Ex120 Submission

Gary Jones

Contents

Executive Summary

Goals

The goal of this exercise was to Uncover remote code execution in a web site.

Risk Ranking/Profile

This risk is critical as this exploit allowed me to inject a program onto the page and access the files that should not be available to myself.

Summary of Findings

I was able to find and access the certification keys of IntermediateCA.txt, RootCA.txt, and Server.txt as well as access the file 'ThisIsTheFileYouAreLookingFor' in the brian/private directory.

Recommendation Summary

The recommendation from this exercise is to use https instead of http.

Attack Narrative

To begin I ran nikto on http://www.artstailor.com/brian and through this the directory /brian/private/ was indicated as being interesting (see figure 1). Opening the web browser I went to artstailor.com/brian and clicked on on image while inspecting the source code for the page and identified that the image source was not the same as the url. I injected raw=true into the web url and then changed the targeted file to htpasswd to get the username and password for the page (see figures 2, 3, and 4). From a google search I found that the password is MD. In order to decrypt it I saved the string into a file and ran it against john the ripper. From this I identified the password to be swordfish (see figure 5).

At this point I was able to gain access to the administrator page using the credentials brian:swordfish (see figure 6). In order to proceed forward I copied the shell.php into the directory /var/www/html/, changed the password for it to one of my design, added 172.24.0.10 to the allowedIPs parameter, and removed the deprecated lines of code on lines 119 and 120. To confirm the Laudanum PHP Shell Access was operational I checked 172.24.0.10/shell.php in the web browser until it was operational (see figures 7, 8, and 9).

Once this the page was complete I turned to Burp Suite and opened its browser. Ensuring that Intercept was on I navigated to http://www.artstailor.com/brian and entered the credentials for administrator privileges. Since this page only allows the import of .png files I copied the file shell.php into shell.png and up-

loaded that onto the website (see figure 10). Once this was intercepted by Burp Suite I changed the filename from shell.png back to shell.php (see figures 11 and 12).

At this point I was now able to go to the directory http://artstailor.com/brian/imgfiles/shell.php and access all files on the website which includes the file 'ThisIsTheFileYouAreLookingFor' in the directory /var/www/html/brian/private and the IntermediateCA.txt, RootCA.txt, and Server.txt files in the directory /var/www/html/certs (see figures 13, 14, 15, and 16).

Figure 1:

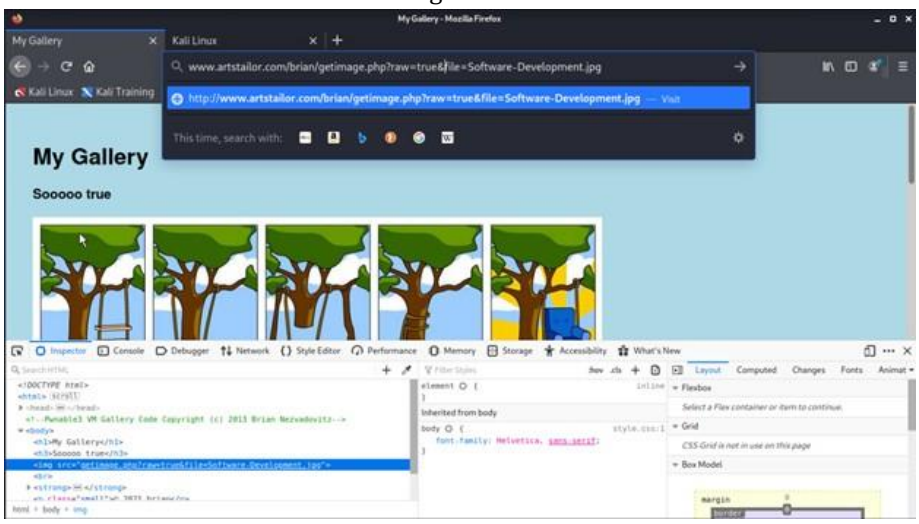
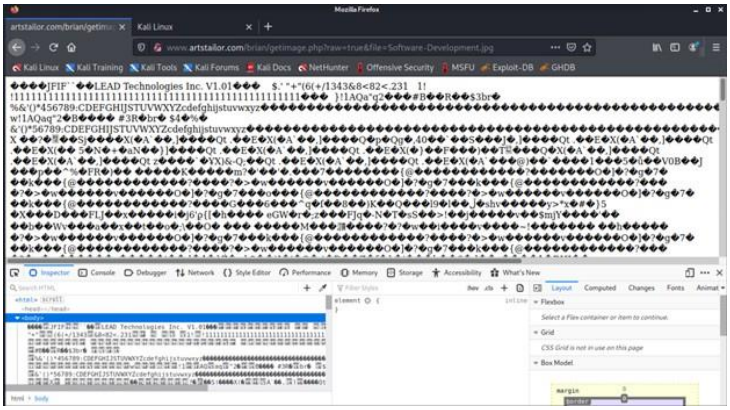


Figure 2:



Figu4re 3:

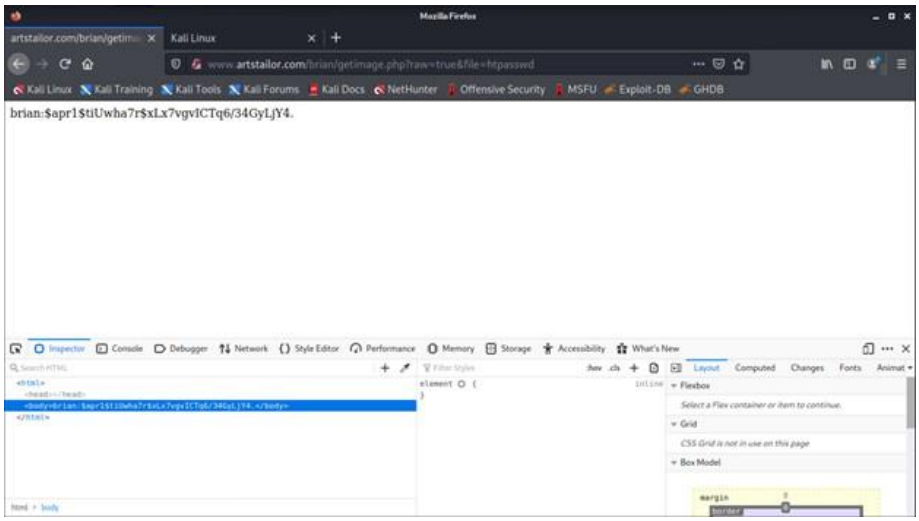


Figure 4:

```
┌──(kali㉿kali)-[~]
└─$ sudo john doc2.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 22 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 33 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 41 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
swordfish        (brian)
1g 0:00:00:00 DONE 2/3 (2021-11-27 16:45) 10.00g/s 27820p/s 27820c/s 27820C/s rockie..121212
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 5:

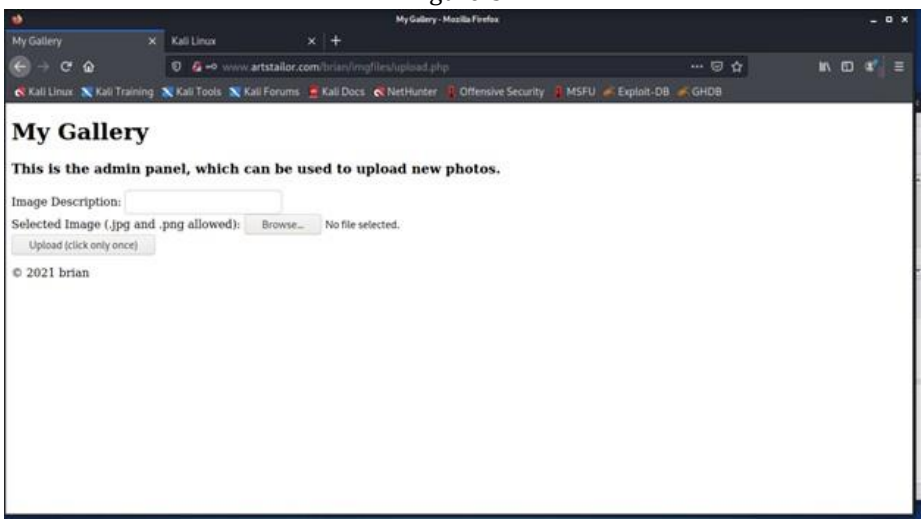


Figure 6:

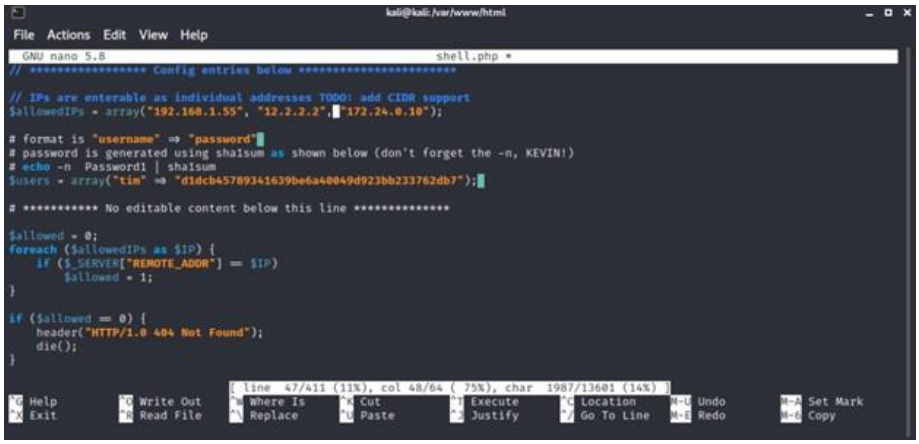


Figure 7:

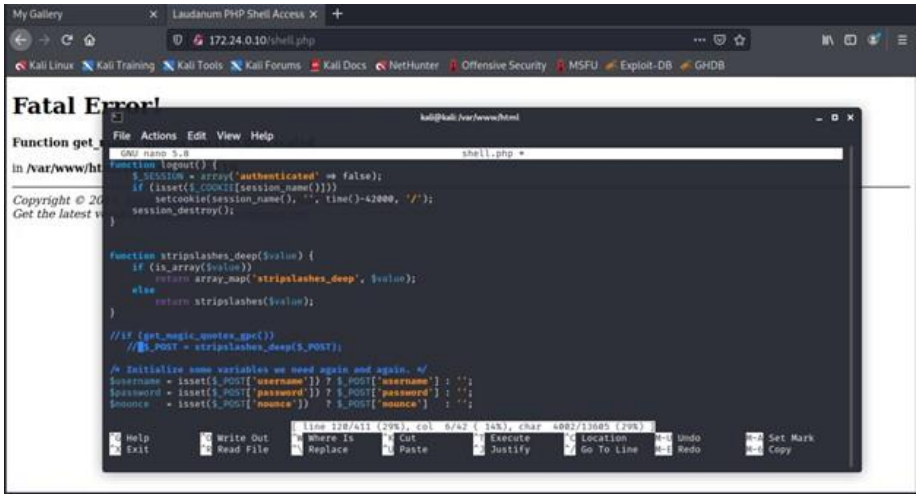


Figure 8:

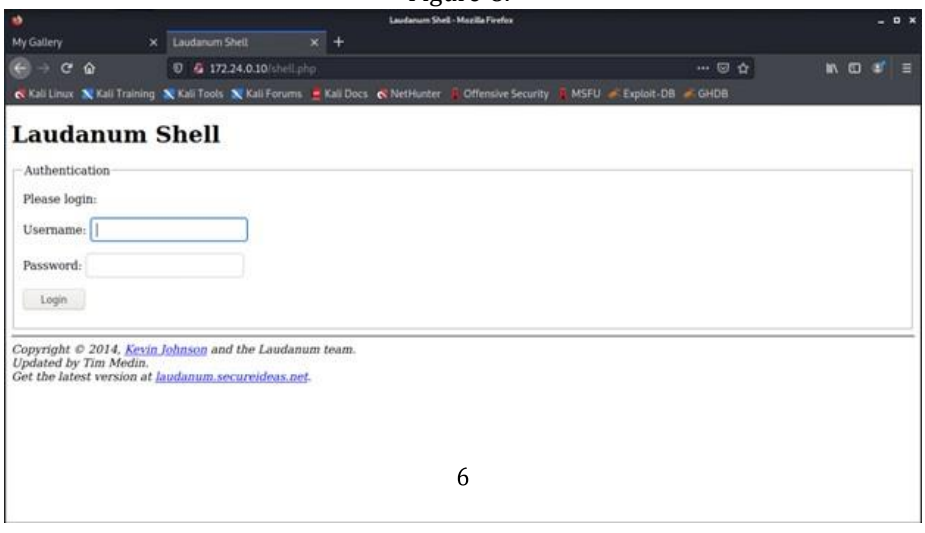


Figure 9:

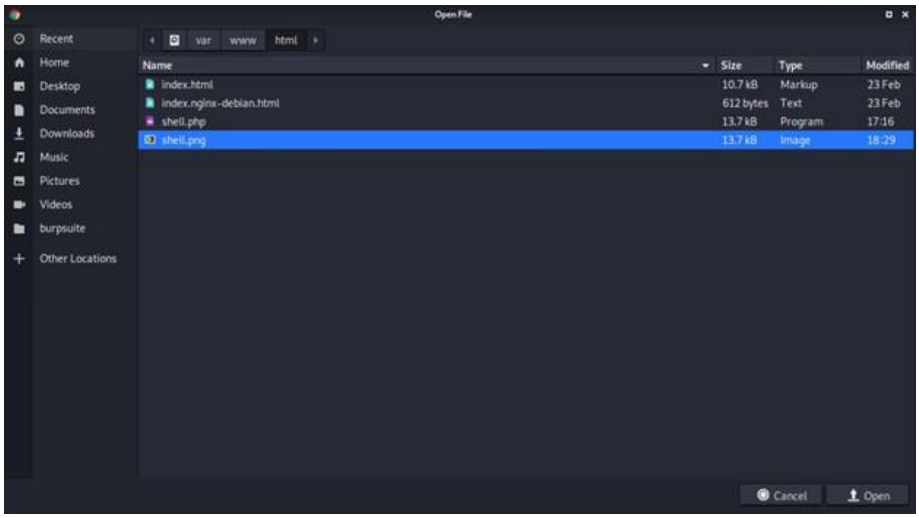


Figure 10:

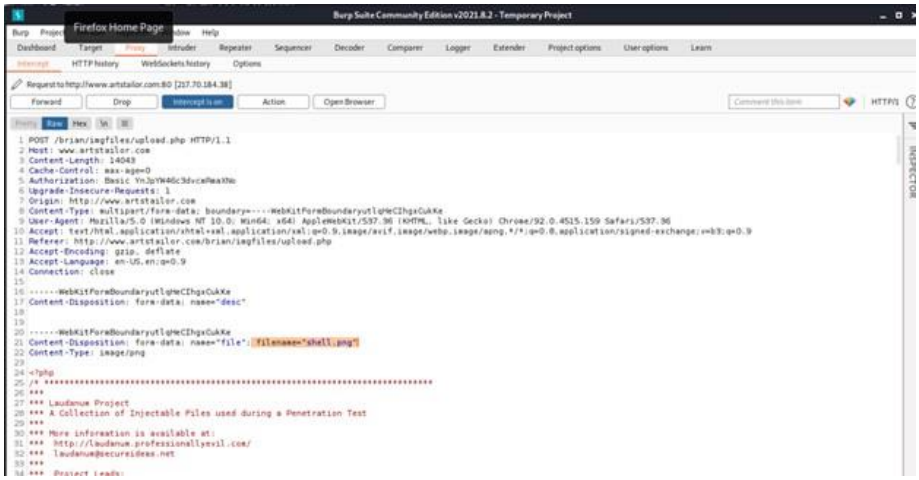


Figure 11:

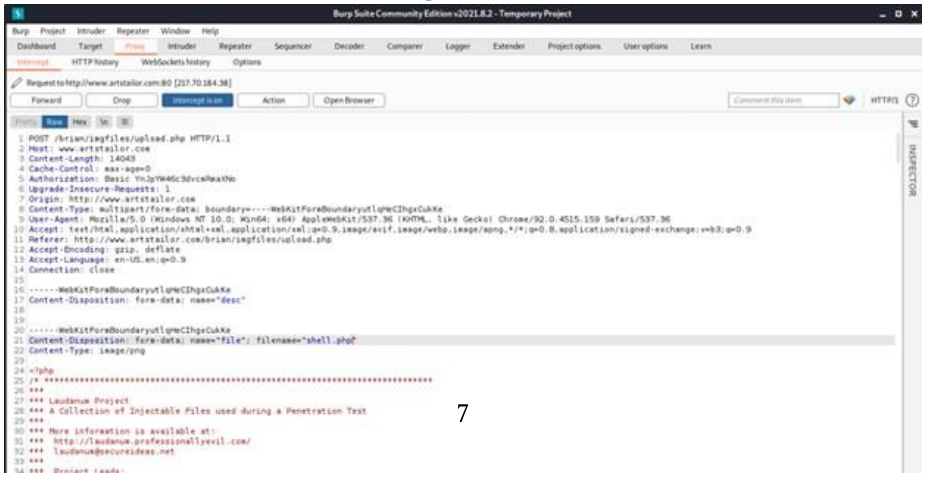


Figure 12:

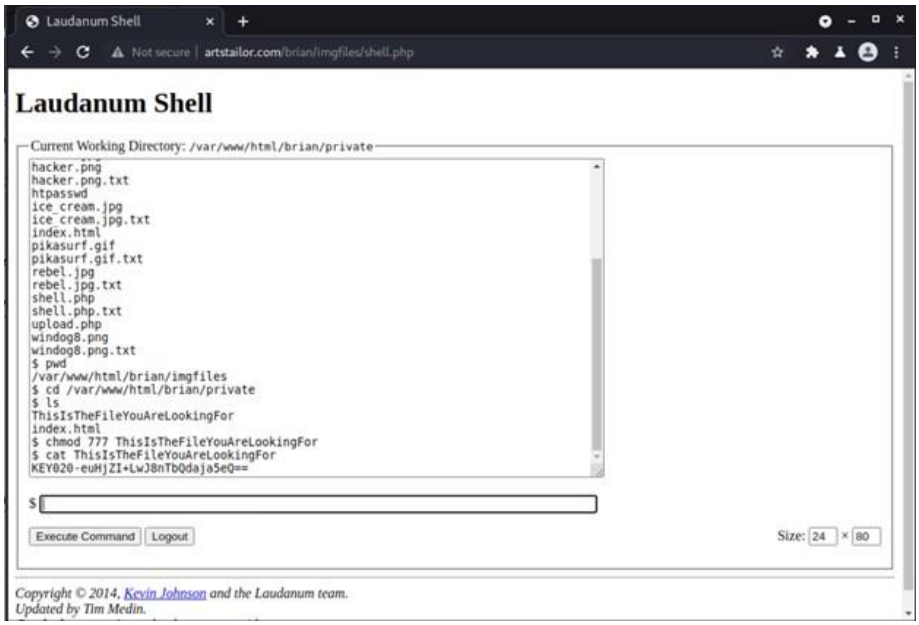


Figure 13:

```
$ cat IntermediateCA.txt
-----BEGIN CERTIFICATE-----
MIIFyTCCA7ECFBwO+UpJPMDH9EuqnzwORFJ9r7YWMA0GCSqGSIb3DQEBCwUAMIGg
MQswCQYDVQQGEwJVUzEQMA4GA1UECAwHRmxvcmlkYTEUMBIGA1UEBwwLR2FpbmVz
dmlsbGUxEzARBgNVBAoMCmFydHN0YWlsb3IxFDASBgNVBAsMC0VuZ2luZWVyaW5n
MRswGQYDVQQDDBJ3d3cuYXJ0c3RhaWxvci5jb20xITAfBgkqhkiG9w0BCQEWEm9w
cEBhcnRzdGFpbG9yLmNvbTAeFw0yMTExMDMwMDI5MjVaFw00OTAzMjEwMDI5MjVa
MIGgMQswCQYDVQQGEwJVUzEQMA4GA1UECAwHRmxvcmlkYTEUMBIGA1UEBwwLR2Fp
bmVzdmlsbGUxEzARBgNVBAoMCmFydHN0YWlsb3IxFDASBgNVBAsMC0VuZ2luZWVy
aW5nMRswGQYDVQQDDBJ3d3cuYXJ0c3RhaWxvci5jb20xITAfBgkqhkiG9w0BCQEW
Em9wcEBhcnRzdGFpbG9yLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoC
ggIBAJ7Up+8qklQvML7zEnyYesjv1ezeho8k2tm/R5xsRULBwUYkYhdObYup4duD
idJWDxLEPK9bfJ//RHGj470v5KEi3yFHfcC/mTJBn2wSLQSkQbVdeW1HT6T9/YHq
0I9jN1IkTTVMCFC1YuAGOHuMLZX3KTnIra8WHPQKYM/gpDy8xer6VbsAPtdAbSdG
dxJh31KraDXQhLTizmxGuauqp+qZesbWkUTxARI1fThDc4t9xHx73IQasF65LLjC
YzvLW0JWRBpBtr+lKvutgo8tYOpkDFVAhiyAue4etx66ZE7lycasAmcVpgNCHNW/
UE+AD4sG3Tbp0OOFWrzsOMvNCUvI93C7xba0o6PzIcXkusZQDOi3V+wNL4bo6TTp
GjxFQO9WMTWdzFfS+G3of1SGn39RRnln4AKvu84e2Jr/UgMk1kc61JOtI+elTkfV
RVW4C5iLxLyak19P2FXG4eTbT21SVtQPfeS0FIFuTHrS+J4+w/2/GtyLrBukknoI
OANIvhLX6cUwoc6S95GBVyxbRx5rt94Qac+sCB8DKP5XhgGXAGnzle39RXstEs1A
L//0X1BnBiOgJusqycJn+HCFDihDU7E9e+Qn1CMnDDXmVsMBk60scmPEI3ob46dz
iYA2bbAtTELU/1tfz9mYHyvMAiGAj9SDPF9sfPLkW4/qDJ0ZAgMBAAEwDQYJKoZI
hvcNAQELBQADggIBAHAG1OcGVNKW4UYPlyDOZtCNOB5SPKac2Ku+kCKRYtuWJDJz
jilNNpaURuHbvF0DxXMBvUciQkGaeacrmUB7yS3E9dZA99D2PxkMPu7Y/KqiUvkF
k61bQ5dE6X32yve6Xem5Vbj9/QJBkwexQTFJlKk1+b7NwUEjjcuE3fBKc45S0yJT
CZrtHnkNfXhBR0kXl8VlFtmmB349umbsh4X2L7BPhYyKMoqoQV0yl7o62mWGGLuX
7pifNBhwnrhQK/U1HFDSihJhNt46O9Obxh5zqB4PjCGpsoook6U08L7xzjarHQul
isZu5kbM36q7juNPlxu2vtPxqnIfiGF1qLbqYNxjLpncQfmIR3QybBdv/m1VEA9C
d7vhNqDrq/V0VU5pNTTTgC2tQIVluGO2tCLtsJcrK3eZQzIjnY7DkpBYwTj3FPmI
QhyX7CFjkW2W8VosOpCIKxDLFjZUb6xyXBs9XCvtU38QUT6xe8y5pYQLCTUWa6NJ
w9i2OqNPD1UWqxJ2u0iaPFdUfUrl6L8WplIpgBAtxIDTIe9MDYHJU/6jLfGWDnko
7aKS9QV0CFXoSXi5VqqcJQfGDQvP4yDXwnfo27LI9XTaf7RxpnwiuM1d2sEraBL3
xR8WSK2oFXbpC384M1MkucSQbTH/Z+X3zZcUl147KrPO2J8QBKWpBuRl6EaK
-----END CERTIFICATE-----
```


Figure 14:

```
$ cat RootCA.txt
-----BEGIN CERTIFICATE-----
MIIGIzCCBAugAwIBAgIUNMrBaSUdw7pS/tlPMUtpKGNhfOwwDQYJKoZIhvcNAQEL
BQAwgaAxCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAdGbG9yaWRhMRQwEgYDVQQHDAtH
YWluZXN2aWxsZTETMBEGA1UECgwKYXJ0c3RhaWxvcjEUMBIGA1UECwwLRW5naW5l
ZXJpbmcxGzAZBgNVBAMMEnd3dy5hcnRzdGFpbG9yLmNvbTEhMB8GCSqGSIb3DQEJ
ARYSb3BwQGFydHN0YWlsb3IuY29tMB4XDTIxMTEwMzAwMjUwOFoXDTQ5MDMyMTAw
MjUwOFowgaAxCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAdGbG9yaWRhMRQwEgYDVQQH
DAtHYWluZXN2aWxsZTETMBEGA1UECgwKYXJ0c3RhaWxvcjEUMBIGA1UECwwLRW5n
aW5lZXJpbmcxGzAZBgNVBAMMEnd3dy5hcnRzdGFpbG9yLmNvbTEhMB8GCSqGSIb3
DQEJARYSb3BwQGFydHN0YWlsb3IuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAvMQedUrt1tN8A5JExv1UORl0gGoVX4Ck0PaMY+9yXUzKx6x/aX0S
lzzfCPBmc1tmI7BbIJSdhO3NBHOqkjAkQfdyGItAKUTl6qyXCl8+Y1u2d6kZYbQM
WZTwQb1GgXEHO7O5SGcIdoEHkcO/lHD98ZEi/LJAs+yk0MDXAgPvVOo+o8WFhthC
TJN/Xv64Q5kIurXEkwed+PHeueCLIOTKYDO+KKPpspF61ejsItRayzVMFeYWMN1n
8Q5U8Yo5DA8PmB8kxvdIKIyHK7iOpz31ESMlt/V0etPsjTNI8xeaA4/t/5UNWt9s
eBoP3L1xOyoHfKyZi4KD6iSXUdk1n7ZXP1pJo8ChRDTK0Pru97ZDungw2IH1KlQr
flTlNWp/DxK9NR3laGsVnZu5/1ZJf++wRHFnXoCgxPIxu3SryzHoa/bBCBvT/Yqj
gEDjBDnYi1H/C5DU9n87T6HDxV7ww7d4oZJnNTB49pgiawcbji4rU1dNkXKfmS2K
0Z1N23EI7Qug2OnWPk/7NU/j5KCpVxFz7WUKENkUyLXnGh+AJ6kJwWw4395527px
9zMUPaSq9npJ7l5+IRjk1OpUX/Bq7w66mfyZerCYmPW+uRcmIuatsNGxrFE0L7SJ
6T/823B0veCE68Bso/Sbuwv/3HOYWls9Bj3HcGGM2DgENT4ScZSQkxcCAwEAAaNT
MFEwHQYDVR0OBBYEFDQImtsYSEHbRgKLi88qUWu2lKleMB8GA1UdIwQYMBaAFDQI
mtsYSEHbRgKLi88qUWu2lKleMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggIBAI+Re5IjdDVgl85KnjM2BJJxBm5D+WwoCLRREbplGsvNagoRViSrnAyB
T/Oa0IlF2NtQGex7vvalV8FG1C69gQ8A3yBidLXeSeqzQ0mfh3GsssVUFaWe+rv1
2M44gPyCqBDHqmZYMFZwIV4FLQ2AIFm5m9MdQJK5q6Gh0Uwul6MgOPEdCToi8sHd
03DEnas9AVZ570c/GW7ac+qc4RIQGfn4Ap3TS0A5RRjGp+pssIaQxGRSFEmY93sQ
4GIcB5iMRer8/Ak82JplGhiP/m+vehHwoBcJ/ncHWb3616YQjV8T5I7lIV3cs3sp
E5i9QL/IeL3oszwjDobuZB00ZVvVAI06AhoN4aW4DimQhdf0ZiI4KF0XMSOM4caz
b29TubbCjBh0rPeNLgf79Tvll71PUqYa2jPQjVsStmbhI5q+LeX5VRAJ7Svvw31+
KR0nYpByG5UC041BtfMH27xTx8cE2zk4OHF/GnqgTgTIC1yOo6sy9Y96d7EOoTaC
xcpw0zXe54HWxlJ1rqdIBl1DTc3QXtbCrgu7SMLyZAmTVjcTSoairj45P0NFjfWu
5/XVgrXQ1aD8awSs73J62vMZYiR/Y3DYuB1YrnESHY4kjoOUDqm084saekQsTVfB
Zv3s4gblLaX6HtwiXWLVa8oa446V8sLBGKF9QlBCB2LrOpD4efek
-----END CERTIFICATE-----
```

Figure 15:

```
$ cat Server.txt
-----BEGIN CERTIFICATE-----
MIIEtjCCAp4CAWUwDQYJKoZIhvcNAQELBQAwgaAxCzAJBgNVBAYTAlVTMRAwDgYD
VQQIDAdGbG9yaWRhMRQwEgYDVQQHDAtHYWluZXN2aWxsZTETMBEGA1UECgwKYXJ0
c3RhaWxvcjEUMBIGA1UECwwLRW5naW5lZXJpbmcxGzAZBgNVBAMMEnd3dy5hcnRz
dGFpbG9yLmNvbTEhMB8GCSqGSIb3DQEJARYSb3BwQGFydHN0YWlsb3IuY29tMB4X
DTIxMTEwMzAwMzIxMloXDTQ5MDMyMTAwMzIxMlowgaAxCzAJBgNVBAYTAlVTMRAw
DgYDVQQIDAdGbG9yaWRhMRQwEgYDVQQHDAtHYWluZXN2aWxsZTETMBEGA1UECgwK
YXJ0c3RhaWxvcjEUMBIGA1UECwwLRW5naW5lZXJpbmcxGzAZBgNVBAMMEnd3dy5h
cnRzdGFpbG9yLmNvbTEhMB8GCSqGSIb3DQEJARYSb3BwQGFydHN0YWlsb3IuY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5f1s7H1lo8HvvA7ogosH
UyvuDjNBFtaAU8VKvmz1jioU93UG56TWrE/fgLWTpF4cYRL/Lq78iZDUhzi2PxlM
jeiOrgGVWmvXCfo+/tbNMv3YMzjt1mUBB281kPZZv2bCwgijU14CfUOM0B52GlKd
Cn11XeE7mCZXLxY6/6Sw9KxHbTOg1h1C76tUKLHREmdpn7cmfoDqOU7gK9F7mkOa
jxSCkWulmNS+V2GvwP/KOMKmWeFhGLXrq15ruaXd7gF6VYwm1vQ6bk68GuJMv7En
2xG1Gk/YhrzmcttoxZ9SYdFo0iOV005brwWmVrXkfTJNiRJU2aPVievpIS+xEeBh
iQIDAQABMA0GCSqGSIb3DQEBCwUAA4ICAQAhvSPNU3+tmYpdacSI8v+cP/omsmyH
84vNgHhKDw0BbJSnFO0A2xphEg0rR3l4h/md1Eq9XasniNy4vkAsfvLiAMz4BcN3
tgNQw1CNBl9tTdCu9p3GrNRcvKHSHh1V7DulV0RhAR5zwmUZd/VlBrWWYgc/Fz+H
bQLoMA8wSDfCIyHrabjqxXolpKsYXFc27T6ZVfp+8yULbQc+/SDkSdCLZJjRG1HH
ZiFlXIk6tXn9RyXV+Y+k+JNISBTjx56WkAJoiDVPamCkIGj0YHwcYvyklfIte1Aa
9iLRLXDJI/5V/nPOjvIZ9BNZt/uZD+uEsLRlbGz11HCT4XaAJcbA1YINqZXWwMKf
s5K7K6KMFcBTTQmMDR1+8O3WeTBEtC9FyfZ6i0suXpwolq5sMJ9l+frQ8XfgWtzz
c40wJXiXYT6KepORqTpkwx0zRXx3JRI4TGVeGBVb/4oWellyF93kRdlG0fxjgzqI
XjTbtWfFUh7bEHoES6KG71bRIjMYdyYH3JjCBHpFqXMtYNs0fTgQttBUweWBKOB+
UumuMeRVQFLPNZyKc1tn0DF+Mz1igsb0dkDUgvm8nchI/idMMHdoB1stMHsTqnsg
h9U+hZEbeCE+kScchlX2YrJwI0DOpOH39aCjoMd4RwzxoG8ABiogWvPnV2mH4HD9
IaaiGbGCxuhS/w==
-----END CERTIFICATE-----
```

Figur9e 16: