Kde se oskenovat?

Hledání alternativy pro Nessus

Edvard Rejthar • edvard.rejthar@nic.cz • 24. 11. 2017

Skener Webu

- pro držitele domén
- metodika OWASP
- zdarma

Skener Webu – motivace

*"Varujete před návštěvou nebezpečných web stránek; **co se mi může stát**, vždyť prohlížeč na disk nic neuloží, a tudíž se mi počítač nemůže virem nakazit. Nebo ne???"*

Skener Webu – závěrečná zpráva

CZ.NIC | SPRÁVCE DOMÉNY CZ

Shmutí

Web umístěný na doméně xxxxxxxxxxxxx byl automaty zkoumán přibližně 6 hodin.

U domény chybí AAAA záznam v DNS serveru. Ačkoliv tato skutečnost bezpečnostní riziko nepředstavuje, do budoucnosti doporučujeme vytvořit podporu taky pro IPv6. To jisté platí u webového serveru.

Přehled

Každý nález je označený mírou rizika: informační, nízké, střední, vysoké, kritické. Jedná se o označení míry rizika testerem. Míra rizika se může lišit vzhledem k charakteru aplikace.

Testování se provádí podle OWASP (Open Web Application Security Project) Top 10. Jedná se o souhrn nejkritičtějších zranitelností, které se ve webové aplikaci mohou vyskytnout.

Testování se vykonává v následujících oblastech:

1 Injektování

Chyby umožňující napadení aplikace vložením kódu přes neošetřený vstup. Vkládáním kódu do neošetřeného vstupu útočník může spouštět příkazy s privilegovanými právy, k nimž by neměl mít přístup.

2 Chybná autentizace a správa sezení

Zranitelnosti umožňující napadení funkcí aplikace, které souvisí s autentizací a správou sezení s cílem převzít identitu jiného uživatele. Funkce, které se vztahují k ověřování a řízení relace často nejsou vytvořeny správně, což útočníkům umožňuje napadnout hesla, tokeny relací, kliče, session aj.

2.1 Autocomplete off

Riziko: informační

Aplikace umožňuje prohlížečům zapamatovat si zadávané přihlašovací údaje na URL http://xxxxxxxxxxxxxxxx/?node=63&uriString=prihlaseni-do-tridni-vyvesky

Doporučené řešení: Doporučujeme zvážit nastavení autocomplete=off. Zabrání se tak nechtěnému uložení uživatelského hesla do prohlížeče, pokud se uživatel přihlašuje z veřejného počítače.

2.2 Chybějí flag "HTTPOnly" (PHPSESSID)

Riziko: střední

U cookies chybí flag HTTPOnly, který snižuje riziko krádeže cookie. Takto chráněná cookie je následně dostupná pouze ze strany serveru. Z uživatelské strany není možné na ni přistoupit a

CZ.NIC | SPRÁVCE DOMÉNY CZ

8 Cross Site Request Forgery

Zranitelnosti umožňující napadení podvržením požadavku webové aplikace.

CSRF útočníkovi umožňuje prohlížeč oběti donutit k vykonání předem autentizovaného požadavku nezabezpečenou aplikací. Tak může útočník např. provést transfer, odeslat zprávu, smazat účet, přidat záznam; útočník může takto provést mnoho jiných operací.

9 Použití známých zranitelností komponent

Zranitelnosti umožňující napadení užitím známých zranitelností komponent.

9.1 Neaktuální verze Apache

Riziko: střední

Verze Apache/2.2.3, kterou na webu využíváte, má více bezpečnostních chyb. Chyby se odstraní updatem systému, proto je ve zprávě nebudeme uvádět.

Doporučené řešení: Doporučujeme updatovat na aktuální verzi.

10 Neošetřené přesměrování

Zranitelnosti umožňující napadení přesměrováním na jiné stránky. Takovým přesměrováním může útočník například dosáhnout nainstalování malware anebo odhalit uživatelské heslo a nebo jiné citlivé informace.

11 Ostatní nálezy

Nálezy, které jsme nezařadili do skupiny OWASP Top 10.

11.1 Otevřené porty

Riziko: Informační

Během testu byly zjištěny následující otevřené porty:

Možnosti penetračního testování

- Arachni, Nikto, OpenVAS, Owasp ZAP, Skipfish, Uniscan, Wapiti
- Acunetix, Appscan, Burp Pro, Nessus, Webinspect







Arachni

```
edvard@jezevec:/opt/arachni-1.5.1-0.5.12/bin$ ./arachni http://vstupnik.cz
Arachni - Web Application Security Scanner Framework v1.5.1
   Author: Tasos "Zapotek" Laskos <tasos.laskos@arachni-scanner.com>

           (With the support of the community and the Arachni Team.)

   Website:       http://arachni-scanner.com
   Documentation: http://arachni-scanner.com/wiki


 [~] No checks were specified, loading all.
 [~] No element audit options were specified, will audit links, forms, cookies, UI inputs, UI forms, JSONs and XMLs.

 [*] Initializing...
 [*] Preparing plugins...
 [*] ... done.
 [*] BrowserCluster: Initializing 6 browsers...
 [*] BrowserCluster: Spawned #1 with PID 10242 [lifeline at PID 10239].
 [*] BrowserCluster: Spawned #2 with PID 10269 [lifeline at PID 10266].
 [*] BrowserCluster: Spawned #3 with PID 10296 [lifeline at PID 10293].
 [*] BrowserCluster: Spawned #4 with PID 10323 [lifeline at PID 10320].
 [*] BrowserCluster: Spawned #5 with PID 10350 [lifeline at PID 10347].
 [*] BrowserCluster: Spawned #6 with PID 10377 [lifeline at PID 10374].
 [*] BrowserCluster: Initialization completed with 6 browsers in the pool.
 [~] Scheduled 301 redirection: http://vstupnik.cz/ => https://vstupnik.cz/

 [*] [HTTP: 301] http://vstupnik.cz/
 [~] Analysis resulted in 0 usable paths.
 [~] DOM depth: 0 (Limit: 5)
 [*] XST: Checking...
 [*] Allowed methods: Checking...
```

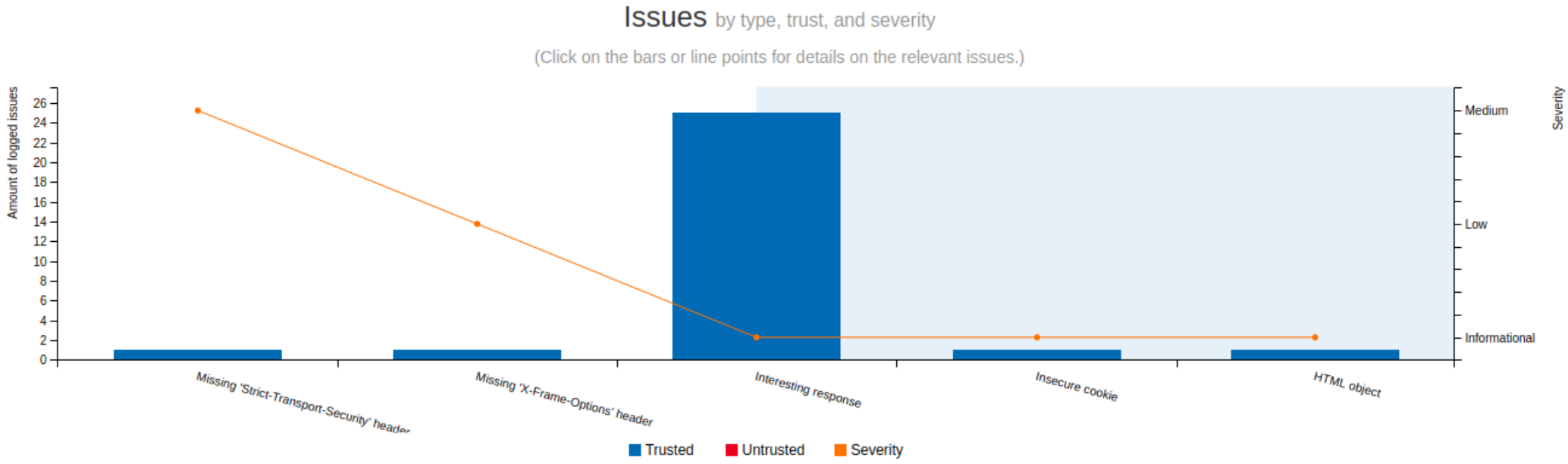
Arachni

```
[~] Audited 2 page snapshots.

[~] Duration: 00:01:19
[~] Processed 651/653 HTTP requests.
[~] -- 12.085 requests/second.
[~] Processed 3/3 browser jobs.
[~] -- 7.0 second/job.

[~] Currently auditing          https://vstupnik.cz/
[~] Burst response time sum     95.64 seconds
[~] Burst response count        110
[~] Burst average response time 0.869 seconds
[~] Burst average               4.099 requests/second
[~] Timed-out requests          379
[~] Original max concurrency    20
[~] Throttled max concurrency   12

[~] Status: Scanning
[~]
[~] Hit:
[~]   'Enter' to go back to status messages.
[~]   'p' to pause the scan.
[~]   'a' to abort the scan.
[~]   's' to suspend the scan to disk.
[~]   'g' to generate a report.
[~]   'v' to enable verbose messages.
[~]   'd' to enable debugging messages.
        (You can set it to the desired level by sending d[1-4], current level is 0).
```

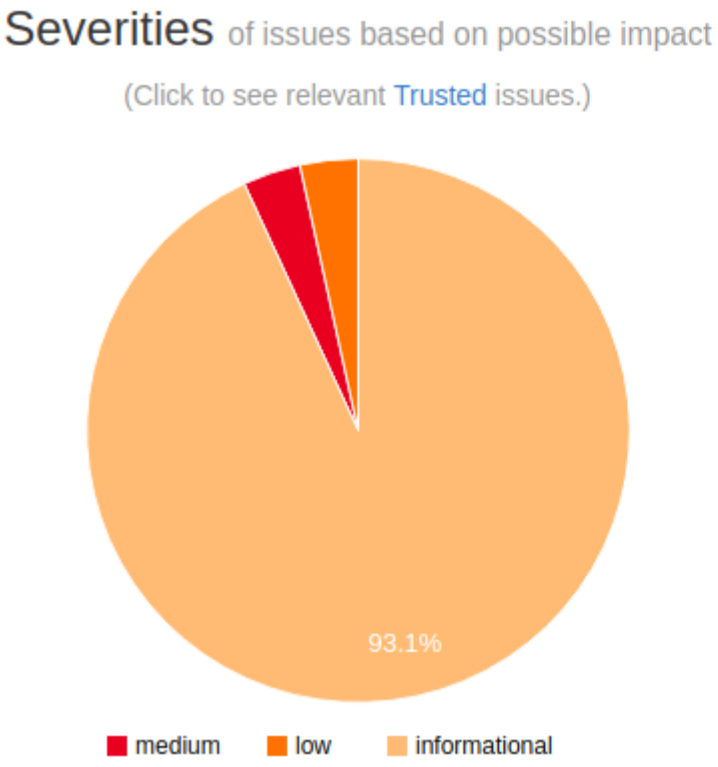
Arachni – reporty

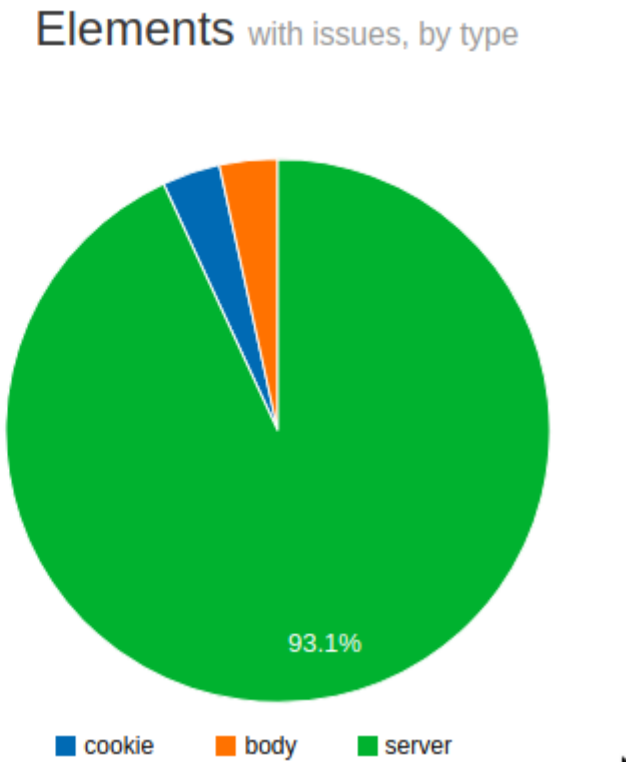
Summary

Charts | Issues 29 | OWASP Top 10



Arachni – reporty





Arachni – reporty

Medium severity 1

Unencrypted password form 1

The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed.

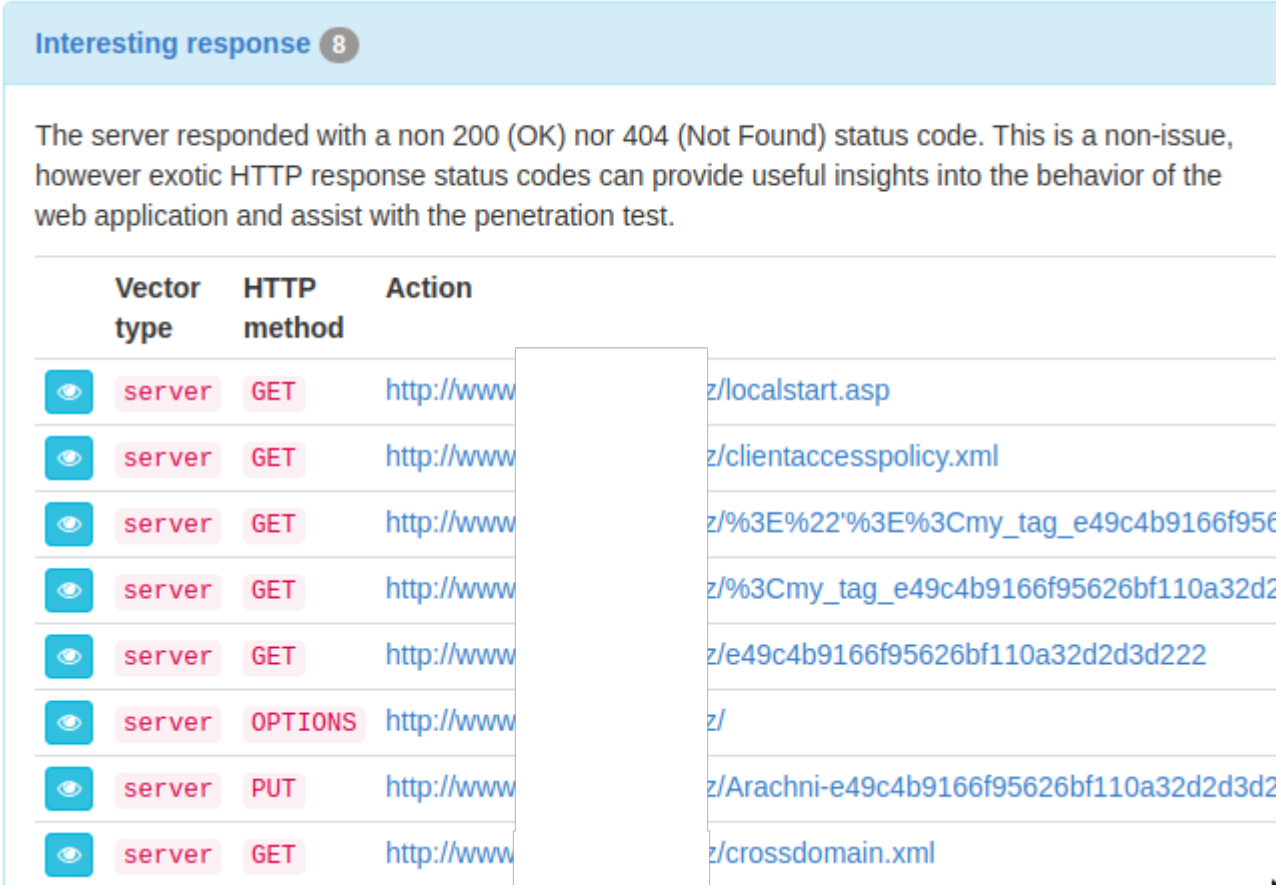
To keep data private, and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL), or Transport Layer Security (TLS). When either of these encryption standards are used it is referred to as HTTPS.

Cyber-criminals will often attempt to compromise credentials passed from the client to the server using HTTP. This can be conducted via various different Man-in-The-Middle (MiTM) attacks or through network packet captures.

Arachni discovered that the affected page contains a `password` input, however, the value of the field is not sent to the server utilising HTTPS. Therefore it is possible that any submitted credential may become compromised.

	Vector type	HTTP method	Action
	`form`	`GET`	http://srv.cz/login.php

Arachni – reporty



Interesting response 8

The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

	Vector type	HTTP method	Action
	server	GET	http://www z/localstart.asp
	server	GET	http://www z/clientaccesspolicy.xml
	server	GET	http://www z/%3E%22'%3E%3Cmy_tag_e49c4b9166f956
	server	GET	http://www z/%3Cmy_tag_e49c4b9166f95626bf110a32d2
	server	GET	http://www z/e49c4b9166f95626bf110a32d2d3d222
	server	OPTIONS	http://www z/
	server	PUT	http://www z/Arachni-e49c4b9166f95626bf110a32d2d3d2
	server	GET	http://www z/crossdomain.xml

Arachni – reporty

Affected page: http://www.[redacted].cz/Arachni-e49c4b9166f95626bf110a32d2d3d222

HTTP request

Raw HTTP request used to retrieve the page.

```
PUT /Arachni-e49c4b9166f95626bf110a32d2d3d222 HTTP/1.1
Host: www[redacted]cz
Accept-Encoding: gzip, deflate
User-Agent: Arachni/v1.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,he;q=0.6
X-Arachni-Scan-Seed: e49c4b9166f95626bf110a32d2d3d222
Content-Length: 55
Expect: 100-continue

Created by Arachni. PUTe49c4b9166f95626bf110a32d2d3d222
```

HTTP response

Raw HTTP response used as the page basis. (Binary bodies will not be disp

```
HTTP/1.1 100 Continue

HTTP/1.1 301 Moved Permanently
Server: nginx/1.11.9
Date: Mon, 11 Sep 2017 13:22:56 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 271
Connection: keep-alive
Keep-Alive: timeout=20
Location: http://[redacted].cz/Arachni-e49c4b9166f95626bf

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://[redacted].cz/A
</body></html>
```

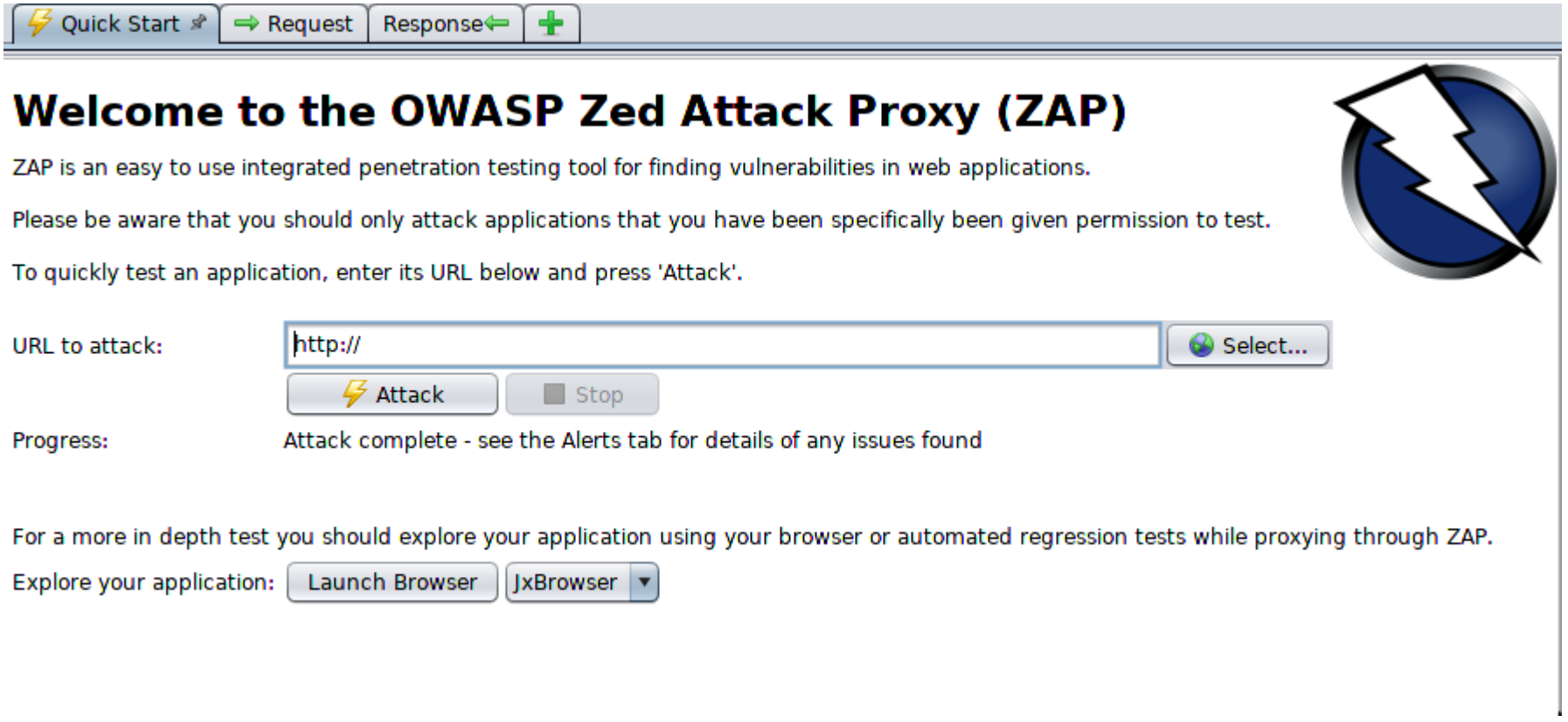
Arachni autologin

arachni http://example.cz

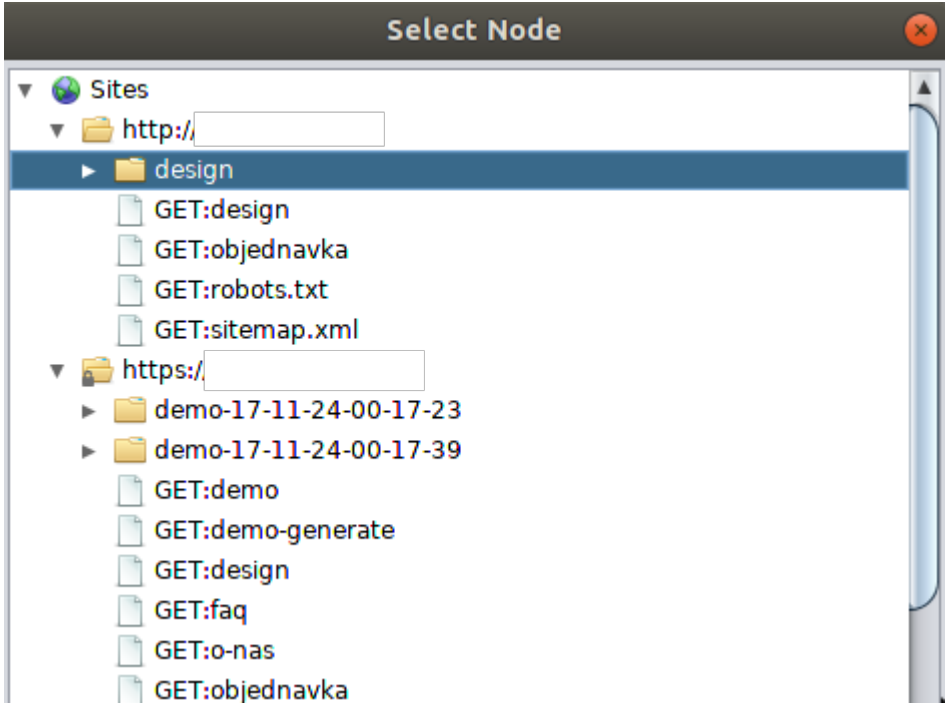
--plugin=autologin:
url=http://example.cz/login.php,
parameters="uid=*test*&passw=*mojeheslo*",
check="Sign Off|MY ACCOUNT"

--scope-exclude-pattern=logout

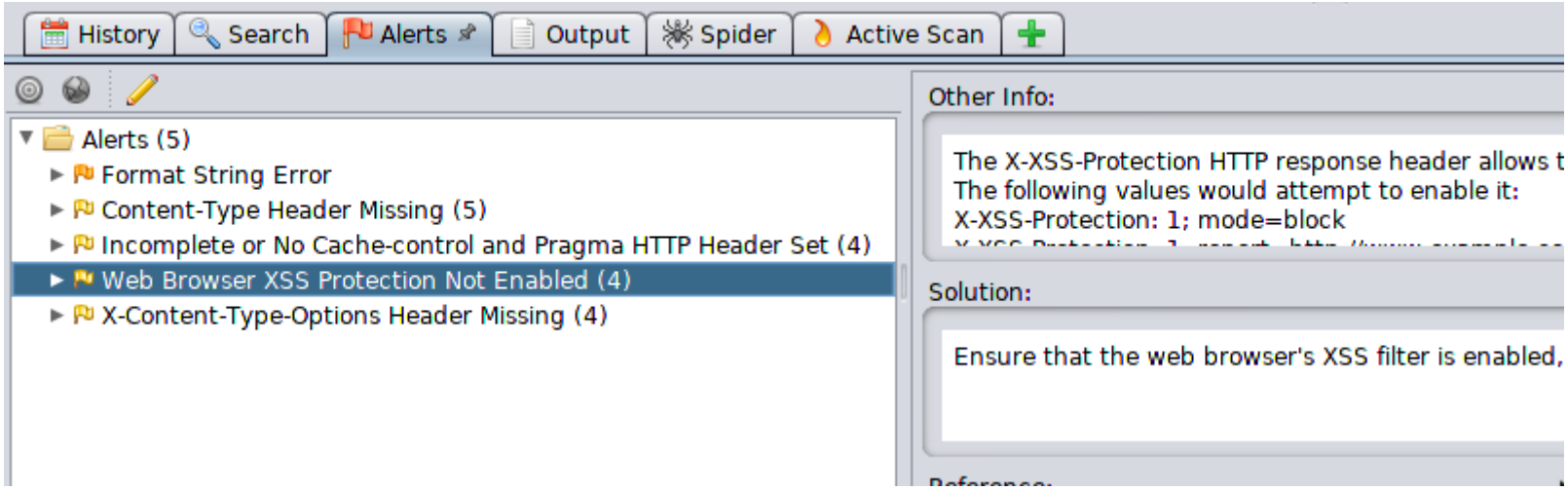
Owasp ZAP


Quick Start
Request
Response
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://
Select...
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.
Explore your application:
Launch Browser
JxBrowser

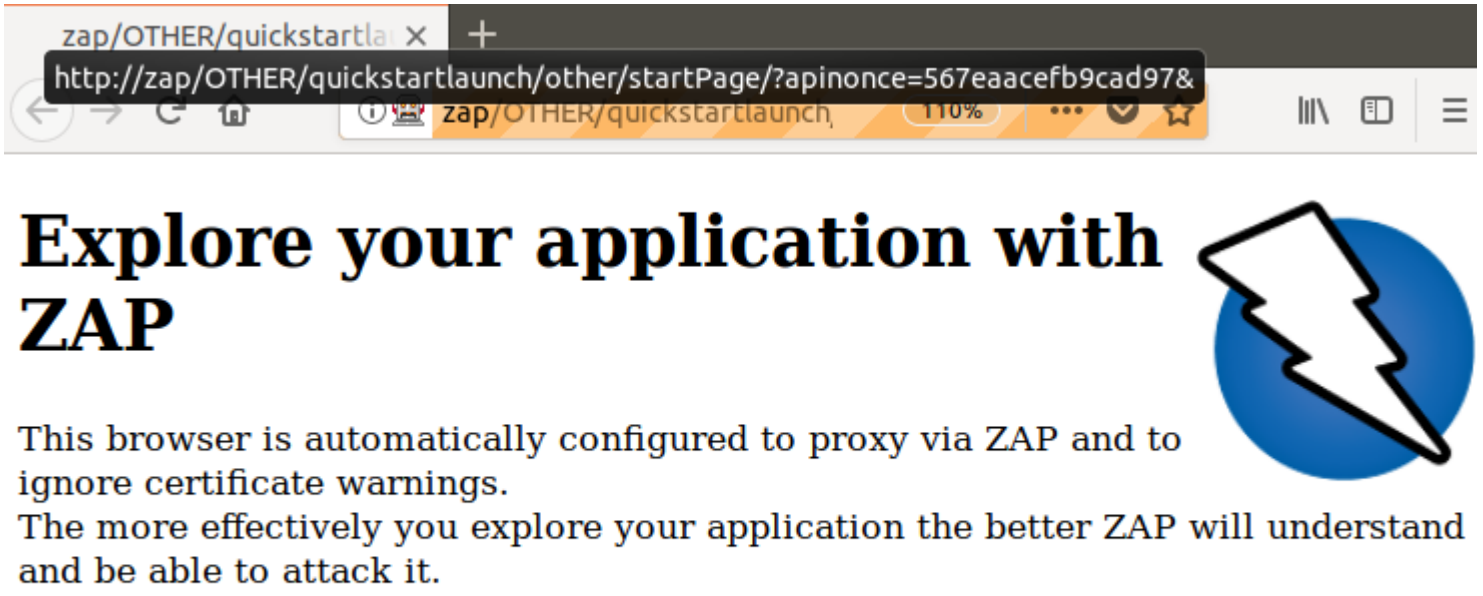
Owasp ZAP


Select Node
Sites
http://
design
GET:design
GET:objednavka
GET:robots.txt
GET:sitemap.xml
https://
demo-17-11-24-00-17-23
demo-17-11-24-00-17-39
GET:demo
GET:demo-generate
GET:design
GET:faq
GET:o-nas
GET:objednavka

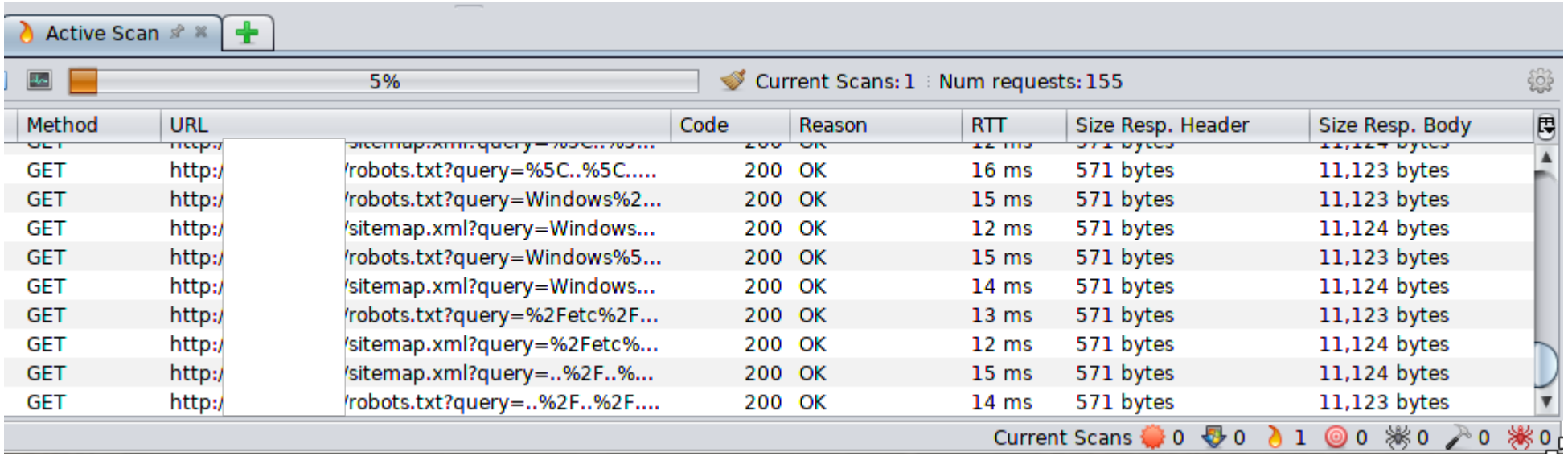
Owasp ZAP


History
Search
Alerts
Output
Spider
Active Scan
Alerts (5)
Format String Error
Content-Type Header Missing (5)
Incomplete or No Cache-control and Pragma HTTP Header Set (4)
Web Browser XSS Protection Not Enabled (4)
X-Content-Type-Options Header Missing (4)
Other Info:
The X-XSS-Protection HTTP response header allows t
The following values would attempt to enable it:
X-XSS-Protection: 1; mode=block
Solution:
Ensure that the web browser's XSS filter is enabled,

Owasp ZAP – pohodlná proxy



Owasp ZAP – průběžné výsledky



Owasp ZAP

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	0
Low	2
Informational	0

Alert Detail

High (Medium)	Path Traversal
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding ("..%255c") of the backslash character.

Owasp ZAP

URL	https://
Method	POST
Parameter	uname
URL	https://
Method	POST
Parameter	password
Reference	http://projects.webappsec.org/Path-Traversal http://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Source ID	1

Nessus

80/tcp	
	78555 - OpenSSL Unsupported
	93814 - OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET32)
	58987 - PHP Unsupported Version Detection
	77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
	11213 - HTTP TRACE / TRACK Methods Allowed
	93112 - OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32)
	64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
	73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
	68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
	62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
	96450 - Apache 2.2.x < 2.2.32 Multiple Vulnerabilities (httpoxy)
	88099 - Web Server HTTP Header Information Disclosure
	34850 - Web Server Uses Basic Authentication Without HTTPS

Nessus

80/tcp

78555 - OpenSSL Unsupported

Synopsis

An unsupported service is running on the remote host.

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer s

Lack of support implies that no new security patches for the product will be released by the vendor.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2014/10/17, Modification date: 2017/01/12

Ports

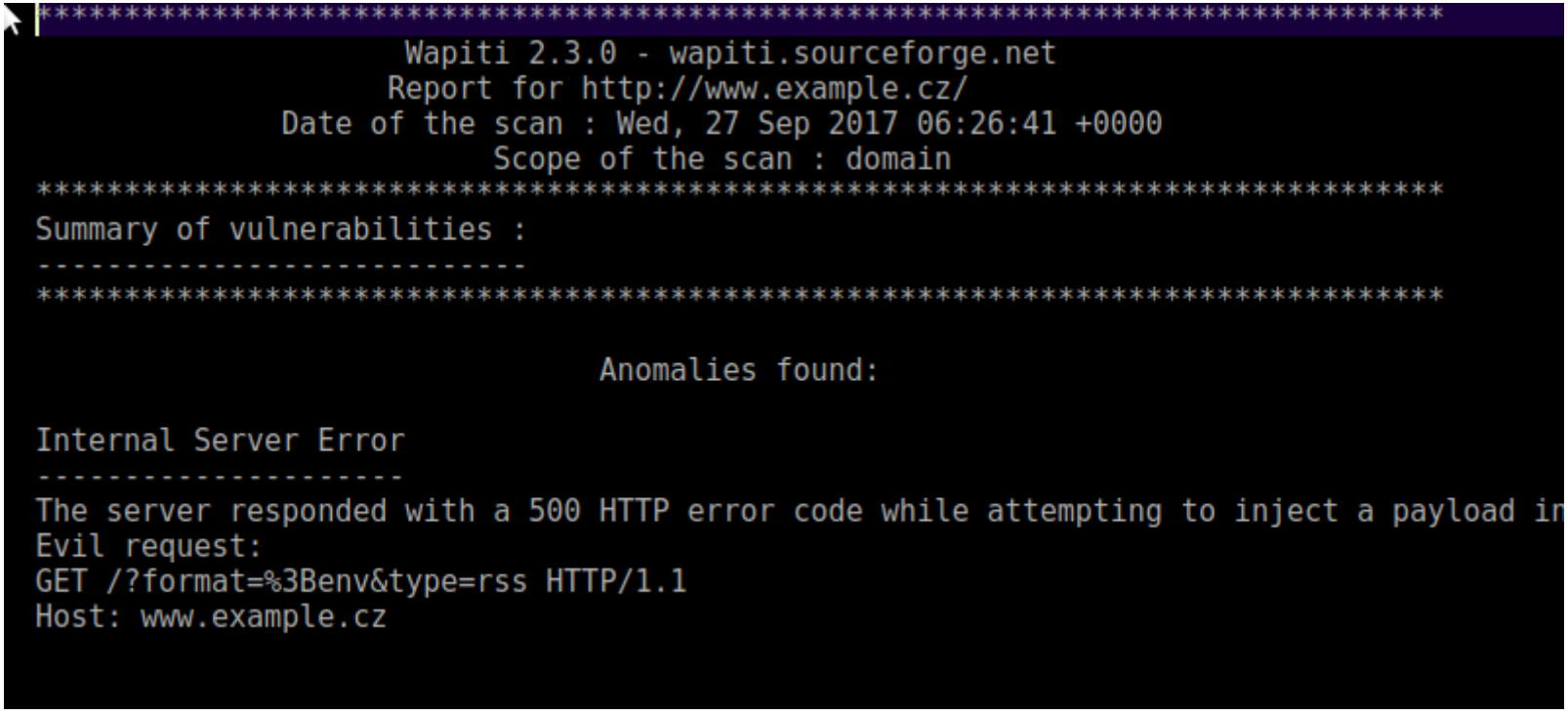
tcp/80

```
Installed version : 1.0.1t
Supported versions : 1.1.0 / 1.0.2
EOL URL : https://www.openssl.org/policies/releasestrat.html
```

Nessus

0/udp
10287 - Traceroute Information
21/tcp
34324 - FTP Supports Cleartext Authentication
14772 - Service Detection (2nd Pass)
14772 - Service Detection (2nd Pass)
10092 - FTP Server Detection
22/tcp
85382 - OpenSSH < 7.0 Multiple Vulnerabilities
73079 - OpenSSH < 6.6 Multiple Vulnerabilities
84638 - OpenSSH < 6.9 Multiple Vulnerabilities
93194 - OpenSSH < 7.3 Multiple Vulnerabilities
90023 - OpenSSH < 7.2p2 X11Forwarding xauth Command Injection

Wapiti


Wapiti 2.3.0 - wapiti.sourceforge.net
Report for http://www.example.cz/
Date of the scan : Wed, 27 Sep 2017 06:26:41 +0000
Scope of the scan : domain
Summary of vulnerabilities :
Anomalies found:
Internal Server Error
The server responded with a 500 HTTP error code while attempting to inject a payload in
Evil request:
GET /?format=%3Benv&type=rss HTTP/1.1
Host: www.example.cz

Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          1.2.3.4
+ Target Hostname:    example.cz
+ Target Port:        80
+ Start Time:         2017-09-25 05:56:56 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.3 (CentOS)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
+ The X-Content-Type-Options header is not set. This could allow the user agent
the MIME type
+ Root page / redirects to: http://www.example.cz/
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.4.12). Apac
+ OSVDB-3092: /manager/: May be a web server or site manager.
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /images/, inode: 246513
+ OSVDB-3233: /icons/README: Apache default file found.
+ Retrieved x-powered-by header: PHP/5.2.10
+ /myadmin/: Admin login page/section found.
+ /server-status: Apache server-status interface found (pass protected)
+ 26390 requests: 13 error(s) and 11 item(s) reported on remote host
+ End Time:           2017-09-25 06:14:31 (GMT-4) (1055 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

WhatWeb

```
WhatWeb report for http://www.example.cz/
Status    : 200 OK
Title     : Náhodný titulek
IP        : <Unknown>
Country   : <Unknown>

Summary   : X-Powered-By[PHP/5.4.21], Cookies[ffd16ba002de7c29a4bc2847e6
search], Apache[2.2.3], PHP[5.4.21], Script[text/javascript], JQuery, Fr
erver[CentOS][Apache/2.2.3 (CentOS)]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : ffd16ba002de7c29a4bc2847e6f329f0

[ Joomla ]
        Opensource CMS written in PHP. Aggressive version detection
        compares just 5 files, valid for versions 1.5.0-1.5.22 and
        1.6.0-1.6.1.

        Certainty    : maybe
        Aggressive function available (check plugin file or details).
        Google Dorks: (1)
        Website      : http://joomla.org
```

Uniscan

SCAN TIME

Scan Started: 27/9/2017 4:36:51

CRAWLING

Directory check:
Skipped because http://www.example.cz/uniscan46/ did not return the code 404

File check:
Skipped because http://www.example.cz/uniscan412/ did not return the code 404

Check robots.txt:
If the xartCMS site is installed within a folder such as at
e.g. www.example.com/xartcms/ the robots.txt file MUST be
moved to the site root at e.g. www.example.com/robots.txt
AND the xartcms folder name MUST be prefixed to the disallowed
path, e.g. the Disallow rule for the /administrator/ folder
MUST be changed to read Disallow: /xartcms/administrator/
#
For more information about the robots.txt standard, see:
http://www.robotstxt.org/orig.html
#
For syntax checking, see:
http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Disallow: /installation/
Disallow: /logs/
Disallow: /tmp/
Sitemap: http://www.helios-servis.cz/index.php?option=com_xmap&view=xml

Check sitemap.xml:

Děkuji za pozornost

Edvard Rejthar • edvard.rejthar@nic.cz

Vzor

-
-
-