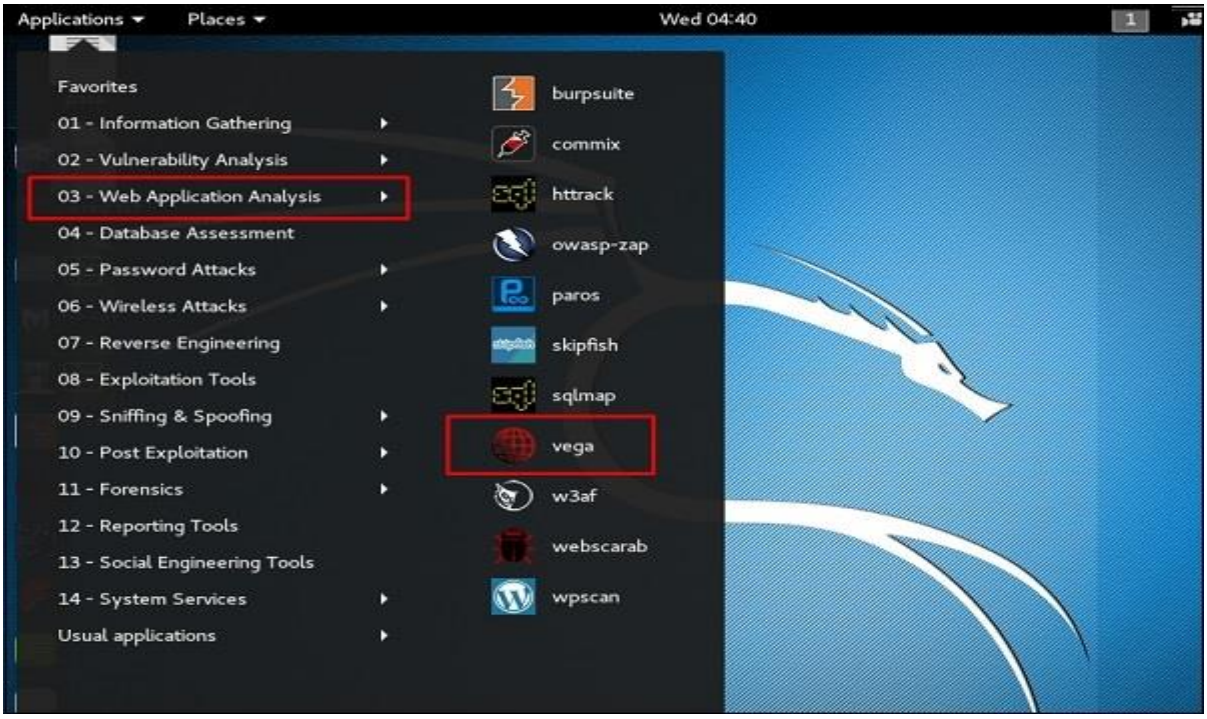
ITA1443-Ethical Hacking For Legal Systems

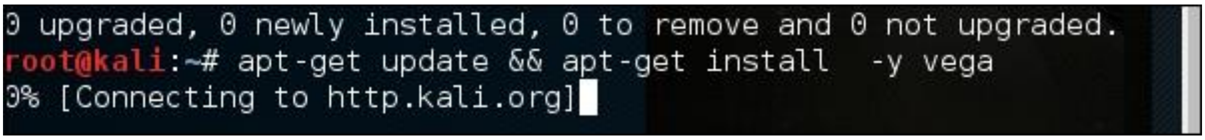
Name:R.Surya

Reg.No:192011244

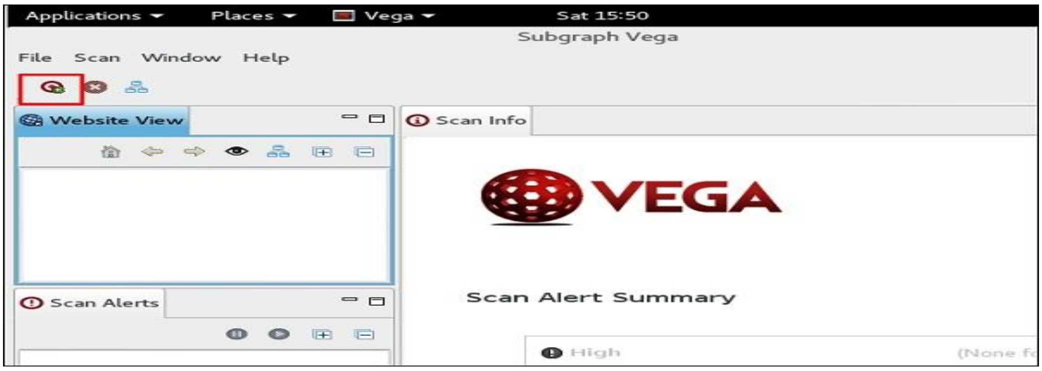
Slot:D

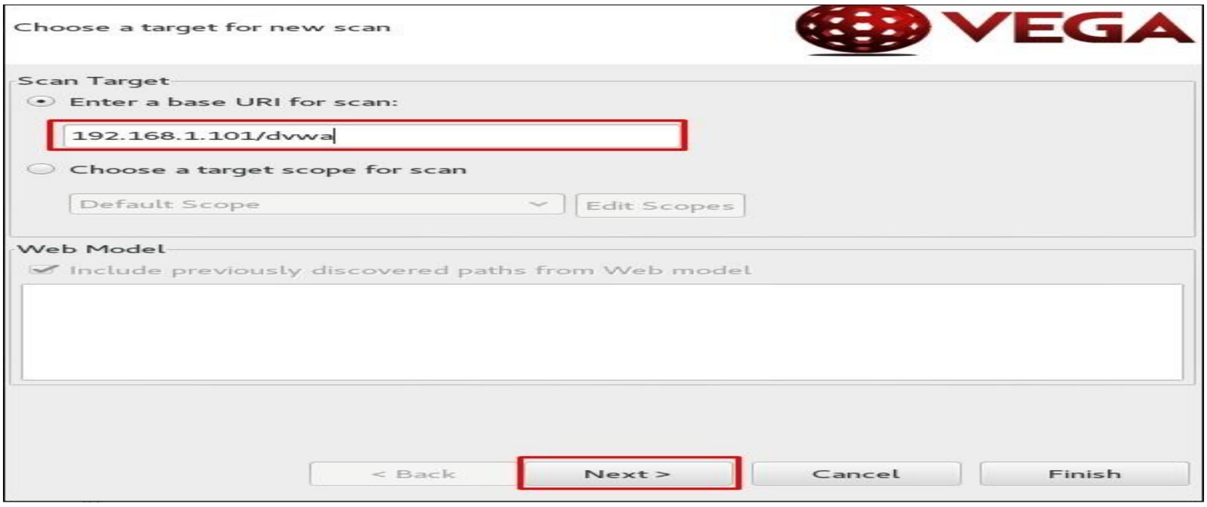
Exercise No 4: Website Penetration Testing





```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# apt-get update && apt-get install  -y vega
0% [Connecting to http.kali.org]
```





Choose a target for new scan

Scan Target

● Enter a base URI for scan:

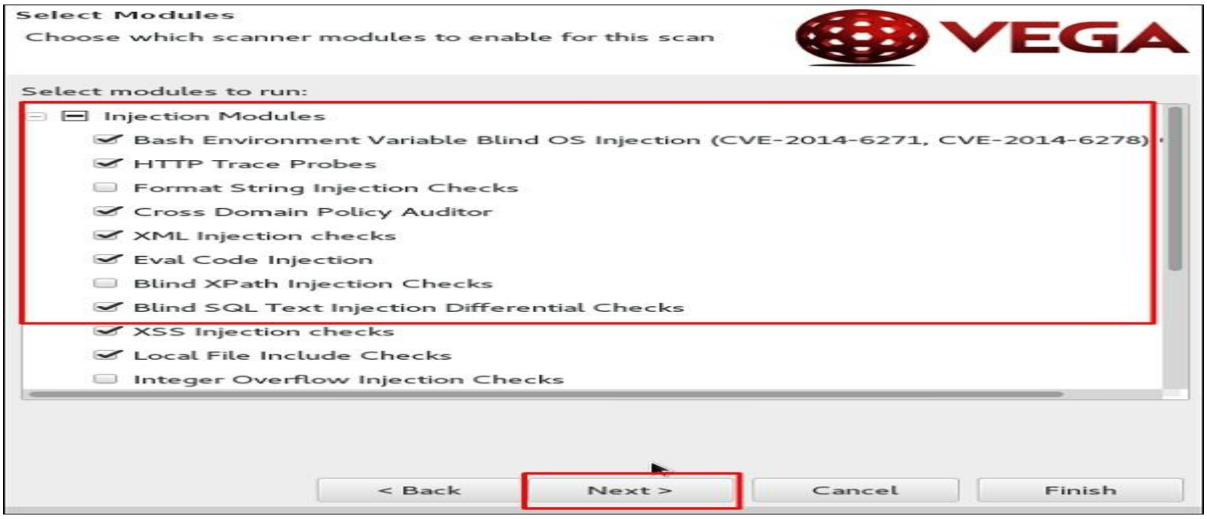
192.168.1.101/dvwa

○ Choose a target scope for scan

Default Scope

Web Model

☑ Include previously discovered paths from Web model

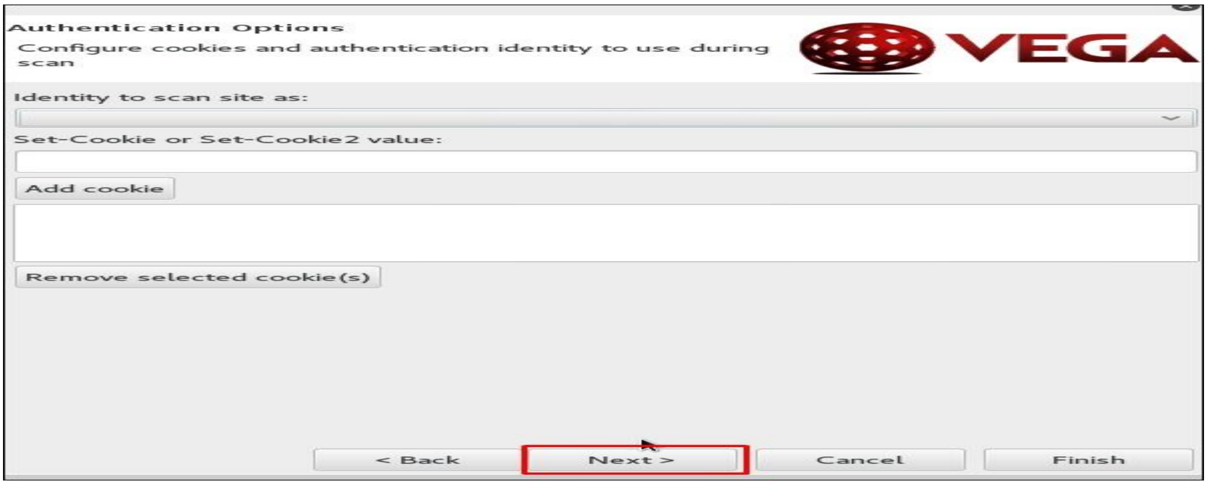


Select Modules

Choose which scanner modules to enable for this scan

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

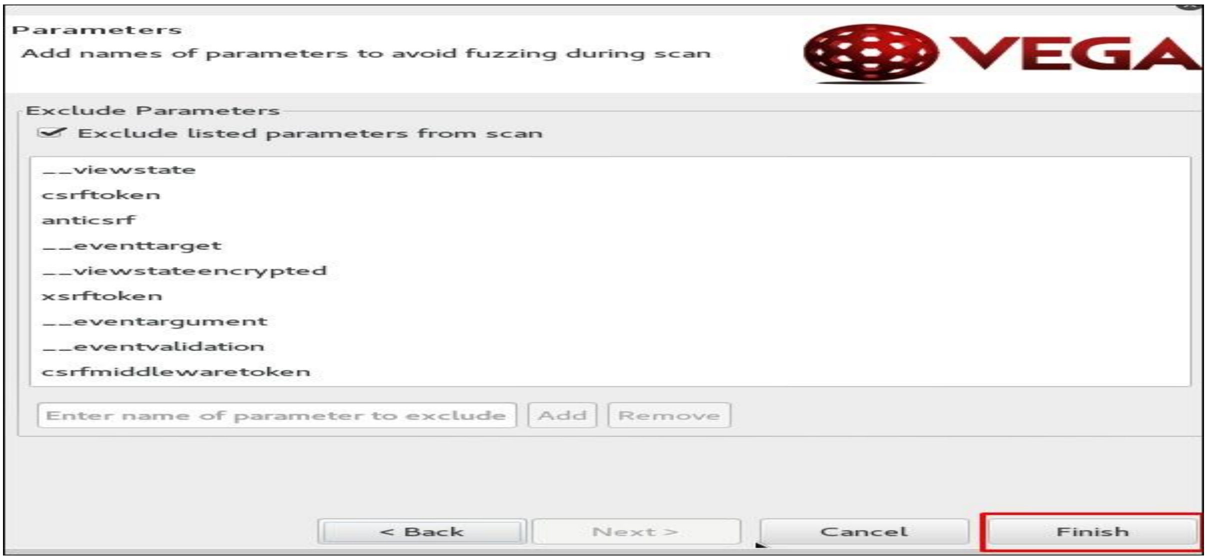


Authentication Options

Configure cookies and authentication identity to use during scan

Identity to scan site as:

Set-Cookie or Set-Cookie2 value:



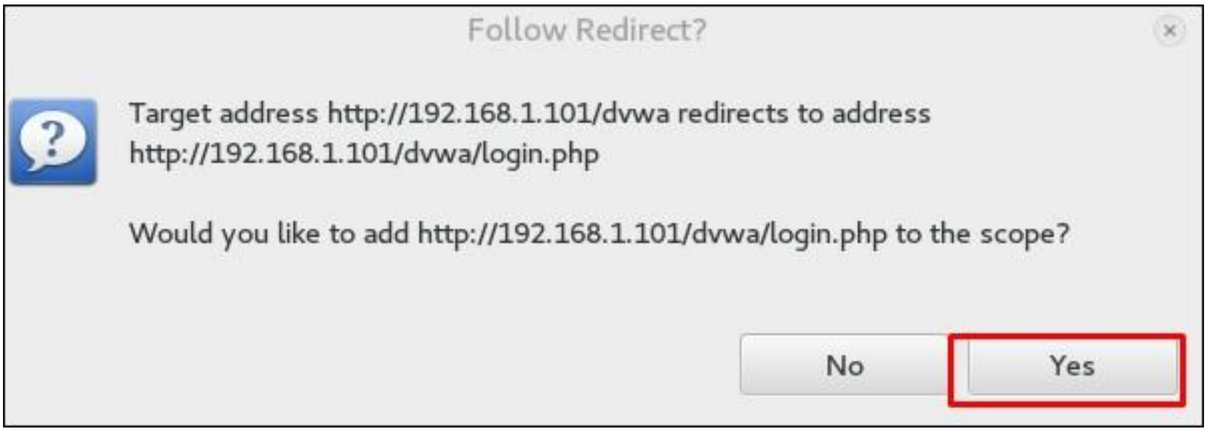
Parameters

Add names of parameters to avoid fuzzing during scan

Exclude Parameters

☑ Exclude listed parameters from scan

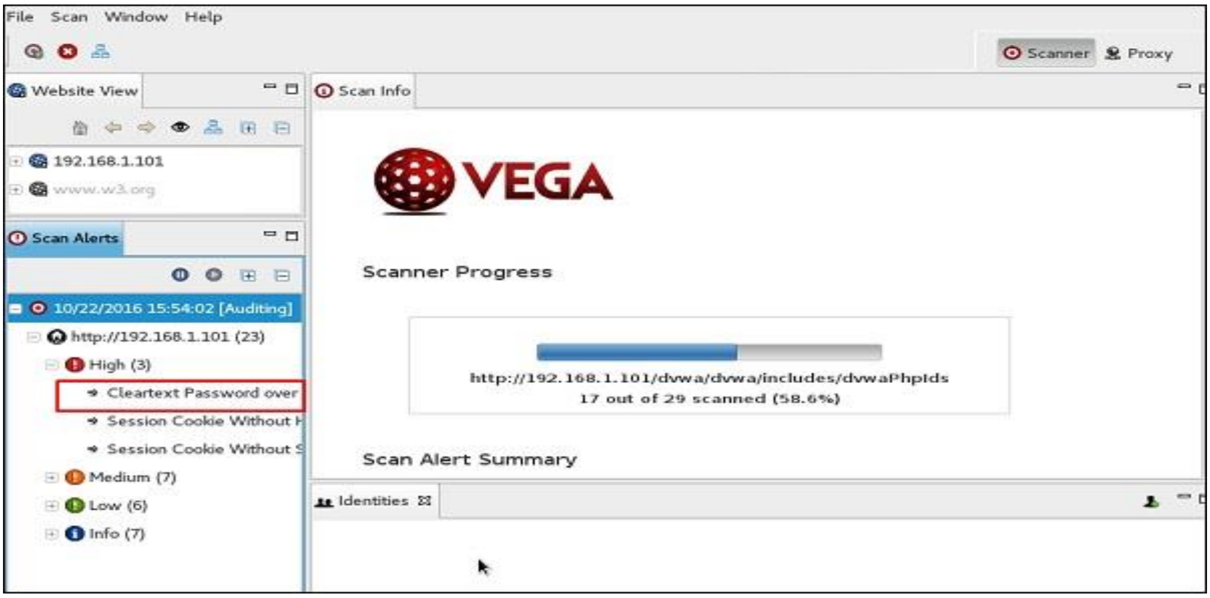
```
__viewstate
csrftoken
anticsrf
__eventtarget
__viewstateencrypted
xsrftoken
__eventargument
__eventvalidation
csrfmiddlewaretoken
```



Follow Redirect?

Target address http://192.168.1.101/dvwa redirects to address http://192.168.1.101/dvwa/login.php

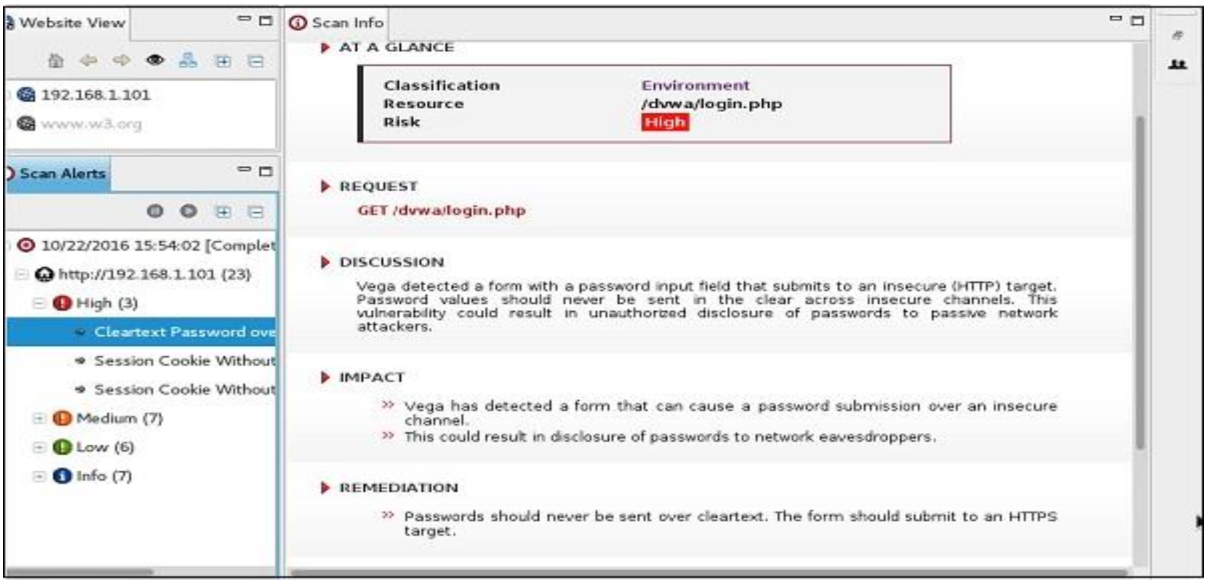
Would you like to add http://192.168.1.101/dvwa/login.php to the scope?



Scanner Progress

http://192.168.1.101/dvwa/dvwa/includes/dvwaPhpIds
17 out of 29 scanned (58.6%)

Scan Alert Summary



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.