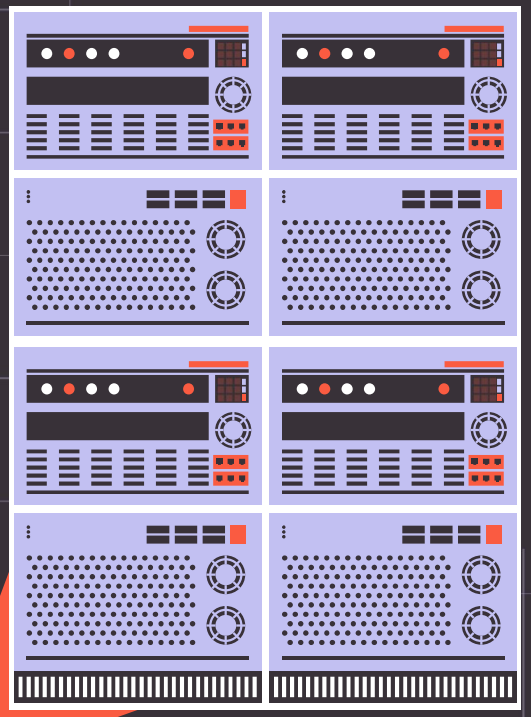
Ministerul Educației și Cercetării al Republicii Moldova
IP Colegiul "Iulia Hasdeu" din Cahul

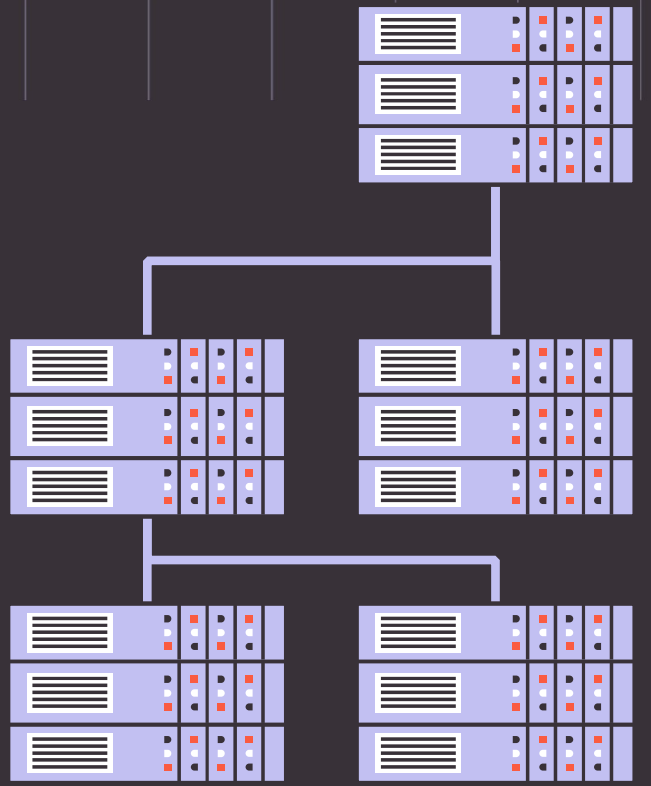
WEB HOSTING



Modele de securitate a WEB-serverelor

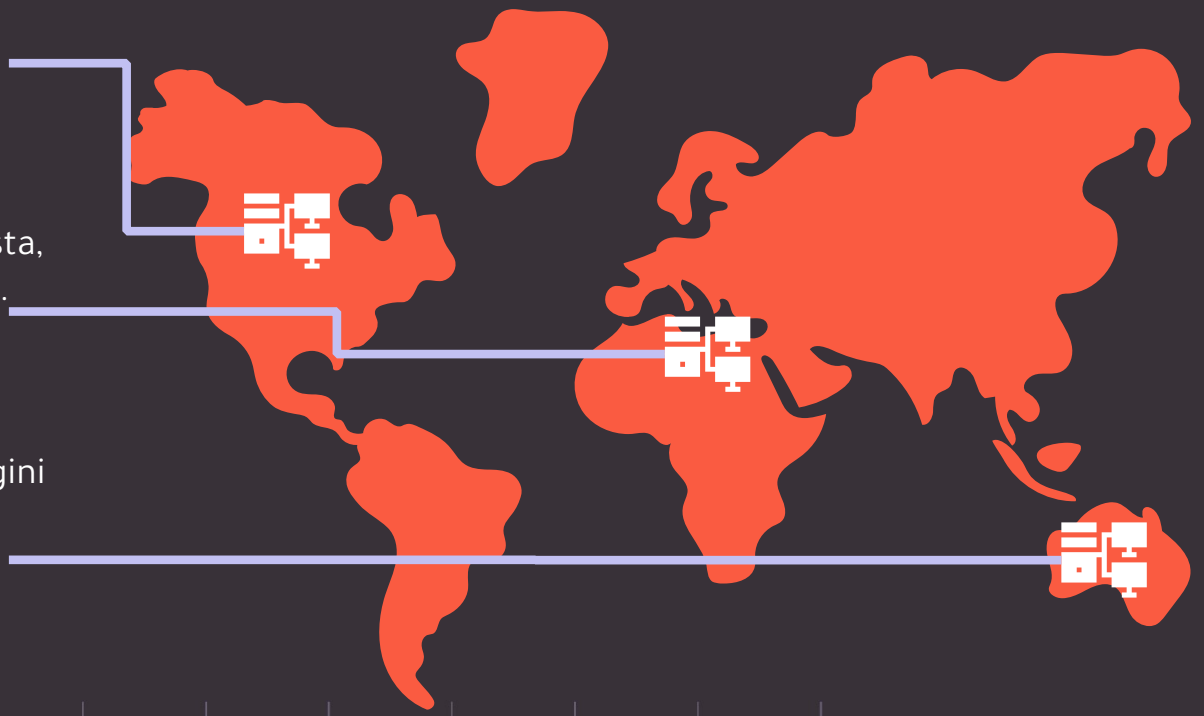
Studiu Individual nr. 3
Administrarea web-serverelor

Cuprins



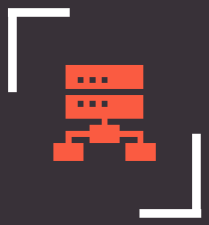
Server WEB

Un server web este un computer care stochează un site web și îl livrează dispozitivelor care solicită accesul la acesta, cum ar fi telefoane, tablete și computere. Găzduiește fișierele și folderele care alcătuiesc site-ul web, rulează software specializat pentru a gestiona solicitările utilizatorilor și livrează conținut web (pagini web, imagini, fișiere) prin internet.



Definiția și importanța securității web-serverelor

Securitatea web-serverelor se referă la ansamblul de măsuri și practici implementate pentru a proteja serverele web de amenințări cibernetice și atacuri malițioase. Este esențială pentru a menține integritatea, confidențialitatea și disponibilitatea datelor și a infrastructurii web.



Importanța securității web-serverelor

- Securitatea adecvată este esențială pentru a preveni furtul, coruperea sau pierderea datelor sensibile.
- Atacurile cibernetice pot deteriora sau dezactiva site-urile web, afectând negativ reputația și imaginea unei organizații.
- Multe organizații sunt obligate prin lege să respecte anumite reglementări privind securitatea datelor.

AMENINTĂRI

LA ADRESA SERVERELOR WEB

Principalele amenințări la adresa web serverelor

01

Injecții SQL

permit atacatorilor să modifice sau să extragă date din bazele de date asociate serverelor web.

02

Cross-Site Scripting (XSS)

Injectarea codului maliţios într-o pagină web, care rulează apoi în browserul utilizatorului, putând fura date sau prelua controlul asupra sesiunii.

03

Cross-Site Request Forgery

Păcălirea utilizatorului autentificat pe un site web să execute o acţiune nedorită pe acel site, în beneficiul atacatorului.

04

Directory Traversal

Exploatarea vulnerabilităţilor pentru a accesa fişiere sau foldere care nu ar trebui să fie accesibile, putând dezvălui informaţii confidenţiale.

05

Denial of service (DoS) Distributed Denial of services

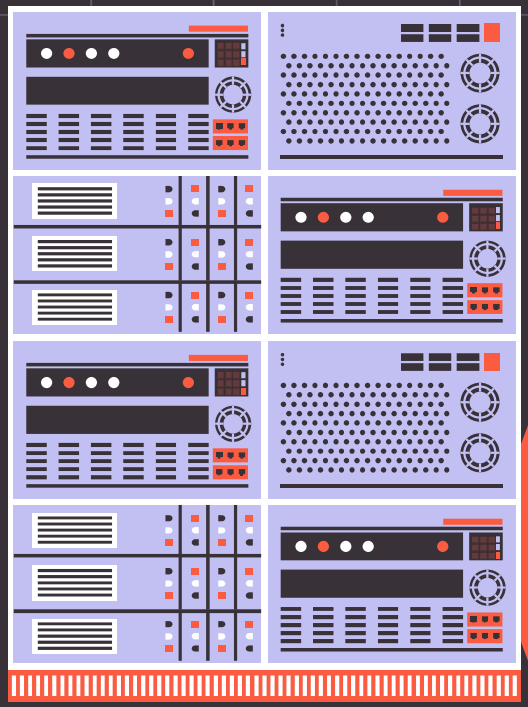
Inundarea serverului web cu trafic inutil pentru a-l suprasolicita şi a-l face inaccesibil utilizatorilor legitimi. (DoS - dintr-o singură sursă, DDoS - din mai multe surse compromise).

Metode de securitate

Configurarea corectă a serverului

Menţinerea serverului web actualizat cu cea mai recentă versiune a software-ului este esenţială pentru a elimina vulnerabilităţile cunoscute.

Instalarea promptă a patch-urilor de securitate lansate de producătorul software-ului este crucială pentru a remedia vulnerabilităţile recent descoperite.



Setări de securitate recomandate

Server web

- Dezactivarea funcţiilor şi a modulelor neutilizate.
- Limitarea accesului la server prin configurarea firewall-ului.
- Utilizarea parolelor puternice, autentificarea cu doi factori.
- Activarea HTTPS pentru a cripta traficul web.

Servicii

- Configurarea securizată a bazei de date, cu parole puternice şi acces limitat.
- Utilizarea unui framework web securizat pentru a evita vulnerabilităţile comune.

Implementarea de certificate SSL/TLS

Certificatele SSL/TLS utilizează **algoritmi de criptare** pentru a transforma datele transmise între serverul web şi browserul utilizatorului într-un format codificat. Acest lucru le face ilizibile pentru interceptează, sporind confidenţialitatea şi integritatea datelor.

Beneficiile implementării certificatelor SSL/TLS

Confidențialitate: Protejează datele sensibile de interceptare şi furt.
Integritate: Asigură că datele nu sunt modificate în timpul transmiterii.
Autenticitate: Permite verificarea identităţii serverului web şi a clientului.

Soluții de firewall și filtrare a traficului

Firewall-uri de aplicație web (WAF):

Un WAF este un firewall specializat care protejează site-urile web de atacuri la nivelul aplicației. WAF-urile analizează traficul web și blochează solicitările care par malițioase, cum ar fi atacurile XSS, SQL injection sau CSRF.

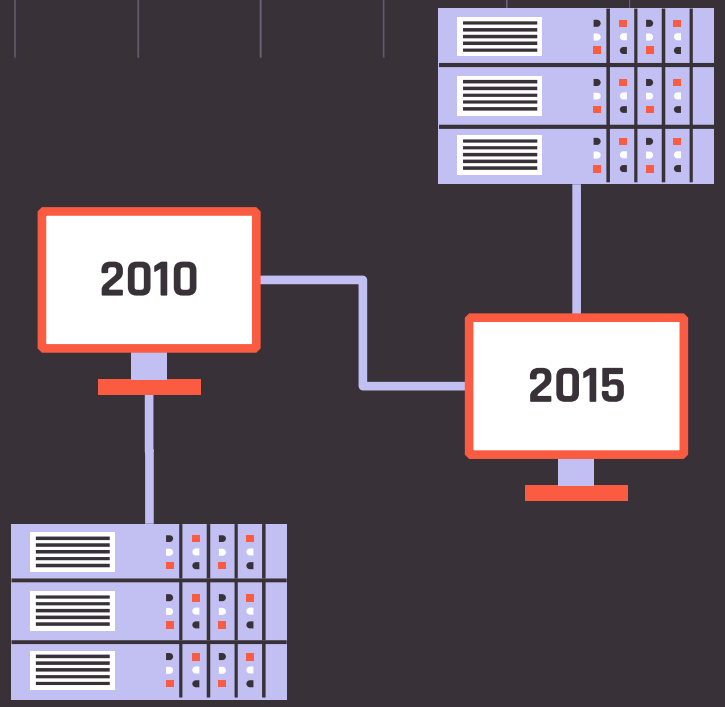
Beneficiile utilizării unui WAF:

- Protejează împotriva atacurilor comune la nivelul aplicației web.
- Poate fi configurat pentru a bloca traficul din anumite surse IP.
- Poate fi configurat pentru a bloca anumite tipuri de solicitări HTTP. Poate fi integrat cu alte soluții de securitate.

Filtrarea traficului pe baza IP-urilor sau a protocoalelor

Filtrarea traficului poate fi utilizată pentru a bloca accesul la serverul web din anumite adrese IP sau pentru a bloca anumite protocoale. De exemplu, se poate bloca accesul din țări cunoscute pentru a fi surse de atacuri cibernetice.

Beneficiile filtrării traficului:
Poate reduce riscul de atacuri din anumite surse.
Poate reduce lățimea de bandă utilizată de traficul nedorit.
Poate îmbunătăți performanța serverului web.



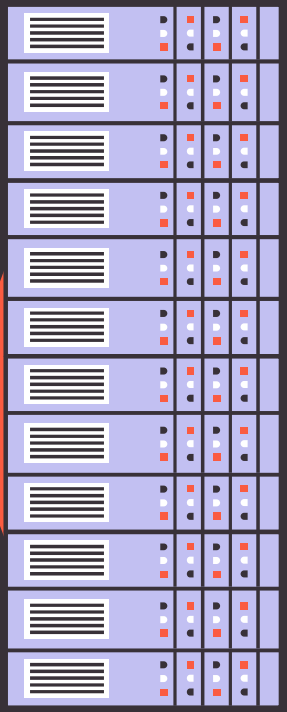
Autentificare și autorizare robustă

2FA adaugă un strat suplimentar de securitate la procesul de autentificare, solicitând utilizatorilor să furnizeze două informaţii de identificare separate. O a doua informaţie de identificare poate fi un cod trimis prin SMS, o amprentă digitală sau o cheie de securitate .

RBAC este un sistem de control al accesului care permite definirea de roluri cu anumite permisiuni. Utilizatorilor li se pot atribui roluri specifice, permiţându-le să acceseze doar resursele la care au nevoie.

Beneficiile utilizării RBAC:

Permite un control granular al accesului la resursele serverului web.
Reduce riscul de acces neautorizat la date sensibile.
Simplifică administrarea utilizatorilor şi a permisiunilor.



1. **Validarea datelor la nivel de aplicație**

   Validarea datelor la nivel de aplicație se referă la verificarea datelor introduse de utilizatori pentru a se asigura că sunt corecte și complete. Această validare poate fi implementată în codul aplicației web.

2. **Filtrarea datelor la nivelul serverului**

   Filtrarea datelor la nivelul serverului se referă la blocarea solicitărilor care conțin date suspecte. Această filtrare poate fi implementată la nivelul firewall-ului web sau a altor soluții de securitate.

concluzie

Securitatea web-serverelor este esențială pentru a proteja datele sensibile și pentru a menține funcționarea corectă a site-urilor web. Modelele de securitate oferă o abordare sistematică pentru a gestiona riscurile și a implementa măsuri de protecție adecvate.

A realizat: Apareci Aurica
Grupa: AAW 2042