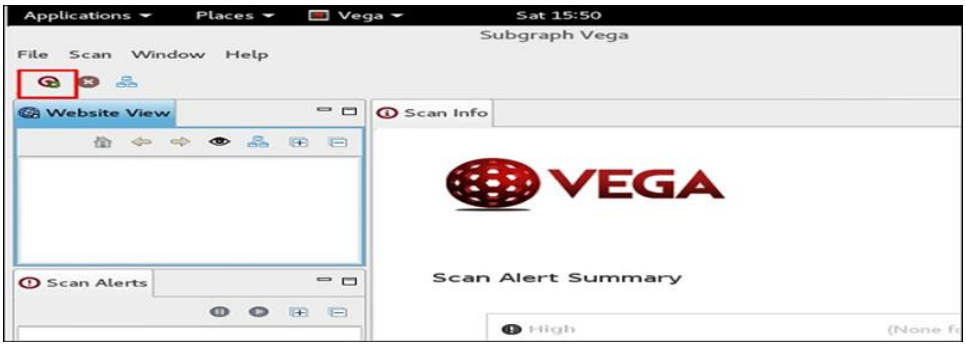
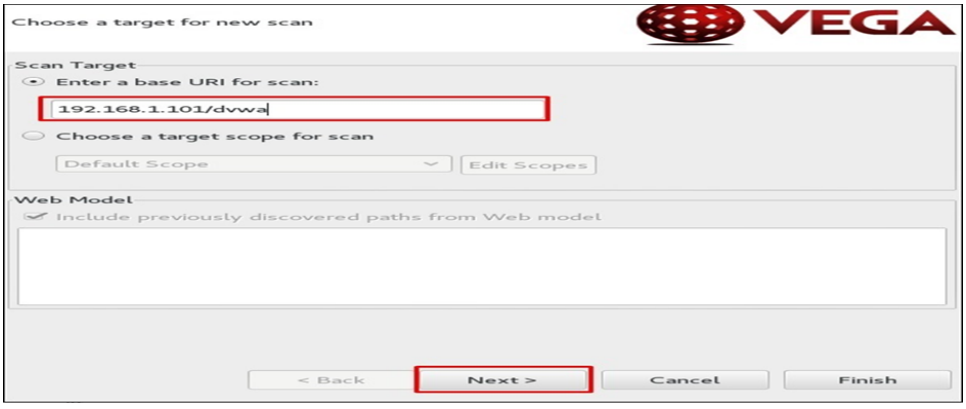
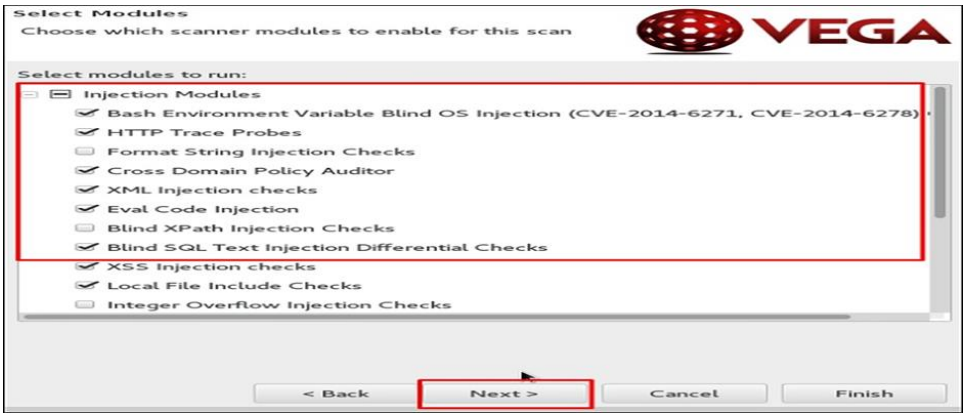
ITA1443-ETHICAL HACKING LAB PROBLEMS

F. ABDUL RAHMAN 192124162

EX-4: VEGA

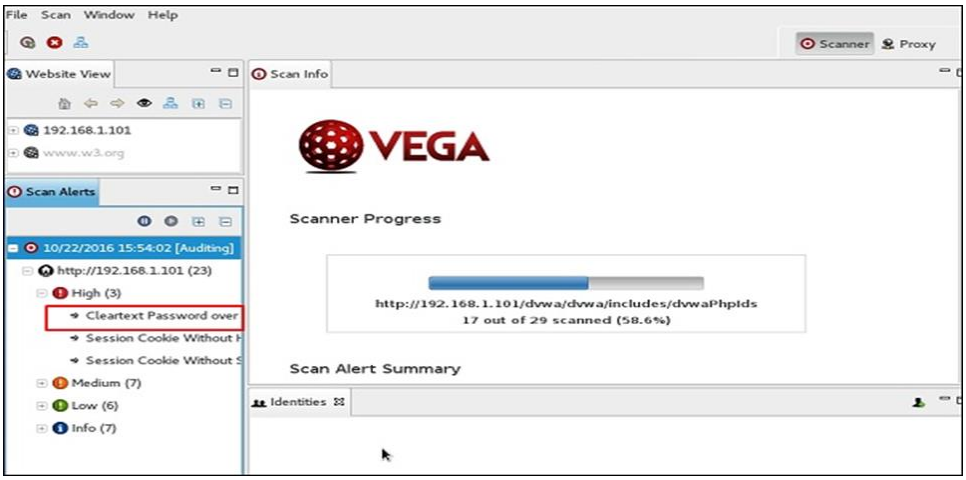





Select Modules
Choose which scanner modules to enable for this scan
VEGA
Select modules to run:
Injection Modules
Bash Environment Variable Blind OS Injection (CVE-2014-6271, CVE-2014-6278)
HTTP Trace Probes
Format String Injection Checks
Cross Domain Policy Auditor
XML Injection checks
Eval Code Injection
Blind XPath Injection Checks
Blind SQL Text Injection Differential Checks
XSS Injection checks
Local File Include Checks
Integer Overflow Injection Checks
< Back
Next >
Cancel
Finish

Authentication Options
Configure cookies and authentication identity to use during scan
VEGA
Identity to scan site as:
Set-Cookie or Set-Cookie2 value:
Add cookie
Remove selected cookie(s)
< Back
Next >
Cancel
Finish

Follow Redirect?
Target address http://192.168.1.101/dvwa redirects to address http://192.168.1.101/dvwa/login.php
Would you like to add http://192.168.1.101/dvwa/login.php to the scope?
No
Yes


File Scan Window Help
Scanner
Proxy
Website View
192.168.1.101
www.w3.org
Scan Alerts
10/22/2016 15:54:02 [Auditing]
http://192.168.1.101 (23)
High (3)
Cleartext Password over
Session Cookie Without
Session Cookie Without
Medium (7)
Low (6)
Info (7)
Scan Info
VEGA
Scanner Progress
http://192.168.1.101/dvwa/dvwa/includes/dvwaPhpIds
17 out of 29 scanned (58.6%)
Scan Alert Summary
Identities

Website View
192.168.1.101
www.w3.org
Scan Alerts
10/22/2016 15:54:02 [Complet
http://192.168.1.101 (23)
High (3)
Cleartext Password ove
Session Cookie Without
Session Cookie Without
Medium (7)
Low (6)
Info (7)
Scan Info
AT A GLANCE
Classification
Environment
Resource
/dvwa/login.php
Risk
High
REQUEST
GET /dvwa/login.php
DISCUSSION
Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in unauthorized disclosure of passwords to passive network attackers.
IMPACT
Vega has detected a form that can cause a password submission over an insecure channel.
This could result in disclosure of passwords to network eavesdroppers.
REMEDIATION
Passwords should never be sent over cleartext. The form should submit to an HTTPS target.