**Περιγραφή Ιστοσελίδας:**

**Έχουμε 3 είδη user:**

1. **Quest: Non-registered user, βλέπει απλά το Login και το Sign Up page της ιστοσελίδας.**
2. **Registered-User: Μπορεί να κάνει login με τα στοιχεία του username/password. Απαντάει σε τεστ, βλέπει τους βαθμούς του και τα στατιστικά όλων στο μάθημα.**
3. **Admin: Registered-user με παραπάνω δικαιώματα. Αξιολογεί, δεν αξιολογείται.**

Είναι πλατφόρμα για Online Tests, στην οποία ο *registered-user* έχει στην διάθεσή του έναν κατάλογο με μαθήματα *(στην συγκεκριμένη περίπτωση υπάρχει μόνο ένα),* για τα οποία υπάρχουν διάφορα test.

Έχει την επιλογή να γράψει όποιο θέλει σε ένα χρονικό διάστημα κ όταν το υποβάλει, περιμένει την αξιολόγησή του από τον admin.

O *admin* (είναι ένας) βαθμολογεί τα όποια test έχουν απαντηθεί, καθώς και δημιουργήσει νέα τεστ, είτε με random ερωτήσεις, είτε με δικές του.

1. ***ΧΑΡΤΟΓΡΑΦΗΣΗ ΠΣ:***

**ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΕΤΑΙΡΙΑΣ**

* Εκπαιδευτική Εταιρία
* Διαθέτει Computer Room με τα ακόλουθα Συστήματα:

- Application Server

- DB Server

- Web Server

- Main Network:

1. Firewall / Router
2. Main Switch

* Χ Laptop
* Y Desktop
* Εγκατεστημένες Εφαρμογές:

1. ERP Software
2. Windows
3. Office

**ΧΑΡΤΟΓΡΑΦΗΣΗ Ι**

* **Μισθοδοσία – Λογιστήριο**

Δεδομένα:

* Προσωπικά δεδομένα υπαλλήλων
* Προσωπικά δεδομένα πελατών
* Τιμολόγια
* Συμβάσεις.
* **Συστήματα:**

**(1) Main Network:**

– Main Router – HW Router

– Main Switch – HW Switch

– Firewall – Firewall SW

**(2) ERP System:**

* Application Server

- DELL Computer System – HW Server

- Linux Server – OS

- ERP Software

* DB Server

- DELL Computer System

- Linux Server

- SQL Server 2008 – DB Server SW

**(3) Workstations:**

– Windows 10 – OS

– DELL – HW – Workstation

– Office 2007 – SW

**ΧΑΡΤΟΓΡΑΦΗΣΗ ΙI**

* **Web Site**

Δεδομένα:

* Πηγαίος κώδικας
* Configuration Data
* **Συστήματα:**

**(1) Main Network:**

– Main Router – HW Router

– Main Switch – HW Switch

– Firewall – Firewall SW

**(2) Web Server:**

- DELL Server – HW

- Kali Linux 2017.2 – OS

- Apache Server – Web Server SW

**(3) DB Server:**

– DELL Server – HW

– Kali Linux 2017.2 – OS

– MySQL Server – DB Server SW

**(4) Admin Workstation:**

– Windows 10 – OS

– Office 2007 – SW

**ΜΈΤΡΑ ΠΟΥ ΛΉΦΘΗΚΑΝ:**

**Αντιμετώπιση Αδυναμιών του Nessus:**

* HTTP TRACE / TRACK Methods Allowed:

1. Πήγαμε στο path: C:\xampp\apache\conf\httpd.conf
2. Επεξεργαστήκαμε το αρχείο “httpd.conf”
3. και προσθέσαμε την εντολή **“TraceEnable off”**

* SMB Signing Disabled

1. Στον σύστημα στο οποίο τρέχει η σελίδα έχει disabled SMB(Service message block) και εμείς κάναμε τις παρακάτω ενέργειες για να το ενεργοποιήσουμε :
2. Cmd
3. Πληκτρολογούμε “regedit.exe”
4. Βρίσκουμε το hlkey\_local\_machine
5. Πάμε στο system current control setservicelanmanserver
6. Πάμε στις μεταβλητές(δεξί παράθυρο) και δημιουργούμε μια νέα μεταβλητή τύπου DWORD 32-bit με ονομασία SMB1.
7. Την τροποποιούμε και της βάζουμε την τιμή 1(Enable=1 , Disable=0).

* Με αυτό τον τρόπο μπλοκάρουμε το ‘eternal blue ‘ exploit το οποίο χρησιμοποιεί αυτό το smb port για να πάρει πρόσβαση στο σύστημα.

***(Οι βαθμοί κρισιμότητας είναι όπως τους είχαν από default όλα τα εργαλεία. Δεν τους ρυθμίσαμε εμείς)***

**Aδυναμίες Nessus μετά την αντιμετώπιση**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Critical** | | **High** | | | | **Medium** | **Low** | **Info** | **Total** | |  | |  | |  | |  | |  | |  | |  | |
| **0** | | | | 0 | 0 | | | **6** | **1** | **35** | **44** | |  | |  | |  | |  | |  | |  | |  | |
| **Details** | | | |  |  | | |  |  |  |  | |  | |  | |  | |  | |  | |  | |  | |
|  | **Severity** | | |  | **Plugin Id** | | | **Name** |  |  |  | | **State** | |  | |  | |  | |  | |  | |  | |
|  | **Medium (6.4)** | | |  | [5119](http://www.nessus.org/plugins/index.php?view=single&id=51192)2 | | | SSL Certificate Cannot Be Trusted | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Medium (6.4)** | | |  | [5758](http://www.nessus.org/plugins/index.php?view=single&id=57582)2 | | | SSL Self-Signed Certificate | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [1121](http://www.nessus.org/plugins/index.php?view=single&id=11213)3 | | | HTTP TRACE / TRACK Methods Allowed | | |  | | solved | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [4541](http://www.nessus.org/plugins/index.php?view=single&id=45411)1 | | | SSL Certificate with Wrong Hostname | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [5760](http://www.nessus.org/plugins/index.php?view=single&id=57608)8 | | | SMB Signing Disabled | |  |  | | solved | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [9311](http://www.nessus.org/plugins/index.php?view=single&id=93112)2 | | | OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [9443](http://www.nessus.org/plugins/index.php?view=single&id=94437)7 | | | SSL 64-bit Block Size Cipher Suites Supported (SWEET32) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Medium (4.0)** | | |  | [3529](http://www.nessus.org/plugins/index.php?view=single&id=35291)1 | | | SSL Certificate Signed Using Weak Hashing Algorithm | | | | | accepted | |  | |  | |  | |  | |  | |  | |
|  |  | | |  | | | |  | | | | |  | |  | |  | |  | |  | |  | |  | |
|  | **Low (2.6)** | | |  | [8387](http://www.nessus.org/plugins/index.php?view=single&id=83875)5 | | | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
|  |  | | |  | | | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1010](http://www.nessus.org/plugins/index.php?view=single&id=10107)7 | | | HTTP Server Type and Version | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1015](http://www.nessus.org/plugins/index.php?view=single&id=10150)0 | | | Windows NetBIOS / SMB Remote Host Information Disclosure | | | | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1028](http://www.nessus.org/plugins/index.php?view=single&id=10287)7 | | | Traceroute Information | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1039](http://www.nessus.org/plugins/index.php?view=single&id=10394)4 | | | Microsoft Windows SMB Log In Possible | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1073](http://www.nessus.org/plugins/index.php?view=single&id=10736)6 | | | DCE Services Enumeration | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1078](http://www.nessus.org/plugins/index.php?view=single&id=10785)5 | | | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure | | | | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1086](http://www.nessus.org/plugins/index.php?view=single&id=10863)3 | | | SSL Certificate Information | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1101](http://www.nessus.org/plugins/index.php?view=single&id=11011)1 | | | Microsoft Windows SMB Service Detection | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1121](http://www.nessus.org/plugins/index.php?view=single&id=11219)9 | | | Nessus SYN scanner | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1193](http://www.nessus.org/plugins/index.php?view=single&id=11936)6 | | | OS Identification | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1950](http://www.nessus.org/plugins/index.php?view=single&id=19506)6 | | | Nessus Scan Information | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2030](http://www.nessus.org/plugins/index.php?view=single&id=20301)1 | | | VMware ESX/GSX Server detection | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2164](http://www.nessus.org/plugins/index.php?view=single&id=21643)3 | | | SSL Cipher Suites Supported | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2296](http://www.nessus.org/plugins/index.php?view=single&id=22964)4 | | | Service Detection | |  |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2426](http://www.nessus.org/plugins/index.php?view=single&id=24260)0 | | | HyperText Transfer Protocol (HTTP) Information | | |  | | accepted | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | | [2691](http://www.nessus.org/plugins/index.php?view=single&id=26917)7 | | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [3571](http://www.nessus.org/plugins/index.php?view=single&id=35716)6 | | | | Ethernet Card Manufacturer Detection | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4311](http://www.nessus.org/plugins/index.php?view=single&id=43111)1 | | | | HTTP Methods Allowed (per directory) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4381](http://www.nessus.org/plugins/index.php?view=single&id=43815)5 | | | | NetBIOS Multiple IP Address Enumeration | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4541](http://www.nessus.org/plugins/index.php?view=single&id=45410)0 | | | | SSL Certificate 'commonName' Mismatch | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4559](http://www.nessus.org/plugins/index.php?view=single&id=45590)0 | | | | Common Platform Enumeration (CPE) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4824](http://www.nessus.org/plugins/index.php?view=single&id=48243)3 | | | | PHP Version Detection | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5084](http://www.nessus.org/plugins/index.php?view=single&id=50845)5 | | | | OpenSSL Detection | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5351](http://www.nessus.org/plugins/index.php?view=single&id=53513)3 | | | | Link-Local Multicast Name Resolution (LLMNR) Detection | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5461](http://www.nessus.org/plugins/index.php?view=single&id=54615)5 | | | | Device Type | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5698](http://www.nessus.org/plugins/index.php?view=single&id=56984)4 | | | | SSL / TLS Versions Supported | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5704](http://www.nessus.org/plugins/index.php?view=single&id=57041)1 | | | | SSL Perfect Forward Secrecy Cipher Suites Supported | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5732](http://www.nessus.org/plugins/index.php?view=single&id=57323)3 | | | | OpenSSL Version Detection | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [6633](http://www.nessus.org/plugins/index.php?view=single&id=66334)4 | | | | Patch Report | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [7054](http://www.nessus.org/plugins/index.php?view=single&id=70544)4 | | | | SSL Cipher Block Chaining Cipher Suites Supported | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [8450](http://www.nessus.org/plugins/index.php?view=single&id=84502)2 | | | | HSTS Missing From HTTPS Server | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [8482](http://www.nessus.org/plugins/index.php?view=single&id=84821)1 | | | | TLS ALPN Supported Protocol Enumeration | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [9698](http://www.nessus.org/plugins/index.php?view=single&id=96982)2 | | | | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [10087](http://www.nessus.org/plugins/index.php?view=single&id=100871)1 | | | | Microsoft Windows SMB Versions Supported (remote check) | | | | | accepted | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [10474](http://www.nessus.org/plugins/index.php?view=single&id=104743)3 | | | | TLS Version 1.0 Protocol Detection | | | | | accepted | |  | |  | |  | |  | |  | |  | |

**Αντιμετώπιση Αδυναμιών του OWASP-ZAP:**

* X-frame-Options Header Not Set:
  + Πήγαμε στο path: C:\xampp\apache\conf\httpd.conf.
  + Επεξεργαστήκαμε το αρχείο και προσθέσαμε την εντολή “ Header always append X-Frame-Options SAMEORIGIN ” .

**-Για προστασία από click jacking attacks.**

* Private IP Disclosure:
  + Πήγαμε στο path: C:\xampp\apache\conf\httpd.conf.
  + Επεξεργαστήκαμε το αρχείο και προσθέσαμε την εντολή “UseCanonicalName Off ”
* X-Content-Type-Options Header Missing:
  + Πήγαμε στο path: C:\xampp\apache\conf\httpd.conf
  + Επεξεργαστήκαμε το αρχείο και προσθέσαμε την εντολή “ Header set X-Content-Type-Options nosniff”.

**Aδυναμίες OWASP-ZPA μετά την αντιμετώπιση**

|  |  |  |  |
| --- | --- | --- | --- |
| Εύρημα | Κρισιμότητα | Κατάσταση | Περιγραφή |
| X-frame-Options Header Not Set | Μέτριο | Αντιμετωπίστηκε | X-frame-Options Header δεν περιέχεται στην HTTP-response για την προφύλαξη ενάντια σε ‘clickjacking’επιθέσεις |
| Private IP Disclosure | Χαμηλό | Αντιμετωπίστηκε | Μια Private IP (όπως 10.x.x.x, 172.x.x.x, 192.168.x.x) ή ιδιωτικό όνομα κεντρικού υπολογιστή (για παράδειγμα, ip-10-0-56-78) του Amazon EC2 βρέθηκε στην HTTP-Response. Αυτές οι πληροφορίες ενδέχεται να είναι χρήσιμες για περαιτέρω επιθέσεις με στόχο τα εσωτερικά συστήματα. |
| Web Browser XSS Protection Not Enabled | Χαμηλό | Αποδέχτηκε | Πλέον οι νέοι browser έχουν από μόνοι τους τρόπους αντιμετώπισης για αυτό το πρόβλημα. Οπότε το αποδεχτήκαμε με χαμηλή Κρισιμότητα |
| X-Content-Type-Options Header Missing | Χαμηλό | Αντιμετωπίστηκε | To Anti-MIME-Sniffing header X-Content-Type-Options δεν έχει οριστεί σε 'nosniff'. Αυτό επιτρέπει στις παλαιότερες εκδόσεις του Internet Explorer και του Chrome να εκτελούν παρεμβολές MIME-sniffing στο response body, ενδεχομένως προκαλώντας την ερμηνεία και εμφάνιση του response body ως τύπο περιεχομένου διαφορετικό από τον δηλωμένο τύπο περιεχομένου. Οι τρέχουσες (αρχές του 2014) και οι παλαιότερες εκδόσεις του Firefox θα χρησιμοποιούν τον δηλωμένο τύπο περιεχομένου (εάν έχει οριστεί), αντί να εκτελούν MIME-sniffing. |

**Recaptcha / Bruteforce protection:**

**(Αν δεν δουλεύει το recaptcha όταν ανοίγεται τη σελίδα,δοκιμάστε να μπείτε γράφοντας "127.0.0.1/...." και όχι με "localhost/....". Διότι δεν το αναγνωρίζει ως συμβατό Domain την ονομασία "Localhost")**

* Μπήκε “recaptcha” στις σελίδες *Login/Register/ForgetMyPassword* ώστε να μην είναι δυνατή η χρήση bot. Αποφεύγοντας έτσι bruteforce επιθέσεις που μπορεί να οδηγήσουν σε DOS.
* Στο αρχείο ***phpIndex.php*** έχει γραφεί κατάλληλος κώδικας, ώστε αν ένα συγκεκριμένο username κάνει 3 φορές λάθος τον κωδικό του, τρώει ban για 10 λεπτά.
* Όταν περάσουν αυτά, μπορεί να ξαναδοκιμάσει άλλες 3 προσπάθειες…. Κλπ

**Forced HTTPS Access:**

Δημιουργήσαμε ένα αρχείο με ονομασία κ κατάληξη «forceHttps.htaccess» το οποίο αυτόματα κάνει redirect se https url, ακόμη και αν δε το βάλει ο user ή αν δοκιμάσει να το σβήσει.

***Περιέχει τον κώδικα:***

RewriteEngine On

RewriteCond %{HTTPS} off

RewriteRule ^(.\*)$ https:///%%7BHTTP\_HOST%7D%%7BREQUEST\_URI%7D [L,R=301]

**Forget My Password / Change My Password:**

1. Πήγαμε στον xampp directory 🡪 php 🡪 php.ini
2. Έπειτα το τροποποιήσαμε προσθέτοντας αυτό το command “sendmail\_path = "\"C:\xampp\sendmail\sendmail.exe\" -t" ”
3. Στην συνέχεια πήγαμε στον φάκελο sendmail 🡪 sendmail.ini και
4. Αντικαταστήσαμε τις παρακάτω εντολές με τις αντίστοιχες δικές μας
5. smtp\_server=smtp.gmail.com
6. smtp\_port=465
7. smtp\_ssl=auto
8. error\_logfile=error.log
9. auth\_username=our-gmail@gmail.com
10. auth\_password=\*\*\*\*\*\*
11. Τέλος φτιάξαμε ένα forgotPassword.php και resetPassword

* resetPassword.php
* forgotPassword.php
* changePassword.php
* changePasswordAdmin.php

**Password Policy:**

* Ορίσαμε ελάχιστο μήκος κωδικού 10 χαρακτήρες, οι οποίοι πρέπει να περιέχουν τουλάχιστον ένα κεφαλαίο και ένα μικρό χαρακτήρα και έναν αριθμό.
* **Μέτρο Ασφάλειας:** Με την εντολή real\_escape\_string αποφεύγουμε τους ειδικούς χαρακτήρες από username password κλπ, μετατρέποντάς τους σε string. Για να αποφύγουμε ανεπιθύμητες ενέργειες στην βάση δεδομένων.

**Backups και φορητές συσκευές:**

* Απαιτείται εβδομαδιαίο backup σε όλα τα κρίσιμα αρχεία, που έχει ανατεθεί σε συγκεκριμένα άτομα.
* Οι φορητές συσκευές που μεταφέρονται κ εκτός του χώρου εργασίας απαιτούνται να είναι κρυπτογραφημένες και να μην χρησιμοποιούνται σε ξένα συστήματα, εκτός των φορητών υπολογιστών(Laptops) της εταιρίας.
* Απαγορεύεται η χρήση εταιρικών συσκευών στο σπίτι από τρίτους, καθώς και για χρήση surfing σε επικίνδυνες ιστοσελίδες, gaming κλπ.