BOLETIM DE SEGURANÇA

Vulnerabilidade de XSS é corrigida em plug-in WP-Members do WordPress

heimdall
security research
A DIVISION OF ISH

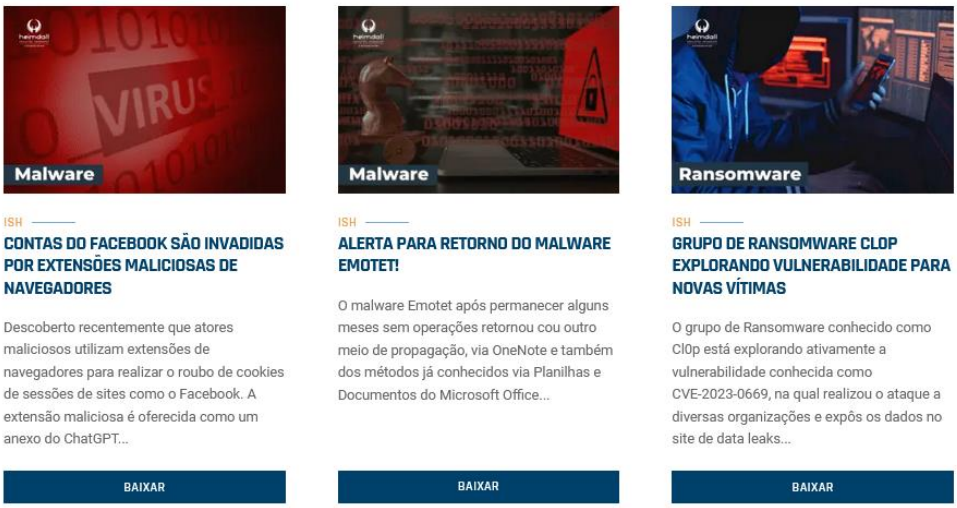
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Em fevereiro de 2024, durante o segundo Bug Bounty Extravaganza, o pesquisador de segurança Webbernaut reportou uma vulnerabilidade classificada como alta de *Cross-Site Scripting* (**XSS**) CVE-2024-1852 não autenticados no plugin WP-Members Membership, presente em mais de 60.000 sites. Essa vulnerabilidade possibilita que invasores insiram JavaScript arbitrário através do cabeçalho X-Forwarded-For, utilizado pelo plugin para registro. Quando um administrador acessa, o código malicioso é ativado no contexto da sessão do navegador do administrador. Isso permite a criação de usuários administradores com intenções maliciosas e a alteração das configurações de um site afetado, podendo resultar no controle total do site.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Essa vulnerabilidade está presente em todas as versões do plugin até a 3.4.9.2, inclusive, e é causada por uma limpeza inadequada de entrada e escape de saída. Isso permite que invasores não autenticados insiram scripts da Web arbitrários em páginas que serão executadas sempre que um usuário acessar uma página injetada, como a página de edição de usuários. A vulnerabilidade foi parcialmente resolvida na versão 3.4.9.2 e completamente corrigida na versão 3.4.9.3.

O WP-Members é um plugin que proporciona aos proprietários de sites a capacidade de monetizar seu conteúdo através de recursos de restrição de conteúdo e registro personalizado. Na fase de configuração inicial, é possível limitar o acesso a postagens e páginas, além de habilitar o registro de usuários. Quando um visitante tenta acessar uma página, ele se depara com uma interface semelhante à mostrada na captura de tela fornecida.

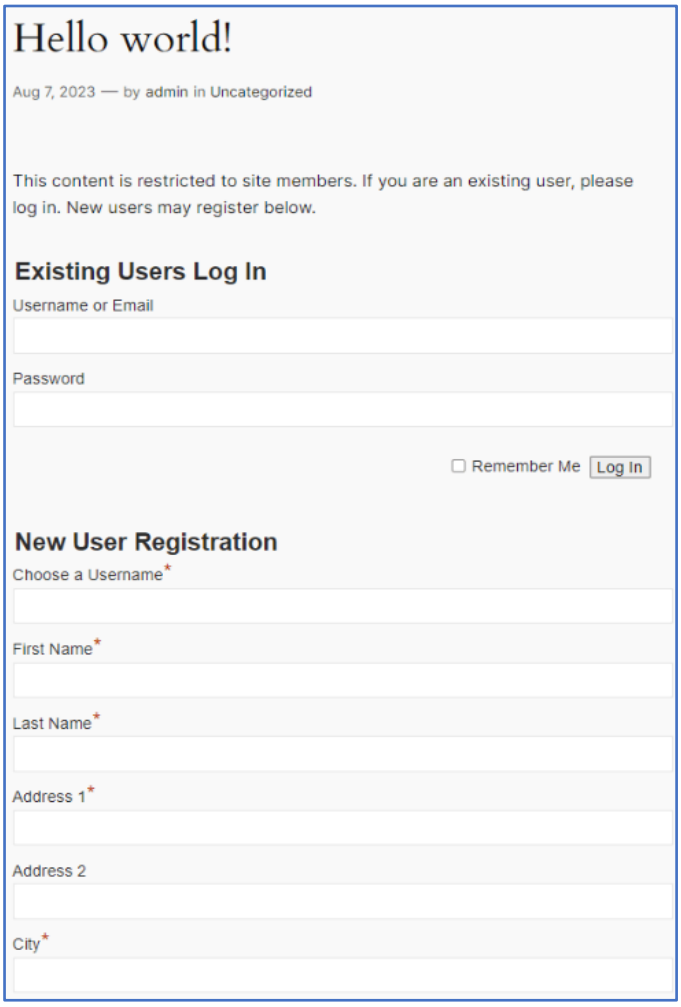


Figura 1 – Formulário de login.

A vulnerabilidade de Cross-Site Scripting pode ser explorada da seguinte maneira: um atacante, após preencher e enviar o formulário de registro, pode interceptar a solicitação de registro. Utilizando um proxy selecionado, o invasor pode alterar a solicitação original para incluir um cabeçalho X-Forwarded-For malicioso, então carga útil maliciosa é inserida dentro das tags de script.

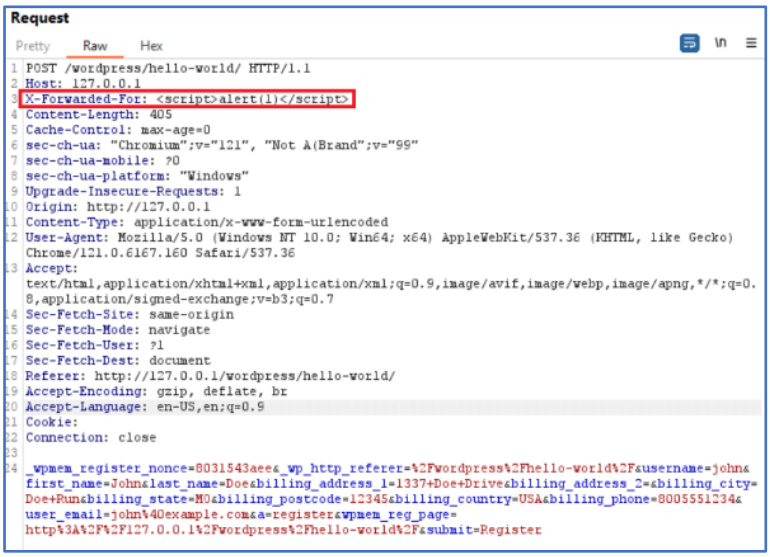


Figura 2 – Solicitação de burp com carga maliciosa.

Após o envio dessa solicitação ao servidor, é gerada uma conta de usuário que parece inofensiva, contendo as informações fornecidas pelo atacante.

Figura 3 – Conta de usuário gerada.

O plugin registra nos perfis dos usuários o endereço IP de quem preencheu o formulário de inscrição. Esse processo é realizado através do código abaixo:

```
157 if ( ! function_exists( 'rktgk_get_user_ip' ) ):
158 /**
159  * Get user IP address.
160  *
161  * From Pippin.
162  * @link https://gist.github.com/pippinsplugins/9641841
163  *
164  * @since 1.0.0
165  *
166  * @return string $ip.
167  */
168 function rktgk_get_user_ip() {
169         if ( ! empty( $_SERVER['HTTP_CLIENT_IP'] ) ) {
170                 //check ip from share internet
171                 $ip = $_SERVER['HTTP_CLIENT_IP'];
172         } elseif ( ! empty( $_SERVER['HTTP_X_FORWARDED_FOR'] ) ) {
173                 //to check ip is pass from proxy
174                 $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
175         } else {
176                 $ip = $_SERVER['REMOTE_ADDR'];
177         }
178         /**
179          * Filter the IP result.
180          *
181          * @since 1.0.0
182          *
183          * @param string $ip
184          */
185         return apply_filters( 'rktgk_get_user_ip', $ip );
186 }
187 endif;
```

Figura 4 – Função rktgk_get_user_ip vulnerável.

A função *rktgk_get_user_ip* verifica a presença dos cabeçalhos **HTTP_CLIENT_IP ou HTTP_X_FORWARDED_FOR** na solicitação. Caso um desses cabeçalhos esteja presente, a função o utiliza como o IP do usuário, substituindo o valor da variável **REMOTE_ADDR**, e retorna esse valor como o endereço IP. No entanto, como os cabeçalhos HTTP podem ser manipulados e a entrada não é higienizada, um usuário pode inserir qualquer valor, incluindo um script da web mal-intencionado, que será registrado como o IP do usuário.

Se um administrador optar por editar ou visualizar a conta desse usuário, o JavaScript injetado a seguir estará presente no código-fonte gerado quando a página for carregada:

```
<h3>WP-Members Additional Fields</h3>
<table class="form-table">
    <tr><th><label>Address 1 <span class="description">(required)</span></label></th><td><input
    <th><label>IP @ registration</label></th>
    <td><script>alert(1)</script></td>
</tr>

</table>
```

Figura 5 – Código-fonte gerado que inclui carga JavaScript maliciosa.

Como resultado, a seguinte carga útil será ativada:

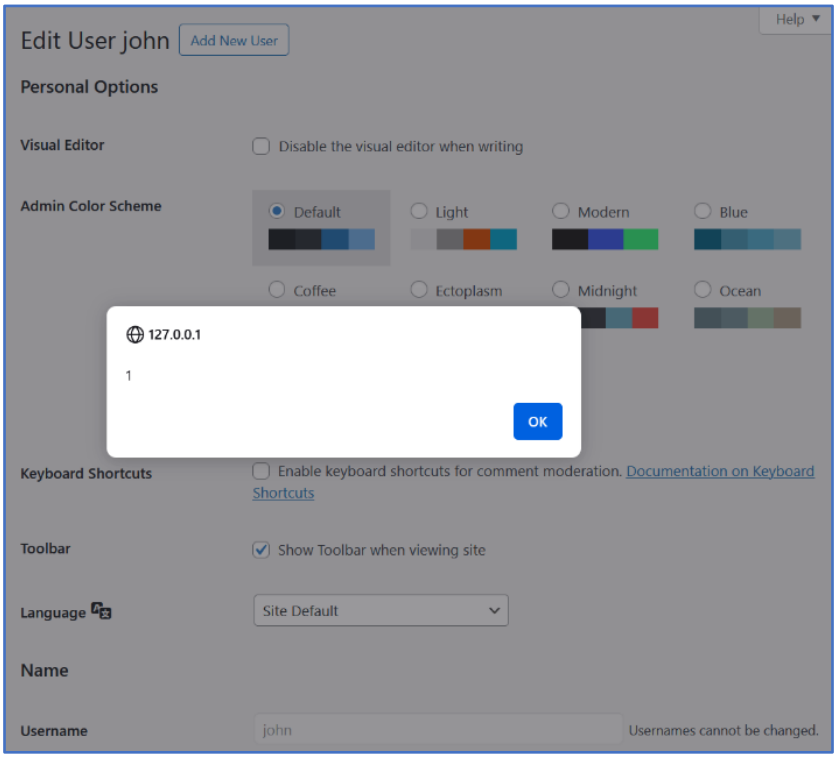


Figura 6 – Exemplo de disparo de carga útil JavaScript básico.

É crucial entender que este código será ativado dentro da sessão do navegador de um administrador. Ele tem o potencial de ser usado para estabelecer contas de usuários com intenções maléficas, desviar visitantes do site para páginas web nocivas e executar outras atividades danosas.

3 RECOMENDAÇÕES

Abaixo são elencadas pela ISH, medidas que poderão ser adotadas visando a mitigação da referida ameaça, como por exemplo:

Mantenha todos os softwares atualizados

- Isso inclui o WordPress, temas e plugins.

Use um firewall de aplicativo web robusto (WAF)

- Os firewalls são a melhor defesa contra ameaças em constante evolução.

Valide e higienize os dados do usuário

- Certifique-se de que todos os dados do usuário sejam validados e higienizados corretamente antes de entrar no seu site.

Políticas de segurança

- Adicione uma política de segurança de conteúdo ao seu cabeçalho.

Instale um bom plugin de segurança do WordPress

- Recomenda-se o uso de plugins de segurança como Sucuri, Wordfence, MalCare e SiteLock.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Wordfance**
- **CVEORG**

heimdall
security research
A DIVISION OF ISH