TPE: Web Application Firewall

Emilio Tylson 54022
Lucas Kania 54257
Diego Vazquez 54377
Federico Bond 52247
Agustin Mounier 54037

Web Application Firewall

- Controla el acceso , entradas y salidas de un servicio o aplicación.
- Controla y monitorea el tráfico a en la capa de aplicación principalmente.
- Previene ataques en la capa de aplicación como cross-site scripting (XSS) o SQL injection.

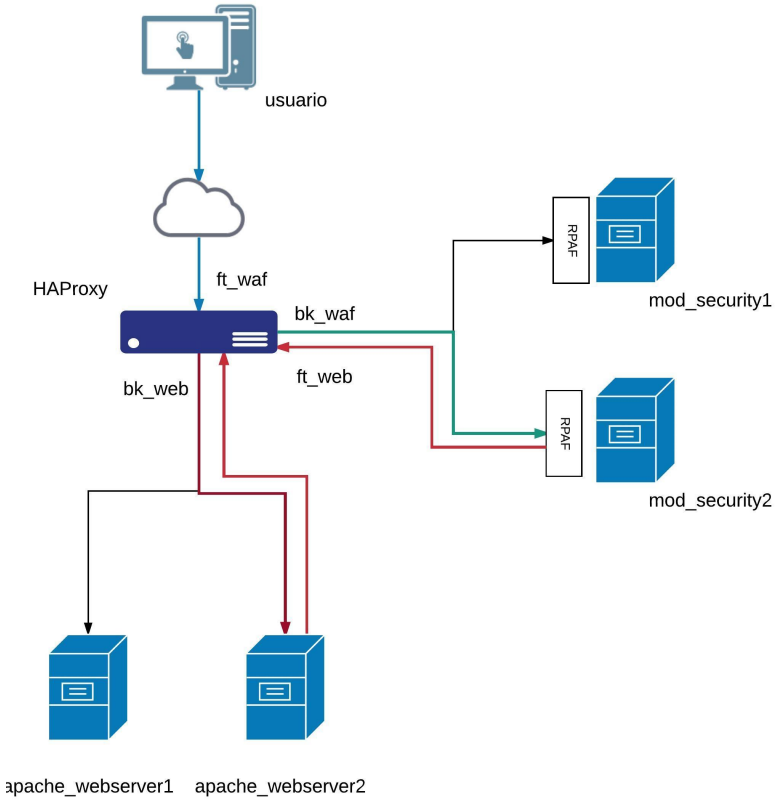
HAProxy (High Availability Proxy)

- Es un load balancer open source, que permite balancear las conexiones TCP hacia los servidores, ofrece high availability y hacer de proxy de aplicaciones basadas en HTTP.
- Funcionalidades principales:
  - HTTP keep alive
  - Stick-tables : contadores para controlar la actividad de entrada.
  - Sticky- session
  - Balanceo escalable de carga, con health checks

ModSecurity

- Es un toolkit open source que monitorea el tráfico web a aplicaciones o servicios.
- Trabaja como módulo de Apache server.
- Intercepta y analiza el tráfico HTTP, en función de reglas.
- Ofrece un lenguaje propio para definir reglas.
- OWASP ofrece un set de reglas para prevenir ataques más frecuentes.

Implementación



Ataques

Diagrama conceptual de la demostración

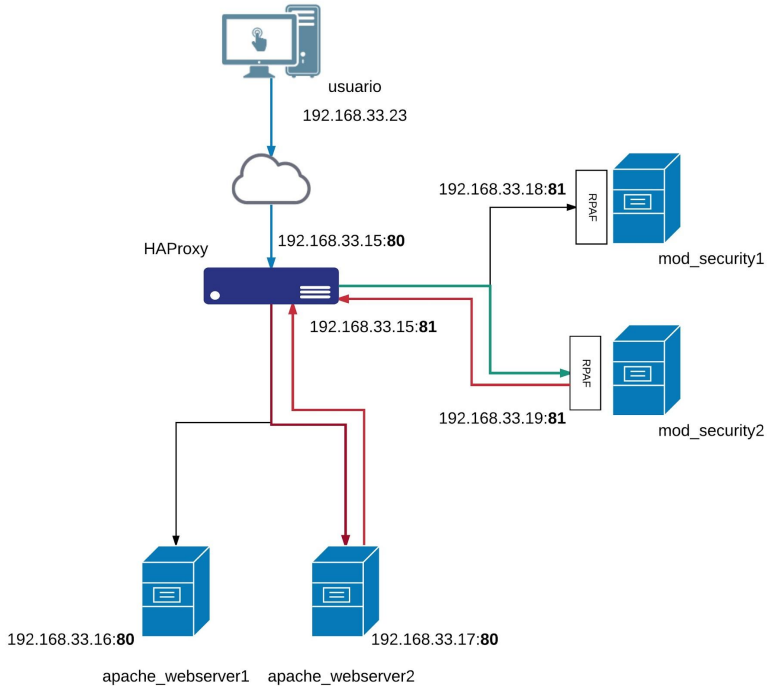
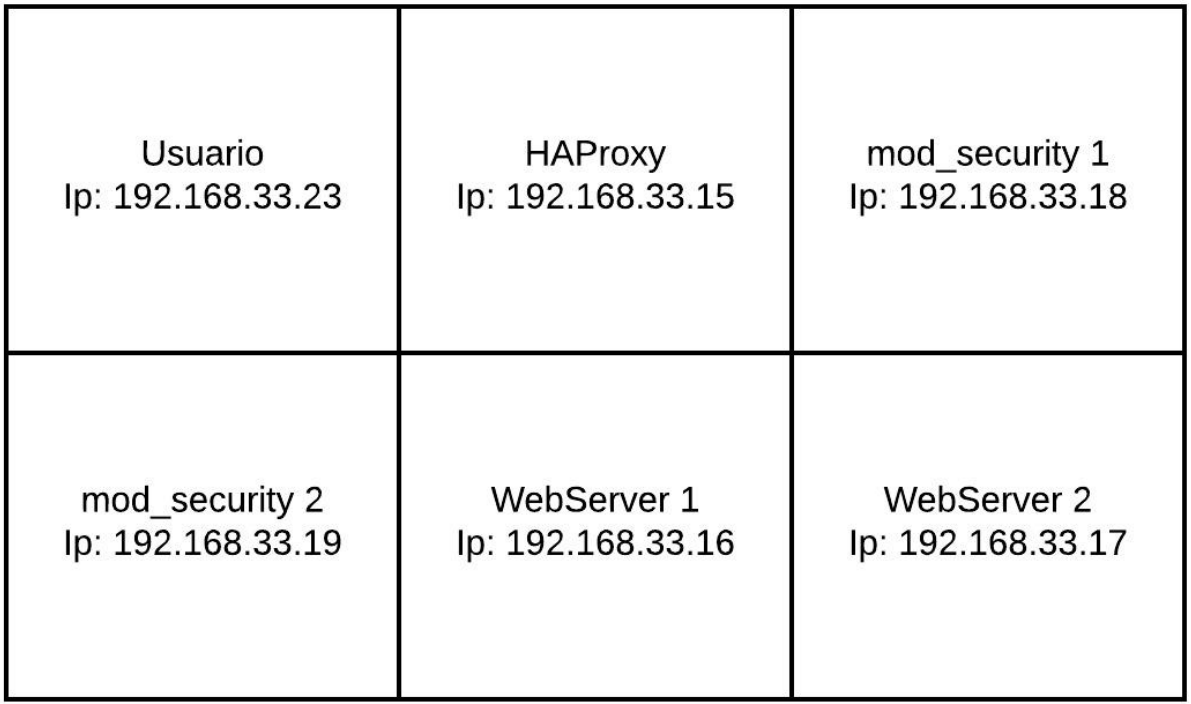


Diagrama conceptual de la terminal



SQL Injection

- Consiste en inyectar un comando SQL en un sitio mediante un campo de input en la aplicación cliente.

```php
<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$username' AND password='$password'");
        if(mysqli_num_rows($result) == 0)
            echo 'Invalid username or password';
        else
            echo '<h1>Logged in</h1><p>A Secret for you....</p>';
    }
    else
    {
?>
```

‘ or true --

Cross-site scripting (XSS)

- Consiste en inyectar código que se ejecute en el cliente de la víctima cuando éstos ingresan a un sitio.
- Su nombre proviene de un ataque realizado ingresando un <iframe>.
- Dos tipos:
  - Persistentes.
  - Reflejados.

Deny of Service

- Es un ataque que consiste en volver inaccesible un recurso o servicio de un servidor o red.
- Se genera mediante la saturación de los puertos con flujo de información basura.
- Una ampliación del ataque DoS es DDoS (Distributed Denial of Service)