

## Scan Report

19 May 2021

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Samuel Tselapedi  
stude5st2

Student  
1 Modderfontein Road Sandringham  
Johannesburg, None 2092  
South Africa

## Target and Filters

Scans (1)

Web Application Discovery Scan - 2021-05-19

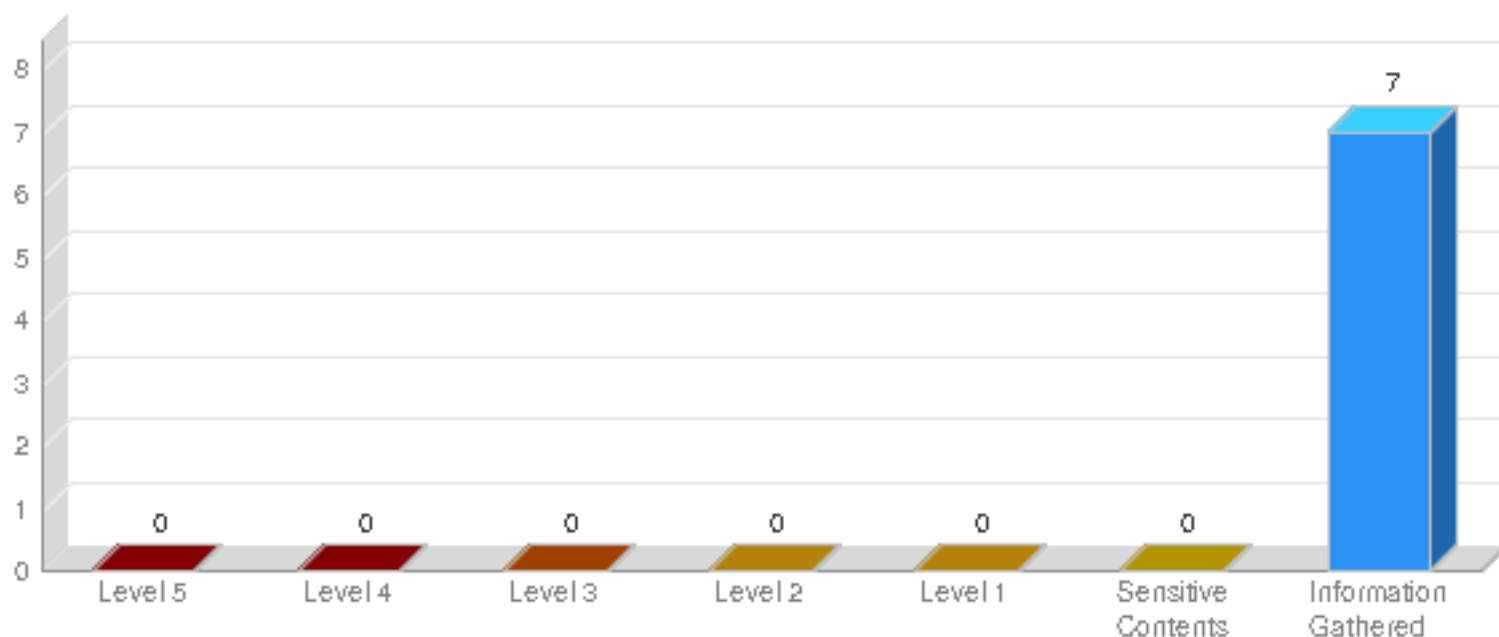
Web Applications (1)

NISM-Group4

## Summary

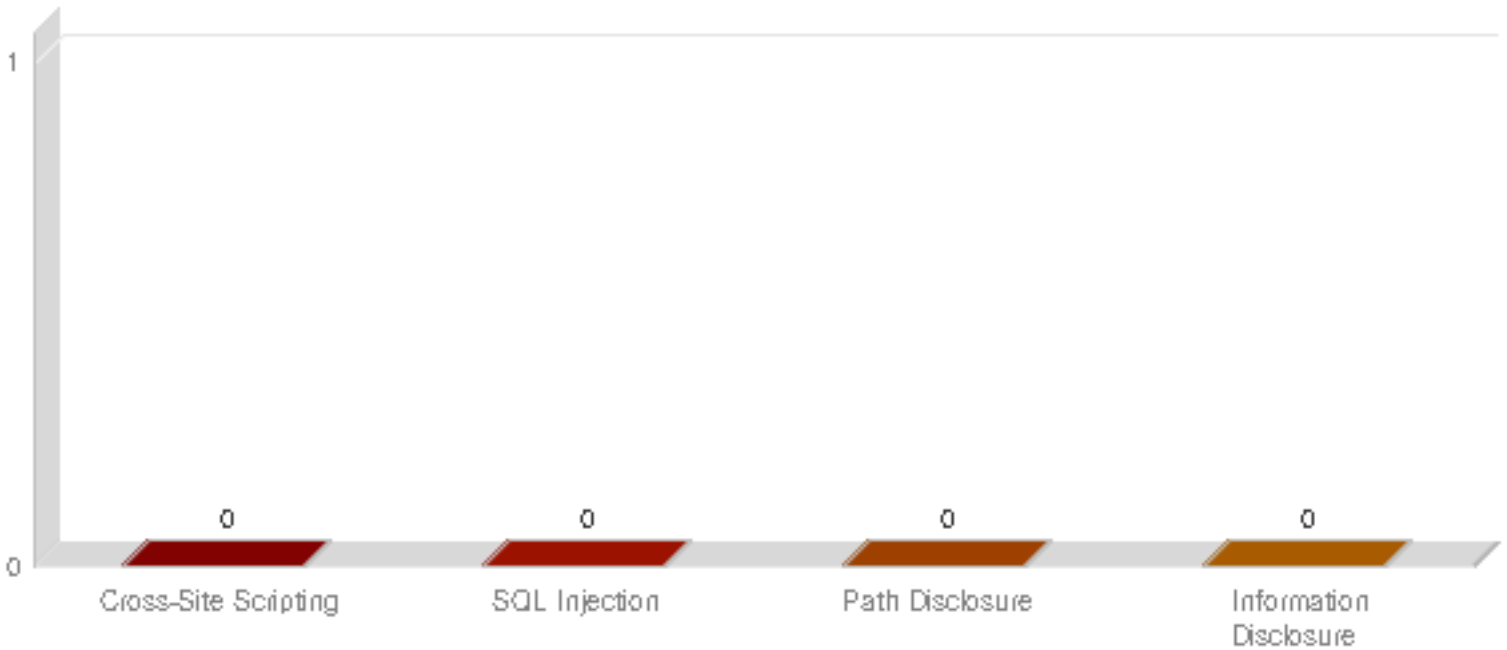
Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
-	0	0	7

### Findings by Severity

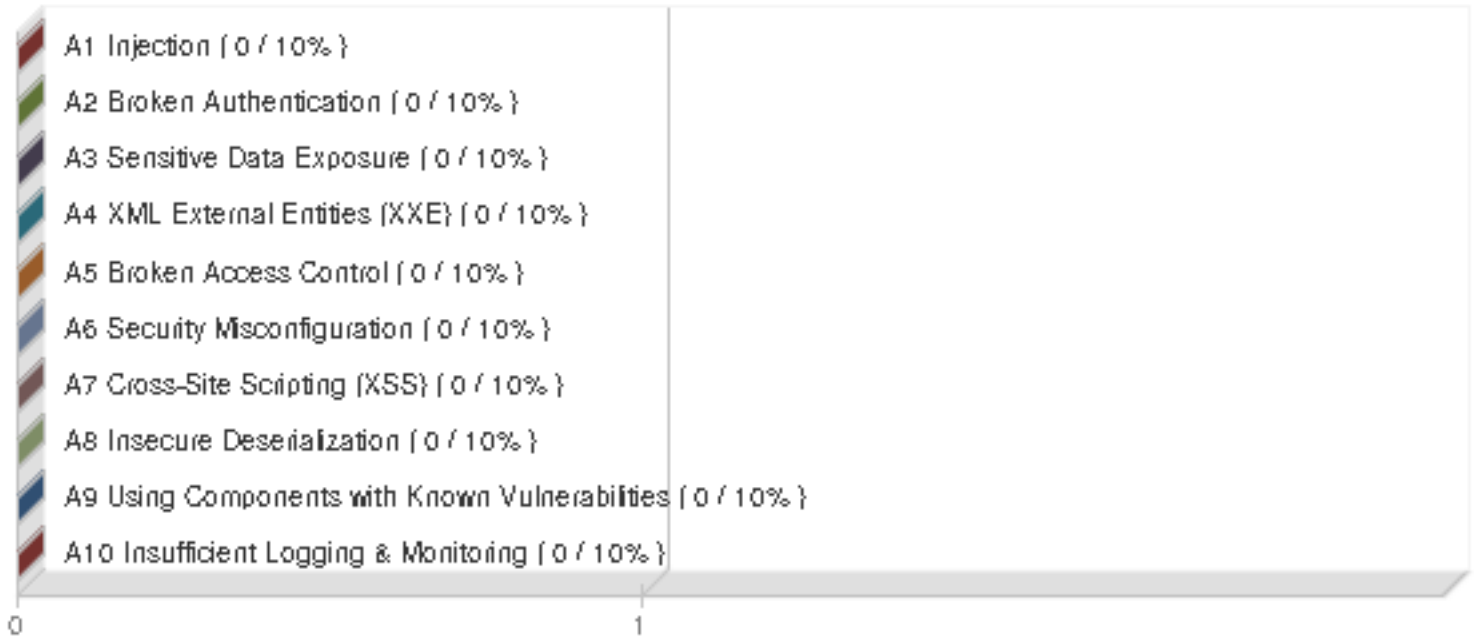


# WAS Scan Report

## Vulnerabilities by Group



## OWASP Top 10 2017 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Web Application Discovery Scan - 2021-05-19	19 May 2021 20:46 GMT +0200	0	0	0	0	0	0	7

CONFIDENTIAL AND PROPRIETARY INFORMATION.

Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2021, Qualys, Inc.

Results(7)

Information Gathered (7)

Scan Diagnostics (7)

6 DNS Host Name (1)

6 DNS Host Name

Finding #	5353483(125766579)	Severity	Information Gathered - Level 1
Unique #	2590605d-6b10-4cfd-97a5-5a9a2fc504b7		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	52.5.180.180
Port	-
Result	#table IP_address Host_name 52.5.180.180 ec2-52-5-180-180.compute-1.amazonaws.com

45038 Host Scan Time (1)

45038 Host Scan Time

Finding #	5353482(125766584)	Severity	Information Gathered - Level 1
Unique #	57d6d874-461b-4feb-8c66-2bca4faecf4a		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

Impact

N/A

Solution

N/A

Results

Scan duration: 56 seconds

Start time: Wed, May 19 2021, 18:46:30 GMT

End time: Wed, May 19 2021, 18:47:26 GMT

150009 Links Crawled (1)

# WAS Scan Report

150009 Links Crawled

Finding #	5353481(125766583)	Severity	Information Gathered - Level 1
Unique #	4af6ba4e-a4ec-462f-8cc0-91efd4ba8efe		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	-		
OWASP	-		
WASC	-		

## Details

### Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

- NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
  - All the forms reported in QID 150152 (Forms Crawled)
  - All the forms in QID 150115 (Authentication Form Found)
  - Certain requests from QID 150172 (Requests Crawled)

### Impact

N/A

### Solution

N/A

## Results

Duration of crawl phase (seconds): 35.00  
Number of links: 5  
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/  
http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/add  
http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/assets/img/background.png  
http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/assets/img/glyphicons-halfplings-white.png  
http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/assets/img/glyphicons-halfplings.png

150010 External Links Discovered (1)

150010 External Links Discovered

Finding #	5353479(125766581)	Severity	Information Gathered - Level 1
Unique #	225d4768-5fa9-40e9-9321-c0560b093975		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact

N/A

Solution

N/A

Results

Number of links: 2  
http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js  
http://html5shim.googlecode.com/svn/trunk/html5.js

150021 Scan Diagnostics (1)

150021 Scan Diagnostics

Finding #	5353478(125766580)	Severity	Information Gathered - Level 1
Unique #	71e1a33b-89b3-46cb-a50e-17f04a45f179		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution


No action is required.

Results

Loaded 0 exclude list entries.  
Loaded 0 allow list entries.  
HTML form authentication unavailable, no WEBAPP entry found  
Target web application page http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/ fetched. Status code:200, Content-Type:text/html, load time:1 milliseconds.  
Ineffective Session Protection. no tests enabled.  
Batch #0 VirtualHostDiscovery: estimated time < 1 minute (70 tests, 0 inputs)  
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 7 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.  
CMS Detection no tests enabled  
Collected 9 links overall in 0 hours 0 minutes duration.  
Cookies Without Consent no tests enabled.  
Total requests made: 95  
Average server response time: 0.18 seconds

150152 Forms Crawled (1)

# WAS Scan Report

 150152 Forms Crawled

Finding #	5353480(125766582)	Severity	Information Gathered - Level 1
Unique #	011d5005-4eb4-44b8-bad9-2672d2b8e96c		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	-		
OWASP	-		
WASC	-		

## Details

### Threat

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

### Impact

N/A

### Solution

N/A

## Results

Total internal forms seen (this count includes duplicate forms): 1

Crawled forms (Total: 1)  
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115  
Form #:1 Action URI:http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/add (found at: http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/add)  
Form Fields: thoughtMessage, thoughtAuthor

 150176 JavaScript Libraries Detected (1)



# WAS Scan Report

150176 JavaScript Libraries Detected

Finding #	5353476(125766578)	Severity	Information Gathered - Level 1
Unique #	7c7cee54-e452-4610-a227-655ec48b806b		
Group	Scan Diagnostics	Detection Date	19 May 2021 20:46 GMT+0200
CWE	CWE-200		
OWASP	-		
WASC	-		

## Details

### Threat

The JavaScript libraries discovered by the scanner are provided in the Results section. The discovered libraries are reported only once based on the page on which they were first detected.

Each library is reported along with other information such as the URL of page on which it was first found, the version, and the URL of the .js file.

### Impact

N/A

### Solution

N/A

## Results

Number of unique JS libraries: 1  
Javascript library : jQuery  
Version : 1.8.3  
Script uri : http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js  
Found on the following page(only first page is reported):  
http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/

Appendix

Scan Details

Web Application Discovery Scan - 2021-05-19

Reference	was/1621449943679.3630911
Date	19 May 2021 20:46 GMT+0200
Mode	On-Demand
Type	Discovery
Authentication	None
Scanner Appliance	External (IP: 64.39.106.91, Scanner: 12.4.33-1, WAS: 8.8.38-1, Signatures: 2.5.190-2)
Profile	Authentication Test
DNS Override	-
Duration	00:00:56
Status	Finished
Authentication Status	None

Option Profile Details

Form Submission	BOTH
Form Crawl Scope	Do not include form action URI in uniqueness calculation
Maximum links to test in scope	100
User Agent	-
Request Parameter Set	Initial Parameters
Document Type	Ignore common binary files
Enhanced Crawling	Disabled
SmartScan	Enabled
SmartScan Depth	5
Timeout Error Threshold	100
Unexpected Error Threshold	300
Performance Settings	Pre-defined
Scan Intensity	Low
Bruteforce Option	Disabled
Detection Scope	Custom Search Lists
Include additional XSS payloads	No
Inclusion Search List Names	Authentication Test
Exclusion Search List Names	-
Inclusion Search List QIDs	150018, 150020, 150021, 150024, 150152, 150025, 150094, 150095, 150028, 150029, 150035, 150097, 150038, 150039, 150036, 150100, 150037, 150101, 150042, 150170, 150040, 150041, 150111, 150115, 150176, 150116, 150006, 150007, 150010, 150008, 150009, 150014, 150143
Exclusion Search List QIDs	-
Credit Card Numbers Search	Off
Social Security Numbers (US) Search	Off

Web Application Details: NISM-Group4

Name	NISM-Group4
ID	25860092

# WAS Scan Report

URL	http://nismphp-env.eba-3mvd2kij.us-east-1.elasticbeanstalk.com/
Owner	Samuel Tselapedi (stude5t2)
Scope	Limit to URL hostname
Tags	-
Custom Attributes	-

## Severity Levels

### Confirmed Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.



Minimal

Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.



Medium

Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.



Serious

Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.



Critical

Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.



Urgent

Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.

### Potential Vulnerabilities

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.



Minimal

Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.



Medium

Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.



Serious

Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.



Critical

Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.



Urgent

Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.

### Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.



Minimal



Medium

Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.



Serious

Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.

Sensitive content was found in the web server response - a valid social security number or credit card information. This information disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.

Information Gathered

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.



Minimal

Intruders may be able to retrieve sensitive information related to the web application platform.



Medium

Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.



Serious

Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.