




## Web Application Vulnerability Scanner


By : Ritek Rounak

Scan Selection 

Download PDF

### 1. flexcase.tech

Entry:  <http://flexcase.tech:8000>

Start:  2023-04-19 17:10:36


End: 2023-04-19 17:12:26

### 2. testphp.vulnweb.com

Entry:  <http://testphp.vulnweb.com>

Start:  2023-04-19 17:06:34

End: 2023-04-19 17:07:32

Severity 

**Informational** - This is a simple information message. It is not a problem, and it is not an error.

**Low risk** - This message is an information message. It is not a problem, and it is not an error.

**Medium risk** - This message is a warning. It is not a problem, but it may become one in the future.

**High risk** - This message is an error. It is a problem, and it must be fixed.

**Debug** - This message is a debug message. It is not a problem, and it is not an error.

## Scan Results

### [High risk] Basic Script - Active / SQL Injection

Detected on: 2023-04-19 17:07:31

```
{
  "request": {
    "request": {
      "url": "http://testphp.vulnweb.com/artists.php?artist=1%27",
      "data": null,
      "headers": {
        "User-Agent": "python-requests/2.28.2",
        "Accept-Encoding": "gzip, deflate",
        "Accept": "*/*",
        "Connection": "keep-alive"
      },
      "cookies": {}
    },
    "response": {
      "code": 200,
      "headers": {
        "Server": "nginx/1.19.0",
        "Date": "Wed, 19 Apr 2023 17:07:29 GMT",
        "Content-Type": "text/html; charset=UTF-8",
        "Transfer-Encoding": "chunked",
        "Connection": "keep-alive",
        "X-Powered-By": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",
        "Content-Encoding": "gzip"
      },
      "content-type": "text/html; charset=UTF-8"
    }
  },
  "match": "Regex Match: error.+?sql was found "
}
```

### [High risk] Basic Script - Active / SQL Injection

Detected on: 2023-04-19 17:07:30

Detected on: 2023-04-19 17:07:30

```
{
  "request": {
    "request": {
      "url": "http://testphp.vulnweb.com/listproducts.php?cat=1%27",
      "data": null,
      "headers": {
        "User-Agent": "python-requests/2.28.2",
        "Accept-Encoding": "gzip, deflate",
        "Accept": "*/*",
        "Connection": "keep-alive"
      },
      "cookies": {}
    },
    "response": {
      "code": 200,
      "headers": {
        "Server": "nginx/1.19.0",
        "Date": "Wed, 19 Apr 2023 17:07:28 GMT",
        "Content-Type": "text/html; charset=UTF-8",
        "Transfer-Encoding": "chunked",
        "Connection": "keep-alive",
        "X-Powered-By": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",
        "Content-Encoding": "gzip"
      },
      "content-type": "text/html; charset=UTF-8"
    }
  },
  "match": "Regex Match: error.+?sql was found "
}
```

## [High risk] Basic Script - Active / SQL Injection

Detected on: 2023-04-19 17:07:29

```
{
  "request": {
    "request": {
      "url": "http://testphp.vulnweb.com/product.php?pic=6%27",
      "data": null,
      "headers": {
        "User-Agent": "python-requests/2.28.2",
        "Accept-Encoding": "gzip, deflate",
        "Accept": "*/*",
        "Connection": "keep-alive"
      },
      "cookies": {}
    }
  }
```

```
    },
    "response": {
      "code": 200,
      "headers": {
        "Server": "nginx/1.19.0",
        "Date": "Wed, 19 Apr 2023 17:07:28 GMT",
        "Content-Type": "text/html; charset=UTF-8",
        "Transfer-Encoding": "chunked",
        "Connection": "keep-alive",
        "X-Powered-By": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",
        "Content-Encoding": "gzip"
      },
      "content-type": "text/html; charset=UTF-8"
    }
  },
  "match": "Regex Match: error.+?sql was found "
}
```

## [High risk] Basic Script - Active / SQL Injection

---

Detected on: 2023-04-19 17:07:28

```
{
  "request": {
    "request": {
      "url": "http://testphp.vulnweb.com/listproducts.php?artist=1%27",
      "data": null,
      "headers": {
        "User-Agent": "python-requests/2.28.2",
        "Accept-Encoding": "gzip, deflate",
        "Accept": "*/*",
        "Connection": "keep-alive"
      },
      "cookies": {}
    },
    "response": {
      "code": 200,
      "headers": {
        "Server": "nginx/1.19.0",
        "Date": "Wed, 19 Apr 2023 17:07:28 GMT",
        "Content-Type": "text/html; charset=UTF-8",
        "Transfer-Encoding": "chunked",
        "Connection": "keep-alive",
        "X-Powered-By": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",
        "Content-Encoding": "gzip"
      },
      "content-type": "text/html; charset=UTF-8"
    }
  }
}
```

```
},  
"match": "Regex Match: error.+?sql was found "  
}
```

## [Low risk] Basic Script - Passive / Server Backend System exposure

Detected on: 2023-04-19 17:07:24

```
{  
  "request": {  
    "request": {  
      "url": "http://testphp.vulnweb.com",  
      "data": null,  
      "headers": {  
        "User-Agent": "python-requests/2.28.2",  
        "Accept-Encoding": "gzip, deflate",  
        "Accept": "*/*",  
        "Connection": "keep-alive"  
      },  
      "cookies": {}  
    },  
    "response": {  
      "code": 200,  
      "headers": {  
        "Server": "nginx/1.19.0",  
        "Date": "Wed, 19 Apr 2023 17:06:58 GMT",  
        "Content-Type": "text/html; charset=UTF-8",  
        "Transfer-Encoding": "chunked",  
        "Connection": "keep-alive",  
        "X-Powered-By": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",  
        "Content-Encoding": "gzip"  
      },  
      "content-type": "text/html; charset=UTF-8"  
    }  
  },  
  "match": "Header x-powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 exists"  
}
```

## [Low risk] Basic Script - Passive / Server header exposure

Detected on: 2023-04-19 17:07:23

```
{  
  "request": {  
    "request": {  
      "url": "http://testphp.vulnweb.com"
```

```

    url : http://testphp.vulnweb.com ,
    "data": null,
    "headers": {
        "User-Agent": "python-requests/2.28.2",
        "Accept-Encoding": "gzip, deflate",
        "Accept": "/*/*",
        "Connection": "keep-alive"
    },
    "cookies": {}
},
"response": {
    "code": 200,
    "headers": {
        "Server": "nginx/1.19.0",
        "Date": "Wed, 19 Apr 2023 17:06:58 GMT",
        "Content-Type": "text/html; charset=UTF-8",
        "Transfer-Encoding": "chunked",
        "Connection": "keep-alive",
        "X-Powered-By": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",
        "Content-Encoding": "gzip"
    },
    "content-type": "text/html; charset=UTF-8"
}
},
"match": "Header server: nginx/1.19.0 exists"
}

```

## [Informational] Basic Script - Filesystem / Admin directory found

Detected on: 2023-04-19 17:06:36

```

{
  "request": {
    "request": {
      "url": "http://testphp.vulnweb.com/admin/",
      "data": null,
      "headers": {
        "User-Agent": "python-requests/2.28.2",
        "Accept-Encoding": "gzip, deflate",
        "Accept": "/*/*",
        "Connection": "keep-alive"
      },
      "cookies": {}
    },
    "response": {
      "code": 200,
      "headers": {
        "Server": "nginx/1.19.0",

```

```
"Date": "Wed, 19 Apr 2023 17:06:36 GMT",
"Content-Type": "text/html",
"Transfer-Encoding": "chunked",
"Connection": "keep-alive",
"Content-Encoding": "gzip"
},
"content-type": "text/html"
}
},
"match": "(Admin directory found) status code: 200 was found"
}
```

© Ritek Rounak