PENETRATION TESTING REPORT

MANOJ V

ANNA UNIVERSITY
REGIONAL CAMPUS
COIMBATORE

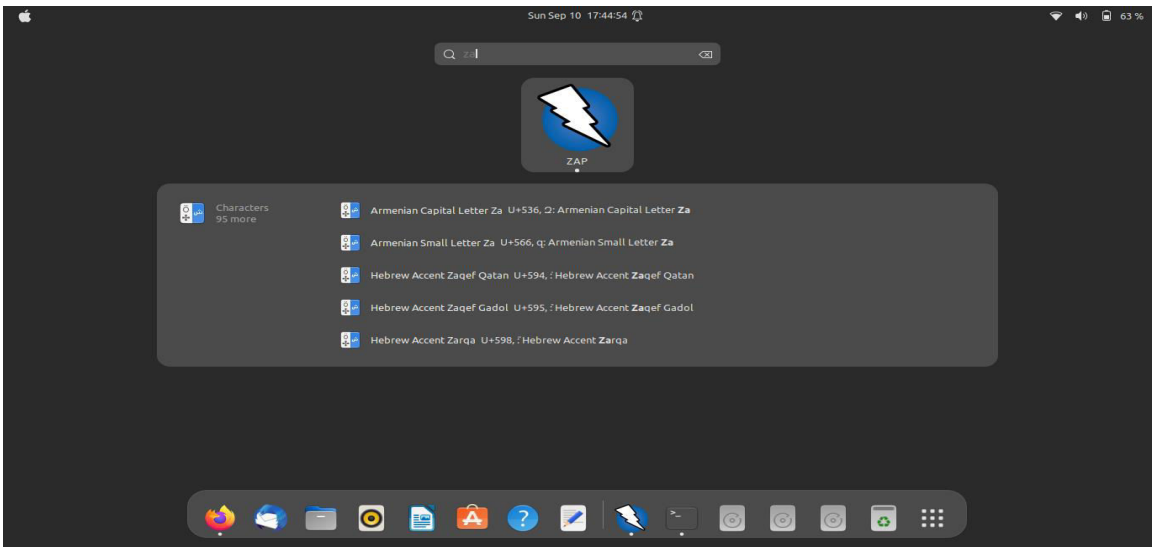
CYBER SECURITY

AUGUST-SEPTEMBER
BATCH

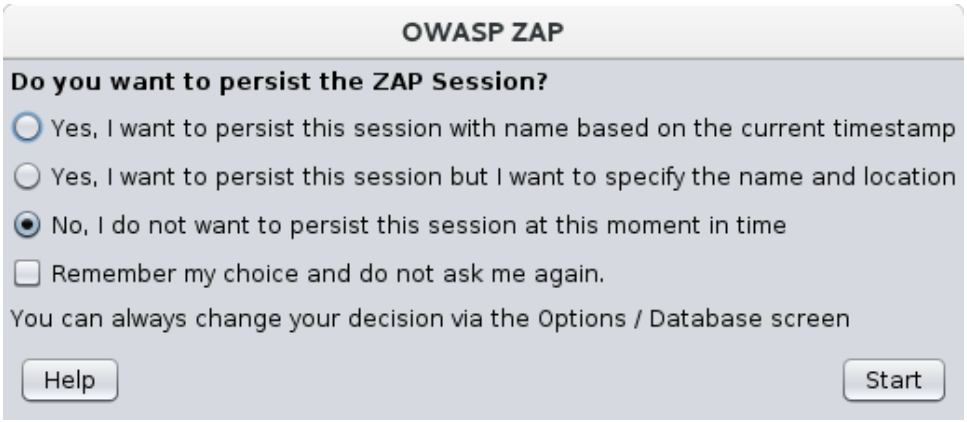
INSTALL AND CONFIGURE ZAP

The first thing is installing ZAP on the system you intend to perform pen testing on any website.

```
manoj@manoj:~$ sudo apt install snapd
[sudo] password for manoj:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snapd is already the newest version (2.58+22.04.1).
snapd set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
manoj@manoj:~$ sudo snap install zaproxy --classic
zaproxy 2.13.0 from Simon Bennetts (psiinon) installed
```

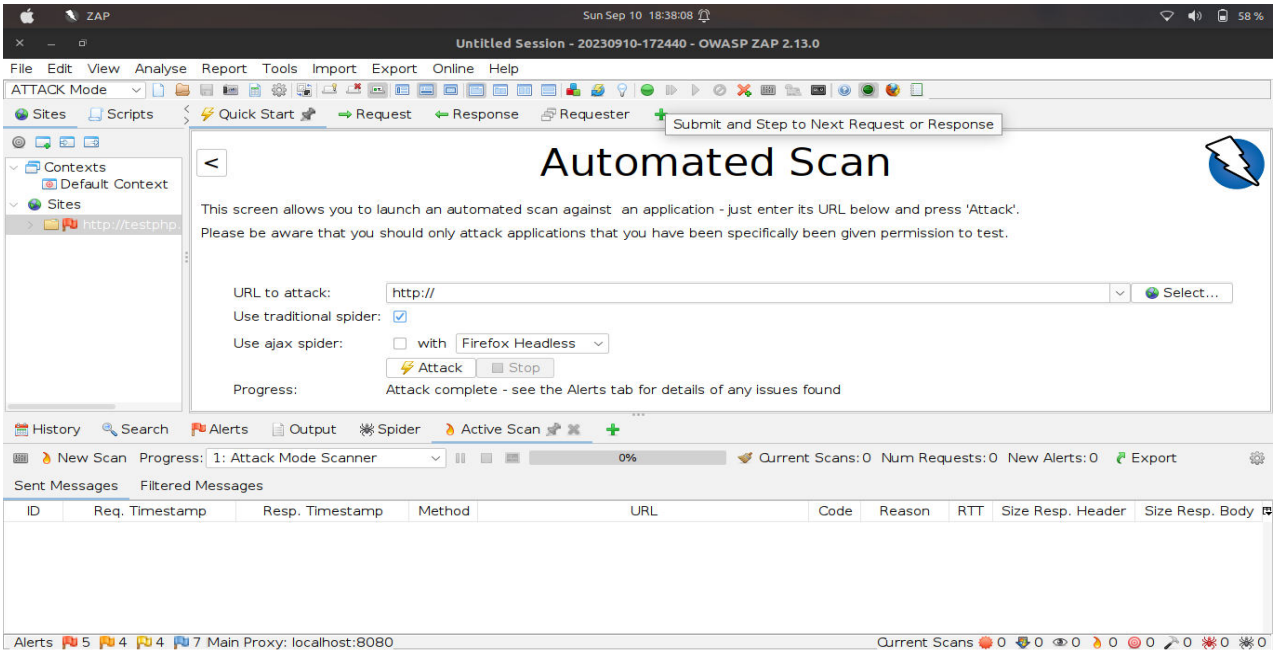


PERSISTING A SESSION



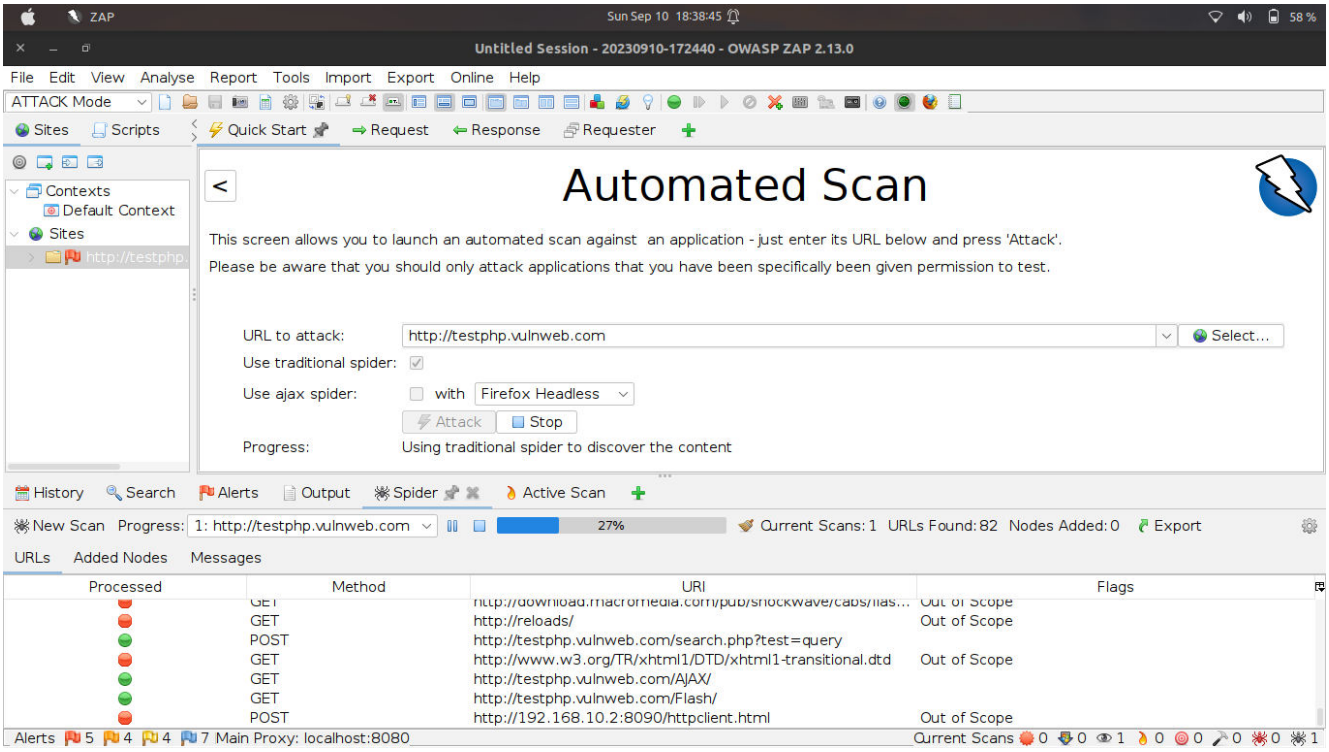
I clicked third option because, I do not want to save the session for this moment.

ZAP DESKTOP UI

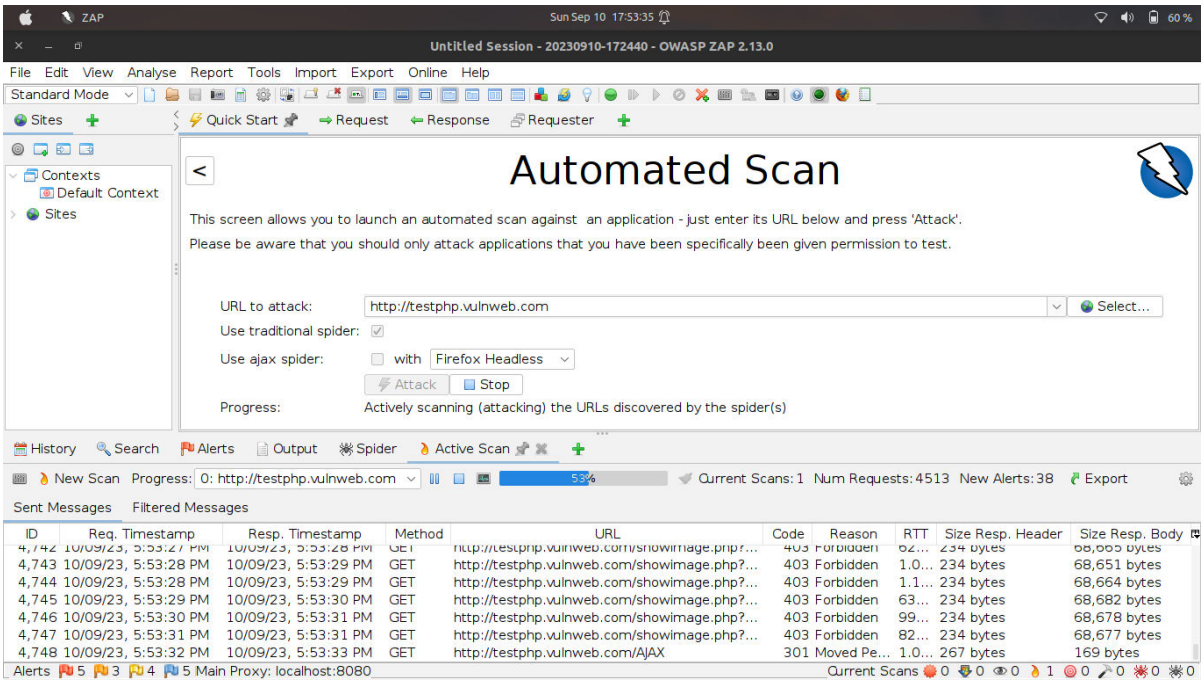


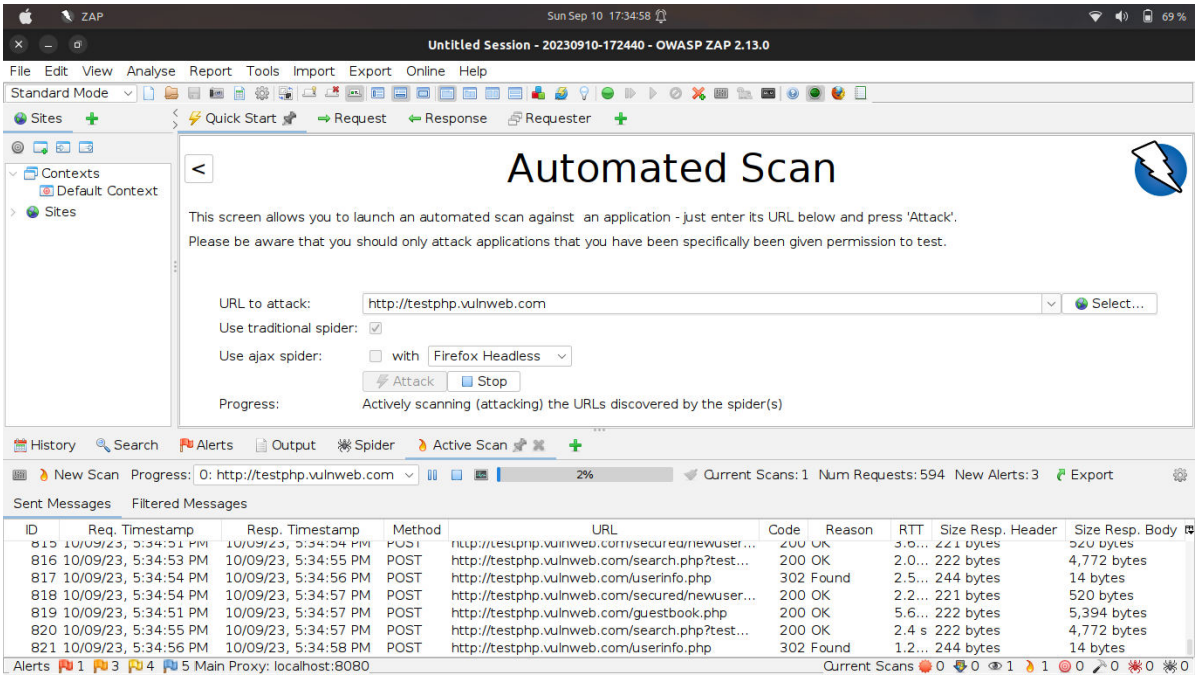
PEN TESTING:

1.Enter the test website link
http://testphp.vulnweb.com



2.Enter the attack button to start the vulnerability test on test website link.





ZAP Scanning Report

Site: http://testphp.vulnweb.com

Generated on Sun, 10 Sep 2023 18:10:46

ZAP Version: 2.13.0

Summary of Alerts

Risk Level	Number of Alerts
High	5
Medium	4
Low	4
Informational	7

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (Reflected)	High	13
Path Traversal	High	3
SQL Injection	High	9
SQL Injection - MySQL	High	6
SQL Injection - SQLite	High	7
.htaccess Information Leak	Medium	7
Absence of Anti-CSRF Tokens	Medium	60
Content Security Policy (CSP) Header Not Set	Medium	68
Missing Anti-clickjacking Header	Medium	44
Private IP Disclosure	Low	20
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	47
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	52
X-Content-Type-Options Header Missing	Low	46
Authentication Request Identified	Informational	1
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	31
GET for POST	Informational	1
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	9
User Agent Fuzzer	Informational	271
User Controllable HTML Element Attribute (Potential XSS)	Informational	3

Alert Detail

High	**Cross Site Scripting (Reflected)**
	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.
Description	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://testphp.vulnweb.com/hpp/?pp=%22%3E%3Cscrlpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Parameter	pp
Attack	"><scrlpt>alert(1);</scRipt>
Evidence	"><scrlpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/hpp/params.php?p=%3Cscrlpt%3Ealert%281%29%3B%3C%2FscRipt%3E&pp=12
Method	GET
Parameter	p
Attack	<scrlpt>alert(1);</scRipt>
Evidence	<scrlpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=%3Cscrlpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET

Parameter	pp
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/listproducts.php?artist=%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E
Method	GET
Parameter	artist
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://testphp.vulnweb.com/listproducts.php?cat=%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E
Method	GET
Parameter	cat
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	name
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	text
Attack	</td><scrIpt>alert(1);</scRipt><td>
Evidence	</td><scrIpt>alert(1);</scRipt><td>
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	searchFor
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uaddress
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST

Parameter	ucc
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uemail
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uphone
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uuname
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Instances	13
Solution	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.

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 **Path Traversal**

Description

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 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://testphp.vulnweb.com/cart.php
Method	POST
Parameter	addcart
Attack	\cart.php
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	text
Attack	\guestbook.php
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	searchFor
Attack	/search.php
Evidence	

Instances 3

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."

Solution 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	**SQL Injection**
Description	SQL injection may be possible.
URL	http://testphp.vulnweb.com/artists.php?artist=5-2
Method	GET
Parameter	artist
Attack	5-2
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3+AND+1%3D1+--+
Method	GET
Parameter	artist
Attack	3 OR 1=1 --
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+
Method	GET
Parameter	cat
Attack	4 OR 1=1 --
Evidence	

URL	http://testphp.vulnweb.com/product.php?pic=9-2
Method	GET
Parameter	pic
Attack	9-2
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uaddress
Attack	AND 1=1 --
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	urname
Attack	ZAP AND 1=1 --
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uuname
Attack	ZAP' OR '1'='1' --
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	pass
Attack	ZAP' OR '1'='1' --
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	uname
Attack	ZAP AND 1=1 --
Evidence	
Instances	9
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	40018
High	**SQL Injection - MySQL**
Description	SQL injection may be possible.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	artist
Attack	3 and 0 in (select sleep(15)) --
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	artist
Attack	3 / sleep(15)
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	cat
Attack	4 / sleep(15)
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	pic
Attack	7 / sleep(15)

Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	searchFor
Attack	ZAP' / sleep(15) / '
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uuname
Attack	ZAP' / sleep(15) / '
Evidence	
Instances	6
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	40019

High **SQL Injection - SQLite**

Description	SQL injection may be possible.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET

Parameter	artist
Attack	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [612] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1,229] milliseconds, when the original unmodified query with value [3] took [1,002] milliseconds.
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	p
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [922] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [923] milliseconds, when the original unmodified query with value [valid] took [870] milliseconds.
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	artist
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [921] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,228] milliseconds, when the original unmodified query with value [3] took [916] milliseconds.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	name
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [921] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [935] milliseconds, when the original unmodified query with value [ZAP] took [908] milliseconds.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	submit
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [849] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,585] milliseconds, when the original unmodified query with value [add message] took [624] milliseconds.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST

Parameter	text
Attack	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [612] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1,220] milliseconds, when the original unmodified query with value [] took [553] milliseconds.
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	signup
Attack	case randomblob(100000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1,191] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1,535] milliseconds, when the original unmodified query with value [signup] took [920] milliseconds.
Instances	7
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

Medium	**.htaccess Information Leak**
Description	htaccess files can be used to alter the configuration of the Apache Web Server software to enable/disable additional functionality and features that the Apache Web Server software has to offer.

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/.htaccess
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 200 OK

Instances	7
Solution	Ensure the .htaccess file is not accessible.
Reference	http://www.htaccess-guide.com/
CWE Id	94
WASC Id	14
Plugin Id	40032

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://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/artists.php?artist=2

Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/Flash/add.swf
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="post" name="faddentry">
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET

Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/images/logo.gif
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/images/remark.gif
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET

Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	<form name="loginform" method="post" action="userinfo.php">
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Method	GET

Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET

Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET

Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET

Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Method	GET

Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	<form id='portal_url' action='http://192.168.10.2:8090/httpclient.html' method= 'POST'>
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	<form name="form1" method="post" action="/secured/newuser.php">
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	
Attack	
Evidence	<form action="" method="post" name="faddentry">
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST

Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Instances	60
Solution	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. 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 **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://testphp.vulnweb.com
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/categories.php
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Flash/add.swf
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/images/logo.gif
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/images/remark.gif
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/privacy.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	
Attack	
Evidence	
Instances	68
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	**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://testphp.vulnweb.com
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/categories.php

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST

Parameter	x-frame-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Instances	44
	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.
Solution	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

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://testphp.vulnweb.com/Flash/add.swf
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/images/logo.gif
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/images/remark.gif
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg

Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160

Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Method	GET

Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	192.168.10.2:8090
Instances	20
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://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/artists.php
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/privacy.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Instances	47
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://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/AJAX/styles.css
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/login.php
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/privacy.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/style.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST

Parameter	
Attack	
Evidence	nginx/1.19.0
Instances	52
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://testphp.vulnweb.com
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/AJAX/styles.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET

Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/style.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Instances	46
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	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uemail
Attack	
Evidence	upass
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Charset Mismatch (Header Versus Meta Content-Type Charset)**
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	

Evidence	
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	

URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3

Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET

Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	
Attack	
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST

Parameter	
Attack	
Evidence	
Instances	31
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	**GET for POST**
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Parameter	
Attack	
Evidence	GET http://testphp.vulnweb.com/cart.php?addcart=3&price=986 HTTP/1.1
Instances	1
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

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://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	where
Instances	1
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://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	titles
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	comment on this artist
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	comment on this artist
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	comment on this artist
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	comment on this artist
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	

Attack	
Evidence	comment on this picture
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	comment on this picture
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Parameter	
Attack	
Evidence	comment on this picture
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Parameter	
Attack	
Evidence	comment on this picture
Instances	9
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://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/AJAX
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Flash

Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Flash
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php

Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/high
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/hpp
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	

URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	

URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/images
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/index.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0

Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	Header User-Agent

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://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/login.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET

Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured

Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/sitemap.xml

Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php

Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	

URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/cart.php
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
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://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	271
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://testphp.vulnweb.com/guestbook.php
Method	POST
Parameter	submit
Attack	
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	goButton
Attack	
Evidence	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	goButton
Attack	
Evidence	
Instances	3
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