

INFO-6076

Web Security

*Web Application
Penetration Testing*



Agenda

- Web Application Penetration Testing
 - Web Application Firewall
 - Load Balancing
 - Reverse Proxies
- Web App Pen Test Tools
- Lab 09 overview

Web Application Penetration Testing

Web App Penetration Testing

- Web Application Firewalls (WAF) can be used to thwart attacks against Web Apps
- These work differently than Intrusion Prevention Systems and regular network firewalls in the sense that they focus on common attacks such as Cross-site Scripting, Injection, etc.
- Normally based on the OWASP list of known attacks

Web App Penetration Testing

Examples of commercial Web application Firewalls:

- Barracuda Networks
- CloudFlare
- Pulse Secure
- Signal Sciences

Web App Penetration Testing

- A Web application Firewall (WAF) may be in place for the site you are testing
- **wafw00f** is the command to use in Kali Linux to test if one is in place
- Examples:
wafw00f transpirenetworks.com
wafw00f fanshawec.ca

Web App Penetration Testing

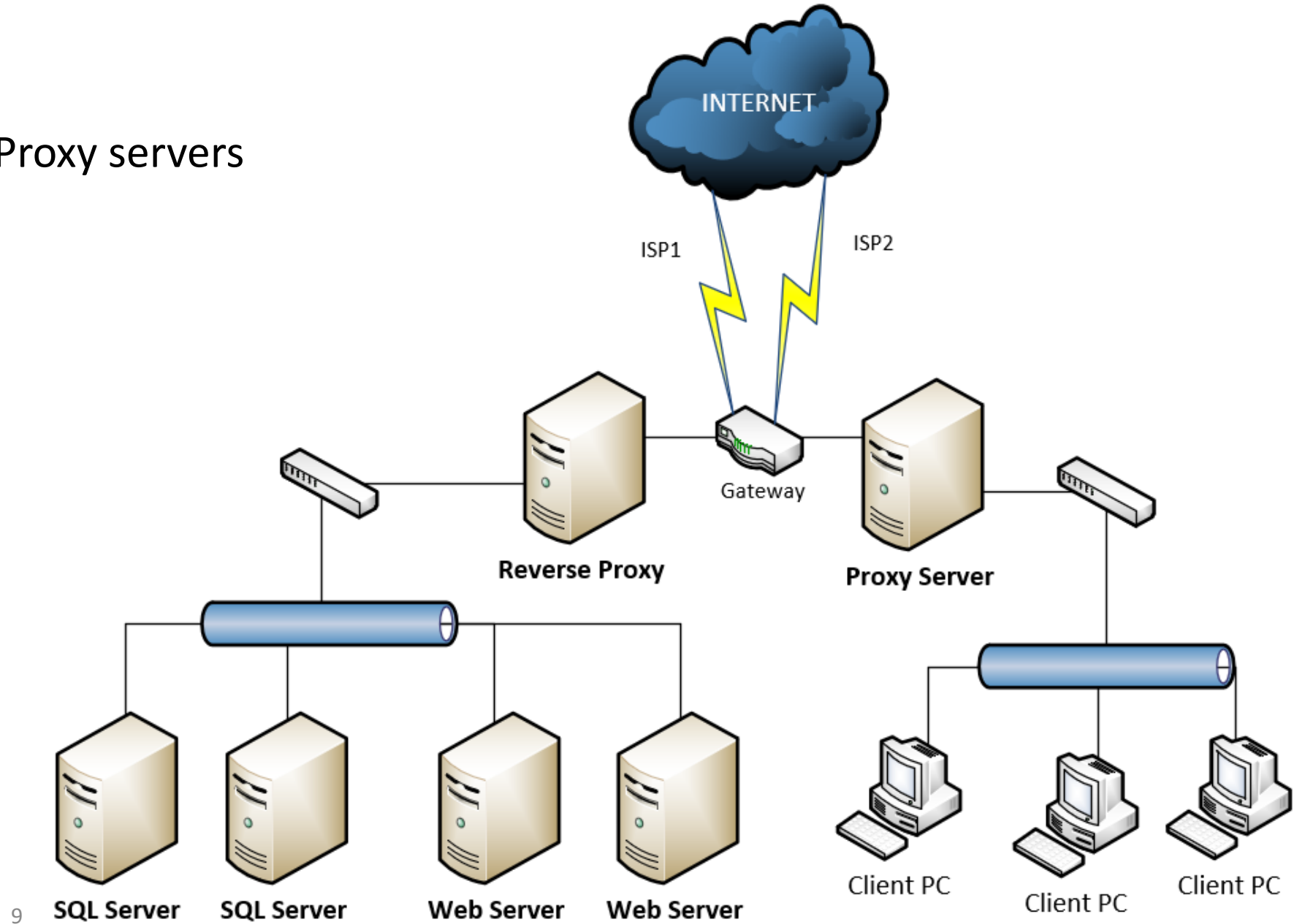
- Load Balancing Detector (**lbd**) can be used to check if DNS or HTTP load balancing is being used by a web server
- The purpose of load balancers is to accept incoming traffic and distribute it across numerous servers to prevent one server from being overloaded and denying service to clients

Web App Penetration Testing

Reverse Proxy

- Reverse Proxies analyze incoming traffic and distribute it to the appropriate internal web server
- Clients will only see the one public IP address but may be retrieving requested resources from multiple web servers

Proxy servers



Web App Penetration Testing

Reverse Proxy

- These can be used in combination with WAFs to enhance Web App security
- Can also provide:
 - A/B Testing
 - Load Balancing
 - TLS Encryption
 - Content caching

Web App Penetration Testing

Reverse Proxy

- Can provide TLS termination (SSL termination)
- Takes incoming TLS traffic and decrypts it before sending it forward on the internal network
- Assumes that the LAN is secure

- Gmail anyone?

<https://www.cbc.ca/news/technology/google-email-encryption-will-hinder-nsa-spying-1.2580881>

Web App Penetration Testing

Black-Box vs. White-Box Testing

- Black-Box testing is done from the outside with no prior knowledge of the technologies used by the web application
- It can be more effective than White-Box testing because automated tools can quickly execute numerous tests

Web App Penetration Testing

Black-Box vs. White-Box Testing

- White-Box testing allows the review of the source code for an application by a tester
- Certain vulnerabilities can be found faster using the code review method

Web App Penetration Testing

Black-Box vs. White-Box Testing

- Ideally a web app pen test would include both methods
- Strange behaviour in a running application can be looked at in the source code
- Automated testing can test the application much faster than manual code review
- Look for a balance between the two methods

Cloud Providers

ASPs

Organizations today host web services using external providers ranging from simple hosting, to full fledged **Application Service Providers (ASPs)**

- Cloud providers will support multiple customer applications on the same infrastructure
- Often victims of defacing when a single shared host is compromised

Shared Hosting

With the introduction of the HOST header in HTTP version 1.1, a web server can be configured to host more than one web application

- Multiple domains can resolve to one public IP

Example Apache Configuration:

```
<VirtualHost *>  
    ServerName info6076.com  
    DocumentRoot /www/first  
</VirtualHost>
```

```
<VirtualHost *>  
    ServerName artmack.com  
    DocumentRoot /www/second  
</VirtualHost>
```

ASPs

Customers who use external providers for web applications will need to interact with the service

- Upload capabilities such as FTP or SCP
- Direct access to ASP infrastructure
 - VPN
 - Database Setup
 - SSH

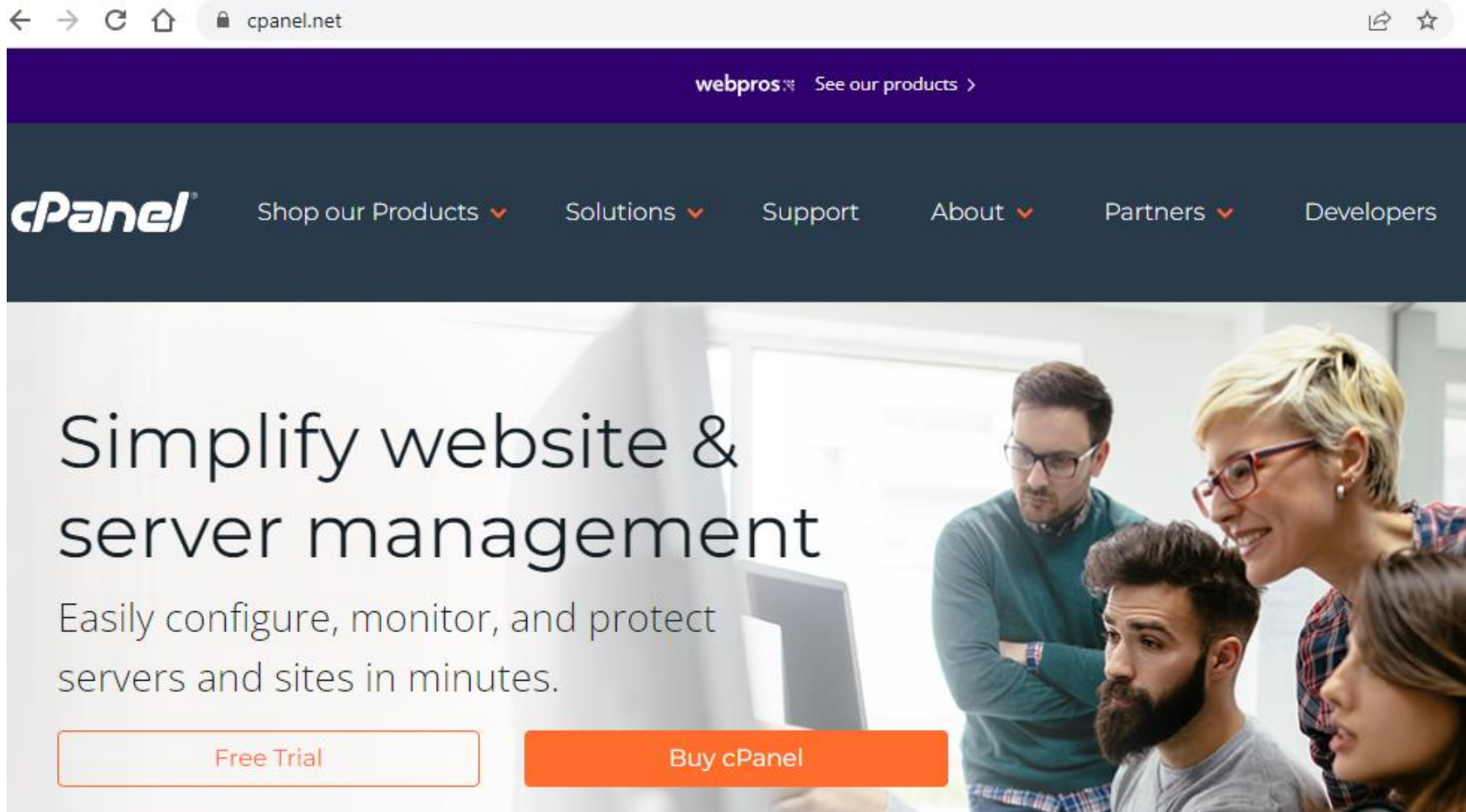
Hosting Control Panels

There are a number of hosting panels available on the market with Cpanel and Plesk being the most popular

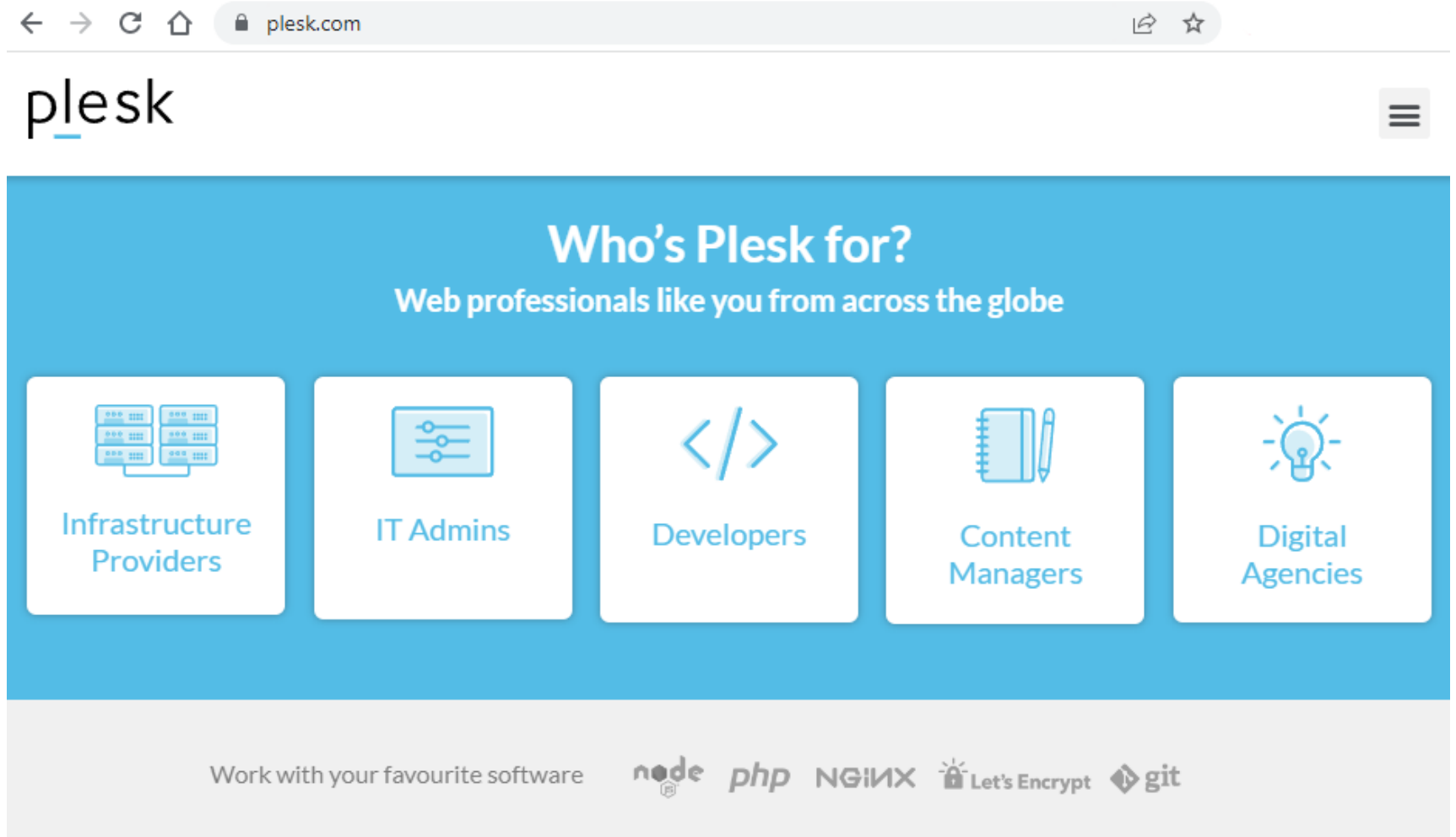
Others include:

- DirectAdmin
- Spanel
- Webmin
- Froxlor

Platform example: CPanel



Platform example: Plesk



The screenshot shows the Plesk website homepage. At the top, there is a navigation bar with the Plesk logo on the left and a hamburger menu icon on the right. Below the navigation bar, the main heading reads "Who's Plesk for?" followed by the subtitle "Web professionals like you from across the globe". Below this, there are five white boxes, each containing an icon and a label: "Infrastructure Providers" (server rack icon), "IT Admins" (control panel icon), "Developers" (code editor icon), "Content Managers" (notebook and pen icon), and "Digital Agencies" (lightbulb icon). At the bottom, there is a footer section with the text "Work with your favourite software" followed by logos for node, php, NGINX, Let's Encrypt, and git.

← → ↻ 🏠 🔒 plesk.com

plesk

Who's Plesk for?

Web professionals like you from across the globe

- Infrastructure Providers
- IT Admins
- Developers
- Content Managers
- Digital Agencies

Work with your favourite software

node php NGINX Let's Encrypt git

Security Concerns with ASPs

Any direct access to the service providers infrastructure needs to be secured

- FTP may be sent in plain text
- Database connections using ODBC can be unencrypted
- Remote access between customers may not be properly segregated

Backdoor Scripts

Not all customers are created equal

- Deliberate backdoors
- Shell scripts

What security level are these shells running in?

Examples:

<https://github.com/bartblaze/PHP-backdoors>

<https://github.com/mattiasgeniar/php-exploit-scripts/>

Malicious users

A PHP script implanted by a customer on a shared web server could allow access to shell commands through a browser

- These may run as a privileged user (www-data)

A vulnerable application could allow the compromise of shared applications through:

- SQL injection flaws
- Path traversal vulnerabilities
- Command injection flaws

Recent Attack Example

GoDaddy

- Approximately 21 million customers
- Hackers had access for several years
- Malware distribution
- Credential harvesting
- Redirection

→ ↺ 🏠 arstechnica.com/information-technology/2023/02/godaddy-says-a-multi-year-breach-hijacked-customer-websites-and-accounts/

HACKED —

GoDaddy says a multi-year breach hijacked customer websites and accounts

Three breaches over as many years all carried out by the same threat actor.

DAN GOODIN - 2/17/2023, 5:43 PM

0365 Attacks

Office 365

- Credential harvesting through phishing

[bloomberg.com/press-releases/2021-05-11/an-alarming-85-of-organizations-using-microsoft-365-have-suffered-email-data-breaches-research-by-egress-reveals](https://www.bloomberg.com/press-releases/2021-05-11/an-alarming-85-of-organizations-using-microsoft-365-have-suffered-email-data-breaches-research-by-egress-reveals)

Bloomberg the Company & Its Products | Bloomberg Terminal Demo Request | [Bloomberg Anywhere Remote Login](#) | [Bloomberg Customer Support](#)

Bloomberg

[Sign In](#)

• [Live Now](#) • [Markets](#) • [Economics](#) • [Industries](#) • [Technology](#) • [Politics](#) • [Wealth](#) • [Pursuits](#) • [Opinion](#) • [Businessweek](#) • [Equality](#) • [Green](#) • [CityLab](#)

Business

An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches, Research by Egress Reveals

May 11, 2021 at 7:00 AM EDT

Share this article



[Gift this article](#)

An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches, Research by Egress Reveals

Research reveals organizations using Microsoft 365 experience more breaches, with more severe impacts

Securing Shared Access

Secure customer access

- Encrypt all remote access
- Grant privileges on a least-privilege basis

Segregate customer functionality

- Read/Write access to file paths
- Reduced access to system functions

Segregate components

- Stored procedures, etc.
- Database servers

Web App Pen Test Tools

Web App Pen Test Tools

Web Crawlers

- These can be used to find login portals, configuration files, backup or OLD copies of pages, administrative notes, etc.

Examples of Crawlers:

- Dirbuster
- Vega
- OWASP-ZAP
- Burp Suite
- Webscarab
- Webslayer

Web App Pen Test Tools

Zed Attack Proxy (ZAP)

- Developed by OWASP
- Automated Scanning
- Proxy
- Spidering
- Testing REST-based functions
- Testing Authentication

Arachni

- Free, open source
- Built in Ruby
- REST-based API

<https://www.arachni-scanner.com/>



Web App Pen Test Tools

Wapiti

Open source

- XSS Injection
- Leftover backup or old files
- SQL Injection
- Misconfigured .htaccess files

Invicti

Netsparker

- Dynamic testing
- HIPPA, PCI, OWASP

<https://www.invicti.com/>

Invicti 

Web App Pen Test Tools

Vega

- Open source
- Written in JAVA
 - XSS Injection
 - File Inclusions
 - SQL Injection
 - TLS

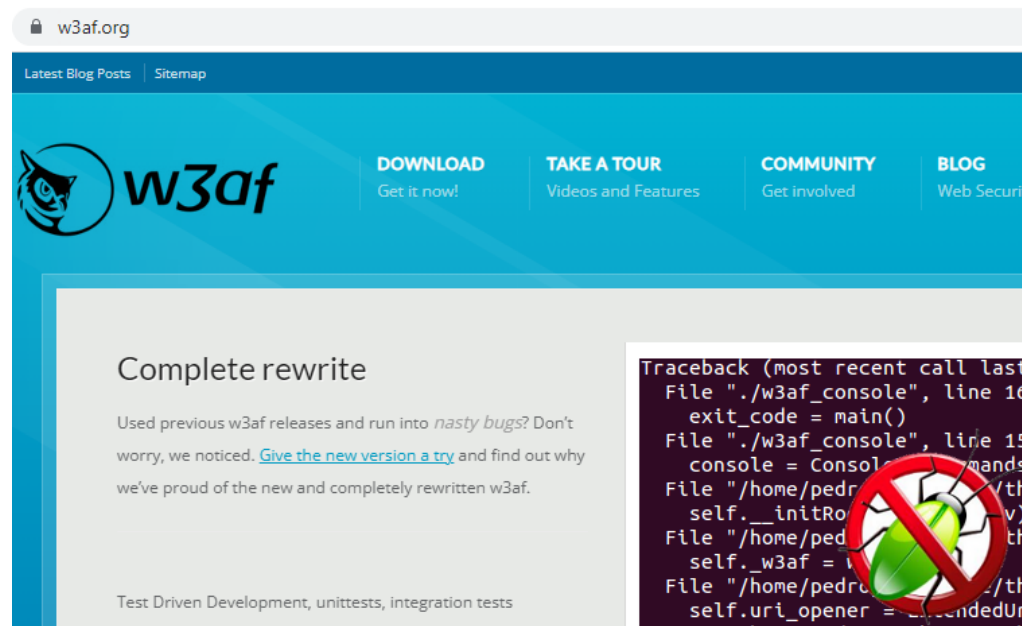


<https://subgraph.com/vega/>

Web App Pen Test Tools

W3af

- Open source
- Written in Python
- Tests for:
 - Buffer overflows
 - SQL Injection
 - CSRF
 - Etc.



<https://w3af.org/>

Web App Pen Test Tools

Skipfish

- Open source
- Written in C
- Provides efficient site mapping with recursive crawling
- Meant to be non-disruptive



<https://github.com/spinkham/skipfish>

<https://www.kali.org/tools/skipfish/>

Web App Pen Test Tools

SQLmap

- Developed by Bernardo Damele and Miroslav Stampar



Web App Pen Test Tools

SQLmap

- Supports automated testing of numerous database management systems
- Ability to crack hashed data such as passwords
- Can be used to upload and download files from the server's filesystem

<https://sqlmap.org/>

Web App Pen Test Tools

Wfuzz

- Developed to brute force web apps
- Checks different injections using the GET and POST methods
- Support for encoding
- Uses payloads
- Available by default in Kali Linux

Web App Pen Test Tools

Grabber

- Written in Python

Tests for:

- SQL Injection
- XSS
- File insertion
- Sessions
- Etc.

Lab Details

LAB-09: Overview

Lab-09: Web App Pen Test Tools

- Change the User-Agent HTTP Header in Firefox
- Skipfish
- Golismero
- Nikto
- Mirror websites with HTTrack
- **Challenge:** Command injection with DVWA