Acunetix
by Invicti

Compliance Report

OWASP TOP 10 2021

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2021 Project document, that can be found at http://www.owasp.org.

http://192.168.1.8:8593/

Scan Type	Critical / High / Medium Risk
Start Time	Nov 1, 2025, 6:25:18 AM GMT
Scan Duration	13 minutes

Requests	42890
Average Response Time	1ms
Maximum Response Time	34537ms
Discovered Hosts	https://fonts.googleapis.com
Application Build	v24.6.240626115
Authentication Profile	-

http://192.168.1.8:80/

Scan Type	Critical / High / Medium Risk
Start Time	Nov 1, 2025, 6:25:18 AM GMT
Scan Duration	4 minutes

Requests	2260
Average Response Time	1ms
Maximum Response Time	29895ms
Application Build	v24.6.240626115
Authentication Profile	-

http://192.168.1.8:3128/

Scan Type	Critical / High / Medium Risk
Start Time	Nov 1, 2025, 6:25:18 AM GMT
Scan Duration	4 minutes

Requests	1639
Average Response Time	750ms
Maximum Response Time	34713ms
Application Build	v24.6.240626115
Authentication Profile	-

http://192.168.1.8:54787/

Scan Type	Critical / High / Medium Risk
Start Time	Nov 1, 2025, 6:25:19 AM GMT
Scan Duration	7 minutes

Requests	17043
Average Response Time	1ms
Maximum Response Time	30496ms
Application Build	v24.6.240626115
Authentication Profile	-

Compliance at a Glance

	CATEGORY
1	A01 Broken Access Control
6	A02 Cryptographic Failures
1	A03 Injection
0	A04 Insecure Design
4	A05 Security Misconfiguration
0	A06 Vulnerable and Outdated Components
4	A07 Identification and Authentication Failures
0	A08 Software and Data Integrity Failures
0	A09 Security Logging and Monitoring Failures
0	A10 Server-Side Request Forgery

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

A01 Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Directory traversal

This script is vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

CWE

CWE-22

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:P

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS3

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

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

http://192.168.1.8:8593/index.php

URL encoded GET input **book** was set to **../../../../../../../../../../../../../../etc/passwd**

File contents found:

```
root:x:0:0:root:/root:/bin/bash
```

Request

```
GET /index.php?book=../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Referer: http://192.168.1.8:8593/
Cookie: PHPSESSID=mfqbmiltq1jvoatr7he5aqi00f
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: 192.168.1.8:8593
Connection: Keep-alive
```

Recommendation

Your script should filter metacharacters from user input.

References

[Acunetix Directory Traversal Attacks](https://www.acunetix.com/websitesecurity/directory-traversal/)
https://www.acunetix.com/websitesecurity/directory-traversal/

A02 Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P

Base Score	5.5
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

http://192.168.1.8:54787/

Version detected: **PHP/7.3.14-1~deb10u1**.

http://192.168.1.8:8593/

Version detected: **PHP/7.3.14-1~deb10u1**.

Recommendation

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

References

[PHP Documentation: header_remove()](https://www.php.net/manual/en/function.header-remove.php)
https://www.php.net/manual/en/function.header-remove.php

[PHP Documentation: php.ini directive expose_php](https://www.php.net/manual/en/ini.core.php#ini.expose-php)
https://www.php.net/manual/en/ini.core.php#ini.expose-php

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.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

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

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

http://192.168.1.8:3128/

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:3128/
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: 192.168.1.8:3128
Connection: Keep-alive
```

http://192.168.1.8:54787/

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:54787/
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: 192.168.1.8:54787
Connection: Keep-alive
```

http://192.168.1.8:8593/

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:8593/
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: 192.168.1.8:8593
Connection: Keep-alive
```

http://192.168.1.8/

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8/
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: 192.168.1.8
Connection: Keep-alive
```

Recommendation

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

A03 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Local File Inclusion

This script is vulnerable to file inclusion attacks.

The script was found to reference and potentially retrieve files from user-specified locations. User input is not sufficiently validated or sanitized prior to being passed to the vulnerable script's include function.

CWE
CWE-20

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	Low

Impact

It is possible for a remote attacker to include a file from local or remote resources and/or execute arbitrary script code with the privileges of the web-server.

http://192.168.1.8:8593/index.php

URL encoded GET input **book** was set to **../../../../../../../../../../../../../../etc/shells**

Pattern found:

```
# /etc/shells:
```

Request

```
GET /index.php?book=../../../../../../../../../../../../../../etc/shells HTTP/1.1
Referer: http://192.168.1.8:8593/
Cookie: PHPSESSID=mfqbmiltq1jvoatr7he5aqi00f
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: 192.168.1.8:8593
Connection: Keep-alive
```

Recommendation

Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list.

For PHP, the option **allow_url_fopen** would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.

References

PHP - Using remote files
https://www.php.net/manual/en/features.remote-files.php

OWASP PHP Top 5
https://www.owasp.org/index.php/PHP_Top_5

Remote file inclusion
https://en.wikipedia.org/wiki/Remote_file_inclusion

A04 Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

No alerts in this category

A05 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securly configured, but they must be patched and upgraded in a timely fashion.

Insecure HTTP Usage

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

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None

Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

http://192.168.1.8:3128/

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: 192.168.1.8:3128
Connection: Keep-alive
```

http://192.168.1.8:54787/

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: 192.168.1.8:54787
Connection: Keep-alive
```

http://192.168.1.8:8593/

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: 192.168.1.8:8593
Connection: Keep-alive
```

http://192.168.1.8/

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: 192.168.1.8
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

A06 Vulnerable and Outdated Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

No alerts in this category

A07 Identification and Authentication Failures

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

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.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

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

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

http://192.168.1.8:3128/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:3128/
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: 192.168.1.8:3128
Connection: Keep-alive
```

http://192.168.1.8:54787/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:54787/
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: 192.168.1.8:54787
```

```
Connection: Keep-alive
```

http://192.168.1.8:8593/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:8593/
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: 192.168.1.8:8593
Connection: Keep-alive
```

http://192.168.1.8/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8/
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: 192.168.1.8
Connection: Keep-alive
```

Recommendation

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

A08 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

No alerts in this category

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category

A10 Server-Side Request Forgery

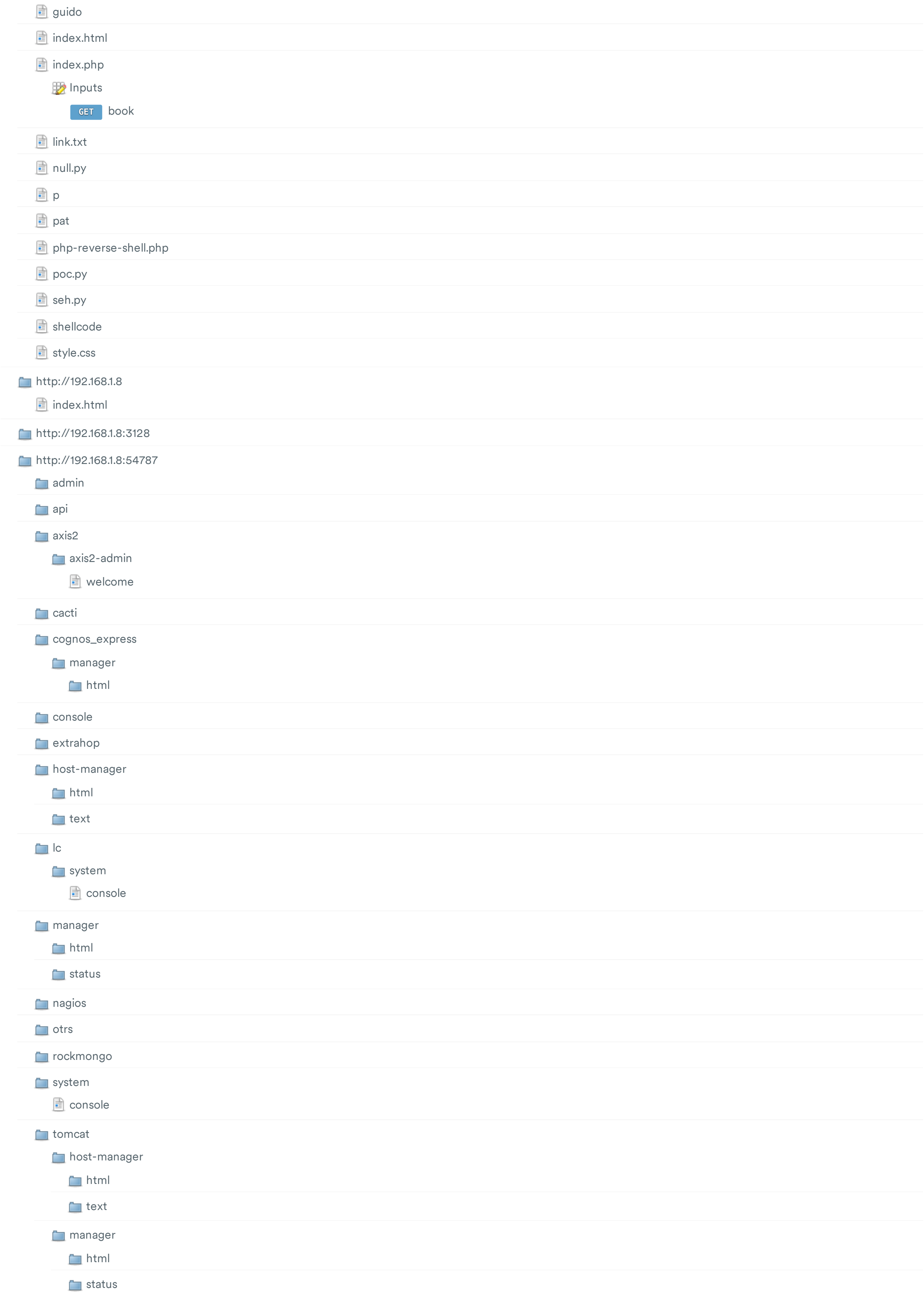
SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

No alerts in this category

Coverage

- http://192.168.1.8:8593
  - .BurpSuite
  - .cache
  - .config
  - .cpan
  - .dbus
  - .gnupg
  - .hashcat
  - .java
  - .john
  - .local
  - .mozilla
  - .msf4
  - .ngrok2
  - .ssh
  - .wine
  - .wpscan
  - admin
  - api
  - axis2
    - axis2-admin
      - welcome
  - binaries
  - cacti
  - cognos_express
    - manager
      - html
  - console
  - crottt
  - Desktop
  - dev
  - Documents
  - dotdotpwn
  - Downloads
  - Exploit-Dev
  - extrahop
  - host-manager
    - html
    - text
  - lc
    - system
      - console
  - manager
    - html
    - status
  - Music
  - nagios

```
otrs
Pictures
Public
rockmongo
Sublist3r
system
    console
Templates
tomcat
    host-manager
        html
        text
    manager
        html
        status
ui
    authentication
Videos
webtools
zabbix
.bash_history
.dmrc
.face
.ftp_history
.ICEauthority
.mysql_history
.nc_history
.profile
.selected_editor
.vboxclient-clipboard.pid
.vboxclient-display-svga.pid
.vboxclient-display.pid
.vboxclient-draganddrop.pid
.vboxclient-seamless.pid
.viminfo
.wget-hsts
.Xauthority
.xsession-errors
.xsession-errors.old
1.py
c0up.sh
cmd.pgif
cmd.pht
crash
crash_c
crash.c
crash.cpp
debug.cpp
dokan.c
```



- guido
- index.html
- index.php
  - Inputs
    - GET book
- link.txt
- null.py
- p
- pat
- php-reverse-shell.php
- poc.py
- seh.py
- shellcode
- style.css

- http://192.168.1.8
  - index.html
- http://192.168.1.8:3128
- http://192.168.1.8:54787
  - admin
  - api
  - axis2
    - axis2-admin
      - welcome
  - cacti
  - cognos_express
    - manager
      - html
  - console
  - extrahop
  - host-manager
    - html
    - text
  - lc
    - system
      - console
  - manager
    - html
    - status
  - nagios
  - otrs
  - rockmongo
  - system
    - console
  - tomcat
    - host-manager
      - html
      - text
    - manager
      - html
      - status

- ui
  - authentication
- webtools
- zabbix