Website Vulnerability Scanner Report (Light)

✔ http://13.70.2.33:5000

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	2
Low:	2
Info:	6

Scan information:

Start time:	2020-04-27 12:52:29 UTC+03
Finish time:	2020-04-27 12:52:51 UTC+03
Scan duration:	22 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	5.0	CVE-2018-1060	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service.	N/A	Python 3.6.9
●	5	CVE-2019-9636	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	N/A	Python 3.6.9

●	5.0	CVE-2019-16056	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.	N/A	Python 3.6.9
●	5	CVE-2018-20406	Modules/_pickle.c in Python before 3.7.1 has an integer overflow via a large LONG_BINPUT value that is mishandled during a "resize to twice the size" attempt. This issue might cause memory exhaustion, but is only relevant if the pickle format is used for serializing tens or hundreds of gigabytes of data.	N/A	Python 3.6.9
●	4.3	CVE-2019-9740	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.	N/A	Python 3.6.9

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Communication is not secure

http://13.70.2.33:5000/

Details

Risk description:
The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Server software and technology found

Software / Version	Category
Flask 1.0.0	Web Frameworks, Web Servers
Python 3.6.9	Programming Languages

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:
https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002).

Missing HTTP security headers

HTTP Security Header	Header Role	Status

X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

Details

Risk description:
Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://www.owasp.org/index.php/Clickjacking

The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

The HTTP X-Content-Type-Options header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend you to add the X-Frame-Options HTTP response header to every page that you want to be protected against Clickjacking attacks.
More information about this issue:
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

We recommend setting the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block".
More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

We recommend setting the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".
More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

No security issue found regarding HTTP cookies

Robots.txt file not found

No security issue found regarding client access policies

Directory listing not found (quick scan)

No password input found (auto-complete test)

No password input found (clear-text submission test)

Scan coverage information

List of tests performed (10/10)

- Fingerprinting the server software and technology...
- Checking for vulnerabilities of server-side software...
- Analyzing the security of HTTP cookies...
- Analyzing HTTP security headers...
- Checking for secure communication...
- Checking robots.txt file...
- Checking client access policies...
- Checking for directory listing (quick scan)...
- Checking for password auto-complete (quick scan)...
- Checking for clear-text submission of passwords (quick scan)...

Scan parameters

Website URL:	http://13.70.2.33:5000
Scan type:	Light
Authentication:	False