New issue

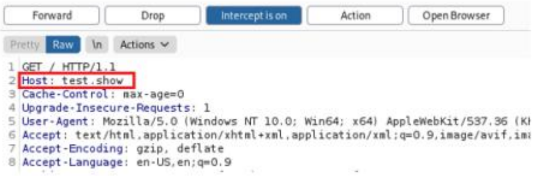
Jump to bottom

HTTP Host Header Attack #1544

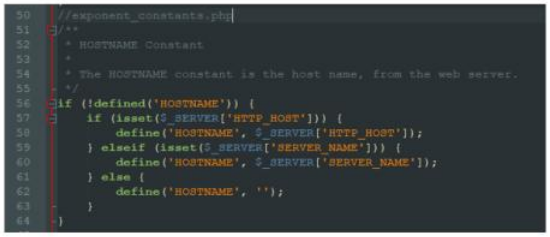
Closed **dumpling-soup** opened this issue on Aug 10, 2021 · 0 comments

dumpling-soup commented on Aug 10, 2021

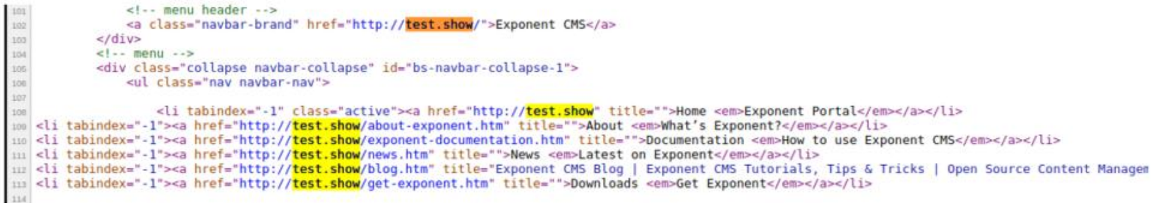
Host value in HTTP header is not checked. Modifying Host header in HTTP request modifies the all links to an arbitrary value. Included example request, result, and location of bug in the source code.



```
GET / HTTP/1.1
Host: test.show
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```



```
//exponent_constants.php
/**
 * HOSTNAME Constant
 *
 * The HOSTNAME constant is the host name, from the web server.
 */
if (!defined('HOSTNAME')) {
    if (isset($_SERVER['HTTP_HOST'])) {
        define('HOSTNAME', $_SERVER['HTTP_HOST']);
    } elseif (isset($_SERVER['SERVER_NAME'])) {
        define('HOSTNAME', $_SERVER['SERVER_NAME']);
    } else {
        define('HOSTNAME', '');
    }
}
```



```
            <!-- menu header -->
            <a class="navbar-brand" href="http://test.show/">Exponent CMS</a>
        </div>
        <!-- menu -->
        <div class="collapse navbar-collapse" id="bs-navbar-collapse-1">
            <ul class="nav navbar-nav">

                <li tabindex="-1" class="active"><a href="http://test.show" title="">Home <em>Exponent Portal</em></a></li>
<li tabindex="-1"><a href="http://test.show/about-exponent.htm" title="">About <em>What's Exponent?</em></a></li>
<li tabindex="-1"><a href="http://test.show/exponent-documentation.htm" title="">Documentation <em>How to use Exponent CMS</em></a></li>
<li tabindex="-1"><a href="http://test.show/news.htm" title="">News <em>Latest on Exponent</em></a></li>
<li tabindex="-1"><a href="http://test.show/blog.htm" title="Exponent CMS Blog | Exponent CMS Tutorials, Tips & Tricks | Open Source Content Managem
<li tabindex="-1"><a href="http://test.show/get-exponent.htm" title="">Downloads <em>Get Exponent</em></a></li>
```

dwisiswant0 mentioned this issue on Aug 16, 2021

Add CVE-2021-38751 projectdiscovery/nuclei-templates#2419

Merged

2 tasks

dleffler referenced this issue on Sep 9, 2021

`fix possible Host Header Injection,CVE-2021-38751` 4042ca2

dleffler closed this as completed on Sep 9, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants