



School of Information Technology and Engineering

Lab Final Assessment Test, JUNE 2021

B.Tech., Winter-2020-2021

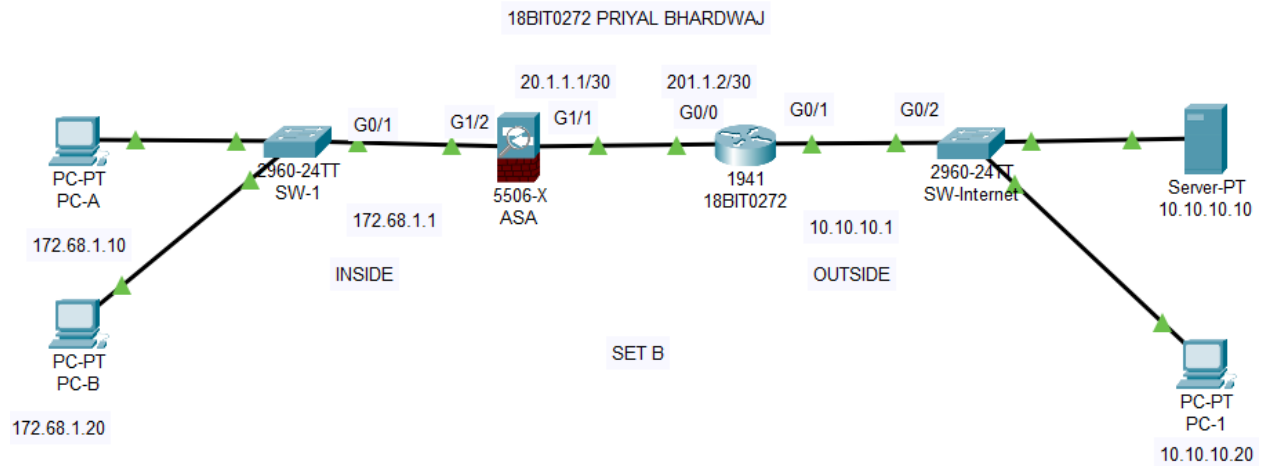
NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3502
COURSE NAME	INFORMATION SECURITY MANAGEMENT
SLOT	L39+L40
FACULTY	Prof. I SUMAIYA THASEEN

Google Drive Link:

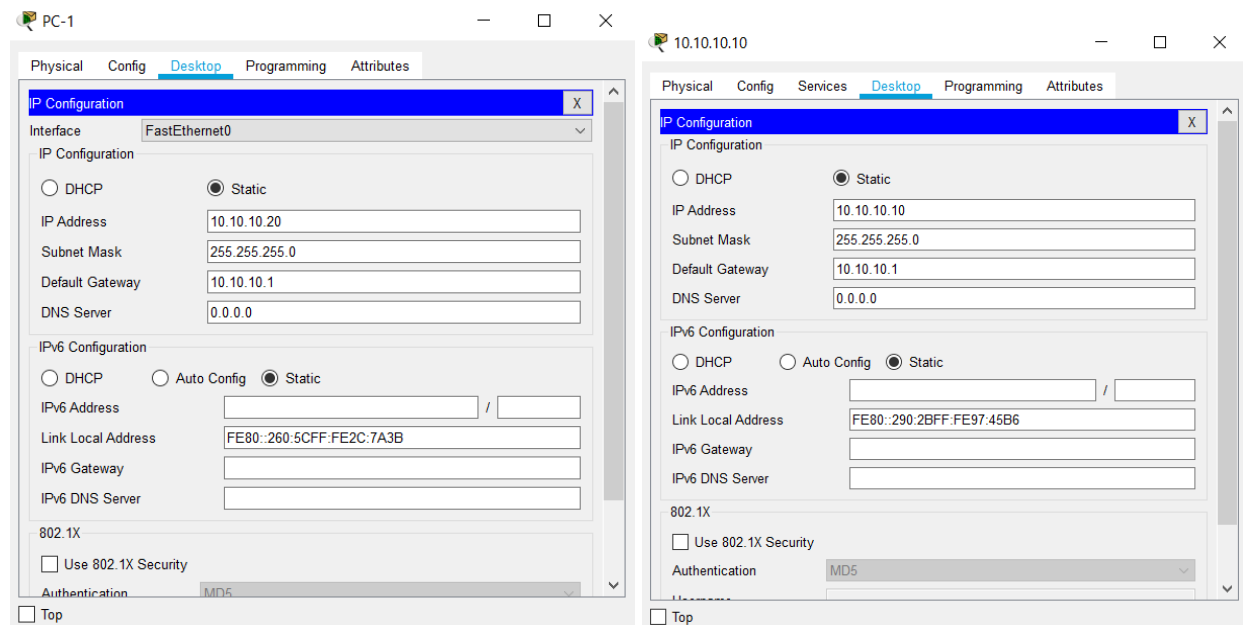
<https://drive.google.com/drive/folders/18j1KD0x2nBwBYt9oaLvWFvgo-RSNKcxH?usp=sharing>

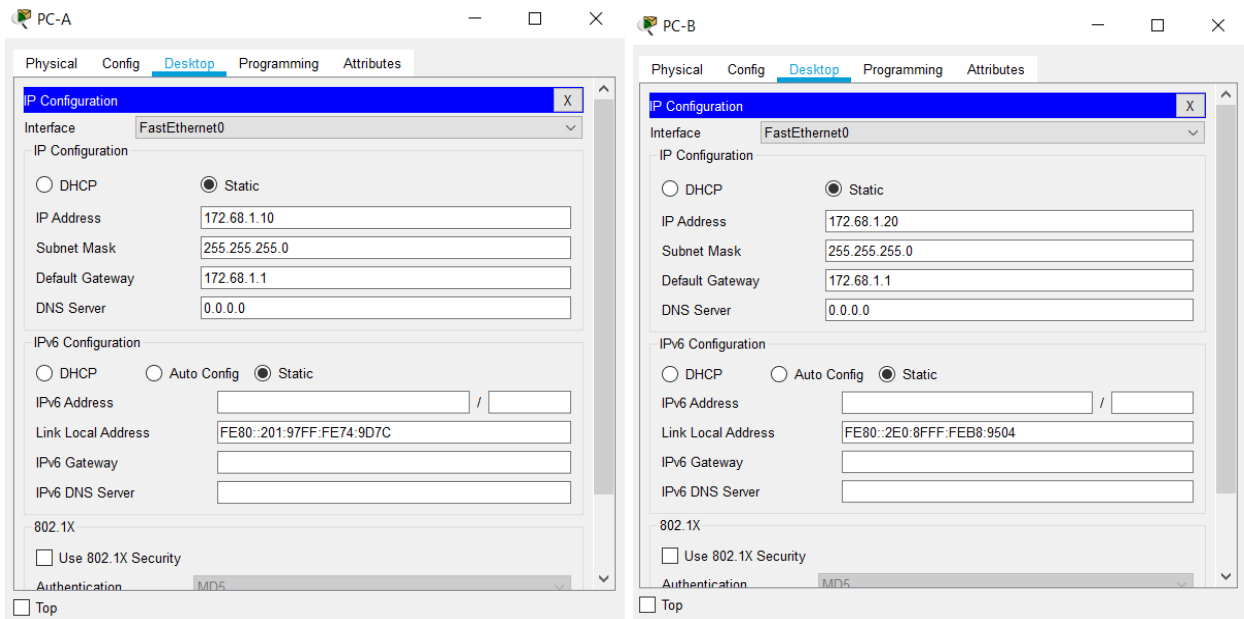
Q.1 NOTE: I have changed the IPs of DNS server as well.

i)

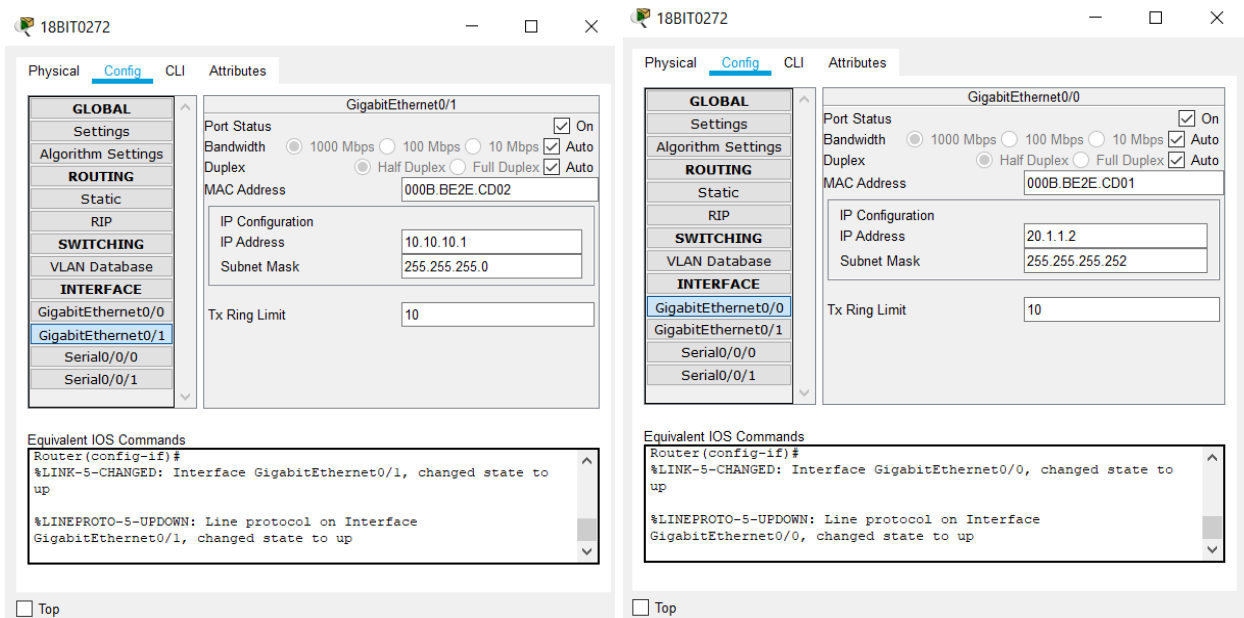


ii)

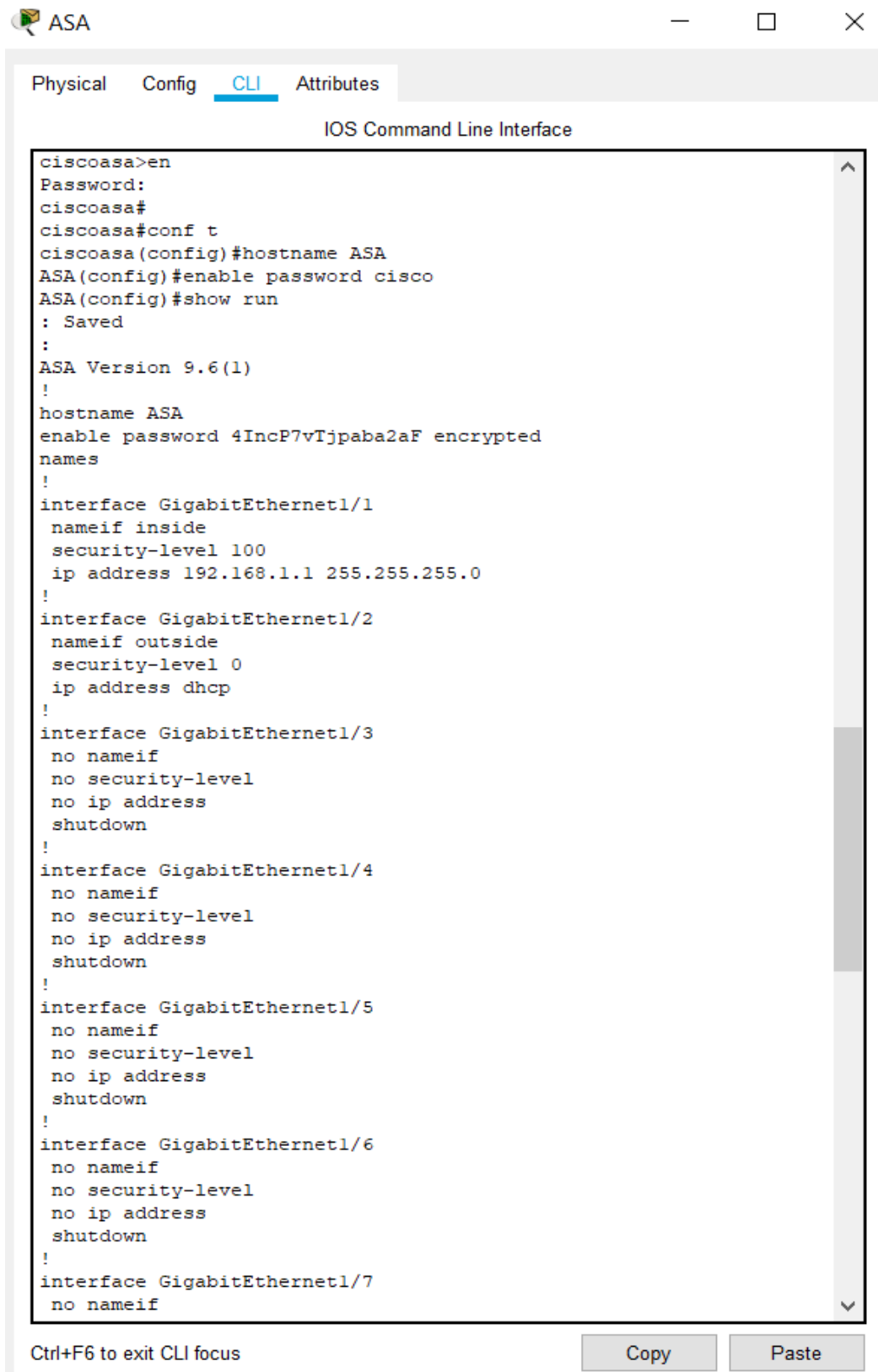




iii)



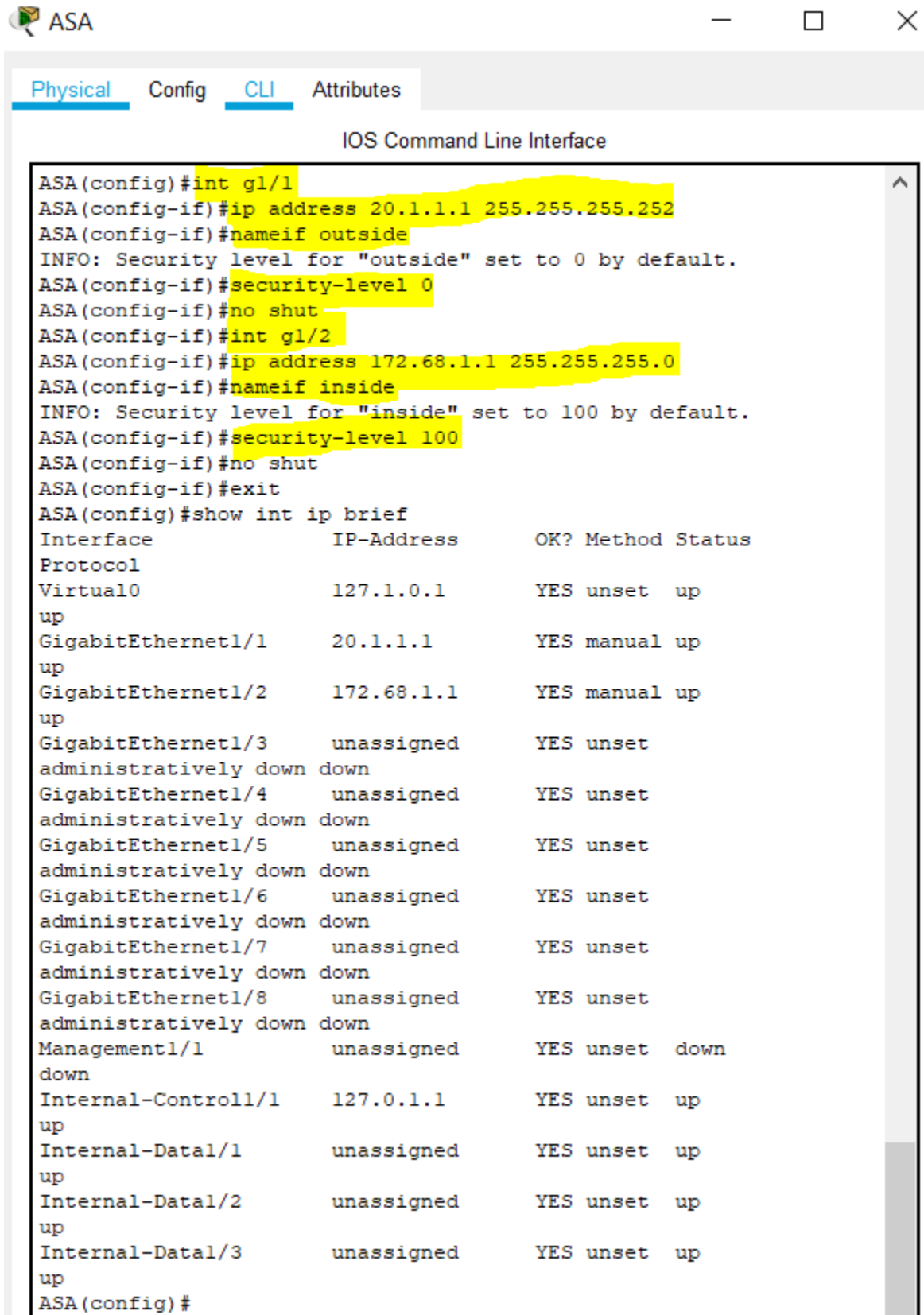
iv)



IOS Command Line Interface

```
ASA(config)#int g1/1
ASA(config-if)#no ip address
ASA(config-if)#no nameif
ASA(config-if)#no security-level
ASA(config-if)#int g1/2
ASA(config-if)#no nameif
ASA(config-if)#no security-level
ASA(config-if)#no ip address dhcp
ASA(config-if)#exit
ASA(config)#show run
: Saved
:
ASA Version 9.6(1)
!
hostname ASA
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface GigabitEthernet1/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/3
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no nameif
 no security-level
 no ip address
<--- More --->
```

a) Configured security levels 0 and 100 for outside and inside respectively on ASA



The screenshot shows the ASA CLI interface with the following commands and output:

```
ASA(config)#int g1/1
ASA(config-if)#ip address 20.1.1.1 255.255.255.252
ASA(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA(config-if)#security-level 0
ASA(config-if)#no shut
ASA(config-if)#int g1/2
ASA(config-if)#ip address 172.68.1.1 255.255.255.0
ASA(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA(config-if)#security-level 100
ASA(config-if)#no shut
ASA(config-if)#exit
ASA(config)#show int ip brief
```

Interface	IP-Address	OK?	Method	Status
Virtual0	127.1.0.1	YES	unset	up
GigabitEthernet1/1	20.1.1.1	YES	manual	up
GigabitEthernet1/2	172.68.1.1	YES	manual	up
GigabitEthernet1/3	unassigned	YES	unset	administratively down
GigabitEthernet1/4	unassigned	YES	unset	administratively down
GigabitEthernet1/5	unassigned	YES	unset	administratively down
GigabitEthernet1/6	unassigned	YES	unset	administratively down
GigabitEthernet1/7	unassigned	YES	unset	administratively down
GigabitEthernet1/8	unassigned	YES	unset	administratively down
Management1/1	unassigned	YES	unset	down
Internal-Controll1/1	127.0.1.1	YES	unset	up
Internal-Data1/1	unassigned	YES	unset	up
Internal-Data1/2	unassigned	YES	unset	up
Internal-Data1/3	unassigned	YES	unset	up

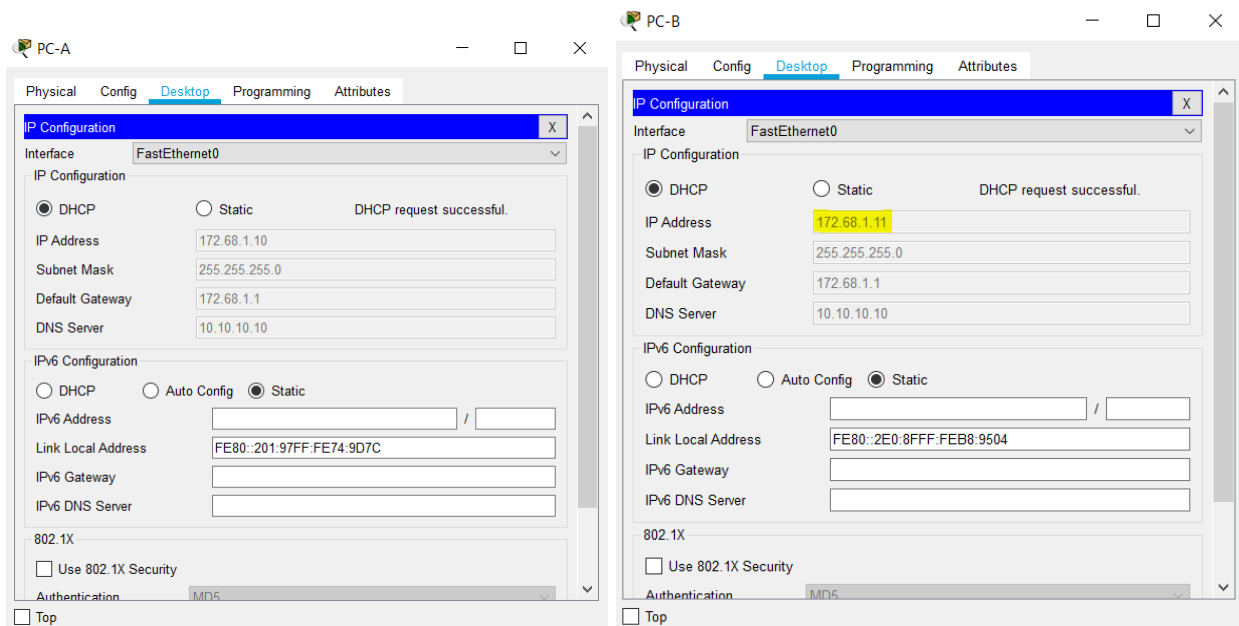
```
ASA(config)#
```

b) DHCP Server configuration

IP address range 172.68.1.10-172.68.1.20

```
ASA(config)#dhcp address 172.68.1.10-172.68.1.20 inside
ASA(config)#dhcp dns 10.10.10.10
ASA(config)#dhcp option 3 ip 172.68.1.1
ASA(config)#dhcp enable inside
```

After DHCP configuration new IPs of PC-A and PC-B

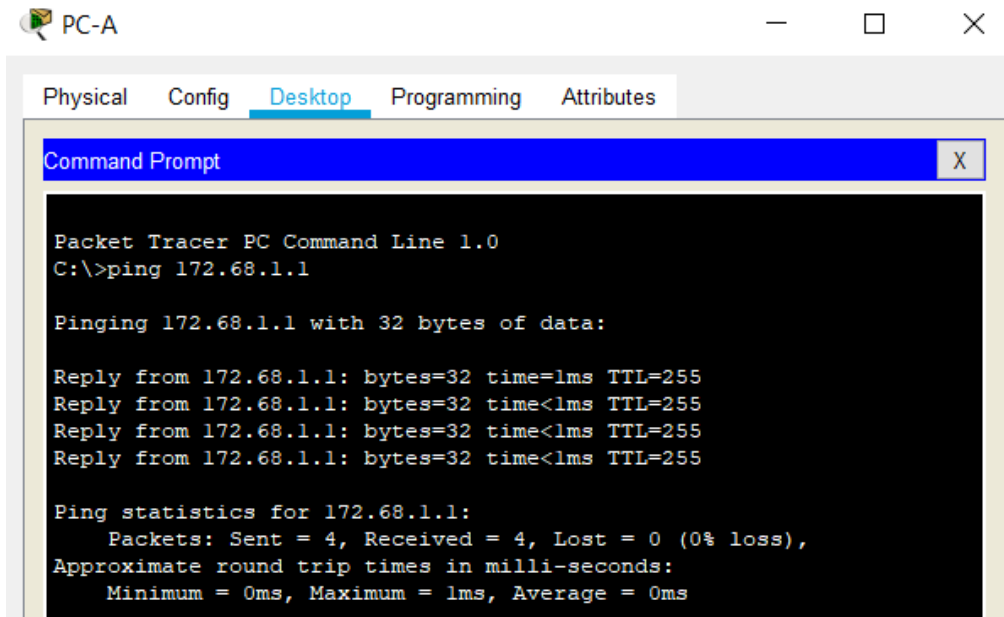


IP address of PC-A was already set as 172.68.1.10 so it is same but IP address of PC-B has changed from 172.68.1.20 to 172.68.1.11

c) NAT object

```
ASA(config)#route outside 0.0.0.0 0.0.0.0 20.1.1.2
ASA(config)#object network INSIDE-NET
ASA(config-network-object)#subnet 172.68.1.0 255.255.255.0
ASA(config-network-object)#nat (inside,outside) dynamic interface
ASA(config-network-object)#exit
```

Ping from PC-A to default gateway i.e. 172.68.1.1 is successful



PC-A

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.68.1.1

Pinging 172.68.1.1 with 32 bytes of data:

Reply from 172.68.1.1: bytes=32 time=1ms TTL=255
Reply from 172.68.1.1: bytes=32 time<1ms TTL=255
Reply from 172.68.1.1: bytes=32 time<1ms TTL=255
Reply from 172.68.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.68.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

v) ASA policy map and inspection policies configuration



ASA

Physical Config **CLI** Attributes

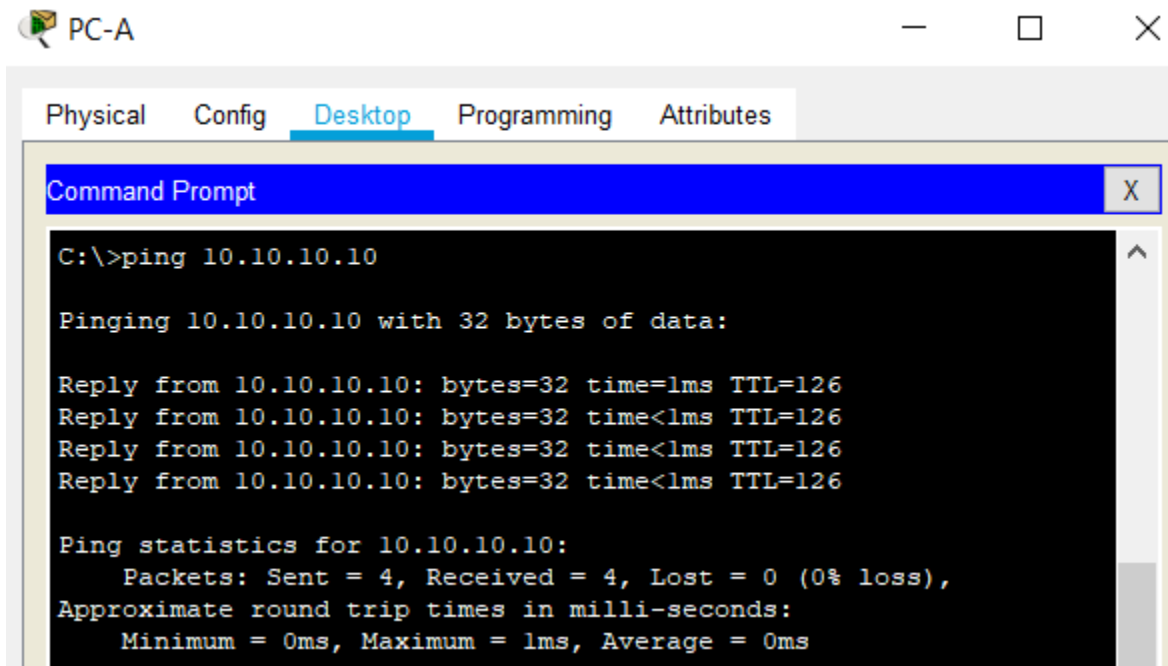
IOS Command Line Interface

```
ASA(config)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#exit
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#exit
ASA(config)#service-policy global_policy global
ASA(config)#show run
: Saved
```

We can see them in show run now

```
!
class-map inspection_default
  match default-inspection-traffic
!
policy-map global_policy
  class inspection_default
    inspect icmp
!
service-policy global_policy global
!
```


Ping from PC-A to dhcp dns server successful:



PC-A

Physical Config Desktop Programming Attributes

Command Prompt

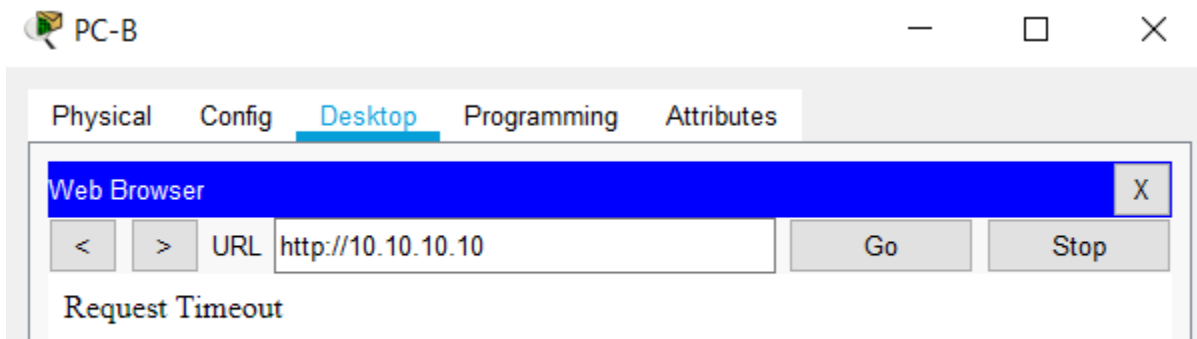
```
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=1ms TTL=126
Reply from 10.10.10.10: bytes=32 time<1ms TTL=126
Reply from 10.10.10.10: bytes=32 time<1ms TTL=126
Reply from 10.10.10.10: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Web browser access on PC-B failed:



PC-B

Physical Config Desktop Programming Attributes

Web Browser

< > URL Go Stop

Request Timeout

Now we inspect http policy in ASA:



ASA

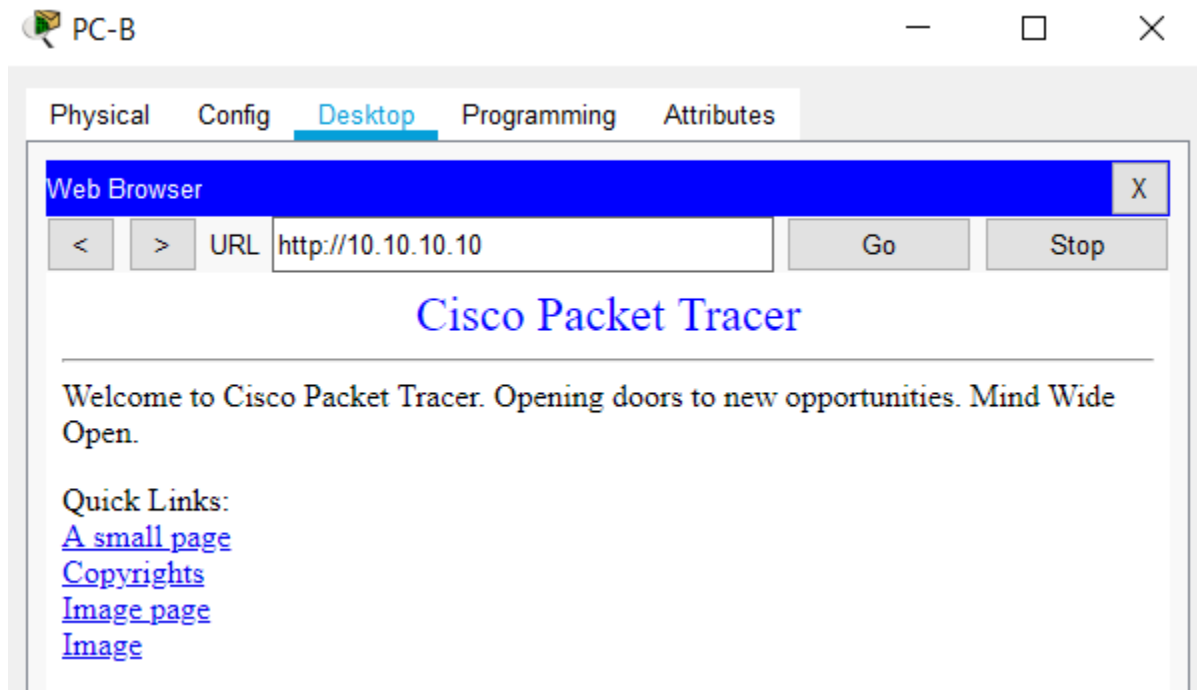
Physical Config CLI Attributes

IOS Command Line Interface

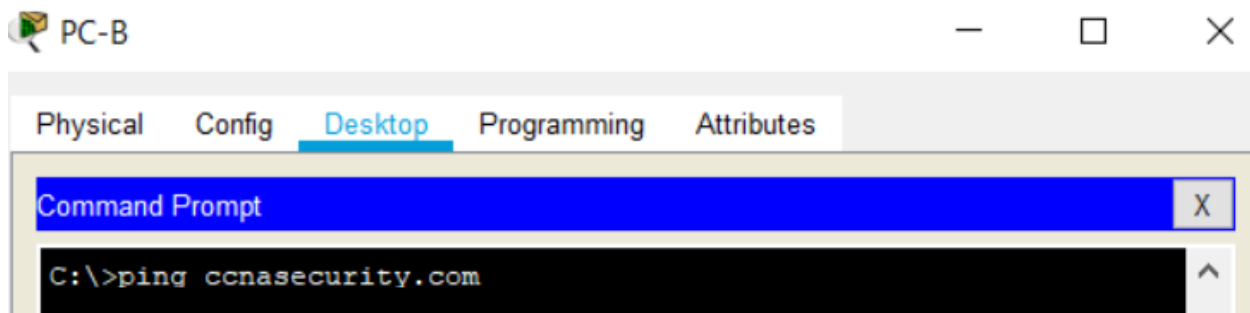
```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect http
ASA(config-pmap-c)#exit
ASA(config)#show run
: Saved
:
ASA Version 9.6(1)
```

```
class-map inspection_default
  match default-inspection-traffic
!
policy-map global_policy
  class inspection_default
    inspect http
    inspect icmp
!
service-policy global_policy global
.
```

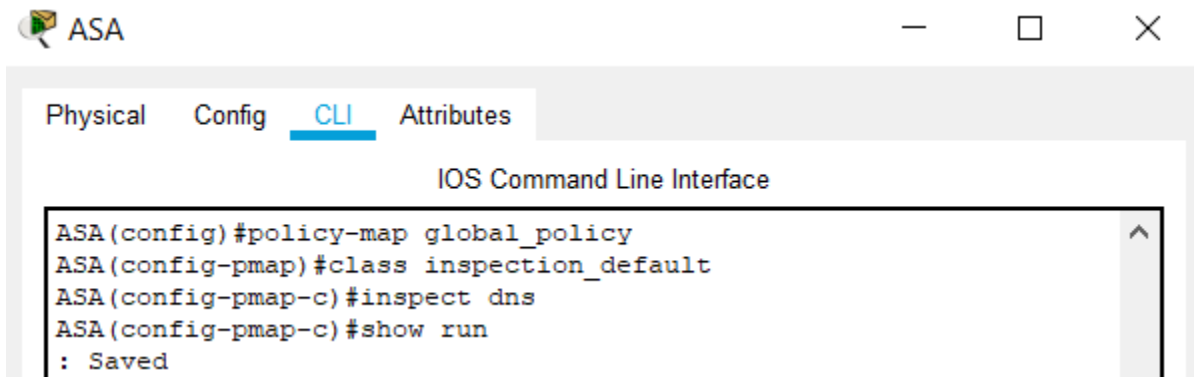
Now web browser access is successful:



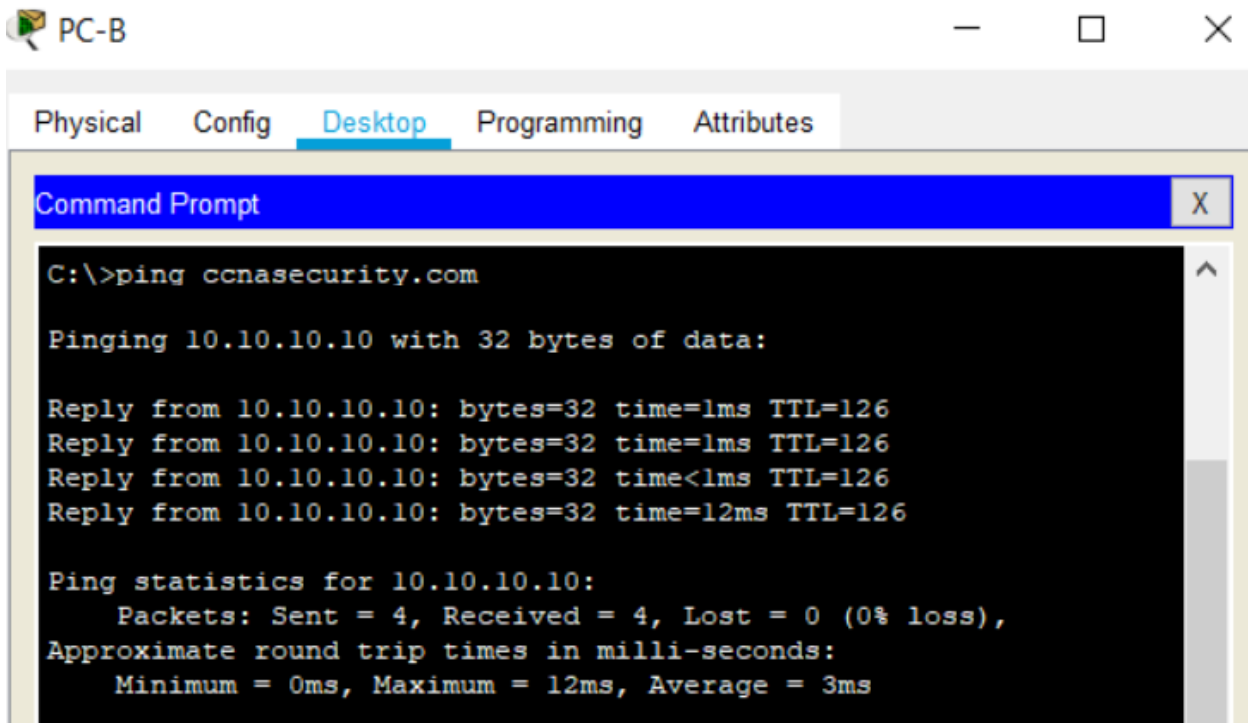
Pinging www.ccnasecurity.com is unsuccessful at first:



Then we inspect dns policy in ASA and it is successful:



```
policy-map global_policy
class inspection_default
inspect dns
inspect http
inspect icmp
.
```



Q.2

Vulnerable Site: <http://testphp.vulnweb.com/>

Ping :

```
C:\Users\PRIYAL BHARDWAJ>ping testphp.vulnweb.com

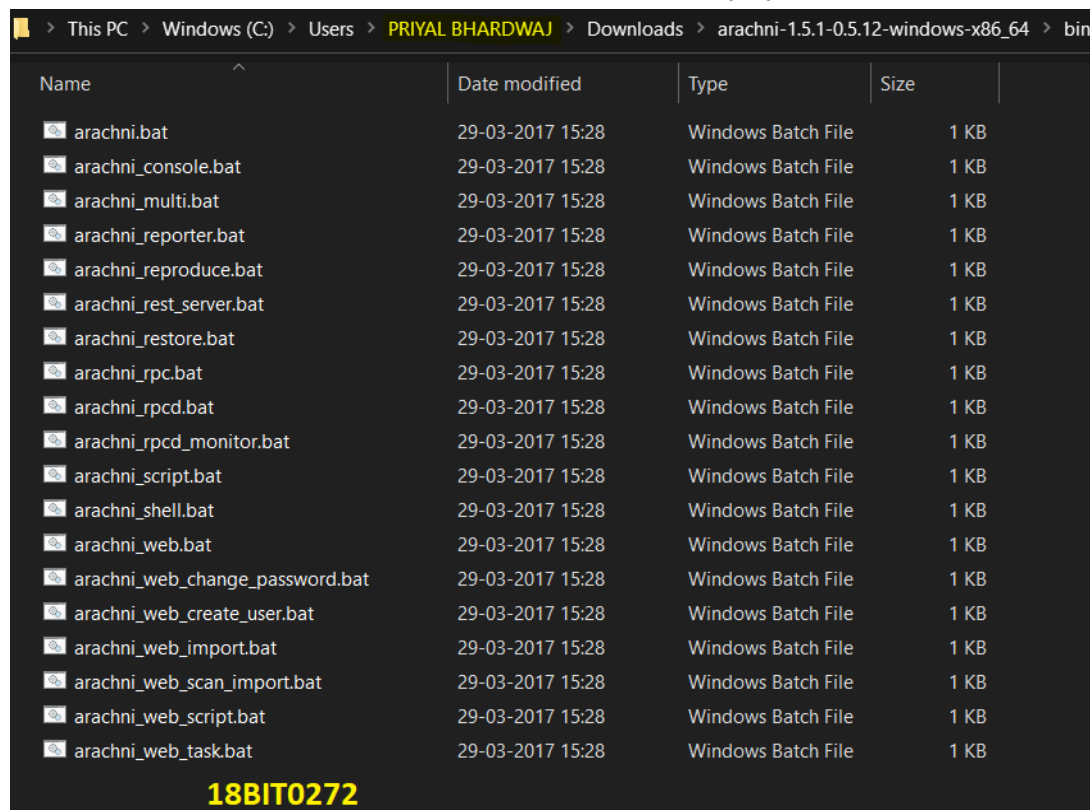
Pinging testphp.vulnweb.com [18.192.172.30] with 32 bytes of data:
Reply from 18.192.172.30: bytes=32 time=144ms TTL=50
Reply from 18.192.172.30: bytes=32 time=144ms TTL=50
Reply from 18.192.172.30: bytes=32 time=144ms TTL=50
Reply from 18.192.172.30: bytes=32 time=146ms TTL=50

Ping statistics for 18.192.172.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 144ms, Maximum = 146ms, Average = 144ms
```

IP Address of <http://testphp.vulnweb.com/> is **18.192.172.30**

Arachni is a Free/Public-Source Web Application Security Scanner that can be **used to** create automated security reports for your website as it evolves.

Downloaded the exe file and then installed Arachni in my system:



Name	Date modified	Type	Size
arachni.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_console.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_multi.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_reporter.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_reproduce.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_rest_server.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_restore.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_rpc.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_rpcd.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_rpcd_monitor.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_script.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_shell.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web_change_password.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web_create_user.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web_import.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web_scan_import.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web_script.bat	29-03-2017 15:28	Windows Batch File	1 KB
arachni_web_task.bat	29-03-2017 15:28	Windows Batch File	1 KB

18BIT0272

After launching arachni_web.bat from cmd it started listening on tcp://localhost:9292.

```
C:\Users\PRIYAL BHARDWAJ\Downloads\arachni-1.5.1-0.5.12-windows-x86_64\bin>arachni_web.bat
Puma 2.14.0 starting...
* Min threads: 0, max threads: 16
* Environment: development
* Listening on tcp://localhost:9292
```

Signed in to arachni using given user credentials and made a New Scan:

localhost:9292/scans/new

Arachni v1.5.1 - WebUI v0.5.12 Scans ▾ Profiles ▾ Dispatchers ▾ Users ▾ [Regular User](#)

Start a scan

The only thing you need to do is provide some basic information and make a simple choice about the type of scan you want to perform.

Default (Global) ▾

Full URL of the targeted web application (must include the appropriate protocol, http or https).

18BIT0272

PRIYAL BHARDWAJ

ISM LAB FAT

VULNERABILITY TESTING

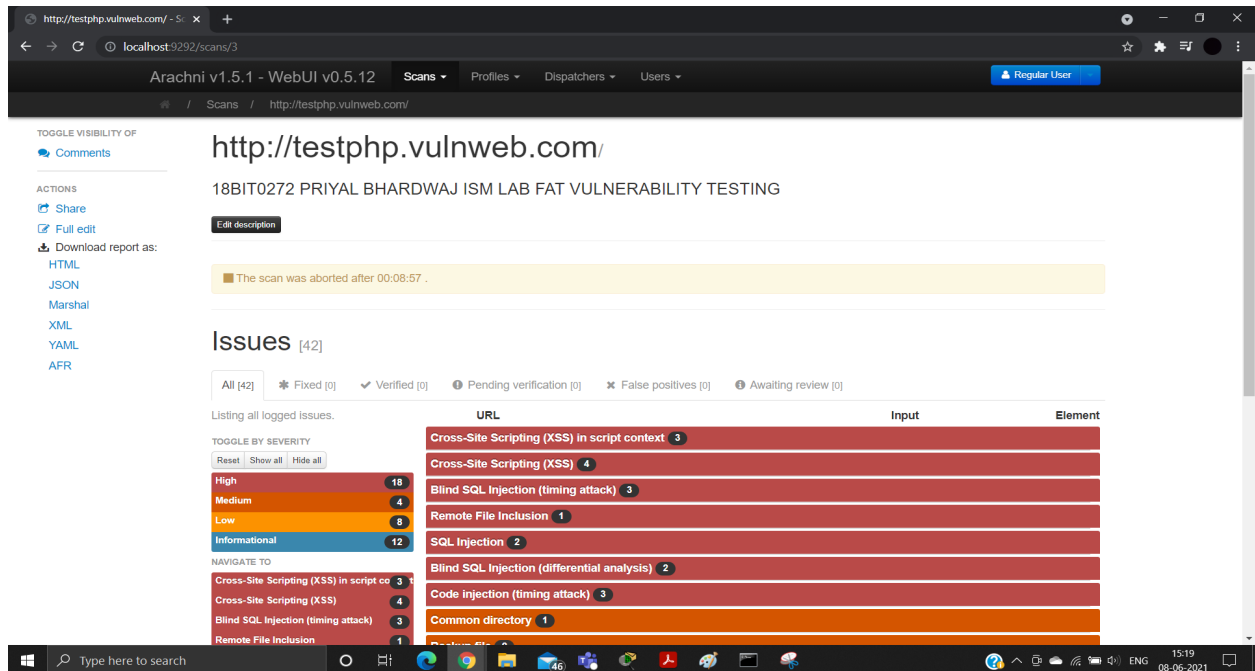
Share with:
Administrator

You can use Markdown for text formatting.

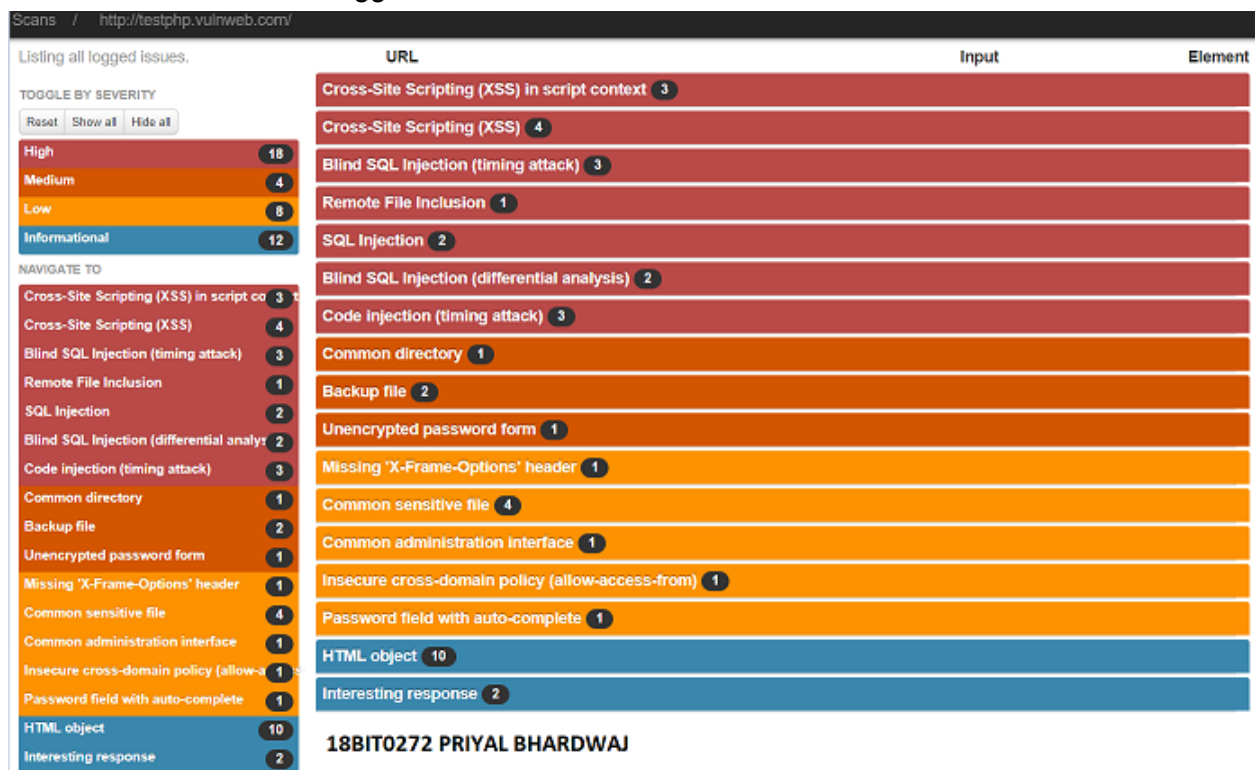
Advanced options

Go!

Scanned the website for about 9 minutes and got 42 issues:



Closer look at the issues logged:



```
C:\Windows\System32\cmd.exe - arachni_web.bat
Microsoft Windows [Version 10.0.19041.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PRIYAL BHARDWAJ\Downloads\arachni-1.5.1-0.5.12-windows-x86_64\bin>arachni_web.bat
Puma 2.14.0 starting...
* Min threads: 0, max threads: 16
* Environment: development
* Listening on tcp://localhost:9292

0:1 - [08/Jun/2021:15:06:31 +0530] "GET /unauthenticated HTTP/1.1" 302 - 0.2383
0:1 - [08/Jun/2021:15:06:32 +0530] "GET /d/users/sign_in HTTP/1.1" 200 - 0.5674
0:1 - [08/Jun/2021:15:06:32 +0530] "GET /d/users/sign_in HTTP/1.1" 404 728 0.0130 - 0.4668
0:1 - [08/Jun/2021:15:06:35 +0530] "POST /d/users/sign_in HTTP/1.1" 302 - 0.4668
0:1 - [08/Jun/2021:15:06:36 +0530] "GET / HTTP/1.1" 200 - 0.7737
0:1 - [08/Jun/2021:15:06:36 +0530] "GET /navigation HTTP/1.1" 304 - 0.0310
0:1 - [08/Jun/2021:15:06:36 +0530] "GET /actions/index&controller=home&partial=true HTTP/1.1" 304 - 0.0190
0:1 - [08/Jun/2021:15:06:41 +0530] "GET /navigation HTTP/1.1" 304 - 0.0402
0:1 - [08/Jun/2021:15:06:41 +0530] "GET /action/index&controller=home&partial=true HTTP/1.1" 304 - 0.0532
0:1 - [08/Jun/2021:15:06:46 +0530] "GET /navigation HTTP/1.1" 304 - 0.0510
0:1 - [08/Jun/2021:15:06:46 +0530] "GET /action/index&controller=home&partial=true HTTP/1.1" 304 - 0.0550
0:1 - [08/Jun/2021:15:06:51 +0530] "GET /navigation HTTP/1.1" 304 - 0.0408
0:1 - [08/Jun/2021:15:06:55 +0530] "GET /navigation HTTP/1.1" 304 - 0.0487
0:1 - [08/Jun/2021:15:06:55 +0530] "GET /action/index&controller=home&partial=true HTTP/1.1" 304 - 0.0530
0:1 - [08/Jun/2021:15:06:55 +0530] "GET /action/index&controller=home&partial=true HTTP/1.1" 304 - 0.0589
0:1 - [08/Jun/2021:15:06:59 +0530] "GET /scans/new HTTP/1.1" 200 - 0.4114
0:1 - [08/Jun/2021:15:06:59 +0530] "GET /navigation HTTP/1.1" 304 - 0.0409
0:1 - [08/Jun/2021:15:07:04 +0530] "GET /navigation HTTP/1.1" 304 - 0.0339
0:1 - [08/Jun/2021:15:07:09 +0530] "GET /navigation HTTP/1.1" 304 - 0.0250
0:1 - [08/Jun/2021:15:07:14 +0530] "GET /navigation HTTP/1.1" 304 - 0.0197
0:1 - [08/Jun/2021:15:07:19 +0530] "GET /navigation HTTP/1.1" 304 - 0.0420
0:1 - [08/Jun/2021:15:07:24 +0530] "GET /navigation HTTP/1.1" 304 - 0.0173
0:1 - [08/Jun/2021:15:07:29 +0530] "GET /navigation HTTP/1.1" 304 - 0.0190
0:1 - [08/Jun/2021:15:07:34 +0530] "GET /navigation HTTP/1.1" 304 - 0.0250
0:1 - [08/Jun/2021:15:07:39 +0530] "GET /navigation HTTP/1.1" 304 - 0.0260
0:1 - [08/Jun/2021:15:07:44 +0530] "GET /navigation HTTP/1.1" 304 - 0.0323
0:1 - [08/Jun/2021:15:07:49 +0530] "GET /navigation HTTP/1.1" 304 - 0.0460
0:1 - [08/Jun/2021:15:07:54 +0530] "GET /navigation HTTP/1.1" 304 - 0.0320
0:1 - [08/Jun/2021:15:07:59 +0530] "GET /navigation HTTP/1.1" 304 - 0.0420
0:1 - [08/Jun/2021:15:08:04 +0530] "GET /navigation HTTP/1.1" 304 - 0.0336
0:1 - [08/Jun/2021:15:08:09 +0530] "GET /navigation HTTP/1.1" 304 - 0.0320
0:1 - [08/Jun/2021:15:08:14 +0530] "GET /navigation HTTP/1.1" 304 - 0.0260
0:1 - [08/Jun/2021:15:08:19 +0530] "GET /navigation HTTP/1.1" 304 - 0.0220
0:1 - [08/Jun/2021:15:08:24 +0530] "GET /navigation HTTP/1.1" 304 - 0.0254
0:1 - [08/Jun/2021:15:08:29 +0530] "GET /navigation HTTP/1.1" 304 - 0.0369
0:1 - [08/Jun/2021:15:08:34 +0530] "GET /navigation HTTP/1.1" 304 - 0.0195
0:1 - [08/Jun/2021:15:08:39 +0530] "GET /navigation HTTP/1.1" 304 - 0.0443
0:1 - [08/Jun/2021:15:08:44 +0530] "GET /navigation HTTP/1.1" 304 - 0.0222
0:1 - [08/Jun/2021:15:08:49 +0530] "GET /navigation HTTP/1.1" 304 - 0.0190
0:1 - [08/Jun/2021:15:08:54 +0530] "GET /navigation HTTP/1.1" 304 - 0.0180
0:1 - [08/Jun/2021:15:08:59 +0530] "GET /navigation HTTP/1.1" 304 - 0.0229
0:1 - [08/Jun/2021:15:09:04 +0530] "GET /navigation HTTP/1.1" 304 - 0.0331
```

We can find a detailed description of the issues logged on Arachni along with CWE link to see solutions for that vulnerability:

Listing all logged issues.

TOGGLE BY SEVERITY

Reset Show all Hide all

High18

Medium4

Low8

Informational12

NAVIGATE TO

Cross-Site Scripting (XSS) in script context3

Cross-Site Scripting (XSS)4

Blind SQL Injection (timing attack)3

Remote File Inclusion1

SQL Injection2

Blind SQL Injection (differential analysis)2

Code injection (timing attack)3

Common directory1

Backup file2

Unencrypted password form1

Missing 'X-Frame-Options' header1

Common sensitive file4

Common administration interface1

Insecure cross-domain policy (allow-s)1

Password field with auto-complete1

HTML object10

Interesting response2

Cross-Site Scripting (XSS) in script context3

Cross-Site Scripting (XSS)4

Blind SQL Injection (timing attack)3

Remote File Inclusion1

SQL Injection2

Due to the requirement for dynamic content of today's web applications, many rely on a database backend to store data that will be called upon and processed by the web application (or other programs). Web applications retrieve data from the database by using Structured Query Language (SQL) queries.

To meet demands of many developers, database servers (such as MSSQL, MySQL, Oracle etc.) have additional built-in functionality that can allow extensive control of the database and interaction with the host operating system itself.

An SQL injection occurs when a value originating from the client's request is used within a SQL query without prior sanitisation. This could allow cyber-criminals to execute arbitrary SQL code and steal data or use the additional functionality of the database server to take control of more server components.

The successful exploitation of a SQL injection can be devastating to an organisation and is one of the most commonly exploited web application vulnerabilities.

This injection was detected as Arachni was able to cause the server to respond to the request with a database related error.

18BIT0272 PRIYAL BHARDWAJ
(CWE)

http://testphp.vulnweb.com/listproducts.phpcatLink

http://testphp.vulnweb.com/search.phptestLink

Blind SQL Injection (differential analysis)2

SQL Injection CWE Screenshot:

http://testphp.vulnweb.com/ - 5 x CWE - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') x +

Not secure | cwe.mitre.org/data/definitions/89.html

CWE Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE - Individual Dictionary Definition (4.4)

Home | About | CWE List | Scoring | Community | News | Guidance | Search

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Weakness ID: 89
Abstraction: Base
Structure: Simple

Status: Stable

Presentation Filter: Complete

Description

The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Extended Description

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.

SQL Injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

Relationships

The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf		943	Improper Neutralization of Special Elements in Data Query Logic
ParentOf		564	SQL Injection: Hibernate
CanFollow		456	Missing Initialization of a Variable

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf		137	Data Neutralization Issues

Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)

Relevant to the view "Architectural Concepts" (CWE-1008)

Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)

Potential Mitigations:

http://testphp.vulnweb.com/ - 5 x CWE - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') x +

Not secure | cwe.mitre.org/data/definitions/89.html

Potential Mitigations

Phase: Architecture and Design
Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, consider using persistence layers such as Hibernate or Enterprise Java Beans, which can provide significant protection against SQL injection if used properly.

Phase: Architecture and Design
Strategy: Parameterization
If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.
Process SQL queries using prepared statements, parameterized queries, or stored procedures. These features should accept parameters or variables and support strong typing. Do not dynamically construct and execute query strings within these features using "exec" or similar functionality, since this may re-introduce the possibility of SQL injection. [REF-967]

Phases: Architecture and Design; Operation
Strategy: Environment Hardening
Run your code using the lowest privileges that are required to accomplish the necessary tasks [REF-76]. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations.
Specifically, follow the principle of least privilege when creating user accounts to a SQL database. The database users should only have the minimum privileges necessary to use their account. If the requirements of the system indicate that a user can read and modify their own data, then limit their privileges so they cannot read/write others' data. Use the strictest permissions possible on all database objects, such as execute-only for stored procedures.

Phase: Architecture and Design
For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-502. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Phase: Implementation
Strategy: Output Encoding
While it is risky to use dynamically-generated query strings, code, or commands that mix control and data together, sometimes it may be unavoidable. Properly quote arguments and escape any special characters within those arguments. The most conservative approach is to escape or filter all characters that do not pass an extremely strict allowlist (such as everything that is not alphanumeric or white space). If some special characters are still needed, such as white space, wrap each argument in quotes after the escaping/filtering step. Be careful of argument injection (CWE-88).
Instead of building a new implementation, such features may be available in the database or programming language. For example, the Oracle DBMS_ASSERT package can check or enforce that parameters have certain properties that make them less vulnerable to SQL injection. For MySQL, the mysql_real_escape_string() API function is available in both C and PHP.

Phase: Implementation
Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does.

CWE Link: <http://cwe.mitre.org/data/definitions/89.html>