ZAP Scanning Report

Relatorio de vulnerabilidades

Site: http://testphp.vulnweb.com

Generated on sáb., 1 mar. 2025 03:46:51

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	3
Médio	2
Baixo	0
Informativo	2

Alertas

Nome	Nível de Risco	Number of Instances
Cross Site Scripting (Refletido)	Alto	19
Cross Site Scripting (baseado em DOM)	Alto	11
Injeção SQL - MySQL	Alto	13
Injeção XSLT	Médio	2
Vazamento de informações .htaccess	Médio	7
GET for POST	Informativo	3
User Agent Fuzzer	Informativo	197

Alert Detail

Alto	Cross Site Scripting (Refletido)
	Cross-site Scripting (XSS) é uma técnica de ataque que envolve a replicação e execução de código fornecido pelo invasor na instância do navegador do usuário. Uma instância do navegador pode ser um cliente de navegador padrão ou um objeto de navegador incorporado em um produto de software, como o navegador no WinAmp, um leitor de RSS ou um cliente de e-mail. O código em si é geralmente escrito em HTML/JavaScript, mas também pode se estender para VBScript, ActiveX, Java, Flash ou qualquer outra tecnologia compatível com navegador. Quando um invasor faz com que o navegador de um usuário execute seu código, o código será executado dentro do contexto de segurança (ou zona) do site de hospedagem. Com este nível de privilégio, o código tem a capacidade de ler, modificar e transmitir quaisquer dados confidenciais acessíveis pelo navegador. Um usuário afetado por script de cross-site pode ter sua conta sequestrada (roubo de cookie), seu navegador redirecionado para outro local ou possivelmente mostrando conteúdo fraudulento fornecido pelo suposto site que está visitando. Os ataques de script cross-site comprometem essencialmente a relação de confiança entre um usuário e o site. Aplicativos que utilizam instâncias de objeto de

Descrição	navegador que carregam conteúdo do sistema de arquivos podem executar código na zona da máquina local, permitindo o comprometimento do sistema. Existem três tipos de ataques de Cross-site Scripting: não persistente, persistente e baseado em DOM. Ataques não persistentes e ataques baseados em DOM exigem que o usuário visite um link especialmente criado com código malicioso ou visite uma página da web maliciosa contendo um formulário da web que, quando postado no site vulnerável, montará o ataque. O uso de um formulário mal-intencionado geralmente ocorre quando o recurso vulnerável aceita apenas solicitações HTTP POST. Nesse caso, o formulário pode ser enviado automaticamente sem o conhecimento da vítima (por exemplo, usando JavaScript). Ao clicar no link malicioso ou enviar o formulário malicioso, a carga XSS será ecoada de volta e será interpretada pelo navegador do usuário e executada. Outra técnica para enviar solicitações quase arbitrárias (GET e POST) é usar um cliente incorporado, como o Adobe Flash. Ataques persistentes ocorrem quando o código malicioso é enviado a um site onde é armazenado por um período de tempo. Exemplos dos alvos favoritos de um invasor geralmente incluem postagens em quadros de mensagens, mensagens de webmail e software de bate-papo na web. Não é requerido do usuário desavisado, que interaja com qualquer site/link adicional (por exemplo, um site invasor ou um link malicioso enviado por e-mail), basta simplesmente visualizar a página da web que contém o código.
URL	http://testphp.vulnweb.com/artists.php?artist=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	"><scrIpt>alert(1);</scRipt>
Evidence	"><scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&pp=12
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET

Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	</td><scrIpt>alert(1);</scRipt><td>
Evidence	</td><scrIpt>alert(1);</scRipt><td>
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=%27%22%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	POST
Ataque	'"<scrIpt>alert(1);</scRipt>
Evidence	'"<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST

Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'"<scrIpt>alert(1);</scRipt>
Evidence	'"<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'"<scrIpt>alert(1);</scRipt>
Evidence	'"<scrIpt>alert(1);</scRipt>

Other Info	
Instances	19
Solution	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Exemplos de bibliotecas e frameworks que facilitam a geração de saída codificada adequadamente incluem a biblioteca Anti-XSS da Microsoft, o módulo de codificação OWASP ESAPI e o Apache Wicket. Fases: Implementação | Arquitetura e Design. Compreenda o contexto no qual seus dados serão usados e a codificação que será esperada. Isso é especialmente importante ao transmitir dados entre componentes diferentes ou ao gerar saídas que podem conter várias codificações ao mesmo tempo, como páginas da web ou mensagens de e-mail com várias partes. Estude todos os protocolos de comunicação e representações de dados esperados para determinar as estratégias de codificação necessárias. Para quaisquer dados que serão enviados para outra página da web, especialmente quaisquer dados recebidos de entradas externas, use a codificação apropriada em todos os caracteres não alfanuméricos. Consulte a Página de Dicas de Prevenção de XSS para obter mais detalhes sobre os tipos de codificação e escape que são necessários. Fase: Arquitetura e Design. Para todas as verificações de segurança realizadas no lado do cliente, certifique-se de que essas verificações sejam duplicadas no lado do servidor, a fim de evitar a CWE-602. Invasores podem ignorar as verificações do lado do cliente, modificando os valores após a realização das verificações ou alterando o cliente para remover as verificações do lado do cliente completamente. Em seguida, esses valores modificados poderiam ser enviados ao servidor. Se disponível, use mecanismos estruturados que impõem automaticamente a separação entre dados e código. Esses mecanismos podem ser capazes de fornecer citação, codificação e validação relevantes automaticamente, em vez de depender do desenvolvedor para fornecer esse recurso em cada ponto onde a saída é gerada. Fase: Implementação. Para cada página web gerada, use e especifique uma codificação de caracteres, como ISO-8859-1 ou UTF-8. Quando uma codificação não é especificada, o navegador pode escolher uma codificação diferente, tentando adivinhar por eliminação qual codificação está realmente sendo usada pela página da web. Isso pode fazer com que o navegador da web trate certas sequências como especiais, abrindo o cliente para ataques XSS sutis. Consulte a CWE-116 para obter mais informações sobre mitigações relacionadas à codificação /escape. Para ajudar a mitigar os ataques XSS contra cookie de sessão do usuário, defina o cookie de sessão como HttpOnly. Em navegadores que suportam o recurso HttpOnly (como versões mais recentes do Internet Explorer e Firefox), esse atributo pode impedir que o cookie de sessão do usuário seja acessível a scripts mal-intencionados do lado do cliente que usam document.cookie. Esta não é uma solução completa, já que HttpOnly não é compatível com todos os navegadores. Mais importante ainda, XMLHTTPRequest e outras poderosas tecnologias de navegadores fornecem acesso de leitura a cabeçalhos HTTP, incluindo o cabeçalho Set-Cookie no qual o sinalizador HttpOnly é definido. Presuma que toda a entrada de dados é maliciosa. Use uma estratégia de validação de entrada "aceita como boa", ou seja, use uma lista de permissões de entradas aceitáveis que estejam estritamente em conformidade com as especificações. Rejeite quaisquer entradas que não estejam estritamente de acordo com as especificações ou transforme-as

	em algo que esteja. Não confie exclusivamente na procura de entradas maliciosas ou malformadas (ou seja, não confie em uma lista de negação). No entanto, as listas de negação podem ser úteis para detectar ataques em potencial ou determinar quais entradas estão tão malformadas que devem ser rejeitadas imediatamente. Ao executar a validação de entradas de dados, considere todas as propriedades potencialmente relevantes, incluindo comprimento, tipo de entrada, a gama completa de valores aceitáveis, entradas ausentes ou extras, sintaxe, consistência entre campos relacionados e conformidade com as regras de negócios. Como um exemplo de lógica de regra de negócios, "barco" pode ser sintaticamente válido porque contém apenas caracteres alfanuméricos, mas não é válido se você estiver esperando cores como "vermelho" ou "azul". Certifique-se de realizar a validação de entrada em interfaces bem definidas dentro do aplicativo. Isso ajudará a proteger o aplicativo, mesmo se um componente for reutilizado ou movido para outro lugar.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40012

Alto	**Cross Site Scripting (baseado em DOM)**
Descrição	Cross-site Scripting (XSS) é uma técnica de ataque que envolve a replicação e execução de código fornecido pelo invasor na instância do navegador do usuário. Uma instância do navegador pode ser um cliente de navegador padrão ou um objeto de navegador incorporado em um produto de software, como o navegador no WinAmp, um leitor de RSS ou um cliente de e-mail. O código em si é geralmente escrito em HTML/JavaScript, mas também pode se estender para VBScript, ActiveX, Java, Flash ou qualquer outra tecnologia compatível com navegador. Quando um invasor faz com que o navegador de um usuário execute seu código, o código será executado dentro do contexto de segurança (ou zona) do site de hospedagem. Com este nível de privilégio, o código tem a capacidade de ler, modificar e transmitir quaisquer dados confidenciais acessíveis pelo navegador. Um usuário afetado por script de cross-site pode ter sua conta sequestrada (roubo de cookie), seu navegador redirecionado para outro local ou possivelmente mostrando conteúdo fraudulento fornecido pelo suposto site que está visitando. Os ataques de script cross-site comprometem essencialmente a relação de confiança entre um usuário e o site. Aplicativos que utilizam instâncias de objeto de navegador que carregam conteúdo do sistema de arquivos podem executar código na zona da máquina local, permitindo o comprometimento do sistema. Existem três tipos de ataques de Cross-site Scripting: não persistente, persistente e baseado em DOM. Ataques não persistentes e ataques baseados em DOM exigem que o usuário visite um link especialmente criado com código malicioso ou visite uma página da web maliciosa contendo um formulário da web que, quando postado no site vulnerável, montará o ataque. O uso de um formulário mal-intencionado geralmente ocorre quando o recurso vulnerável aceita apenas solicitações HTTP POST. Nesse caso, o formulário pode ser enviado automaticamente sem o conhecimento da vítima (por exemplo, usando JavaScript). Ao clicar no link malicioso ou enviar o formulário malicioso, a carga XSS será ecoada de volta e será interpretada pelo navegador do usuário e executada. Outra técnica para enviar solicitações quase arbitrárias (GET e POST) é usar um cliente incorporado, como o Adobe Flash. Ataques persistentes ocorrem quando o código malicioso é enviado a um site onde é armazenado por um período de tempo. Exemplos dos alvos favoritos de um invasor geralmente incluem postagens em quadros de mensagens, mensagens de webmail e software de bate-papo na web. Não é requerido do usuário desavisado, que interaja com qualquer site/link adicional (por exemplo, um site invasor ou um link malicioso enviado por e-mail), basta simplesmente visualizar a página da web que contém o código.
	http://testphp.vulnweb.com#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%

URL	0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/artists.php?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/cart.php?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/categories.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/disclaimer.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/guestbook.php?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/index.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/login.php?name=abc#<img src="random.gif" onerror=alert(5397) >
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/product.php?pic=6#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/signup.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	Tag name: input Att name: goButton Att id:
URL	http://testphp.vulnweb.com/search.php?test=query#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	POST
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	
Instances	11
	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Exemplos de bibliotecas e frameworks que facilitam a geração de saída codificada adequadamente incluem a biblioteca Anti-XSS da Microsoft, o módulo de codificação OWASP ESAPI e o Apache Wicket. Fases: Implementação | Arquitetura e Design.

Solution	Compreenda o contexto no qual seus dados serão usados e a codificação que será esperada. Isso é especialmente importante ao transmitir dados entre componentes diferentes ou ao gerar saídas que podem conter várias codificações ao mesmo tempo, como páginas da web ou mensagens de e-mail com várias partes. Estude todos os protocolos de comunicação e representações de dados esperados para determinar as estratégias de codificação necessárias. Para quaisquer dados que serão enviados para outra página da web, especialmente quaisquer dados recebidos de entradas externas, use a codificação apropriada em todos os caracteres não alfanuméricos. Consulte a Página de Dicas de Prevenção de XSS para obter mais detalhes sobre os tipos de codificação e escape que são necessários. Fase: Arquitetura e Design. Para todas as verificações de segurança realizadas no lado do cliente, certifique-se de que essas verificações sejam duplicadas no lado do servidor, a fim de evitar a CWE-602. Invasores podem ignorar as verificações do lado do cliente, modificando os valores após a realização das verificações ou alterando o cliente para remover as verificações do lado do cliente completamente. Em seguida, esses valores modificados poderiam ser enviados ao servidor. Se disponível, use mecanismos estruturados que impõem automaticamente a separação entre dados e código. Esses mecanismos podem ser capazes de fornecer citação, codificação e validação relevantes automaticamente, em vez de depender do desenvolvedor para fornecer esse recurso em cada ponto onde a saída é gerada. Fase: Implementação. Para cada página web gerada, use e especifique uma codificação de caracteres, como ISO-8859-1 ou UTF-8. Quando uma codificação não é especificada, o navegador pode escolher uma codificação diferente, tentando adivinhar por eliminação qual codificação está realmente sendo usada pela página da web. Isso pode fazer com que o navegador da web trate certas sequências como especiais, abrindo o cliente para ataques XSS sutis. Consulte a CWE-116 para obter mais informações sobre mitigações relacionadas à codificação /escape. Para ajudar a mitigar os ataques XSS contra cookie de sessão do usuário, defina o cookie de sessão como HttpOnly. Em navegadores que suportam o recurso HttpOnly (como versões mais recentes do Internet Explorer e Firefox), esse atributo pode impedir que o cookie de sessão do usuário seja acessível a scripts mal-intencionados do lado do cliente que usam document.cookie. Esta não é uma solução completa, já que HttpOnly não é compatível com todos os navegadores. Mais importante ainda, XMLHTTPRequest e outras poderosas tecnologias de navegadores fornecem acesso de leitura a cabeçalhos HTTP, incluindo o cabeçalho Set-Cookie no qual o sinalizador HttpOnly é definido. Presuma que toda a entrada de dados é maliciosa. Use uma estratégia de validação de entrada "aceita como boa", ou seja, use uma lista de permissões de entradas aceitáveis que estejam estritamente em conformidade com as especificações. Rejeite quaisquer entradas que não estejam estritamente de acordo com as especificações ou transforme-as em algo que esteja. Não confie exclusivamente na procura de entradas maliciosas ou malformadas (ou seja, não confie em uma lista de negação). No entanto, as listas de negação podem ser úteis para detectar ataques em potencial ou determinar quais entradas estão tão malformadas que devem ser rejeitadas imediatamente. Ao executar a validação de entradas de dados, considere todas as propriedades potencialmente relevantes, incluindo comprimento, tipo de entrada, a gama completa de valores aceitáveis, entradas ausentes ou extras, sintaxe, consistência entre campos relacionados e conformidade com as regras de negócios. Como um exemplo de lógica de regra de negócios, "barco" pode ser sintaticamente válido porque contém apenas caracteres alfanuméricos, mas não é válido se você estiver esperando cores como "vermelho" ou "azul". Certifique-se de realizar a validação de entrada em interfaces bem definidas dentro do aplicativo. Isso ajudará a proteger o aplicativo, mesmo se um componente for reutilizado ou movido para outro lugar.

Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40026

Alto	**Injeção SQL - MySQL**
Descrição	SQL injection may be possible.
URL	http://testphp.vulnweb.com/artists.php?artist=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/listproducts.php?artist=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/listproducts.php?cat=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/product.php?pic=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/search.php?test=%27
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised

URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	ZAP'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	3 and 0 in (select sleep(15)) --
Evidence	
Other Info	O tempo da query é controlável utilizando o valor do parâmetro [3 and 0 in (select sleep(15)) --], o qual causou a requisição a levar [15.125] milissegundos, enquanto o valor original da query sem modificação com o valor [3] levou [0] milissegundos
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	6 and 0 in (select sleep(15)) --
Evidence	
Other Info	O tempo da query é controlável utilizando o valor do parâmetro [6 and 0 in (select sleep(15)) --], o qual causou a requisição a levar [15.125] milissegundos, enquanto o valor original da query sem modificação com o valor [6] levou [0] milissegundos
URL	http://testphp.vulnweb.com/secured/newuser.php

Método	POST
Ataque	ZAP' / sleep(15) / '
Evidence	
Other Info	O tempo da query é controlável utilizando o valor do parâmetro [ZAP' / sleep(15) / '], o qual causou a requisição a levar [15.121] milissegundos, enquanto o valor original da query sem modificação com o valor [ZAP] levou [0] milissegundos
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	ZAP' / sleep(15) / '
Evidence	
Other Info	O tempo da query é controlável utilizando o valor do parâmetro [ZAP' / sleep(15) / '], o qual causou a requisição a levar [15.128] milissegundos, enquanto o valor original da query sem modificação com o valor [ZAP] levou [0] milissegundos
Instances	13
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Médio	**Injeção XSLT**
Descrição	Injection using XSL transformations may be possible, and may allow an attacker to read system information, read and write files, or execute arbitrary code.
URL	http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E
Método	GET
Ataque	<xsl:value-of select="document('http://testphp.vulnweb.com:22')"/>
Evidence	failed to open stream

Other Info	Port scanning may be possible.
URL	http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E&size=160
Método	GET
Ataque	<xsl:value-of select="document('http://testphp.vulnweb.com:22')"/>
Evidence	failed to open stream
Other Info	Port scanning may be possible.
Instances	2
Solution	Sanitize and analyze every user input coming from any client-side.
Reference	https://www.contextis.com/blog/xslt-server-side-injection-attacks
CWE Id	91
WASC Id	23
Plugin Id	90017

Médio	**Vazamento de informações .htaccess**
Descrição	Os arquivos htaccess podem ser usados para alterar a configuração do software Apache Web Servidor para habilitar/desabilitar funcionalidades e recursos adicionais que o software Apache Web Servidor tem a oferecer.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/.htaccess
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/.htaccess
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/.htaccess
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/.htaccess

Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/.htaccess
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/.htaccess
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	7
Solution	Certifique-se de que o arquivo .htaccess não esteja acessível.
Reference	https://developer.mozilla.org/en-US/docs/Learn/Server-side/Apache_Configuration_htaccess https://httpd.apache.org/docs/2.4/howto/htaccess.html
CWE Id	94
WASC Id	14
Plugin Id	40032

Informativo	**GET for POST**
Descrição	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	GET http://testphp.vulnweb.com/cart.php?addcart=6&price=10000 HTTP/1.1
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	GET http://testphp.vulnweb.com/guestbook.php?name=anonymous%20user&submit=add%20message&text= HTTP/1.1
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	GET

Ataque	
Evidence	GET http://testphp.vulnweb.com/search.php?goButton=go&searchFor=ZAP HTTP/1.1
Other Info	
Instances	3
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

Informativo	**User Agent Fuzzer**
Descrição	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash

Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php

Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET

Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET

Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET

Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php

Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php

Método	POST
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST

Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST

Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	197
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104