6/13/2023 1:51:42 AM (UTC+05:30)

Detailed Scan Report

http://127.0.0.1:5000/predict

Scan Time	6/13/2023 1:41:27 AM (UTC+05:30)
Scan Duration	00:00:02:49
Total Requests	: 2,043
Average Speed	: 12.0r/s

Risk Level:
MEDIUM

17 IDENTIFIED	**1** CONFIRMED	**0** CRITICAL
0 HIGH	3 MEDIUM	5 LOW
	4 BEST PRACTICE	5 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	5
Best Practice	4
Information	5
TOTAL	**17**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	0
Best Practice	0
Information	1
TOTAL	**1**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Bootstrap)	GET	http://127.0.0.1:5000/static/js/bootstrap.min.js	
	Out-of-date Version (jQuery)	GET	http://127.0.0.1:5000/predict	
	SSL/TLS Not Implemented	GET	https://127.0.0.1/predict	
	[Possible] Cross-site Request Forgery	GET	http://127.0.0.1:5000/predict	
	[Possible] Phishing by Navigating Browser Tabs	GET	http://127.0.0.1:5000/predict	
	Missing X-Frame-Options Header	GET	http://127.0.0.1:5000/predict	
	Version Disclosure (Python)	GET	http://127.0.0.1:5000/predict	
	Version Disclosure (Werkzeug Python WSGI Library)	GET	http://127.0.0.1:5000/predict	
	Content Security Policy (CSP) Not Implemented	GET	http://127.0.0.1:5000/predict	
	Missing X-XSS-Protection Header	GET	http://127.0.0.1:5000/predict	
	Referrer-Policy Not Implemented	GET	http://127.0.0.1:5000/predict	
	Subresource Integrity (SRI) Not Implemented	GET	http://127.0.0.1:5000/predict	
	Expect-CT Security Header Errors and Warnings	GET	http://127.0.0.1:5000/predict	
	Out-of-date Version (Modernizr)	GET	http://127.0.0.1:5000/predict	
	Python Identified	GET	http://127.0.0.1:5000/predict	
	Werkzeug Python WSGI Library Identified	GET	http://127.0.0.1:5000/predict	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	OPTIONS Method Enabled	OPTIONS	http://127.0.0.1:5000/	

1. Out-of-date Version (Bootstrap)

MEDIUM | 1

Netsparker identified that the target web site is using Bootstrap and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Affected Versions

1.0.0 to 3.3.7

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2018-14042

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Affected Versions

3.0.0 to 3.3.7

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2016-10735

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

Affected Versions

1.0.0 to 3.3.7

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2018-20676

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.

Affected Versions
1.0.0 to 3.3.7

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2018-20677

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Affected Versions
1.0.0 to 3.4.0

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2019-8331

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

Affected Versions
1.0.0 to 3.3.7

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2018-14040

Vulnerabilities

1.1. http://127.0.0.1:5000/static/js/bootstrap.min.js

Identified Version
- 3.3.5

Latest Version
- 3.4.1 (in this branch)

Overall Latest Version
- 5.3.0

Vulnerability Database
- Result is based on 06/06/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET /static/js/bootstrap.min.js HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://127.0.0.1:5000/predict
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 619.8885 Total Bytes Received : 37208 Body Length : 36816 Is Compressed : No

```
HTTP/1.1 200 OK
Content-Type: application/javascript; charset=utf-8
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 36816
Last-Modified: Sat, 27 May 2023 03:37:10 GMT
ETag: "1685158630.0-36816-1818039741"
Content-Disposition: inline; filename=bootstrap.min.js
Date: Mon, 12 Jun 2023 20:11:53 GMT
Date: Mon, 12 Jun 2023 20:11:53 GMT
C
…
Tag: "1685158630.0-36816-1818039741"
Content-Disposition: inline; filename=bootstrap.min.js
Date: Mon, 12 Jun 2023 20:11:53 GMT
Date: Mon, 12 Jun 2023 20:11:53 GMT
Cache-Control: no-cache

/*!
* Bootstrap v3.3.5(http://getbootstrap.com)
* Copyright 2011-2015 Twitter, Inc.
* Licensed under the MIT license
*/
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(
…
```

Remedy

Please upgrade your installation of Bootstrap to the latest stable version.

Remedy References

- Downloading Bootstrap

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	937, 1035
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

2. Out-of-date Version (jQuery)

MEDIUM | 1

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Affected Versions

1.8.0 to 2.2.4

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2015-9251

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-11022

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions
1.0 to 3.3.1

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2019-11358

Vulnerabilities

2.1. http://127.0.0.1:5000/predict

Identified Version
- 2.1.4

Latest Version
- 2.2.4 (in this branch)

Overall Latest Version
- 3.7.0

Vulnerability Database
- Result is based on 06/06/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 Total Bytes Received : 7523 Body Length : 7348 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

- Downloading jQuery

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	937, 1035
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

3. SSL/TLS Not Implemented

MEDIUM | 1

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Vulnerabilities

3.1. https://127.0.0.1/predict

Certainty

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1 **Total Bytes Received** : 16 **Body Length** : 0 **Is Compressed** : No

```
[SSL Connection]
```

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot toolprovided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

PCI DSS v3.2	6.5.4

OWASP 2013	A6
OWASP 2017	A3
CWE	311
CAPEC	217
WASC	4
HIPAA	164.306
ASVS 4.0	9.1.1
NIST SP 800-53	SC-8
DISA STIG	3.7.4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

4. [Possible] Cross-site Request Forgery

LOW | 1

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

4.1. http://127.0.0.1:5000/predict

Form Action(s)

- /predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 Total Bytes Received : 7523 Body Length : 7348 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 20
…
a random one from our dataset to try it.</p>
</div>
</div>
</div>
<div class="login">
<h1>Predict Fake News</h1>

<!-- Main Input For Receiving Query to our ML -->
<form action="/predict"method="post">
<input type="text" name="news" placeholder="Enter the news " required="required"  style="margin: 100
px; width:85%;"/>
<button type="submit" class="btn btn-primary btn-block
…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ASVS 4.0	4.2.2
NIST SP 800-53	SC-23
DISA STIG	3.10.6
ISO27001	A.14.2.5

5. [Possible] Phishing by Navigating Browser Tabs

LOW 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

5.1. http://127.0.0.1:5000/predict

External Links

- https://colorlib.com
- http://unsplash.co/
- http://pexels.com/

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 20
…
r CC BY 3.0. -->
Copyright &copy;<script>document.write(new Date().getFullYear());</script> All rights reserved | Thi
s template is made with <i class="icon-heart3" aria-hidden="true"></i> by <a href="https://colorlib.
com" target="_blank">Colorlib</a>
<!-- Link back to Colorlib can't be removed. Template is licensed under CC BY 3.0. --></small><br>
<small class="block">Demo Images: <a href="http://unsplash.co/" target="_blank">Unsplash</a>, <a hre
f="http://pexels.com/" target="_blank">Pexels</a></small>
</p>
</div>
</div>
</div>
</div>
</footer>
</div>

<div class="gototop js-top">
<a href="#" class="js-gotop"><i class="icon-arrow-up2"></i></a>
</div>

…
```

Remedy

- Add `rel=noopener`to the linksto prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener*property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer`which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target=" blank" - the most underestimated vulnerability ever

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.1.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

6. Missing X-Frame-Options Header

LOW | 1

Netsparker detected a missing `X-Frame-Options`header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options`HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame`or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

6.1. http://127.0.0.1:5000/predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY`It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN`It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ASVS 4.0	14.4.7
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

7. Version Disclosure (Python)

LOW 1

Netsparker identified a version disclosure (Python) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Python.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

7.1. http://127.0.0.1:5000/predict

Extracted Version

- 3.11.3

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Remedy

Configure your web server to prevent information leakage from the SERVERheader of its HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(A), 164.308(A)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	3.13
ISO27001	A.18.1.3

8. Version Disclosure (Werkzeug Python WSGI Library)

LOW 1

Netsparker identified a version disclosure (Werkzeug) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Werkzeug.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

8.1. http://127.0.0.1:5000/predict

Extracted Version

- 2.3.4

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Remedy

Configure your application to prevent information leakage from the SERVER header of its HTTP response.

External References

- Werkzeug's official website

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(A), 164.308(A)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	3.13
OWASP Proactive Controls	N/A
ISO27001	A.18.1.3

9. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:**The base element is used to resolve a relative URL to an absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to the base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe on the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly end with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Vulnerabilities

9.1. http://127.0.0.1:5000/predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

10. Missing X-XSS-Protection Header

BEST PRACTICE | 1

Netsparker detected a missing `X-XSS-Protection`header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

10.1. http://127.0.0.1:5000/predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- ```
  X-XSS-Protection: 1; mode=block
  ```

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

CWE	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5
  ```

11. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

11.1. http://127.0.0.1:5000/predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ASVS 4.0	14.4.6
NIST SP 800-53	AC-22
DISA STIG	3.13
ISO27001	A.14.2.5

12. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

12.1. http://127.0.0.1:5000/predict

Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Poppins:300,400,700,900
- https://fonts.googleapis.com/css?family=Montserrat:300,400,700

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 20
…
iction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!--
…
```

Remedy

Using Subresource Integrity is simply to add *integrity*attribute to the *script*tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384**or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

CWE	16

WASC	15
ASVS 4.0	10.3.2, 14.2.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

13. Expect-CT Security Header Errors and Warnings

INFORMATION 1

Netsparker detected errors during parsing of Expect-CT header.

Vulnerabilities

13.1. http://127.0.0.1:5000/predict

Error	Resolution
Expect-CT header should be served with a hostname as known Expect-CT hosts are identified only by domain names, and never IP addresses.	Serve Expect-CT header with a defined hostname.

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	9.2.4
NIST SP 800-53	CM-6
DISA STIG	3.5.1
OWASP Proactive Controls	C10
ISO27001	A.14.1.2

14. OPTIONS Method Enabled

INFORMATION 1 | CONFIRMED 1

Netsparker detected that `OPTIONS`method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Vulnerabilities

14.1. http://127.0.0.1:5000/

CONFIRMED

Allowed methods

- HEAD, OPTIONS, GET

Request

```
OPTIONS / HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 75.5355 **Total Bytes Received** : 199 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Allow: HEAD, OPTIONS, GET
Content-Length: 0
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:12:01 GMT
```

Remedy

Disable `OPTIONS`method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	14
ASVS 4.0	14.5.1
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

15. Out-of-date Version (Modernizr)

INFORMATION 1

Netsparker identified that the target web site is using Modernizr and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Vulnerabilities

15.1. http://127.0.0.1:5000/predict

Identified Version

- 2.6.2

Latest Version

- 3.12.0

Vulnerability Database

- Result is based on 06/06/2023 20:30:00 vulnerability database content.

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 20
…
xt/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->

</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class
…
```

Remedy

Please upgrade your installation of Modernizr to the latest stable version.

Remedy References

- Downloading Modernizr

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	937, 1035

CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

16. Python Identified

INFORMATION 1

Netsparker identified a Python in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

16.1. http://127.0.0.1:5000/predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

External References

- Python

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	3.13
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

17. Werkzeug Python WSGI Library Identified

INFORMATION 1

Netsparker identified Werkzeug, a comprehensive Python WSGI library.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

17.1. http://127.0.0.1:5000/predict

Certainty

Request

```
GET /predict HTTP/1.1
Host: 127.0.0.1:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 190.2133 **Total Bytes Received** : 7523 **Body Length** : 7348 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.3
Connection: close
Content-Length: 7348
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Jun 2023 20:11:28 GMT

<!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Fake News Prediction</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<meta name="author" content="" />


<link href="https://fonts.googleapis.com/css?family=Poppins:300,400,700,900" rel="stylesheet">
<link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet">

<!-- Animate.css -->
<link rel="stylesheet" type="text/css" href="static/css/animate.css">
<!-- Icomoon Icon Fonts-->
<link rel="stylesheet" type="text/css" href="static/css/icomoon.css">
<!-- Bootstrap  -->
<link rel="stylesheet" type="text/css" href="static/css/bootstrap.css">

<!-- Magnific Popup -->
<link rel="stylesheet" type="text/css" href="static/css/magnific-popup.css">

<!-- Flexslider  -->
<link rel="stylesheet" type="text/css" href="static/css/flexslider.css">

<!-- Owl Carousel -->
<link rel="stylesheet" type="text/css" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" type="text/css" href="static/css/owl.theme.default.min.css">

<!-- Flaticons  -->
<link rel="stylesheet" type="text/css" href="static/fonts/flaticon/font/flaticon.css">

<!-- Theme style  -->
<link rel="stylesheet" type="text/css" href="static/css/style.css">

<!-- Modernizr JS -->
<script src="../static/js/modernizr-2.6.2.min.js"></script>
<!-- FOR IE9 below -->
<!--[if lt IE 9]>
<script src="js/respond.min.js"></script>
<![endif]-->
```

```
</head>
<body>

<div class="colorlib-loader"></div>

<div id="page">
<nav class="colorlib-nav" role="navigation">
<div class="top-menu">
<div class="container">
<div class="row">
<div class="col-md-2 text-cent
…
```

External References

- Werkzeug's official website

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	3.13
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
Arbitrary Files (IAST),
BREACH Attack,
Code Evaluation,
Code Evaluation (IAST),
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Command Injection (IAST),
Configuration Analyzer (IAST),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),

	Custom Script Checks (Singular), Drupal Remote Code Execution, Expect Certificate Transparency (Expect-CT), Expression Language Injection, File Upload, Header Analyzer, Heartbleed, HSTS, HTML Content, HTTP Header Injection, HTTP Header Injection (IAST), HTTP Methods, HTTP Status, HTTP.sys (CVE-2015-1635), IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content, JavaScript Libraries, JSON Web Token, Local File Inclusion, Local File Inclusion (IAST), Login Page Identifier, Mixed Content, Open Redirection, Oracle WebLogic Remote Code Execution, Referrer Policy, Reflected File Download, Remote File Inclusion, Remote File Inclusion (Out of Band), Reverse Proxy Detection, RoR Code Execution, Server-Side Request Forgery (DNS), Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (IAST), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	: Heuristic
Detected URL Rewrite Rule(s)	: None

Excluded URL Patterns	: gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	: None
Authentication Profile	: None
Scheduled	: No
Additional Website(s)	: None