



8.08.2022 01:31:31 (UTC+03:00)

Detailed Scan Report

<http://www.kriptarium.com/>

Scan Time : 8.08.2022 00:04:21 (UTC+03:00)
Scan Duration : 00:01:02:04
Total Requests : 46.004
Average Speed : 12,4r/s

Risk Level:
MEDIUM

22
IDENTIFIED

5
CONFIRMED

0
CRITICAL

0
HIGH

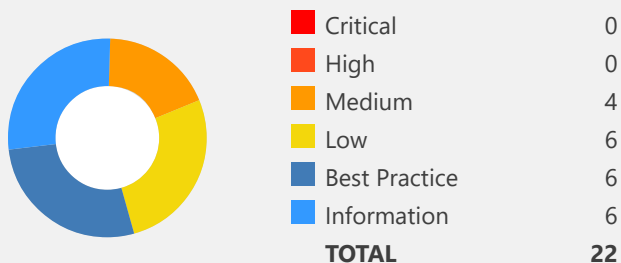
4
MEDIUM

6
LOW

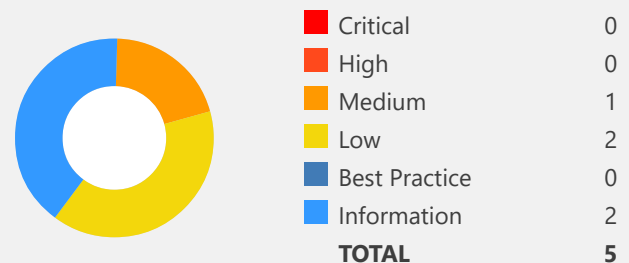
6
BEST PRACTICE

6
INFORMATION

































Identified Vulnerabilities















Confirmed Vulnerabilities



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	 [Possible] Cross-site Scripting	POST	http://www.kriptarium.com/ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails]	
	 [Possible] Cross-site Scripting	POST	http://www.kriptarium.com/ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails]	
	 Out-of-date Version (jQuery).	GET	http://www.kriptarium.com/	
	 Weak Ciphers Enabled	GET	https://www.kriptarium.com/	
	 [Possible] Cross-site Request Forgery	GET	http://www.kriptarium.com/304leti351im.html	
	 [Possible] Phishing by Navigating Browser Tabs	GET	http://www.kriptarium.com/	
	 Missing Content-Type Header	GET	http://www.kriptarium.com/sitemap.xml.gz	
	 Missing X-Frame-Options Header	GET	http://www.kriptarium.com/	
	 Cookie Not Marked as HttpOnly	GET	http://www.kriptarium.com/	
	 Insecure Frame (External)	GET	http://www.kriptarium.com/304leti351im.html	
	 Content Security Policy (CSP) Not Implemented	GET	http://www.kriptarium.com/	
	 Expect-CT Not Enabled	GET	https://www.kriptarium.com/	
	 Missing X-XSS-Protection Header	GET	http://www.kriptarium.com/	
	 Referrer-Policy Not Implemented	GET	http://www.kriptarium.com/	
	 SameSite Cookie Not Implemented	GET	http://www.kriptarium.com/	
	 Subresource Integrity (SRI) Not Implemented	GET	http://www.kriptarium.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
 	Apache Web Server Identified	GET	http://www.kriptarium.com/	
 	Email Address Disclosure	GET	http://www.kriptarium.com/	
 	Nginx Web Server Identified	GET	http://www.kriptarium.com/files/theme/	
 	Sitemap Detected	GET	http://www.kriptarium.com/sitemap.xml	
 	Forbidden Resource	POST	http://www.kriptarium.com/uumlruumlner.html	
 	Robots.txt Detected	GET	http://www.kriptarium.com/robots.txt	

1. [Possible] Cross-site Scripting

MEDIUM



2

Netsparker detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript*, *VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

1.1. [http://www.kriptarium.com/ajax/api/JsonRPC/CustomAccounts/?CustomerAccounts\[CustomAccounts::getAccountDetails\]](http://www.kriptarium.com/ajax/api/JsonRPC/CustomAccounts/?CustomerAccounts[CustomAccounts::getAccountDetails])

Method	Parameter	Value
POST	jsonrpc	2.0
POST	id	3
POST	method	'><net_sparker=netsparker(0x003229)>
POST	CustomerAccounts[CustomerAccounts::getAccountDetails]	

Notes

- To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty



Request

```
POST /ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails] HTTP/1.1
Host: www.kriptarium.com
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 86
Content-Type: application/json; charset=UTF-8
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659907525.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; language=en
Origin: http://www.kriptarium.com
Referer: http://www.kriptarium.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Requested-With: XMLHttpRequest
X-Scanner: Netsparker

{"jsonrpc":"2.0","method":"","><net_sparker=netsparker(0x003229)>","params":[],"id":"3"}
```

Response

Response Time (ms) : 473,9096 Total Bytes Received : 369 Body Length : 145 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Content-Length: 145
X-UA-Compatible: IE=edge,chrome=1
X-Host: grn66.sf2p.intern.weebly.net
Content-Type: application/json
Date: Sun, 07 Aug 2022 21:25:30 GMT
Vary: X-W-SSL,User-Agent

{"jsonrpc":"2.0","method":"","><net_sparker=netsparker(0x003229)>","error":{"code":-32001,"message":"invalid namespace or function name"},"id":"3"}
```

1.2. [http://www.kriptarium.com/ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts\[CustomerAccounts::getAccountDetails\]](http://www.kriptarium.com/ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails])

Method	Parameter	Value
POST	jsonrpc	2.0
POST	id	'><net_sparker=netsparker(0x002F61)>
POST	method	CustomerAccounts::getAccountDetails
POST	CustomerAccounts[CustomerAccounts::getAccountDetails]	

Notes

- To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty



Request

```
POST /ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails] HTTP/1.1
Host: www.kriptarium.com
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 120
Content-Type: application/json; charset=UTF-8
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; language=en; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659907442.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*
Origin: http://www.kriptarium.com
Referer: http://www.kriptarium.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Requested-With: XMLHttpRequest
X-Scanner: Netsparker

{"jsonrpc":"2.0","method":"CustomerAccounts::getAccountDetails","params":[],"id":"'><net_sparker=netsparker(0x002F61)>'>"}
```

Response

Response Time (ms) : 505,2569 Total Bytes Received : 711 Body Length : 487 Is Compressed : No

HTTP/1.1 200 OK

Server: Apache

Content-Length: 487

X-UA-Compatible: IE=edge,chrome=1

X-Host: grn13.sf2p.intern.weebly.net

Content-Type: application/json

Date: Sun, 07 Aug 2022 21:24:17 GMT

Vary: X-W-SSL,User-Agent

```
{ "jsonrpc": "2.0", "id": ">net sparker=netsparker(0x002F61)>", "method": "CustomerAccounts::getAccountDetails", "result": { "success": false, "message": "M\u00fc\u015fteri hesaplar\u0131 k\u0131s\u0131tl\u0131 veya etkin de\u011fil.", "event": "", "data": { "code": "dontShow", "message": "M\u00fc\u015fteri hesaplar\u0131 k\u0131s\u0131tl\u0131 veya etkin de\u011fil.", "message_tl": "M\u00fc\u015fteri hesaplar\u0131 k\u0131s\u0131tl\u0131 veya etkin de\u011fil." }, "total": null, "http_response_code": 401 } }
```

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include [OWASP Reform](#) and [Microsoft Anti-Cross-site Scripting](#) libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- [OWASP - Cross-site Scripting](#)
- [Cross-site Scripting Web Application Vulnerability](#)
- [XSS Shell](#)
- [XSS Tunnelling](#)

Remedy References

- [Content Security Policy \(CSP\) Explained](#)
- [Negative Impact of Incorrect CSP Implementations](#)
- [\[ASP.NET\] - Microsoft Anti-XSS Library](#)
- [OWASP XSS Prevention Cheat Sheet](#)



CLASSIFICATION

PCI DSS v3.2	6.5.7
OWASP 2013	A3
OWASP 2017	A7
SANS Top 25	79
CAPEC	19
WASC	8
HIPAA	164.308(A)
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	7,4 (High)
Temporal	7,4 (High)
Environmental	7,4 (High)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	7,4 (High)
Temporal	7,4 (High)
Environmental	7,4 (High)

CVSS Vector String

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

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

External References

- [CVE-2015-9251](#)

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

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The `jQuery(strInput)` function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the `'<'` character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the `'<'` character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Affected Versions

1.8.0 to 1.8.3

External References

- [CVE-2012-6708](#)

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

jQuery prior to 1.9.0 allows Cross-site Scripting attacks via the `load` method. The `load` method fails to recognize and remove `"<script>"` HTML tags that contain a whitespace character, i.e: `"</script >"`, which results in the enclosed script logic to be executed.

Affected Versions

1.8.0 to 1.8.3

External References

- [CVE-2020-7656](#)

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

1.8.0 to 1.8.3

External References

- [CVE-2020-11022](#)

🚩 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

1.8.0 to 1.8.3

External References

- [CVE-2020-11023](#)

🚩 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

External References

- [CVE-2019-11358](#)

Vulnerabilities

2.1. <http://www.kriptarium.com/>

Identified Version

- 1.8.3

Latest Version

- 1.12.4 (in this branch)

Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-A
...
yle>

<script>
var STATIC_BASE = '//cdn1.editmysite.com/';
var ASSETS_BASE = '//cdn2.editmysite.com/';
var STYLE_PREFIX = 'wsite';
</script>
<script src='https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js'></script>


<script type="text/javascript" src="//cdn2.editmysite.com/js/lang/tr/stl.js?buildTime=1659481470"></script>
<script src="//cdn2.editmysite.com/js/site/main.js?buildTime=1659481470"></script>
...
```

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
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

3. Weak Ciphers Enabled

MEDIUM

1

CONFIRMED

1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

3.1. <https://www.kriptarium.com/>
CONFIRMED

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10-2017 A3-Sensitive Data Exposure](#)
- [Zombie Poodle - Golden Doodle \(CBC\)](#)
- [Mozilla SSL Configuration Generator](#)
- [Strong Ciphers for Apache, Nginx and Lighttpd](#)



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6,8 (Medium)
Temporal	6,8 (Medium)
Environmental	6,8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6,8 (Medium)
Temporal	6,8 (Medium)
Environmental	6,8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

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://www.kriptarium.com/304leti351im.html>

Form Action(s)

- [//www.weebly.com/weebly/apps/formSubmit.php](http://www.weebly.com/weebly/apps/formSubmit.php)

Certainty



Request

```
GET /304leti351im.html HTTP/1.1
Host: www.kriptarium.com
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
Cookie: is_mobile=0; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906441.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; language=en
Referer: http://www.kriptarium.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 500,0141 Total Bytes Received : 42591 Body Length : 42159 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:07:29 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 10001
X-UA-Compatible: IE=edge,chrome=1
X-Host: grn13.sf2p.intern.weebly.net
ETag: W/"933e4765d4dc7ee2e9cf461e6bfa74e-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:07:29 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-C
...
er ile ilgili g&ouml;r&uuml;&#351;/&ouml;neri ve &#351;ikayetlerinizi a&#351;a&#287;&#305;daki ba&#351;
vuru formunu doldurarak iletebilirsiniz.&nbsp;</div>

<div>
<form enctype="multipart/form-data" action="//www.weebly.com/weebly/apps/formSubmit.php"method="POST" i
d="form-308081456301334584">
<div id="308081456301334584-form-parent" class="wsite-form-container"
style="margin-top:10px;">
<ul class="formlist" id="308081456301334584-form-
...
```

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
SANS Top 25	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
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://www.kriptarium.com/>

External Links

- https://twitter.com/kriptarium_
- [//instagram.com/kriptarium_](https://instagram.com/kriptarium_)
- https://uk.linkedin.com/company/kriptarium---fth-bilgi-iletisim-teknolojileri?trk=public_profile_result-card_subtitle-click
- <https://www.youtube.com/channel/UCN-0SgO68y9jyEZrJitS1nw>
- [//facebook.com/kriptarium/](https://facebook.com/kriptarium/)
- [//twitter.com/kriptarium_](https://twitter.com/kriptarium_)
- <https://tr.linkedin.com/pub/fatih-ozkaynak/64/852/5a3>
- <https://www.youtube.com/channel/UCN-0SgO68y9jyEZrJitS1nw>
- [//instagram.com/kriptarium_](https://instagram.com/kriptarium_/)

Certainty

Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```


Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-A
...
v>
```

```
<div style="text-align:center;"><div style="height:0px;overflow:hidden"></div>
<span class="wsite-social wsite-social-default"><a class='first-child wsite-social-item wsite-social-tw
itter' href='https://twitter.com/kriptarium_' target='_blank' alt='Twitter' aria-label='Twitter'><span
class='wsite-social-item-inner'></span></a><a class='wsite-social-item wsite-social-instagram' href='
//instagram.com/kriptarium_' target='_blank' alt='Instagram' aria-label='Instagram'><span class='wsite-
social-item-inner'></span></a><a class='wsite-social-item wsite-social-linkedin' href='https://uk.linke
din.com/company/kriptarium---fth-bilgi-iletisim-teknolojileri?trk=public_profile_result-card_subtitle-c
lick' target='_blank' alt='Linkedin' aria-label='Linkedin'><span class='wsite-social-item-inner'></span>
</a><a class='wsite-social-item wsite-social-mail' href='mailto:iletisim@kriptarium.com' target='_blan
k' alt='Mail' aria-label='Mail'><span class='wsite-social-item-inner'></span></a><a class='last-child w
site-social-item wsite-social-youtube' href='https://www.youtube.com/channel/UCN-0Sg068y9jyEZrJitS1nw'
target='_blank' alt='Youtube' aria-label='Youtube'><span class='wsite-social-item-inner'></span></a></
span>
<div style="height:0px;overflow:hidden"></div></div>
```

```
<div><div style="height: 20px; over
...
>
```

```
<div style="text-align:right;"><div style="height:10px;overflow:hidden"></div>
<span class="wsite-social wsite-social-default"><a class='first-child wsite-social-item wsite-social-fa
cebook' href='//facebook.com/kriptarium/' target='_blank' alt='Facebook' aria-label='Facebook'><span cl
ass='wsite-social-item-inner'></span></a><a class='wsite-social-item wsite-social-twitter' href='//twit
ter.com/kriptarium_' target='_blank' alt='Twitter' aria-label='Twitter'><span class='wsite-social-item-
inner'></span></a><a class='wsite-social-item wsite-social-linkedin' href='https://tr.linkedin.com/pub/
fatih-ozkaynak/64/852/5a3' target='_blank' alt='Linkedin' aria-label='Linkedin'><span class='wsite-soci
al-item-inner'></span></a><a class='wsite-social-item wsite-social-mail' href='mailto:iletisim@kriptari
um.com' target='_blank' alt='Mail' aria-label='Mail'><span class='wsite-social-item-inner'></span></a><
a class='wsite-social-item wsite-social-youtube' href='https://www.youtube.com/channel/UCN-0Sg068y9jyEZ
rJitS1nw' target='_blank' alt='Youtube' aria-label='Youtube'><span class='wsite-social-item-inner'></sp
an></a><a class='last-child wsite-social-item wsite-social-instagram' href='//instagram.com/kriptarium_
/' target='_blank' alt='instagram' aria-label='instagram'><span class='wsite-social-item-inner'></span>
```



```
</a></span>
<div style="height:0px;overflow:hidden"></div></div>

<div class="paragraph" style="
...
```

Remedy

- Add `rel=noopener` to the links to 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
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

6. Cookie Not Marked as HttpOnly

LOW



1

CONFIRMED



1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

6.1. <http://www.kriptarium.com/>

CONFIRMED

Identified Cookie(s)

- language
- is_mobile

Cookie Source

- HTTP Header

Request

GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-AHTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com

Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/

Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
...
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. *(After these changes javascript code will not be able to read cookies.)*

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as [XSS Tunnel](#) to bypass HTTPOnly protection.

External References

- [Netsparker - Security Cookies - HTTPOnly Flag](#)
- [OWASP HTTPOnly Cookies](#)
- [MSDN - ASP.NET HTTPOnly Cookies](#)



CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

7. Insecure Frame (External)

LOW



1

CONFIRMED



1

Netsparker identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the `sandbox` attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox` attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

- allow-same-origin will not treat it as a unique origin.
- allow-top-navigation will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- allow-forms will allow form submissions from inside the iframe.
- allow-popups will allow popups.
- allow-scripts will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

7.1. <http://www.kriptarium.com/304leti351im.html>

CONFIRMED

Frame Source(s)

- <http://www.weebly.com/weebly/apps/generateMap.php?map=google&elementid=220376965441473536&ineditor=0&control=3&width=auto&height=250px&overviewmap=0&scalecont>

Parsing Source

- DOM Parser

Request

```
GET /304leti351im.html HTTP/1.1
Host: www.kriptarium.com
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
Cookie: is_mobile=0; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906441.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; language=en
Referer: http://www.kriptarium.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 500,0141 Total Bytes Received : 42591 Body Length : 42159 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:07:29 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 10001
X-UA-Compatible: IE=edge,chrome=1
X-Host: grn13.sf2p.intern.weebly.net
ETag: W/"933e4765d4dc7ee2e9cf461e6befa74e-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:07:29 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head>
<title>&#304;leti&#351;im - Kriptarium</title><meta property="og:site_name" content="Kriptarium" />
<meta property="og:title" content="&#304;leti&#351;im" />
<meta property="og:description" content="Ürün ve hizmetlerimizi geliştirebilmemiz için görüş ve önerileriniz bizim için son derece önemlidir. Hizmet ve ürünler ile ilgili görüş/öneri ve şikayetlerinizi aşağıdaki..." />
<meta property="og:image" content="http://www.kriptarium.com/uploads/4/1/0/0/41002523/published/267656.jpg?1628198633" />
<meta property="og:url" content="http://www.kriptarium.com/304leti351im.html" />

<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/sites.css?buildTime=1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=1659481470" media="screen,projection" />
<link rel="stylesheet" type="text/css" href="/files/main_style.css?1659537024" title="wsite-theme-css" />

<link href="//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subset=latin,latin-ext" rel="stylesheet" type="text/css" />
<link href="//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subset=latin,latin-ext" rel="stylesheet" type="text/css" />
...
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of seamlessattribute and allow-top-navigation, allow-popupsand allow-scriptsin sandbox attribute.

External References

- [HTML5 Security Cheat Sheet](#)

Remedy References

- [How to Safeguard your Site with HTML5 Sandbox](#)
- [Play safely in sandboxed IFrames](#)



CLASSIFICATION

OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

8. Missing Content-Type Header

LOW



1

Netsparker detected a missing Content-Type header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Vulnerabilities

8.1. <http://www.kriptarium.com/sitemap.xml.gz>

Certainty



Request

```
GET /sitemap.xml.gz HTTP/1.1
Host: www.kriptarium.com
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
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906463.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; language=en
Referer: http://www.kriptarium.com/sitemap.xml.gz
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 265,7229 Total Bytes Received : 258 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Content-Length: 0
X-UA-Compatible: IE=edge,chrome=1
X-Host: grn139.sf2p.intern.weebly.net
ETag: W/"d41d8cd98f00b204e9800998ecf8427e"
Date: Sun, 07 Aug 2022 21:08:05 GMT
Vary: X-W-SSL,User-Agent
Cache-Control: public
```

Remedy

1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

```
Content-Type: text/html
```

2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

```
X-Content-Type-Options: nosniff
```

External References

- [MIME Sniffing: feature or vulnerability?](#)
- [X-Content-Type-Options HTTP Header](#)



CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

9. 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

9.1. <http://www.kriptarium.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head>
<title>Kriptarium - Ana Sayfa</title><meta property="og:site_name" content="Kriptarium" />
<meta property="og:title" content="Kriptarium" />
<meta property="og:description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta property="og:image" content="http://www.kriptarium.com/uploads/4/1/0/0/41002523/published/267656.
jpg?1628198633" />
<meta property="og:url" content="http://www.kriptarium.com/" />

<meta name="description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta name="keywords" content="kriptoloji, bilgi güvenliği, yazılım, biyometrik güvenlik, mobil çözümler, e-ticaret uygulamaları" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/sites.css?
buildTime=1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=16594
81470" media="screen,projection" />
<link rel="stylesheet" type="text/css" href="/files/main_style.css?1659537024" title="wsite-theme-css"
/>

<link href='//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subse
t=latin,latin-ext' rel='stylesheet' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Open+Sans:4
...
```

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: DENYIt completely denies to be loaded in frame/iframe.
 - X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
 - X-Frame-Options: ALLOW-FROM URLIt 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
SANS Top 25	693
CAPEC	103
ISO27001	A.14.2.5

10. 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**: Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to `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` in 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 ends 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 this extra layer of security.

Vulnerabilities

10.1. <http://www.kriptarium.com/>

Certainty

Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```


Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head>
<title>Kriptarium - Ana Sayfa</title><meta property="og:site_name" content="Kriptarium" />
<meta property="og:title" content="Kriptarium" />
<meta property="og:description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta property="og:image" content="http://www.kriptarium.com/uploads/4/1/0/0/41002523/published/267656.
jpg?1628198633" />
<meta property="og:url" content="http://www.kriptarium.com/" />

<meta name="description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta name="keywords" content="kriptoloji, bilgi güvenliği, yazılım, biyometrik güvenlik, mobil çözümler, e-ticaret uygulamaları" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/sites.css?
buildTime=1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=16594
81470" media="screen,projection" />
<link rel="stylesheet" type="text/css" href="/files/main_style.css?1659537024" title="wsite-theme-css"
/>

<link href='//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subse
t=latin,latin-ext' rel='stylesheet' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Open+Sans:4
...
```

Actions to Take

- Enable CSP on your website by sending the Content-Security-Policyin 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-Policyin 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

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

11. Expect-CT Not Enabled

BEST PRACTICE



1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissued certificates to be used.

Vulnerabilities

11.1. <https://www.kriptarium.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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
Connection: Keep-Alive
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906572.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; language=en
Referer: https://www.kriptarium.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1187,55 Total Bytes Received : 691 Body Length : 350 Is Compressed : No

```
HTTP/1.1 301 Moved Permanently
Server: Apache
Content-Length: 350
Connection: Keep-Alive
X-UA-Compatible: IE=edge,chrome=1
X-Host: grn69.sf2p.intern.weebly.net
Content-Type: text/html; charset=UTF-8
Location: http://www.kriptarium.com/
Keep-Alive: timeout=10, max=71
Date: Sun, 07 Aug 2022 21:09:49 GMT
Vary: X-W-SSL,User-Agent

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='http://www.kriptarium.com/'" />

<title>Redirecting to http://www.kriptarium.com/</title>
</head>
<body>
Redirecting to <a href="http://www.kriptarium.com/">http://www.kriptarium.com/</a>.
</body>
</html>
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

External References

- [Expect-CT Extension for HTTP](#)
- [Expect-CT HTTP Header](#)

- [Expect-CT Header](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

12. Missing X-XSS-Protection Header

BEST PRACTICE



1

Netsparker detected a missing X-XSS-Protectionheader 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

12.1. <http://www.kriptarium.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head>
<title>Kriptarium - Ana Sayfa</title><meta property="og:site_name" content="Kriptarium" />
<meta property="og:title" content="Kriptarium" />
<meta property="og:description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta property="og:image" content="http://www.kriptarium.com/uploads/4/1/0/0/41002523/published/267656.
jpg?1628198633" />
<meta property="og:url" content="http://www.kriptarium.com/" />

<meta name="description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta name="keywords" content="kriptoloji, bilgi güvenliği, yazılım, biyometrik güvenlik, mobil çözümler, e-ticaret uygulamaları" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/sites.css?
buildTime=1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=16594
81470" media="screen,projection" />
<link rel="stylesheet" type="text/css" href="/files/main_style.css?1659537024" title="wsite-theme-css"
/>

<link href='//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subse
t=latin,latin-ext' rel='stylesheet' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Open+Sans:4
...
```

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

SANS Top 25	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5

13. 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

13.1. <http://www.kriptarium.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head>
<title>Kriptarium - Ana Sayfa</title><meta property="og:site_name" content="Kriptarium" />
<meta property="og:title" content="Kriptarium" />
<meta property="og:description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta property="og:image" content="http://www.kriptarium.com/uploads/4/1/0/0/41002523/published/267656.
jpg?1628198633" />
<meta property="og:url" content="http://www.kriptarium.com/" />

<meta name="description" content="Bilgi Güvenliği ve Kriptoloji Çözümleri" />
<meta name="keywords" content="kriptoloji, bilgi güvenliği, yazılım, biyometrik güvenlik, mobil çözümler, e-ticaret uygulamaları" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/sites.css?
buildTime=1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=16594
81470" media="screen,projection" />
<link rel="stylesheet" type="text/css" href="/files/main_style.css?1659537024" title="wsite-theme-css"
/>

<link href='//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subse
t=latin,latin-ext' rel='stylesheet' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Open+Sans:4
...
```

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
SANS Top 25	200
ISO27001	A.14.2.5

14. SameSite Cookie Not Implemented

BEST PRACTICE



1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

14.1. <http://www.kriptarium.com/>

Identified Cookie(s)

- language
- is_mobile

Cookie Source

- HTTP Header

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-AHTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com

Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/

Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
...
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...` attribute to the `Set-Cookie` header. There are three possible values for the `SameSite` attribute:

- **Lax:** In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- **Strict:** In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- **None:** In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None` must also specify the `Secure` attribute to transfer them via a secure context. Setting a `SameSite=None` cookie without the `Secure` attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- [Security Cookies - SameSite Attribute - Netsparker](#)
- [Using the Same-Site Cookies Attribute to Prevent CSRF Attacks](#)
- [Same-site Cookies](#)
- [Preventing CSRF with the same-site cookie attribute](#)
- [SameSite cookies explained](#)
- [Get Ready for New SameSite=None; Secure Cookie Settings](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

15. 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

15.1. <http://www.kriptarium.com/>

Identified Sub Resource(s)

- <http://cdn2.editmysite.com/css/sites.css?buildTime=1659481470>
- <http://cdn2.editmysite.com/css/old/fancybox.css?1659481470>
- <http://cdn2.editmysite.com/css/social-icons.css?buildtime=1659481470>
- <http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subset=latin,latin-ext>
- <http://fonts.googleapis.com/css?family=Montserrat:400,700&subset=latin,latin-ext>
- <https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js>
- <http://cdn2.editmysite.com/js/lang/tr/stl.js?buildTime=1659481470&>
- <http://cdn2.editmysite.com/js/site/main.js?buildTime=1659481470>
- <http://cdn2.editmysite.com/js/site/main-customer-accounts-site.js?buildTime=1659481470>

Certainty

Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```


Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-A
...
venlik, mobil çözümler, e-ticaret uygulamaları" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/sites.css?
buildTime=1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1659481470" />
<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=16594
81470" media="screen,projection" />
<link rel="stylesheet" type="text/css" href="/files/main_style.css?1659537024" title="wsite-theme-css"
/>

<link href='//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subse
t=latin,latin-ext' rel='stylesheet' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,700,400italic,700italic&subse
t=latin,latin-ext' rel='stylesheet' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Montserrat:400,700&subset=latin,latin-ext' rel='styleshee
t' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Montserrat:400,700&subset=latin,latin-ext' rel='styleshee
t' type='text/css' />
<link href='//fonts.googleapis.com/css?family=Montserrat:400,700&subset=
...
t-title {}
.wsite-product .wsite-product-price a {}
}</style>

<script>
var STATIC_BASE = '//cdn1.editmysite.com/';
var ASSETS_BASE = '//cdn2.editmysite.com/';
var STYLE_PREFIX = 'wsite';
</script>
<script src='https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js'></script>
```

```

<script type="text/javascript" src="//cdn2.editmysite.com/js/lang/tr/stl.js?buildTime=1659481470"></script>
<script src="//cdn2.editmysite.com/js/site/main.js?buildTime=1659481470"></script><script type="text/javascript">
function initCustomerAccountsModels() {
(function(){_W.setup_rpc({"url":"\\ajax\\api\\JsonRPC\\CustomerAccounts\\","actions":{"CustomerAccounts":[{"name":"login"}]}
...
7250"></script>
<script src="/files/theme/jquery.loadTemplate.min.js?1620177250"></script>
<script src="/files/theme/custom.js?1620177250"></script>
<div id="customer-accounts-app"></div>
<script src="//cdn2.editmysite.com/js/site/main-customer-accounts-site.js?buildTime=1659481470"></script>

<script type="text/javascript">
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-7870337-1']);
_gaq.push(['_setDomainName', 'none']);
_gaq.push(['_setAllowLinker', true]);

(function() {
...

```

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/ztc4Z1RqWjqIuvf6RX5yb/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

SANS Top 25

[16](#)

WASC

[15](#)

ISO27001

[A.14.2.5](#)

16. Apache Web Server Identified

INFORMATION ⓘ

1

Netsparker identified a web server (Apache) 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://www.kriptarium.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-AHTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encod
...
```

External References

- [Apache ServerTokens Directive](#)



CLASSIFICATION

SANS Top 25	200
WASC	13
OWASP Proactive Controls	C7
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. Email Address Disclosure

INFORMATION ⓘ

1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

17.1. <http://www.kriptarium.com/>

Email Address(es)

- iletisim@kriptarium.com

Certainty



Request

```
GET / HTTP/1.1
Host: www.kriptarium.com
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/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```


Response

Response Time (ms) : 6530,0177 Total Bytes Received : 39406 Body Length : 38914 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: is_mobile=0; path=/; domain=www.kriptarium.com
Set-Cookie: language=en; expires=Sun, 21-Aug-2022 21:05:08 GMT; Max-Age=1209600; path=/
Server: Apache
Content-Length: 9037
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu106.sf2p.intern.weebly.net
ETag: W/"98dd2ec8ae03d9a1a206d25607ec8c0b-gzip"
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:05:08 GMT
Vary: X-W-SSL,Accept-Encoding,User-A
...
c_profile_result-card_subtitle-click' target='_blank' alt='Linkedin' aria-label='Linkedin'><span class
='wsite-social-item-inner'></span></a><a class='wsite-social-item wsite-social-mail' href='mailto:iletisim@kriptarium.com' target='_blank' alt='Mail' aria-label='Mail'><span class='wsite-social-item-inner'>
</span></a><a class='last-child wsite-social-item wsite-social-youtube' href='https://www.youtube.com/c
hannel/UCN-0
...
in.com/pub/fatih-özkanak/64/852/5a3' target='_blank' alt='Linkedin' aria-label='Linkedin'><span class
='wsite-social-item-inner'></span></a><a class='wsite-social-item wsite-social-mail' href='mailto:iletisim@kriptarium.com' target='_blank' alt='Mail' aria-label='Mail'><span class='wsite-social-item-inner'>
</span></a><a class='wsite-social-item wsite-social-youtube' href='https://www.youtube.com/channel/UCN-
0Sg068y9jyEZ
...
```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- [Wikipedia - Email Spam](#)



CLASSIFICATION

SANS Top 25	200
CAPEC	118
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.9.4.1

CVSS 3.0 SCORE

Base	5,3 (Medium)
Temporal	5,3 (Medium)
Environmental	5,3 (Medium)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	5,3 (Medium)
Temporal	5,3 (Medium)
Environmental	5,3 (Medium)

CVSS Vector String

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



18. Forbidden Resource

INFORMATION ⓘ

1

CONFIRMED ⓘ

1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

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

Vulnerabilities

18.1. <http://www.kriptarium.com/uumlruumlner.html>

CONFIRMED

Request

```
POST /uumlruumlner.html HTTP/1.1
Host: www.kriptarium.com
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
Content-Length: 124
Content-Type: application/xml
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionali
tyCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; _sn
ow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906463.1659906368.7e8c1260-78c8-4747-a
2ce-a0147847ed33; _snow_ses.fc27=*; language=en
Referer: http://www.kriptarium.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 577,6975 Total Bytes Received : 216 Body Length : 72 Is Compressed : No

HTTP/1.1 403 Forbidden

Server: Apache

Content-Length: 72

Content-Type: text/html; charset=iso-8859-1

Date: Sun, 07 Aug 2022 21:08:02 GMT

This site is currently undergoing maintenance, and will be back shortly.



CLASSIFICATION

OWASP Proactive Controls

[C8](#)

ISO27001

[A.8.1.1](#)

19. Nginx Web Server Identified

INFORMATION ⓘ

1

Netsparker identified a web server (Nginx) 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

19.1. <http://www.kriptarium.com/files/theme/>

Certainty



Request

```
GET /files/theme/ HTTP/1.1
Host: www.kriptarium.com
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
Cookie: is_mobile=0; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906441.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; language=en
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 671,8805 Total Bytes Received : 3948 Body Length : 3739 Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: nginx
Connection: keep-alive
Content-Length: 3739
Content-Type: text/html
Date: Sun, 07 Aug 2022 21:07:29 GMT
ETag: "61c39c46-e9b"
X-Host: blu50.HTTP/1.1 404 Not Found
Server: nginx
Connection: keep-alive
Content-Length: 3739
Content-Type: text/html
Date: Sun, 07 Aug 2022 21:07:29 GMT
ETag: "61c39c46-e9b"
X-Host: blu50.sf2p.intern.weebly.net

<!DOCTYPE html PUBLIC "-//W3
...
```



CLASSIFICATION

SANS Top 25	200
WASC	13
OWASP Proactive Controls	C7
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

20. Robots.txt Detected

INFORMATION

1

CONFIRMED

1

Netsparker detected a Robots.txt file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

20.1. <http://www.kriptarium.com/robots.txt>

CONFIRMED

Interesting Robots.txt Entries

- Sitemap: <http://www.kriptarium.com/sitemap.xml>
- Disallow: /
- Disallow: /ajax/
- Disallow: /apps/

Request

GET /robots.txt HTTP/1.1
Host: www.kriptarium.com
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
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906463.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; language=en
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

Response

Response Time (ms) : 386,2587 Total Bytes Received : 471 Body Length : 130 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Content-Length: 111
X-UA-Compatible: IE=edge,chrome=1
X-Host: grn40.sf2p.intern.weebly.net
ETag: W/"763cb23a01f99f6fa2b1ab6c67fc8e8a-gzip"
Content-Type: text/plain; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:08:05 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: public
```

Sitemap: <http://www.kriptarium.com/sitemap.xml>

```
User-agent:NerdyBot
Disallow:/
```

```
User-agent:*
Disallow:/ajax/
Disallow:/apps/
```

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.

`Robots.txt` is only used to instruct search robots which resources should be indexed and which ones are not.

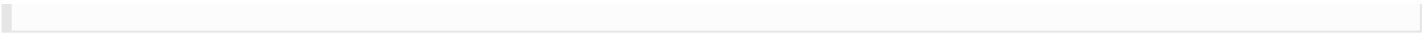
The following block can be used to tell the crawler to index files under `/web/` and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag` can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```



By using X-Robots-Tag you don't have to list the these files in your Robots.txt.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. X-Robots-Tag resolves this issue as well.


For Apache, the following snippet can be put into httpd.conf or an .htaccess file to restrict crawlers to index multimedia files without exposing them in Robots.txt

```
<Files ~ "\.pdf$">
# Don't index PDF files.
Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
#Don't index image files.
Header set X-Robots-Tag "noindex"
</Files>
```

External References

- [What Content Is Not Crawled? - Google](#)
- [How Search organizes information](#)
- [X-Robots-Tag: A Simple Alternate For Robots.txt and Meta Tag](#)

 CLASSIFICATION	
OWASP Proactive Controls	C7
ISO27001	A.18.1.3

21. Sitemap Detected

INFORMATION ⓘ

1

Netsparker detected a sitemap file on the target website.

Impact

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

Vulnerabilities

21.1. <http://www.kriptarium.com/sitemap.xml>

Certainty

Request

```
GET /sitemap.xml HTTP/1.1
Host: www.kriptarium.com
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
Cookie: is_mobile=0; cookie-consent=%7B%22allowStrictlyNecessaryCookies%22%3Atrue%2C%22allowFunctionalityCookies%22%3Atrue%2C%22allowPerformanceCookies%22%3Atrue%2C%22allowTargetingCookies%22%3Atrue%7D; _snow_id.fc27=ac06c639-73a9-4e40-bdb0-008d7c402301.1659906368.1.1659906463.1659906368.7e8c1260-78c8-4747-a2ce-a0147847ed33; _snow_ses.fc27=*; language=en
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 712,8098 Total Bytes Received : 4719 Body Length : 4380 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Content-Length: 461
X-UA-Compatible: IE=edge,chrome=1
X-Host: blu69.sf2p.intern.weebly.net
ETag: W/"f3ffb9cc94192a6d17f79db92aa0bfad2-gzip"
Content-Type: text/xml; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:07:54 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-
...
pe: text/xml; charset=UTF-8
Content-Encoding:
Date: Sun, 07 Aug 2022 21:07:54 GMT
Vary: X-W-SSL,Accept-Encoding,User-Agent
Cache-Control: public

<?xml version="1.0" encoding="UTF-8"?>
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
<url>
<loc>http://www.kriptarium.com/dersler.html</loc>
<lastmod>2022-08-03T14:30:24+00:00</lastmod>
</url>
<url>
<loc>http://www.kriptarium.com/algorithm.html</loc>
<lastmod>2
...
```



CLASSIFICATION

OWASP Proactive Controls

[C7](#)

ISO27001

[A.18.1.3](#)

Show Scan Detail

Enabled Security Checks

: Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
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 Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
Local File Inclusion,
Login Page Identifier,
Mixed Content,
Open Redirection,
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 (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 : (log|sign)\-?(out|off)
exit
endsession
gtm\.js
WebResource\.axd
ScriptResource\.axd

Authentication : None

Scheduled : No

Additional Website(s) : None

This report created with 5.8.1.28119-master-bca4e4e
<https://www.netsparker.com>