

---

# IMMUNIWEB EMAIL SECURITY TEST

---

## Table of Contents

1.	General Overview.....	3
2.	High-Level Overview .....	6
3.	Email Server, Blacklists and DNS Security Overview .....	7

## 1. General Overview

### API Specifications

Field Name	Value
Protocol	HTTPS
Request Type	POST
URLs	<p>To initiate the test:  <a href="https://www.immuniweb.com/email/api/v1/check/[ustamp].html">https://www.immuniweb.com/email/api/v1/check/[ustamp].html</a></p> <p>To fetch the results:  <a href="https://www.immuniweb.com/email/api/v1/get_result/[ustamp].html">https://www.immuniweb.com/email/api/v1/get_result/[ustamp].html</a></p> <p>Where <code>[ustamp]</code> is an arbitrary UNIX time-stamp (must be an integer).                      Such construction is done to prevent caching on client side.</p>

### POST Specifications

Field Name	Value
domain	<p><b>Must</b> be a valid domain name.</p> <p>Example: <code>"domain=twitter.com"</code></p>
show_test_results	"false" means that test results will be hidden, "true" means that test results will be displayed in Latest Tests section on ImmuniWeb's website.
recheck	<p>"false" will either use the results from the cache, or start a new test if the target has never been scanned.</p> <p>"true" will start a new test without checking the cache (requires a valid API key, purchased from <a href="https://www.immuniweb.com/email/api">https://www.immuniweb.com/email/api</a> page).</p>
api_key	The optional secret token which you can submit alongside with the request (used only for commercial access).

## Example of a request using cURL

### Step 1: Starting the test

```
curl -d "domain=twitter.com&show_test_results=true&recheck=false"  
https://www.immuniweb.com/email/api/v1/check/1451425590.html
```

If you receive the “test\_cached” status in the response, please proceed to [Step 2.b](#)

If you receive the “test\_started” status in the response, please proceed to [Step 2.a](#)

Response Example (if the test has been found in the cache)

```
{  
  "test_id": "cd9ee9ba7d1d6ba265c1f97bcabf954fa0c1eb84cf6727394d0ef6db536d0c58",  
  "status": "test_cached",  
  "status_id": 3,  
  "message": "Test is cached"  
}
```

Response Example (if the test has **not** been found in the cache):

```
{  
  "job_id": "2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc",  
  "status": "test_started",  
  "status_id": 3,  
  "message": "Test has started"  
}
```

**Step 2.a: Fetching the results if the test was **not** found in the cache (call this until the test is finished)**

```
curl -d "job_id=[job_id FROM STEP 1 RESPONSE]"  
https://www.immuniweb.com/email/api/v1/get_result/1451425590.html
```

Response Example (if the test is **not** finished yet):

```
{  
  "job_id": "0b8c7fdc3fbc97a0ffd309fea77651cc603e64bf710a83642bd442829492e8a9",  
  "status": "in_progress",  
  "status_id": 2,  
  "eta": 2,  
  "message": "Your test is in progress"  
}
```

**Step 2.b: Fetching the results if the test was found in the cache ("test\_cached" status)**

```
curl -d "id=[test_id FROM THE STEP 1 RESPONSE]"  
https://www.immuniweb.com/email/api/v1/get_result/1451425590.html
```

Example with an error

```
curl -d "domain=0.0.0.0&show_test_results=true&recheck=false"  
https://www.immuniweb.com/email/api/v1/check/1451425590.html
```

```
{  
  "error": "Please enter a valid domain name to start the test.",  
  "error_id": 29  
}
```

How to download the PDF

```
curl -d "api_key=YOUR-API-KEY"  
https://www.immuniweb.com/email/gen_pdf/[test_id]/ > report.pdf
```

## 2. High-Level Overview

The output will be composed of the following main elements:

Field Name	Type	Always present	Description
internals	object	Yes	Contains internal information such test IDs, dates, tested domain, etc.
summary	object	Yes	Contains the summary of the test.
test_email	object	Yes	Contains all information from Email Server Security Overview, DNS Security Overview and Email Server Blacklists sections.
test_ssl	object	Yes	Contains the test IDs with all information from Email SSL/TLS Encryption Overview section.  For information on how to use the IDs and request the data from SSL Security Test, please check <a href="https://www.immuniweb.com/ssl/api">https://www.immuniweb.com/ssl/api</a> page.
test_darkweb	object	Yes	Contains the test IDs with all information from Compromised Credentials Overview and Phishing and Domain Squatting Overview sections.  For information on how to use the IDs and request the data from DarkWeb Exposure Security Test, please check <a href="https://www.immuniweb.com/darkweb/api">https://www.immuniweb.com/darkweb/api</a> page.

### 3. Email Server, Blacklists and DNS Security Overview

The “**test\_email**” object contains all information from Email Server Security Overview, DNS Security Overview and Email Server Blacklists sections.

The object consists of 4 other major objects:

- “**main**”, which contains information about the main email security-related DNS records
- “**mx**”, which contains information about the email server’s security configuration and it’s mentions in blacklists or Indicator of Compromise feeds.
- “**dns**”, which contains information about the domain’s SPF, DKIM and DMARC DNS records and related issues.
- “**dnssec**”, which contains information about the DNSSEC configuration and related issues.

Field Name	Type	Always present	Description
main.host	string	Yes	Contains the tested hostname.
main.alerts	object	Yes	Contains high-level summary information about SPF, DKIM and DMARC DNS records checks.
mx.priority	integer	Yes	Indicates the specific MX server’s priority.
mx.alerts	object	Yes	Contains information about Open Relay, VRFY, EXPN, RCPT commands and plain-text authentication checks’ results.
mx.is_firewalled	bool	Yes	Indicates whether the scan has been unsuccessful due to a firewall protection.
mx.ioc_cnt	array	Yes	Indicates the number of Indicator of Compromise (IoC) feeds that the server is mentioned in.
mx.bl_cnt	integer	Yes	Indicates the number of DNS blacklists that the server is mentioned in.
mx.open_ports	array	Yes	Contains information about open SMTP ports on the host.
mx.hostname	string	Yes	Contains the tested hostname.
mx.ip	string	Yes	Contains the IP address that hostname resolves to.
mx.location	object	Yes	Contains the information about the server’s geolocation.
mx.PTR	object	Yes	Contains the results of the server’s PTR record’s check.

dns.spf	object	Yes	Contains the results of the SPF record's analysis. Consists of 2 objects: <ul style="list-style-type: none"><li>• “<b>results</b>”: contains the main results of the checks.</li><li>• “<b>highlights</b>”: contains high-level summary.</li></ul>
dns.dkim	object	Yes	Contains the results of the DKIM record's analysis. Consists of 2 objects: <ul style="list-style-type: none"><li>• “<b>results</b>”: contains the main results of the checks.</li><li>• “<b>highlights</b>”: contains high-level summary.</li></ul>
dns.dmarc	object	Yes	Contains the results of the DMARC record's analysis. Consists of 2 objects: <ul style="list-style-type: none"><li>• “<b>results</b>”: contains the main results of the checks.</li><li>• “<b>highlights</b>”: contains high-level summary.</li></ul>
dnssec.results	object	Yes	Contains the results of the DNSSEC's analysis. Consists of several objects that corresponds to the checked DNS records (e.g. MX, etc).