Acunetix Website Audit

7 January, 2016

Web Application Security Consortium: Threat Classification

~ compliance report ~

Web Application Security Consortium: Threat Classification

compliance report

Description

The Web Security Threat Classification is a cooperative effort to clarify and organize the threats to the security of a web site. The members of the Web Application Security Consortium have created this project to develop and promote industry standard terminology for describing these issues. Application developers, security professionals, software vendors, and compliance auditors will have the ability to access a consistent language for web security related issues.

The Web Security Threat Classification will compile and distill the known unique classes of attack, which have presented a threat to web sites in the past.

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 the information in this report is taken from Web Application Security Consortium "Threat Classification" document, that can be found at http://www.webappsec.org/.

Scan

URL	**https://pulse:59980/index.php**
Scan date	07/01/2016 07:53:41
Duration	13 hours, 44 minutes
Profile	eurysco

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- Authentication: Brute Force (1.1)
  No alerts in this category
- Insufficient Authentication (1.2)
  No alerts in this category
- Weak Password Recovery Validation (1.3)
  No alerts in this category
- Credential/Session Prediction (2.1)
  No alerts in this category
- Insufficient Authorization (2.2)
  No alerts in this category
- Insufficient Session Expiration (2.3)
  No alerts in this category
- Session Fixation (2.4)
  No alerts in this category
- Content Spoofing (3.1)
  No alerts in this category

- Cross-site Scripting (3.2)
  - **No alerts in this category**
- Buffer Overflow (4.1)
  - **No alerts in this category**
- Format String Attack (4.2)
  - **No alerts in this category**
- LDAP Injection (4.3)
  - **No alerts in this category**
- OS Commanding (4.4)
  - **No alerts in this category**
- SQL Injection (4.5)
  - **No alerts in this category**
- SSI Injection (4.6)
  - **No alerts in this category**
- XPath Injection (4.7)
  - **No alerts in this category**
- Directory Indexing (5.1)
  - **No alerts in this category**
- Information Leakage (5.2)
  - **No alerts in this category**
- Path Traversal (5.3)
  - **No alerts in this category**
- Predictable Resource Location (5.4)
  - **No alerts in this category**
- Abuse of Functionality (6.1)
  - **No alerts in this category**
- Denial of Service (6.2)
  - **No alerts in this category**
- Insufficient Anti-automation (6.3)
  - **No alerts in this category**
- Insufficient Process Validation (6.4)
  - **No alerts in this category**

Compliance According to Categories: A Detailed Report

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

(1.1) Authentication: Brute Force

A Brute Force attack is an automated process of trial and error used to guess a person's username, password, credit-card number or cryptographic key.

Acunetix authentication tester can be used to bruteforce authentication schemes based either on HTTP protocol NTLM or Basic authentication or HTML form based authentication.

No alerts in this category.

(1.2) Insufficient Authentication

Insufficient Authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate. Web-based administration tools are a good example of web sites providing access to sensitive functionality. Depending on the specific online resource, these web applications should not be directly accessible without the user required to properly verify their identity.

To get around setting up authentication, some resources are protected by "hiding" the specific location and not linking the location into the main web site or other public places. However, this approach is nothing more than "Security Through Obscurity". Its important to understand that simply because a resource is unknown to an attacker, it still remains accessible directly through a specific URL. The specific URL could be discovered through a Brute Force probing for common file and directory locations (/admin for example), error messages, referrer logs, or perhaps documented in help files. These resources, whether they are content or functionality driven, should be adequately protected.

No alerts in this category.

(1.3) Weak Password Recovery Validation

Weak Password Recovery Validation is when a web site permits an attacker to illegally obtain, change or recover another user's password. Conventional web site authentication methods require users to select and remember a password or passphrase. The user should be the only person that knows the password and it must be remembered precisely. As time passes, a user's ability to remember a password fades. The matter is further complicated when the average user visits 20 sites requiring them to supply a password. (RSA Survey: http://news.bbc.co.uk/1/hi/technology/3639679.stm) Thus, Password Recovery is an important part in servicing online users.

No alerts in this category.

(2.1) Credential/Session Prediction

Credential/Session Prediction is a method of hijacking or impersonating a web site user. Deducing or guessing the unique value that identifies a particular session or user accomplishes the attack. Also known as Session Hijacking, the consequences could allow attackers the ability to issue web site requests with the compromised user's privileges.

No alerts in this category.

(2.2) Insufficient Authorization

Insufficient Authorization is when a web site permits access to sensitive content or functionality that should require increased access control restrictions. When a user is authenticated to a web site, it does not necessarily mean that he should have full access to all content and that functionality should be granted arbitrarily.

Authorization procedures are performed after authentication, enforcing what a user, service or application is permitted to do. Thoughtful restrictions should govern particular web site activity according to policy. Sensitive portions of a web site may need to be restricted to everyone expect to perhaps an administrator.

No alerts in this category.

(2.3) Insufficient Session Expiration

Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorization. Insufficient Session Expiration increases a web site's exposure to attacks that steal or impersonate other users.

No alerts in this category.

(2.4) Session Fixation

Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value. These techniques range from Cross-site Scripting exploits to peppering the web site with previously made HTTP requests. After a user's session ID has been fixed, the attacker will wait for them to login. Once the user does so, the attacker uses the predefined session ID value to assume their online identity.

No alerts in this category.

(3.1) Content Spoofing

Content Spoofing is an attack technique used to trick a user into believing that certain content appearing on a web site is legitimate and not from an external source.

Some web pages are served using dynamically built HTML content sources. For example, the source location of a frame
<frame src="http://foo.example/file.html">
could be specified by a URL parameter value:

http://foo.example/page?frame_src=http://foo.example/file.html

An attacker may be able to replace the "frame_src" parameter value with "
frame_src=http://attacker.example/spoof.html
". When the resulting web page is served, the browser location bar visibly remains under the user expected domain (foo.example), but the foreign data (attacker.example) is shrouded by legitimate content.

No alerts in this category.

(3.2) Cross-site Scripting

Cross-site Scripting (XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.

When an attacker gets a user's browser to execute his code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Crosssite Scripting attacks essentially compromise the trust relationship between a user and the web site.

No alerts in this category.

(4.1) Buffer Overflow

Buffer Overflow exploits are attacks that alter the flow of an application by overwriting parts of memory. Buffer Overflow is a common software flaw that results in an error condition. This error condition occurs when data written to memory exceed the allocated size of the buffer. As the buffer is overflowed, adjacent memory addresses are overwritten causing the software to fault or crash. When unrestricted, properly-crafted input can be used to overflow the buffer resulting in a number of security issues.

A Buffer Overflow can be used as a Denial of Service attack when memory is corrupted, resulting in software failure. Even more critical is the ability of a Buffer Overflow attack to alter application flow and force unintended actions. This scenario can occur in several ways. Buffer Overflow vulnerabilities have been used to overwrite stack pointers and redirect the program to execute malicious instructions. Buffer Overflows have also been used to change program variables.

No alerts in this category.

(4.2) Format String Attack

Format String Attacks alter the flow of an application by using string formatting library features to access other memory space. Vulnerabilities occur when user-supplied data are used directly as formatting string input for certain C/C++ functions (e.g. fprintf, printf, sprintf, setproctitle, syslog, ...).

If an attacker passes a format string consisting of printf conversion characters (e.g. "%f", "%p", "%n", etc.) as parameter value to the web application, they may:

- Execute arbitrary code on the server
- Read values off the stack
- Cause segmentation faults / software crashes

No alerts in this category.

(4.3) LDAP Injection

LDAP Injection is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.

Lightweight Directory Access Protocol (LDAP) is an open-standard protocol for both querying and manipulating X.500 directory services. The LDAP protocol runs over Internet transport protocols, such as TCP. Web applications may use user-supplied input to create custom LDAP statements for dynamic web page requests.

No alerts in this category.

(4.4) OS Commanding

OS Commanding is an attack technique used to exploit web sites by executing Operating System commands through manipulation of application input.

When a web application does not properly sanitize user-supplied input before using it within application code, it may be possible to trick the application into executing Operating System commands. The executed commands will run with the same permissions of the component that executed the command (e.g. Database server, Web application server, Web server, etc.).

No alerts in this category.

(4.5) SQL Injection

SQL Injection is an attack technique used to exploit web sites that construct SQL statements from user-supplied input.

When a web application fails to properly sanitize user-supplied input, it is possible for an attacker to alter the construction of backend SQL statements. When an attacker is able to modify a SQL statement, the process will run with the same permissions as the component that executed the command. (e.g. Database server, Web application server, Web server, etc.). The impact of this attack can allow attackers to gain total control of the database or even execute commands on the system.

No alerts in this category.

(4.6) SSI Injection

SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server. SSI Injection exploits a web application's failure to sanitize user-supplied data before they are inserted into a server-side interpreted HTML file.

If an attacker submits a Server-side Include statement, he may have the ability to execute arbitrary operating system commands, or include a restricted file's contents the next time the page is served.

No alerts in this category.

(4.7) XPath Injection

XPath Injection is an attack technique used to exploit web sites that construct XPath queries from user-supplied input.

XPath 1.0 is a language used to refer to parts of an XML document. It can be used directly by an application to query an XML document, or as part of a larger operation such as applying an XSLT transformation to an XML document, or applying an XQuery to an XML document.

No alerts in this category.

(5.1) Directory Indexing

Automatic directory listing/indexing is a web server function that lists all of the files within a requested directory if the normal base file (index.html/home.html/default.htm) is not present. When a user requests the main page of a web site, they normally type in a URL such as: http://www.example.com - using the domain name and excluding a specific file. The web server processes this request and searches the document root directory for the default file name and sends this page to the client. If this page is not present, the web server will issue a directory listing and send the output to the client. Essentially, this is equivalent to issuing an "ls" (Unix) or "dir" (Windows) command within this directory and showing the results in HTML form. From an attack and countermeasure perspective, it is important to realize that unintended directory listings may be possible due to software vulnerabilities.

No alerts in this category.

(5.2) Information Leakage

Information Leakage is when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system. Sensitive information may be present within HTML comments, error messages, source code, or simply left in plain sight. There are many ways a web site can be coaxed into revealing this type of information. While leakage does not necessarily represent a breach in security, it does give an attacker useful guidance for future exploitation. Leakage of sensitive information may carry various levels of risk and should be limited whenever possible.

No alerts in this category.

(5.3) Path Traversal

The Path Traversal attack technique forces access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTPbased interface is potentially vulnerable to Path Traversal.

Most web sites restrict user access to a specific portion of the filesystem, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executables necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences.

No alerts in this category.

(5.4) Predictable Resource Location

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses, the attack is a brute force search looking for content that is not intended for public viewing. Temporary files, backup files, configuration files, and sample files are all examples of potentially leftover files. These brute force searches are easy because hidden files will often have common naming convention and reside in standard locations. These files may disclose sensitive information about web application internals, database information, passwords, machine names, file paths to other sensitive areas, or possibly contain vulnerabilities. Disclosure of this information is valuable to an attacker.

No alerts in this category.

(6.1) Abuse of Functionality

Abuse of Functionality is an attack technique that uses a web site's own features and functionality to consume, defraud, or circumvents access controls mechanisms. Some functionality of a web site, possibly even security features, may be abused to cause unexpected behavior. When a piece of functionality is open to abuse, an attacker could potentially annoy other users or perhaps defraud the system entirely. The potential and level of abuse will vary from web site to web site and application to application.

No alerts in this category.

(6.2) Denial of Service

Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity. DoS attacks, which are easily normally applied to the network layer, are also possible at the application layer. These malicious attacks can succeed by starving a system of critical resources, vulnerability exploit, or abuse of functionality.

No alerts in this category.

(6.3) Insufficient Anti-automation

Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually. Certain web site functionalities should be protected against automated attacks.

Left unchecked, automated robots (programs) or attackers could repeatedly exercise web site functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service.

No alerts in this category.

(6.4) Insufficient Process Validation

Insufficient Process Validation is when a web site permits an attacker to bypass or circumvent the intended flow control of an application. If the user state through a process is not verified and enforced, the web site could be vulnerable to exploitation or fraud.

No alerts in this category.

Scanned items (coverage report)

https://pulse:59980/

No vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
8850a96d6ce5608	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
74efab27c34c8b6	URL encoded POST
changepassword	URL encoded POST

https://pulse:59980/index.php

No vulnerabilities have been identified for this URL

7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
6444fc169591f55	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
7ba456c9183076d	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
acda8cbde4da6df	URL encoded POST
changepassword	URL encoded POST

Input scheme 4	
Input name	Input type
Host	HTTP Header

https://pulse:59980/autosuggest

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/autosuggest/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/autosuggest/js/bsn.autosuggest_2.1.3.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/assets

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/assets/jquery-2.1.4.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/assets/jquery.mousewheel.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/assets/moment.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/assets/jquery.timeentry.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/dropdown.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/accordion.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/buttonset.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/input-control.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/pagecontrol.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/calendar.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/dialog.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/js/modern/pagelist.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/plupload

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/plupload/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/plupload/js/plupload.full.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

https://pulse:59980/systemjq.php

No vulnerabilities have been identified for this URL

30 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
009de6f2dffe343	URL encoded GET
domain	URL encoded GET
manufacturer	URL encoded GET
model	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
5c894195fab04a7	URL encoded GET
domain	URL encoded GET
manufacturer	URL encoded GET
model	URL encoded GET
phptimeout	URL encoded GET

Input scheme 3	
Input name	Input type
_	URL encoded GET
b2bd8ca06f16034	URL encoded GET
domain	URL encoded GET
manufacturer	URL encoded GET
model	URL encoded GET
phptimeout	URL encoded GET

Input scheme 4	
Input name	Input type
_	URL encoded GET
4ecbc2ad8e61dcb	URL encoded GET
domain	URL encoded GET
manufacturer	URL encoded GET
model	URL encoded GET
phptimeout	URL encoded GET

Input scheme 5	
Input name	Input type
_	URL encoded GET
a23f7a680876e30	URL encoded GET

domain	URL encoded GET
manufacturer	URL encoded GET
model	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/about.php

No vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
changepassword	URL encoded POST
eb6abd5a03fd49f	URL encoded POST

Input scheme 2	
Input name	Input type
changepassword	URL encoded POST
de8c9c86cbc0e74	URL encoded POST

https://pulse:59980/core.php

No vulnerabilities have been identified for this URL

26 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
a289c96c5a038f9	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
	URL encoded POST
a289c96c5a038f9	URL encoded POST
corelisteningport	URL encoded POST
corephpport	URL encoded POST
coreservicedisplayname	URL encoded POST
coreservicelogonas	URL encoded POST
coreservicename	URL encoded POST
coreservicestartuptype	URL encoded POST
coretrustedcertificate	URL encoded POST
deleteconfiguration	URL encoded POST
submitform	URL encoded POST

Input scheme 3	
Input name	Input type
5a8ca4470b5ad4b	URL encoded POST
changepassword	URL encoded POST

Input scheme 4	
Input name	Input type
	URL encoded POST
5a8ca4470b5ad4b	URL encoded POST
corelisteningport	URL encoded POST
corephpport	URL encoded POST
coreservicedisplayname	URL encoded POST
coreservicelogonas	URL encoded POST
coreservicename	URL encoded POST

coreservicestartuptype	URL encoded POST
coretrustedcertificate	URL encoded POST
deleteconfiguration	URL encoded POST
submitform	URL encoded POST

https://pulse:59980/nodes.php

No vulnerabilities have been identified for this URL

57 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
4c13f3b08e0b965	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
1890d4483f8a393	URL encoded GET
find	URL encoded GET
findtype	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
1890d4483f8a393	URL encoded GET
find	URL encoded GET
findtype	URL encoded GET
metering	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
1890d4483f8a393	URL encoded GET
remmetering	URL encoded GET
remmeteringname	URL encoded GET

Input scheme 5	
Input name	Input type
4c13f3b08e0b965	URL encoded POST
removedeploy	URL encoded POST

Input scheme 6	
Input name	Input type
4c13f3b08e0b965	URL encoded POST
confirmdeploy	URL encoded POST

Input scheme 7	
Input name	Input type
4c13f3b08e0b965	URL encoded POST
agentrefresh	URL encoded POST

Input scheme 8	
Input name	Input type
4c13f3b08e0b965	URL encoded POST
cmd	URL encoded POST
find	URL encoded POST
findtype	URL encoded POST
orderby	URL encoded POST

Input scheme 9	
Input name	Input type
find	URL encoded GET
findtype	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
results	URL encoded GET

Input scheme 10	
Input name	Input type
find	URL encoded GET
findtype	URL encoded GET

Input scheme 11	
Input name	Input type
changepassword	URL encoded POST
ed89df0d8109b99	URL encoded POST

Input scheme 12	
Input name	Input type
9cc435848440980	URL encoded GET
find	URL encoded GET
findtype	URL encoded GET
orderby	URL encoded GET

Input scheme 13	
Input name	Input type
9cc435848440980	URL encoded GET
find	URL encoded GET
findtype	URL encoded GET
metering	URL encoded GET
orderby	URL encoded GET

Input scheme 14	
Input name	Input type
9cc435848440980	URL encoded GET
remmetering	URL encoded GET
remmeteringname	URL encoded GET

Input scheme 15	
Input name	Input type
ed89df0d8109b99	URL encoded POST
removedeploy	URL encoded POST

Input scheme 16	
Input name	Input type
confirmdeploy	URL encoded POST
ed89df0d8109b99	URL encoded POST

Input scheme 17	
Input name	Input type
agentrefresh	URL encoded POST
ed89df0d8109b99	URL encoded POST

Input scheme 18	
Input name	Input type
cmd	URL encoded POST
ed89df0d8109b99	URL encoded POST
find	URL encoded POST

findtype	URL encoded POST
orderby	URL encoded POST

https://pulse:59980/nodesjq.php

No vulnerabilities have been identified for this URL

18 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
_	URL encoded GET
1890d4483f8a393	URL encoded GET
confirmdeploy	URL encoded GET
find	URL encoded GET
findtype	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET
results	URL encoded GET

Input scheme 2

Input name	Input type
_	URL encoded GET
9cc435848440980	URL encoded GET
confirmdeploy	URL encoded GET
find	URL encoded GET
findtype	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET
results	URL encoded GET

https://pulse:59980/xml.php

No vulnerabilities have been identified for this URL

12 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
1890d4483f8a393	URL encoded GET
export	URL encoded GET
source	URL encoded GET

Input scheme 2

Input name	Input type
export	URL encoded GET
f22fe6d757316f7	URL encoded GET
source	URL encoded GET

Input scheme 3

Input name	Input type
9cc435848440980	URL encoded GET
export	URL encoded GET
source	URL encoded GET

Input scheme 4

Input name	Input type
6219157ab0a5545	URL encoded GET

export	URL encoded GET
source	URL encoded GET

https://pulse:59980/nodes_nagios.php

No vulnerabilities have been identified for this URL

37 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
changepassword	URL encoded POST
f6e686c385649cf	URL encoded POST

Input scheme 3	
Input name	Input type
b79a926245ba467	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
b6f2c07ffb4fae9	URL encoded POST
changepassword	URL encoded POST

Input scheme 6	
Input name	Input type
b118d5f357ce28b	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET

executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

https://pulse:59980/nodes_nagiosjq.php

No vulnerabilities have been identified for this URL

20 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
_	URL encoded GET
b79a926245ba467	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2

Input name	Input type
_	URL encoded GET
b118d5f357ce28b	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nodes_inventory.php

No vulnerabilities have been identified for this URL

16 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2

Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
b78f1bc917b24b8	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
6fa327741c0d3b8	URL encoded POST
changepassword	URL encoded POST

https://pulse:59980/nodes_programs.php

No vulnerabilities have been identified for this URL

55 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
13a19ff57c34b2e	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
479b221ad685d1b	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
13a19ff57c34b2e	URL encoded POST
uninstallidprogram	URL encoded POST
uninstallnameprogram	URL encoded POST
uninstallprogramconf	URL encoded POST
uninstallversprogram	URL encoded POST

Input scheme 5	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET

filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 6	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
6af335d9e7e58e3	URL encoded POST
changepassword	URL encoded POST

Input scheme 7	
Input name	Input type
computerip	URL encoded GET
d01d663ec78f3e8	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 8	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
6af335d9e7e58e3	URL encoded POST
uninstallidprogram	URL encoded POST
uninstallnameprogram	URL encoded POST
uninstallprogramconf	URL encoded POST
uninstallversprogram	URL encoded POST

https://pulse:59980/nodes_programsjq.php

No vulnerabilities have been identified for this URL

24 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
479b221ad685d1b	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
d01d663ec78f3e8	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nodes_processes.php

No vulnerabilities have been identified for this URL

53 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
34b390859b6adca	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
181bee69d16f4c8	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
34b390859b6adca	URL encoded POST
endidprocess	URL encoded POST
endnameprocess	URL encoded POST
endtypeprocess	URL encoded POST

Input scheme 5	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 6	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
cd168b53c47fd12	URL encoded POST
changepassword	URL encoded POST

Input scheme 7	
Input name	Input type
a451cb49ec70c2e	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 8	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
cd168b53c47fd12	URL encoded POST
endidprocess	URL encoded POST
endnameprocess	URL encoded POST
endtypeprocess	URL encoded POST

https://pulse:59980/nodes_processesjq.php

No vulnerabilities have been identified for this URL

24 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
181bee69d16f4c8	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET

orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
a451cb49ec70c2e	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nodes_services.php

No vulnerabilities have been identified for this URL

53 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
2013b1582956c53	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
71af0547deca579	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
2013b1582956c53	URL encoded POST

serviceidexec	URL encoded POST
servicenameexec	URL encoded POST
servicetypeexec	URL encoded POST

Input scheme 5	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 6	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
52d399227a26090	URL encoded POST
changepassword	URL encoded POST

Input scheme 7	
Input name	Input type
975276f5972b461	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 8	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
52d399227a26090	URL encoded POST
serviceidexec	URL encoded POST
servicenameexec	URL encoded POST
servicetypeexec	URL encoded POST

https://pulse:59980/nodes_servicesjq.php

No vulnerabilities have been identified for this URL

24 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
71af0547deca579	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET

filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
975276f5972b461	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nodes_netstat.php

No vulnerabilities have been identified for this URL

55 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
29c76253ba4f2d9	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
73a068013d782b6	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET

executorport	URL encoded GET
node	URL encoded GET
29c76253ba4f2d9	URL encoded POST
uninstallidprogram	URL encoded POST
uninstallnameprogram	URL encoded POST
uninstallprogramconf	URL encoded POST
uninstallversprogram	URL encoded POST

Input scheme 5	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 6	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
2298e6d2f4221fd	URL encoded POST
changepassword	URL encoded POST

Input scheme 7	
Input name	Input type
27d7800b555dd4e	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 8	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
2298e6d2f4221fd	URL encoded POST
uninstallidprogram	URL encoded POST
uninstallnameprogram	URL encoded POST
uninstallprogramconf	URL encoded POST
uninstallversprogram	URL encoded POST

https://pulse:59980/nodes_netstatjq.php

No vulnerabilities have been identified for this URL

20 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET

73a068013d782b6	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
27d7800b555dd4e	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nodes_scheduler.php

No vulnerabilities have been identified for this URL

56 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
81efd8daa3a2f1e	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
9452a9cab1c8a53	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
osversion	URL encoded GET

Input scheme 4	
Input name	Input type

computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
81efd8daa3a2f1e	URL encoded POST
commandtaskname	URL encoded POST
commandtitletask	URL encoded POST
commandtype	URL encoded POST

Input scheme 5

Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
osversion	URL encoded GET
page	URL encoded GET

Input scheme 6

Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
5541e51f848024f	URL encoded POST
changepassword	URL encoded POST

Input scheme 7

Input name	Input type
b5c7788a618bcd9	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
osversion	URL encoded GET

Input scheme 8

Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
5541e51f848024f	URL encoded POST
commandtaskname	URL encoded POST
commandtitletask	URL encoded POST
commandtype	URL encoded POST

https://pulse:59980/nodes_schedulerjq.php

No vulnerabilities have been identified for this URL

26 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
9452a9cab1c8a53	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
osmver	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
b5c7788a618bcd9	URL encoded GET
cid	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
message	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
osmver	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nodes_eventviewer.php

No vulnerabilities have been identified for this URL

37 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET

Input scheme 2	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
changepassword	URL encoded POST
fb7e094125b10a5	URL encoded POST

Input scheme 3	
Input name	Input type
259db1811013f36	URL encoded GET

computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
node	URL encoded GET
changepassword	URL encoded POST
f0b0cc0966753ae	URL encoded POST

Input scheme 6	
Input name	Input type
99d068414750982	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET

https://pulse:59980/nodes_eventviewerjq.php

No vulnerabilities have been identified for this URL

20 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
259db1811013f36	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET

99d068414750982	URL encoded GET
computerip	URL encoded GET
domain	URL encoded GET
executorport	URL encoded GET
filter	URL encoded GET
node	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/nagios.php

No vulnerabilities have been identified for this URL

13 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
610ec8df04c2f9f	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
4258765c41ab762	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 4	
Input name	Input type
b172856838fa292	URL encoded POST
changepassword	URL encoded POST

Input scheme 5	
Input name	Input type
49fd38988be41e7	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

https://pulse:59980/nagiosjq.php

No vulnerabilities have been identified for this URL

16 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
4258765c41ab762	URL encoded GET
filter	URL encoded GET
nrpepathname	URL encoded GET
nscppathname	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
49fd38988be41e7	URL encoded GET
filter	URL encoded GET
nrpepathname	URL encoded GET
nscppathname	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/inventory.php

No vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
32a16d54be57288	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
9cb0a65940ab209	URL encoded POST
changepassword	URL encoded POST

https://pulse:59980/programs.php

No vulnerabilities have been identified for this URL

23 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
changepassword	URL encoded POST
daeb787e85f613c	URL encoded POST

Input scheme 2	
Input name	Input type
50915c241f849e3	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
daeb787e85f613c	URL encoded POST
uninstallidprogram	URL encoded POST
uninstallnameprogram	URL encoded POST
uninstallprogramconf	URL encoded POST
uninstallversprogram	URL encoded POST

Input scheme 4	
Input name	Input type
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type

3dd8c640445c91a	URL encoded POST
changepassword	URL encoded POST

Input scheme 6	
Input name	Input type
d8d51d79469d3fe	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 7	
Input name	Input type
3dd8c640445c91a	URL encoded POST
uninstallidprogram	URL encoded POST
uninstallnameprogram	URL encoded POST
uninstallprogramconf	URL encoded POST
uninstallversprogram	URL encoded POST

https://pulse:59980/programsjq.php

No vulnerabilities have been identified for this URL

12 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
50915c241f849e3	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
d8d51d79469d3fe	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/wmiexplorer.php

No vulnerabilities have been identified for this URL

17 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
18d5382cb09087e	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
c1a5da8e31f5004	URL encoded GET
filter	URL encoded GET
wmiclasses	URL encoded GET
wminamespace	URL encoded GET

Input scheme 3	
Input name	Input type
filter	URL encoded GET
lastfilter	URL encoded GET
page	URL encoded GET
wmiclasses	URL encoded GET
wminamespace	URL encoded GET

Input scheme 4	
Input name	Input type
56852d25a0e8899	URL encoded POST
changepassword	URL encoded POST

Input scheme 5	
Input name	Input type
f6585ab7f514a2e	URL encoded GET
filter	URL encoded GET
wmiclasses	URL encoded GET
wminamespace	URL encoded GET

https://pulse:59980/wmiexplorerjq.php

No vulnerabilities have been identified for this URL

16 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
c1a5da8e31f5004	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET
wmiclasses	URL encoded GET
wminamespace	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
f6585ab7f514a2e	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET
wmiclasses	URL encoded GET
wminamespace	URL encoded GET

https://pulse:59980/shutdown.php

No vulnerabilities have been identified for this URL

18 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
6f203ca593bea55	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
6f203ca593bea55	URL encoded POST
shutdowncommand	URL encoded POST
shutdowndate	URL encoded POST
shutdowntime	URL encoded POST
shutdowntype	URL encoded POST

Input scheme 3	
Input name	Input type
6f203ca593bea55	URL encoded POST
toolssendcommand	URL encoded POST

Input scheme 4	
Input name	Input type
6626f6737e9ee0e	URL encoded POST
changepassword	URL encoded POST

Input scheme 5	
Input name	Input type
6626f6737e9ee0e	URL encoded POST
shutdowncommand	URL encoded POST
shutdowndate	URL encoded POST
shutdowntime	URL encoded POST
shutdowntype	URL encoded POST

Input scheme 6	
Input name	Input type
6626f6737e9ee0e	URL encoded POST
toolssendcommand	URL encoded POST

https://pulse:59980/shutdownjq.php

No vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
6bdc4700fb46e5c	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
879478982f9abbb	URL encoded GET

https://pulse:59980/processes.php

No vulnerabilities have been identified for this URL

22 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
6d1a5982cc7a445	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
41ef3ee3097f64b	URL encoded GET

filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
6d1a5982cc7a445	URL encoded POST
endidprocess	URL encoded POST
endnameprocess	URL encoded POST
endtypeprocess	URL encoded POST

Input scheme 4	
Input name	Input type
cpucount	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
c237c49f0d6c50e	URL encoded POST
changepassword	URL encoded POST

Input scheme 6	
Input name	Input type
5f94a8f92bb0561	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 7	
Input name	Input type
c237c49f0d6c50e	URL encoded POST
endidprocess	URL encoded POST
endnameprocess	URL encoded POST
endtypeprocess	URL encoded POST

https://pulse:59980/processesjq.php

No vulnerabilities have been identified for this URL

14 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
41ef3ee3097f64b	URL encoded GET
cpucount	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
5f94a8f92bb0561	URL encoded GET
cpucount	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

phptimeout	URL encoded GET

https://pulse:59980/services.php

No vulnerabilities have been identified for this URL

21 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
86acfd40125e08f	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
816bcb22f14740c	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
86acfd40125e08f	URL encoded POST
serviceidexec	URL encoded POST
servicenameexec	URL encoded POST
servicetypeexec	URL encoded POST

Input scheme 4	
Input name	Input type
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
4cbfa472deb02e3	URL encoded POST
changepassword	URL encoded POST

Input scheme 6	
Input name	Input type
c5e501955a0e694	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 7	
Input name	Input type
4cbfa472deb02e3	URL encoded POST
serviceidexec	URL encoded POST
servicenameexec	URL encoded POST
servicetypeexec	URL encoded POST

https://pulse:59980/servicesjq.php

No vulnerabilities have been identified for this URL

12 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
816bcb22f14740c	URL encoded GET
filter	URL encoded GET

orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
c5e501955a0e694	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/netstat.php

No vulnerabilities have been identified for this URL

21 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
changepassword	URL encoded POST
d67610e803c6829	URL encoded POST

Input scheme 2	
Input name	Input type
8a73a6c947e1213	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
commandtaskname	URL encoded POST
commandtitletask	URL encoded POST
commandtype	URL encoded POST
d67610e803c6829	URL encoded POST

Input scheme 4	
Input name	Input type
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
76ba8869c6128d3	URL encoded POST
changepassword	URL encoded POST

Input scheme 6	
Input name	Input type
0ab161e5c72a3cb	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 7	
Input name	Input type
76ba8869c6128d3	URL encoded POST
commandtaskname	URL encoded POST
commandtitletask	URL encoded POST
commandtype	URL encoded POST

https://pulse:59980/netstatjq.php

No vulnerabilities have been identified for this URL

12 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
8a73a6c947e1213	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
0ab161e5c72a3cb	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/scheduler.php

No vulnerabilities have been identified for this URL

21 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
872404d36d8d3e0	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
525eecd78d7a3ee	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
872404d36d8d3e0	URL encoded POST
commandtaskname	URL encoded POST
commandtitletask	URL encoded POST
commandtype	URL encoded POST

Input scheme 4	
Input name	Input type
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
changepassword	URL encoded POST
f8b6ab4ce92cc8c	URL encoded POST

Input scheme 6	
Input name	Input type
dd26ff2444ad3c4	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 7	
Input name	Input type
commandtaskname	URL encoded POST
commandtitletask	URL encoded POST
commandtype	URL encoded POST
f8b6ab4ce92cc8c	URL encoded POST

https://pulse:59980/schedulerjq.php

No vulnerabilities have been identified for this URL

14 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
525eecd78d7a3ee	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
osmver	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
dd26ff2444ad3c4	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
osmver	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/eventviewer.php

No vulnerabilities have been identified for this URL

13 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
b9aebe7054003b3	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
1c677486971571a	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 3	
Input name	Input type
filter	URL encoded GET

orderby	URL encoded GET
page	URL encoded GET

Input scheme 4	
Input name	Input type
af4c7ee5e58045f	URL encoded POST
changepassword	URL encoded POST

Input scheme 5	
Input name	Input type
36249109f0e5fa6	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET

https://pulse:59980/eventviewerjq.php

No vulnerabilities have been identified for this URL

12 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
1c677486971571a	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
36249109f0e5fa6	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/registry.php

No vulnerabilities have been identified for this URL

30 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
b00400153fde3a7	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
b00400153fde3a7	URL encoded POST
regexportconf	URL encoded POST

Input scheme 3	
Input name	Input type
be7b6a059db3713	URL encoded GET
hkey	URL encoded GET

Input scheme 4	
Input name	Input type

be7b6a059db3713	URL encoded GET
filter	URL encoded GET
hkey	URL encoded GET
keypath	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET

Input scheme 5	
Input name	Input type
filter	URL encoded GET
keypath	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 6	
Input name	Input type
changepassword	URL encoded POST
e889816a0638bc2	URL encoded POST

Input scheme 7	
Input name	Input type
e889816a0638bc2	URL encoded POST
regexportconf	URL encoded POST

Input scheme 8	
Input name	Input type
34a65c5f86e6fdd	URL encoded GET
hkey	URL encoded GET

Input scheme 9	
Input name	Input type
34a65c5f86e6fdd	URL encoded GET
filter	URL encoded GET
hkey	URL encoded GET
keypath	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET

https://pulse:59980/registryjq.php

No vulnerabilities have been identified for this URL

18 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
be7b6a059db3713	URL encoded GET
filter	URL encoded GET
hkey	URL encoded GET
keypath	URL encoded GET
lastfilter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
34a65c5f86e6fdd	URL encoded GET
filter	URL encoded GET
hkey	URL encoded GET
keypath	URL encoded GET
lastfilter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/cli.php

No vulnerabilities have been identified for this URL

18 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
170b260a94220ad	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
170b260a94220ad	URL encoded POST
resetviewconf	URL encoded POST

Input scheme 3	
Input name	Input type
170b260a94220ad	URL encoded POST
cldrive	URL encoded POST
cltimeout	URL encoded POST
cmd	URL encoded POST
cmdmemlist	URL encoded POST

Input scheme 4	
Input name	Input type
changepassword	URL encoded POST
d0e02832ab4a728	URL encoded POST

Input scheme 5	
Input name	Input type
d0e02832ab4a728	URL encoded POST
resetviewconf	URL encoded POST

Input scheme 6	
Input name	Input type
cldrive	URL encoded POST
cltimeout	URL encoded POST
cmd	URL encoded POST
cmdmemlist	URL encoded POST
d0e02832ab4a728	URL encoded POST

https://pulse:59980/explorer.php

No vulnerabilities have been identified for this URL

31 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
path	URL encoded GET

Input scheme 2	
Input name	Input type
64a7bd73df58438	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
64a7bd73df58438	URL encoded POST
openclidrive	URL encoded POST
openclipath	URL encoded POST

Input scheme 4	
Input name	Input type
7b35efdfcdf6589	URL encoded GET
path	URL encoded GET

Input scheme 5	
Input name	Input type
7b35efdfcdf6589	URL encoded GET
filter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
path	URL encoded GET

Input scheme 6	
Input name	Input type
filter	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
path	URL encoded GET

Input scheme 7	
Input name	Input type
1dc00018a31be32	URL encoded POST
changepassword	URL encoded POST

Input scheme 8	
Input name	Input type
1dc00018a31be32	URL encoded POST
openclidrive	URL encoded POST
openclipath	URL encoded POST

Input scheme 9	
Input name	Input type
daa74063f1e8fa6	URL encoded GET
path	URL encoded GET

Input scheme 10	
Input name	Input type
daa74063f1e8fa6	URL encoded GET
filter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET

path	URL encoded GET

https://pulse:59980/explorerjq.php

No vulnerabilities have been identified for this URL

45 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
_	URL encoded GET
43171a50e2d2614	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
path	URL encoded GET
phptimeout	URL encoded GET

Input scheme 2

Input name	Input type
_	URL encoded GET
7f17aba5e5c8bca	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
path	URL encoded GET
phptimeout	URL encoded GET

Input scheme 3

Input name	Input type
_	URL encoded GET
7b35efdfcdf6589	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
path	URL encoded GET
phptimeout	URL encoded GET

Input scheme 4

Input name	Input type
_	URL encoded GET
840dd4a4d2db950	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
path	URL encoded GET
phptimeout	URL encoded GET

Input scheme 5

Input name	Input type

_	URL encoded GET
daa74063f1e8fa6	URL encoded GET
filter	URL encoded GET
lastfilter	URL encoded GET
lastpath	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
path	URL encoded GET
phptimeout	URL encoded GET

https://pulse:59980/users.php

No vulnerabilities have been identified for this URL

21 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
7f32df868948a8e	URL encoded POST
changepassword	URL encoded POST

Input scheme 2

Input name	Input type
	URL encoded POST
7f32df868948a8e	URL encoded POST
newaccount	URL encoded POST
newuserauth	URL encoded POST
newusername	URL encoded POST
newuserpsw	URL encoded POST
newuserpswc	URL encoded POST
newusertype	URL encoded POST

Input scheme 3

Input name	Input type
changegroup	URL encoded GET

Input scheme 4

Input name	Input type
03927dc420933e2	URL encoded POST
changepassword	URL encoded POST

Input scheme 5

Input name	Input type
	URL encoded POST
03927dc420933e2	URL encoded POST
newaccount	URL encoded POST
newuserauth	URL encoded POST
newusername	URL encoded POST
newuserpsw	URL encoded POST
newuserpswc	URL encoded POST
newusertype	URL encoded POST

https://pulse:59980/audit.php

No vulnerabilities have been identified for this URL

15 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type

392d116c6bfd1d1	URL encoded POST
changepassword	URL encoded POST

Input scheme 2	
Input name	Input type
0920ccd2eae120d	URL encoded GET
file	URL encoded GET

Input scheme 3	
Input name	Input type
filter	URL encoded GET
orderby	URL encoded GET

Input scheme 4	
Input name	Input type
	URL encoded GET
file	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET

Input scheme 5	
Input name	Input type
a07c50c85f56b0b	URL encoded POST
changepassword	URL encoded POST

Input scheme 6	
Input name	Input type
2c4b299d8066c98	URL encoded GET
file	URL encoded GET

https://pulse:59980/auditjq.php

No vulnerabilities have been identified for this URL

14 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
0920ccd2eae120d	URL encoded GET
file	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
srvrun	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
2c4b299d8066c98	URL encoded GET
file	URL encoded GET
filter	URL encoded GET
orderby	URL encoded GET
page	URL encoded GET
srvrun	URL encoded GET

https://pulse:59980/tail.php

No vulnerabilities have been identified for this URL

41 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET

Input scheme 2	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET
132ea0ed0727a88	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET
132ea0ed0727a88	URL encoded POST
openeditconf	URL encoded POST
tailoutput	URL encoded POST

Input scheme 4	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET
132ea0ed0727a88	URL encoded POST
openeditconf	URL encoded POST

Input scheme 5	
Input name	Input type
file	URL encoded GET
path	URL encoded GET

Input scheme 6	
Input name	Input type
	URL encoded GET
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET

Input scheme 7	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET
a3115049a276a45	URL encoded POST
changepassword	URL encoded POST

Input scheme 8	
Input name	Input type

download	URL encoded GET
file	URL encoded GET
path	URL encoded GET
a3115049a276a45	URL encoded POST
openeditconf	URL encoded POST
tailoutput	URL encoded POST

Input scheme 9	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
path	URL encoded GET
a3115049a276a45	URL encoded POST
openeditconf	URL encoded POST

https://pulse:59980/tailjq.php

No vulnerabilities have been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
7795f3c0f3385e5	URL encoded GET
file	URL encoded GET
openeditconf	URL encoded GET
path	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
8a7f12f5a59bf47	URL encoded GET
file	URL encoded GET
openeditconf	URL encoded GET
path	URL encoded GET

https://pulse:59980/7zip.php

No vulnerabilities have been identified for this URL

18 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
name	URL encoded GET
path	URL encoded GET

Input scheme 2	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
name	URL encoded GET
path	URL encoded GET
acc6f4627e4d0b3	URL encoded POST
changepassword	URL encoded POST

Input scheme 3	
Input name	Input type
file	URL encoded GET
path	URL encoded GET

Input scheme 4	
Input name	Input type
download	URL encoded GET
file	URL encoded GET
name	URL encoded GET
path	URL encoded GET
023806f61b78653	URL encoded POST
changepassword	URL encoded POST

https://pulse:59980/7zipjq.php

No vulnerabilities have been identified for this URL

16 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_	URL encoded GET
7c5b7928957f918	URL encoded GET
extract	URL encoded GET
extractfolder	URL encoded GET
extractpass	URL encoded GET
file	URL encoded GET
lock	URL encoded GET
path	URL encoded GET

Input scheme 2	
Input name	Input type
_	URL encoded GET
1cc2b262087d2e4	URL encoded GET
extract	URL encoded GET
extractfolder	URL encoded GET
extractpass	URL encoded GET
file	URL encoded GET
lock	URL encoded GET
path	URL encoded GET

https://pulse:59980/download.php

No vulnerabilities have been identified for this URL

12 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
7795f3c0f3385e5	URL encoded GET
download	URL encoded GET
path	URL encoded GET

Input scheme 2	
Input name	Input type
7c5b7928957f918	URL encoded GET
download	URL encoded GET
path	URL encoded GET

Input scheme 3	
Input name	Input type
8a7f12f5a59bf47	URL encoded GET
download	URL encoded GET
path	URL encoded GET

Input scheme 4	
Input name	Input type
1cc2b262087d2e4	URL encoded GET
download	URL encoded GET
path	URL encoded GET