

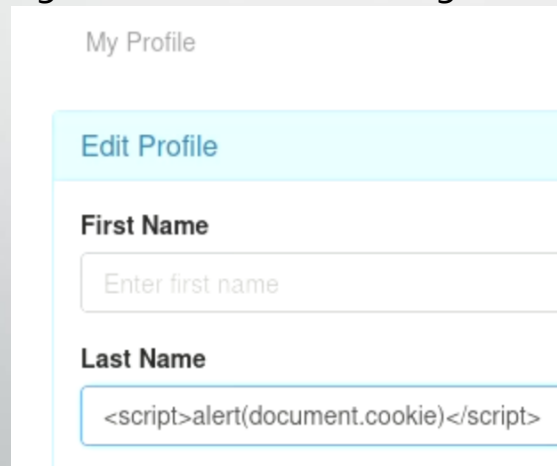
An abstract geometric design in the top-left corner of the slide. It consists of several thick, parallel lines in red and grey, forming a series of nested, angular shapes that point towards the top-left corner.

NodeGoat

By: Theodore Corrello and Mia Weber

A3 Cross Site Scripting (XSS)

- XSS allows attackers to execute code on the target's browser.
- Is usually caused by improper input sanitation.
- To prevent it:
 - Verify that user inputs are being sanitized before being used



My Profile

Edit Profile

First Name

Enter first name

Last Name

<script>alert(document.cookie)</script>

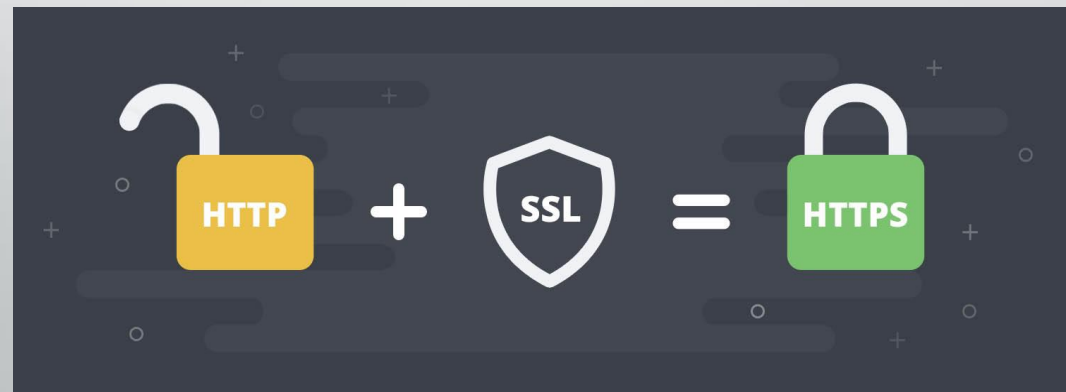
A5 Misconfiguration

- Misconfiguration allows an attacker to access resources they should not have access to and may give them information on how the application is ran.
- Security misconfiguration can happen if the default configurations are kept as is.
- To prevent it:
 - Make sure that all default credentials are changed.
 - Consult documentation to verify any insecure settings are changed.

```
▼ Response Headers (232 B)
? Connection: keep-alive
? Content-Length: 9439
? Content-Type: text/html; charset=utf-8
? Date: Sun, 19 Nov 2023 18:16:51 GMT
? ETag: W/"24df-4b1oU8XBuu1O9Aacy5XippMYB3s"
? Keep-Alive: timeout=5
X-Powered-By: Express
```

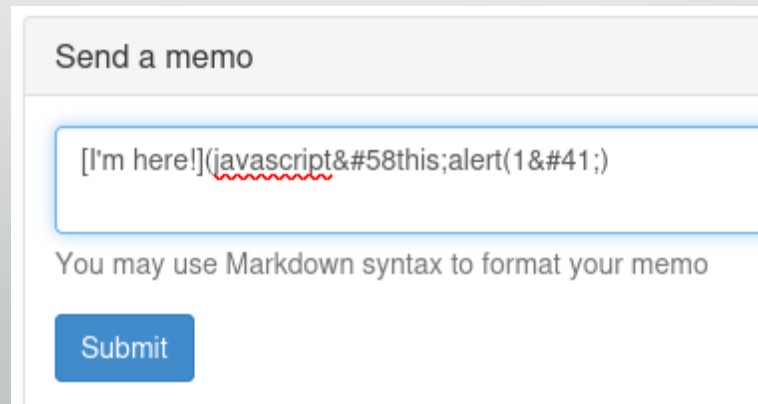
A6 Sensitive Data

- Allows an attacker to access sensitive data such as credit cards, authentication credentials, etc.
- If a site doesn't use SSL/TLS for authenticated pages, an attacker can monitor network traffic and steal a users' session cookie.
- To prevent it:
 - Use HTTPS network protocol
 - Encrypt sensitive data at rest & at transit
 - Use strong standard algorithms and strong keys and ensure proper key management
 - Disable autocomplete on forms collecting sensitive data and disable caching for pages with sensitive data



Ag Insecure Components

- Libraries, frameworks, and other software modules with known vulnerabilities may enable a range of possible attacks.
- Using insecure npm packages can lead to this vulnerability.
- To prevent it:
 - Use resources such as npm audit to keep track of any existing vulnerabilities in installed packages




Send a memo

[I'm here!](javascript:this;alert(1))

You may use Markdown syntax to format your memo

Submit

The screenshot shows a web form titled "Send a memo". It has a text input field containing the text "[I'm here!](javascript:this;alert(1))". The underlined portion of the text is highlighted with a red wavy line, indicating a detected vulnerability or malicious code. Below the input field is a hint that says "You may use Markdown syntax to format your memo". At the bottom of the form is a blue "Submit" button.



Demonstration and Patching Vulnerabilities