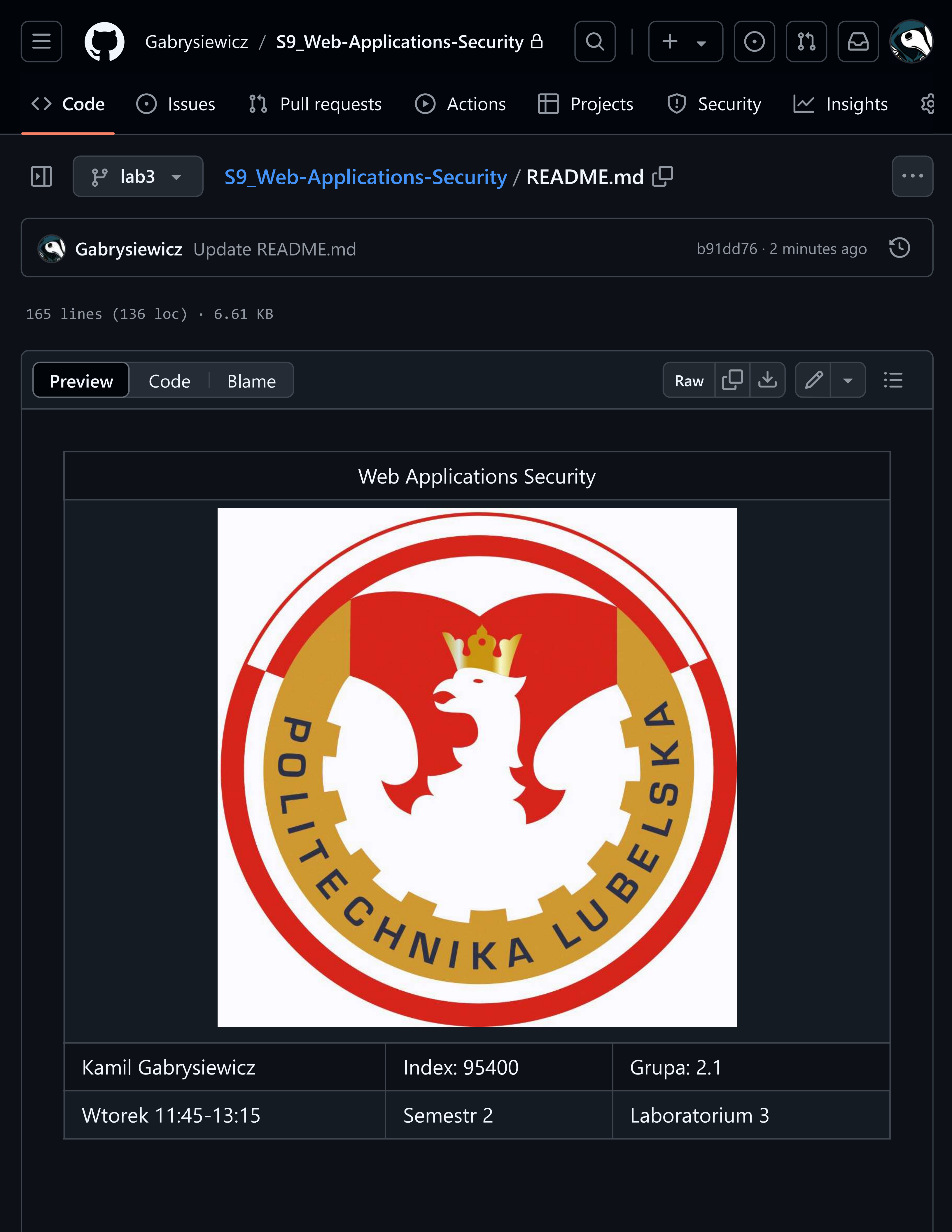
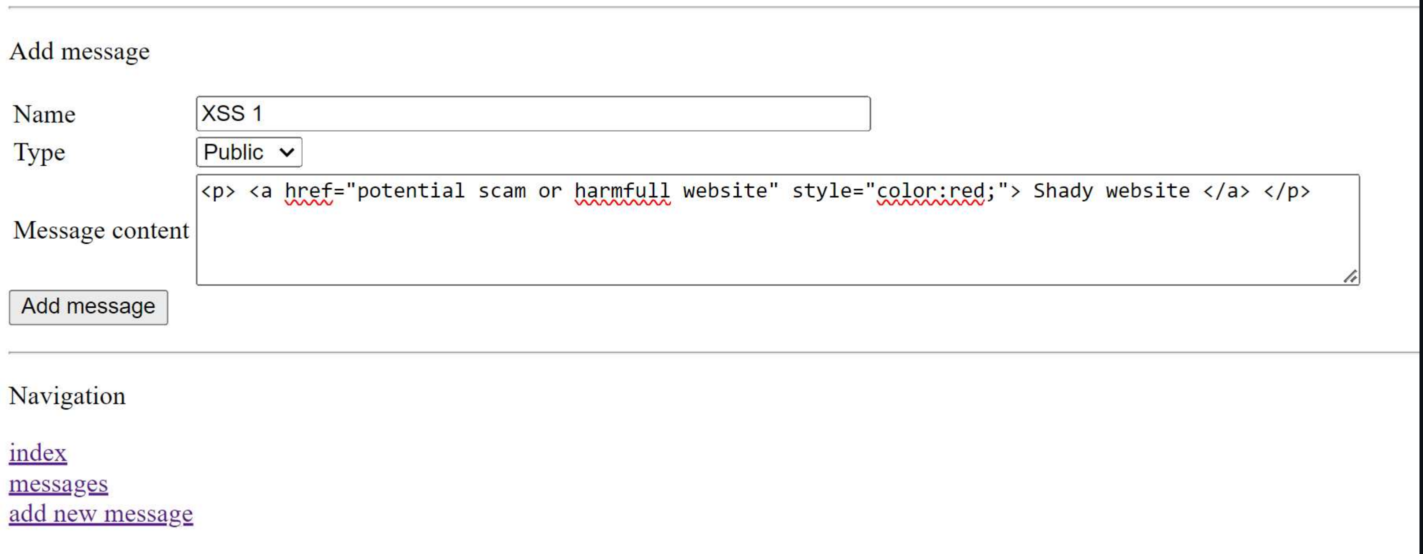

Gabrysiewicz / S9_Web-Applications-Security
Code
Issues
Pull requests
Actions
Projects
Security
Insights
lab3
S9_Web-Applications-Security / README.md
Gabrysiewicz Update README.md
b91dd76 · 2 minutes ago
165 lines (136 loc) · 6.61 KB
Preview
Code
Blame
Raw
POLITECHNIKA LUBELSKA

Web Applications Security		
Kamil Gabrysiewicz	Index: 95400	Grupa: 2.1
Wtorek 11:45-13:15	Semestr 2	Laboratorium 3

Task 3.1.

Based on the lecture materials and sources available on the Internet, develop several XSS attacks on the application used during the laboratory. Present the attacks and their effects. Evaluate how dangerous they may be for the application.

With the use of XSS the content and the visuals of the website could be changed in a way not intended by the developer. Additional unitended content such as links can be added with a delivery to eitherway harmfull or suspicious website, like scam websites or downloadable content that might be malware.



Add message

Name: XSS 1

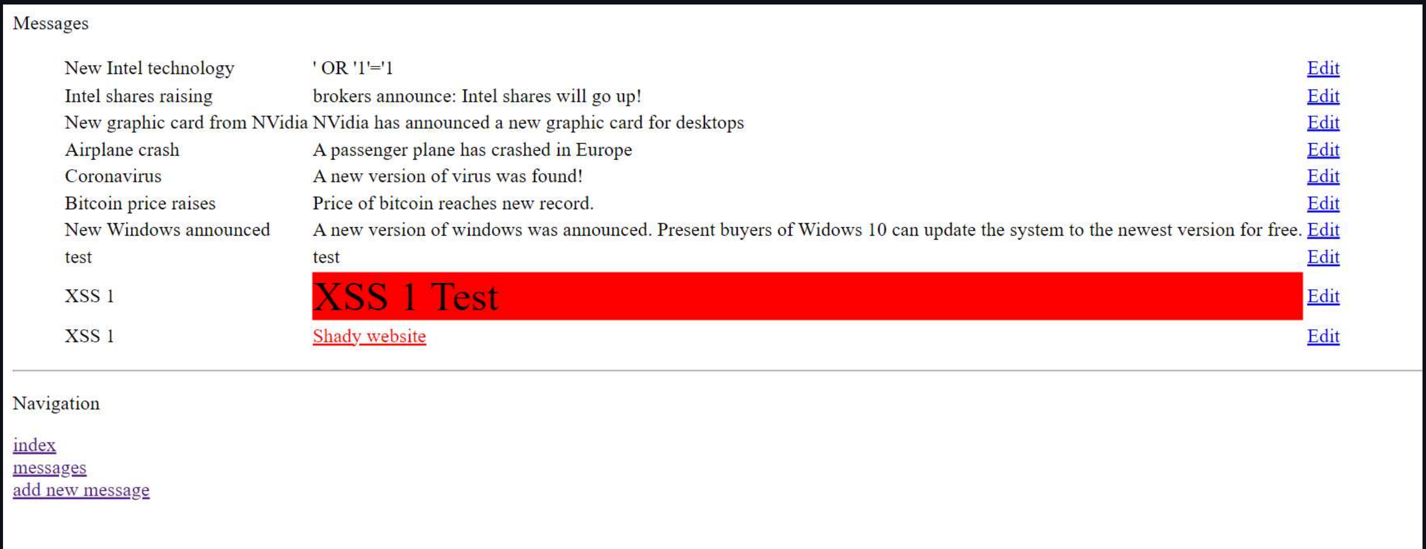
Type: Public

Message content:

```
<p> <a href="potential scam or harmfull website" style="color:red;"> Shady website </a> </p>
```

Navigation

index
messages
add new message



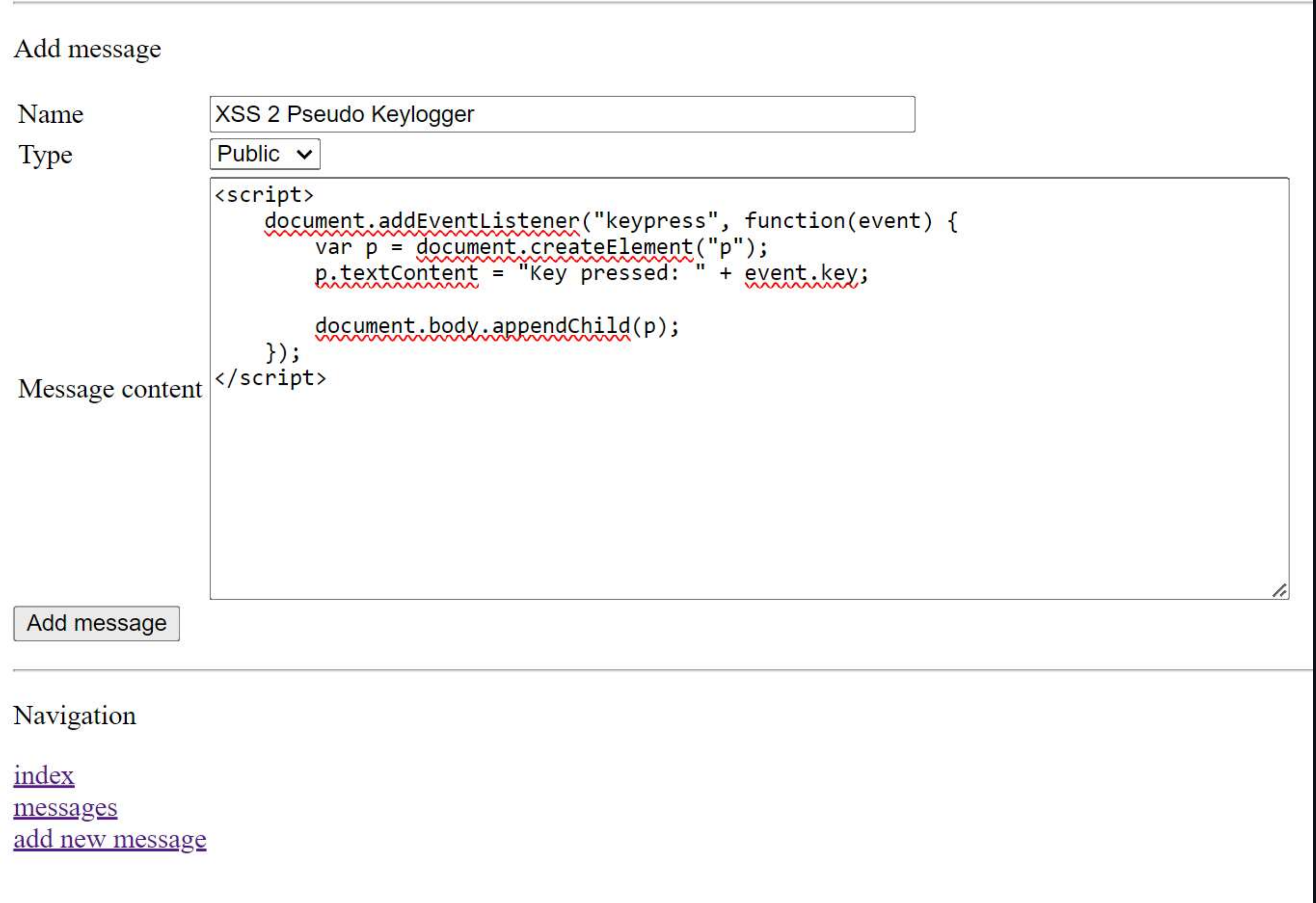
Messages

New Intel technology	' OR '1'='1	Edit
Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit
test	test	Edit
XSS 1	XSS 1 Test	Edit
XSS 1	Shady website	Edit

Navigation

index
messages
add new message

There might be more harmfull ways of using XSS such as keylogger that in other scenario would send data to some endpoint. With the use of XSS attacker might be able to steal cookie, or insert a form that might convince user into inserting sensitive data into it.



Add message

Name: XSS 2 Pseudo Keylogger

Type: Public

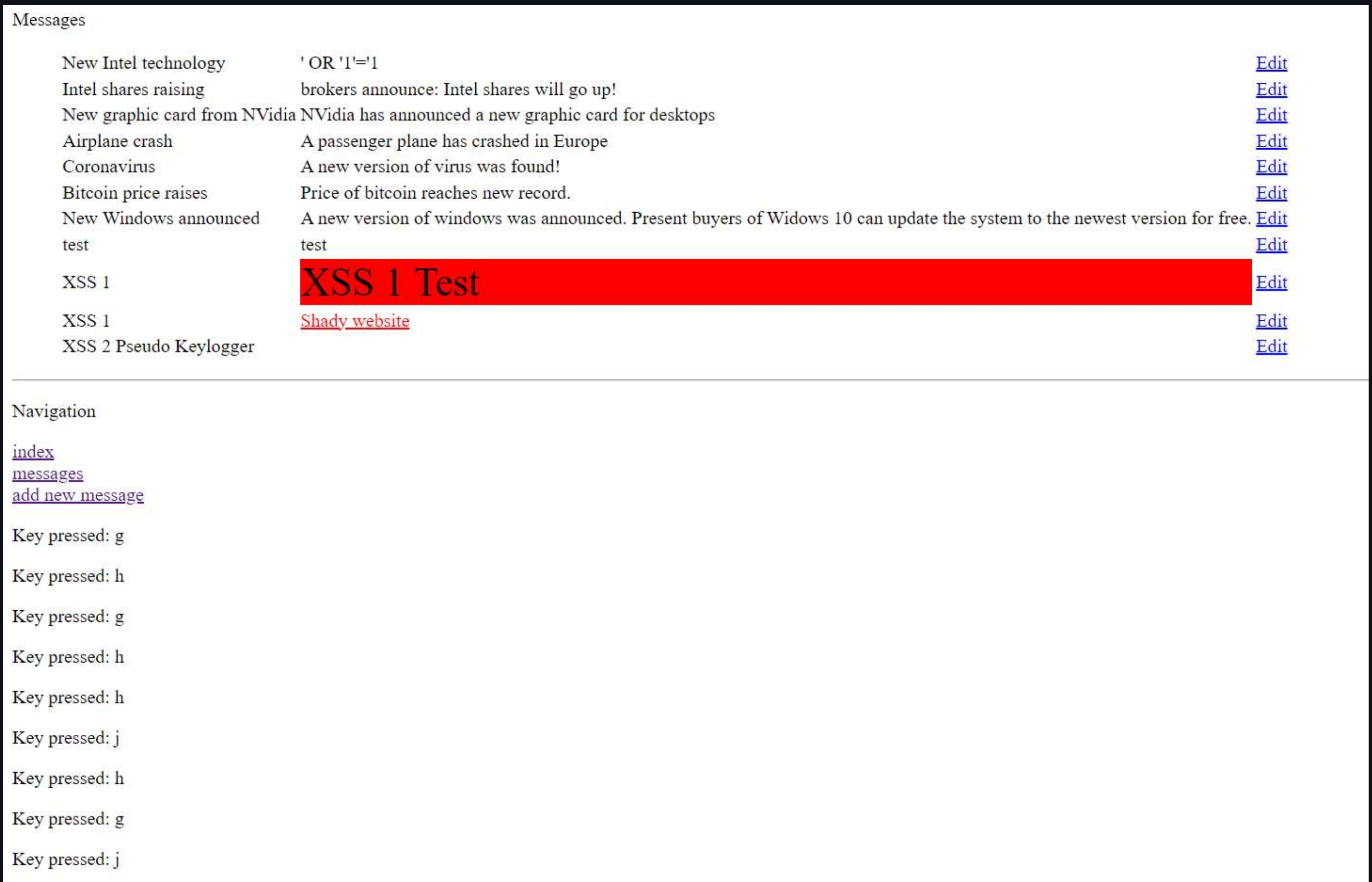
Message content:

```
<script>
    document.addEventListener("keypress", function(event) {
        var p = document.createElement("p");
        p.textContent = "Key pressed: " + event.key;

        document.body.appendChild(p);
    });
</script>
```

Navigation

index
messages
add new message



Messages

New Intel technology	' OR '1'='1	Edit
Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit
test	test	Edit
XSS 1	XSS 1 Test	Edit
XSS 1	Shady website	Edit
XSS 2 Pseudo Keylogger		Edit

Navigation

index
messages
add new message

```
Key pressed: g

Key pressed: h

Key pressed: g

Key pressed: h

Key pressed: h

Key pressed: j

Key pressed: h

Key pressed: g

Key pressed: j
```

Overall XSS attacks can lead to various malicious actions, including:

- Stealing user credentials
- Spreading web worms or malware
- Accessing user’s browser history or controlling the browser remotely
- Analyzing and using other applications

Task 3.2.

Verify the operation of the addslashes function in the context of protection against XSS attacks. Check if this feature prevents HTML or JavaScript injection.

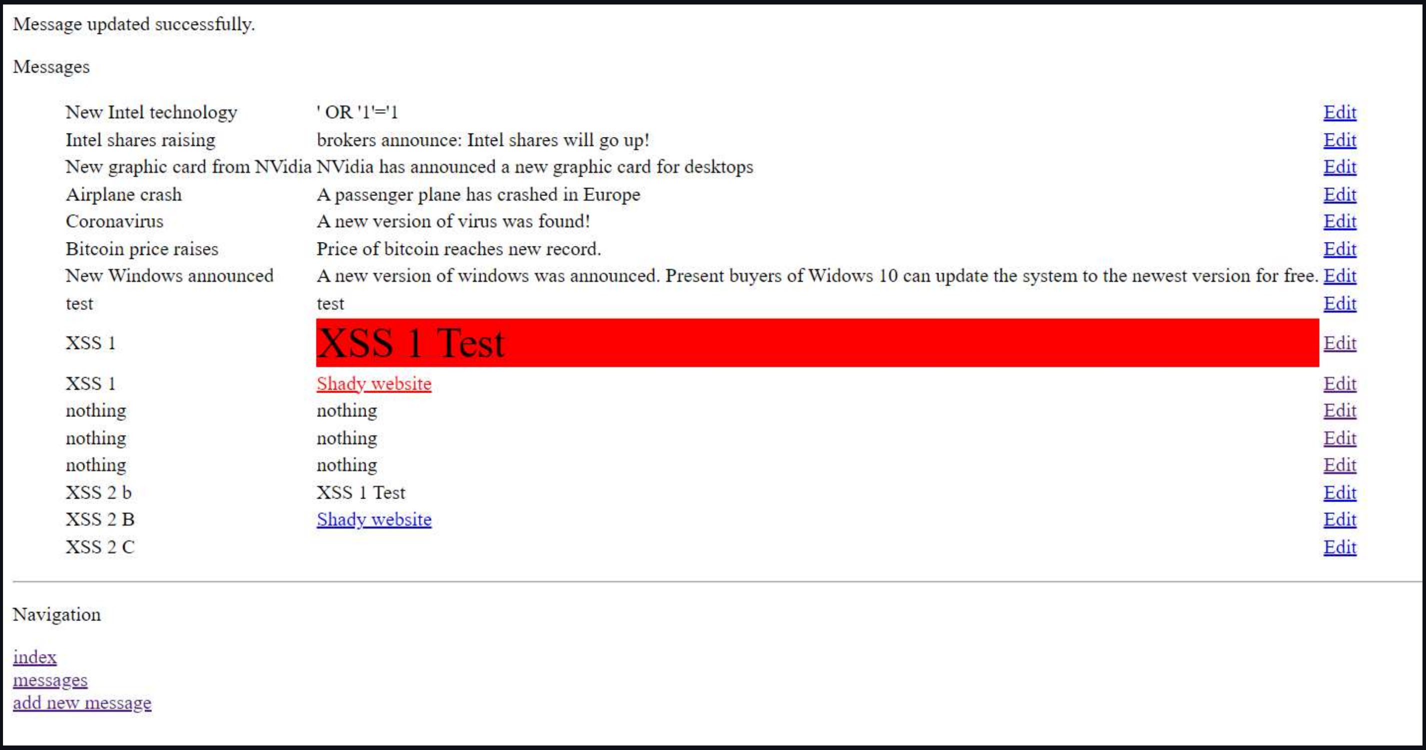
```
if (isset($_POST['add_message'])) {
    // whitelist
    $allowed_types = ['public', 'private'];

    try {
        $name = addslashes($_REQUEST['name']);
        $type = addslashes($_REQUEST['type']);
        $content = addslashes($_REQUEST['content']);

        if (!$db->addMessageBasic($name, $type, $content)) {
            echo "<p style='color:red;'>Adding new message failed.</p>";
        }
    } catch (InvalidArgumentException $e) {
        echo "<p style='color:red;'>{$e->getMessage()}</p>";
    }
}
```

```
public function addMessageBasic($name, $type, $content) {
        $name = addslashes($_REQUEST['name']);
        $type = addslashes($_REQUEST['type']);
        $content = addslashes($_REQUEST['content']);

        $sql = "INSERT INTO message (`name`, `type`, `message`, `deleted`)
VALUES (:name, :type, :content, 0)";
        try {
            $stmt = $this->pdo->prepare($sql);
            $stmt->bindParam(':name', $name);
            $stmt->bindParam(':type', $type);
            $stmt->bindParam(':content', $content);
            return $stmt->execute();
        } catch (PDOException $e) {
            echo "Add message failed: " . $e->getMessage();
            return false;
        }
    }
```



Message updated successfully.

Messages

New Intel technology	' OR '1'='1	Edit
Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit
test	test	Edit
XSS 1	XSS 1 Test	Edit
XSS 1	Shady website	Edit
nothing	nothing	Edit
nothing	nothing	Edit
nothing	nothing	Edit
XSS 2 b	XSS 1 Test	Edit
XSS 2 B	Shady website	Edit
XSS 2 C		Edit

Navigation

index
messages
add new message

The use of **addslashes()** partialy worked, it didnt allowed keyloger and other **style** based XSS but it still somehow allowed suspicious link to pass. So as it solved some issues with XSS there are still some left to take care of.

Task 3.3. & Task 3.4

Protect the rest of your application against XSS attacks. Modify the Filter class created in the previous lab so that it filters data not only for SQLI attacks but also for XSS attacks.

Verify the vulnerability of the secured application to XSS attacks. Conduct several selected attacks on the application and present their results.

Filter.php code snippet

```
public static function filter_name($name) {
        if (!is_string($name)) {
            throw new InvalidArgumentException("Name must be a string.");
        }
        if (preg_match('/[^a-zA-Z\s]/', $name)) {
            throw new InvalidArgumentException('Invalid input detected.
Only letters and spaces are allowed.');
        }
        return addslashes(htmlspecialchars(trim($name)));
    }
```

Db.php code snippet

```
public function addMessage($name, $type, $content) {
        $filtered_name = Filter::filter_name($name);
        $filtered_type = Filter::filter_type($type);
        $filtered_content = Filter::filter_general($content);

        $sql = "INSERT INTO message (`name`, `type`, `message`, `deleted`)
VALUES (:name, :type, :content, 0)";
        try {
            $stmt = $this->pdo->prepare($sql);
            $stmt->bindParam(':name', $filtered_name);
            $stmt->bindParam(':type', $filtered_type);
            $stmt->bindParam(':content', $filtered_content);
            return $stmt->execute();
        } catch (PDOException $e) {
            echo "Add message failed: " . $e->getMessage();
            return false;
        }
    }
```

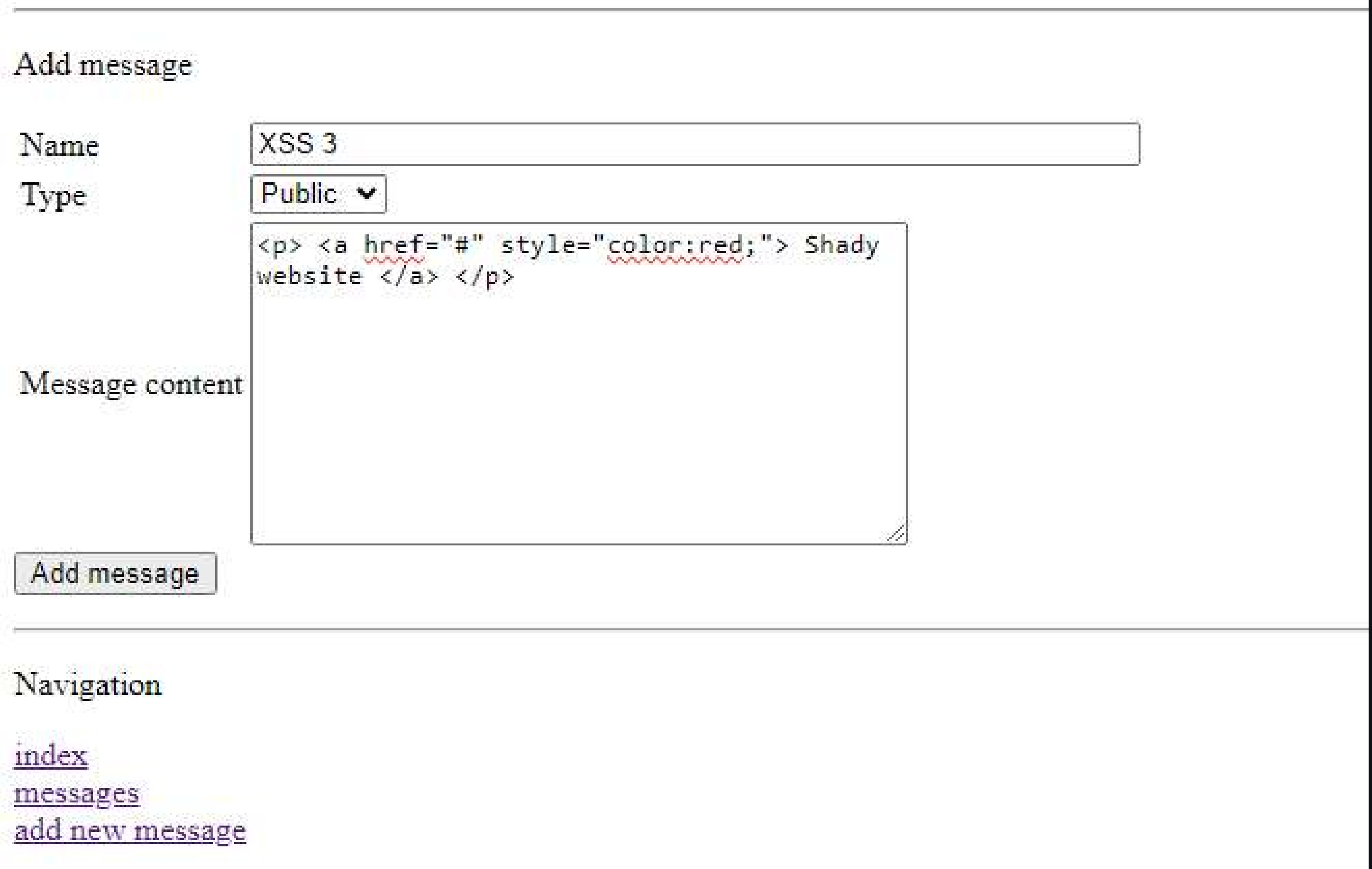
messages.php code snippet

```
// Adding a new message
if (isset($_POST['add_message'])) {
    $name = $_POST['name'];
    $type = $_POST['type'];
    $content = $_POST['content'];

    // whitelist
    $allowed_types = ['public', 'private'];

    try {
        if (!$db->addMessage($name, $type, $content)) {
            echo "<p style='color:red;'>Adding new message failed.</p>";
        }
    } catch (InvalidArgumentException $e) {
        echo "<p style='color:red;'>{$e->getMessage()}</p>";
    }
}
```

XSS: suspicious/malware link



Add message

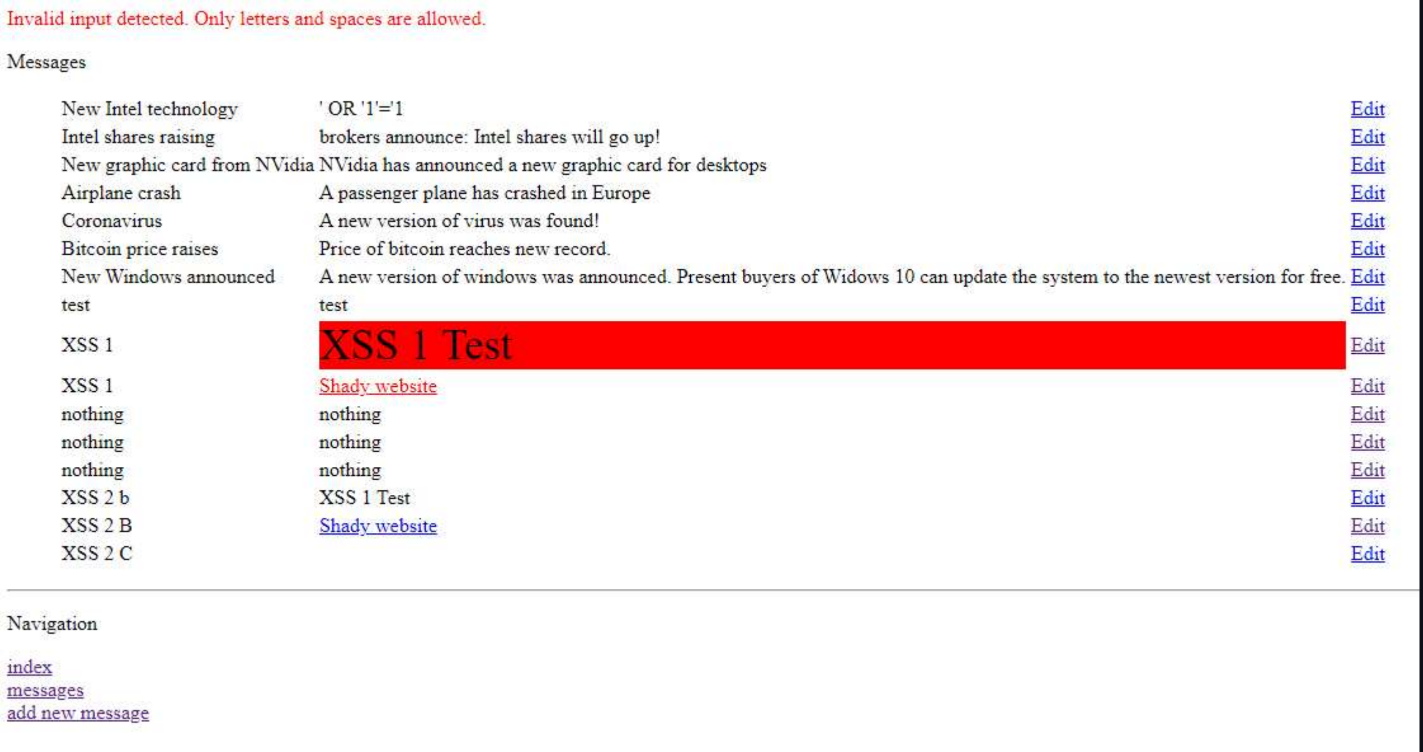
Name XSS 3

Type Public

Message content <p> <a href="#" style="color:red;"> Shady website </a> </p>

Navigation

index
messages
add new message



Invalid input detected. Only letters and spaces are allowed.

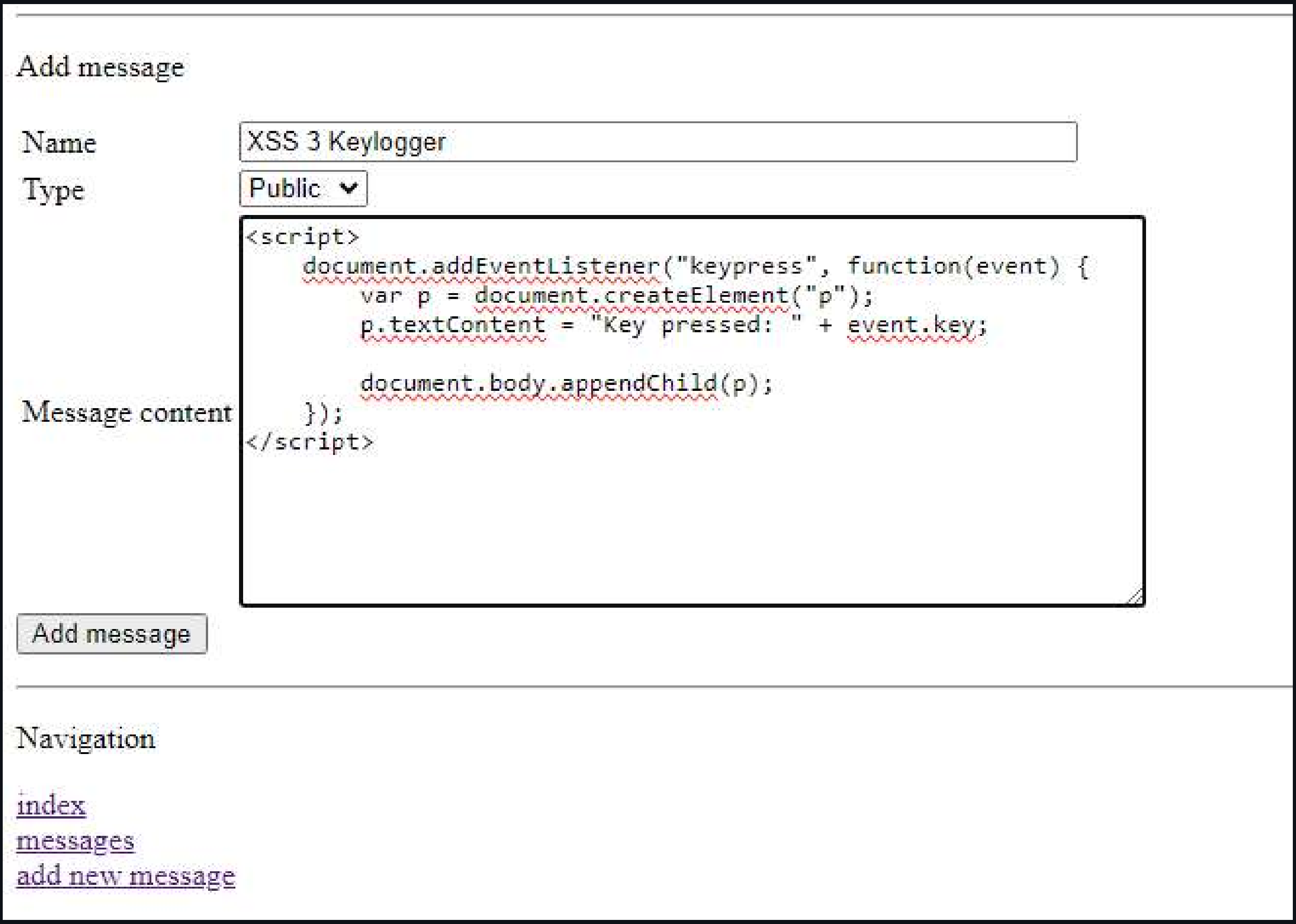
Messages

New Intel technology	' OR '1'='1	Edit
Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit
test	test	Edit
XSS 1	XSS 1 Test	Edit
XSS 1	Shady website	Edit
nothing	nothing	Edit
nothing	nothing	Edit
nothing	nothing	Edit
XSS 2 b	XSS 1 Test	Edit
XSS 2 B	Shady website	Edit
XSS 2 C		Edit

Navigation

index
messages
add new message

XSS: Semi-Keyloger



Add message

Name: XSS 3 Keylogger

Type: Public

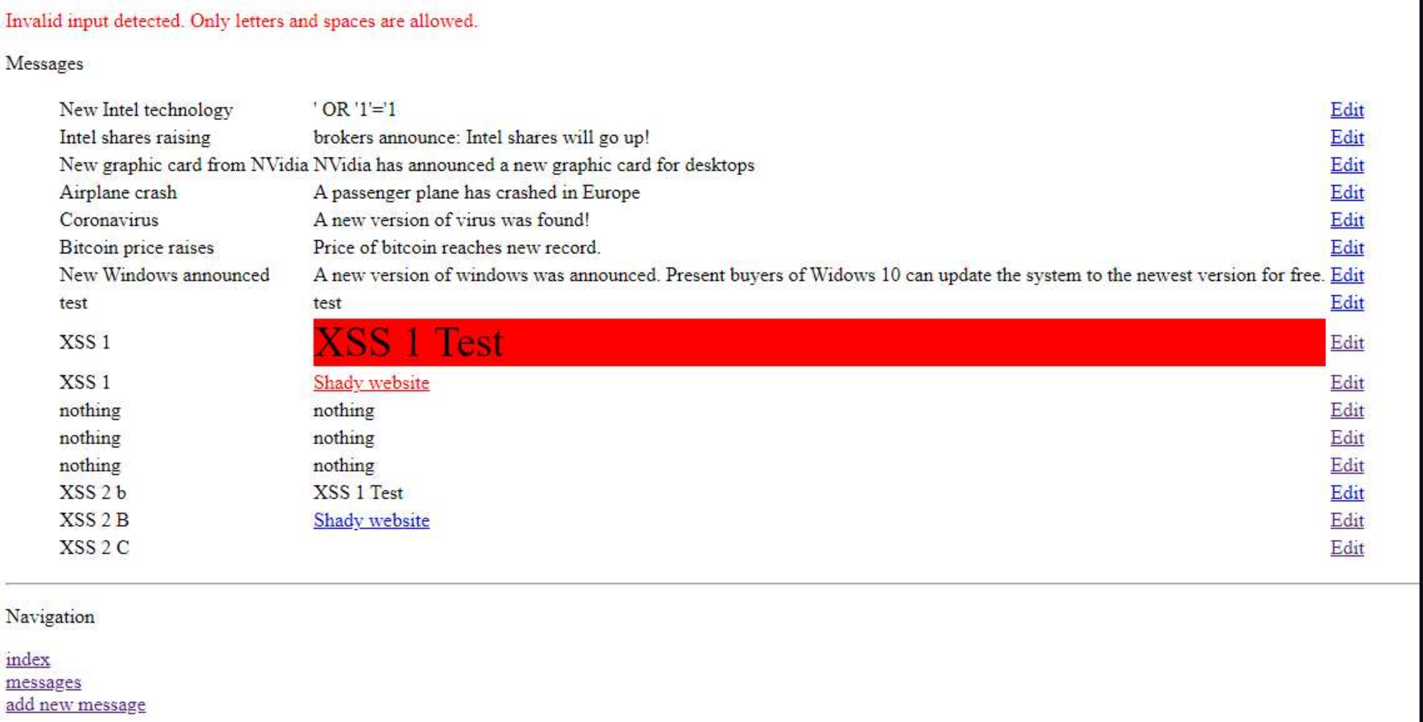
Message content:

```
<script>
    document.addEventListener("keypress", function(event) {
        var p = document.createElement("p");
        p.textContent = "Key pressed: " + event.key;

        document.body.appendChild(p);
    });
</script>
```

Navigation

index
messages
add new message



Invalid input detected. Only letters and spaces are allowed.

Messages

New Intel technology	' OR '1'='1	Edit
Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit
test	test	Edit
XSS 1	XSS 1 Test	Edit
XSS 1	Shady website	Edit
nothing	nothing	Edit
nothing	nothing	Edit
nothing	nothing	Edit
XSS 2 b	XSS 1 Test	Edit
XSS 2 B	Shady website	Edit
XSS 2 C		Edit

Navigation

index
messages
add new message

In my program, any attempt to submit suspicious content triggers an exception. The only drawback of this approach is that users cannot enter certain inputs into the form. This limitation restricts user options on one hand but enhances application security on the other. This trade-off is likely worth it, as achieving security often makes the experience slightly more difficult for regular users, but ultimately helps protect both the user and the application.