kiwiz.co.uk

Scan time

Scan started
2018-01-04 16:12

Scan finished
2018-01-04 18:32

detectify

Finding summary

🔴	Login Cross Site Request Forgery (CSRF/XSRF)	2
🟠	Cross Site Request Forgery (CSRF/XSRF)	1
🟠	Login over HTTP-GET	2
🟠	Name Server Unavailable	1
🟠	External Links using target='_blank'	1
🟠	SSL Certificate Name Mismatch	1
🟠	TLS 1.0 Deprecated Protocol	5
🔵	Lacking HSTS Response Header	1
🔵	Referrer-Policy Not Implemented	8
🟢	Content Sniffing	2
🟢	Crawled URL's	1
🟢	Discovered Host(s)	1
🟢	Email Enumeration	1
🟢	Fingerprinted Software	8
🟢	HTML Comments	1

Scan settings

Scan subdomains	Yes
Scan as device	Detectify

●	Remote Administration Portal	2
●	Service Providers	1
●	WHOIS	1

● Login Cross Site Request Forgery (CSRF/XSRF)

What does this mean?

The web site seems to be lacking CSRF token on a login form.

our knowledge base (http://support.detectify.com/customer/portal/articles/1969819-login-csrf).

What can happen?

An attacker can force an unsuspecting user to sign in to the attacker's account. What can be done from there depends on the application. Example: An attacker can force an unsuspecting user to login to the attacker's account and when the user buys something, the credit card is added to the attacker's account.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	6.2
2	https://box.kiwiz.co.uk/admin	6.2

1. Login Cross Site Request Forgery (CSRF/XSRF)

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
6.2 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-inline" role="form" onsubmit="return do_add_user(); return false;">
  <div class="form-group">
    <label class="sr-only" for="adduserEmail">Email address</label>
    <input type="email" class="form-control" id="adduserEmail" placeholder="Email Address">
  </div>
  <div class="form-group">
    <label class="sr-only" for="adduserPassword">Password</label>
    <input type="password" class="form-control" id="adduserPassword"
placeholder="Password">
  </div>
  <div class="form-group">
    <select class="form-control" id="adduserPrivs">
      <option value="">Normal User
      <option value="admin">Administrator
    </select>
  </div>
  <button type="submit" class="btn btn-primary">Add User</button>
</form>
```

Resources

REMEDIATION - Detectify Support Center - Login CSRF
REMEDIATION - Detectify Support Center - CSRF
STACK OVERFLOW - How to protect against login CSRF?
VIDEO - What is a CSRF?

1. Login Cross Site Request Forgery (CSRF/XSRF)

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
6.2 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-horizontal" role="form" onsubmit="do_login(); return false;">
  <div class="form-group">
   <label for="inputEmail3" class="col-sm-3 control-label">Email</label>
   <div class="col-sm-9">
    <input name="email" type="email" class="form-control" id="loginEmail"
placeholder="Email">
   </div>
  </div>
  <div class="form-group">
   <label for="inputPassword3" class="col-sm-3 control-label">Password</label>
   <div class="col-sm-9">
    <input name="password" type="password" class="form-control" id="loginPassword"
placeholder="Password">
   </div>
  </div>
  <div class="form-group">
   <div class="col-sm-offset-3 col-sm-9">
    <div class="checkbox">
     <label>
      <input name='remember' type="checkbox" id="loginRemember"> Remember me
     </label>
    </div>
   </div>
  </div>
  <div class="form-group">
   <div class="col-sm-offset-3 col-sm-9">
    <button type="submit" class="btn btn-default">Sign in</button>
   </div>
  </div>
 </form>
```

Resources

REMEDIATION - Detectify Support Center - Login CSRF
REMEDIATION - Detectify Support Center - CSRF
STACK OVERFLOW - How to protect against login CSRF?
VIDEO - What is a CSRF?

● Cross Site Request Forgery (CSRF/XSRF)

What does this mean?

The site doesn't check for tokens or make sure that the request really is from the user in any other way.

here (http://support.detectify.com/customer/portal/articles/2792245-csrf).

What can happen?

An attacker can force a victim to perform unwanted actions at the site.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	5.8

1. Cross Site Request Forgery (CSRF/XSRF)

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
5.8 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-horizontal" role="form" onsubmit="do_set_custom_dns(); return false;">
  <div class="form-group">
    <label for="customdnsQname" class="col-sm-1 control-label">Name</label>
    <div class="col-sm-10">
      <table style="max-width: 400px">
      <tr><td>
        <input type="text" class="form-control" id="customdnsQname" placeholder="subdomain">
      </td><td style="padding: 0 1em; font-weight: bold;">.</td><td>
        <select id="customdnsZone" class="form-control"> </select>
      </td></tr></table>
      <div class="text-info" style="margin-top: .5em">Leave the left field blank to set a record on
the chosen domain name, or enter a subdomain.</div>
    </div>
  </div>
  <div class="form-group">
    <label for="customdnsType" class="col-sm-1 control-label">Type</label>
    <div class="col-sm-10">
      <select id="customdnsType" class="form-control" style="max-width: 400px"
onchange="show_customdns_rtype_hint()">
        <option value="A" data-hint="Enter an IPv4 address (i.e. a dotted quad, such as
123.456.789.012).">A (IPv4 address)
        <option value="AAAA" data-hint="Enter an IPv6 address.">AAAA (IPv6 address)
        <option value="CAA" data-hint="Enter a CA that can issue certificates for this domain in
the form of FLAG TAG VALUE. (0 issuewild &quot;letsencrypt.org&quot;)">CAA (Certificate
Authority Authorization)
        <option value="CNAME" data-hint="Enter another domain name followed by a period at the
end (e.g. mypage.github.io.).">CNAME (DNS forwarding)
        <option value="TXT" data-hint="Enter arbitrary text.">TXT (text record)
        <option value="MX" data-hint="Enter record in the form of PRIORITY DOMAIN., including
trailing period (e.g. 20 mx.example.com.).">MX (mail exchanger)
        <option value="SRV" data-hint="Enter record in the form of PRIORITY WEIGHT PORT
TARGET., including trailing period (e.g. 10 10 5060 sip.example.com.).">SRV (service record)
        <option value="SSHFP" data-hint="Enter record in the form of ALGORITHM TYPE
FINGERPRINT.">SSHFP (SSH fingerprint record)
        <option value="NS" data-hint="Enter a hostname to which this subdomain should be
delegated to">NS (DNS subdomain delegation)
      </select>
    </div>
  </div>
  <div class="form-group">
    <label for="customdnsValue" class="col-sm-1 control-label">Value</label>
    <div class="col-sm-10">
      <input type="text" class="form-control" id="customdnsValue" placeholder="">
      <div id="customdnsTypeHint" class="text-info" style="margin-top: .5em"></div>
    </div>
  </div>
  <div class="form-group">
    <div class="col-sm-offset-1 col-sm-11">
      <button type="submit" class="btn btn-primary">Set Record</button>
    </div>
  </div>
</form>
```

Resources

REMEDIATION - Detectify Support Center - CSRF
DETECTIFY - CAPTCHA does not prevent CSRF
VIDEO - What is a CSRF?

● Login over HTTP-GET

What does this mean?

The login form is sending data using HTTP GET-request.

What can happen?

Passwords may appear visible in the URL and stored in the browser's history. It may also be cached by immediate proxies and getting stored in remote server logs.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	5
2	https://box.kiwiz.co.uk/admin	5

1. Login over HTTP-GET

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
5 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-inline" role="form" onsubmit="return do_add_user(); return false;">
  <div class="form-group">
    <label class="sr-only" for="adduserEmail">Email address</label>
    <input type="email" class="form-control" id="adduserEmail" placeholder="Email Address">
  </div>
  <div class="form-group">
    <label class="sr-only" for="adduserPassword">Password</label>
    <input type="password" class="form-control" id="adduserPassword"
placeholder="Password">
  </div>
  <div class="form-group">
    <select class="form-control" id="adduserPrivs">
      <option value="">Normal User
      <option value="admin">Administrator
    </select>
  </div>
  <button type="submit" class="btn btn-primary">Add User</button>
</form>
```

Resources

VIDEO - What is Missing Function Level Access Control?

1. Login over HTTP-GET

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
5 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-horizontal" role="form" onsubmit="do_login(); return false;">
  <div class="form-group">
   <label for="inputEmail3" class="col-sm-3 control-label">Email</label>
   <div class="col-sm-9">
    <input name="email" type="email" class="form-control" id="loginEmail"
placeholder="Email">
   </div>
  </div>
  <div class="form-group">
   <label for="inputPassword3" class="col-sm-3 control-label">Password</label>
   <div class="col-sm-9">
    <input name="password" type="password" class="form-control" id="loginPassword"
placeholder="Password">
   </div>
  </div>
  <div class="form-group">
   <div class="col-sm-offset-3 col-sm-9">
    <div class="checkbox">
     <label>
      <input name='remember' type="checkbox" id="loginRemember"> Remember me
     </label>
    </div>
   </div>
  </div>
  <div class="form-group">
   <div class="col-sm-offset-3 col-sm-9">
    <button type="submit" class="btn btn-default">Sign in</button>
   </div>
  </div>
 </form>
```

Resources

VIDEO - What is Missing Function Level Access Control?

● Name Server Unavailable

What does this mean?

A name server is unavailable.

What can happen?

If the name server fails to respond to queries, no one will be able to access the web site.

Summary

Entry	Found at	CVSS
1	188.213.174.30	5

1. Name Server Unavailable

Summary

Found At
188.213.174.30

CVSS
5 of 10.0

Details

Affecting the domains kiwiz.co.uk and www.kiwiz.co.uk.

● External Links using target='_blank'

What does this mean?

Links using target='_blank' gain partial access to the linking page via the window.opener object.

here (http://support.detectify.com/customer/portal/articles/2792257-external-links-using-target-_blank-).

What can happen?

The linked page will be able to interact with the originating tab, reading the tab's current URL and redirecting the user to other domains. The linked page will have access to the tab for as long as it remains open.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	4.9

1. External Links using target='_blank'

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
4.9 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<a href="https://letsencrypt.org/" target="_blank">Let&rsquo;s Encrypt</a>
```

In order to mitigate the issue, add the following attribue to your link(s): rel="noopener noreferrer"

Resources

REMEDIATION - Detectify Support Center - External Links using target='_blank'
MISC - Target="_blank"?-?the most underestimated vulnerability ever
HN - Hacker News Discussion
GITHUB - Target Blank Vulnerability
MISC - When to use target="_blank"

● SSL Certificate Name Mismatch

What does this mean?

The domain name specified in the requested certificate mismatches the requested origin.

here (http://support.detectify.com/customer/portal/articles/2792277-ssl-certificate-name-mismatch).

What can happen?

The web server is likely misconfigured and uses a certificate from another domain. This will cause errors for end-users which is hard to distinguish from real man-in-the-middle (MITM) attacks.

Summary

Entry	Found at	CVSS
1	https://ns1.box.kiwiz.co.uk/	4.8

1. SSL Certificate Name Mismatch

Summary

Found At
https://ns1.box.kiwiz.co.uk/

CVSS
4.8 of 10.0

Details

We analyzed the hostname 'ns1.box.kiwiz.co.uk' against the common name (CN) 'box.kiwiz.co.uk, and against the subject alternative names (SAN) 'box.kiwiz.co.uk', 'kiwiz.co.uk', 'www.kiwiz.co.uk'.

Resources

REMEDIATION - Detectify Support Center - SSL Certificate Name Mismatch
DETECTIFY - A general guide to implementing HTTPS
DETECTIFY - How SSL affects SEO

● TLS 1.0 Deprecated Protocol

What does this mean?

The server accepts TLS 1.0 as encryption protocol, which is no longer considered secure by the credit card industry (PCI DSS 3.1).

However, disabling it may cause some issues with older clients. If a lot of visitors are using web browsers that has not been updated since 2014 it might be required to still support TLS 1.0.

What can happen?

It is possible for an intercepting attacker to either force or downgrade a connection to TLS 1.0 which may be prone to the POODLE vulnerability.

Summary

Entry	Found at	CVSS
1	https://188.213.174.30/	4
2	https://box.kiwiz.co.uk/	4
3	https://kiwiz.co.uk/	4
4	https://ns1.box.kiwiz.co.uk/	4
5	https://www.kiwiz.co.uk/	4

1. TLS 1.0 Deprecated Protocol

Summary

Found At
https://188.213.174.30/

CVSS
4 of 10.0

Details

Affecting the domains kiwiz.co.uk and www.kiwiz.co.uk.

Resources

PCI - Date Change for Migrating from SSL and Early TLS
QUALYS - TLSv1.0- how to disable? should I disable?
STACKEXCHANGE - Should I disable TLS 1.0 on my servers?

1. TLS 1.0 Deprecated Protocol

Summary

Found At
https://box.kiwiz.co.uk/

CVSS
4 of 10.0

Resources

PCI - Date Change for Migrating from SSL and Early TLS
QUALYS - TLSv1.0- how to disable? should I disable?
STACKEXCHANGE - Should I disable TLS 1.0 on my servers?

1. TLS 1.0 Deprecated Protocol

Summary

Found At
https://kiwiz.co.uk/

CVSS
4 of 10.0

Resources

PCI - Date Change for Migrating from SSL and Early TLS
QUALYS - TLSv1.0- how to disable? should I disable?
STACKEXCHANGE - Should I disable TLS 1.0 on my servers?

1. TLS 1.0 Deprecated Protocol

Summary

Found At
https://ns1.box.kiwiz.co.uk/

CVSS
4 of 10.0

Resources

PCI - Date Change for Migrating from SSL and Early TLS
QUALYS - TLSv1.0- how to disable? should I disable?
STACKEXCHANGE - Should I disable TLS 1.0 on my servers?

1. TLS 1.0 Deprecated Protocol

Summary

Found At
https://www.kiwiz.co.uk/

CVSS
4 of 10.0

Resources

PCI - Date Change for Migrating from SSL and Early TLS
QUALYS - TLSv1.0- how to disable? should I disable?
STACKEXCHANGE - Should I disable TLS 1.0 on my servers?

● Lacking HSTS Response Header

What does this mean?

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS).

What can happen?

The lack of HSTS allows an attacker to perform Man-in-the-middle attacks on clients on WiFi-networks.

Summary

Entry	Found at	CVSS
1	https://www.kiwiz.co.uk/	2.4

1. Lacking HSTS Response Header

Summary

Found At
https://www.kiwiz.co.uk/

CVSS
2.4 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	www.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 301 Moved Permanently

Connection	keep-alive
Content-Length	178
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Location	https://kiwiz.co.uk/
Server	nginx

Details

The header must be tested with a low timeout before being pushed to production websites. Once you have confirmed that the header works as expected, then increase the timeout to the industry best practice of 31536000-seconds (a year). Failure to properly sanity check that the header works as expected can cause the site to be unreachable for the amount of seconds set in the header value.

Resources

OWASP - Test HTTP Strict Transport Security
OWASP - HTTP Strict Transport Security Cheat Sheet
OWASP - Transport Layer Protection Cheat Sheet
MOZILLA - Strict-Transport-Security
WIKIPEDIA - HTTP Strict Transport Security
MISC - What Is HSTS and How Do I Implement It?
MISC - HTTP Strict Transport Security for Apache, NGINX and Lighttpd
MISC - How to enable HTTP Strict Transport Security (HSTS) in IIS7+

● Referrer-Policy Not Implemented

What does this mean?

No referrer policy was found in the response and browsers will therefore use their default referrer policy.

What can happen?

Browsers may send sensitive information if it is stored in the URL to external websites.

Summary

Entry	Found at	CVSS
1	http://box.kiwiz.co.uk/	1.8
2	http://kiwiz.co.uk/	1.8
3	http://ns1.box.kiwiz.co.uk/	1.8
4	http://www.kiwiz.co.uk/	1.8
5	https://box.kiwiz.co.uk/	1.8
6	https://kiwiz.co.uk/	1.8
7	https://ns1.box.kiwiz.co.uk/	1.8
8	https://www.kiwiz.co.uk/	1.8

1. Referrer-Policy Not Implemented

Summary

Found At
http://box.kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US
Host	box.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 301 Moved Permanently

Connection	keep-alive
Content-Length	178
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Location	https://box.kiwiz.co.uk/
Server	nginx

Details

> No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
http://kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 301 Moved Permanently

Connection	keep-alive
Content-Length	178
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Location	https://kiwiz.co.uk/
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
http://ns1.box.kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	ns1.box.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 301 Moved Permanently

Connection	keep-alive
Content-Length	178
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Location	https://box.kiwiz.co.uk/
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
http://www.kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	www.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 301 Moved Permanently

Connection	keep-alive
Content-Length	178
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Location	https://www.kiwiz.co.uk/
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
https://box.kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	box.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
Connection	keep-alive
Strict-Transport-Security	max-age=31536000
Content-Encoding	gzip
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Last-Modified	Thu, 04 Jan 2018 16:01:53 GMT
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
https://kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
Connection	keep-alive
Strict-Transport-Security	max-age=31536000
Content-Encoding	gzip
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Last-Modified	Thu, 04 Jan 2018 16:01:53 GMT
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
https://ns1.box.kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	ns1.box.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
Connection	keep-alive
Strict-Transport-Security	max-age=31536000
Content-Encoding	gzip
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Last-Modified	Thu, 04 Jan 2018 16:01:53 GMT
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy

MISC - Using CORS policies to implement CSRF protection

MOZILLA - Tighter Control Over Your Referrers

MOZILLA - Referrer-Policy

OWASP - Secure Headers Project

W3C - Referrer Policy

1. Referrer-Policy Not Implemented

Summary

Found At
https://www.kiwiz.co.uk/

CVSS
1.8 of 10.0

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Host	www.kiwiz.co.uk
Cache-Control	no-store, no-cache
Pragma	no-cache

Response Headers

HTTP/ 1.1 301 Moved Permanently

Connection	keep-alive
Content-Length	178
Content-Type	text/html
Date	Thu, 04 Jan 2018 16:32:29 GMT
Location	https://kiwiz.co.uk/
Server	nginx

Details

No Referrer-Policy was found in the response headers. It must be implemented to prevent the application from sending CSRF tokens, PII and other sensitive information stored in URL parameters to third party websites.

Resources

MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
MOZILLA - Tighter Control Over Your Referrers
MOZILLA - Referrer-Policy
OWASP - Secure Headers Project
W3C - Referrer Policy

● Content Sniffing

What does this mean?

The web site lacks content sniffing hardening techniques.

here (http://support.detectify.com/customer/portal/articles/2792034-content-sniffing).

What can happen?

This may open up for XSS attacks as browsers will attempt to guess how to render specific resources without the correct policies.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin/assets/bootstrap/js/bootstrap.min.js	0
2	https://box.kiwiz.co.uk/admin/assets/jquery.min.js	0

1. Content Sniffing

Summary

Found At
https://box.kiwiz.co.uk/admin/assets/bootstrap/js/bootstrap.min.js

CVSS
0 of 10.0

Request Headers

GET /admin/assets/bootstrap/js/bootstrap.min.js HTTP/1.1

User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Referer	https://box.kiwiz.co.uk/admin
Accept-Encoding	gzip, deflate
Accept-Language	en-US
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1

Response Headers

HTTP/ 1.1 200 OK

Accept-Ranges	bytes
Strict-Transport-Security	max-age=31536000
Server	nginx
ETag	"579627ea-90b5"
Connection	keep-alive
Last-Modified	Mon, 25 Jul 2016 14:53:30 GMT
Content-Length	37045
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	application/x-javascript

Details

Add a X-Content-Type-Options header and set the value to nosniff.

Resources

REMEDIATION - Detectify Support Center - Content sniffing

1. Content Sniffing

Summary

Found At
https://box.kiwiz.co.uk/admin/assets/jquery.min.js

CVSS
0 of 10.0

Request Headers

GET /admin/assets/jquery.min.js HTTP/1.1

User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Referer	https://box.kiwiz.co.uk/admin
Accept-Encoding	gzip, deflate
Accept-Language	en-US
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1

Response Headers

HTTP/ 1.1 200 OK

Accept-Ranges	bytes
Strict-Transport-Security	max-age=31536000
Server	nginx
ETag	"553fb284-14979"
Connection	keep-alive
Last-Modified	Tue, 28 Apr 2015 16:17:08 GMT
Content-Length	84345
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	application/x-javascript

Details

Add a X-Content-Type-Options header and set the value to nosniff.

Resources

REMEDIATION - Detectify Support Center - Content sniffing

● Crawled URL's

What does this mean?

This finding is generated for debugging purposes. A link is associated with this finding containing a CSV file with all crawled URL's.

What can happen?

A scan might take too long due to representative content on the application. Vulnerabilities may also be missed if Detectify lack coverage in some area of the application. If you suspect Detectify can perform better, then take a look at the associated CSV.

Summary

Entry	Found at	CVSS
1	kiwiz.co.uk	0

1. Crawled URL's

Summary

Found At
kiwiz.co.uk

CVSS
0 of 10.0

Details

Detectify tried to access 36 URL's, 28 of these were identified as unique during crawling and went through further testing.

Resources

DETECTIFY - Download Crawled URL's CSV

● Discovered Host(s)

What does this mean?

Detectify has found the following hosts. This is in no way a vulnerability, but should be considered an indicator for what has been covered.

here (http://support.detectify.com/customer/portal/articles/2792024-discovered-endpoint).

Summary

Entry	Found at	CVSS
1	kiwiz.co.uk	0

1. Discovered Host(s)

Summary

Found At
kiwiz.co.uk

CVSS
0 of 10.0

Details

Detectify found and tried to access 4 domains, and have analyzed them for security flaws.

```
Domains:
box.kiwiz.co.uk
kiwiz.co.uk
ns1.box.kiwiz.co.uk
www.kiwiz.co.uk



box.kiwiz.co.uk:
> 188.213.174.30
  80/tcp open
  443/tcp open
  1443/tcp closed
  2082/tcp closed
  2083/tcp closed
  3000/tcp closed
  3001/tcp closed
  3128/tcp closed
  3790/tcp closed
  4443/tcp closed
  4444/tcp closed
  4502/tcp closed
  4505/tcp closed
  4567/tcp closed
  5000/tcp closed
  5050/tcp closed
  5051/tcp closed
  7001/tcp closed
  8069/tcp closed
  8080/tcp closed
  8081/tcp closed
  8111/tcp closed
  8161/tcp closed
  8181/tcp closed
  8443/tcp closed
  8500/tcp closed
  8888/tcp closed
  8983/tcp closed
  9200/tcp closed
  11211/tcp closed
  17000/tcp closed
  61680/tcp closed
  61681/tcp closed
```

```
kiwiz.co.uk:
> 188.213.174.30
  80/tcp open
  443/tcp open
  1443/tcp closed
  2082/tcp closed
  2083/tcp closed
  3000/tcp closed
  3001/tcp closed
  3128/tcp closed
  3790/tcp closed
  4443/tcp closed
  4444/tcp closed
  4502/tcp closed
  4505/tcp closed
  4567/tcp closed
  5000/tcp closed
  5050/tcp closed
  5051/tcp closed
  7001/tcp closed
  8069/tcp closed
  8080/tcp closed
  8081/tcp closed
  8111/tcp closed
  8161/tcp closed
  8181/tcp closed
  8443/tcp closed
  8500/tcp closed
  8888/tcp closed
  8983/tcp closed
  9200/tcp closed
  11211/tcp closed
  17000/tcp closed
  61680/tcp closed
  61681/tcp closed



ns1.box.kiwiz.co.uk:
> 188.213.174.30
  80/tcp open
  443/tcp open
  1443/tcp closed
  2082/tcp closed
  2083/tcp closed
  3000/tcp closed
  3001/tcp closed
  3128/tcp closed
  3790/tcp closed
  4443/tcp closed
  4444/tcp closed
  4502/tcp closed
  4505/tcp closed
  4567/tcp closed
  5000/tcp closed
  5050/tcp closed
  5051/tcp closed
  7001/tcp closed
  8069/tcp closed
  8080/tcp closed
  8081/tcp closed
  8111/tcp closed
  8161/tcp closed
  8181/tcp closed
  8443/tcp closed
  8500/tcp closed
  8888/tcp closed
  8983/tcp closed
  9200/tcp closed
  11211/tcp closed
  17000/tcp closed
  61680/tcp closed
  61681/tcp closed
```

```
www.kiwiz.co.uk:
> 188.213.174.30
  80/tcp open
  443/tcp open
  1443/tcp closed
  2082/tcp closed
  2083/tcp closed
  3000/tcp closed
  3001/tcp closed
  3128/tcp closed
  3790/tcp closed
  4443/tcp closed
  4444/tcp closed
  4502/tcp closed
  4505/tcp closed
  4567/tcp closed
  5000/tcp closed
  5050/tcp closed
  5051/tcp closed
  7001/tcp closed
  8069/tcp closed
  8080/tcp closed
  8081/tcp closed
  8111/tcp closed
  8161/tcp closed
  8181/tcp closed
  8443/tcp closed
  8500/tcp closed
  8888/tcp closed
  8983/tcp closed
  9200/tcp closed
  11211/tcp closed
  17000/tcp closed
  61680/tcp closed
  61681/tcp closed
```

● Email Enumeration

What does this mean?

The web site reveals one or more email addresses in plain text.

here (http://support.detectify.com/customer/portal/articles/2792087-email-enumeration).

What can happen?

Spammers can easily gather these email addresess and use them in spam campaigns. An attacker may also use those email adressess for spear phishing and other attacks.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	0

1. Email Enumeration

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
0 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Email

```
me@mydomain.com

my_email@mydomain.com

new_alias@mydomail.com

new_user@mydomail.com

you@yourdomain.com
```

Resources

REMEDIATION - Detectify Support Center - Email enumeration

Fingerprinted Software

What does this mean?

When Detectify audits an application, it collects various fingerprints that indicate what software is running. These fingerprints then allow Detectify to run specific tests when the time is right.

Please make sure Detectify provide accurate data for these fingerprints, by sending us a message in the feedback form on the finding details page.

What can happen?

Invalid fingerprints may cause a audit to take longer, and the lack of fingerprints may cause Detectify to miss running specific tests.

Summary

Entry	Found at	CVSS
1	http://box.kiwiz.co.uk/	0
2	http://kiwiz.co.uk/	0
3	http://ns1.box.kiwiz.co.uk/	0
4	http://www.kiwiz.co.uk/	0
5	https://box.kiwiz.co.uk/	0
6	https://kiwiz.co.uk/	0
7	https://ns1.box.kiwiz.co.uk/	0
8	https://www.kiwiz.co.uk/	0

1. Fingerprinted Software

Summary

Found At
http://box.kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
http://kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
http://ns1.box.kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
http://www.kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
https://box.kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx


Vendor:   jquery
Software: jquery
Version:  2.1.4
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
https://kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
https://ns1.box.kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

1. Fingerprinted Software

Summary

Found At
https://www.kiwiz.co.uk/

CVSS
0 of 10.0

Details

```
Vendor:   nginx
Software: nginx
```

Resources

DETECTIFY - An intelligent way to look for vulnerabilities
DETECTIFY - What's under the hood

● HTML Comments

What does this mean?

knowledge base (http://support.detectify.com/customer/en/portal/articles/2243487-html-comments).

What can happen?

The snippets of code within comments will remain inactive until you remove the comment brackets.
The comments might also contain sensitive information not meant for the public.

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	0

1. HTML Comments

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
0 of 10.0

Details

```
<!--/.navbar-collapse -->

<!-- /col -->

<!-- /row -->

<!-- LOCAL BACKUP -->

<!-- RSYNC BACKUP -->

<!-- S3 BACKUP -->

<!-- Common -->

<!-- /container -->
```

Resources

REMEDIATION - Detectify Support Center - HTML Comments

● Remote Administration Portal

What does this mean?

A remote administration interface has been found.

here (http://support.detectify.com/customer/portal/articles/2792091-remote-administration-portal).

Summary

Entry	Found at	CVSS
1	https://box.kiwiz.co.uk/admin	0
2	https://box.kiwiz.co.uk/admin	0

1. Remote Administration Portal

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
0 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-inline" role="form" onsubmit="return do_add_user(); return false;">
  <div class="form-group">
    <label class="sr-only" for="adduserEmail">Email address</label>
    <input type="email" class="form-control" id="adduserEmail" placeholder="Email Address">
  </div>
  <div class="form-group">
    <label class="sr-only" for="adduserPassword">Password</label>
    <input type="password" class="form-control" id="adduserPassword"
placeholder="Password">
  </div>
  <div class="form-group">
    <select class="form-control" id="adduserPrivs">
      <option value="">Normal User
      <option value="admin">Administrator
    </select>
  </div>
  <button type="submit" class="btn btn-primary">Add User</button>
</form>
```

Resources

REMEDIATION - Detectify Support Center - Remote Administration Portal

1. Remote Administration Portal

Summary

Found At
https://box.kiwiz.co.uk/admin

CVSS
0 of 10.0

Request Headers

GET /admin HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response Headers

HTTP/ 1.1 200 OK

Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

```
<form class="form-horizontal" role="form" onsubmit="do_login(); return false;">
  <div class="form-group">
   <label for="inputEmail3" class="col-sm-3 control-label">Email</label>
   <div class="col-sm-9">
    <input name="email" type="email" class="form-control" id="loginEmail"
placeholder="Email">
   </div>
  </div>
  <div class="form-group">
   <label for="inputPassword3" class="col-sm-3 control-label">Password</label>
   <div class="col-sm-9">
    <input name="password" type="password" class="form-control" id="loginPassword"
placeholder="Password">
   </div>
  </div>
  <div class="form-group">
   <div class="col-sm-offset-3 col-sm-9">
    <div class="checkbox">
     <label>
      <input name='remember' type="checkbox" id="loginRemember"> Remember me
     </label>
    </div>
   </div>
  </div>
  <div class="form-group">
   <div class="col-sm-offset-3 col-sm-9">
    <button type="submit" class="btn btn-default">Sign in</button>
   </div>
  </div>
 </form>
```

Resources

REMEDIATION - Detectify Support Center - Remote Administration Portal

● Service Providers

What does this mean?

The listed providers are authorized to host different parts of your infrastructure.

here (http://support.detectify.com/customer/portal/articles/2792249-service-providers).

What can happen?

Anyone can retrieve this data. It's only here to serve as an indicator of what vendors have access to.

Summary

Entry	Found at	CVSS
1	kiwiz.co.uk	0

1. Service Providers

Summary

Found At
kiwiz.co.uk

CVSS
0 of 10.0

Name Service Provider

Self-Hosted

Hosting Provider

Self-Hosted

Mail Provider

Self-Hosted

Resources

REMEDIATION - Detectify Support Center - Service Providers

● WHOIS

What does this mean?

External parties may look up contact information and other data related to your server environment and employees by querying a whois server. These types of lookup services could be used by an attacker to gather intelligence about you and your domain. However, there should always be whois records available. It's a fundamental part of being a domain owner.

here (http://support.detectify.com/customer/portal/articles/2792025-whois).

Summary

Entry	Found at	CVSS
1	kiwiz.co.uk	0

1. WHOIS

Summary

Found At
kiwiz.co.uk

CVSS
0 of 10.0

Command

```
telnet.exe whois.nic.uk 43
kiwiz.co.uk
```

Details

```
Server: whois.nic.uk:43
```

```
    Domain name:
        kiwiz.co.uk

    Registrant:
        Scott D

    Registrant type:
        UK Individual

    Registrant's address:
        The registrant is a non-trading individual who has opted to have their
        address omitted from the WHOIS service.

    Data validation:
        Nominet was not able to match the registrant's name and/or address against a 3rd party
source on 20-Oct-2017

    Registrar:
        eNom LLC [Tag = ENOM]
        URL: http://www.enom.com

    Relevant dates:
        Registered on: 02-Nov-2015
        Expiry date:  02-Nov-2018
        Last updated:  20-Oct-2017

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.box.kiwiz.co.uk       188.213.174.30
        ns2.box.kiwiz.co.uk       188.213.174.30

    DNSSEC:
        Signed

    WHOIS lookup made at 16:16:55 04-Jan-2018

--
This WHOIS information is provided for free by Nominet UK the central registry
for .uk domain names. This information and the .uk WHOIS are:

    Copyright Nominet UK 1996 - 2018.

You may not access the .uk WHOIS or use any data from it except as permitted
by the terms of use available in full at http://www.nominet.uk/whoisterms,
which includes restrictions on: (A) use of the data for advertising, or its
repackaging, recompilation, redistribution or reuse (B) obscuring, removing
or hiding any or all of this notice and (C) exceeding query rate or volume
limits. The data is provided on an 'as-is' basis and may lag behind the
register. Access may be withdrawn or restricted at any time.
```

Resources

REMEDIATION - Detectify Support Center - WHOIS