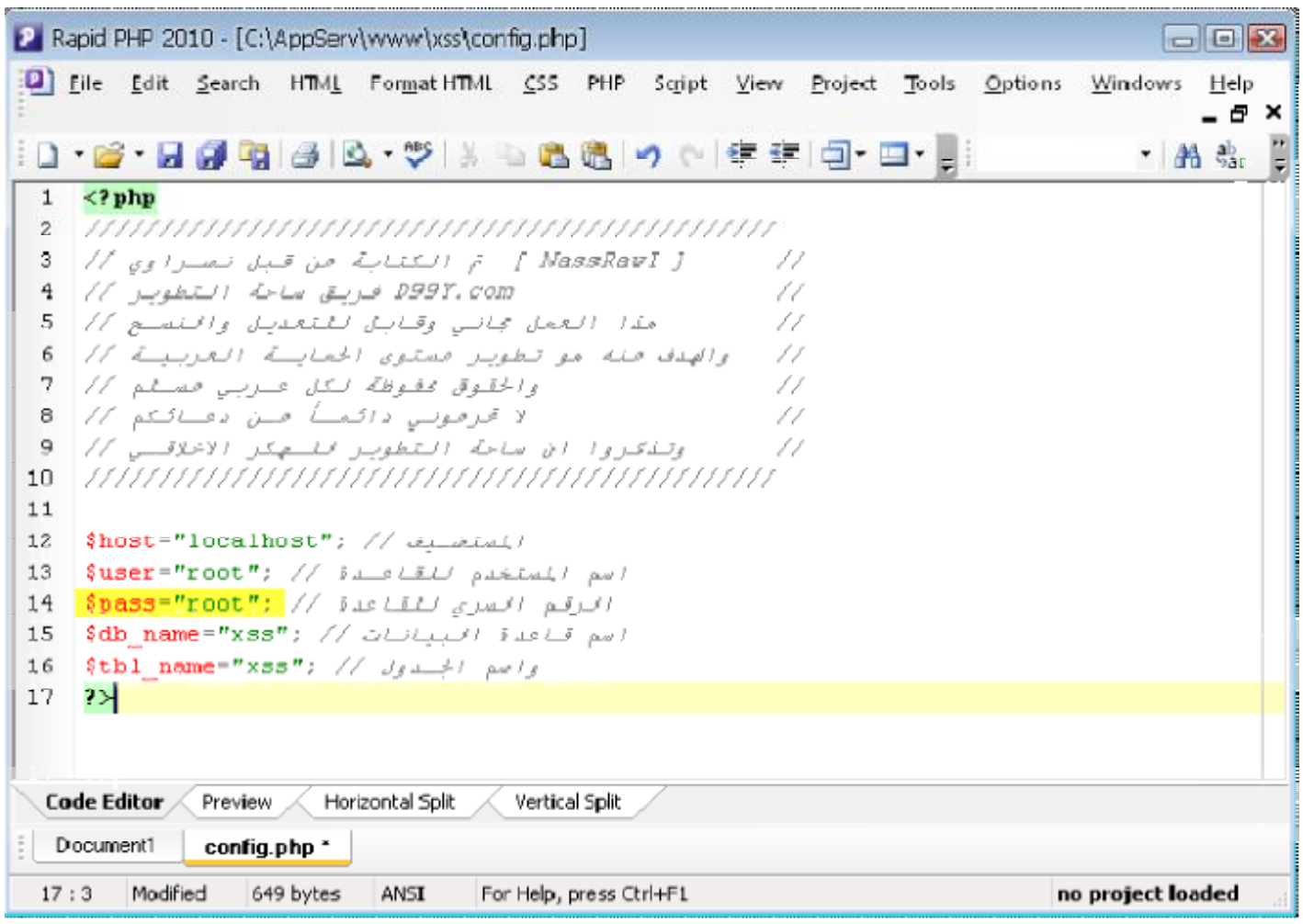
نقوم بالضغط على تنفيذ لاستيراد القاعدة . .



تم الاستيراد وكما تشاهد تم تكوين الجدول وحقوله بنجاح . .

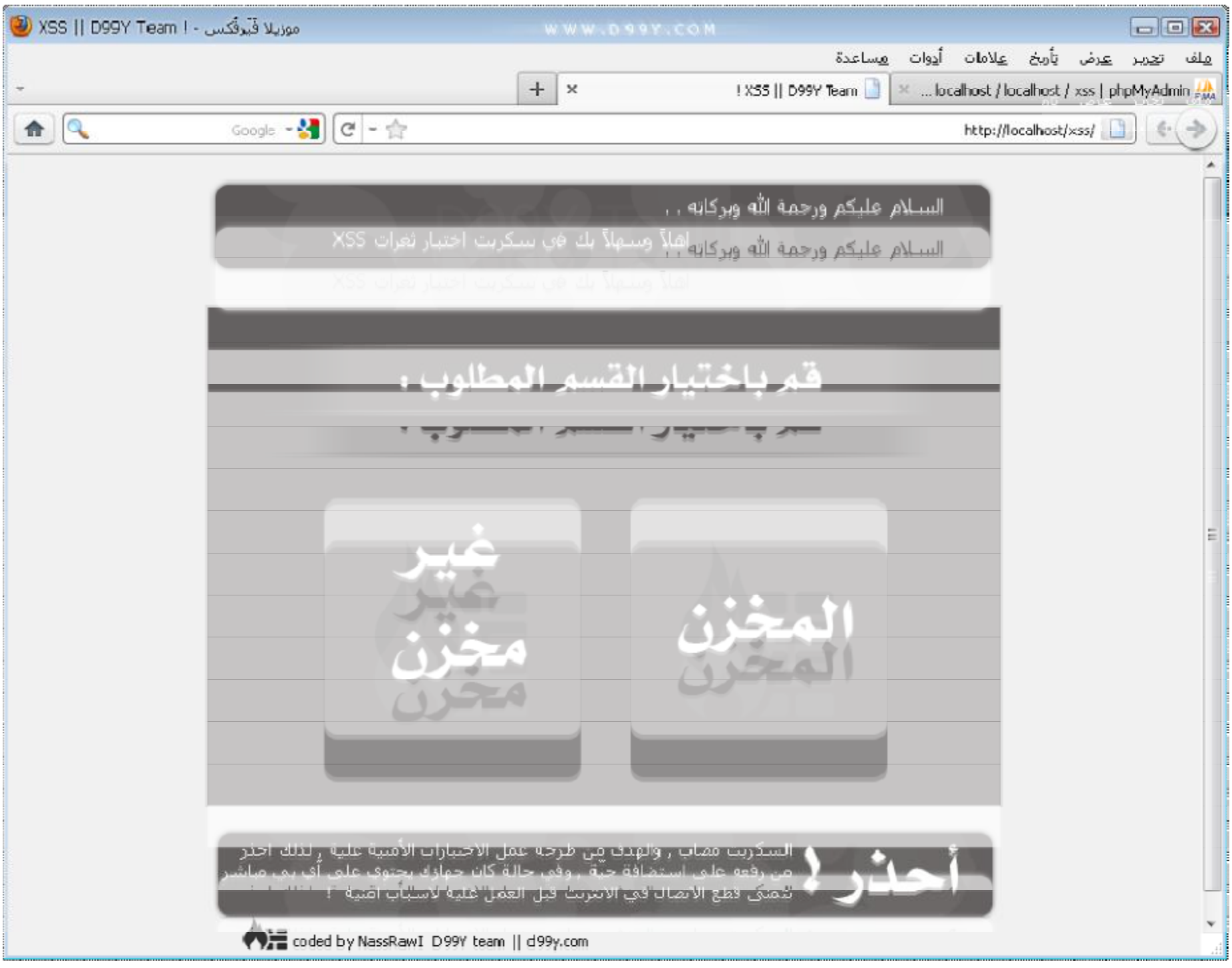
الان نقوم بنقل مجلد السكربت الى السيرفر المحلي داخل مجلد www طبعاً. .

نقوم بتحرير ملف الكونفق! config.php



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

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



كما ذكرت لكم سابقاً ساعمل السكربت وفقاً لانواع الثغرة لكي نعمل المقارنة بالشكّل الجيد .

طبعاً التصميم كلاسيكي متوافق مع هدف السكربت 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 جيّد ومُفيد

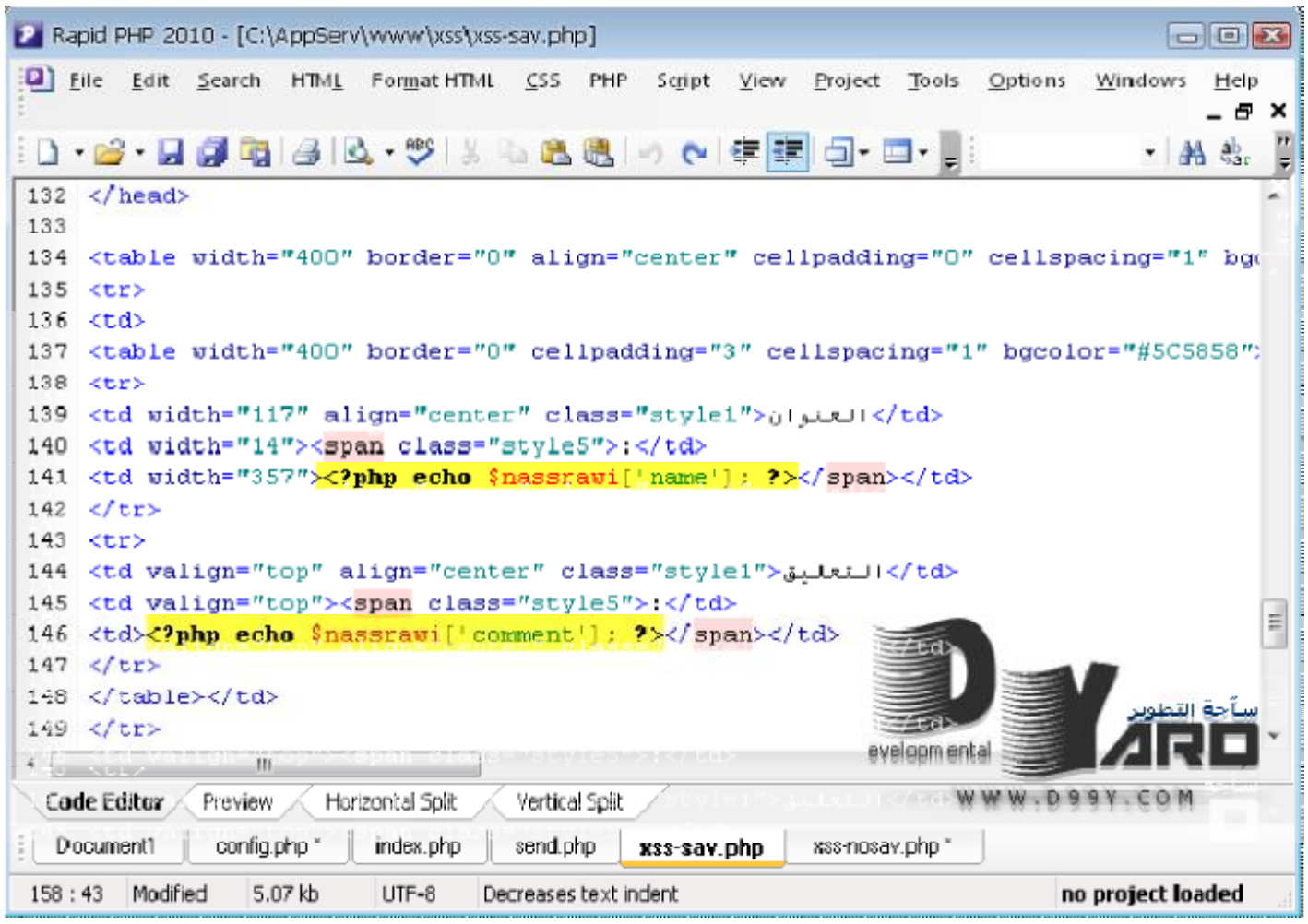
بالنسبة للتحذير ، هو بشكل عام وليس بشكل خاص ، لان السكربت مصاب وقد اعمل سكربتات اخرى اكثر خطورة من ناحية الاستغلال كما ان السكربت مصاب في xss وهو خطير بالفعل ، وبما يخص قطع الاتصال لاصحاب الاتصالات المباشرة مثل الكونكت ، وذلك لان الآي بي لجهازك في حالة كان مباشر يمكن للجميع استعراض سيرفرك في الانترنت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

نقوم باختيار المخزن الاكثر خطورة والاقل في الانتشار. .

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 مُحرّر. .



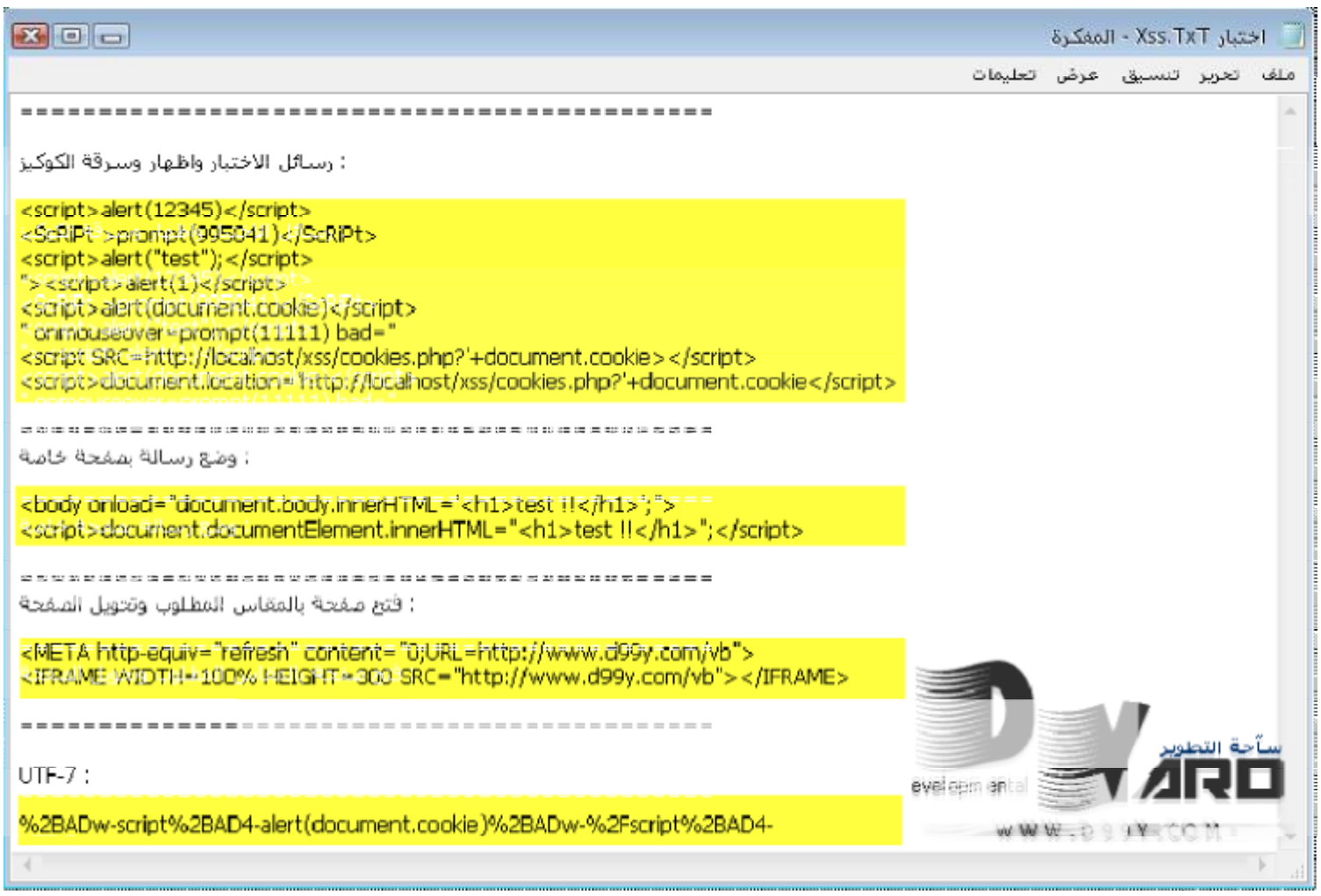
كما تُشاهد هنا ، ان المبرمج طلب طباعة الموجود في حقل الـ name و comment واقصد بها العنوان والتعليق ، دون اي فلترة ، فوراً اطبع وهنا الخطأ البرمجي واضح وهو عدم تأمين المخرجات من القاعده في السطر ! 141 + 146

جيّد تم اكتشاف الخطأ البرمجي ، والان بامكاننا اختبار السكربت , وعمل بعض الاستغلالات عليه . .

اولاً نقوم بتحميل الملف التالي . .

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

الملف يحتوي على ..



اهم الاستغلالات التي اختبر بها السكربتات دائماً . .

في حالة تم تنفيذ اي من الاكواد السابقه هذا يعني ان السكربت مصاب . .

نقوم بتجربة كود اظهار رسالة! alert

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

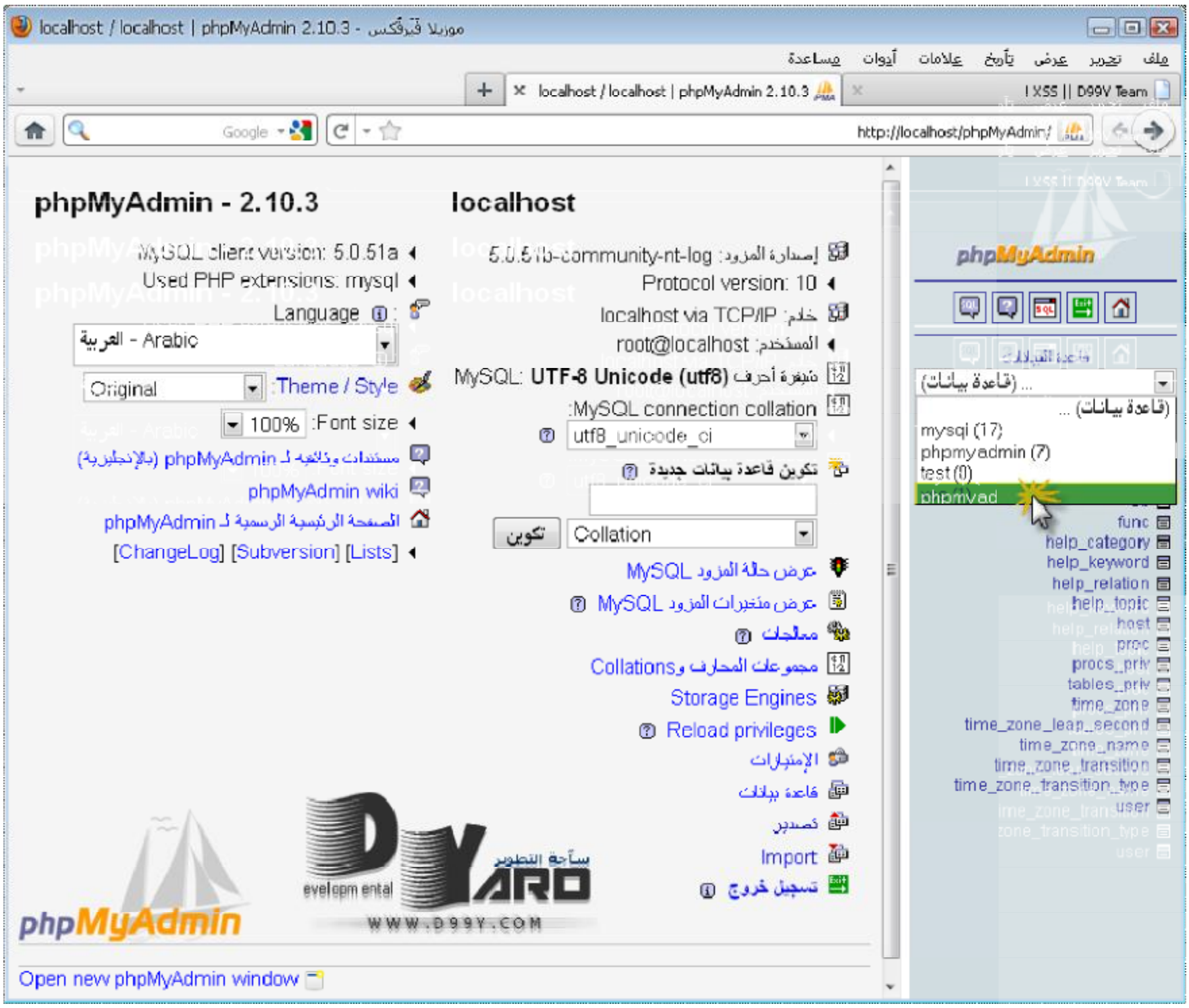
كما تشاهد هنا ظهرت لنا رسالة تحتوي على الارقام المدخله سابقاً ، الان نقول وبكل قوة ان السكربت مصاب نتيجة تجربة احد اكواد الجافا سكربت وتم تنفيذه كما تُشاهد . .

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

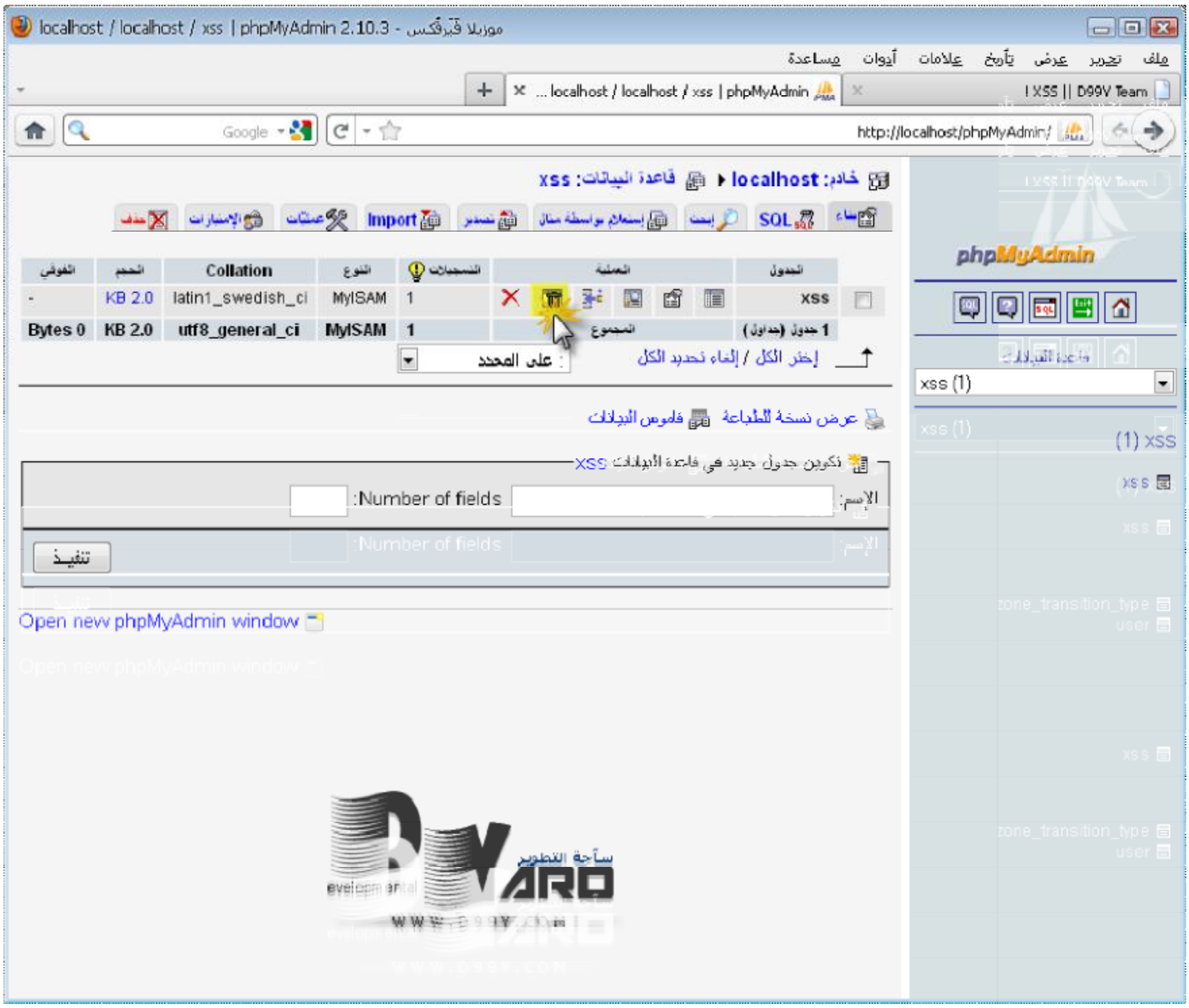
وبامكانك تجربة باقي اكواد التحذير. .

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 .

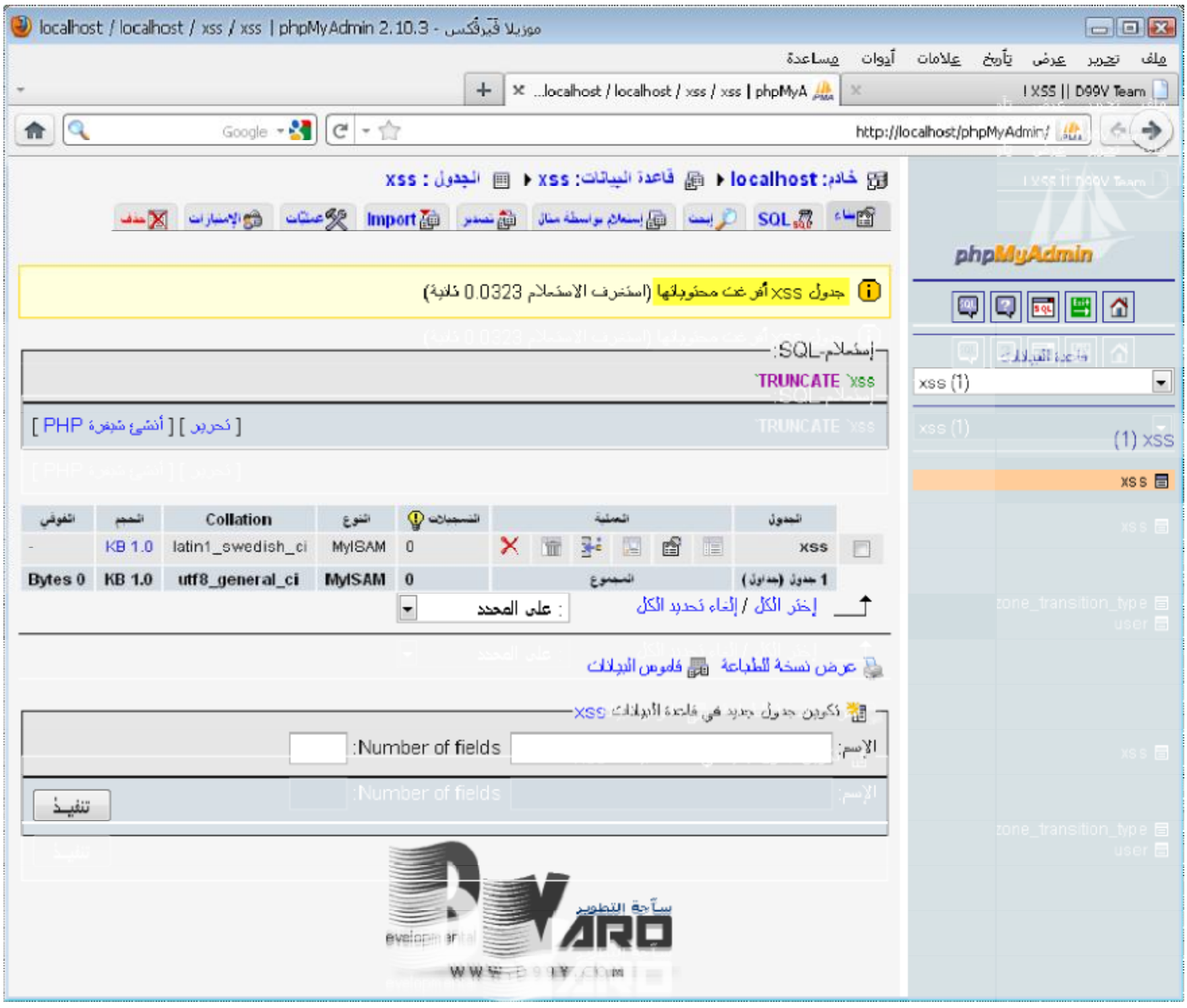


قم بالدخول الى قاعدة البيانات! XSS



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

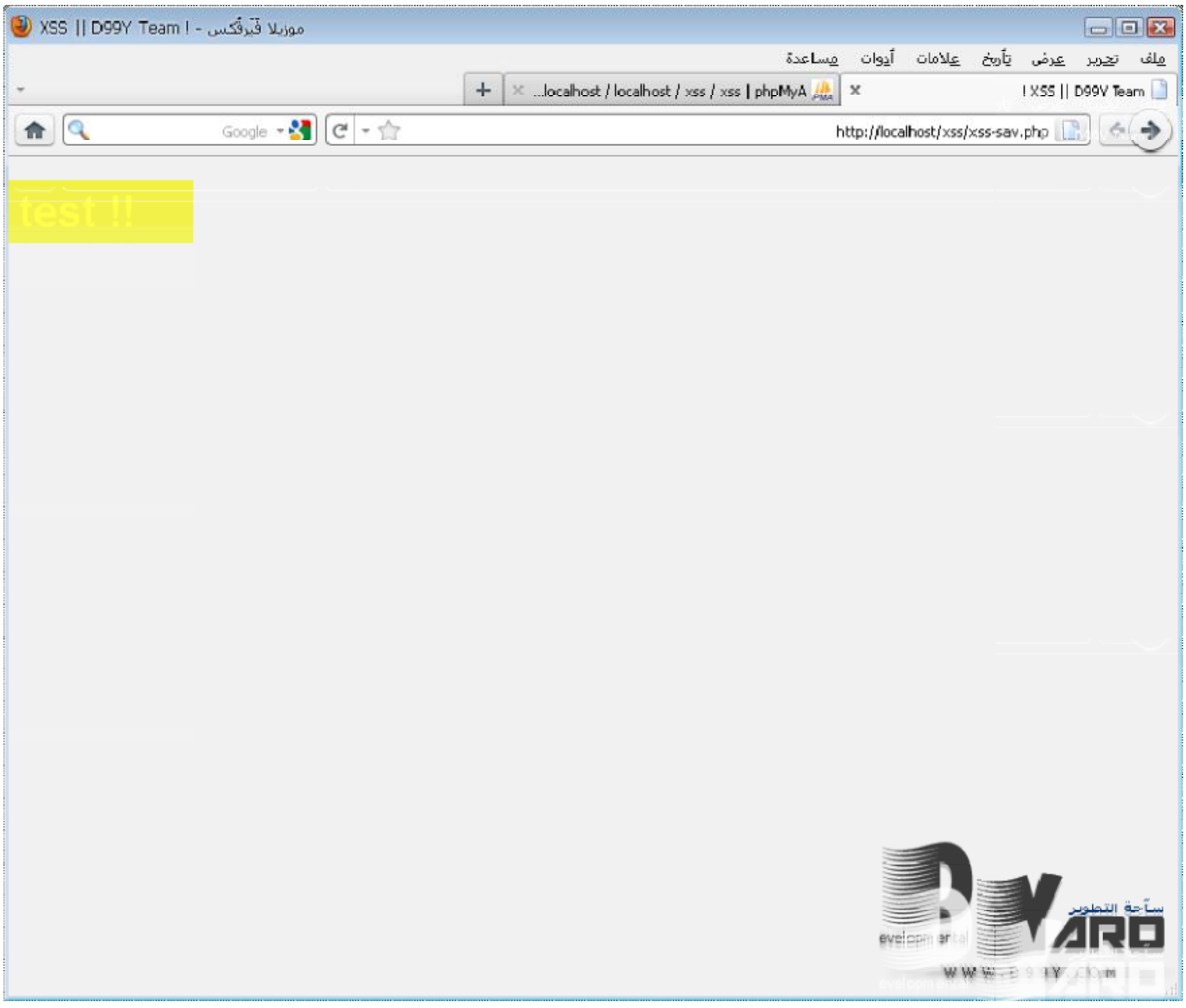
نقوم بالضغط على موافق للموافقة على تفريغ الجدول ..



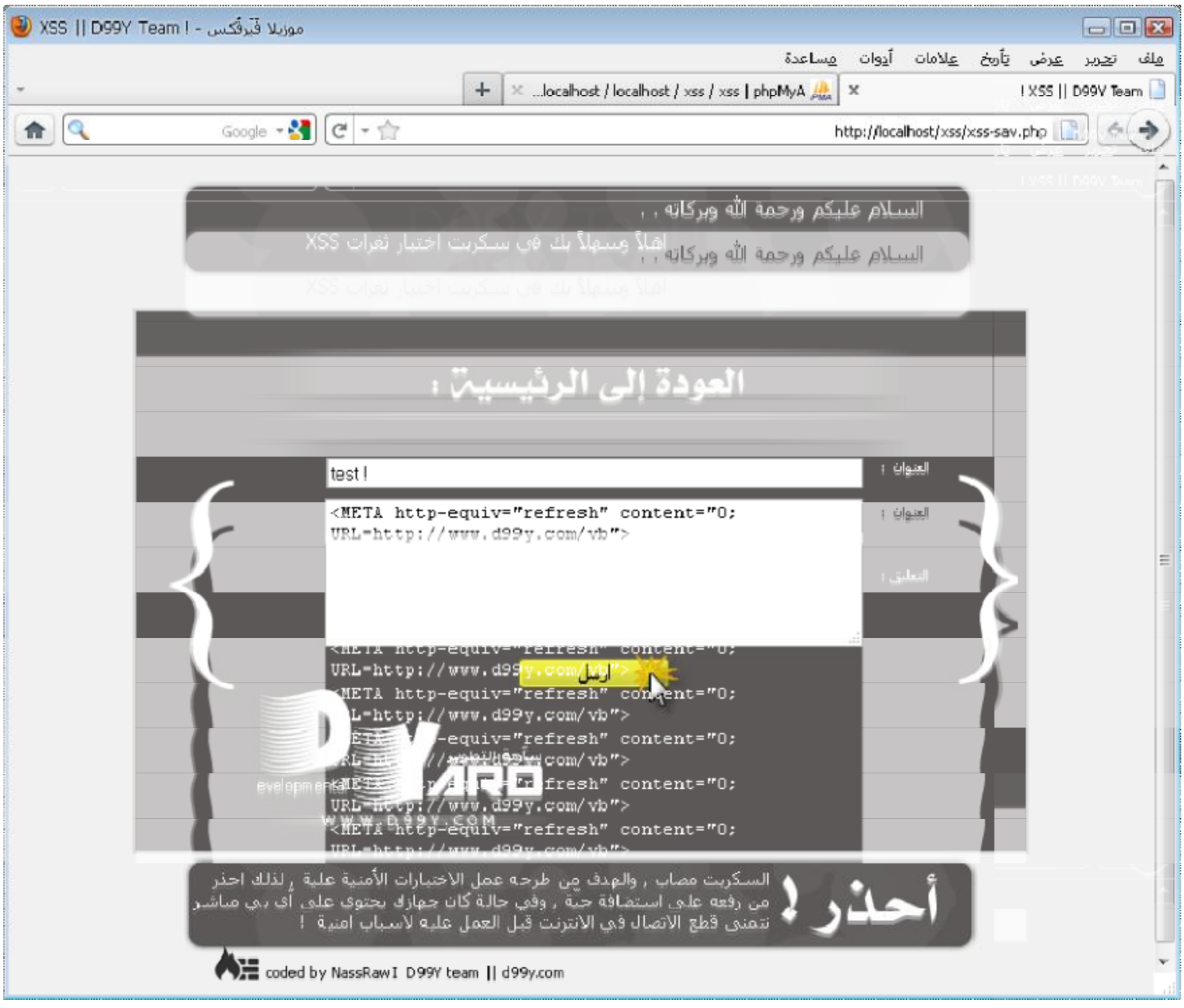
كما تشاهد تم تفريغ الجدول بنجاح. .

والان 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



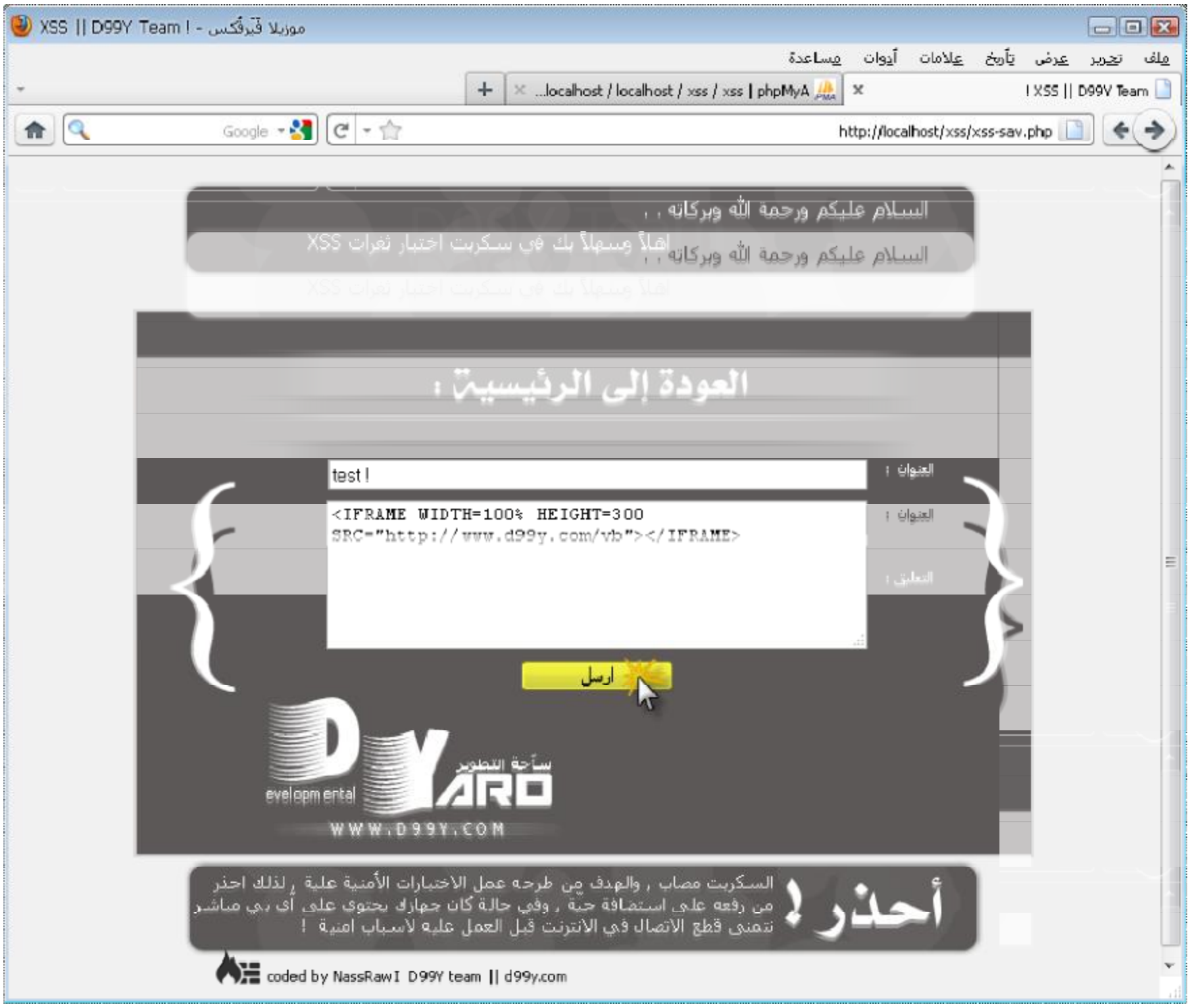
كما تشاهد خطر الثغرة يصل حتى الى تشويه الاندكس واظهار رسالة ، نقوم بتفرغ القاعده كما تعلمنا سابقاً لتجربة استغلال اخر. .



نقوم بتجربة كود التحويل بعد فتح الصفحة نجد ..

كما تشاهد بعد فتح الصفحة تجد ان المتصفح يقوم بفتح الموقع

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



هذا كود الفلاش وللاسف 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 الكبيره ، باختراق جهاز صاحب السكربت وكذلك الزوار , عن طريق استخدام الاستغلال السابق وفتح صفحة ملغّمه في اي ثغرة يقبلها نظام صاحب السكربت + بعرض وارتفاع صغير وهذا يعني انه لا يرى فتح الصفحة ولكن سيتم فتح الصفحة!!

طبعاً هذا الاستغلال خاص في مخترقي الانظمة وليس مخترقي السكربتات ، لذلك عملت فديو 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_dllloader داخل مشروع الـ , metasploit ووضع رابط المجلد المصاب داخل الصفحة بعرض وارتفاع صغير لكود الفلاش المعروف. .

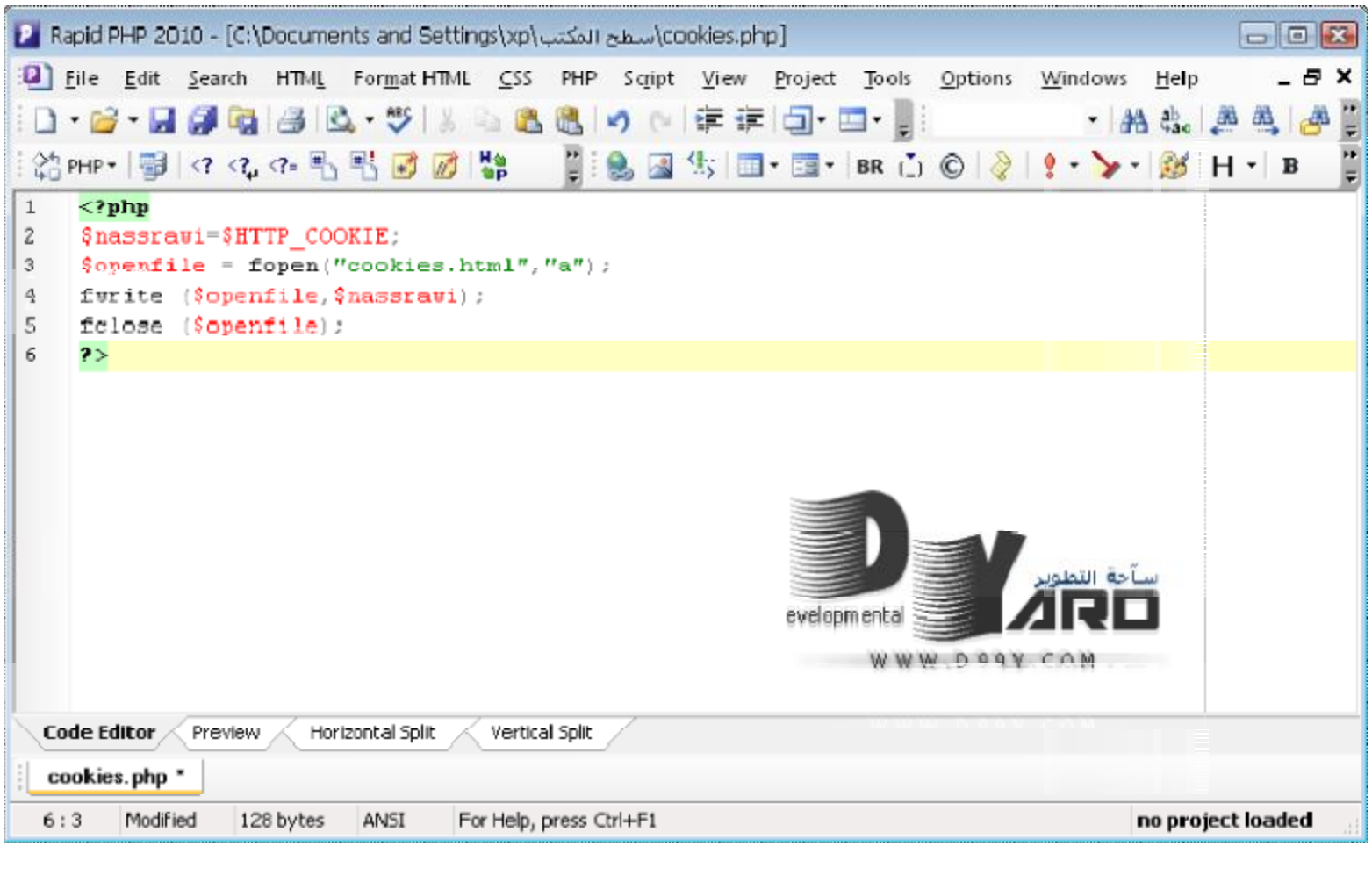
وكما تشاهد تم اختراق الجهاز بنجاح , وهذا يعني اختراق مدير السيرفر والزوّار كذلك ، لذلك ذكرت ان ثغرة XSS خطيره جداً ولا يستهان ابداً بها. .

نذهب اخيراً الى اخر استغلال واقدم استغلال ، وهو سرقة الكوكيز ، كما يعلم الجميع ان اي عضوية تقوم بتسجيل الدخول لها رمز امني يمّيزها 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 طلبات وشخصية الزائر ، فمثلاً هناك اللغه اسفل المنتدى ان قمت باختيار اللغه الانجليزيه مثلاً هناك كوكيز يميّزك وفي دخولك مستقبلاً للموقع تجد انه فعلاً لازال حافظ تغيّراتك للغه 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 سكربت بسيط يحتوي على. .



كما تشاهد سكربت بسيط هدفه سرقة الكوكيز وفتح ملف باسم co okies.html بدون مسافة وكتابة الكوكيز المسروق فيه . .

للتحميل.

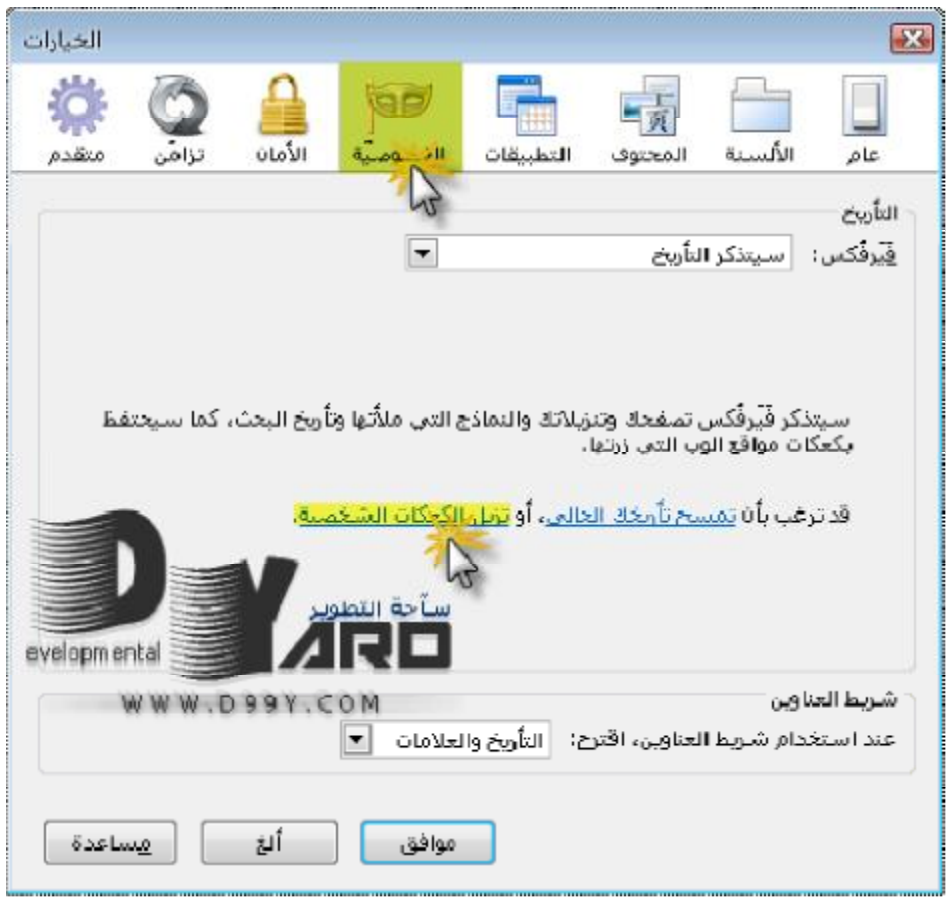
http://www.mediafire.com/?4if697yals6lfaz

نقوم بنقله الى مجلد السكربت . . XSS

اولاً نقوم بعمل اختبار لاظهار الكوكيز , وبعد ذلك نقوم بسرقته . .

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 سرقته . .

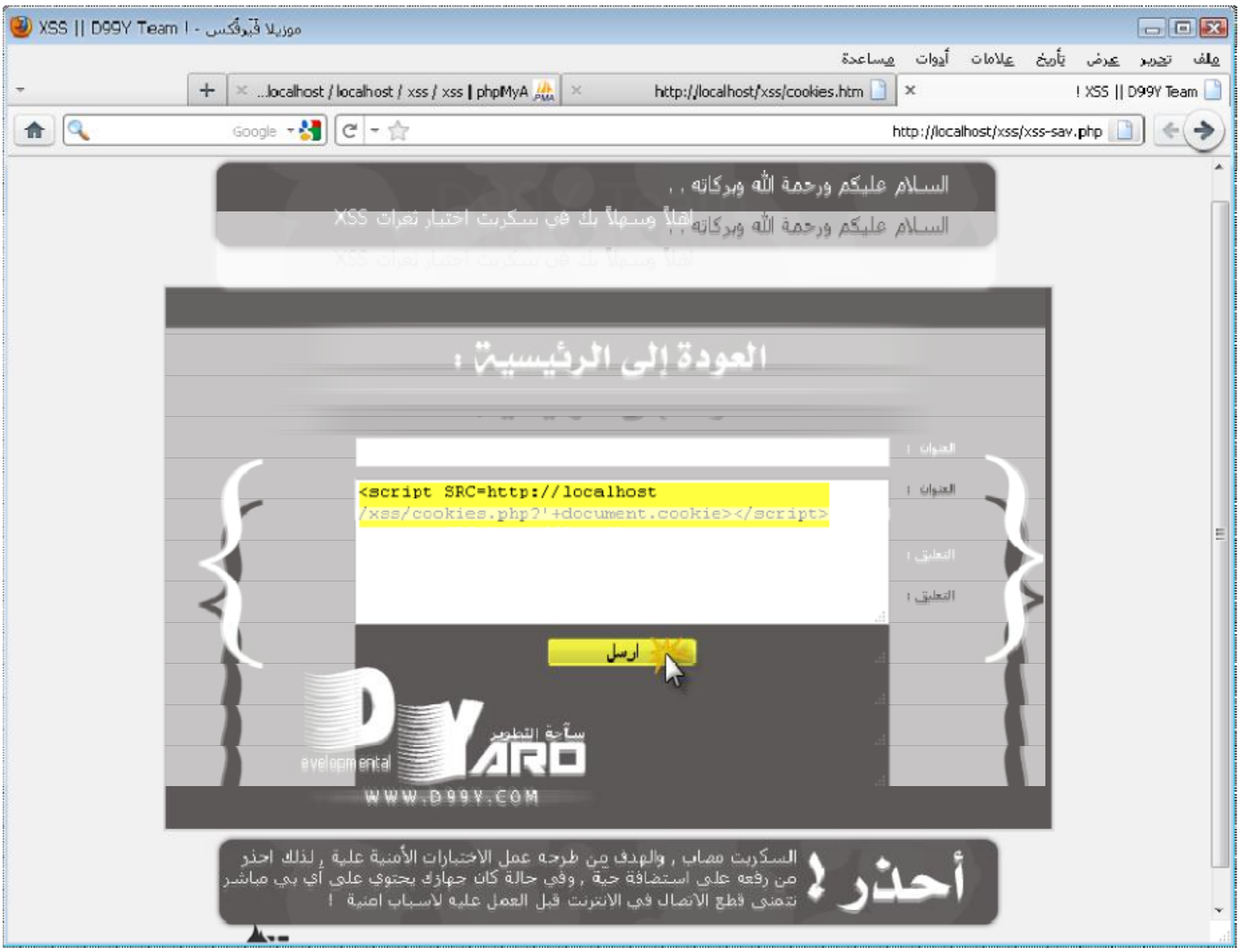
طبعاً بامكانك عرض الكوكيز من المتصفح. .



الخصوصية + تنزيل الكعكات الشخصية . .

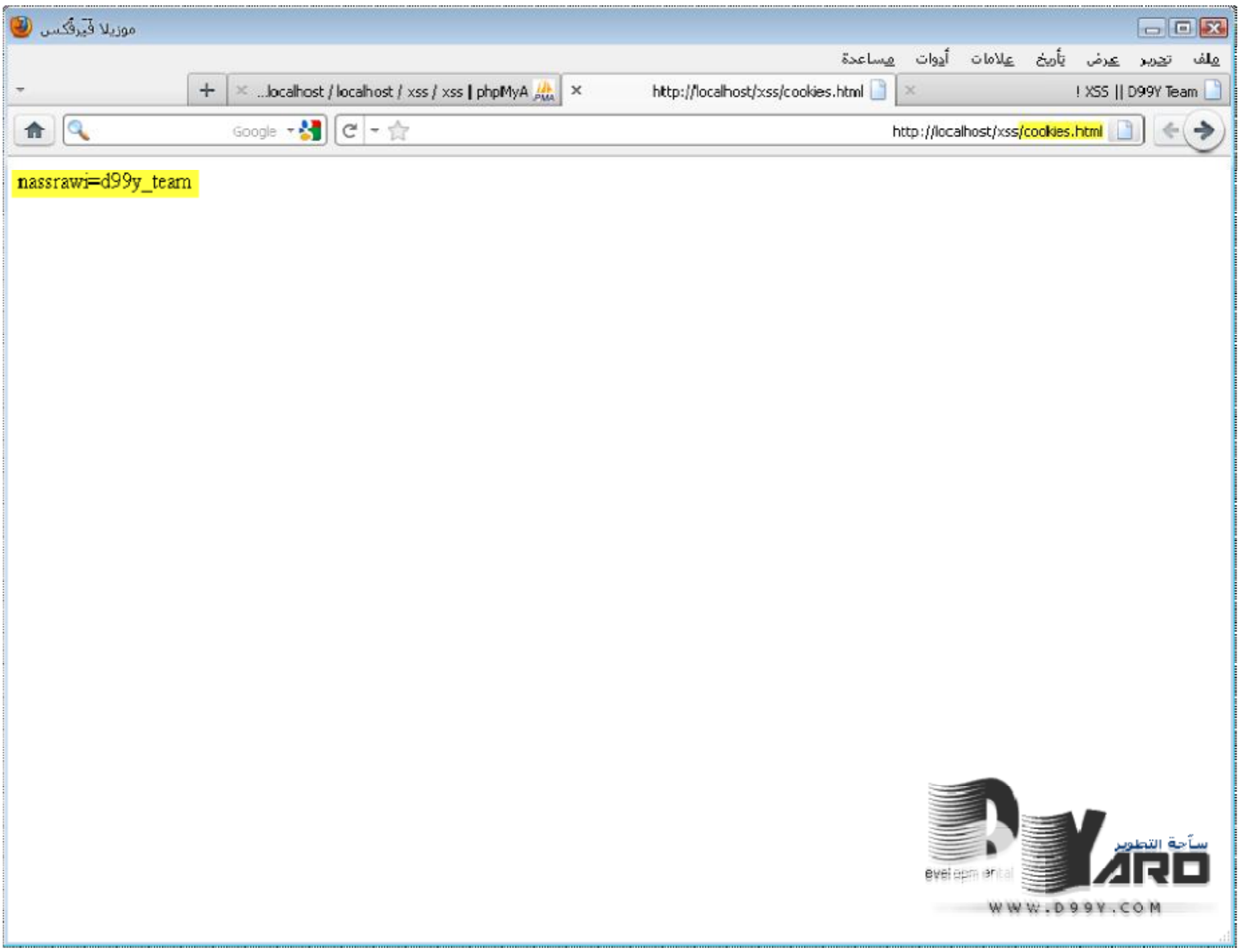
كما تشاهد الكوكيز ، ولكن انا القصد من اظهار الكوكيز من السكربت وذلك لاني اعمل اختبار امني للسكربت ، واتأكد اني قادر فعلاً على سرقة الكوكيز الذي املكه!

بعد نقل الملف co okies.html بدون مسافة الى مجلد السكربت نقوم بعمل الاختبار

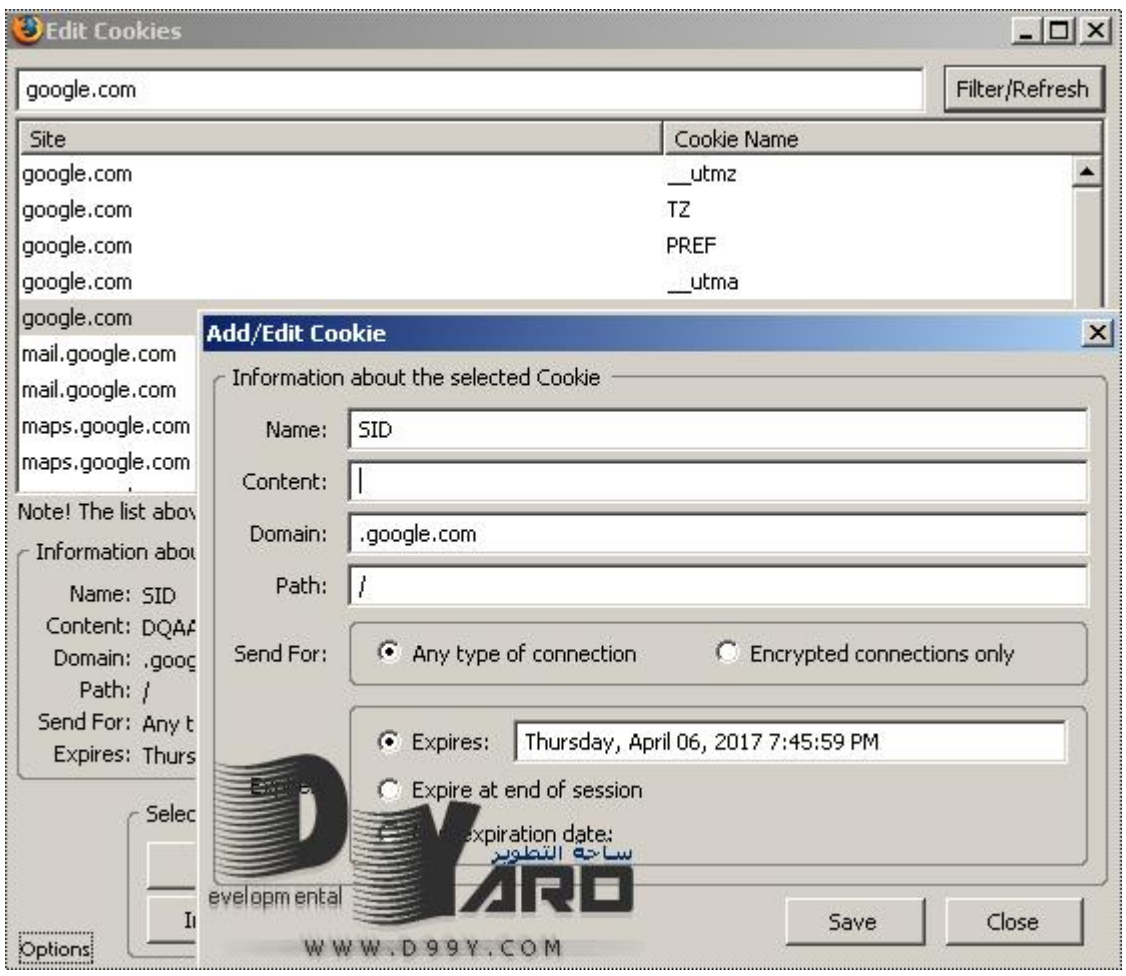


نقوم باستخدام الاستغلال الخاص في سرقة الكوكيز كمثال للسكربت الذي قمنا بتنزيله سابقاً . . .

الان نقوم باستعراض ملف co okies.html بدون المسافة الذي عمله السكربت الخاص في سرقة الكوكيز . .

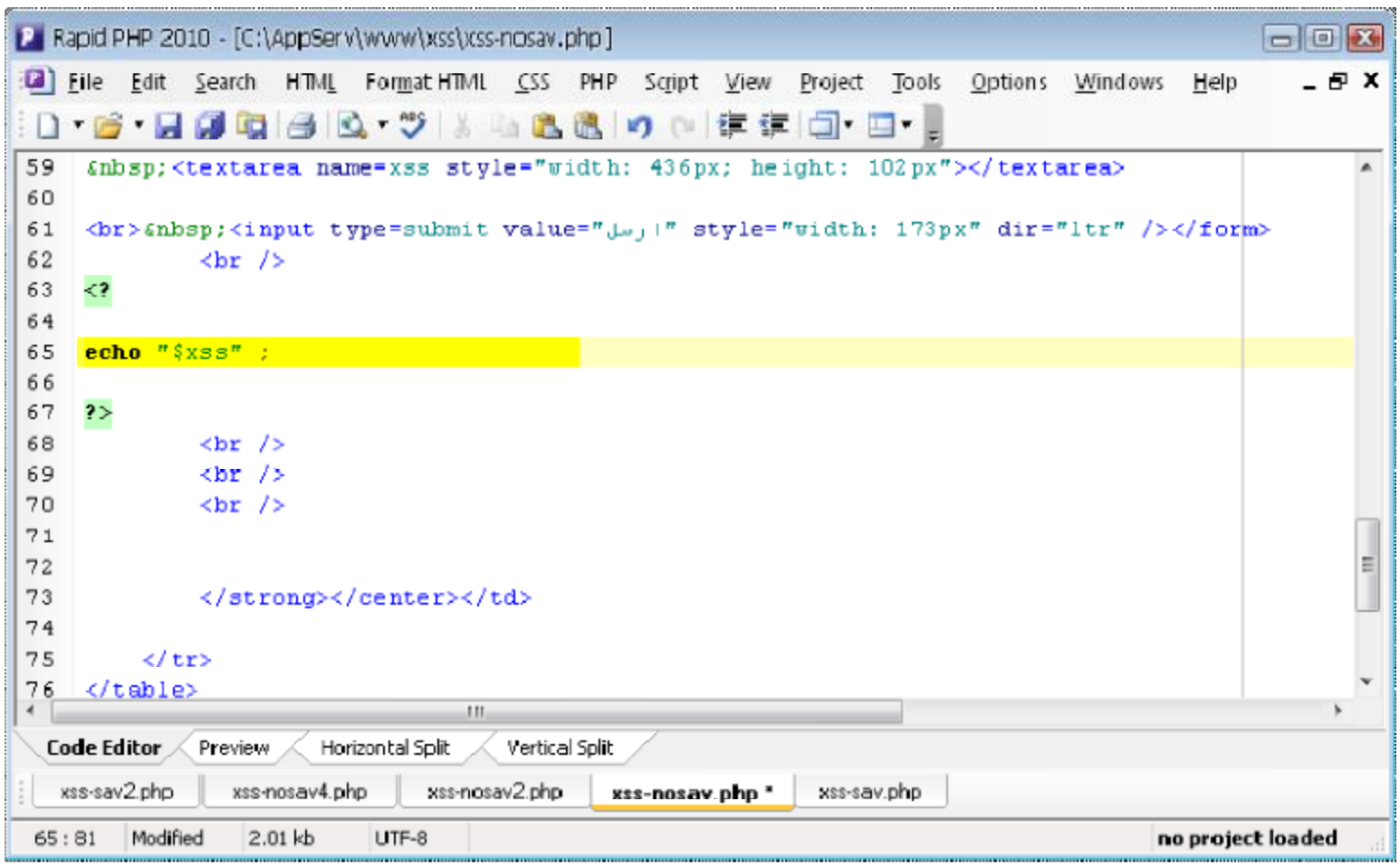


وكما تشاهد تم سرقة الكوكيز بنجاح , والاستغلال خطير ، للسكربتات التي لها منافذ تسجيل دخول ، ويمكنك تعديل الكوكيز الى المسروق بواسطة. .

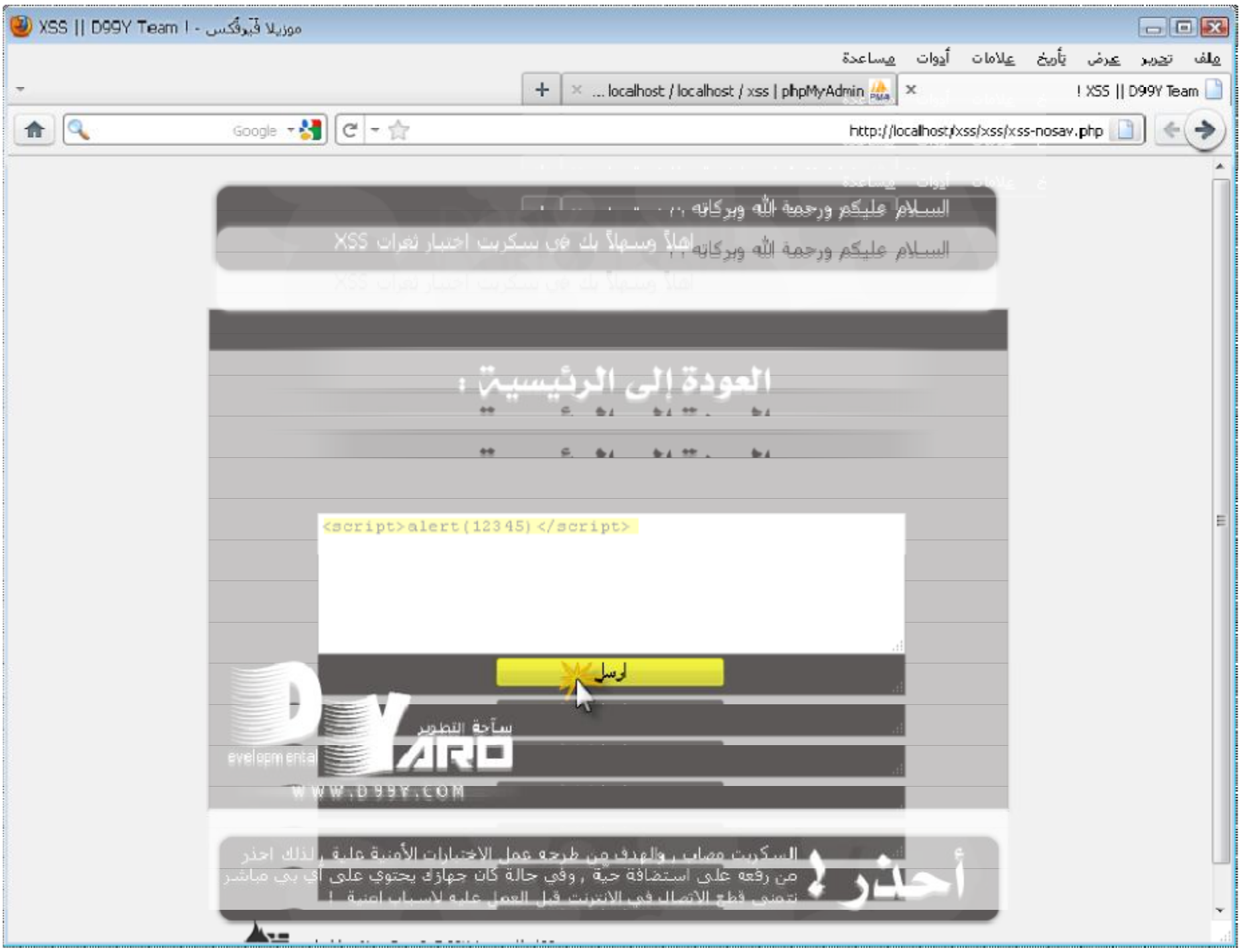


اضافة Edit Co okies المعروفة للفايرفوكس ، وبذلك الدخول الى عضوية الادمن ، ولكن بوجهة نظري ان اختراق الجهاز الاستغلال الاكثر خطورة اما سرقة الكوكيز سيكون بصلاحيات محدوده بعكس عندما يملك الرقم السري الفعلي للعضوية يمكنه التحكم بشكل كامل وتعديل الاعدادات واعادة تغيير الرقم السري ويملك جهاز المُدير كذلك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

واخيراً الان نقوم بالدخول الى النوع الغير مُخزّن!

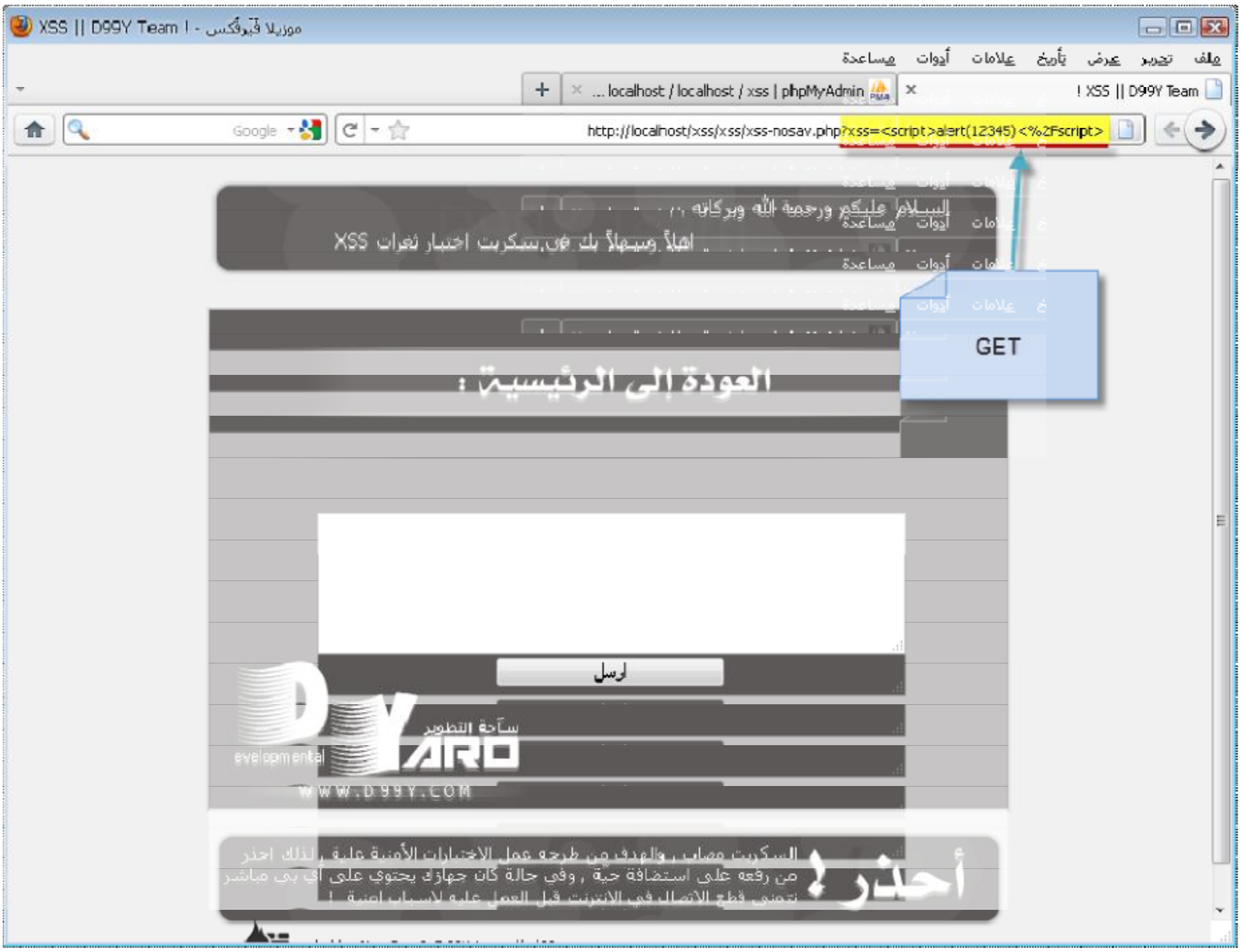


اولاً كما تشاهد الخطأ البرمجي واضح في سطر 65 عدم تأمين المُخرجات . .



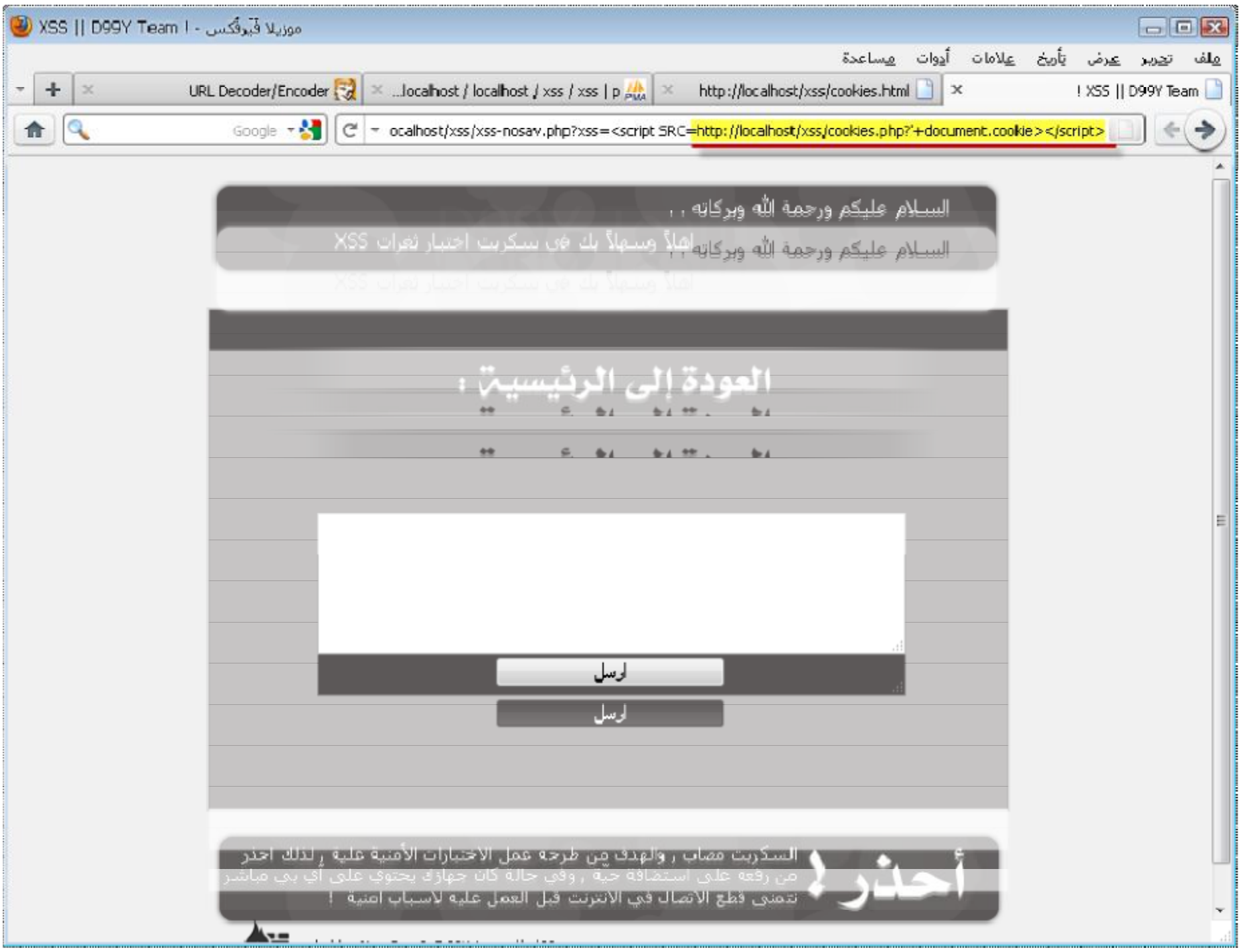
نقوم بعمل رسالة اختبار 12345 كما تعلمنا في السكربت المُخزّن . .

وكما تشاهد تم التّنفيذ بنجاح . .



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

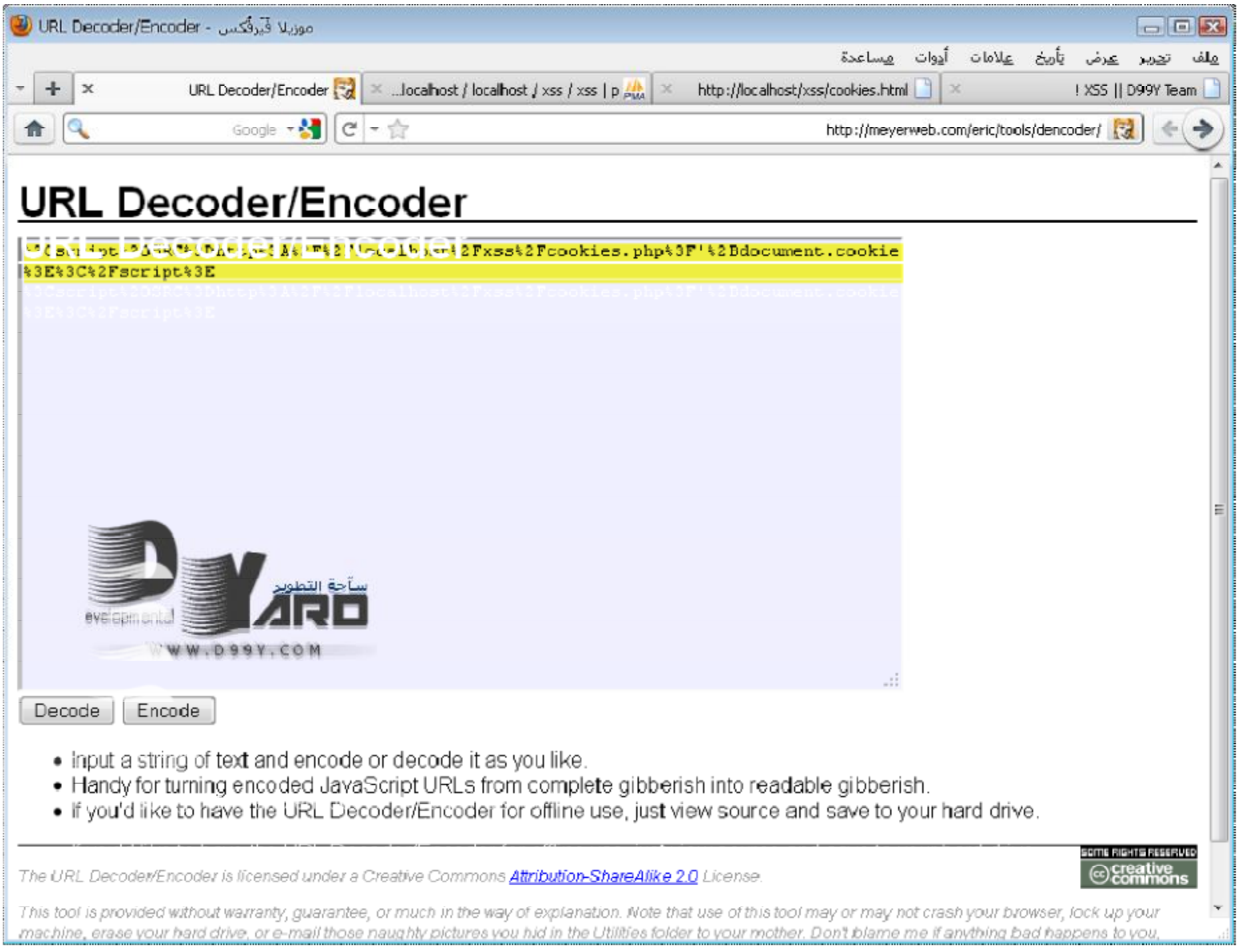
ولكن الحاجة ام الاختراع والمُخترق دائماً يضع افكار توصله لنتائج مفيده ، مثلاً الان كما نشاهد في السكربت الغير مُخزّن ان المدخل يظهر في الرابط سواءً GET | POST وسيتمكن من الاستغلال ، لذلك من الممكن للمخترق ان يستغل الامر بارسال الرابط الذي يحتوي مثلاً على استغلال سرقة الكوكيز ، الى مُدير السكربت وبذلك اختراقه ولكن عن طريق الارسال ودخول الرابط بعكس السابق . .



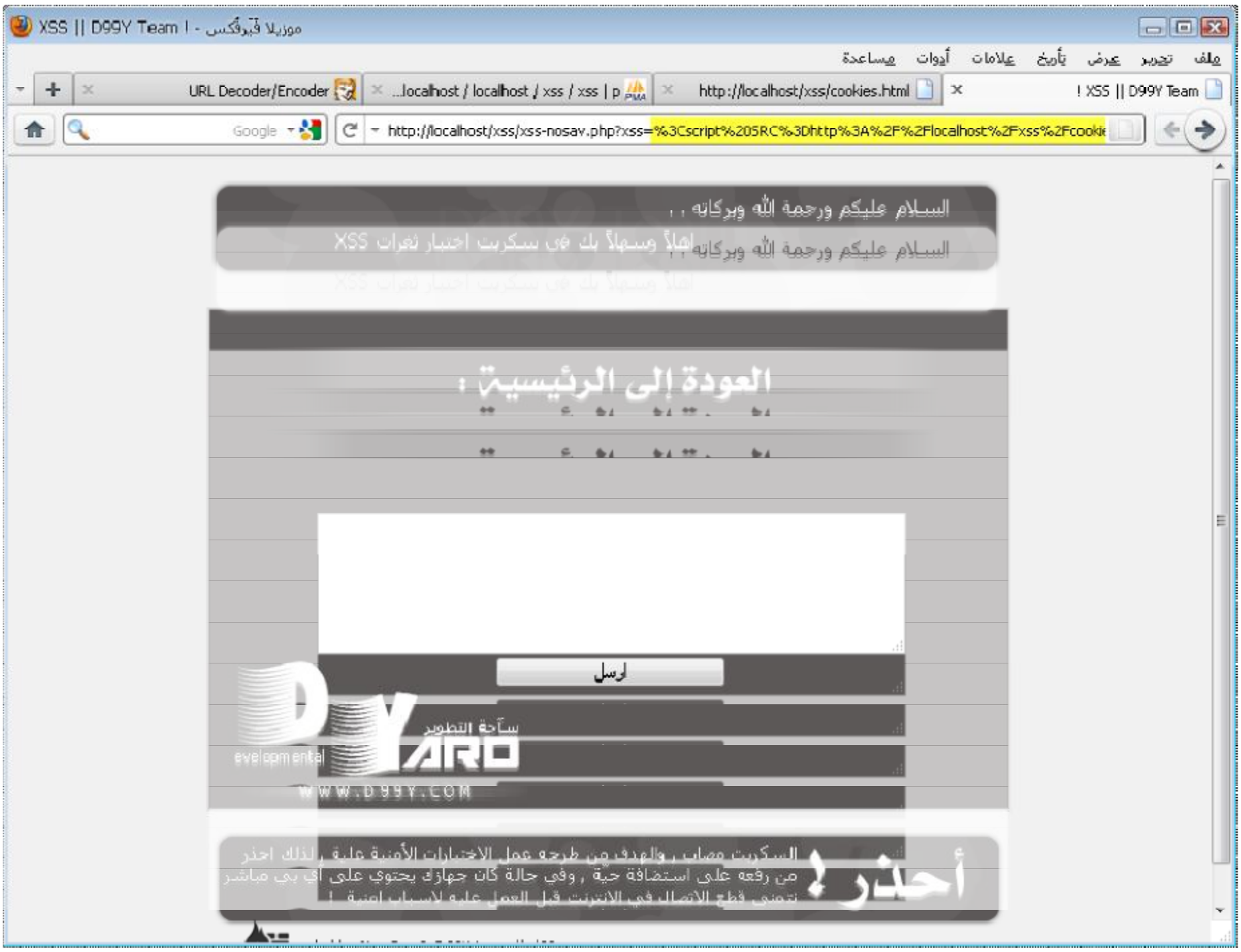
كما تُشاهد نقوم بارسال الرابط بهذا الشكل لغرض سرقة الكوكيز ، قد يأتي شخص ويقول ان الاستغلال واضح لمدير الموقع ، من الممكن تشفير الرابط مابعد الاستغلال في موقع يقدم خدمة تشفير الروابط وهو . .

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

نقوم بالدخول الى الموقع وتشفير كود الجافا سكربت للمراوغة



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



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

الان تعلّمنا ان السكربت المخزن حين دخول الشخص الى السكربت ، سيجد الرد الملغّم 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 مُخزّن . .

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

اخيراً الترقيع

اهلاً وسهلاً بكم احبّتي ، واتمنى للجميع بالصحة والعافية

تمّ بحمد الله الانتهاء من المقدمه والاستغلال والاكتشاف ، والان حان وقت ترقيع الثغرة ، والتأكد من سلامة الترقيع . .

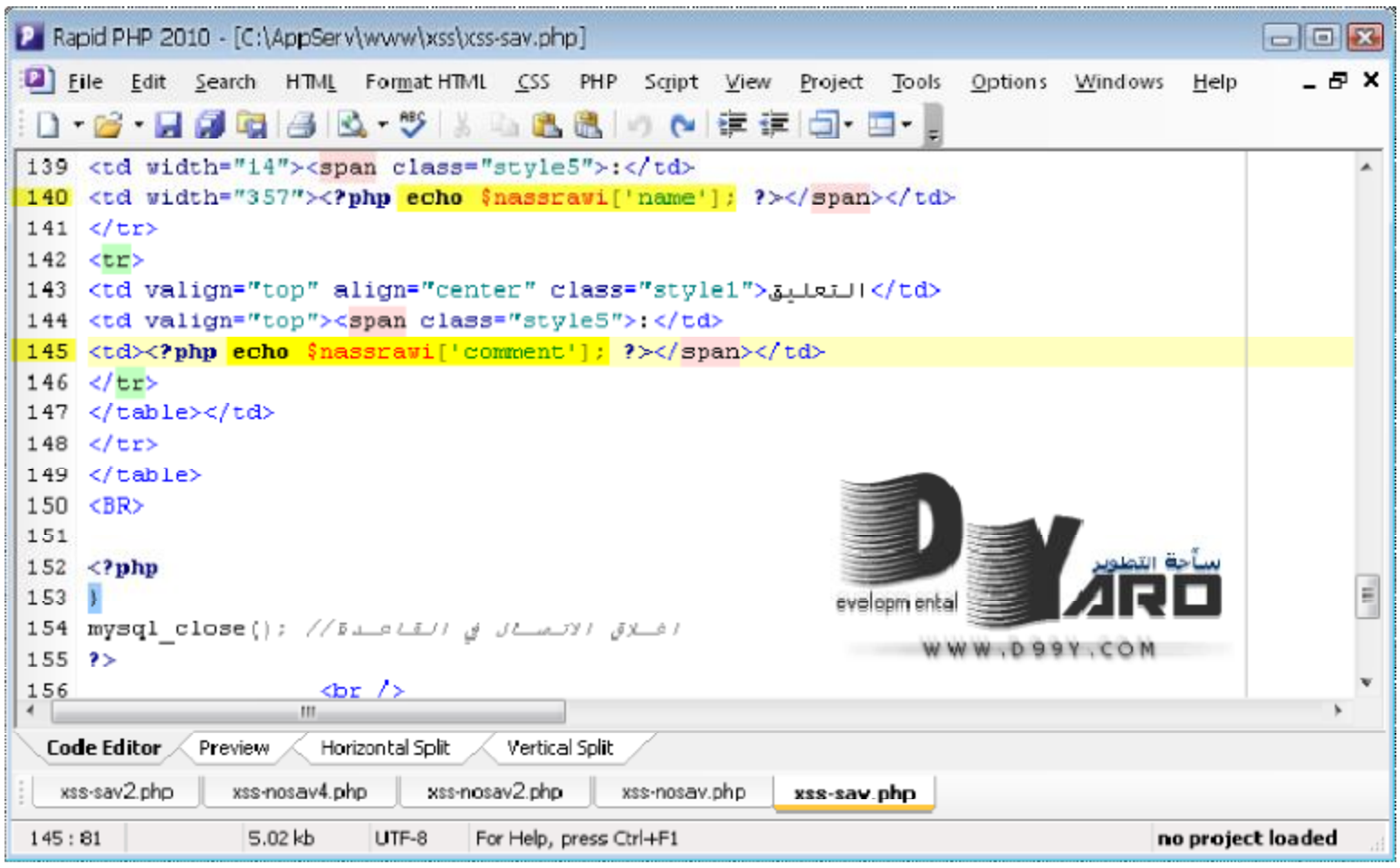
تعرّفنا سابقاً ان الثغرة تقوم على سبب عدم فلترة المُخرجات , وكذلك تعرّفنا ان المخترق يحتاج الى وسوم html , Java script والخ لحقنها في الصفحة وتنفيذها. .

طبعاً الـ php وفرت وظائف داخليه لفلترة المخرجات مثل تعطيل الوسوم الهامه < , > , " , ' , / وجميع الرموز التي لابد من توفّرها لتفعيل الكود. .

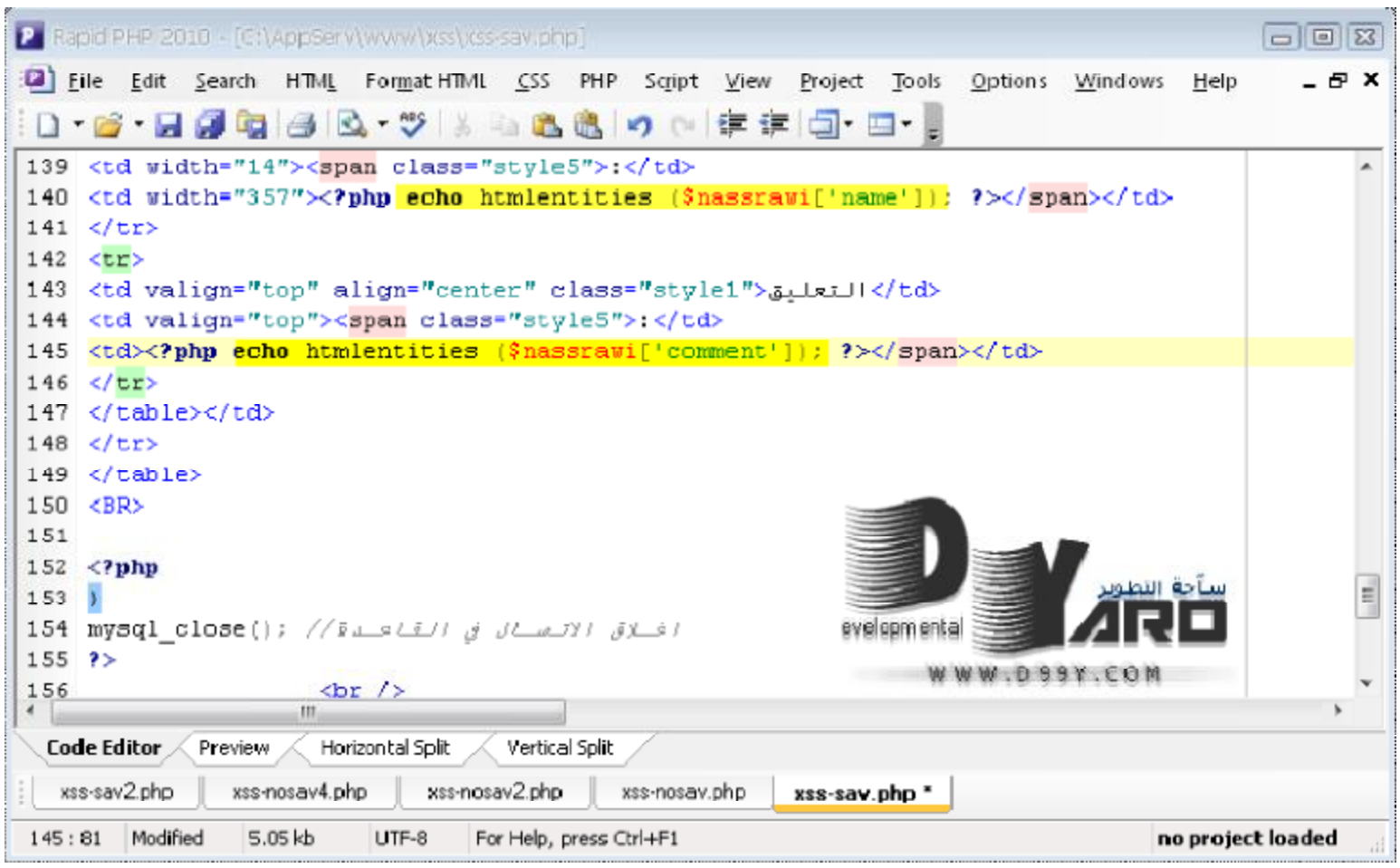
هناك دوال تقوم بحذفها والاخرى تقوم بتعطيلها وطباعتها , سأقوم بشرح افضل الدوال حتى الان متوفره وجاهزه في الـ PHP وحلول فاشله ، وكذلك عمل دالة خاصة بنا للترقيع!

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

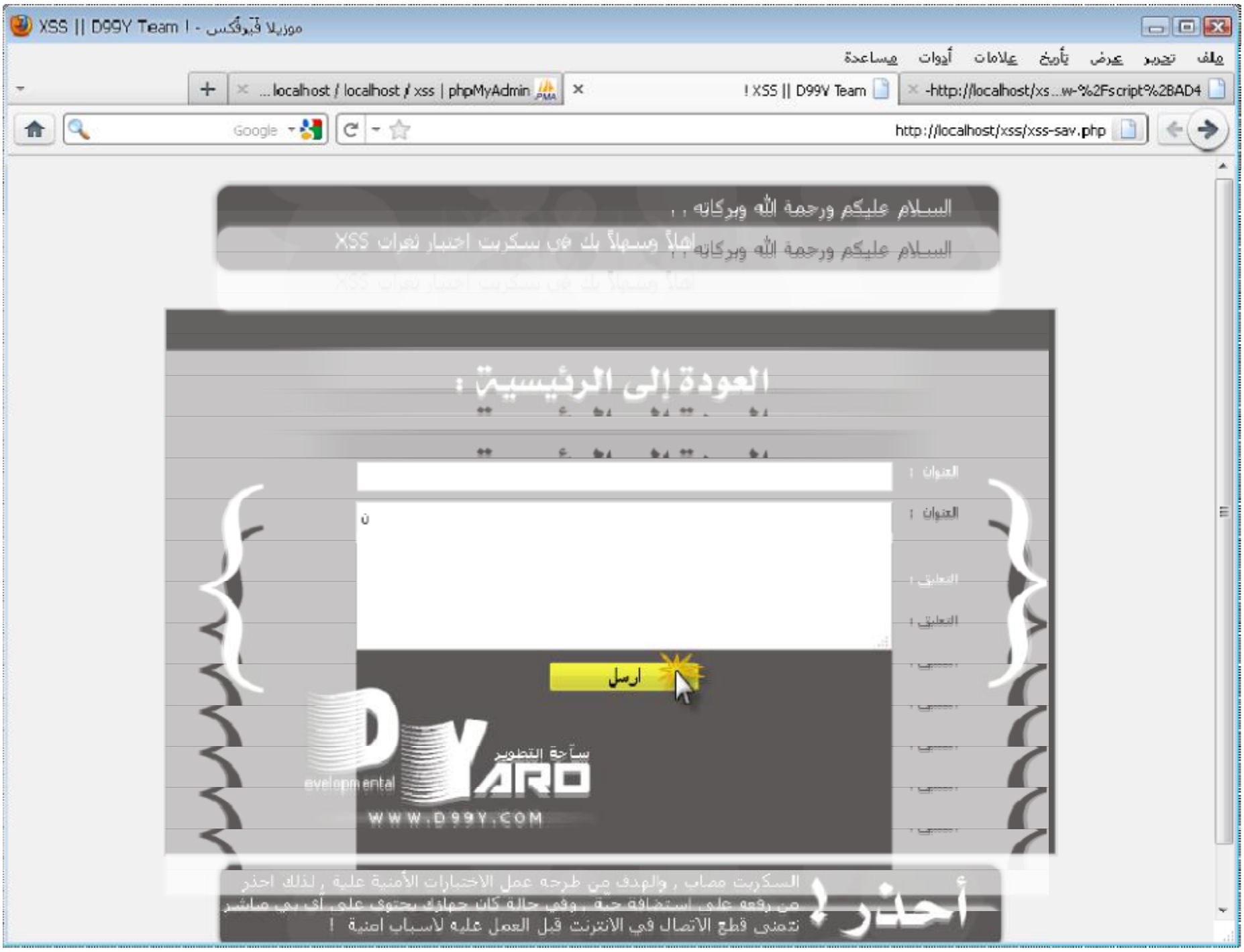
تجربة الدالة . .



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



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



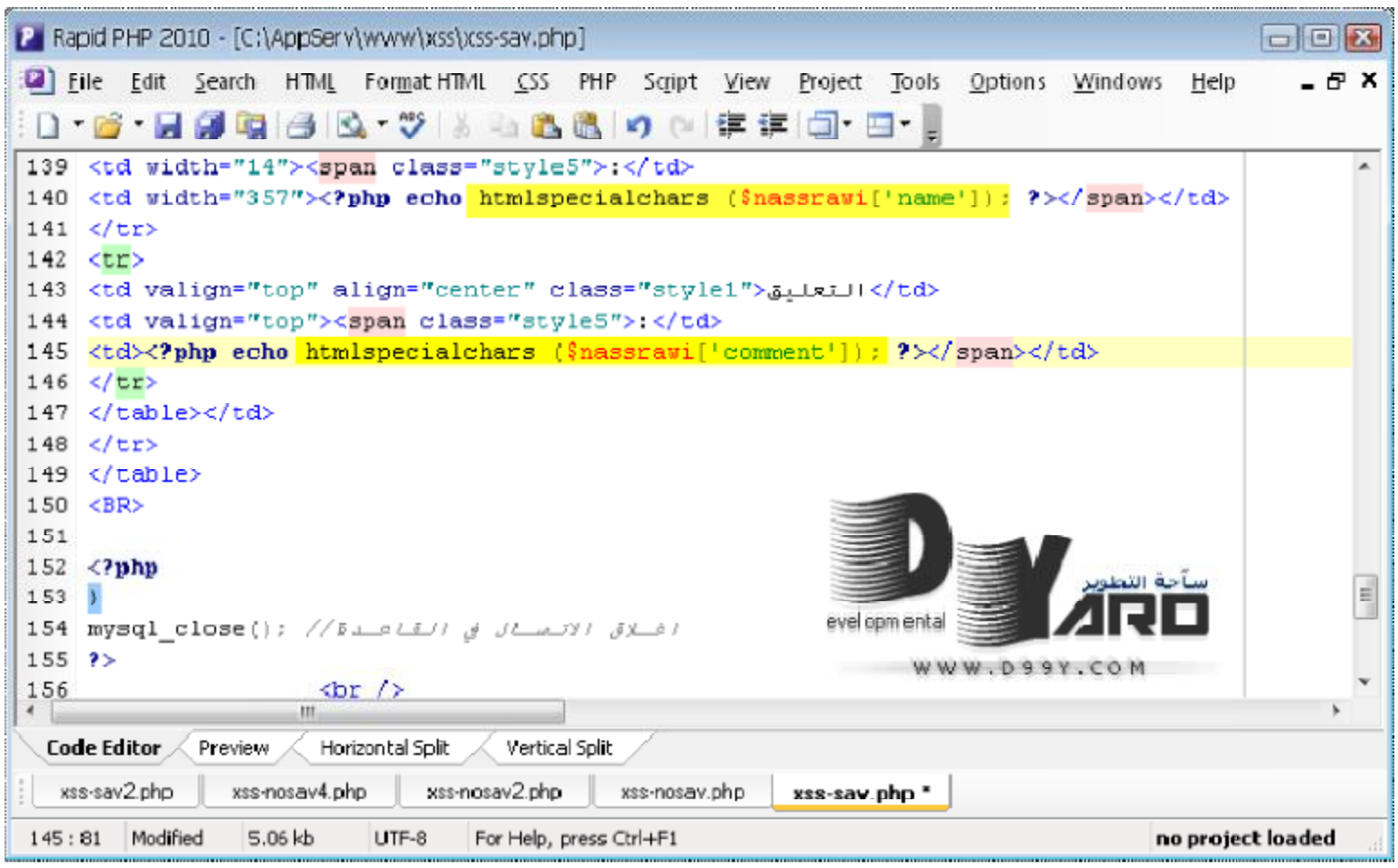
نقوم بادخال حرف عربي كمثال . .

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

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

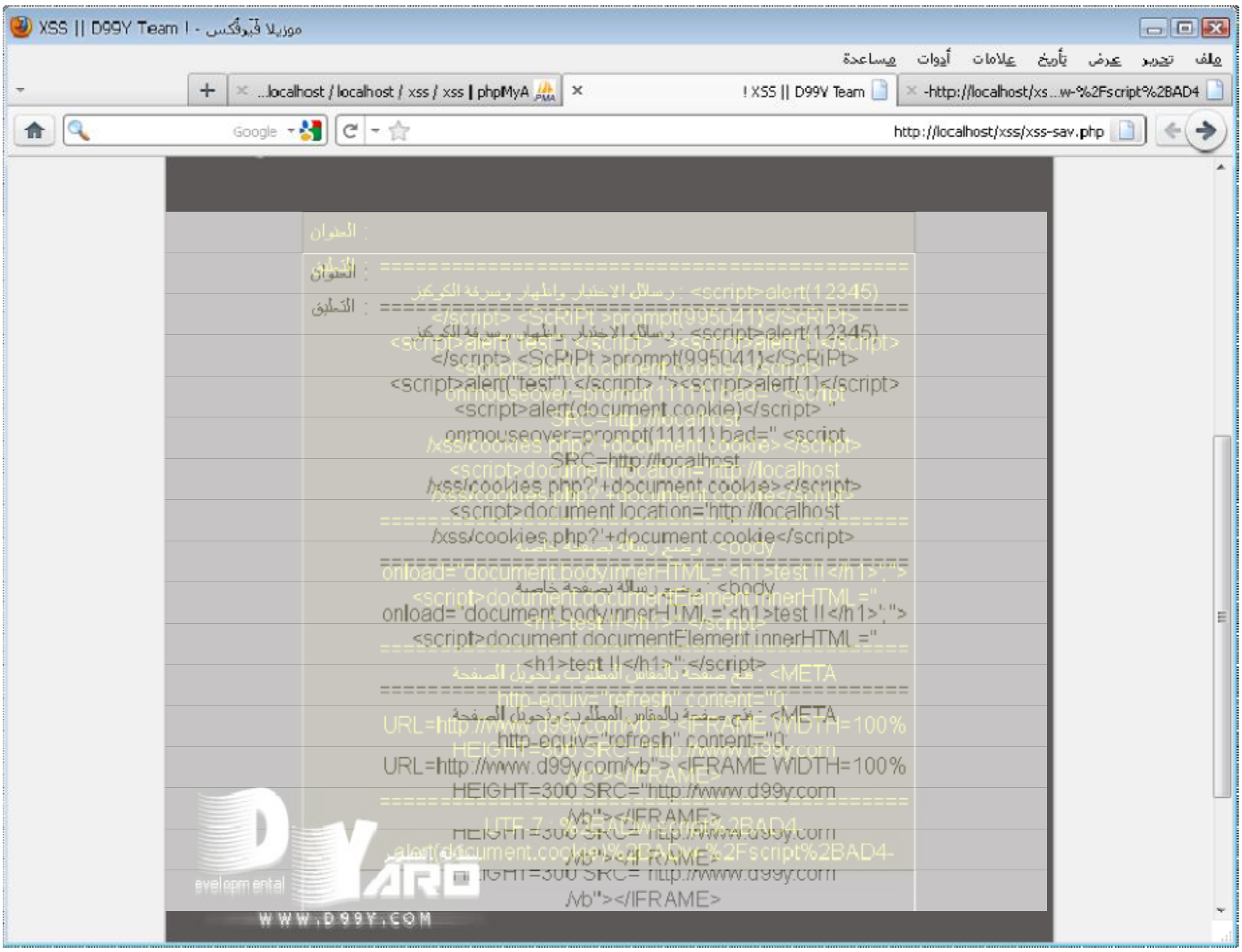
وكما تشاهد تم الطباعه دون التنّفيذ , وهذا يعني انه ترقيع جميل ولكن كما ذكرت ان مشاكل اللغه العربيه وعدد الاحرف لا تنتهي . .

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

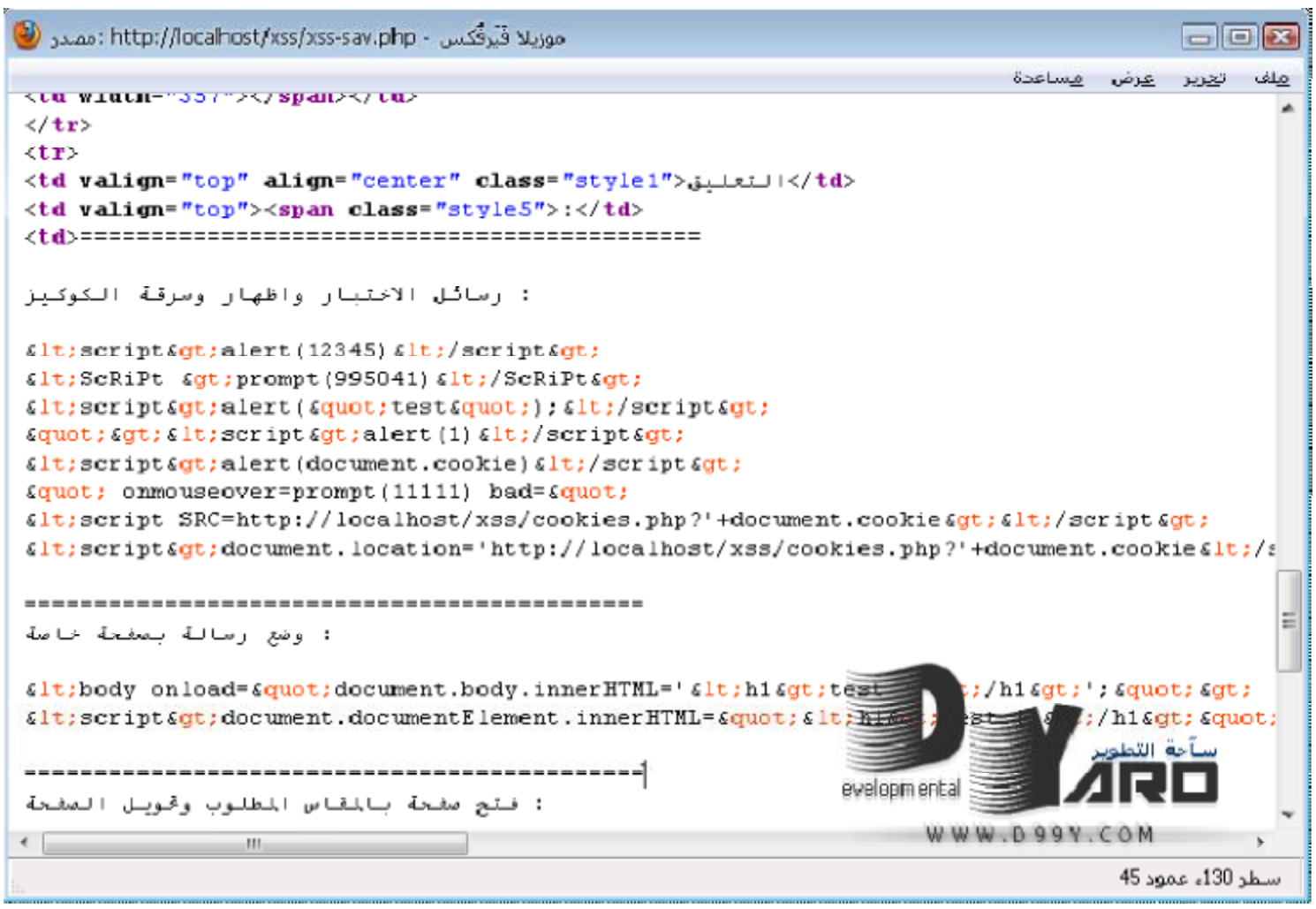


نقوم باستخدام الدالة كما تعلمنا سابقاً ، ونحفظ الملف . .

انسخ المستند بأكمله والصقه ..



وكما تشاهد تم الطباعه دون الحذف والتنفيذ . .



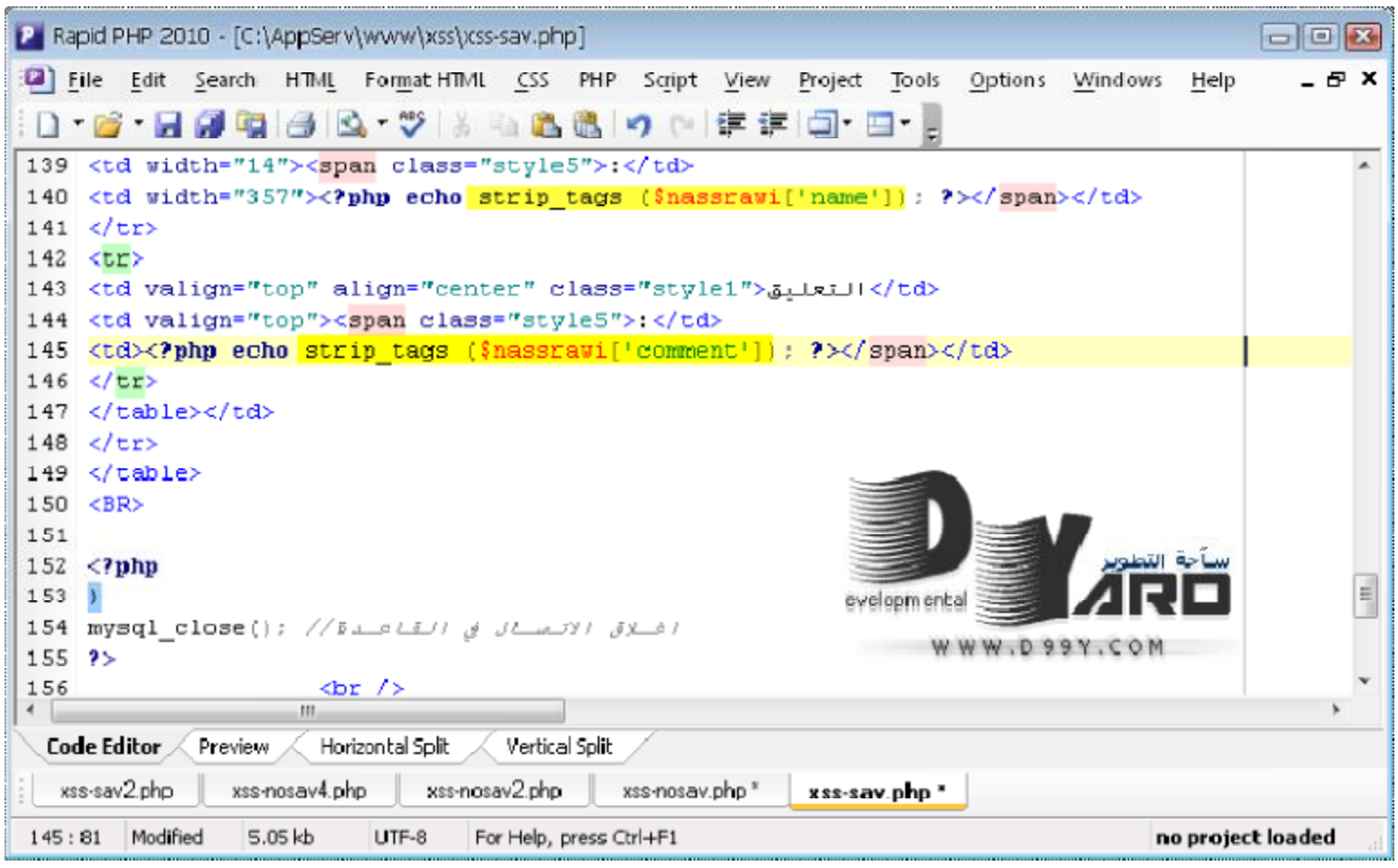
طبعاً بعد عرض المصدر وكما تشاهد تم تحويل الوسوم الضرورية الى ASCII وبذلك عرض دون تنفيذ ، طبعاً الـ / بسبب ان الـ Magic Quotes مُفعّل وان شاء الله مستقبلاً سنتعلّم فوائده

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 نصراوي انا احتاج الى بعض الوسوم الخاصة في الـ HTML في صندوق الرد مثل <b> 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 السابقه بكل تأكيد وهي تقوم" بالحذف " للاكواد الخطيرة وعمل تحويل لبعض الوسوم ، هي جيّده فعلاً ويستخدمها الكثير ولكن" الحذف "غير مقنع للبعض , على العموم سنقوم باستخدام الدالة بالشكل الافتراضي



كما تعلّمنا سابقاً .

قم بتجربة الاستغلالات. .

وكما تشاهد تم الحذف والتعديل والتعطيل والخ . .

جيّد الان نعود الى محور حديثنا كيفية السماح الى بعض الوسوم المفيده مثل! <b>

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

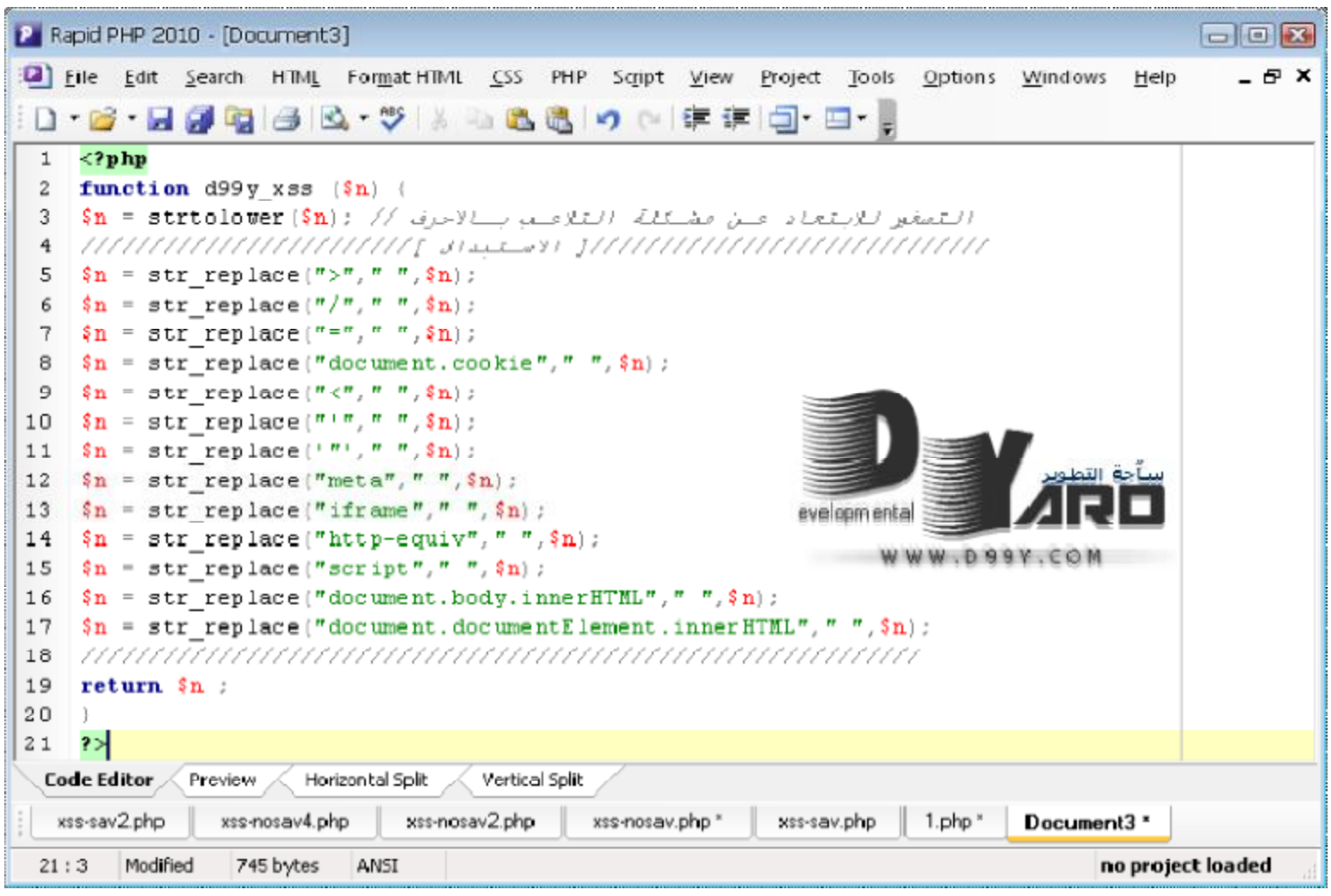
```
136 <table width="400" border="0" cellpadding="3" cellspacing="1" bgcolor="#5C5858">
137 <tr>
138 <td width="117" align="center" class="style1">العنوان</td>
139 <td width="14"><span class="style5">:</td>
140 <td width="357"><?php echo strip_tags ($nassrawi['name'],"<b>"); ?></span></td>
141 </tr>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

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

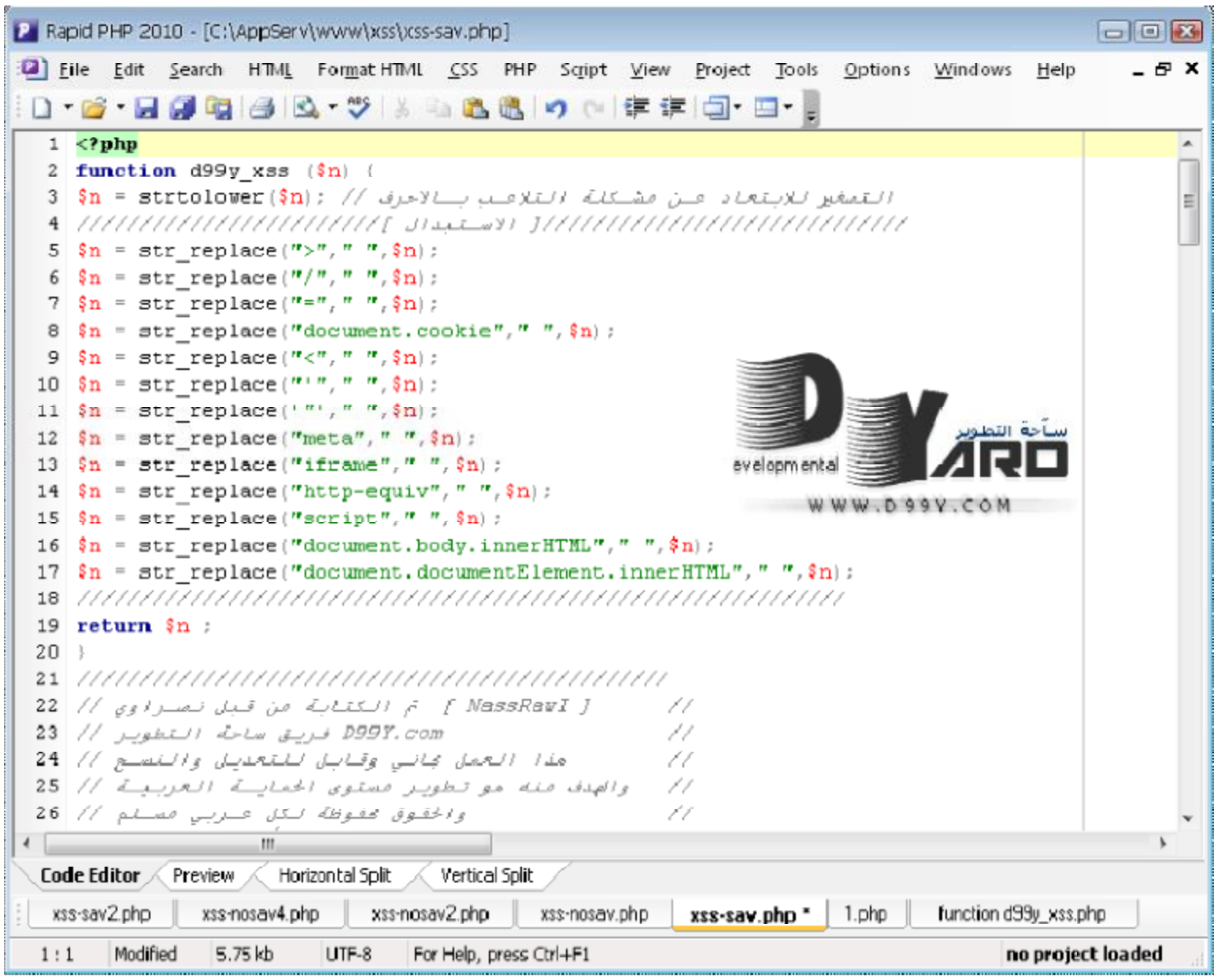
وبعد الاستخدام كما تشاهد النص اصبح عريض , وهذا يعني ان الدالة سامحه للوسم المختار سابقاً وبامكانك اختيار جميع الوسوم الغير ضارة والمفيده مثل <b>
 <h1> والخ . .

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

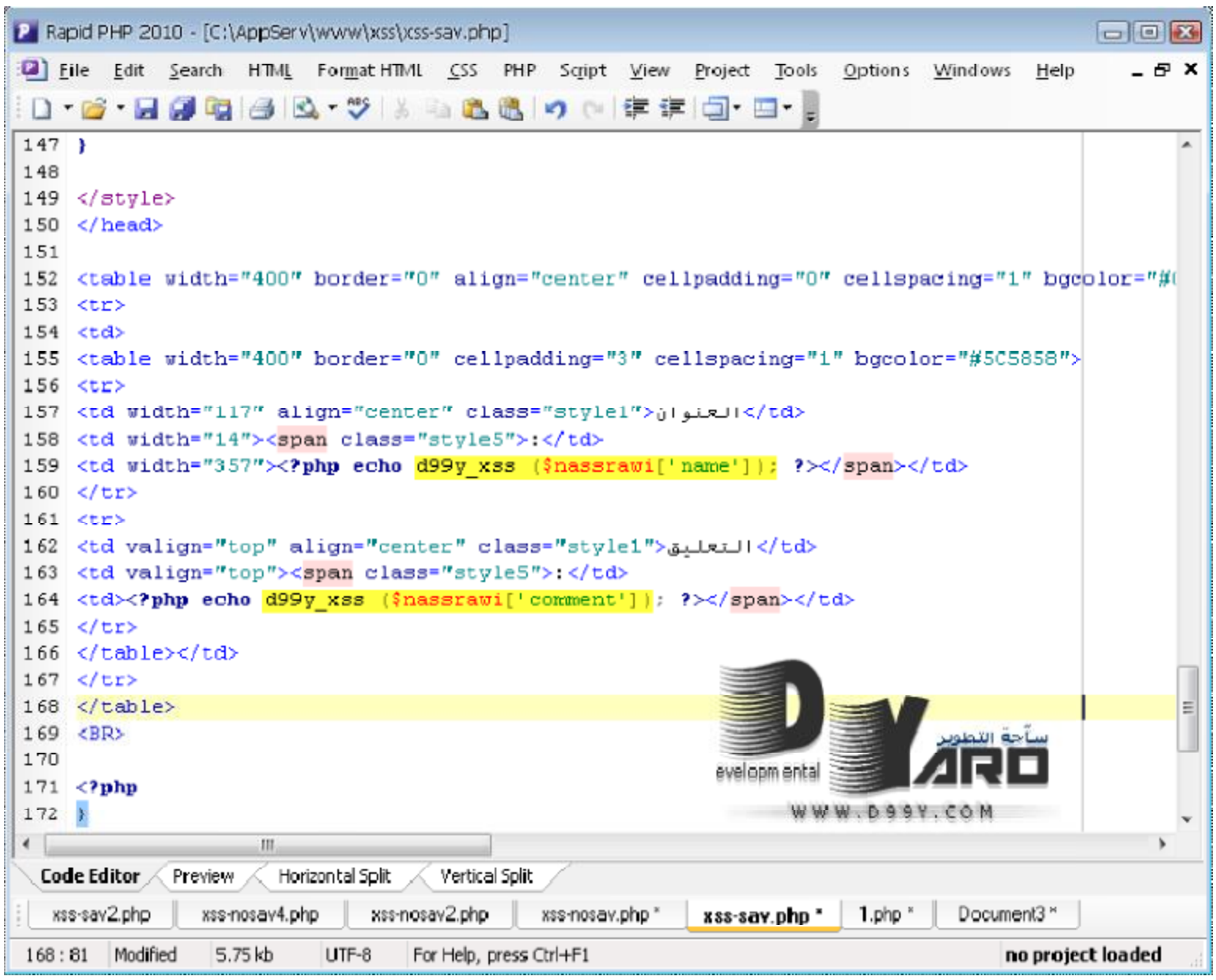


وكما تشاهد عملت function جديد باسم d99y_xss واستخدمت دوال النصوص المعروفة وهي strtolower لتحويل الحروف من كبتل الى سمول ، للابتعاد عن مشكلة التلاعب في الاحرف ، واستخدمت دالة الاستبدال str_replace وقمت باستبدال جميع الوسوم التي نحتاجها في عملية الاستغلال ، الى مسافه ، وبذلك الان عملنا وظيفة جديده تقوم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

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



وهنا نقوم بالتجربة ضع الـ function طبعاً داخل وسوم php وبعد ذلك نستخدمها . .



كما تعلمنا سابقاً نضع اسم الـ function ونقوم بالتجربة!

وضعت المستند بأكمله وقمت بالضغط على ارسل . .

وكما 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 الـ 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]

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

```
55           <br />
56          <br />
57          <br />
58          <form method=GET>
59   <textarea name=xss style="width: 436px; height: 102px"></textarea>
60
61  <br> <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
73          </strong></center></td>
74
75      </tr>
76  </table>
77  <p class="style3"><span lang="ar-sa"><img src="images/fot.png"></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 *

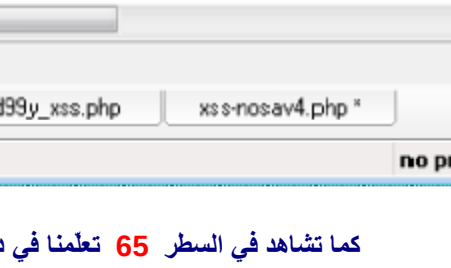
65 : 81 | Modified | 2.01 kb | UTF-8 | For Help, press Ctrl+F1 | no project loaded

كما تشاهد في السطر 65 تعلّمنا 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           <br />
56          <br />
57          <br />
58          <form method=GET>
59   <textarea name=xss style="width: 436px; height: 102px"></textarea>
60
61  <br> <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
73          </strong></center></td>
74
75      </tr>
76  </table>
77  <p class="style3"><span lang="ar-sa"><img src="images/fot.png"></span>
78
79  <body bgcolor=#f1f1f1 text=white>
80
```



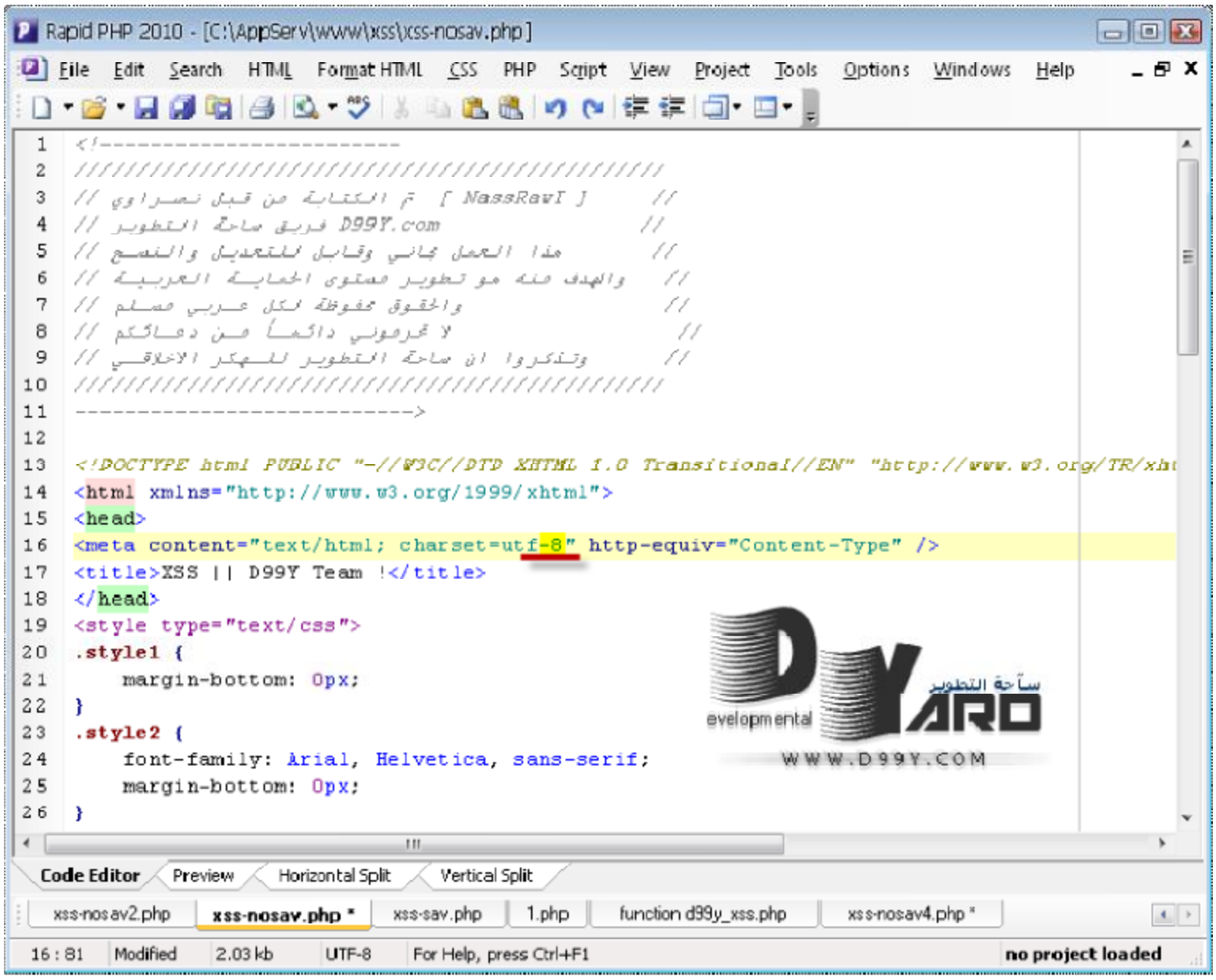
Code Editor | Preview | Horizontal Split | Vertical Split

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

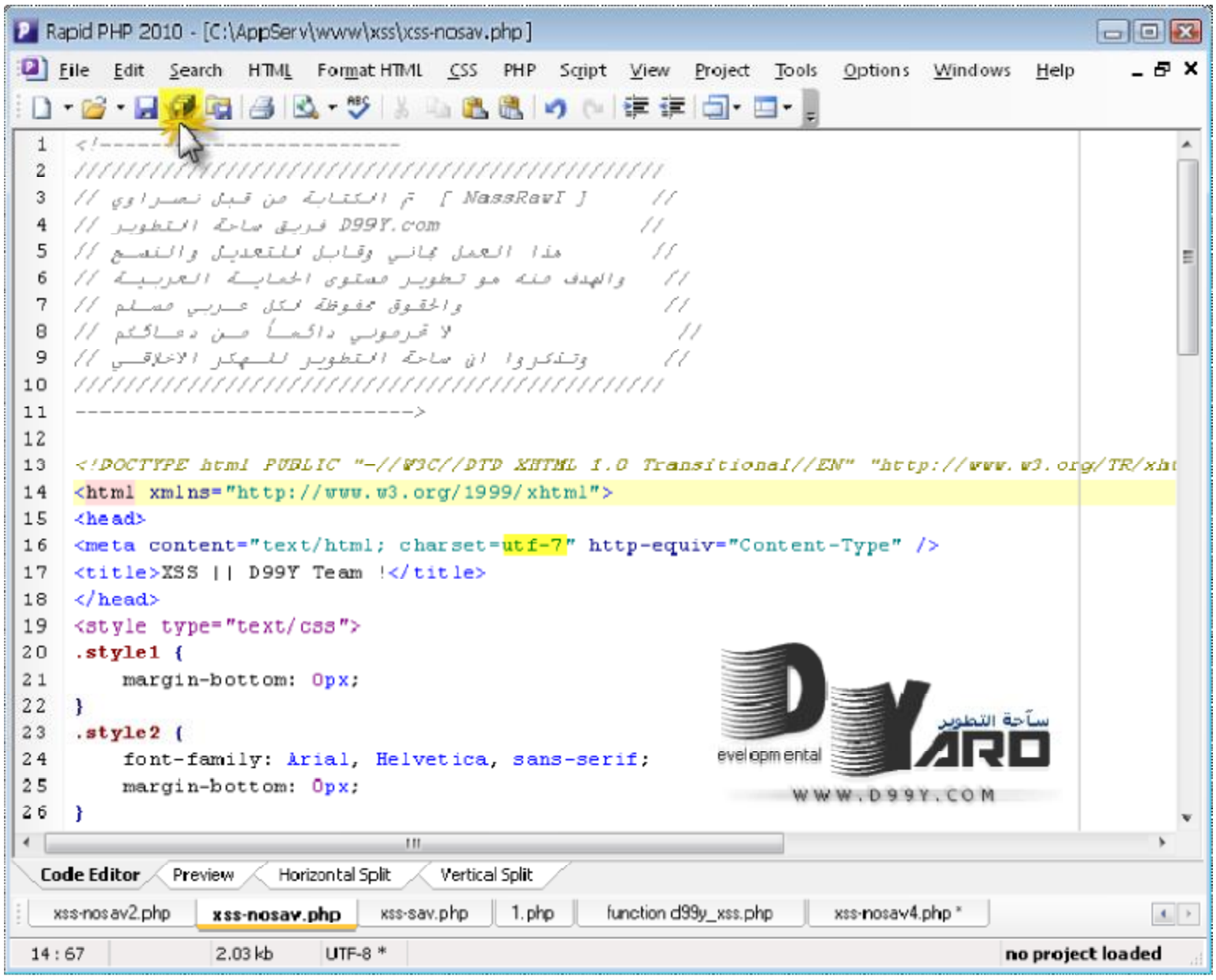
65 : 81 | Modified | 2.03 kb | UTF-8 | For Help, press Ctrl+F1 | no project loaded

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

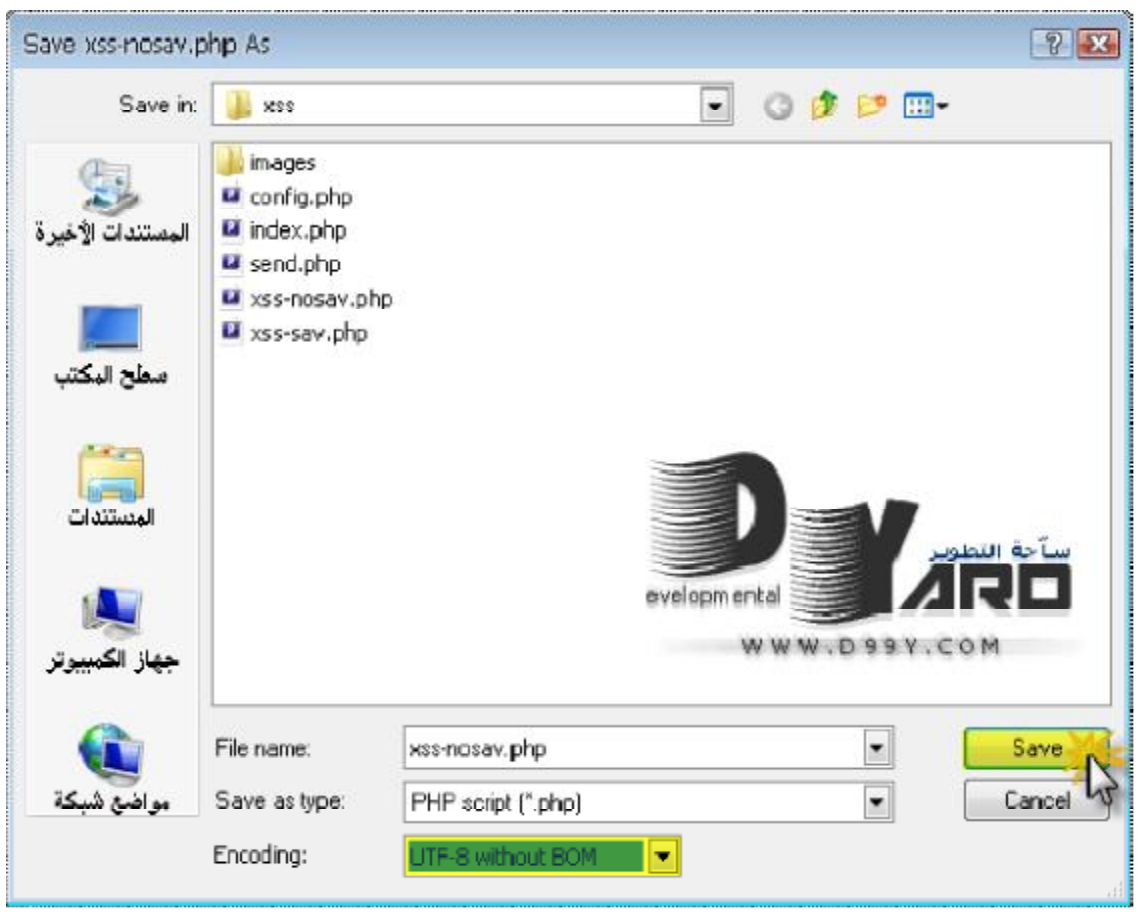
واخيراً تم ترقيع XSS بنجاح ، وبطرق واساليب كثيره ولك الحرية الكامله في الاختيار ، ولكن هناك مشكلة صغيرة في ترميز UTF-7 طبعاً الترميز لا اعتقد ان هناك مخلوق في عام 2011يستخدمه , ولكن حرصاً على ايصال فكرة الحماية بشكل جيّد. .



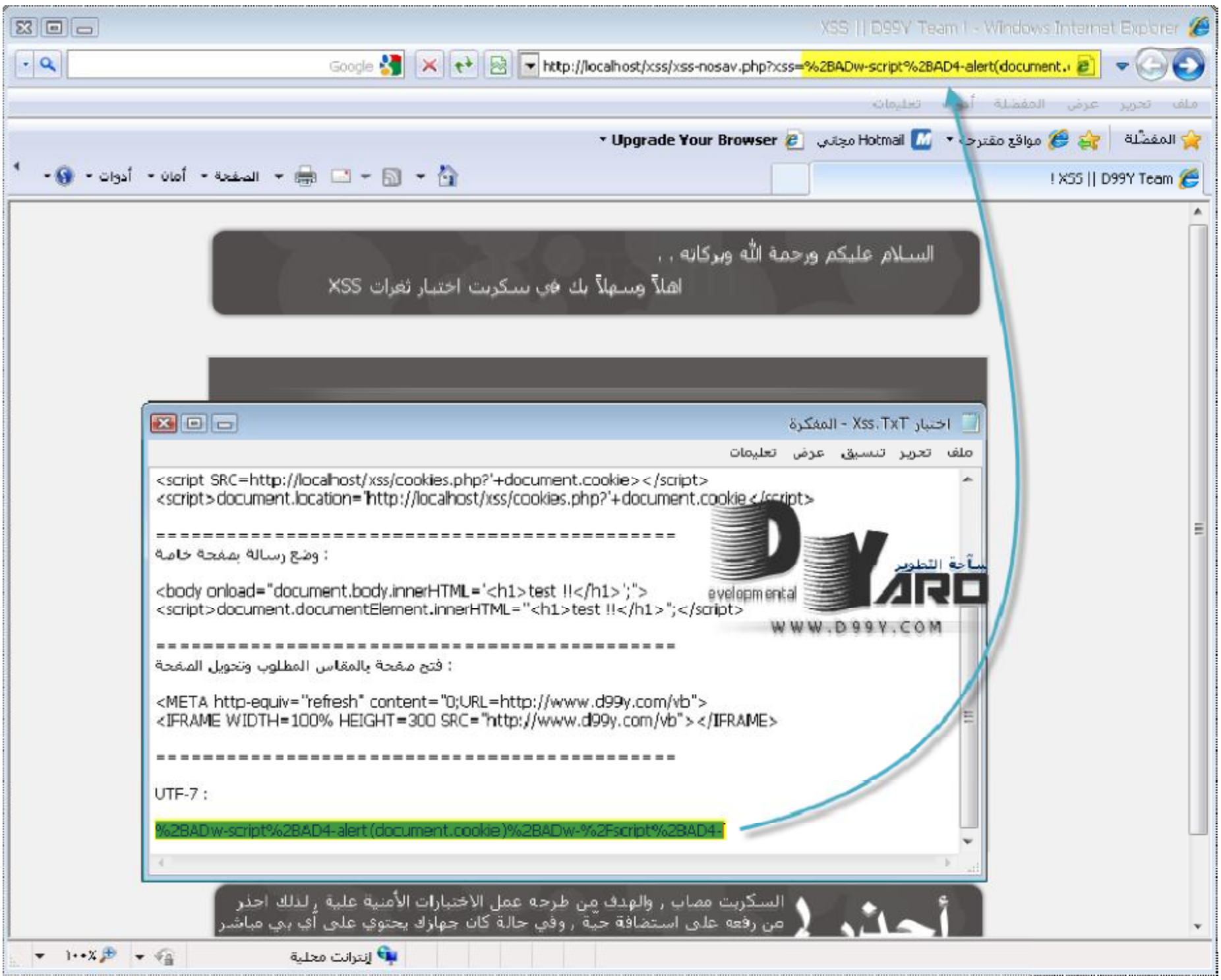
نقوم بالتطبيق على ملف xss-nosav.php كما تشاهد نحول الترميز . .



نحوله الى UTF-7 وندوس على حفظ باسم. .



نحفظه بنوع . . without BOM



طبعاً لابد من استخدام متصفح قديم مثل Internet Explorer 6,7,8 واصدارات الفايرفوكس القديمه , اما الجديده جميعها لا تنفذ الثغرة ، لانه تمّ 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..

www.d99y.com ساحة التطوير

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

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

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

NassRawI

http://www.d99y.com