# 

[**2. Findings**](#_x8yjk25v8ewa) **2**

[2.1. template chapter](#_mpbe3ux0c9if) 2

[2.2. outdated jquery version used](#_4qkvkkiy31) 2

[2.3. outdated Bootstrap Responsive used](#_2hcvoofrh0ru) 3

[2.4. outdated SSH protocol running](#_bqd9aho2r64l) 3

[2.5. deprecated PHP version running](#_1ssilc15rpvh) 4

[2.6. http traffic instead of https](#_fy83hg6ysz2h) 4

# 

# 

# 2. Findings

## 2.1. template chapter

| Owner |  |
| --- | --- |
| Vulnerability description |  |
| target |  |
| CVSS |  |
| Cyber Kill Chain |  |
| Proof of concept |  |
| Remediation |  |
| References |  |

## 2.2. Outdated jQueryversion used (1.8.3)

| Owner | Jan |
| --- | --- |
| Vulnerability description | jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the &#39;&lt;&#39; character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the &#39;&lt;&#39; character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.  jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed. |
| target | <http://nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com/> |
| Risk Score:  Medium |  |
| CVSS |  |
| Proof of concept |  |
| Remediation | update to jQuery 3.60 |
| References | <https://snyk.io/test/npm/jquery/1.8.3>  <https://jquery.com/download/>  Netsparker |

## 2.3. outdated Bootstrap Responsive used

| Owner | Jan |
| --- | --- |
| Vulnerability description | Bootstrap v 2.2.2 is used |
| target | <http://nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com/> |
| CVSS |  |
| Proof of concept |  |
| Remediation | update to Bootstrap v 4.0.0 |
| References | <https://getbootstrap.com/docs/4.0/getting-started/download/> |

## 2.4. outdated SSH protocol running

| Owner | Jan |
| --- | --- |
| Vulnerability description | outdated OpenSSH 7.4 (protocol 2.0) version running on port 22 |
| target | <http://nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com/> |
| CVSS |  |
| Proof of concept |  |
| Remediation | 1. block incoming traffic port 22 (recommended if SSH is not used or 2nd remediation cannot be installed timely) 2. update SSH version |
| References | <https://nvd.nist.gov/vuln/search/results?form_type=Advanced&cves=on&cpe_version=cpe:/a:openbsd:openssh:7.4> |

## 2.5. deprecated PHP version running

deprecated PHP 7.3 running

## 2.6. http traffic instead of https

## 2.6. SQL injection

## 2.6. week AWS password

→ burp bruteforce password?

2.7. Referrer‐Policy Not Implemented

| Owner |  |
| --- | --- |
| Vulnerability description | Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.The lack of Referrer-Policy header might affect privacy of the users and site's itself |
| target | <http://nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com/> |
| Risk Score  Information |  |
| CVSS |  |
| Proof of concept |  |
| Remediation | Implementing a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It’s also possible to control referrer information over an HTML-element by using the rel attribute.  In a response header:    Referrer‐Policy: no‐referrer | same‐origin | origin | strict‐origin | no‐origin‐when‐downgrading  In a META tag  <meta name="Referrer‐Policy" value="no‐referrer | same‐origin"/>  In an element attribute  <a href="[http://crosssite.example.com](http://crosssite.example.com/)" rel="noreferrer"></a>  or    <a href="[http://crosssite.example.com](http://crosssite.example.com/)" referrerpolicy="no‐referrer | same‐origin | origin | strict‐origin | no‐origin‐when‐downgrading"></a> |
| References | [A new security header: Referrer Policy (scotthelme.co.uk)](https://scotthelme.co.uk/a-new-security-header-referrer-policy/) https://scotthelme.co.uk/a-new-security-header-referrer-policy/ |