Acunetix Website Audit

7 January, 2016

2011 CWE/SANS Top 25 Most Dangerous Software Errors

~ compliance report ~

2011 CWE/SANS Top 25 Most Dangerous Software Errors

compliance report

Description

The 2011 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

The Top 25 list is a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities that plague the software industry, by identifying and avoiding all-too-common mistakes that occur before software is even shipped. Software customers can use the same list to help them to ask for more secure software. Researchers in software security can use the Top 25 to focus on a narrow but important subset of all known security weaknesses. Finally, software managers and CIOs can use the Top 25 list as a measuring stick of progress in their efforts to secure their software.

The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts in the US and Europe. It leverages experiences in the development of the SANS Top 20 attack vectors (http://www.sans.org/top20/) and MITRE's Common Weakness Enumeration (CWE) (http://cwe.mitre.org/). MITRE maintains the CWE web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 programming errors along with authoritative guidance for mitigating and avoiding them. The CWE site contains data on more than 800 programming errors, design errors, and architecture errors that can lead to exploitable vulnerabilities.

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.

This document was generated using information provided in "2010 CWE/SANS Top 25 Most Dangerous Software Errors", that can be found at http://cwe.mitre.org/top25/.

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.

- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (1)
  No alerts in this category
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (2)
  No alerts in this category
- Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (3)
  No alerts in this category

- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (4)
  - **No alerts in this category**
- Missing Authentication for Critical Function (5)
  - **No alerts in this category**
- Improper Access Control (Authorization) (6)
  - **No alerts in this category**
- Use of Hard-coded Credentials (7)
  - **No alerts in this category**
- Missing Encryption of Sensitive Data (8)
  - **No alerts in this category**
- Unrestricted Upload of File with Dangerous Type (9)
  - **No alerts in this category**
- Reliance on Untrusted Inputs in a Security Decision (10)
  - **No alerts in this category**
- Execution with Unnecessary Privileges (11)
  - **No alerts in this category**
- Cross-Site Request Forgery (CSRF) (12)
  - **No alerts in this category**
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (13)
  - **No alerts in this category**
- Download of Code Without Integrity Check (14)
  - **No alerts in this category**
- Incorrect Authorization (15)
  - **No alerts in this category**
- Inclusion of Functionality from Untrusted Control Sphere (16)
  - **No alerts in this category**
- Incorrect Permission Assignment for Critical Resource (17)
  - **No alerts in this category**
- Use of Potentially Dangerous Function (18)
  - **No alerts in this category**
- Use of a Broken or Risky Cryptographic Algorithm (19)
  - **No alerts in this category**
- Incorrect Calculation of Buffer Size (20)
  - **No alerts in this category**
- Improper Restriction of Excessive Authentication Attempts (21)
  - **No alerts in this category**
- URL Redirection to Untrusted Site ('Open Redirect') (22)
  - **No alerts in this category**
- Uncontrolled Format String (23)
  - **No alerts in this category**
- Integer Overflow or Wraparound (24)
  - **No alerts in this category**
- Use of a One-Way Hash without a Salt (25)
  - **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) Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They'll even steal data one byte at a time if they have to, and they have the patience and know-how to do so.

No alerts in this category.

(2) Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Your software is often the bridge between an outsider on the network and the internals of your operating system. When you invoke another program on the operating system, but you allow untrusted inputs to be fed into the command string that you generate for executing that program, then you are inviting attackers to cross that bridge into a land of riches by executing their own commands instead of yours.

No alerts in this category.

(3) Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Buffer overflows are Mother Nature's little reminder of that law of physics that says: if you try to put more stuff into a container than it can hold, you're going to make a mess. The scourge of C applications for decades, buffer overflows have been remarkably resistant to elimination. However, copying an untrusted input without checking the size of that input is the simplest error to make in a time when there are much more interesting mistakes to avoid. That's why this type of buffer overflow is often referred to as "classic." It's decades old, and it's typically one of the first things you learn about in Secure Programming 101.

No alerts in this category.

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

Cross-site scripting (XSS) is one of the most prevalent, obstinate, and dangerous vulnerabilities in web applications. It's pretty much inevitable when you combine the stateless nature of HTTP, the mixture of data and script in HTML, lots of data passing between web sites, diverse encoding schemes, and feature-rich web browsers. If you're not careful, attackers can inject Javascript or other browser-executable content into a web page that your application generates. Your web page is then accessed by other users, whose browsers execute that malicious script as if it came from you (because, after all, it *did* come from you). Suddenly, your web site is serving code that you didn't write. The attacker can use a variety of techniques to get the input directly into your server, or use an unwitting victim as the middle man in a technical version of the "why do you keep hitting yourself?" game.

No alerts in this category.

(5) Missing Authentication for Critical Function

In countless action movies, the villain breaks into a high-security building by crawling through heating ducts or pipes, scaling elevator shafts, or hiding under a moving cart. This works because the pathway into the building doesn't have all those nosy security guards asking for identification. Software may expose certain critical functionality with the assumption that nobody would think of trying to do anything but break in through the front door. But attackers know how to case a joint and figure out alternate ways of getting into a system.

No alerts in this category.

(6) Improper Access Control (Authorization)

Suppose you're hosting a house party for a few close friends and their guests. You invite everyone into your living room, but while you're catching up with one of your friends, one of the guests raids your fridge, peeks into your medicine cabinet and ponders what you've hidden in the nightstand next to your bed. Software faces similar authorization problems that could lead to more dire consequences. If you don't ensure that your software's users are only doing what they're allowed to, then attackers will try to exploit your improper authorization and exercise unauthorized functionality that you only intended for restricted users.

No alerts in this category.

(7) Use of Hard-coded Credentials

Hard-coding a secret password or cryptograpic key into your program is bad manners, even though it makes it extremely convenient - for skilled reverse engineers. While it might shrink your testing and support budgets, it can reduce the security of your customers to dust. If the password is the same across all your software, then every customer becomes vulnerable if (rather, when) your password becomes known. Because it's hard-coded, it's usually a huge pain for sysadmins to fix. And you know how much they love inconvenience at 2 AM when their network's being hacked - about as much as you'll love responding to hordes of angry customers and reams of bad press if your little secret should get out. Most of the CWE Top 25 can be explained away as an honest mistake; for this issue, though, customers won't see it that way. Another way that hard-coded credentials arise is through unencrypted or obfuscated storage in a configuration file, registry key, or other location that is only intended to be accessible to an administrator. While this is much more polite than burying it in a binary program where it can't be modified, it becomes a Bad Idea to expose this file to outsiders through lax permissions or other means.

No alerts in this category.

(8) Missing Encryption of Sensitive Data

Whenever sensitive data is being stored or transmitted anywhere outside of your control, attackers may be looking for ways to get to it. Thieves could be anywhere - sniffing your packets, reading your databases, and sifting through your file systems. If your software sends sensitive information across a network, such as private data or authentication credentials, that information crosses many different nodes in transit to its final destination. Attackers can sniff this data right off the wire, and it doesn't require a lot of effort. All they need to do is control one node along the path to the final destination, control any node within the same networks of those transit nodes, or plug into an available interface. If your software stores sensitive information on a local file or database, there may be other ways for attackers to get at the file. They may benefit from lax permissions, exploitation of another vulnerability, or physical theft of the disk. You know those massive credit card thefts you keep hearing about? Many of them are due to unencrypted storage.

No alerts in this category.

(9) Unrestricted Upload of File with Dangerous Type

You may think you're allowing uploads of innocent images (rather, images that won't damage your system - the Interweb's not so innocent in some places). But the name of the uploaded file could contain a dangerous extension such as .php instead of .gif, or other information (such as content type) may cause your server to treat the image like a big honkin' program. So, instead of seeing the latest paparazzi shot of your favorite Hollywood celebrity in a compromising position, you'll be the one whose server gets compromised.

No alerts in this category.

(10) Reliance on Untrusted Inputs in a Security Decision

In countries where there is a minimum age for purchasing alcohol, the bartender is typically expected to verify the purchaser's age by checking a driver's license or other legally acceptable proof of age. But if somebody looks old enough to drink, then the bartender may skip checking the license altogether. This is a good thing for underage customers who happen to look older. Driver's licenses may require close scrutiny to identify fake licenses, or to determine if a person is using someone else's license. Software developers often rely on untrusted inputs in the same way, and when these inputs are used to decide whether to grant access to restricted resources, trouble is just around the corner.

No alerts in this category.

(11) Execution with Unnecessary Privileges

Your software may need special privileges to perform certain operations, but wielding those privileges longer than necessary can be extremely risky. When running with extra privileges, your application has access to resources that the application's user can't directly reach. For example, you might intentionally launch a separate program, and that program allows its user to specify a file to open; this feature is frequently present in help utilities or editors. The user can access unauthorized files through the launched program, thanks to those extra privileges. Command execution can happen in a similar fashion. Even if you don't launch other programs, additional vulnerabilities in your software could have more serious consequences than if it were running at a lower privilege level.

No alerts in this category.

(12) Cross-Site Request Forgery (CSRF)

You know better than to accept a package from a stranger at the airport. It could contain dangerous contents. Plus, if anything goes wrong, then it's going to look as if you did it, because you're the one with the package when you board the plane. Cross-site request forgery is like that strange package, except the attacker tricks a user into activating a request that goes to your site. Thanks to scripting and the way the web works in general, the user might not even be aware that the request is being sent. But once the request gets to your server, it looks as if it came from the user, not the attacker. This might not seem like a big deal, but the attacker has essentially masqueraded as a legitimate user and gained all the potential access that the user has. This is especially handy when the user has administrator privileges, resulting in a complete compromise of your application's functionality. When combined with XSS, the result can be extensive and devastating. If you've heard about XSS worms that stampede through very large web sites in a matter of minutes, there's usually CSRF feeding them.

No alerts in this category.

(13) Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

While data is often exchanged using files, sometimes you don't intend to expose every file on your system while doing so. When you use an outsider's input while constructing a filename, the resulting path could point outside of the intended directory. An attacker could combine multiple ".." or similar sequences to cause the operating system to navigate out of the restricted directory, and into the rest of the system.

No alerts in this category.

(14) Download of Code Without Integrity Check

You don't need to be a guru to realize that if you download code and execute it, you're trusting that the source of that code isn't malicious. Maybe you only access a download site that you trust, but attackers can perform all sorts of tricks to modify that code before it reaches you. They can hack the download site, impersonate it with DNS spoofing or cache poisoning, convince the system to redirect to a different site, or even modify the code in transit as it crosses the network. This scenario even applies to cases in which your own product downloads and installs its own updates. When this happens, your software will wind up running code that it doesn't expect, which is bad for you but great for attackers.

No alerts in this category.

(15) Incorrect Authorization

While the lack of authorization is more dangerous (see elsewhere in the Top 25), incorrect authorization can be just as problematic. Developers may attempt to control access to certain resources, but implement it in a way that can be bypassed. For example, once a person has logged in to a web application, the developer may store the permissions in a cookie. By modifying the cookie, the attacker can access other resources. Alternately, the developer might perform authorization by delivering code that gets executed in the web client, but an attacker could use a customized client that removes the check entirely.

No alerts in this category.

(16) Inclusion of Functionality from Untrusted Control Sphere

The idea seems simple enough (not to mention cool enough): you can make a lot of smaller parts of a document (or program), then combine them all together into one big document (or program) by "including" or "requiring" those smaller pieces. This is a common enough way to build programs. Combine this with the common tendency to allow attackers to influence the location of some of these pieces - perhaps even from the attacker's own server - then suddenly you're importing somebody else's code. In these Web 2.0 days, maybe it's just "the way the Web works," but not if security is a consideration.

No alerts in this category.

(17) Incorrect Permission Assignment for Critical Resource

It's rude to take something without asking permission first, but impolite users (i.e., attackers) are willing to spend a little time to see what they can get away with. If you have critical programs, data stores, or configuration files with permissions that make your resources readable or writable by the world - well, that's just what they'll become. While this issue might not be considered during implementation or design, sometimes that's where the solution needs to be applied. Leaving it up to a harried sysadmin to notice and make the appropriate changes is far from optimal, and sometimes impossible.

No alerts in this category.

(18) Use of Potentially Dangerous Function

Safety is critical when handling power tools. The programmer's toolbox is chock full of power tools, including library or API functions that make assumptions about how they will be used, with no guarantees of safety if they are abused. If potentially-dangerous functions are not used properly, then things can get real messy real quick.

No alerts in this category.

(19) Use of a Broken or Risky Cryptographic Algorithm

If you are handling sensitive data or you need to protect a communication channel, you may be using cryptography to prevent attackers from reading it. You may be tempted to develop your own encryption scheme in the hopes of making it difficult for attackers to crack. This kind of grow-your-own cryptography is a welcome sight to attackers. Cryptography is just plain hard. If brilliant mathematicians and computer scientists worldwide can't get it right (and they're always breaking their own stuff), then neither can you. You might think you created a brand-new algorithm that nobody will figure out, but it's more likely that you're reinventing a wheel that falls off just before the parade is about to start.

No alerts in this category.

(20) Incorrect Calculation of Buffer Size

In languages such as C, where memory management is the programmer's responsibility, there are many opportunities for error. If the programmer does not properly calculate the size of a buffer, then the buffer may be too small to contain the data that the programmer plans to write - even if the input was properly validated. Any number of problems could produce the incorrect calculation, but when all is said and done, you're going to run head-first into the dreaded buffer overflow.

No alerts in this category.

(21) Improper Restriction of Excessive Authentication Attempts

An often-used phrase is "If at first you don't succeed, try, try again." Attackers may try to break into your account by writing programs that repeatedly guess different passwords. Without some kind of protection against brute force techniques, the attack will eventually succeed. You don't have to be advanced to be persistent.

No alerts in this category.

(22) URL Redirection to Untrusted Site ('Open Redirect')

While much of the power of the World Wide Web is in sharing and following links between web sites, typically there is an assumption that a user should be able to click on a link or perform some other action before being sent to a different web site. Many web applications have implemented redirect features that allow attackers to specify an arbitrary URL to link to, and the web client does this automatically. This may be another of those features that are "just the way the web works," but if left unchecked, it could be useful to attackers in a couple important ways. First, the victim could be autoamtically redirected to a malicious site that tries to attack the victim through the web browser. Alternately, a phishing attack could be conducted, which tricks victims into visiting malicious sites that are posing as legitimate sites. Either way, an uncontrolled redirect will send your users someplace that they don't want to go.

No alerts in this category.

(23) Uncontrolled Format String

The mantra is that successful relationships depend on communicating clearly, and this applies to software, too. Format strings are often used to send or receive well-formed data. By controlling a format string, the attacker can control the input or output in unexpected ways - sometimes, even, to execute code.

No alerts in this category.

(24) Integer Overflow or Wraparound

In the real world, 255+1=256. But to a computer program, sometimes 255+1=0, or 0-1=65535, or maybe 40,000+40,000=14464. You don't have to be a math whiz to smell something fishy. Actually, this kind of behavior has been going on for decades, and there's a perfectly rational and incredibly boring explanation. Ultimately, it's buried deep ir the DNA of computers, who can't count to infinity even if it sometimes feels like they take that long to complete an important task. When programmers forget that computers don't do math like people, bad things ensue - anywhere from crashes, faulty price calculations, infinite loops, and execution of code.

No alerts in this category.

(25) Use of a One-Way Hash without a Salt

Salt might not be good for your diet, but it can be good for your password security. Instead of storing passwords in plain text, a common practice is to apply a one-way hash, which effectively randomizes the output and can make it more difficult if (or when?) attackers gain access to your password database. If you don't add a little salt to your hash, then the health of your application is in danger.

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