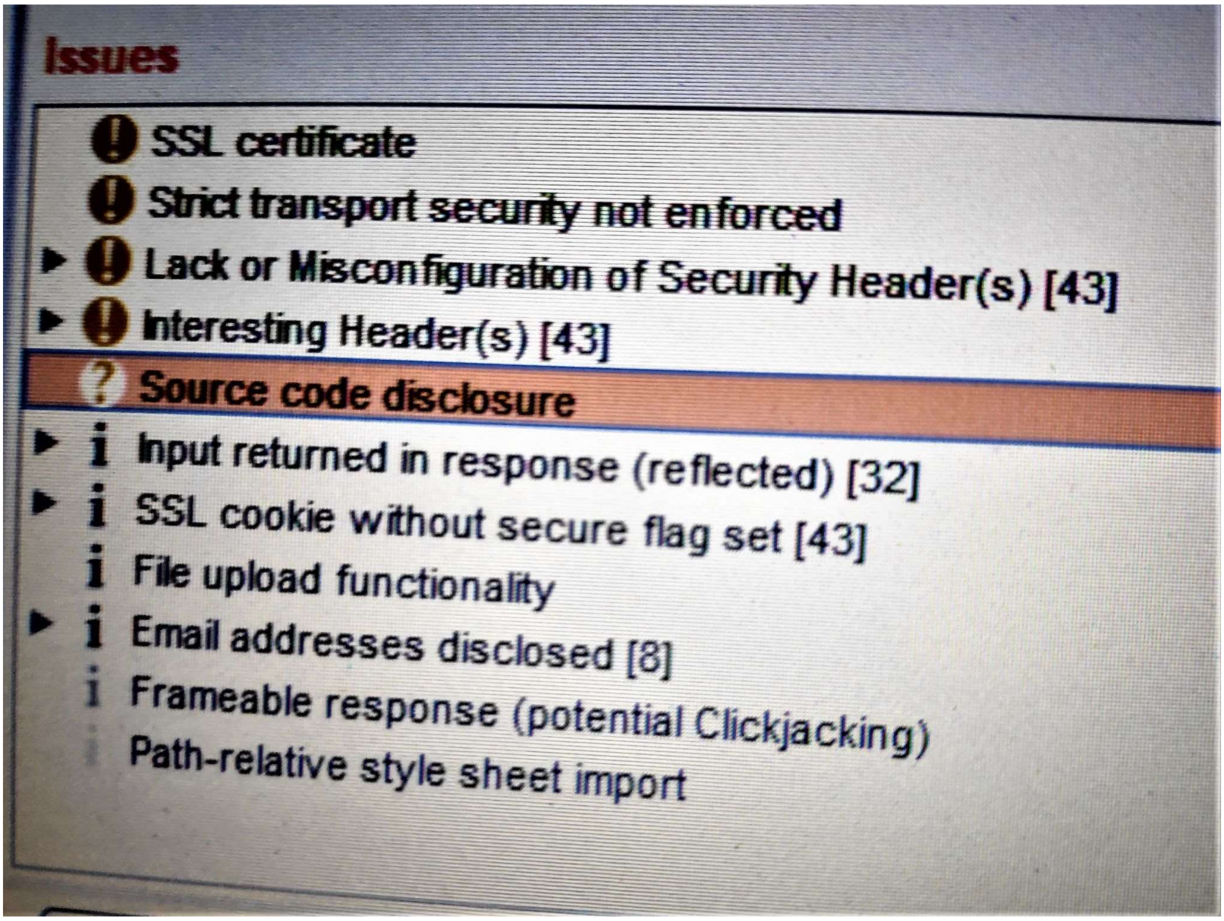
PES UNIVERSITY
INFORMATION SECURITY
BUG BOUNTY

Aayush Kapoor PES2201800211

NOTE: All the severity are in relation to the website https://demopes.eoxvantage.com

Issues:
Listed below are issues found after scanning the website in burp suite pro version.



Issues

- SSL certificate
- Strict transport security not enforced
- Lack or Misconfiguration of Security Header(s) [43]
- Interesting Header(s) [43]
- Source code disclosure
- Input returned in response (reflected) [32]
- SSL cookie without secure flag set [43]
- File upload functionality
- Email addresses disclosed [8]
- Frameable response (potential Clickjacking)
- Path-relative style sheet import

SSL Certificate -

- TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity.
- Severity - Medium

Strict transport security not enforced -

- The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users.
- Enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS.
- Severity - Low

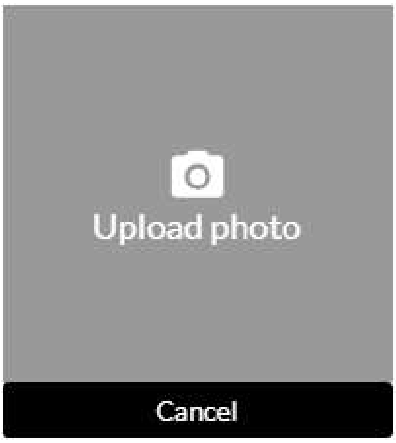
Lack or misconfiguration of security header -

- HTTP security headers are a subset of HTTP headers and are exchanged between a web client (usually a browser) and a server to specify the security-related details of HTTP communication. Some HTTP headers that are indirectly related to privacy and security can also be considered HTTP security headers.
- Severity - Medium

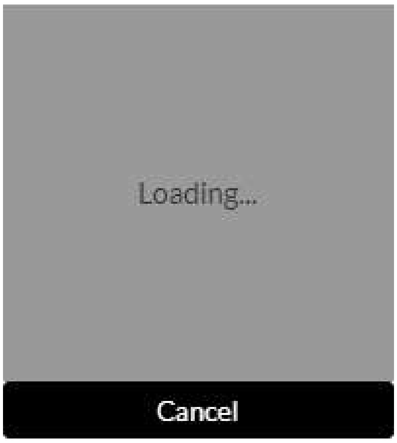
File Upload functionality -

- Whether file/(s) can be uploaded to the website which can be malicious in nature.
- The website does not allow file uploading, other than images like jpeg,png,jpg.
- Severity - Low

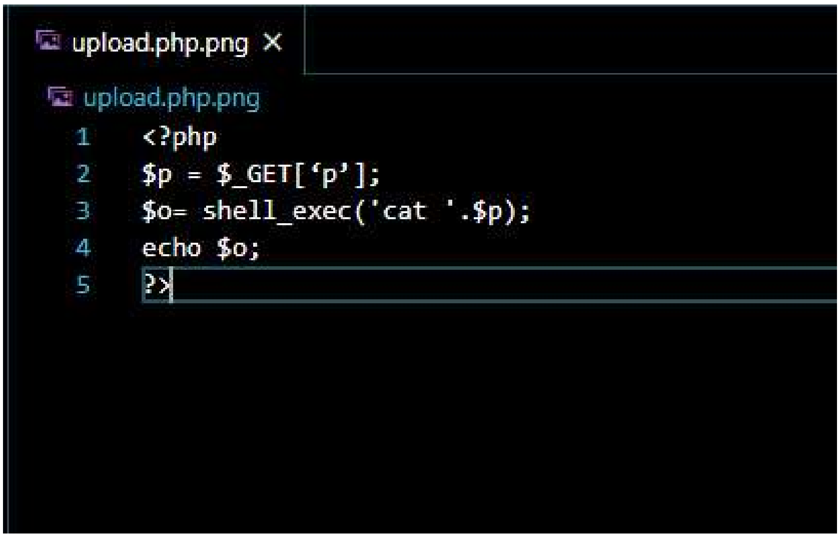
The placeholder for uploading photo/image:



If the format is correct then the image gets uploaded, otherwise throws an error.



Tried uploading a malicious php file as png, but it is protected at it’s best to not allow malicious files onto the server.

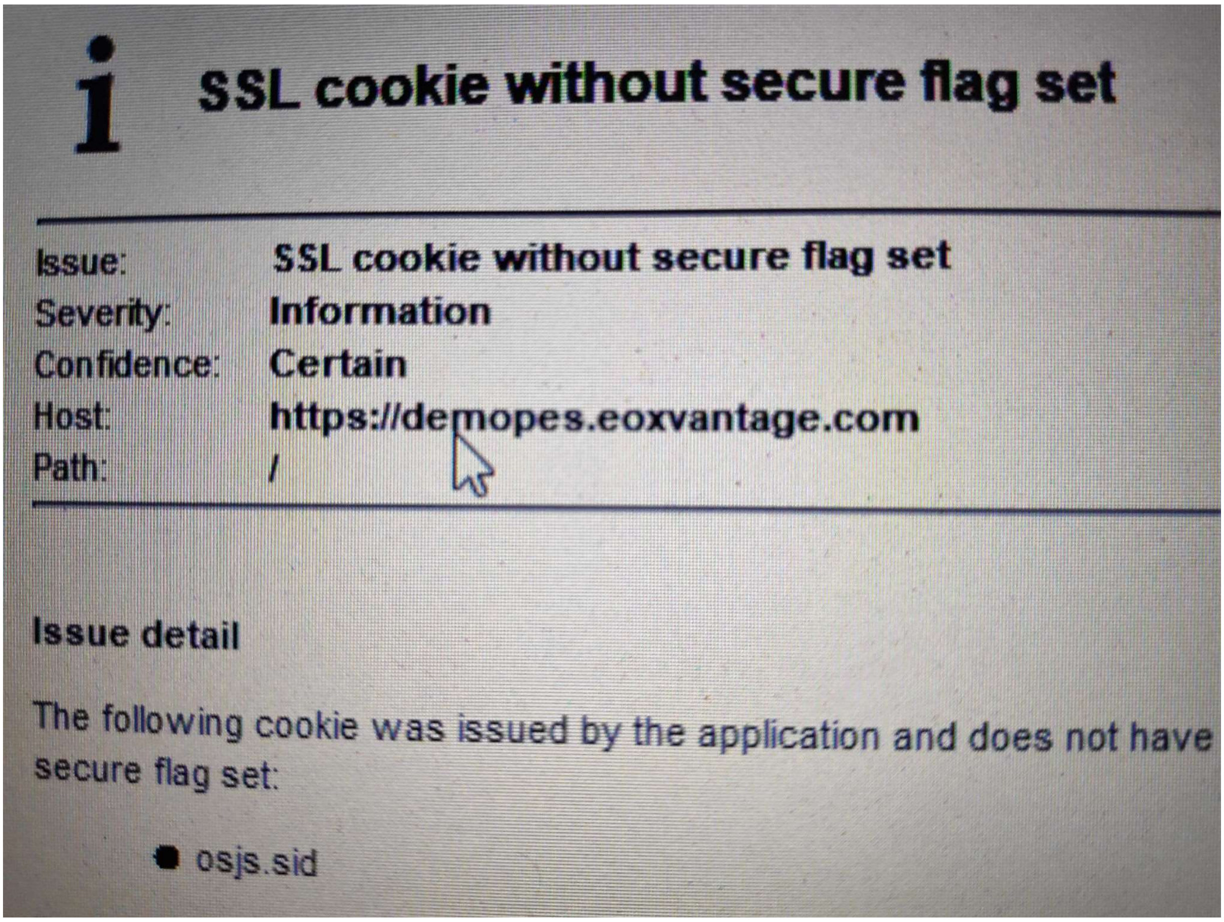


```php
<?php
$p = $_GET[‘p’];
$o= shell_exec('cat '.$p);
echo $o;
?>
```

Referred link:
https://portswigger.net/kb/issues

SSL cookie without secure flag set -

- The cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site.
- The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS.
- Severity - Medium



i SSL cookie without secure flag set

Issue: SSL cookie without secure flag set
Severity: Information
Confidence: Certain
Host: https://demopes.eoxvantage.com
Path: /

Issue detail

The following cookie was issued by the application and does not have secure flag set:

- osjs.sid

Email addresses disclosed -

- Email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel.
- Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.
- There were 8 email addresses found during the scan.
- Severity - Medium

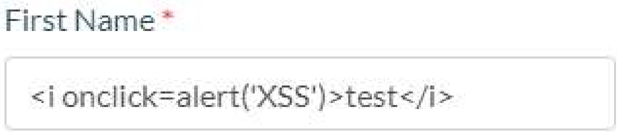
Clickjacking (UI redressing) -

- Clickjacking is an interface-based attack in which a user is tricked into clicking on actionable content on a hidden website by clicking on some other content in a decoy website
- The website does not allow Clickjacking attack.
- Severity - Low

DOM-BASED XSS -

- DOM based XSS is a client side injection issue.
- All the input containers in ‘Edit Profile’ are exposed to DOM-based XSS.
- The site does not implement HTML encoding.
- Severity - High

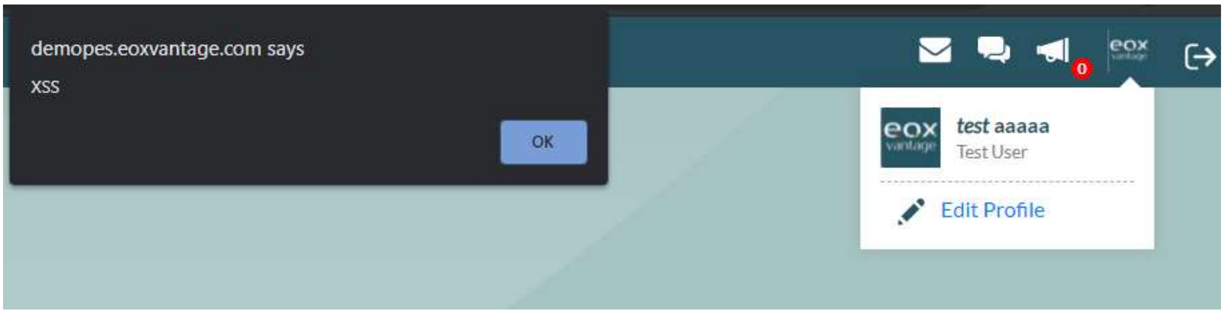
The XSS code:



First Name *

```
<i onclick=alert('XSS')>test</i>
```

Output on clicking *test* (right side of aaaaa):



demopes.eoxvantage.com says

XSS

Referred link: https://portswigger.net/web-security/cross-site-scripting/cheat-sheet

SQL INJECTION -

- Tried sql injection in the login page, but there was none.
- The input is sanitized properly and does not allow attackers to write malicious sql queries in the username and password section.
- Severity - Low

Referred links :
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://portswigger.net/web-security/sql-injection/cheat-sheet

Input returned in response (reflected) -

- Reflection of input arises when data is copied from a request and echoed into the application's immediate response.
- Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection.
- Severity - Medium

Missing Headers -

- Header-name: x-frame-options
- Header-name: x-content-type-options
- Header-name: strict-transport-security
- Header-name: content-security-policy
- Header-name: x-permitted-cross-domain-policies