Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

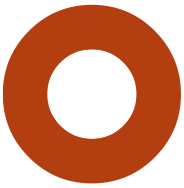
Scan Detail

Target	http://10.22.169.100:80/
Scan Type	Full Scan
Start Time	Nov 4, 2025, 3:12:12 PM GMT
Scan Duration	11 minutes
Requests	22570
Average Response Time	1ms
Maximum Response Time	122782ms
Application Build	v24.6.240626115
Authentication Profile	-

0	2	14	2	5
Critical	High	Medium	Low	Informational

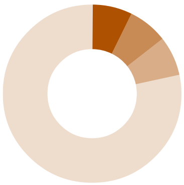
Severity	Vulnerabilities	Instances
Critical	0	0
High	1	2
Medium	14	14
Low	2	2
Informational	4	5
Total	21	23

High Severity



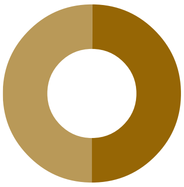
		Instances
■	Cross-site Scripting	2

Medium Severity



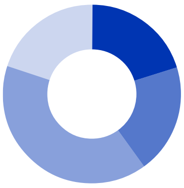
		Instances
■	Apache httpOnly cookie disclosure	1
■	Apache httpd remote denial of service	1
■	Bootstrap Improper Neutralization of Input...	1
■	Others	11

Low Severity



		Instances
■	Apache mod_negotiation filename brutefo...	1
■	[Possible] Internal IP Address Disclosure	1

Informational



		Instances
■	Content Security Policy (CSP) Not Implem...	1
■	Generic Email Address Disclosure	1
■	Outdated JavaScript libraries	2
■	Others	1

Impacts

SEVERITY	IMPACT
High	2 Cross-site Scripting
Medium	1 Apache httpd remote denial of service
Medium	1 Apache httpOnly cookie disclosure
Medium	1 Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 Insecure HTTP Usage
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 JQuery Prototype Pollution Vulnerability
Medium	1 Select2 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 SSL/TLS Not Implemented
Medium	1 Test CGI script leaking environment variables
Medium	1 Vulnerable JavaScript libraries
Low	1 [Possible] Internal IP Address Disclosure
Low	1 Apache mod_negotiation filename bruteforcing

SEVERITY	IMPACT	
ⓘ Informational	1	Content Security Policy (CSP) Not Implemented
ⓘ Informational	1	Generic Email Address Disclosure

Cross-site Scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

http://10.22.169.100/cgi-bin/

URI was set to **<isindex type=image src=1 onerror=OwjV(9651)>**
The input is reflected inside a text element.

Request

```
GET /cgi-
bin/test.cgi/%3C%69%73%69%6E%64%65%78%20%74%79%70%65%3D%69%6D%61%67%65%20%73%72%63%3D%31%20%6F%6E%65
%72%72%6F%72%3D%4F%77%6A%56%28%39%36%35%31%29%3E HTTP/1.1
Referer: http://10.22.169.100/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

http://10.22.169.100/cgi-bin/test.cgi Verified

HTTP Header input **Referer** was set to **https://www.google.com/search?hl=en&q=testing'"()&%<zzz><ScRiPt >u4gs(9293)</ScRiPt>**

Request

```
GET /cgi-bin/test.cgi HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing'"()&%<zzz><ScRiPt >u4gs(9293)</ScRiPt>
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

Cross-site Scripting (XSS) Attack - Acunetix
https://www.acunetix.com/websitesecurity/cross-site-scripting/

Types of XSS - Acunetix
https://www.acunetix.com/websitesecurity/xss/

XSS Filter Evasion Cheat Sheet
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Excess XSS, a comprehensive tutorial on cross-site scripting
https://excess-xss.com/

Cross site scripting
https://en.wikipedia.org/wiki/Cross-site_scripting

Apache httpd remote denial of service

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Impact

Remote Denial of Service

http://10.22.169.100/

Version detected: 2.2.17 .

Recommendation

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

References

CVE-2011-3192
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

Apache HTTPD Security ADVISORY
http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E

Apache httpd Remote Denial of Service (memory exhaustion)
https://www.exploit-db.com/exploits/17696

Apache httpOnly cookie disclosure

Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Affected Apache versions (up to 2.0.21).

Impact

Information disclosure.

http://10.22.169.100/

Pattern found:

```
<pre>
Cookie: testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Request

```
GET / HTTP/1.1
Cookie:
testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Upgrade Apache 2.x to the latest version. Apache 2.2.22 is the first version that fixed this issue.

References

Fixed in Apache httpd 2.2.22
http://httpd.apache.org/security/vulnerabilities_22.html

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
https://www.securityfocus.com/bid/51706

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.

Impact

http://10.22.169.100/

bootstrap.js v4.0.0-beta-4.0.0-beta

References

CVE-2018-14040
https://nvd.nist.gov/vuln/detail/CVE-2018-14040

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.

Impact

http://10.22.169.100/

bootstrap.js v4.0.0-beta-4.0.0-beta

References

CVE-2018-14042
https://nvd.nist.gov/vuln/detail/CVE-2018-14042

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-target property of scrollspy.

Impact

http://10.22.169.100/

bootstrap.js v4.0.0-beta-4.0.0-beta

References

CVE-2018-14041
https://nvd.nist.gov/vuln/detail/CVE-2018-14041

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://10.22.169.100/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

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.

Impact

http://10.22.169.100/

jquery v3.2.1-3.2.1

References

CVE-2020-11023
https://nvd.nist.gov/vuln/detail/CVE-2020-11023

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

Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.

Impact

http://10.22.169.100/

jquery v3.2.1-3.2.1

References

CVE-2020-23064
https://nvd.nist.gov/vuln/detail/CVE-2020-23064

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.

Impact

http://10.22.169.100/

jquery v3.2.1-3.2.1

References

CVE-2020-11022
https://nvd.nist.gov/vuln/detail/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.

Impact

http://10.22.169.100/

jquery v3.2.1-3.2.1

References

CVE-2019-11358
https://nvd.nist.gov/vuln/detail/CVE-2019-11358

Select2 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Select2 through 4.0.5, as used in Snipe-IT and other products, rich selectlists allow XSS. This affects use cases with Ajax remote data loading when HTML templates are used to display listbox data.

Impact

http://10.22.169.100/

select2 v4.0.3-4.0.3

References

CVE-2016-10744
https://nvd.nist.gov/vuln/detail/CVE-2016-10744

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

http://10.22.169.100/ Verified

Request

```
GET / HTTP/1.1
Referer: http://10.22.169.100/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Test CGI script leaking environment variables

A test CGI (Common Gateway Interface) script was found on this server. The response page returned by this CGI script is leaking a list of server environment variables.

Environment variables are a set of dynamic named values that can affect the way running processes will behave on a computer. For example, an environment variable with a standard name can designate the location that a particular computer system uses to store temporary files but this may vary from one computer system to another.

Impact

Environment variables may leak sensitive information to a potential attacker. An attacker can use this information to conduct further attacks.

http://10.22.169.100/

Filename: **/cgi-bin/test.cgi**

Request

```
GET /cgi-bin/test.cgi HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Restrict access to this CGI file or remove it from your system.

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

http://10.22.169.100/ Confidence: 95%

- jQuery 3.2.1
  - URL: http://10.22.169.100/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: 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. / 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. / jQuery 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.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request

```
GET / HTTP/1.1
Referer: http://10.22.169.100/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

[Possible] Internal IP Address Disclosure

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

Impact

Possible sensitive information disclosure.

http://10.22.169.100/

Pages with internal IPs:

- http://10.22.169.100/cgi-bin/test.cgi
  10.22.169.33

Request

```
GET /cgi-bin/test.cgi HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

Apache mod_negotiation filename bruteforcing

mod_negotiation is an Apache module responsible for selecting the document that best matches the clients capabilities, from one of several available documents. If the client provides an invalid Accept header, the server will respond with a 406 Not Acceptable error containing a pseudo directory listing. This behaviour can help an attacker to learn more about his target, for example, generate a list of base names, generate a list of interesting extensions, look for backup files and so on.

Impact

Possible information disclosure: directory listing, filename bruteforcing, backup files.

http://10.22.169.100/

Pattern found:

```
<title>406 Not Acceptable</title>
```

Request

```
GET /index HTTP/1.1
Accept: ofmosdfo/gskc
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Disable the MultiViews directive from Apache's configuration file and restart Apache.
You can disable MultiViews by creating a **.htaccess** file containing the following line:

```
Options -Multiviews
```

References

mod_negotiation: directory listing, filename bruteforcing
http://www.ush.it/2008/07/02/mod_negotiation-directory-listing-filename-bruteforcing/

Multiviews Apache, Accept Requests and free listing
http://www.wisec.it/sectou.php?id=4698ebdc59d15

Apache Module mod_negotiation
http://httpd.apache.org/docs/2.2/mod/mod_negotiation.html

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://10.22.169.100/

Paths without CSP header:

- http://10.22.169.100/
- http://10.22.169.100/cgi-bin/test.cgi
- http://10.22.169.100/index
- http://10.22.169.100/index.html

Request

```
GET / HTTP/1.1
Referer: http://10.22.169.100/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Generic Email Address Disclosure

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

http://10.22.169.100/

Emails found:

- http://10.22.169.100/
  ex@abc.xyz
- http://10.22.169.100/index
  ex@abc.xyz
- http://10.22.169.100/index.html
  ex@abc.xyz

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](https://en.wikipedia.org/wiki/Anti-spam_techniques)
https://en.wikipedia.org/wiki/Anti-spam_techniques

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

http://10.22.169.100/ Confidence: 95%

- **bootstrap.js 4.0.0-beta**
  - URL: http://10.22.169.100/vendor/bootstrap/js/bootstrap.min.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
GET /vendor/bootstrap/js/bootstrap.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

http://10.22.169.100/ Confidence: 95%

- **Select2 4.0.3**
  - URL: http://10.22.169.100/vendor/select2/select2.min.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/select2/select2/tags

Request

```
GET /vendor/select2/select2.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

http://10.22.169.100/

Locations without Permissions-Policy header:

- http://10.22.169.100/
- http://10.22.169.100/images/
- http://10.22.169.100/index
- http://10.22.169.100/cgi-bin/test.cgi
- http://10.22.169.100/index.html
- http://10.22.169.100/fonts/font-awesome-4.7.0/fonts/
- http://10.22.169.100/images/icons/
- http://10.22.169.100/js/

- http://10.22.169.100/css/
- http://10.22.169.100/cgi-bin/
- http://10.22.169.100/fonts/Lato/
- http://10.22.169.100/fonts/
- http://10.22.169.100/fonts/Poppins/
- http://10.22.169.100/vendor/
- http://10.22.169.100/fonts/font-awesome-4.7.0/
- http://10.22.169.100/fonts/font-awesome-4.7.0/css/
- http://10.22.169.100/vendor/animate/
- http://10.22.169.100/vendor/countdowntime/
- http://10.22.169.100/vendor/jquery/
- http://10.22.169.100/vendor/tilt/
- http://10.22.169.100/vendor/bootstrap/

Request

```
GET / HTTP/1.1
Referer: http://10.22.169.100/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Host: 10.22.169.100
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

Coverage

- http://10.22.169.100
  - Inputs
    - GET email
  - cgi-bin
    - test.cgi
  - css
    - main.css
    - util.css
  - fonts
    - font-awesome-4.7.0
      - css
        - font-awesome.min.css
      - fonts
    - Lato
    - Poppins
  - images
    - icons
  - js
    - main.js
  - vendor
    - animate
      - animate.css
    - bootstrap
      - css
        - bootstrap.min.css
      - js
        - bootstrap.min.js
        - popper.js
    - countdowntime
      - countdowntime.js
      - moment-timezone-with-data.min.js

        - moment-timezone.min.js
        - moment.min.js
    - jquery
        - jquery-3.2.1.min.js
    - select2
        - select2.min.css
        - select2.min.js
    - tilt
        - tilt.jquery.min.js
- index
    - Inputs
        - GET email
- index.html
    - Inputs
        - GET email
- robots.txt